УДК 004.056(075.8)
DOI: 10.31673/2412-9070.2021.041719
М. М. ЗАПОРОЖЧЕНКО, асистент кафедри;
Т. М. ДЗЮБА, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

ЖИТТЄВИЙ ЦИКЛ ТА РІЗНОВИДИ СОЦІОІНЖЕНЕРНИХ АТАК

Сьогодні соціоінженерні атаки є одним із найбільш звичних для зловмисників методів злому комп'ютерних мереж та інформаційних систем організацій, викрадення облікових даних та іншої конфіденційної інформації користувачів та здійснення різноманітних кіберзлочинів. Особливу загрозу соціоінженерні атаки становлять для компаній, в яких працює велика кількість співробітників. Без належного тренування та навчання персоналу атака на співробітника, який не має ніякого стосунку до інформаційної безпеки, з більшою ймовірністю буде успішною, але навіть такий співробітник може хоч і не бути головною причиною інциденту в інформаційній безпеці компанії, але стати однією з ланок у ланцюгу атаки, яку створив зловмисник для досягнення своєї кінцевої мети. З огляду на це, сьогодні нагальною потребою є підвищення обізнаності щодо соціоінженерних атак, а саме в який спосіб вони реалізуються та які їх різновиди існують.

У статті розглянуто життєвий цикл соціоінженерних атак та основні методи, які використовують зловмисники для здійснення таких атак. Співробітники компанії мають на практиці бути ознайомлені з ознаками та прикладами різних типів соціоінженерних атак, принципами та правилами роботи з інформацією, а також відповідальністю за порушення цих правил. Для забезпечення безпеки даних мають бути створені та доведені до персоналу регламенти та інструкції, в яких чітко прописано правила зберігання, оброблення, поширення та передавання інформації третім особам. Підвищення обізнаності співробітників компанії щодо різновидів соціоінженерних атак дасть можливість зменшити кількість інцидентів, які були реалізовані внаслідок них.

Ключові слова: соціальна інженерія; інформаційна безпека; кібербезпека; життєвий цикл атаки; фішинг.

Вступ

Постановка проблеми. Термін «соціальна інженерія» використовується для того, щоб підкреслити участь людського фактора в процесі реалізації атаки. Тобто небезпека соціоінженерних атак полягає в тому, що вони ґрунтуються на помилках людей, а не тільки на вразливостях у програмному забезпеченні чи операційних системах. Помилки авторизованих користувачів системи менш передбачувані, тому їх набагато складніше виявити та попередити, ніж атаки, що базуються на шкідливому програмному забезпеченні. Через це дуже важливим є підвищення обізнаності користувачів щодо методів, якими зловмисники можуть послуговуватися, аби змусити користувача допомогти їм провести вдалу атаку.

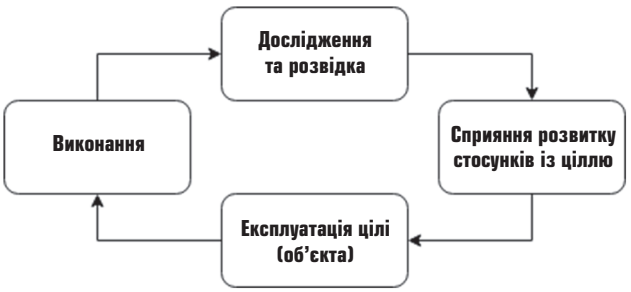
Аналіз останніх досліджень і публікацій. До наукових розвідок, присвячених проблемам соціальної інженерії, можна віднести публікації авторів: Zuoguang Wang, Hongsong Zhu, Limin Sun [1], Nina Klimburg-Witjes, Alexander Wentland [2], Chloe Pilette [3], D. E. Capano [4].

Метою статті є підвищення обізнаності щодо етапів реалізації та різновидів соціоінженерних атак.

Основна частина

Соціоінженерні атаки передбачають маніпулювання людьми з метою досягнення цілей зловмисником — здобуття конфіденційної інформації чи доступу до мережі, системи, приміщення тощо. Для цього зловмисник виконує певні дії.

