УДК 004.738.5:004.722.056

КІБЕРБЕЗПЕКА ІНТЕРНЕТУ РЕЧЕЙ (IOT)

Старченко Д. М.
e-mail:dmytro.starchenko@nure.ua
Харківський національний університет радіоелектроніки, каф. РТІКС
м. Харків, Україна

The technology around us is becoming smarter. Many devices are already able not only to transmit information to a person, but also to exchange data with each other, forming the Internet of Things, IoT. But such a solution has both advantages and disadvantages. Making our lives more comfortable, smart technology simultaneously creates new threats. Cyberattacks on IoT devices are more serious than the uprising of machines from science fiction films, because they are our reality today. They are able to disable engineering systems, jeopardize privacy and provide attackers with information for blackmail.

В епоху Інтернету речей (IoT) кібербезпека стає важливою проблемою, яка потребує серйозної уваги та дій. У міру того, як все більше пристроїв стають підключеними до мережі, загрози для безпеки даних та конфіденційності стають все більш складними та різноманітними.

Одним із основних ризиків є можливість хакерського злому пристроїв IoT. Зламані пристрої можуть використовуватися для проведення кібератак, витоку конфіденційної інформації або навіть набрання чинності шкідливими програмами. Це створює загрозу як для кінцевих користувачів, так і для організацій, включаючи критичну інфраструктуру та системи безпеки [1].

Інший важливий аспект кібербезпеки у сфері IoT – це захист особистої інформації. Багато пристроїв IoT збирають і передають великі обсяги даних про користувачів, їх звички та переваги. Недостатній захист цих даних може призвести до їх витікання або зловживання, що може завдати серйозної шкоди як приватним особам, так і компаніям [1].

Головна мета будь-яких злочинців – отримання матеріальної вигоди неправомірним шляхом. Простіше кажучи, метою атак є швидке збагачення коштом інших людей. А от методи досягнення цієї цілі можуть бути різними [2]:

- крадіжка даних;
- порушення приватності;
- знищення або зміна даних;
- для боротьби з цими загрозами необхідно вживати низку заходів;
- атаки на критичну інфраструктуру.

Кіберзагрози для пристроїв інтернету речей є цілком реальними для бізнесу та урядових організацій, відомих персон і пересічних громадян. Мішенню зловмисників може стати будь-хто в будь-який момент, і передбачити таку атаку дуже складно. Саме тому потрібно знати про наслідки,

до яких призведе успішний злам IoT-інфраструктури [2]:

– фінансові збитки; порушення конфіденційності; фізичні ушкодження та збої у роботі; економічні та соціальні наслідки; правові наслідки.

Зважаючи на вразливість мережі інтернету речей і серйозність наслідків кібератак, варто заздалегідь вживати ефективних заходів для мінімізації ризиків. Ось шість ключових стратегій, які допоможуть захистити пристрої від IoT-кіберзагроз.

Шифрування даних – класичний метод захисту даних, що залишається актуальним донині. Сьогодні у цій сфері використовуються надійні стандарти AES, RCA та ECC. Окрім того, розробники користуються такими протоколами захищеного зв'язку, як TLS (Transport Layer Security), для забезпечення безпечної передачі даних між пристроями та серверами. Вони також шукають окремі рішення для захисту даних у стані простою пристрою (at rest) та під час передачі даних (in transit). Ще один важливий аспект шифрування – правильне керування криптографічними ключами. Вони мають зберігатися в безпечному середовищі [2].

Автентифікація та контроль доступу. Важливо переконатися, що доступ до конкретного пристрою може отримати лише його власник чи авторизований користувач. Для цього використовуються надійні протоколи автентифікації, наприклад OAuth 2.0 або Kerberos. Вони спрощують надання доступу, водночас підвищуючи рівень кібербезпеки. Ще один дієвий метод – багатофакторна автентифікація (MFA). Вона вимагає підтверджувати особистість за допомогою двох або більше незалежних факторів: знання (пароль), володіння (ключ-токен або смартфон) та інгерентності (відбиток пальця або розпізнавання обличчя). На глибшому рівні варто подбати й про автентифікацію пристроїв, які взаємодіють між собою в інтернеті речей [2].

