УДК 004.519.217

Кнуренко В.О., студент.
Шарай О.І., студент.
Рогочий С.Ю., студент.
Полтавський національний технічний університет імені Юрія Кондратюка

ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ СИСТЕМИ INTERNET OF THINGS НА ОСНОВІ МОДЕЛІ АРХІТЕКТУРИ ХМАРНОГО СЕРВІСУ ТА ПАРАМЕТРИЗАЦІЇ ВИБІРОК ВРАЗЛИВОСТЕЙ ІЗ ВІДКРИТИХ БАЗ

***Анотація**. Зростання кількості пристроїв з можливістю підключення до глобальної мережі викликало необхідність їх поєднання в множини. Це дозволило як централізувати управління, моніторинг та обслуговування, так і розширити функціональні можливості утвореної системи Internet of Things. З іншого боку пристрої таких систем є об'єктами атак, що обумовлює необхідність моделювання ризиків кібербезпеки на етапі проектування.*

***Ключові слова:** internet of things, кібербезпека, архітектура хмарного сервісу.*

Вступ

Інтернет речей (англ. Internet of Things, IoT) - концепція обчислювальної мережі фізичних предметів («речей»), оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем, яка розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, і частково виключає необхідність участі людини [1].

З початку 2010-х років «інтернет речей» стає рушійною силою парадигми «туманних обчислень» (англ. Fog computing), що розповсюджує принципи

хмарних обчислень від центрів обробки даних до величезної кількості взаємодіючих географічно розподілених пристроїв, і розглядається як платформа «інтернету речей».

На даний час термін «Інтернет речей» поширюється не тільки на системи для «домашнього» застосування, але і на промислові об'єкти. Розвиток концепції «Інтелектуальних будівель» отримав назву «Building Internet of Things» (BIoT), розвиток розподіленої мережевої інфраструктури в автоматизованих системах управління технологічними процесами привів до появи «Industrial Internet of Things» (IIoT) [3].

Всебічне поширення загроз, вплив яких може мати катастрофічні наслідки для всієї критично важливої інфраструктури, змусили аналітиків звернутися для захисту кіберпростору до стандартів оцінки ризиків [4]. Достовірність оцінки ризиків залежить від кількісного аналізу загроз, вразливостей і їх наслідків, що передбачає збір і вивчення величезних обсягів інформації, розробку і дослідження відповідних математичних моделей.

Огляд хмарної інфраструктури системи «Internet of Things»

Стандартна архітектура IoT згідно [3] включає кілька зон компонентів. До них відносяться (рис.1):

- зона кінцевих пристроїв.
- зона польового шлюзу.
- зона хмарного шлюзу.
- зона служб.

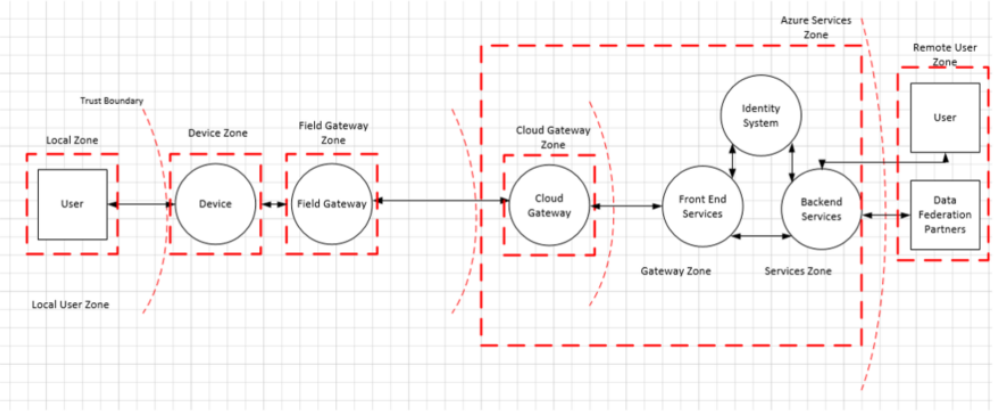

Рис. 1. Стандартна архітектура IoT [3]

