УДК 004.77:004.056

ЗАГРОЗИ ПРИСТРОЇВ У СКЛАДІ РОЗУМНОГО ДОМУ

Грабар М.В.
Науковий керівник – к.т.н., доц. Іванова О.О.
Харківський національний університет радіоелектроніки,
каф. КРіСТЗІ, м. Харків, Україна
e-mail: mariia.hrabar@nure.ua

The phrase "smart home" can hardly surprise anyone these days. These words mean comfort, saving resources, the ability to control many processes in the house remotely. But the main thing that the system should provide is the security of a smart home.

За сьогоднішніми загальносвітовими оцінкам, в середньому на один будинок припадає дев'ять підключених пристроїв, а в деяких країнах це кількість досягає 20 і більше. Споживачі все більше залежать від якісного підключення до глобальної мережі. Підприємства та бізнес також отримують масу переваг, пов'язаних із Інтернетом речей (IoT). З іншого боку, швидке поширення підтримуючих IoT-пристроїв створює для зловмисників небувалі можливості для піратських дій та вторгнення в домашні мережі. Якщо, звичайно, захист цих пристроїв недостатньо надійний.

За результатами дослідження, проведеного Sonicwal у 2020 р., кількість кібератак на пристрої IoT порівняно з минулими роками. підвищилося на 215% [1]. Сьогодні небезпека ще більше зростає, оскільки несподівано різко збільшилася кількість людей, практично постійно працюючи з дому. Багато з них, коли працювали з офісу, були захищені корпоративними міжмережевими екранами, але таких екранів немає у будинках. "Домашній офіс" - це всього лише ще один пристрій підключеного дома (ноутбук або планшет), тому ризик зловмисного проникнення у домашню мережу зростає експоненціально. Більше того, коли людина працює з дому, атака на будинок може розвинутися в атаку на корпоративну мережу роботодавця. При цьому домогосподарства нездатні самі забезпечити свою безпеку. Проведене Broadband Genie дослідження показало, що 86% споживачів ніколи не оновлювали вбудоване ПЗ свого маршрутизатору.

У 2018 р. відділення Market Intelligence компанії Microsoft опублікувало огляд, в якому особлива увага приділялася побоюванням споживачів відносно їх цифрових пристроїв, та основною проблемою було визнано відсутність належної захищеності персональної інформації та даних. Цифрові пристрої, що підключені в будинку, слід оцінювати з боку не тільки функціональності та ціни, але також і безпеки.

Зловмисники будуть приділяти цифровим пристроям більше "уваги", ніж будь-яким іншим пристроям, оскільки помічники можуть відігравати

роль центрального елементу, що контролює всі інші елементи домашньої мережі. Це ж відноситься і до маршрутизаторів, що можуть виступають як її шлюзи.

На сьогоднішній день стає питання-проблема, хто повинен відповідати за безпеку IoT-пристроїв і всього розумного вдома – постачальник послуг, виробник пристроїв чи споживач?

Безперечно, споживачі та постачальники послуг не можуть довірити безпеку та надійність роботи своїх мереж виробникам пристроїв IoT. Коли йдеться мова про маршрутизатор то постачальник послуг - оператор зв'язку часто нездатний зазирнути за шлюз, щоб перевірити роботу пристроїв та отримати відомості про них з метою вирішення проблем, що виникають.

Але у теперішній час на ринку присутня безліч виробників пристроїв, які постачальники послуг здатні запропонувати споживачам, тобто таке нове рішення, яке захистить увесь будинок. Оператори зв'язку просто повинні знайти рішення, завдяки якому вони зможуть отримувати інформацію про те, що відбувається в домашній мережі. Проведені дослідження показують, що споживачі згодні платити за захист своїх пристроїв та даних. Так, у проведеному раніше дослідженні Blackberry стверджується, що 58% споживачів готові платити більше за підключені пристрої, якщо вони впевнені в тому, що їх дані та конфіденційність будуть захищені. [2-3].

Тому операторам зв'язку необхідні інструменти, що підвищують ефективність вирішення проблем з безпекою та якістю наданих споживачам послуг. Найважливішою частиною будь-якого рішення є технологія Fingerprinting в IoT. Вона забезпечує отримання споживачем та його постачальником послуг повної та достовірної інформації про підключені до домашньої мережі пристроїв. Тобто операторам зв'язку необхідно знайти технологію для забезпечення безпеки, що захищає підключений будинок повністю, включаючи маршрутизатор. Передові рішення повинні забезпечувати блокування вхідного та вихідного зловмисного трафіку, включати в себе пристрої обробки Fingerprinting та виявляти аномальну поведінку за допомогою штучного інтелекту. Штучний інтелект може стати для розумного будинку основним засобом виявлення загроз та нестандартної поведінки у режимі реального часу.

Список використаних джерел:

1. https://irdeto.sharepoint.com/:b:/s/d_mi/EdiRtYpvXG5FosIu7fQSmdIBvyXgX8zn86ehQ_zHbkCfDA
2. https://www.kaspersky.ru/resource-center/threats/how-safe-is-your-smart-home
3. https://eset.ua/ru/news/view/665/zashchita-umnogo-doma-kak-zashchitit-umnyy-dom-ot-kiberprestupnikov