Оновлення і патчінг програмного забезпечення. Застаріле програмне забезпечення призводить не лише до погіршення функціональності пристрою, а й до появи нових вразливостей, якими користуються зловмисники. Тому дуже важливо, щоб виробники підтримували свої пристрої протягом усього життєвого циклу, надаючи регулярні оновлення ПЗ та оперативно виправляючи помилки за допомогою патчів. Їм необхідно інформувати користувачів про наявність нових версій та обов'язково попереджати про необхідність ручної інсталяції програм. Але найкращим рішенням буде впровадження механізмів автоматичного оновлення, які працюють без втручання користувача. Вони мають бути реалізовані з урахуванням вимог безпеки – з перевіркою підпису виробника, яка запобігає підміні ПЗ [2].

Моніторинг та виявлення аномалій. Розвиток штучного інтелекту та технології машинного навчання дає змогу виявляти потенційні загрози та реагувати на них в режимі реального часу. Це особливо актуально для захисту від потужних атак, коли рахунок йде на хвилини чи навіть секунди.

Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) здатні аналізувати трафік та поведінку пристроїв, виявляючи аномалії, які можуть свідчити про кібератаку на IoT-засоби. Інтеграція з SIEM-системами (Security Information and Event Management) допомагає централізувати збір та аналіз даних безпеки, що полегшує керування та реагування на інциденти [2].

Але щоб предиктивний і превентивний захист був максимально ефективним, важливо забезпечувати ШІ та класичні системи безпеки необхідним масивом даних. Для цього потрібно налаштувати аналіз логів і повідомлень [2].

Сегментація мережі – це своєрідний цифровий карантин, який дає змогу відокремлювати різні типи пристроїв інтернету речей. Розділення мережі на окремі логічні або фізичні сегменти, кожен з яких має свої правила безпеки та обмеження доступу, дає змогу мінімізувати потенційний вплив атаки на всю інфраструктуру. Це особливо актуально для розподілених мереж, які обслуговують великі підприємства та організації. Приємним бонусом сегментації буде поліпшення керування IT-інфраструктурою та підвищення продуктивності, адже вона зменшує об’єм трафіку між різними секціями. Класичним рішенням для контролю трафіку між сегментами є використання віртуальних локальних мереж (VLAN) та правил брандмауера [2].

Безпечна розробка і впровадження. Принцип безпечної розробки означає, що девелопери мають застосовувати такі практики кодування, як перевірка вхідних даних, керування помилками та уникнення відомих вразливостей. Загалом вони можуть спиратися на документи, подібні до OWASP Top Ten, в яких описано ключові правила кібербезпеки. Позитивними практиками також будуть проведення регулярних кодових ревю, використання інструментів статичного та динамічного аналізу, проведення пенетраційного тестування та моделювання загроз. Вони допоможуть комплексно оцінити стійкість системи до відомих методів атак. Але правила кібербезпеки не обмежуються лише розробкою. Важливо організувати й безпечне впровадження ПЗ [2].

Список використаних джерел:

1. Кібербезпека в епоху Інтернету Речей: Ризики та Заходи захист. [Електронний ресурс] – URL: https://suri.com.ua/kiberbezpeka-v-epokhu-internetu-rechei-ryzyky-ta-zakhody-zakhyst/?srsltid=AfmBOoq0WFVLHIMSoKtizPJhdS7ZmuY-MqrkvwTn10kFooHq650odrCn

2. Кіберзагрози для інтернету речей (IoT): захист смарт-пристроїв. [Електронний ресурс] – URL: https://wezom.com.ua/ua/blog/kiberzagrozi-dlya-internetu-rechey-iot-zahist-smart-pristroyiv