До архітектури хмарного сервісу включені шлюз, система ідентифікування та сервери FrontEnd та BackEnd. Хмарний шлюз являє собою систему для віддаленого обміну даними між різними пристроями і польовими шлюзами [3]. Дані, як правило, надходять від різних сайтів в загальнодоступній мережі в хмарну систему аналізу і контролю даних. У ряді випадків хмарний шлюз може надавати прямий доступ до спеціалізованих пристроїв з таких терміналів, як планшетні ПК і телефони. Терміном «хмара» позначається спеціалізована система обробки даних, яка не прив'язана до того ж сайту, що і підключення пристрою або польові шлюзи. У зоні хмари також можна реалізувати оперативні заходи щодо запобігання навмисного фізичного доступу.

Хмарний шлюз дозволяє ізолювати всі підключені до нього пристрої або польові шлюзи від будь-якого мережевого трафіку [4]. Сам по собі хмарний шлюз не є ні системою керування кінцевими пристроями, ні системою обробки або зберігання даних цих пристроїв, однак шлюз взаємодіє з усіма зазначеними системами.

Формування вибірок із відкритих баз вразливостей

В даний час існує велика кількість баз даних (БД) вразливостей, як відкритих для загального доступу, так і закритих, що використовуються в комерційних продуктах. Такі бази можна поділити на дві групи. Перша група – це БД компаній в яких лише вразливості власних продуктів. Друга група – це

узагальнюючі БД, які будуються на основі декількох БД з першої групи .

Однією з найвідоміших баз вразливостей є «Загальні вразливості та ризики» (Common Vulnerabilities and Exposures - CVE) [6] компанії MITRE. Вона має велику кількість джерел що надають списки вразливостей. Недоліком цієї БД є відсутність в описі вразливостей специфікації програмно-апаратного забезпечення. Для визначення цієї специфікації потрібно використовувати джерела які надали інформацію.

Оцінювання ризиків кібербезпеки системи Internet of Things

Хоча кількісна оцінка ризиків і була віднесена міжнародними стандартами до одного з провідних досягнень в цій області, конкретних методів і додатків поки що представлено мало. Серед останніх стандартизованих ініціатив можна відзначити NIST Special Publication 800-39 і Common Vulnerability Scoring System (CVSS). В обох випадках автори документів визнають необхідність врахування людського фактора, але конкретних настанов щодо застосування в них фактично немає.

Загальна система оцінки вразливостей (Common Vulnerability Scoring System, CVSS) об'єднує критерії оцінки вразливостей киберсистем для конкретних загроз і їх потенційних наслідків. CVSS формує загальний опис для організації комунікацій і порівняння вразливостей, однак інструкцій щодо ефективного усунення виявлених вразливостей ця система не надає. Більш того, критерії стосуються тільки вразливостей системи і впливу загроз - про самі загрози нічого не сказано, тому остаточні оцінки і вектор атаки можуть бути обрані невірно, якщо виходити з того, що ризики визначаються тріадою критеріїв. Можна зробити висновок про те, що CVSS не базується на ризиках, а оцінює уразливості і їх наслідки, причому не загрози, до яких відноситься, наприклад, ймовірність атак.

Ризик – поєднання ймовірності та наслідків настання несприятливих подій. Також ризиком часто називають безпосередньо певну подію, здатну принести кому-небудь збиток. Ризик завжди передбачає імовірнісний характер

результату.

Оцінка ризику є частиною процесу менеджменту ризику і являє собою структурований процес, в рамках якого ідентифікують способи досягнення поставлених цілей, проводять аналіз наслідків та ймовірності виникнення небезпечних подій для прийняття рішення про необхідність обробки ризику [5].

Оцінка ризику є процесом, що об'єднує ідентифікацію, аналіз ризику і порівняльну оцінку ризику. Спосіб реалізації цього процесу залежить не тільки від сфери застосування ризик-менеджменту, але також і від методів оцінки ризику.

