Папій Т.О.,
студентка 6 курсу, 7 групи, факультету адвокатури Національного юридичного університету імені Ярослава Мудрого

ОГЛЯД ПРОБЛЕМАТИКИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ЯК ІНСТРУМЕНТУ ВЧИНЕННЯ КІБЕРЗЛОЧИНІВ

Ключові слова: соціальна інженерія, кіберзлочинність, запобігання кіберзлочинам.

Анотація. У тезах висвітлено проблему використання соціальної інженерії у якості способу вчинення кіберзлочинів. Розглянуто механізм дії та види цього явища. Автором запропоновано ряд заходів щодо протидії атакам із застосуванням методів соціальної інженерії.

Аннотация. В тезисах освещена проблема использования социальной инженерии в качестве способа совершения кибепреступлений. Рассмотрен механизм действия и виды этого явления. Автором предложено ряд мероприятий касательно противодействия атакам с применением методов социальной инженерии.

Ключевые слова: социальная инженерия, киберпреступность, предотвращение киберпреступлений.

Summary. In summaries the problem of using social engineering as a means of cybercrimes is reported. The mechanism and types of this phenomenon are discussed. The author offers a range of measures to counteract social engineering attacks.

Keywords: social engineering, cybercrime, counteraction of cybercrimes.

Сьогодні переважна більшість людей сприймають інформаційні технології та штучний інтелект як повсякденні явища, без яких

комфортне життя у XXI столітті практично неможливе. Разом з тим, діджиталізація різноманітних сфер суспільного буття несе в собі не лише позитивні, але й негативні явища, серед яких визначальне місце посідає кіберзлочинність. Цей феномен не є новим, однак наразі він перейшов на якісно новий рівень. А в умовах пандемії Covid-19, коли значний відсоток населення планети навчається та працює дистанційно, питання безпеки віртуального простору набуває ще більшої актуальності.

Як відомо, складовими компонентами кібербезпеки є технології, процеси та люди. Саме людський фактор є найбільш вразливим серед усіх названих елементів. На ньому і побудований один із поширених інструментів кіберзлочинності – соціальна інженерія. Під нею розуміють маніпулювання індивідами з метою спонукання їх до виконання певних дій або розголошення інформації, яка може бути корисною для зловмисника [1, с. 3]; мистецтво збору інформації, яка не повинна бути розголошена та розповсюджена за нормальних умов, що здійснюється шляхом використання методів впливу та переконання [2, с. 2].

Основу методів соціальної інженерії складають гра на емоціях та природніх слабкостях людини: цікавість, страх, почуття вини, бажання легкого та швидкого збагачення, злість, захват, лінь, довірливість тощо. Успішність соціальної інженерії полягає у використанні мінімальної кількості ресурсів. Так, кіберзлочинцю достатньо зрозуміти мотиви поведінки особи, а потім необхідно лише підібрати найбільш підходящий інструмент маніпуляції для досягнення поставленої мети.

Загалом, можна виокремити декілька етапів кібератаки, побудованої на базі соціальної інженерії. Спеціаліст з питань інформаційної безпеки Dinesh Shetty називає це «життєвим циклом соціальної інженерії» (англ. – *the Social Engineering Life Cycle*). Так, перший етап носить назву *footprinting,* тобто збір інформації. Зловмисник акумулює дані про жертву (жертв) та її оточення. На другому етапі відбувається встановлення довіри, що в подальшому дасть можливість «соціальному інженеру» дізнатися конфіденційну інформацію, яка потенційно здатна завдати шкоди. Третій етап – власне психологічна маніпуляція. Після накопичення всього масиву необхідних даних, кіберзлочинець може перейти до наступної цілі або

продовжувати експлуатацію. І останній крок – «вихід» (*the exit*). Соціальний інженер намагається уникнути підозри та не залишити слідів, які могли б розкрити його справжню особистість або причетність до несанкціонованого входу в певну систему [3]. На цьому етапі також відбувається повне припинення взаємовідносин з жертвою, після того як хакер досяг бажаної мети [4].

