УДК 004.056
В. Єпур
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА МЕТОДОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ВІД АТАК ЧЕРЕЗ ПОСЕРЕДНИКА НА ПІДПРИЄМСТВАХ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

UDC 004.056
V. Yepur

DEVELOPMENT OF INFORMATION PROTECTION METHODOLODY AGAINST MAN-IN-THE-MIDDLE ATTACKS IN SMALL AND MEDIUM-SIZED BUSINESSES

Атака посередника (MITM) – одна з найрозповсюдженіших типів кібератак. Суть атаки полягає у втручанні зловмисника в процес передачі даних між двома користувачами. Результатом цього несанкціонованого втручання може бути перегляд, редагування та видалення даних. При цьому ні відправник, ні отримувач даних не підозрює в існуванні третьої особи, яка здійснює несанкціоновані дії з інформацією.

Захист інформаційно-комунікаційних систем на підприємствах малого та середнього бізнесу часто залишається поза увагою, оскільки це потребує впровадження додаткових методів захисту, спеціаліста та, відповідно, фінансових затрат. Через це на підприємствах часто свідомо або несвідомо йдуть на ризики бути підданим «атаці через посередника».

Тому актуальним є завдання пошуку методології захисту від даного типу атаки, які можуть бути застосовані та використані на невеликих підприємствах для посилення стійкості до кібератак з боку зацікавлених осіб.

Серед розповсюджених методів атаки через посередника, які можуть бути застосовані на незахищених підприємствах, є «Підміна IP-адреси», «Викрадення електронної пошти», «Підміна HTTPS» «Підслуховування по Wi-Fi» [1]. Для захисту від даних типів атак можна використовувати прості програмні та організаційні методи запобігання та попередження. Серед них – використання VPN, використання захищених програм для обміну даних, запобігання фішінговому шахрайству.

В ході дослідження було проаналізовано вимоги чинного законодавства до забезпечення інформаційного захисту на підприємствах. Також досліджено вже існуючі методи реалізації атаки через посередника. Виконано порівняння існуючих методів забезпечення захисту від різних типів атак. На основі проведених досліджень було розроблено методологію захисту від атак через посередника, яка може бути використана на підприємствах малого та середнього бізнесу. Необхідність використання методології захисту обумовлена вимогами чинного законодавства та нормативно–правовими документи, які регламентують вимоги до зберігання та використання даних в інформаційно-комунікаційних системах підприємств.

Для досягнення стійкого захисту бажано застосовувати спеціалізоване програмне забезпечення для вчасного виявлення спроби реалізації атаки через посередника та використовувати багатофакторну автентифікацію (MFA) [2]. Використання додаткових методів перевірки користувача може перешкодити зловмиснику отримати доступ до важливої інформації та до фінансів. Це забезпечує конфіденційність, цілісність та доступність інформації під час її передачі по незахищеним каналам зв’язку, коли існують найбільші ризики реалізації атаки через посередника.

Література.

1. How to defend against man-in-the-middle attacks. URL: https://www.itgovernance.eu/blog/en/how-to-defend-against-man-in-the-middle-attacks. Last accessed: 27.11.2021.
2. Prevent a Man-in-the-Middle Cyberattack. URL: https://www.fool.com/the-blueprint/mitm/. Last accessed: 27.11.2021.