У простішому випадку цикл соціоінженерної атаки складається з чотирьох основних фаз: підготовчої (дослідження і розвідка), установлення та розвитку стосунків та взаєморозуміння з ціллю, експлуатації цілі та виконання (використання здобутих даних, доступу тощо) (рисунок).



Життєвий цикл соціоінженерної атаки

Проте іноді цикл атаки або окремі його етапи можуть повторюватись залежно від обставин [2]. Наприклад, повторення циклу атаки може бути необхідним у разі, коли зловмисник не може відразу дістатися до потрібної йому цілі без інформації, яку він має спочатку отримати від проміжних цілей — його колег, друзів, родичів та ін.

Підготовчий етап є найважливішим, оскільки від нього залежить, наскільки успішною буде вся атака, тому на цей етап витрачається найбільша кількість часу. Першочергово соціальний інженер вибирає ціль залежно від її статусу в організації, легкості доступу тощо. Основною метою для нього на цьому етапі є збір якомога більше даних про його ціль. Зловмисника може зацікавити

така інформація, як місце роботи та посада, інформація про друзів, родичів, інтереси тощо, а також соціальні мережі, телефони, електронна пошта для встановлення подальшого зв'язку. На основі зібраної інформації зловмисник може визначити найвдаліший метод та вектор атаки, створити реєстр можливих паролів, заздалегідь підготувати перелік питань та можливих відповідей з боку цілі. Також важливим завданням є формулювання вагомих приводів для стимулювання цілі виконати необхідні дії для зловмисника.

На наступному етапі зловмисник вступає в контакт із ціллю та встановлює з нею робочі стосунки, рівень яких буде впливати на рівень співпраці та міру того, що саме може зробити ціль, аби допомогти зловмиснику. В окремих випадках зловмисник видає себе за надійне джерело, наприклад за співробітника технічної підтримки в компанії, в якій працює ціль. Основне завдання цього етапу — за допомогою різноманітних прийомів соціальної інженерії ввійти в довіру та стимулювати ціль для подальших дій, зокрема розкриття конфіденційної інформації або інформації, потрібної для подальшого розвитку атаки, надання доступу до критично важливих ресурсів тощо.

На етапі експлуатації зловмисники використовують інформацію і стосунки, здобуті на попередніх етапах. Експлуатація може проявлятися в розголошенні навіть незначної інформації або наданні доступу зловмиснику. Прикладами успішної експлуатації можуть бути, скажімо, потрапляння зловмисника всередину приміщення, завантаження зараженого вкладення чи перехід за шкідливим посиланням, переданими електронною поштою, розкриття облікових даних користувача, комерційної таємниці тощо.

Реалізація останнього етапу — виконання — зазвичай свідчить про те, що зловмисник досягнув своєї кінцевої цілі або йому необхідно було припинити атаку, аби не викликати підозри. Найчастіше атаки закінчуються до того, як ціль починає вагатися, і зловмисник намагається забезпечити можливість подальшої взаємодії, створюючи враження того, що він зробив щось добре та корисне для когось. Також важливим завданням зловмисника на цьому етапі буде видалення всіх ознак упровадженого шкідливого програмного забезпечення та інших слідів своєї активності. В ідеалі зловмисник дістає одразу дві переваги: по-перше, ціль не зрозуміє, що було реалізовано атаку, а по-друге, зловмисник не викриє свою особу.

Найбільш поширеним типом соціоінженерних атак є ***фішингові атаки***, які здебільшого розповсюджуються електронною поштою та містять прикріплені файли, завантаження або відкриття яких може призвести до зараження комп'ютера, на якому їх було відкрито, або шкідливі посилання, котрі можуть перенаправляти користувача на клон сайту, де зловмисник має змогу вкрасти його облікові дані. Зібравши достатньо інформації, зловмисник може здійснити цільову фішингову атаку, спрямовану на конкретного користувача. Тематика листів може бути будь-якою: це й лист від імені особи, яку знає жертва та якій вона довіряє, або ж, проаналізувавши інтереси жертви, зловмисник може написати листа з посиланням на курси, виставку тощо, що ймовірно зацікавить ціль [3].

