УДК 004.7
Б. Цюприк, О. Ясній
(Тернопільський національний технічний університет імені Івана Пулюя)

БЕЗПЕКА МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

UDC 004.7
B. Tsiupryk, O. Yasniy
(Ternopil Ivan Puluj National Technical University, Ukraine)

INTERNET OF THINGS SECURITY

Інтернет речей (англ. Internet of Things, IoT) знаходиться лише на початку свого шляху, але вже розвивається з величезною швидкістю, і всі впроваджені нововведення додають серйозних проблем, що пов'язані з інформаційною безпекою.

Крім порушення конфіденційності традиційних мереж зв'язку (повтори, підслуховування, спотворення інформації і т. д.), виникають проблеми із захистом споживчої складової. Вони зумовлені:

1. відсутністю серйозного збитку;
2. відсутністю стандартів не тільки захисту, але і взаємодії;
3. відсутністю в наші дні інтересу у виробників, як першої щаблі реалізації.

Велику загрозу несе керування пристроїв за допомогою міжмашинної взаємодії. Жодну написану людиною програму не можна вважати стовідсотково точною; для неї пишуться різні патчі для виправлення помилок. Така ж доля чекає датчики в інтернет-пристроях. Із посиленням ролі даних пристроїв в житті людей буде збільшуватися загроза безпеці всіх даних, навіть найнезначніших на перший погляд. Необхідно оцінювати будь-який витік інформації, так як резюмування її складових може представляти небезпеку для життя як фізичних, так і юридичних осіб.

Компанія ESET описую три простих кроки для посилення захисту мережі інтернету речей:

- Багатофакторна аутентифікація: використовуйте апаратні токени або спеціальне програмне забезпечення для управління даними облікових записів. Двофакторна аутентифікація використовується на додаток до базової (наприклад, ім'я користувача та пароля) під час входу в систему або програму. Як правило, на попередньо визначену адресу електронної пошти або за допомогою текстового повідомлення надсилається одноразовий код. Ця комбінація може бути використана тільки для аутентифікації одного сеансу протягом обмеженого часу (наприклад, 60 секунд).

- Мережевий інтелект (network intelligence): багато пристроїв IoT здебільшого підключаються до роутера, тому пошук загроз можна здійснювати за допомогою аналізу аномалій мережевого трафіку. Різні постачальники пропонують обладнання, яке підключається до роутера та надає можливість дізнатися про підозрілі події, а також забезпечує огляд мережевої поведінки пристроїв IoT.

- Резервне копіювання. Забезпечення регулярних і надійних резервних копій систем і даних є необхідним кроком для запобігання втратам важливих даних. У разі наявності резервних копій можна відновити випадково видалений файл або дані на пошкодженому жорсткому диску, а також забезпечити безперервність роботи під час інцидентів.

Ці три базові кроки не забезпечать повного захисту світу Інтернету речей, але дозволять покращити стан безпеки корпоративної мережі, в якій використовуються пристрої IoT, та дозволять запобігти можливим фінансовим втратам.