Секція 1

АНАЛІЗ ЗАГРОЗ, СПРЯМОВАНИХ НА МЕДИЧНІ ЗАКЛАДИ ЗІ СПІЛЬНИМ СЕРВЕРОМ ТА ДОСТУПОМ ДО НЬОГО МЕДИЧНИХ ПРАЦІВНИКІВ

Рябко І. Б.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Желтухін О. В.

Актуальність. За останні роки стало очевидним, що кібербезпека в медичних установах є критично важливою проблемою. Зростаюча кількість витоків медичних даних та вразливість серверів у медичних закладах викликали серйозні обурення і підкреслили необхідність удосконалення заходів безпеки в цьому секторі [1, 2].

Метою нашої дослідницької роботи є ретельний аналіз угроз серверам медичних установ, що виникають через користувачів, а також розробка практичних рекомендацій для запобігання подібним загрозам. Ми прагнемо розкрити сутність ризиків та визначити стратегії для підвищення кібербезпеки в цій галузі [3].

Основні положення. Однією з ключових загроз є витоки медичних даних та ідентифікаційної інформації пацієнтів через недбалість або помилки користувачів [1]. Деякі із цих витоків можуть призвести до надзвичайно серйозних наслідків, таких як порушення конфіденційності та незаконний доступ до особистих медичних записів пацієнтів [2].

Розглянемо приклад фішинг-атаки на медичних працівників. Зловмисник створює підроблену електронну пошту, видаючи себе за офіційне джерело. Пошта може містити додатковий файл або посилання на веб-сторінку для введення облікових даних. Зловмисник розсилає листи медичним працівникам з медичної організації, видаючи себе за важливе повідомлення з безпеки, яке потребує входу в систему. Якщо медичний працівник не підозрює обману і натискає на посилання або відкриває доданий файл, зловмисник отримує доступ до його облікових даних. Після отримання доступу до облікових даних медичного працівника, зловмисник може проникнути в систему медичної організації, звертаючись до даних пацієнтів або порушуючи цілісність медичних записів. Зловмисник може отримати доступ до медичних даних пацієнтів, що може призвести до витоку чутливої інформації. Зловмисник може змінювати медичні записи, що може вплинути на якість медичної допомоги та безпеку пацієнтів. Атака може призвести до блокування доступу медичних працівників до даних, що може призупинити надання медичної допомоги. Витік даних і атаки можуть завдати серйозної шкоди репутації медичної організації.

Заходи безпеки, такі як встановлення потужних паролів, двофакторної аутентифікації та обмеження прав доступу, виявляються надзвичайно

важливими для захисту серверів медичних установ від недозволених дій користувачів [3]. Освіта та навчання медичного персоналу щодо кібербезпеки також можуть сприяти усвідомленню ризиків та зниженню ймовірності помилок, оскільки більшість атак відбуваються саме за допомогою фішингу електронних пошт працівників [4].

Висновки. У звязку із зростаючою загрозою витоків медичних даних через користувачів, медичні установи повинні приділити особливу увагу кібербезпеці. Комплексний підхід до цієї проблеми, включаючи технічні, організаційні та навчальні заходи, є надзвичайно важливим для захисту даних пацієнтів та забезпечення довіри до медичних установ. Забезпечення безпеки медичних даних на серверах вимагає постійної уваги і зусиль для запобігання потенційним загрозам.

Список літератури

1. Kim, D. S., Lee, S. M., & Koo, H. J. (2015). «Data breach and medical identity theft: The growing epidemics.» Healthcare Informatics Research, 21(1), 1-3.;
2. Raghavan, S., Peterson, R., Xiong, X., & Du, W. (2017). «Patient identity theft: Prevention and detection.» Health Informatics Journal, 23(3), 187-199.;
3. Reid, P., Fan, J., & Small, D. (2018). «Patient information breach threats: A healthcare provider perspective.» Healthcare Management Science, 21(4), 545-558.;
4. Nursing Informatics for the Advanced Practice Nurse: Patient Safety, Quality, Outcomes, and Interprofessionalism, Second Edition. (2016). Springer Publishing Company. (Chapter 10: Health Information Systems, p. 181-194);
5. Hoyt, R. E., & Yoshihashi, A. K. (2017). Health Informatics: Practical Guide for Healthcare and Information Technology Professionals. Lulu. (Chapter 9: Information Security and Confidentiality, p. 137-155).

Відомості про авторів

Рябко Іван Богданович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.b.ryabko@student.csn.khai.edu
Желтухін Олександр Васильович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.zheltukhin@csn.khai.edu