Лякаюче програмне забезпечення (Scareware) — це шкідливе програмне забезпечення, яке має на меті налякати жертву, а отже, стимулювати її швидко виконати певні дії, не даючи при цьому шанс на роздуми. Такий тип соціоінженерної атаки зазвичай має вигляд спливаючих вікон або електронних листів, в яких зазначено, що пристрій жертви під загрозою, та щоб позбутися вірусів або шкідливих програм потрібно негайно виконати певні дії, заздалегідь прописані зловмисником, у такий спосіб надаючи йому доступ до важливих даних або взагалі до керування комп'ютером.

Злам електронної пошти та розсилка спаму контактам. Такий тип атак передбачає розсилку зловмисником спаму зі скомпрометованої електронної пошти переліку наявних у ній контактів. Оскільки отримання листа від знайомого скоріш за все не викличе підозри у звичайного користувача, це сприятиме поширенню шкідливого програмного забезпечення та заволодінню зловмисником облікових даних користувачів, які стали жертвами такого типу атак.

Претекстинг — це тип атаки, який передбачає попереднє створення переконливих сценаріїв для того, щоб змусити жертву повірити зловмиснику та допомогти йому, надавши доступ до своїх облікових даних чи іншої необхідної зловмиснику інформації, а також доступ у захищуване приміщення тощо. Для створення правдоподібних сценаріїв зловмисники використовують OSINT, тобто розвідку по відкритих джерелах, і використовують інформацію з опублікованих документів, соціальних мереж тощо. Претекстинг є фундаментом для великої кількості інших типів соціоінженерних атак.

Access tailgating. Буквально цей тип атаки означає прохід системи контрою доступу за авторизованим користувачем. Такий тип фізичних атак доволі поширений та застосовується тоді, коли зловмиснику необхідно потрапити до захищеного приміщення або майданчика, до якого він не має доступу. Для цього використовуються психологічні прийоми, у разі вдалої реалізації яких зловмисник потрапить всередину, наприклад, під прикриттям авторизованого користувача або ско-

риставшись його ID-карткою. Така атака здійснюється в сукупності з претекстингом, аби переконати ціль у щирості та законності своїх дій. Способів реалізації такої атаки дуже багато: зловмисник може видавати себе за іншого співробітника компанії, за працівника доставки або обслуговувальний персонал, або ж обманом та переконанням попросити ціль пропустити його всередину.

Приманка (baiting). Цей тип атак експлуатує такі вразливості людини, як цікавість та жадібність. У класичному випадку варіантом такого типу атак є використання зараженого USB-нагромаджувача, який залишають у тому місці, де його може знайти ціль та зацікавитися ним: це може бути автостоянка чи столик у ресторані або інші місця, які часто відвідує ціль; одне з приміщень офісу, куди зміг потрапити зловмисник за допомогою тейлгейтингу. Такі USB-нагромаджувачі зазвичай мають особливий вигляд, який привертає до себе увагу. Так, наприклад, на них може бути нанесено логотип компанії або написано щось на кшталт «фінансовий звіт», або прізвище співробітника компанії. Під час підімкнення такого нагромаджувача на комп'ютер завантажується шкідливе програмне забезпечення, яке надає доступ до мережі зловмиснику. Використовуючи флешку-приманку, зловмисник може потрапити навіть усередину системи, яку не підімкнено до зовнішньої мережі.

