УДК 004.384

Лобанчикова Н. М., канд. техн. наук, доц.
Серденюк Б. О., студент, гр. ІСТ-2М
Житомирський державний технологічний університет

ДОСЛІДЖЕННЯ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ В IoT

У червні 2018 року компанія Juniper Research у дослідженні ринку інтернету речей спрогнозувала зростання вдвічі кількості таких пристроїв до 2022 року. Якщо зараз аналітики оцінюють число активних IoT-пристроїв у 21 мільярд, то через чотири роки їх кількість перевищить 50 мільярдів. У зв'язку з розвитком IoT-технологій висловлюють занепокоєння фахівці у сфері інформаційної безпеки. На їхню думку, величезна кількість погано захищених інтернет-девайсів дає нові можливості кіберзлочинцям, яким уже вдалося зламати ряд IoT-систем.

Гучна кібератака трапилася в жовтні 2016 року, коли недоступним виявився ряд популярних ресурсів, сервісів і соціальних мереж: Amazon, Pinterest, Twitter, Soundcloud, Spotify, Reddit, GitHub, Starbucks, CNN, The New York Time та ін. Через атаки постраждали власники сайтів, які працюють на серверах компанії Dyn. Відомо, що зловмисники використовували програму Mirai, здатну знаходити в мережі незахищені пристрої інтернету речей, такі, як роутери, камери стеження, цифрові відеомагнітофони і т.д. У ботнет, згідно з даними Dyn, були об'єднані понад 100 000 незахищених підключених пристроїв, оскільки працювали без захисту паролів. Робота атакованих сайтів була відновлена лише через 14 годин.

Актуальність проблеми підкреслюється інцидентами, втрати капіталу від яких вимірюються мільярдами доларів: Industroyer, BrickerBot, Mirai – і це лише видима верхівка айсберга.

Дані досліджень корпорації HP, метою яких було не виявити якісь конкретні небезпечні інтернет-пристрої і викрити їх виробників, але позначити проблему ІБ-ризиків в світі IoT в цілому, звертають увагу на проблеми як з боку власників пристроїв, так і на проблеми, над усуненням яких повинні працювати розробники. Так, на самому початку експлуатації користувачеві обов'язково потрібно замінити фабричний пароль, встановлений за замовчуванням, на свій особистий, оскільки фабричні паролі однакові на всіх пристроях і не відрізняються стійкістю. Оскільки не всі прилади мають вбудовані засоби ІБ-захисту, власникам також слід подбати про встановлення зовнішнього захисту, призначеного для домашнього використання, щоб інтернет-пристрої не стали відкритими шлюзами в домашню мережу або прямими інструментами заподіяння шкоди.

У ході проведеного HP дослідження виявлено, що приблизно в 70% проаналізованих пристроїв не шифрується бездротовий трафік. Веб-інтрефейс 60% пристроїв експерти HP вважають небезпечним через недосконалу організацію доступу і високий ризик міжсайтового скриптингу. У більшості пристроїв передбачені паролі недостатньої стійкості. Приблизно 90% пристроїв збирають ту чи іншу персональну інформацію про власника без його відома.

Всього ж фахівці HP нарахували близько 25 різних вразливостей у кожному з досліджених пристроїв і їх мобільних та хмарних компонентах.

Висновок експертів HP невтішний: безпечної системи IoT сьогодні не існує. Особлива небезпека для інтернету речей прихована в контексті поширення цільових атак (APT). Варто тільки зловмисникам проявити інтерес до будь-кого, і наші помічники зі світу IoT перетворюються на зрадників, нарозхрист відкривають доступ у світ своїх власників.

Були виділені такі слабкі місця IoT:

– перехід на IPv6;
– живлення датчиків;
– стандартизація архітектури і протоколів, сертифікація пристроїв;
– інформаційна безпека;
– стандартні облікові записи від виробника, слабка аутентифікація;
– відсутність підтримки з боку виробника для усунення вразливостей;
– важко або неможливо оновити ПЗ і ОС;
– використання текстових протоколів і непотрібних відкритих портів;
– використовуючи слабкість одного гаджета, хакеру легко потрапити в усю мережу;
– використання незахищених мобільних технологій;
– використання незахищеної хмарної інфраструктури;
– використання небезпечного ПЗ.

Оскільки питання стоїть надзвичайно гостро, компанії-розробники техніки, засобів комунікації, мережних пристроїв, програмного забезпечення, кіберзахисні компанії переймаються пошуками засобів захисту пристроїв IoT. Однією з провідних компаній у розробці засобів безпеки в IoT є Cisco Systems, яка відіграла провідну роль у розробці моделі IoT на Всесвітньому форумі IoT (IWF), розробила фреймворк

безпеки IoT, що став корисним доповненням до еталонної моделі. На рисунку 1 продемостроване середовище безпеки, пов'язане з логічною структурою IoT.

