Урбанский Лев Евгеньевич

студент

Сапожников Игорь Дмитриевич

студент

Гагарина Лариса Геннадьевна

д-р техн. наук, профессор, заведующая кафедрой

ФГАОУ ВО «Национальный исследовательский университет

«Московский институт электронной техники»

г. Москва

«ИНТЕРНЕТ ВЕЩЕЙ» И ВОЗМОЖНОСТИ ДЛЯ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация: *в статье рассматриваются проблемы информационной безопасности устройств «Интернета вещей», приведены примеры инцидентов и рекомендации по предотвращению происшествий.*

Ключевые слова: *Интернет вещей, киберпреступления, информационная безопасность.*

Термин «Интернет вещей» относится к любому объекту или устройству, которое подключается к Интернету и которое автоматически отправляет и/или получает данные.

Все больше предприятий и простых домовладельцев используют устройства, подключенные к сети, для повышения эффективности или облегчения повседневной жизни. В то же время, подключение к сети этих устройств представляют серьезную угрозу безопасности пользователей.

Что представляют из себя устройства «Интернета вещей»?

– устройства, управляющие дистанционно или удаленно освещением или отоплением;

– системы безопасности, например, сигнализация или Wi-Fi камеры;

– медицинские устройства, например, датчики сердечного ритма;

– термостаты;

– фитнес-трекеры;

– «умные» холодильники или телевизоры;

– офисные устройства, например, принтеры.

Как подключаются устройства?

Устройства «Интернета вещей» подключаются через компьютерные сети для обмена данными с производителем, оператором или другими устройствами в сети.

Каковы риски?

Сложности в обновлении устройств, а также недостаточная информированность пользователей предоставляет злоумышленникам использовать уязвимости для проникновения в другие системы, кражи личной информации, рассылки вредоносного ПО или управление системами безопасности. Основными уязвимыми местами являются:

– эксплуатация протокола Universal Plug and Play (UPnP) для получения управления устройствами. UPnP описывает сценарий, в котором устройство удалённо подключается и обменивается информацией по сети без аутентификации, что делает протокол уязвимым для изменения конфигурации и незаконного сбора информации;

– использования стандартных паролей;

– захват управление устройством для причинения физического вреда;

– перегрузка устройства для вывода его из строя;

– вмешательство в бизнес-транзакции.

Примеры инцидентов:

1. Киберпреступники могут воспользоваться уязвимостями в замкнутых видео-системах, таких как камеры наблюдения, используемые на предприятиях, либо встроенные камеры на видео-нянях, используемых в частных домах или пансионатах. На многих подобных устройствах установлены пароли по умолчанию, которые известны злоумышленникам, некоторые также передают свое местоположение в интернет. Подобные устройства, не отвечающие требованиям безопасности, могут быть обнаружены и взломаны злоумышленниками, а, в

дальнейшем, использованы, чтобы транслировать происходящее перед камерой прямо в интернет, где это сможет увидеть любой желающий. Все пароли по умолчанию должны быть изменены в обязательном порядке и как можно скорее, а беспроводная сеть должна обязательно быть защищена паролем и брандмауэром.

2. Злоумышленники могут воспользоваться незащищенными беспроводными сетями, используемыми для автоматизированных устройств, таких как системы безопасности, гаражные ворота, термостаты и системы освещения. Уязвимости позволят преступникам получить полный доступ к автоматизированным устройствам, и как только злоумышленник получит такой доступ, он сможет проникнуть в домашнюю или корпоративную сеть и собирать конфиденциальную информацию, либо дистанционно наблюдать за пользователем, узнать его привычки, а также перехватить интернет-траффик. Если пользователь не сменит стандартный пароль, либо установит недостаточно сложный пароль, киберпреступники могут легко использовать интернет вещей для открытия дверей, отключения систем безопасности, записи аудио и видео, а также для доступа к конфиденциальной информации.

3. Спам-атаки через электронную почту осуществляются не только с помощью ноутбуков и стационарных компьютеров, либо мобильных устройств. Для этих целей злоумышленники также могут использовать домашние роутеры, сетевые медиа-центры, телевизоры и прочие устройства, использующие беспроводные сети. Такие устройства, обычно, уязвимы, как правило, из-за того, что на них установлен пароль по умолчанию, либо используется незащищенная беспроводная сеть.

4. Злоумышленники могут получить доступ к незащищенным устройствам, используемым в домашней медицине, таким как устройства для сбора и передачи медицинских показаний и устройства для повременной выдачи медикаментов. Как только злоумышленники получают доступ к таким устройствам, они получают доступ и к личной и медицинской информации, которая хранится на этих устройствах, а также они могут изменить дозировку лекарств, либо подменить

передаваемые устройствами медицинские показатели. Устройства могут быть подвержены риску взлома, если они способны передавать данные на большие расстояния.

5. Киберпреступники также могут осуществять атаки на критически важные устройства, подключенные к Интернет, такие как, например, системы мониторинга и контроля нефтяных насосов. Такая атака может привести к тому, что злоумышленники смогут передавать насосу неверные данные о наполнении топливной ёмкости, тем самым, либо, не заполнить ёмкость до конца, либо, наоборот, переполнить до критически опасного уровня, вызвав риск пожара и взрыва, также злоумышленники смогут пустить топливо в обход системы регистрации, таким образом, топливо не будет оплачено.

Защита потребителей и рекомендации по безопасности:

– устройства, реализующие Интернет вещей должны располагаться в собственной изолированной и защищенной сети;

– необходимо отключать UPnP на домашних роутерах;

– необходимо выяснить, действительно ли необходимо использовать именно Интернет вещей для решения поставленных задач;

– необходимо приобретать устройства только от надежных производителей, гарантирующих защищенность устройств;

– когда это возможно, необходимо устанавливать самые последние обновления для устройств;

– потребители должны быть осведомлены о возможностях устройств, устанавливаемых в их домах и офисах. Если на устройстве установлен пароль по умолчанию, его в обязательном порядке необходимо сменить. Если устройство использует незащищенное Wi-Fi соединение, его необходимо защитить надежным паролем и установить сетевой брандмауер;

– пользуйтесь текущими указаниями при подключении к устройствам по беспроводным сетям, а также при удаленном подключении;

– пациенты должны быть осведомлены о работе медицинских приборов, установленных у них дома. Если устройство поддерживает беспроводное управление, то это может быть мишенью для злоумышленников;

– убедитесь, что все пароли по умолчанию изменены на надежные. Никогда не используйте пароль по умолчанию, установленный производителем устройства, такие пароли легко найти в интернете. Для паролей не используйте словарные слова, либо личную информацию, такую как важные даты, имена детей или домашних животных. Если пароль на самом устройстве изменить невозможно – обеспечьте для данного устройства безопасное беспроводное соединение, защищенное надежным паролем.

Список литературы

1. [Электронный ресурс]. – Режим доступа: http://www.ic3.gov/media/2015/150910.aspx