Висновки

Здебільшого передусім саме співробітники компанії, які не мають відношення до інформаційної безпеки, стають жертвами соціальних інженерів. З огляду на тенденцію до зростання кількості випадків соціоінженерних атак та кількості їх різновидів застосування лише програмних та технічних засобів захисту, найімовірніше, не надасть належного захисту, оскільки з появою нових засобів захисту в зловмисників з'являються і нові ідеї, в який спосіб їх можна обійти за допомогою співробітників компанії. Тому для зменшення кількості інцидентів, причиною яких стали соціоінженерні атаки, потрібно проводити регулярне навчання та тестування персоналу компанії, щоб забезпечити мінімум навичок: знати, як саме зберігати, поширювати, використовувати та видаляти інформацію, яку інформацію можна передавати третім особам і в якому разі, а також уміти розпізнавати соціоінженерні, особливо фішингові атаки.

Список використаної літератури

*1. **Wang Z., Sun L., Zhu H.** Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods // IEEE Access. 2021. Vol. 9. P. 11895–11910. [Електронний ресурс]. URL:*

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9323026

*2. **Klimburg-Witjes N., Wentland A.** Hacking Humans? Social Engineering and the Construction of the «Deficient User» in Cybersecurity Discourses // Science, Technology, & Human Values. 2021. Vol. 46, issue 6. P. 1316–1339. [Електронний ресурс]. URL:*

https://journals.sagepub.com/doi/full/10.1177/0162243921992844

*3. **Pilette C.** What is social engineering? A definition + techniques to watch for. 2021. [Електронний ресурс]. URL:*

https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

*4. **Capano D. E.** Understand the cyber-attack lifecycle. Control Engineering. 2019. [Електронний ресурс]. URL:*

https://www.controleng.com/articles/understand-the-cyber-attack-lifecycle/

М. М. Запорожченко, Т. М. Дзюба

ЖИЗНЕННЫЙ ЦИКЛ И РАЗНОВИДНОСТИ СОЦИОИНЖЕНЕРНЫХ АТАК

Сегодня социоинженерные атаки являются одним из наиболее привычных для злоумышленников методов взлома компьютерных сетей и информационных систем организаций, кражи учетных данных и другой конфиденциальной информации пользователей и совершения различных киберпреступлений. Особую угрозу социоинженерные атаки представляют для компаний, в которых работает большое количество сотрудников. Без надлежащей тренировки и обучения персонала атака на сотрудника, не имеющего отношения к информационной безопасности, с большей вероятностью будет успешной, но даже такой сотрудник может хоть и не быть основной причиной инцидента в информационной безопасности компании, но стать одним из звеньев в цепи атаки, которую создал злоумышленник для достижения своей конечной цели. Учитывая это, сегодня насущной необходимостью является повышение осведомленности о социоинженерных атаках, а именно каким образом они реализуются и какие их разновидности существуют.

В статье описан жизненный цикл социоинженерных атак и основные методы, которые используются злоумышленниками для реализации таких атак. Сотрудники компании должны на практике ознакомиться с признаками и примерами различных типов социоинженерных атак, принципами и правилами работы с информацией, а также ответственностью за нарушение этих правил. Для обеспечения безопасности данных должны быть созданы и доведены до персонала регламенты и инструкции, в которых четко прописаны правила хранения, обработки, распространения и передачи информации третьим лицам. Повышение осведомленности сотрудников компании по разновидностям социоинженерных атак позволит уменьшить количество инцидентов, реализованных в результате их возникновения.

Ключевые слова: социальная инженерия; информационная безопасность; кибербезопасность; жизненный цикл атаки; фишинг.

M. M. Zaporozhchenko, T. M. Dzyuba

SOCIAL ENGINEERING ATTACKS LIFE CYCLE AND TYPES

Today, social engineering attacks are one of the most common methods for hackers to hack computer networks and information systems of organizations, steal credentials and other confidential information of users, and commit various cybercrimes. Socio-engineering attacks pose a particular threat to companies with large numbers of employees. Without proper training and education of staff, an attack on an employee who is not related to information security is more likely to be successful, but even such an employee may not be the main cause of a company's information security incident, but become one of the links in the attack chain. which the attacker created to achieve his ultimate goal. Given this, the need to raise awareness about socio-engineering attacks, namely how they are implemented and what types of them exist. This article describes the life cycle of social engineering attacks and the main methods that are used by attackers to implement such attacks. Company employees should be familiar with the signs and examples of various types of social engineering attacks in practice, the principles and rules for working with information, as well as the responsibility for violating these rules. To ensure data security, regulations and instructions should be created and communicated to the personnel, which should clearly spell out the rules for storing, processing, distributing and transferring information to third parties. Raising the awareness of the company's employees about the types of social engineering attacks will reduce the number of incidents implemented as a result of their occurrence.

