www.orange-business.ru

Москва, 30 сентября 2014 г.

насколько безопасен интернет вещей

интернет вещей ближе, чем кажется, но безопасен ли он?

По оценкам аналитической фирмы IDC число подключенных к интернету устройств **к концу 2020 года достигнет 212 миллиардов.** Интернет вещей будет контролировать все сферы жизни: общественный транспорт, здравоохранение, дома, оборудование, автомобили, безопасность, бытовые приборы. **Все жизненные сферы будут взаимосвязаны.**

подключение

Подключенные к сети устройства будут собирать данные для повышения удобства и эффективности. Однако некоторые данные конфиденциальны, поэтому безопасность информации ставится под сомнение.

Сегодня безопасность интернета невысока. Отдел Fortify компании Hewlett-Packard провел исследование, в ходе которого изучалась безопасность некоторых «умных» устройств, таких как телевизоры, веб-камеры, термостаты, розетки, дверные замки и системы управления домом.

Каждое устройство взаимодействовало с каким-то облачным сервисом, а также мобильными приложениями. Тесты выявили у популярных представителей «интернета вещей» порядка **250 уязвимостей**, так что над безопасностью необходимо работать. (Полная версия отчета в формате PDF доступна по этой ссылке.)

уязвимость

По словам исследователей, «шесть из десяти устройств с пользовательским интерфейсом уязвимы – в частности, подвержены XSS-атакам и недостаточно защищены от несанкционированного доступа». Было обнаружено, что 90% устройств собирают персональную информацию, а 60% – обладают небезопасным пользовательским интерфейсом.

Исследование показало, что:

- 76% устройств используют незашифрованные сетевые сервисы, что делает их уязвимыми для «атак через посредника»;
- 80% устройств используют ненадежные пароли. Иногда **для защиты устройств и управления ими через «облачные» или мобильные приложения используются простые пароли наподобие «1234» или «123456»;**
- 60% устройств не защищают внутреннее ПО во время загрузки путем шифрования передачи, за счет чего хакеры могут внедрять в файлы дополнительные данные.

Исследователи считают, что «для получения доступа к устройству злоумышленник может воспользоваться такими уязвимостями, как слабые пароли, небезопасные механизмы восстановления паролей, плохо защищенные учетные записи и т. д.».

Но почему это так важно, когда речь идет всего лишь о бытовом приборе? Дело в том, что каждое подключенное к сети устройство взаимодействует с устройствами, которые находятся рядом с ним, обменивается информацией с облачными сервисами и передает ее другим устройствам.

Каждое устройство в сети отправляет и получает данные в потоке информации. Решения с потенциальной уязвимостью в такой цепи становятся приманкой для злоумышленников.

вопросы безопасности

На конференции Black Hat в 2014 году специалисты по безопасности доказали, что могут взломать термостат Nest за 15 секунд, всего лишь получив непрерывный доступ к устройству и заменив его прошивку на базе Linux вредоносным кодом, способным перехватывать сетевой трафик. Один из исследователей, Даниэль Буэнтелло (Daniel Buentello), предупреждал, что подключенные друг к другу бытовые приборы могут работать против нас. В ходе своего выступления «Превращаем кофеварку в оружие» он взломал выключатель света с поддержкой Wi-Fi.

В подтверждение отчета HP участники Black Hat 2014 узнали следующее: «большая часть современных устройств «интернета вещей» и компактных мобильных устройств страдают от одинаковых проблем **и не имеют надлежащей аппаратной защиты от подобных атак**».

Во время другого выступления на конференции Black Hat консультант по безопасности Хесус Молина (Jesus Molina) рассказал о недостатках системы автоматизации отеля**, позволивших ему получить управление почти всеми его бытовыми приборами.**

незначительная угроза

Уязвимость в «интернете вещей» уже не просто вызывает интерес – она представляет собой реальную угрозу. В этом году поступило множество сообщений об атаках на домашние роутеры и другие подключенные к сети системы, включая видеорегистраторы.

«По мере постоянного увеличения количества устройств «интернета вещей» проблемы безопасности растут в геометрической прогрессии. Пара мелочей на одном мобильном телефоне может перерасти в 50–60 проблем в домашней или рабочей сети со множеством устройств «интернета вещей», – сообщает HP Fortify.

Эти проблемы с безопасностью имеют еще большее значение, когда речь заходит о компактных мобильных устройствах, например, для здоровья и фитнеса. Незаконные действия по отношению к таким данным являются уже не просто вторжением в личную жизнь, но и могут представлять для злоумышленников коммерческий интерес. При сборе предприятиями конфиденциальных данных об автомобилях, домах и других подключенных к сети системах объем и ценность информации повышается в несколько раз.

И эти системы уже подверглись атакам: в прошлом году злоумышленники получили доступ к торговой системе крупной розничной сети в США и украли данные кредитных карт, **взломав компьютерную сеть предприятия через незащищенную систему кондиционирования воздуха.** Компания Qualys утверждает, что большинство из почти 55 000 систем кондиционирования, подключенных к интернету за последние два года, имеют уязвимости, которыми легко могут воспользоваться хакеры.

подумайте о безопасности

Какие меры могут предпринять поставщики решений для «интернета вещей» на таком огромном рынке?

Один из вариантов – смириться с рисками, внедрить системы для получения сообщений об уязвимостях и устранять их по мере обнаружения. Карстен Эйрам (Carsten Eiram), исследователь компании Risk Based Security, предупреждает о том, что у многих поставщиков такие системы отсутствуют.

HP Fortify считает, что поставщикам следует проверить существующие решения по списку **10 основных уязвимостей**, которым эти устройства подвержены в настоящее время. Этот список был составлен организацией Open Web Application Security Project («Проект безопасности открытых веб-приложений», OWASP).

Пользователям также необходимо сделать выводы. Если такие устройства есть у вас дома, необходимо выяснить, как защитить свою сеть и использовать предусмотренные в каждом устройстве средства безопасности. Джон Стюарт (John Stewart), директор по безопасности компании Cisco, предупреждает, что по мере увеличения количества подключенных к сети устройств «даже самые опытные специалисты по безопасности **с трудом** успевают за динамикой происходящего».

Однако точно известно, что использование таких подключенных к сети устройств в качестве объектов атаки может стать источником прибыли для злоумышленников. Учитывая развитие киберпреступности, любая брешь в системе безопасности «интернета вещей» может повлечь за собой **огромный урон** для всей планеты и создать существенную угрозу для мировой экономики.

Контакты для СМИ:
Дарья Абрамова
руководитель дирекции маркетинговых коммуникаций
Orange Business Services в России и СНГ
Т. +7 (495) 777-0-800 доб. 5817
М. +7 (919) 998-0750
dariya.abramova@orange.com