Існує різноманітна кількість видів соціальної інженерії, серед яких фішинг (*fishing*) – використовується для отримання облікових даних або поширення шкідливого програмного забезпечення, як правило, через заражені вкладення у електронних листах або посилання на шкідливі веб-сайти; смішинг (*smishing*) або SMS-фішинг; вішинг (*vishing*) або голосовий фішинг, коли жертвам по телефону повідомляють, що їх банківський рахунок зламано і просять ввести їх облікові дані через мобільну клавіатуру, тим самим отримуючи до них доступ; байтинг (*baiting*) – приваблення жертви шляхом безкоштовних роздач (*giveaways*) або розповсюдження заражених пристроїв; претекстинг (*pretexting*) – початкова стадія більш складних атак, коли шахрай завойовує довіру жертви зазвичай шляхом створення передісторії; атаки *quid pro quo* (з лат. «послуга за послугу») апелюють до почуття взаємності, зловмисники пропонують надати щось в обмін на інформацію тощо [5]. Це далеко не повний список всіх видів злочинних дій, які ґрунтуються на методах соціальної інженерії. Кожен з них має свою специфіку і потребує окремого аналізу та подальшого дослідження.

Часто користувачі покладаються на те, що антивірусне програмне забезпечення, вбудовані інструменти веб-браузерів та фільтри електронних скриньок, які відправляють підозрілі листи в папку «Спам», здатні вберегти їх від будь-яких загроз та атак. Але в контексті соціальної інженерії таке твердження є помилковим, оскільки шкідливий програмний код може бути майстерно прихований. Більше того, не виключаються також випадки, коли витік даних відбувається за неусвідомленою згодою особи без застосування будь-яких вірусів та шпіонських додатків (наприклад, у електронному листі зловмисник представляється представником банку та просить надіслати інформацію щодо картки, включаючи її термін дії та CVV-код, а особа довірливо передає ці дані).

На нашу думку, основу протидії соціальній інженерії складає кібергігієна як сукупність рекомендацій та правил поведінки у віртуальному просторі, які здатні застерегти користувачів від потенційних загроз. Ключові заходи в рамках кібергігієни можна поділити на дві групи: пов'язані із застосуванням технологічної складової (1); засновані виключно на поведінці особи (2). Першу групу складають наступні рекомендації: встановлювати ліцензійні програми та додатки, регулярно їх оновлювати; користуватися антивірусним програмним забезпеченням; щоразу перед початком роботи здійснювати сканування Wi-Fi мережі; уникати підключення до публічнихWi-Fi мереж, якщо це неможливо – використовувати VPN-з'єднання; встановити складні паролі для різних акаунтів та налаштувати мультифакторну автентифікацію. Також варто створити на пристрої, з якого відбувається вихід в мережу Інтернет, окремий обліковий запис без прав адміністратора. Цей варіант підходить, зокрема, для убезпечення даних від недосвідчених або тимчасових користувачів, оскільки без повних прав вони не можуть змінювати системні налаштування, інсталювати програмне забезпечення, а у випадку зараження шкідливим кодом, такий код не поширюється за межі облікового запису.

Інша група заходів протидії соціальній інженерії спрямована на підвищення рівня обізнаності людей про потенційні ризики, якими переповнений віртуальний простір та вироблення навичок обачної поведінки в мережі Інтернет. Насамперед, варто навчитися виявляти підозрілі об'єкти.