Keywords: social engineering; information security; cybersecurity; attack life cycle; phishing.

УДК 004.738.5+681.5

DOI: 10.31673/2412-9070.2021.042025

М. О. МАКАРЦЕВ, магістр;
А. М. ТУШИЧ, доктор філософії, доцент;
І. В. ЗАМРІЙ, канд. техн. наук, доцент;
Л. Т. АЛЕКСІНА, ст. викладач,
Державний університет телекомунікацій, Київ

ПРОБЛЕМИ, ТРУДНОЩІ і МОЖЛИВОСТІ IoT ТА ХМАРНИХ ОБЧИСЛЕНЬ

З розвитком Індустріального Інтернету речей (IIoT) спостерігається постійне зростання обсягу інформації. Проте недоцільно зберігати всі необроблені дані в пристроях IIoT, оскільки енергія кінцевих пристроїв не є невичерпною, а додаткові приміщення жорстко обмежені. Мережі IoT розширюють можливості присвоєного асортименту інформації та розподіленого сховища, незалежно від штучної природи IoT. Існує низка невизначених гарантій для проблем IoT та інтеграції у хмару. Хмарні обчислення є високоефективними, зберігання стає дедалі актуальнішим, і деякі групи зараз пересилають свої дані з власних записів у центри постачальників хмарних обчислень. Інтенсивні програми IoT для робочих навантажень і даних можуть спричинити труднощі під час використання розподілених обчислювальних апаратів. У статті досліджено IoT та хмарні обчислення, а також розглянуто сумісні з хмарою проблеми та обчислювальні техніки для сприяння стабільному переходу програм IoT до хмари.

Ключові слова: Інтернет речей; IoT; хмарні обчислення; безпека; IoT-хмара.

ВСТУП

Публічна хмара та IoT — це дві окремі, але міцні системи, інтегровані, щоб стати важливою частиною майбутнього інтернету. Ці інтеграції розглядаються як величезний диверсійний процес із великими перевагами в майбутньому. Значна зміна вноситься в IoT та хмару. Для розв'язання проблем, що постали в процесі аналізу інтеграції IoT з хмарними обчисленнями, нам знадобиться відповісти на такі запитання:

• Яка потреба в інтеграції IoT з хмарними обчисленнями?

• Чи спричинить інтеграція IoT з хмарою будь-які проблеми?

Мета статті полягає у вивченні можливостей та проблем застосування IoT та хмарних обчислень, вирішенні проблем, сумісних із хмарою, та обчислювальних технік для сприяння стабільному переходу програм IoT до хмари.

ОСНОВНА ЧАСТИНА

Останніми роками хмарні обчислення та IoT дуже швидко поширились у всьому світі. Характеристики, які вони демонструють, можуть бути доволі корисними в поєднанні. Кожен із них справді особливий і важливий один для одного. Оскільки IoT отримує допомогу від хмарного сховища та обчислювальних можливостей, дослідники запланували низку програм, що стосуються координації хмари та Інтернету речей, для розроблення та нагромадження даних. Архітектуру Cloud-IoT (Cloud and IoT), в якій прикладний, мережний та сенсорний рівні знань взаємозв'язані, зображено на рис. 1.

Об'єкти, здатні зчитувати та збирати дані через різні системи IoT, розміщують через протоколи візуалізації IoT. Для полегшення оброблення ці знання можуть упорядковуватися в хмарі. Прикладний рівень може сприймати дані навколиш-