УДК 004.056:004.07

К. Р. Салієва

НЕБЕЗПЕКА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В ІТ-КОМПАНІЯХ

Вінницький національний технічний університет

Анотація

Розглянуто небезпеку соціальної інженерії, що загрожує сучасним ІТ-компаніям, та наслідки впливу на роботу компанії. Запропоновано методи боротьби, порядок дій та розроблено пропозиції для запобігання від майбутніх загроз.

Ключові слова: соціальна інженерія, безпека, методи захисту, ІТ-компанії, захист компаній, персонал, інформаційна безпека, людський чинник, небезпека, електронна пошта.

Annotation

The dangers of social engineering that threaten modern IT companies and the consequences of the impact on the company's work are considered. Methods of struggle, the order of actions are offered and offers for prevention of the future threats are developed.

Keywords: social engineering, security, protection methods, IT companies, company protection, personnel, information security, human factor, danger, e-mail.

Вступ

Нині кількість атак соціальної інженерії в Україні набирають великих обертів, тому що саме людський фактор стає найголовнішою проблемою в усіх масштабних атаках, адже зловмисники цим уміло користуються не витрачаючи лишній час і зусилля. Навіть досвідчений спеціаліст ІТ-компанії може бути легкою мішенню соціальної інженерії через особистісні та професійні слабкості. Завдяки цьому серйозному недоліку кіберзлочинці проводять атаки на персонал успішних організацій, витягуючи через них конфіденційні дані. Часто такі атаки проходять доволі успішно і компанії несуть великі матеріальні втрати. Багато відомих закордонних та вітчизняних вчених вивчали та досліджували проблему соціальної інженерії, а саме: В. Л. Бурячок, В. Б. Толубков, В. О. Хорошко, С. В. Толюпа, М. Якобссон, Кевин Д. Митник та Вільям Л. Саймон.

Метою роботи є огляд небезпеки соціальної інженерії в ІТ-компаніях та розроблення методу боротьби, порядку дій та запропоновано ряд порад для запобігання атак в майбутньому.

Результати дослідження

Термін «соціальна інженерія» використовується для широкого спектра шкідливих дій, які здійснюються через взаємодію з людьми. Вона уміло використовує психологічні маніпуляції та слабкості, щоб обманними шляхами змусити користувачів знехтувати своєю безпекою через цікавість або несвідомо видати конфіденційну інформацію третій особі.

Соціальна інженерія відбувається в декілька етапів: спочатку зловмисник збирає для себе всю необхідну інформацію, яка стосується його майбутньої жертви; потім зловмисник намагається втертися в довіру до жертви та спонукати її зробити дії, які порушують безпеку, наприклад, розголошення конфіденційної інформації або надання доступу до критичних ресурсів. Найбільшою небезпекою соціальної інженерії є її орієнтування на людські помилки, а не на проблемне програмне забезпечення (ПЗ) та вразливі операційні системи (ОС). Помилки, які були допущені працівником, набагато важче виявити та запобігти, ніж вторгненню на основі зловмисного ПЗ [1].

Соціальна інженерія має небезпечні та різноманітні методи атак, що є доволі ефективними та розповсюдженими. Вони використовують такі вектори нападу, якими людина користується та зустрічається в повсякденному житті: телефон, онлайн, цифрове сміття, використовують фізичні та особисті підходи, застосовують реверсивну соціальну інженерію. Але, окрім цього, необхідно також знати й про мету нападу та ціль зловмисника. Найчастіше це соціальне становище і самоствердження, гроші.

Серед методів соціальної інженерії можна виділити наступні види: претекстінг, фішинг, троянський кінь, послуга за послугу, дорожнє яблуко, байтинг, зворотна соціальна інженерія, дружні листи, вішинг та контакти. Всі ці методи є небезпечними та обманливими, але на сьогодні в компаніях працівники найбільше стають жертвами від найвідоміших та простих методик – спаму та фішингу. Листи з незрозумілим наповненням, що приходять на електронні пошти, SMS та соціальні мережі, стають найбільшою проблемою працівників, адже хто б не хотів виграти мільйон доларів або поїхати на відпочинок. Сторонні особи, що втерлися в довіру, починають обманними шляхами або погрозами виманювати конфіденційну інформацію у нетямущого працівника. Через це IT-компанії й стають жертвами соціальної інженерії через простий людський фактор [2].

Для того, щоб захистити свою компанію від соціальної інженерії, керівництво повинне сформувати глобальну культуру безпеки, зокрема: поінформованість, відповідальність, реагування, етика, демократія, оцінка ризику, проектування та провадження засобів забезпечення безпеки, управління забезпеченням безпеки, переоцінка. Також можна виділити та запропонувати наступні заходи [3]:

– проводити ретельний підбір кадрів, наголосити працівникам про важливість інформації;

– визначити кому можна розголошувати її та надавати доступ, обмежити права користувача в системі, на комп'ютерах кожного працівника має обов'язково бути антивірусне ПЗ;

– проводити навчальні лекції, інструкції та тестування для працівників про небезпеку соціальної інженерії та як убезпечити себе від неї, наголосити про те, що потрібно бути пильними щодо джерела, яке запитує конфіденційні дані, ніколи не відкривати підозрілий вміст додатків та скептично ставитися до отриманих повідомлень, ні в якому разі не довіряти особам, що намагаються вивідати інформацію.

Також необхідно, щоб управлінням інцидентами кібербезпеки займалися кваліфіковані та довірені спеціалісти фірми, які швидко та професійно зможуть виправити подію, яка все-таки трапилася. Лише правильно донесена інформація до працівників може унеможливити атаки соціальної інженерії на IT-компанії, але потрібно пам'ятати, що повністю убезпечити себе на 100% неможливо.

Висновки

На сьогодні через велику конкуренцію між компаніями в IT-сфері поширюється використання методів «нечесної» боротьби за лідерство та першість на світовому ринку. Працівники IT-компаній стають мішенями для кіберзлочинців. Компаніям перш за все потрібно подбати про свою та безпеку інших людей, що працюють безпосередньо на їх просторах.

Починати укріплювати безпеку компанії від соціальної інженерії потрібно від навчання працівників: надавати інструкції щодо атак, особливо фішингових, регулярно проводити навчання та тестування. Персонал повинен знати принципи роботи з корпоративними даними та усвідомлювати всю відповідальність, яка покладена на них. Адміністрація повинна розробити регламент та інструкції стосовно зберігання, використання, розповсюдження та передачі інформації третім особам. Працівники мають знати, яку інформацію вони мають право розголошувати, а яку ні. Якщо трапиться спроба сторонньої особи отримати доступ до конфіденційної інформації, персонал повинен доповісти негайно про подію службі безпеки IT-компанії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Social Engineering [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.imperva.com/learn/application-security/social-engineering-attack/.

2. Власьєв К. Є. Загрози і захист від соціальної інженерії / К. Є. Власьєв. // Науково-технічний журнал "Захист інформації". – 2010. – №2. – С. 24.

3. Кібербезпека в цифровому навчальному середовищі [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://core.ac.uk/download/pdf/233898878.pdf.

Салієва Катерина Рустамівна - студентка групи КІТС-18б, факультет менеджменту інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: kate228778@gmail.com

Kateryna Salieva - student of the KITS-18b group, Faculty of Management Information Security, Vinnitsa National Technical University, Vinnitsa, email: kate228778@gmail.com