ЗАХИСТ ІНФОРМАЦІЇ В КЛІНІЧНОМУ ІНТЕРНЕТІ РЕЧЕЙ

Кирсанов О.О. Безлуцький В.О.
Науковий керівник – к.т.н., доц. Кривенко С.А.
Харьківський національній університет радоелеткроніки
(61166, Харьків, пр. Науки,14, каф. інформаційно-мережної інженерії)

This document illustrates a considered approach for analyzing the security considerations for components, systems and operational environments related to Clinical IoT Data and Devices. The determination of usefulness and applicability of this approach and the viability of the resulting recommendations for a specific component, device, system or operational environment is the joint responsibility of the parties who engineer the systems and devices; the parties who determine the suitability of components, devices and systems in a given operating environment.

Стандарт P2733 встановлює рамки з принципами TIPPSS (Довіра, Ідентичність, Конфіденційність, Захист, Безпека, Безпека) для даних клінічного Інтернету речей (IOT) та перевірки та сумісності пристроїв. Сюди входять клінічні IOT та сумісність із системами охорони здоров'я, включаючи Електронні записи здоров'я (EHR), Електронні медичні записи (EMR), інші клінічні пристрої IOT, на лікарняних пристроях та майбутні пристрої та підключені системи охорони здоров'я [1].

Метою даної роботи є аналіз міркувань безпеки для компонентів, систем та операційних середовищ, пов'язаних з клінічними даними і пристроями інтернету речей.

Зловмисними суб'єктами можуть бути або люди, або ті,що не є особами, наприклад, комп'ютерні боти, віруси, хробаки тощо. Зловмисні суб'єкти здійснюють атаки на свої цілі. Зловмисна поведінка зазвичай має один з двох шляхів: (1) зловживання процесом, технологією або даними людей; або (2) використання вразливостей і недоліків в дизайні, конфігурації і експлуатації пристроїв на які базуються пристрої.

Аналіз безпеки складається з перерахування атак, сценаріїв атак, кампаній атак та оцінки релевантності цих атак, сценаріїв атак і кампаній атак для конкретного пристрою, системи та операційного середовища. Актуальність будь-якої атаки заснована на оцінці серйозності, ймовірності та впливу атаки на передбачувану операцію і передбачуваний результат роботи компонента та системи.

Зловмисник заражає пристрої з метою масового злому пристроїв для отримання доступу до внутрішніх корпоративних мереж для одного з наступних:

– встановити програмне забезпечення для вимагання в корпоративній мережі;

– для вилучення даних;

– для зараження систем, що за корпоративною прошивкою;

– зловмисне перенастроювана пристроїв IoMT для шахрайських цілей.

Приклад переліку кампаній нападів на клінічні системи IOT: порушення ділових операцій: шахрайський суб'єкт проникає в клінічне IoT-операційне середовище з метою негативного впливу на функціонування одного або декількох бізнес-процесів; фінансовий прибуток через вимагання: шахрайський суб'єкт проникнув у клінічне операційне середовище IoT з метою утримання даних для подальшого викупу; крадіжка інтелектуальної власності: шахрайський суб'єкт проникнув у клінічне операційне середовище IoT з метою збору і вилучення програмного забезпечення та операційних даних.

Сценарії атаки:

– несправний або погано налаштований пристрій має порти, піддані доступу до Інтернету. Націлене зловмисне програмне забезпечення визначає та розпізнає його та заражає його;

– Несправний або погано налаштований пристрій має порти, піддані надійному з'єднанню. Націлене зловмисне програмне забезпечення визначає та розпізнає його та заражає його;

– ПК або ноутбук у мережі які були заражені зловмисним програмним забезпеченням або іншим чином піддаються ризику. Потім цей пристрій використовується для пошуку вразливих пристроїв [2].

Список використаної літератури

[1] T. Thompson, «P2733 - Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS,» 20.02.2020. [Онлайновий]. Available: https://standards.ieee.org/project/2733.html.

[2] М.-Б. Алєксандер. 20.02.2020. [Онлайновий]. Available: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/10448. [Дата звернення: 20.02.2020].