Перша річ, на що потрібно звертати увагу, – це емоційний підйом, який відчуває людина, коли «соціальний інженер» намагається нею маніпулювати. Будучи особливо зацікавленою, наляканою або схвильованою, особа у меншій мірі здатна оцінити наслідки своїх дій. Другий крок – ідентифікація відправника. Після одержання підозрілого листа або повідомлення необхідно уважно перевірити адресу електронної пошти або профіль відправника у соцмережі. У листі можуть бути символи, що імітують інші, наприклад, «torn@example.com» замість «tom@example.com». Поширені також випадки розповсюдження рейкових акаунтів, у яких дублюється фото «друзів» та інші деталі справжніх профілів. Якщо адресантом є знайома особа, не буде зайвим

запитати її особисто або по телефону, чи дійсно вона відправляла повідомлення відповідного змісту, оскільки не виключено, що її особисту сторінку зламали. У разі, коли невідомий відправник відмовляється підтвердити свою особистість, у жодному разі не потрібно надавати йому доступ до будь-яких даних. По-третє, перебуваючи на сторонніх веб-сайтах, не слід ігнорувати такі деталі, які помилки в URL-адресі, низька якість зображень, старі або неправильні логотипи компаній, опечатки. Нерідко усе це – індикатори підробленого веб-сайту. По-четверте, завжди потрібно раціонально оцінювати ту чи іншу пропозицію. Чи не звучить вона занадто добре, щоб бути правдою? Безкоштовні роздачі та інші методи таргетингу є потужною мотивацією для успішного просування атаки, побудованої на методах соціальної інженерії [4].

Однак, варто погодитись з думкою, що рішучий зловмисник, який має відповідні навички, ресурси та, врешті-решт, везіння, здатний отримати потрібну йому інформацію. У зв'язку з цим організаціям та приватним особам варто розробити план заходів щодо реагування на успішну атаку та відновлення після неї [1, с. 3]. Одним із способів відновлення втраченої інформації є періодичний бекап даних у хмарні сховища (які, у свою чергу, також потребують захисту) та на зовнішні носії. Слід звернути також увагу на обережність багатьох дослідників при формуванні підходів до так званої «нової злочинності» [6; 7, с. 91].

Таким чином, соціальна інженерія представляє собою потужний та ефективний засіб вчинення кіберзлочинів, що пояснюється її маніпулятивною природою та низькою ресурсозатратністю. На сьогодні відомо безліч видів соціальної інженерії, кожен з яких має свої особливі риси. Тому виникає потреба у подальших наукових розробках окресленої проблематики, оскільки лише глибоке розуміння сутності цього феномену допоможе детально розкрити механізм його дії та виявити слабкі місця. Це, у свою чергу, закладає основи методів протидії соціальній інженерії, першочергове місце серед яких займають превентивні заходи.

ЛІТЕРАТУРА:

1. An introduction to social engineering. *UKCERT*. URL: https://info.publicintelligence.net/UK-CERT-SocialEngineering.pdf (дата звернення: 25.10.2020).

2. Tolga Mataracioglu, Sevgi Ozkan. User Awareness Measurement Through Social Engineering. URL: https://arxiv.org/ftp/arxiv/papers/1108/1108.2149.pdf (дата звернення: 26.10.2020).

3. Dinesh Shetty. Social Engineering: The Human Factor. URL: https://www.exploit-db.com/docs/english/18135-social-engineering---the-human-factor.pdf (дата звернення: 25.10.2020).

4. What is Social Engineering? *Kaspersky*. URL: https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering (дата звернення: 25.10.2020).

5. Social Engineering Attacks. *IT Governance.* URL: https://www.itgovernance.co.uk/social-engineering-attacks. (дата звернення: 26.10.2020)

6. Головкін Б. М. Про детермінацію злочинності. *Часопис Київського університету права*. 2020. № 1. С. 274-280. URL: http://kul.kiev.ua//images//A/Chasopis/CHAS20_1.pdf

7. Сметаніна Н. В. Наукові підходи до теорії злочинності у сучасній українській кримінології : монографія / за заг. ред. В. В. Голіни. Харків: Право, 2016. 192 с.

Науковий керівник: к.ю.н, ас. Н. В. Сметаніна