ЗАХИСТ ІНФОРМАЦІЇ В МЕДИЧНИХ ПРОГРАМНИХ ЗАБЕЗПЕЧЕННЯХ В УМОВАХ ВІЙНИ

НТУ «Дніпровська політехніка»

Шипаєва Діана Володимирівна
***Науковий керівник*: д.т.н., проф. Лактіонов Іван Сергійович**

В наш час з розвитком технологій, автоматизація торкається всіх сфер людського життя, одна з них є медична. В Україні було запроваджено систему eHealth, що є центральною базою даних для зберігання та обробки медичної інформації. Доступ до цих даних має Міністерство охорони здоров'я, НСЗУ та медичні установи, які підключенні до системи. Лікарня або приватні медичні заклади мають змогу підключитися до ЦБД через медичну інформаційну систему (МІС).

МІС для медичного закладу – це інструмент, призначений не тільки для передавання даних в ЦБД eHealth, але також для вирішення локальних питань управління медичним закладом [1]. До її роботи входять такі функції як: онлайн запис до лікаря, отримання електронного рецепта, телемедицина та інше. Впровадження МІС дає змогу ефективно використовувати дані та істотно зменшує час, що витрачається на паперову документацію.

Але, важливим постає питання інформаційної безпеки даних, які використовуються в МІС. Медичні установи є одні з важливих інституцій в Україні, передусім у військовий час, коли в лікарнях знаходяться військові, конфіденційність яких є одним з пріоритетів. Починаючи від ПІБ пацієнта, адресу проживання, телефонний номер, біометрична ідентифікація, медична історія тощо. Особливої ваги кібербезпека набуває під час війни, що відбувається не тільки на фронті, але і в інформаційному просторі. [2]

Кібератаки не завжди мають на меті викрадення інформації, також можуть здійснюватись DDOS-атаки, що перевантажують сервера та перешкоджають доступ до інформації, пошкодження даних тощо.

Для забезпечення безпеки інформації використовуються хмарні сховища, кодування даних (шифрування), впровадження дій у разі кібератаки та план дій по відновленню системи у разі її виникнення, розподіл надання інформації користувачам в залежності від їх ролі (адміністратор чи звичайний гість). [3]

Далі представлено аналіз основних дій щодо захисту інформації в медичних програмних забезпеченнях. Ціллю є розробка програмного забезпечення таким чином, щоб мінімізувати кількість інформації, яка зберігається. Можливим є збереження ID пацієнта і використовувати це ID для пошуку розширеною інформації в базі даних. Основа полягає в тому, щоб зберігати як найменше інформації на комп'ютері, тим часом основні дані мають знаходитись у зашифрованому вигляді.

Відповідно до законів Європейського Союзу про захист даних (GDPR), анонімізація даних це "інформація, що не стосується чи не ідентифікує фізичну особу або особисті дані, надано таким чином, що втрачається можливість ідентифікувати фізичну особу". [4] Наприклад, замість того, щоб вказувати

прямий вік в базі даних, ми можемо замінити 45 років на 45-50. Тепер ці дані важко зіставити з окремою людиною, якщо ми не маємо доповненої інформації про цю фізичну особу.

Процес шифрування використовує секретні ключі, цими ключами і є “додаткова інформація”, що дає змогу зробити особисті дані читабельними та з можливістю ідентифікації. Тобто, використання “додаткової інформації” дає змогу ідентифікувати особу. [5]

Ваговим є відслідковувати кому надається інформації. Надавати інформацію тільки довіреним особам та обмежити доступ до неї, використовуючи розподіл користувачів за ролями. Надати логін та пароль для доступу даних або ж для більшого посилання безпеки притримуватись двофакторної та біометричної аутентифікації. Маючи доступ до фізичного комп’ютера має бути жорсткий диск, дані на якому мусять бути зашифровані, щоб у разі втрати диску, зловмисники не змогли скористатися інформацією на ньому.

Зберігання даних у хмарі є одним з ефективних способів кіберзахисту інформації. По-перше, працівники медичного закладу не мають прямого доступу до серверів. По-друге, інформація що знаходиться у хмарі зашифрована, що значно ускладнює доступ кіберзлочинцям.

Використання моделювання загроз дає змогу підготуватись до потенційних загроз. Для цього складають модель загроз за вказівками онлайн спільноти OWASP (рис.1). [6]

Рис. 1. Основні пункти моделі OWASP

Згідно до вказівок OWASP, розробники мають відповісти на чотири основні питання, що стосуються кібербезпеки: 1. Що розробляється? 2. Що може піти не так? (Наприклад, як може бути здійснена кібератака) 3. Які дії будуть впроваджені у разі інциденту? 4. Чи достатньо добре зроблена робота?

Завжди потрібно розуміти середовище та ризики, що впливає на систему та дані. Важливо вміти вчасно виявляти інциденти та бути в змозі відреагувати та стримати кібератаку. Мають бути плани по відновленню системи після інциденту.

Виконувати цільовий пошук компонентів/модулів на вразливість або слабкі місця. До цього входить: статичний аналіз коду, тестування надійності, сканування вразливостей. Опис того, як пристрій є або може бути захищеним, можливо дізнатись за допомогою захищеної конфігурації. Захищена конфігурація може включати засоби захисту кінцевих точок, такі як захист від зловмисного програмного забезпечення, брандмауер/правила брандмауера, білий список, параметри подій безпеки, фізична безпека тощо.

Як пристрій або допоміжна система сповіщатиме користувача про виявлення аномальних подій, такі як зміни конфігурації, аномалії мережі, несанкціоновані спроби входу, аномальний трафік.

Виробники медичних пристроїв повинні бути готові до реагування на інциденти, зокрема як це буде впливати на пацієнтів. Повинен бути розроблений план реагування на інциденти та відповідних дій під час інциденту. Виявлення, звітування, оцінка та прийняття рішень, отриманні з цього висновки.

Як висновок, можна додати такі правила кібербезпеки: необхідно забезпечувати безпечну комунікацію між пристроями, підтримувати захист даних, тобто їх шифрування, має дотримуватись цілісність пристроїв, відсутність несанкціонованих змін, має бути аутентифікація користувача та розподіл їх за ролями, має бути обслуговування програмного забезпечення та вчасне встановлення нових версій ОС.

Перелік посилань

1. Електронна система охорони здоров’я в Україні [Електронний ресурс]. URL: https://ehealth.gov.ua/ (дата звернення: 27.02.2023)
2. OWASP Foundation Owasp Top Ten [Електронний ресурс]. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 27.03.2023)
3. European Data Protection Supervisor 10 Misunderstandings related to anonymisation: технічний документ / EDPS, 2021. 7с.
4. Dr Choong May Ling, Mimi, IMDRF Chair Principles and Practices for Medical Device Cybersecurity : технічний документ / IMDRF, 2020. 46 с.
5. European Data Protection Supervisor [Електронний ресурс]. URL: https://edps.europa.eu/data-protection/data-protection/glossary/d_en (дата звернення: 29.03.2023)

OWASP Foundation Threat Modeling [Електронний ресурс]. URL: https://owasp.org/www-community/Threat_Modeling