УДК 004.031.6
О.Р. Оробчук, доктор філософії, І.М. Кивацький
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ СТРАТЕГІЙ КІБЕРЗАХИСТУ СИСТЕМ КЕРУВАННЯ РОЗУМНИМ БУДИНКОМ

O.R. Orobchuk, Dr, I.M. Kyvatskyi

RESEARCH OF CYBER PROTECTION STRATEGIES OF SMART HOME CONTROL SYSTEMS

Технології розумного будинку з року в рік демонструють значний прогрес. Але разом з цим все більш актуальним стають і проблеми кібербезпеки. Стратегії кіберзахисту систем керування розумним будинком включають комплекс заходів для запобігання, виявлення та відповіді на можливі кіберзагрози які можуть виникати під час користування розумним будинком.

Важливим аспектом кіберзахисту розумного будинку є авторизація та аутентифікація, у OWASP Top 10 2021 згадано про Broken Access Control і Identification and Authentication Failures як одні з найчастіших вразливостей, як за кількістю так і за можливими збитками.

Можливою стратегією для забезпечення більшої надійності є використання двофакторної аутентифікації – це суттєво може ускладнити несанкціонований доступ.

Згідно OWASP TOP 10 2021 Cryptographic Failures посідає друге місце серед вразливостей, це означає, що для передачі даних між пристроями та сервером потрібно використовувати виключно шифрований зв’язок згідно стандартам, уникаючи використання застарілих методів шифрування та протоколів зв'язку.

Важливо використовувати в системі актуальні версії зовнішніх бібліотек та фреймворків, уникаючи використання компонентів з відомими вразливостями, для цього потрібно використовувати спеціальне програмне забезпечення яке дозволяє відслідковувати появу вразливостей в версіях компонентів та шляхи оновлення до безпечних версій. Більш ефективним буде включення автооновлення прошивки.

Для відслідковування збоїв та можливих атак варто використовувати моніторинг та логування, яке дозволяє відслідковувати дії в системі, та у випадку виникнення помилки чи атаки отримати кроки для її відтворення та подальшого вирішення.

Відстежувати цифрові підписи вхідного трафіку та попереджати про виявлення шкідливого контенту дозволить інвестування в надійний брандмауер та використання VPN.

Моніторинг дозволяє переглядати навантаження на систему, і при потребі підключати нові інстанси. При правильно налаштованому моніторингу можна швидко дізнатись про DDOS атаку на сервер.

Сучасною стратегією є також використання технології блокчейн, яка може забезпечити безпечну та децентралізовану платформу для пристроїв IoT.

Для організацій актуальною буде розробка і застосування політики безпеки з описом оптимальних методів захисту пристроїв IoT, а також її регулярний перегляд і оновлення.

Література

1. Джермен Галегуа. Розумні міста — ArtHuss 2021. — 129 р.

2. Кеньо Г. В., Хома В. В.. Моделювання розумного будинку в середовищі Cisco Packet Tracer – Львів : Львівська політехніка 2022 – 104 р.