«Сейфуллин оқулары – 16: Жаңа формациядағы жастар ғылыми – Қазақстанның болашағы» атты халықаралық ғылыми-теориялық конференциясының материалдары = Материалы Международной научно-теоретической конференции «Сейфуллинские чтения – 16: Молодежная наука новой формации – будущее Казахстана». - 2020. - Т.I, Ч.3 - С.140-142

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ И СПОСОБЫ ИХ РЕШЕНИЯ

Толегенова А.С., Игібай Н.Х.

Вопрос безопасности IoT – одна из главных проблем быстрого роста, которые неминуемо возникают, когда отрасль стремительно развивается. Согласно информации портала Statista, в 2025 году в мире будет 75 млрд. подключенных к сети устройств, которые необходимо защитить от виртуальных и физических атак. Многие устройства, подключенные к IoT, имеют ограниченную или вообще не обеспечивают эффективную защиту информации. Неспособность обеспечить эффективную безопасность имеет важные последствия для конфиденциальности и физической безопасности.

Компания OpenDNS, исходя из результатов исследования, заявила: безопасного IoT не существует. Инфраструктура, которая используется для подключения устройств в корпоративные сети, не контролируется ни пользователями, ни IT-специалистами. Вот лишь некоторые выкладки из экспертного отчета :

- только 35% компаний используют отдельную Wi-Fi сеть для потенциально небезопасных «интернет-вещей»;
- видеокамеры, медицинские гаджеты, фитнес-браслеты и другое оборудование передают данные за пределы корпоративной сети;
- жесткие диски используют для хранения данных небезопасные облачные серверы.

Чтобы помочь улучшить состояние безопасности устройств IoT , ниже приведены 10 рекомендаций, разработанных для устранения угрозы, с которой сталкивается практически любая организация [1].

1. Поместите устройства IoT в свою собственную сеть, защищенную брандмауэром и контролируемую сеть.

Когда дело доходит до подключения устройств IoT потребительского уровня на предприятии, вам необходимо применять упреждающий подход. Вы можете заблокировать входящий трафик на него, чтобы люди не могли атаковать изнутри, а также можете контролировать и пристально следить за ним.

2. Регулярно обновлять пароль. Использовать многофакторной аутентификации.

Многофакторная аутентификация может быть относительно простым способом повысить безопасность многих устройств IoT с помощью пользовательского интерфейса.

3. Отключите функциональность, когда она не нужна

Одна из наиболее важных стратегий безопасности - максимально сократить поверхность атаки.

4. Обеспечить защиту от физического вторжение

Есть несколько подключаемых устройств, которые уязвимы после полной перезагрузки. Если есть, рассмотрите возможность их блокировки, когда это возможно.

5. Остерегайтесь автоматических подключений Wi-Fi

Большое количество устройств IoT потребительского уровня предназначено для обнаружения Wi-Fi и просто подключается к любой сети, которую они могут найти, это может быть SSID, который не защищен паролем.

6. Блокируйте входящий трафик, когда это возможно. Если нет, следите за открытыми портами

Многие устройства IoT поставляются с открытыми портами для поддержки функций управления, а не стандартных функций, доступных через пользовательский интерфейс.

Опять же, смысл в том, чтобы максимально уменьшить поверхность атаки. Это может означать полную блокировку всего входящего трафика с помощью брандмауэра. Но в других случаях это будет означать только сохранение того, какие порты TCP и UDP вам нужны. Некоторые устройства IoT могут иметь нестандартные открытые порты[2].

7. Сделать шифрование по умолчанию

Зашифровать данные не всегда возможно для некоторых корпоративных приложений, зависящих от времени, но для большинства устройств IoT потребительского уровня можно гарантировать, что данные никогда не отправляются в виде открытого текста. Когда невозможно зашифровать, организации должны использовать VPN или другие средства маскировки своих данных.

8. Проводите исследования при использовании внутренних служб или приложений для устройств IoT

Избегайте использования любого веб-сервиса, о которых у вас нету никакой информации. Существует ряд инструментов, с помощью которых вы можете оценить безопасность веб-служб, которые могут быть подключены к вашим устройствам Интернета вещей. Такие службы проверяют, имеют ли они, скажем, хорошую конфигурацию для своих соединений TLS / SSL, используют ли они проверенные протоколы и имеют ли надежные конфигурации сайтов.

9. Обновите прошивку и программное обеспечение

Этот совет является одним из самых важных в списке. Если устройство IoT не может быть обновлено, его, вероятно, не должно быть на вашем предприятии.

В то время как большинство известных IoT-устройств, ориентированных на потребителя, поддерживают обновления, недорогие камеры видеонаблюдения являются одними из худших в этом отношении. Они часто используют готовые программные стеки с известными

уязвимостями, используют жестко запрограммированные пароли и не поддерживают обновления[3].

Хотя некоторые обновления могут быть автоматизированы, обновления встроенного программного обеспечения, как правило, выполняются вручную.

10. Следите за жизненным циклом IoT-устройств и откажитесь, когда это необходимо.

Если производитель, скажем, IoT-устройства внезапно выходит из бизнеса, может возникнуть необходимость избавиться от своего продукта. В некоторых случаях устройство все еще будет работать, но не будет обновляться, что возвращает нас к предыдущему пункту. Но в других случаях несуществующий производитель - или производитель, который убивает продуктовую линейку - блокирует устройства, которые он больше не производит, делая их бесполезными[4].

Список литературы

1. Интернет вещей: обзор проблем безопасности // Блог о разном: тренды, идеи, развитие. - 2017. [Электронный ресурс]. URL: https://business-online.su/blog/internet-veshchey-problemy-bezopasnosti/ (дата обращения: 22.12.2019).
2. Из чего состоит IoT // Хабрхабр. - 2019. [Электронный ресурс]. URL: https://habr.com/ru/post/436708/ (дата обращения: 24.12.2019).
3. Проблемы использования технологий интернет вещей / И.Я. Львович, А.П. Преображенский, Ю.П. Преображенский, О.Н. Чопоров // Вестник Воронежского института высоких технологий. — 2019. — № 1 (28).
4. Liu, Yahong; Jin, Xueyu; Zhou, Xin; и др. A phased array antenna with a broadly steerable beam based on a low-loss metasurface lens, JOURNAL OF PHYSICS D-APPLIED PHYSICS, Том: 49,Выпуск: 40, 12, 2016.