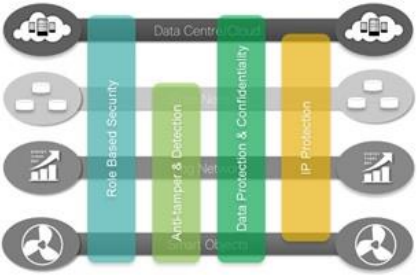

Рис.1. Середовище безпеки IoT

Модель Cisco IoT є спрощеною версією моделі Всесвітнього форуму IoT. Вона складається з наступних рівнів:

1. «Розумні» об'єкти та вбудовані системи: ця частина IoT найбільш вразлива.

2. Туманна, периферійна мережа: цей рівень включає дротові та бездротові з'єднання пристроїв IoT. Ключовою проблемою є велика варіативність мережевих технологій і протоколів, використовуваних різними пристроями IoT, і необхідність вироблення і втілення єдиної політики безпеки.

3. Ядро мережі: рівень ядра мережі надає шляхи для передачі даних між платформами в центрі мережі і пристроями IoT. Тут проблеми безпеки ті ж, що в традиційних мережах. Однак величезна кількість кінцевих вузлів, з якими треба взаємодіяти і управляти ними, створює значну проблему для безпеки.

4. Центр даних та хмарні сервіси: цей рівень містить платформи для додатків, зберігання даних і управління мережею. IoT не додає на цей рівень ніяких нових проблем безпеки, крім необхідності мати справу з величезною кількістю окремих кінцевих вузлів.

За допомогою цієї чотирьохрівневої архітектури модель Cisco визначає чотири загальних можливості безпеки, що охоплюють кілька рівнів:

1. Безпека на основі ролей: системи управління доступом на основі ролей призначають права доступу ролям, а не окремим користувачам. Користувачам, в свою чергу, зіставляються різні ролі, або статично, або динамічно, відповідно обов'язків.

2. Захист від втручання і виявлення втручань: ця функція особливо важлива на рівні пристроїв і туманної мережі, але поширюється також і на рівень ядра мережі. Всі ці рівні можуть використовувати компоненти, що фізично знаходяться на території вільного доступу до них будь-ким.

3. Захист даних і конфіденційність: ці функції охоплюють всі рівні архітектури.

4. Захист протоколів інтернету: захист «даних в русі» від прослуховування і перехоплення важливий для всіх рівнів.

На рисунку 1 відзначені конкретні функціональні області безпеки поверх чотирьох рівнів моделі IoT. У документі Cisco також пропонується концепція безпеки IoT, що визначає компоненти функції безпеки для IoT, яка охоплює всі рівні:

1. Аутентифікація: цей компонент охоплює елементи, які ініціюють доступ, і в першу чергу ідентифікує пристрої IoT. На відміну від типових корпоративних мережевих пристроїв, кінцеві пристрої IoT повинні оснащуватися такими методами аутентифікації, які не вимагають втручання людини. До таких методів належать радіочастотні мітки, сертифікати x.509 або MAC-адреси кінцевих пристроїв.

2. Авторизація: авторизація управляє доступом до пристрою через структуру мережі. Цей елемент включає в себе контроль доступу. Разом з рівнем аутентифікації він виробляє необхідні параметри для того, щоб дозволити обмін інформацією між пристроями та між пристроями і прикладними платформами, тим самим забезпечуючи роботу IoT-служб.

3. Мережева політика: цей компонент охоплює всі елементи, які здійснюють маршрутизацію і транспортування трафіку з кінцевих пристроїв інфраструктурою, будь то контроль, управління або власне трафік даних.

4. Аналітика безпеки: цей компонент включає всі функції, необхідні для централізованого управління пристроями IoT. На основі видимості виникає здатність здійснювати контроль, включаючи конфігурацію, патчі і оновлення, а також контрзаходи для припинення загроз.

У процесі дослідження розробляється комплекс заходів та засобів підвищення безпеки для IoT.

Багато компаній на сьогодні представили свої моделі захисту, які постійно намагаються стандартизувати, співвіднести та впровадити. Дослідження технологій та засобів безпеки в IoT, пошук оптимальних моделей безпеки в усіх рівнях: апаратної частини, програмної частини, рівні користувача є надважливим завданням сьогодення. Завданням, з яким поки світові IT-гіганти не можуть впоратися.