УДК 004.771

Аюпов А.Я.,
студент
2 курс, факультет «Информационная безопасность»
Нефтекамский филиал Башкирского Государственного Университета
Россия, г. Нефтекамск
Научный руководитель: Аюпова А.Р.,
доцент кафедры математического анализа и информационной безопасности
Нефтекамский филиал Башкирского Государственного Университета
Россия, г. Нефтекамск

БЕЗОПАСНОСТЬ IOT-ПРОДУКТОВ

Аннотация: *В данной обзорной статье рассматривается проблемы IoT-продуктов и возможности использования дыр в безопасности, а так же некоторая статистика.*

Ключевые слова: *IoT-продукты, IoT-технологии, информационная безопасность, взлом, кибер-преступления, кибер-мошейничество.*

Abstract: *This review article discusses the problems of IoT products and the possibility of using security holes, as well as some statistics.*

Keywords*: IoT products, IoT technologies, information security, hacking, cybercrimes, cyberfraud.*

Эксперты Информационной Безопасности настойчиво утверждают, что производители, разработчики услуг и устройств рынка-IoT нарушают принцип сквозной информационной безопасности (ИБ), который рекомендован для

всех ИКТ-продуктов и услуг. Согласно этому принципу, ИБ должна контролироваться на начальном этапе проектирования продукта или услуги и поддерживаться вплоть до завершения разработки и выпуска. Слабые места IoT: Переход на IPv6.

- Питание датчиков.
- Стандартизация архитектуры и протоколов, сертификация устройств.
- Информационная безопасность.
- стандартные учётные записи от производителя, слабая аутентификация
- отсутствие поддержки со стороны производителе для устранения уязвимостей
- трудно или невозможно обновить ПО и ОС
- использование текстовых протоколов и ненужных открытых портов
- используя слабость одного гаджета, хакеру легко попасть во всю сеть
- использование незащищённых мобильных технологий
- использование незащищённой облачной инфраструктуры
- использование небезопасного ПО

Некоторые исследователи обращают внимание на проблемы как на стороне владельцев устройств, так и на проблемы, над которыми должны подумать разработчики. Так, в самом начале эксплуатации пользователю обязательно нужно заменить фабричный пароль, установленный по умолчанию, на свой личный, поскольку фабричные пароли одинаковы на всех устройствах и не отличаются стойкостью. К сожалению, делают это меньшинство пользователей. Поскольку не все продукты имеют встроенные средства ИБ-защиты, владельцам поэтому следует что позаботиться об установке дополнительной внешней защиты с тем чтобы интернет-устройства не стали открытыми шлюзами в домашнюю сеть или прямыми инструментами причинения ущерба.

В ходе исследований обнаружено, что примерно в 70% проанализированных устройств не шифруется беспроводной трафик. Веб-

интрефейс 60% устройств считаются небезопасными из-за небезопасной организации доступа и высоких рисков межсайтового общения устройств. В большинстве устройств предусмотрены пароли слабые по стойкости ко взлому. Примерно почти 90% устройств собирают ту или иную персональную информацию о владельце без его ведома.

Всего же насчитывают около 25 различных уязвимостей в каждом из исследованных устройств и их мобильных и облачных компонентах. Примерно атака происходит следующим образом:

Хакер меняет цвет или яркость лампы, чтобы обмануть пользователей: это заставляет их думать, что у лампы происходит сбой. Лампа отображается как «Недоступно» в пользовательском приложении управления, поэтому владельцы попытаются сбросить настройки.

Единственный способ сбросить настройки — удалить лампочку из приложения, а затем поручить контрольному сетевому мосту заново обнаружить лампу.

Контролирующий мост обнаруживает скомпрометированную хакерами лампу, и именно ее пользователь добавляет обратно в свою сеть.

Управляемая хакером лампочка с обновленной микропрограммой использует уязвимости протокола ZigBee, чтобы вызвать переполнение буфера на мосту управления, посылая ему большой объем данных. Эти данные также позволяют хакеру установить вредоносное ПО на мосту, который, в свою очередь, подключен к нужной компании или домашней сети.

Вредоносная программа подключается обратно к хакеру и злоумышленник, используя известный эксплойт (например, такой как EternalBlue), может проникать в нужную IP-сеть с моста для распространения вымогателей или шпионских программ

Вывод: безопасной целостной системы IoT продуктов на сегодняшний день не существует. IoT-вещ скрывают в себе возможности распространения целевых атак (APT). Стоит только злоумышленникам захотеть, найти цель и

любой из нас может стать их жертвой, и наши верные помощники из мира IoT превращаются в предателей, которые открывают доступ в мир своих владельцев.

Интернет вещи (IoT) становятся популярнее и потому распространяются по миру и находятся на пороге всплеска развития. Этому способствуют несколько факторов: появление 5G, промышленная революция, растущие возможности микропроцессорных вычислений.

Сегмент IoT-устройств имеют схожие проблемы внедрения – отсутствие единых стандартов, в том числе стандартизированной документации, качественного описания протоколов и соединений и соответствующая высокая цена анализа уровня фактической защищенности, отсутствие стандартизации функций защиты и, как правило, недостаток ресурсов микрочипов на качественное внедрение этих функций (шифрование, аутентификация и т.д.).

Из последних новостей стоит отметить Российский сегмент IoT-взлома. Так, например в Даркнете хакеры из России активно ищут возможности модификации и продажи специализированных прошивок для умных счётчиков газа, электричества и воды, так как российское правительство санкционировало замену всех коммунальных счетчиков на умные, подключенные к интернету. По истории сообщений, на форумах даркнета, пока имеется лишь один концептуальный план монетизации, напрямую продавать модифицированные счетчики как средства экономии на ежемесячных коммунальных счетах за электроэнергию, воду и газ. Наверно, в будущем взлом счетчиков станет новым способом криминального заработка, но на сентябрь 2020 года взлом этих устройств больше похож на ребячество, чем на профессиональные атаки. Так же IoT-вещи могут использованы для DDOS-атак и могут использованы в качестве узлов выхода VPN, связи с этим вы можете даже не подозревать что участвуете в ней. «Умный" счетчик может стоить до 12 тысяч рублей, однако цена тех, которые будут устанавливать

компании, окончательно прояснится после того, как правительство примет постановление с минимальными требованиями к таким приборам учета. [1]«В связи с этим «Умный счетчик» оборудуют каким либо сигнализатором об взломе или неисправности.

В заключение можно сказать что IoT-мир не идеален и стоит хорошо подготовиться перед тем как устанавливать такие устройства в свой дом и постоянно соблюдать нормы безопасности.

Использованные источники:

1. Архитектура интернета вещей. /Перри Ли, Райтман М.А., Мовчан Д. А. ДМК-Пресс, 2019 г.

2. Уязвимость, позволяющая хакерам проникнуть в сети с помощью эксплойта в протоколе ZigBee [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Продукт:Philips_Hue (Дата обращения: 23.11.2020).

3. Свет на учете. Госдума приняла закон об установке "умных" счетчиковэлектроэнергии во всех домах [Электронный ресурс]. URL: https://rg.ru/2018/12/20/gosduma-priniala-zakon-ob-ustanovke-umnyh-schetchikov-elektroenergii-vo-vseh-domah.html (Дата обращения: 22.11.2020).

[1] . Свет на учете. Госдума приняла закон об установке "умных" счетчиков электроэнергии во всех домах