УДК 004.056:355.451

СУЧАСНІ КІБЕР-РИЗИКИ ІНТЕРНЕТУ РЕЧЕЙ ТА МЕТОДИ ЗАХИСТУ ВІД НИХ

Качан В.Є., Нгуєн Х.Н.
Науковий керівник – к.т.н., доц. Куля Ю.Е.
Харківський національний університет радіоелектроніки
(61166, м. Харків, пр. Науки, 14, кафедра ІКІ імені В.В. Поповського,
тел. +38(050) 702-55-92), e-mail: vadym.kachan@nure.ua , khai.nhuien@nure.ua

This work is devoted to assessing current cyber risks of the IoT (Internet of Things) and best practices for protection against them. The use of IoT devices in botnets is considered.

Існують мільйони «розумних» підключених до Інтернету пристроїв, які складають IoT, починаючи від мобільних телефонів і закінчуючи комп'ютерами, домашніми термостатами, камерами відеоспостереження та кавоварками. Інтернет речей має як переваги, так і низку недоліків безпеки. Наприклад, пристрої Інтернету речей часто не мають вбудованих потужних функцій безпеки, які запобігають доступу хакерів до них. Окрім проблем особистої конфіденційності та безпеки, які виникають через ці прогалини в безпеці, більша небезпека полягає в тому, що ці пристрої можуть бути використані хакерами для створення ботнету, який є мережею з пристроями зараженими шкідливим програмним забезпеченням без відома користувача.

У світі пристроїв Інтернету речей існує ряд кібер-ризиків [1]. Деякі з основних кіберзагроз IoT в нинішній час включають наступні ризики:

1. відсутність регулярних оновлень і слабкі механізми оновлення;
2. слабкий захист паролем;
3. незахищені інтерфейси. Вразливості в інтерфейсах дозволяються хакерам зламувати пристрої IoT, а далі і проникати у локальну мережу користувачів;
4. шкідливе програмне забезпечення. Після зараження пристроїв IoT шкідливим програмним забезпеченням вони можуть бути використані в DDoS (Distributed Denial of Service) атаках [2], використання таких пристроїв є сучасним трендом у формуванні ботнетів. Такими атаками є, наприклад SYN (Syncronized) flood або UDP (User Datagram Protocol) flood;
5. незашифровані дані. Відсутність шифрування може дозволити суб'єктам загрози перехоплювати пакети з мережі пристроїв за допомогою атак «людина посередині» або інших методів втручання в мережу та отримання доступ до конфіденційних даних. Незашифровані дані та мережі є актуальною проблемою, яка є причиною катастрофічних зломів компаній. Серед кращих практик захисту від атак на IoT можна виділити декілька [3].

1. Зміна налаштувань маршрутизатора за замовчуванням. Більшість людей забувають перейменувати маршрутизатор і залишають назву за замовчуванням. Це може зашкодити безпеці приватного Wi-Fi (Wireless Fidelity). Рекомендується змінити ім'я, яке не містить у собі особисту інформацію. Wi-Fi є першим рубежем, що потребує захисту від хакерів, оскільки багато пристроїв IoT підключено до нього.

2. Від'єднання пристроїв IoT, коли вони не потрібні. Більшість сучасних пристроїв можуть підключатися до Інтернету, наприклад, холодильники та телевізори. Але це не означає, що потрібно підключати їх до Інтернету. Рекомендується уважно ознайомитися з функціями пристроїв і точно дізнатися, який пристрій потребує підключення до Інтернету.

3. Вибір надійного паролю. Для надійного захисту слід використовувати принцип "три з чотирьох", тобто використовувати хоча б три параметри з чотирьох в паролі - великі і малі літери, цифри, спеціальні символи.

4. Уникнення використання Universal Plug and Play. Хоча Universal Plug and Play (UPnP) має своє застосування, він може зробити принтери, маршрутизатори, камери та пристрої IoT вразливими до кібератак. UPnP дозволяє полегшити підключення пристроїв та допомогти їм автоматично виявляти один одного. Тим не менш, це приносить більше користі хакерам, ніж користувачам, оскільки вони можуть виявляти всі пристрої Інтернету речей за межами локальної мережі. Тому краще повністю вимкнути UPnP.

5. Постійне оновлення вбудованого та встановленого ПЗ (програмного забезпечення). Оновлення ПЗ пристрою IoT гарантує, що пристрій має найактуальнішу систему безпеки. Крім того, це допомагає системі усунути недоліків безпеки старих версій ПЗ. Незважаючи на ризики, малоймовірно, що IoT перестане розповсюджуватись у домах, офісах і т.д. Через це, нікуди не дінуться і хакери. Тому, найголовнішим є пам'ятати про безпеку своїх пристроїв. Розуміння їхніх вразливостей і використання правильних інструментів захисту необхідні для протистояння загрозам у мінливому світі IoT.

Список використаних джерел:

1. Cyber Threats Haunting IoT Devices in 2021 [Електронний ресурс] – Режим доступу до ресурсу: https://securityboulevard.com/2021/09/cyber-threats-haunting-iot-devices-in-2021/. 2. Reo J. DDoS Hackers Using IoT Devices to Launch Attacks [Електронний ресурс] / Joy Reo – Режим доступу до ресурса: https://www.corero.com/blog/ddos-hackers-using-iot-devices-to-launch-attacks/.

3. Swamini K. How to secure IoT devices and protect them from cyber attacks [Електронний ресурс] / Kulkarni Swamini – Режим доступу до ресурсу: https://bit.ly/3B4R8Ah.