Секція 1

АНАЛІЗ АТАК НА СИСТЕМУ eHealth МОЗ УКРАЇНИ

Храмцов М. Ю.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Пєвнєв В.Я.

Актуальність. Цифровізація охорони здоров'я почалася 2016 року з Концепції реформи фінансування, яка вбачає якісний доступ до медичної допомоги. Медичні дані вважаються чутливими. Електронна система охорони здоров'я eHealth – це інструмент для забезпечення прозорості процесів в охороні здоров'я [1]. І найголовніше – це система, якій люди довіряють дані про своє здоров'я.

В Україні в цілях забезпечення захисту персональних даних, до яких стосуються і дані про стан здоров'я, біометричні або генетичні дані, діє Закони України «Основи законодавства України про охорону здоров'я» [2] та «Про захист персональних даних». Саме вони регулюють питання забезпечення захисту персональних даних у сфері охорони здоров'я.

Мета. Провести аналіз можливих загроз щодо захисту персональних даних, які використовуються в системі охорони здоров'я eHealth.

Основні положення. Персональні дані пацієнтів у електронну систему eHealth можуть вводити лише визначені медичним закладом уповноважені особи. В електронній системі працює етап підтвердження входу - CAPTCHA - автоматизований комп'ютерний тест, який аналізує «поведінку» користувача при вході та може відрізнити людину від бота. На програмному рівні безпечний доступ ґрунтується на технології двофакторної авторизації протоколу Oauth.2 [3]. Саме цей протокол забезпечує верифікацію входу та розгалуження прав доступу до даних.

Передача інформації здійснюється у зашифрованому вигляді згідно з вимогами законодавства. Додатково в системі реалізовано принцип відокремленого зберігання персональних та медичних даних пацієнта. Однак ризики щодо стороннього втручання у дану платформу досі існує. Одними із можливих атак на систему eHealth може бути [4]:

– denial of service (DoS attack) — мережева атака, завданням якої є перенавантаження компонентів комп'ютерних систем;

– malware — запуск усередину комп'ютера шкідливого програмного забезпечення (віруси, трояни);

– phishing — атака з використанням технічних засобів і засобів соціальної інженерії з метою введення в оману авторизованих користувачів;

– ransomware — запуск всередину комп'ютера шкідливого програмного забезпечення, що шифрує дані або робить їх копію;

– man-in-the-middle — мережева атака, завданням якої є додавання стороннього користувача до вже наявного каналу зв'язку між двома системами;

– zero-day exploit — атака на вразливі місця ліцензованого програмного забезпечення, задля втручання в нього та виконання потрібних хакеру задач;

– cross-site scripting (XSS) — атака на користувачів безпечного сайту внаслідок додавання до нього небезпечного коду;

– logic bombs — атака за допомогою легальних програм через додавання до них шкідливого коду, що виконується за певних умов.

Висновки. Електронні реєстри не дають можливості так легко отримати інформацію, але особи, які мають спеціальні знання та навички роботи в комп'ютерних системах, здатні на це.

Незважаючи на безліч плюсів електронної медицини вона має низку недоліків. І основний з них — ризик, що персональні дані пацієнта з легкої руки кіберзлочинців можуть опинитися в руках шахраїв.

Список літератури

4. Кожне робоче місце підключено до електронної системи охорони здоров'я. URL: https://nszu.gov.ua/academy/osnovni-kroki-2020/pidkluch-mic (дата звернення: 18.06.2022);

5. Закон України «Основи законодавства України про охорону здоров'я». URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text (дата звернення: 20.06.2022);

6. Як захищений вхід до системи eHealth. *Ezdorovya*. URL: https://www.facebook.com/ezdorovya/posts/ (дата звернення: 22.06.2022);

7. What is a Cyber Attack? *IBM*. URL – https://www.ibm.com/topics/cyber-attack (дата звернення: 24.06.2022).

Відомості про авторів

Храмцов Микола Юрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 095-304-66-95, nickthomson769@gmail.com

Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu