АСПЕКТИ БЕЗПЕКИ МЕРЕЖ IoT ТА IIoT

Ступак Г.В., старший викладач, glib.stupak@donntu.edu.ua
Донецький національний технічний університет, м. Покровськ, Україна

Сьогодні вже неможливо точно сказати, скільки пристроїв мають прямий контакт з Інтернет, але за різними прогнозами ця кількість вже понад як в п’ять разів перевищила кількість населення на землі. Незалежно від типу пристроїв, вони зазвичай мають обмежений функціонал захисту, що власне несе найбільший ризик, і порушує кібербезпеку мережі, в якій цей пристрій розташований. Мережа, яка сформована з пристроїв і призначена для взаємодії пристроїв між собою має назву мережа Інтернету речей (IoT). Дуже важливим є той фактор, що до мереж IoT все частіше ставляться не тільки побутові застосунки, але й промислові мережі, які по своїй суті є цифровими, двонаправленими, багатоточковими послідовними телекомунікаційними мережами, що зв'язують територіально розподілені датчики, виконавчі механізми, промислові контролери і використовуються в промисловій автоматизації для побудови єдиного інформаційного і керуючого середовища, котре об’єднує інтелектуальні технологічні пристрої і контролери цехового рівня.

Відповідно до багаторівневої архітектури IoT/IIoT-систем, можна виділити наступні три ділянки, на яких необхідно забезпечити інформаційну безпеку:

- smart-пристрої - «розумні» датчики, сенсори і іншими прилади, які збирають інформацію з обладнання і відправляють її в хмару, передаючи назад керуючі сигнали зі зміни стану речей;
- мережеві шлюзи і канали передачі даних (провідні та безпровідні протоколи);
- програмні IoT-платформи - хмарні Big Data сервіси зберігання та обробки інформації [1].

Але як виявляється на практиці майже всі ділянки IoT-мереж є незахищеними. На це є кілька очевидних причин, які є наслідком стрімкого розвитку технологій та жагою надприбутків деяких виробників обладнання:

1. Швидке проникнення IoT-рішень і масштабування виробничої інфраструктури. Компанії бачать технологічні нововведення і прагнуть їх швидше використовувати в гонитві за оптимізацією бізнес-процесів і виробництва. Відповідно, різні рішення впроваджуються без належного контролю з точки зору кібербезпеки;
2. Ненадійні системи аутентифікації користувачів. Незважаючи на те, що використовуються надійні системи аутентифікації, IoT-пристроїв це зазвичай не стосується.
3. Різнорідність IoT-рішень. Налічується кілька тисяч компаній, які виробляють IoT-рішення, і на одному і тому ж підприємстві можуть бути

встановлені системи різних виробників, які мають різні рівні інформаційної безпеки.

4. Для прискорення виведення продукту на ринок багато компаній не створюють пристрій з нуля, а використовують готові компоненти, включаючи чіп, камеру, бездротові модулі зв'язку і т.п. Будь-який з цих елементів може бути підданий злому [2].

Також тенденцією, що дуже насторожує, є все частіша заміна виробниками промислових ПЛК та SCADA систем пропрієтарних протоколів зв'язку мережевими протоколами Ethernet і TCP/IP. Таке тенденція носить позитивний характер у вигляді уніфікації продуктів і стандартів, але ж водночас розширена мережева взаємодія означає, що промислові підприємства мають велику площу атаки. Більш того, багато систем моніторингу і контролю використовуються роками, а іноді й десятиліттями, без своєчасного отримання або можливості отримувати оновлення безпеки.

Це призводить до численних незначних цілей в додатку з промисловим контролем системи. Тому очевидно, що ці важливі, але вразливі системи повинні бути захищені. Багато компаній встановлюють міжмережеві екрани по периметру на кордоні своїх промислових мереж, щоб захистити нестійкі цілі в своїх промислових додатках від загроз з Інтернету або з офісних мереж. Хоча це необхідний крок, сучасна мережева безпека вимагає набагато більшого, ніж просто захист периметра [3].