Модель ризиків кібербезпеки системи Internet of Things включає оцінку наступних елементів:

1. Процеси (веб-служби, служби Win32, керуючі програми *.nix). Деякі складні об'єкти (наприклад, польові шлюзи і датчики) можна абстрактно сприймати як процеси.
2. Сховища даних (файли конфігурації або бази даних).
3. Потік даних (маршрут переміщення даних між елементами системи Internet of Things).
4. Зовнішні об'єкти (всі об'єкти, які взаємодіють з системою, але не контролюються нею, наприклад, користувачі і канали зв‘язку).

Висновок

У статті розглянуто процеси оцінювання ризиків кібербезпеки системи Internet of Things. Розглянуто особливості моделі архітектури хмарного сервісу та її компоненти – хмарного шлюзу. Визначено напрямки параметризації вибірок вразливостей із відкритих баз. Подальші дослідження слід спрямувати на розробку інтегрованих засобів побудови вибірок із баз вразливостей, уточнення даних в базах за відкритими зв‘язками та вдосконалення методів параметризації для подальшого використання оцінок в моделях ризиків.

Посилання

1. ISO/IEC 17789:2014 Information technology - Cloud computing - Reference architecture [Text]. – impl. 10.10.2014. – Brussels: European Committee for Electrotechnical Standardization, 2014. – 53 p.

2. Roy A. Cyber security analysis using attack countermeasure trees [Text] / A. Roy, Dong Seong Kim, K.S. Trivedi // In: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '10), ACM, New York, 2010. – P. 1-4.

3. Безпека в IoT: Архітектура системи безпеки [Електронний ресурс] – Режим доступу: http://it-ua.info/news/2017/01/04/bezpeka-v-iot-arhtektura-sistemi-bezpeki.html– 24.11.2017 р.

4. Microsoft Azure: Cloud Computing Platform & Services [Електронний ресурс] – Режим доступу: https://azure.microsoft.com/en-us/ – 24.11.2017 р.

5. IEC 31010:2009. Risk management — Risk assessment techniques [Text]. – impl. 12.01.2009. – Brussels: European Committee for Electrotechnical Standardization, 2009. – 176 p.

6. Рекомендация МСЭ-Т Х.1524. Перечень общеизвестных слабых мест [Текст]. – введ. 02.03.2012. – Женева: Международный союз элек-тросвязи, 2012. – 22с.

Authors:
Knurenko Vladislav, Sharai Alexey, Rogochii Sergey

ASSESSMENT OF THE CYBERSECURITY RISKS OF THE INTERNET OF THINGS SYSTEM BASED ON ARCHITECTURE MODEL CLOUD SERVICES AND SELECTION PARAMETRIES VULNERABILITIES OPEN BASES

Abstract. The growth in the number of devices with the ability to connect to the global network caused the need for their combination in a plurality. This allowed to centralize the management, monitoring and maintenance, as well as to expand the functionality of the established Internet of Things system. On the other hand, the devices of such systems are attack objects, which makes it necessary to model the risks of cybersecurity at the design stage.

Keywords: internet of things, cybersecurity, cloud service architecture.

Авторы:
Кнуренко Владислав Александрович, Шарай Алексей Игоревич, Рогочий Сергей Юрьевич

ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ СИСТЕМЫ INTERNET OF THINGS НА ОСНОВЕ МОДЕЛИ АРХИТЕКТУРЫ ОБЛАЧНЫХ СЕРВИСОВ И ПАРАМЕТРИЗАЦИИ ВЫБОРОК УЯЗВИМОСТЕЙ ИЗ ОТКРЫТЫХ БАЗ

Аннотация. Рост количества устройств с возможностью подключения к глобальной сети вызвал необходимость их объединения в подмножества. Это позволило не только централизовать управление, мониторинг и обслуживание, но и расширить функциональные

возможности созданной системы Internet of Things. С другой стороны устройства таких систем являются объектами атак, что обусловливает необходимость моделирования рисков кибербезопасности на этапе проектирования.

Ключевые слова: internet of things, кибербезопасность, архитектура облачного сервиса.