Одним з найдієвіших засобів убезпечення IoT/IIoT мереж від вторгнень та кібератак є застосування політики зонування мереж. Сучасна модель мережі промислового підприємства

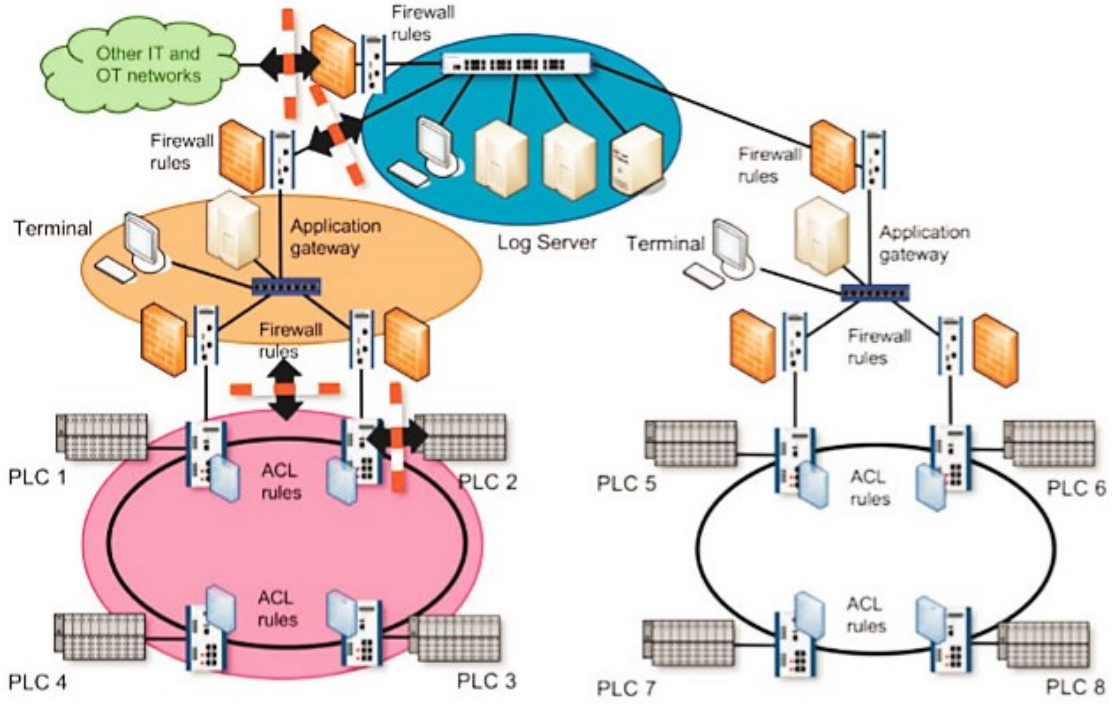

Рисунок 1 – Зонування промислових і звичайних мереж

Всеосяжні концепції мережевої безпеки повинні враховувати як різні методи атаки, так і різні типи атакуючих. Це включає в себе сценарії, коли перша лінія захисту вже була зламана, тобто фаєрвол на кордоні між виробничою мережею і офісною мережею або Інтернетом. Як тільки зловмисник проникне в мережу, він може швидко завдати серйозної шкоди, якщо архітектура і конфігурація мережі будуть обрані без урахування безпеки. Тому один з важливих етапів при проектуванні мереж – створення грамотної політики рівнів доступу та зонування з використанням відокремлених за структурним призначенням сегментів.

Література

1. Как сделать интернет вещей безопасным: 3 вида cybersecurity в Big Data [Електронний ресурс] – Режим доступу до ресурсу: https://www.bigdataschool.ru/blog/iot-cybersecurity-tools-big-data.html
2. Этот опасный IoT: угрозы бизнесу и способы решения проблемы [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/company/zyxel/blog/463835/
3. Мережева безпека [Електронний ресурс] – Режим доступу до ресурсу: https://www.proxis.ua/uk/show-article/207/

Анотація

IoT мережі все більше проникають в побут, але також присутня тенденція створення IIoT – індустріальних мереж Інтернету речей, яка конкурує з промисловими мережами, тому питання безпеки IoT набувають актуального застосунку в площині промислових додатків.

Ключові слова: IoT, кібербезпека, промислова мережа.

Аннотация

IoT сети все больше проникают в быт, но также присутствует тенденция создания IIoT - индустриальных сетей Интернета вещей, которая конкурирует с промышленными сетями, поэтому вопросы безопасности IoT приобретают актуальности в плоскости промышленных приложений.

Ключевые слова: IoT, кибербезопасность, промышленная сеть

Abstract

IoT networks are increasingly penetrating into everyday life, but there is also a tendency to create IoT - industrial networks of the Internet of Things, which competes with industrial networks, therefore, IoT security issues are becoming relevant in the plane of industrial applications.

Keywords: IoT, cybersecurity, industrial network