Осторожно — доступ разрешен!

Беседовал Александр Калигин

С повсеместным проникновением интернет-доступа и увеличением количества подключенных к Сети устройств все более остро встает вопрос обеспечения безопасности пользователей от злоумышленников. Но до сих пор основное внимание специалисты по безопасности уделяют персональным гаджетам — смартфонам, планшетам, ноутбукам. Мы же обсудили вопросы безопасности домашних подключенных устройств — ТВ-приставок и Wi-Fi-роутеров с и. о. руководителя службы информационной безопасности АО «ЭР-Телеком Холдинг» (торговая марка «Дом.ru») Михаилом Терешковым.

Насколько уязвимы домашние абонентские подключенные устройства — роутеры, ТВ-приставки, Smart TV и прочие? Какой тип устройств наиболее небезопасен?

В сети Интернет существует множество уязвимых устройств. Большинство из них известны и контролируемы, но периодически появляются новые способы взлома и несанкционированного доступа к абонентскому оборудованию.

Все домашние Wi-Fi-сети защищены паролем, поэтому просто подключиться к ним нельзя. Однако существуют программы для взлома роутеров. Сделать это можно во время подключения к беспроводной сети, когда к роутеру приходит запрос на разрешение и абонент вводит пароль, а также во время работы, когда роутер продолжает обмениваться данными, посылая пакеты информации, среди которой указывается и пароль сети. Эти пакеты данных можно перехватить и расшифровать, а в дальнейшем узнать пароль и взломать чужую сеть. Часть программ работает по принципу перебора паролей. В этих случаях очень важно заменить заводской пароль на более сложный и выбрать устойчивый способ шифрования Wi-Fi-сети. В некоторые роутеры встроена блокировка перебора паролей, что дополнительно защищает пользователя от взлома.

Также несанкционированный доступ к роутеру возможен через внешний IP-адрес роутера или IPTV-приставки. Если оператор устанавливает собственное оборудование, то техник сервиса обязан произвести корректную настройку конфигурации межсетевого экрана (Firewall) и заблокировать наиболее уязвимые параметры и ресурсы своей сети. При обнаружении новых уязвимостей, оператор дистанционно обновляет прошивку пользовательских оконечных устройств.

IPTV-приставка, как и Wi-Fi-роутер, имеет собственный IP-адрес и может быть доступна в сети. Поэтому для домашней сети рекомендуется использовать локальные, частные IP-адреса, которые не доступны из сети Интернет. IPTV-приставки имеют собственное программное обеспечение, обновление которого должно осуществляться оператором.

Какие именно риски несут в себе подключенные абонентские устройства? Эти риски актуальны только для абонентов или же и для самих провайдеров?

Из всех рисков можно выделить несколько наиболее актуальных:

- взлом оборудования с целью кражи учетных данных и совершения мошеннических действий со счетом клиента;
- взлом оборудования с целью несанкционированного использования канала связи;
- взлом оборудования с целью создания бот-сети для атак на ресурсы в Глобальной сети;
- взлом оборудования с целью майнинга криптовалют.

Перечисленные риски актуальны как для абонентов, так и для провайдеров, с той лишь разницей, что сети провайдеров, как правило, защищены несколькими уровнями систем безопасности.

Уровень их безопасности в большей степени зависит от аппаратной или программной части?

Уровень безопасности абонентских устройств в основном зависит от программной части.

Какие устройства предлагает абонентам ваша компания и почему именно их?

Доступ к цифровому ТВ «Дом.ru TV» можно получить с помощью одного из трех устройств: одноименной многофункциональной ТВ-приставки на базе моделей Humax 7000i и 9000i, созданной эксклюзивно для «Дом.ru», приставки «Дом.ru TV Mini» производства Kaon или CAM-модуля. С помощью каждого из устройств наши клиенты могут смотреть до 219 цифровых телеканалов, в том числе сразу 85 — в HD-формате.

ТВ-приставка «Дом.ru TV» — максимально технологичное решение для продвинутых пользователей, она открывает доступ к широкому ряду функций цифрового ТВ. В их числе catch up — трехдневный телеархив, многоуровневый поиск контента, запись эфира на внешний USB-носитель и постановка на паузу, выбор языка канала, родительский контроль — пароль на каналы и другие.

Приставка «Дом.ru TV Mini» интересна тем, что может быть подключена практически к любой модели телевизора. Клиенты могут смотреть цифровые и HD-каналы даже на устаревших телевизорах. Также с ее помощью можно осуществить запись на внешний USB-носитель, поставить эфир на паузу или пароль на каналы, выбрать язык канала, сформировать личные списки.

Пользователи, которые хотят смотреть «цифру» без дополнительных устройств, выбирают компактный CAM-модуль, который вставляется в специальный слот в телевизоре.

Нам важно, чтобы устройство поддерживало все современные технологии мультимедиа, включая VoD, потоковое видео, возможность отправить видео на другое устройство. Ключевой момент — это удобство пользователя. Мы стремимся сделать интерфейс устройства интуитивно понятным, работу всех функций — быстрой, а размеры приставок — минимальными.

Пользователи услуги Интернет от «Дом.ru» могут выбрать один из трех Wi-Fi-роутеров: обычный, двухдиапазонный или двухдиапазонный гигабитный. Первый обеспечивает среднюю скорость до 50 Мбит/с, легок в настройке и работает на частоте 2,4 ГГц. Второй работает в двух диапазонах — 2.4 ГГц и 5 ГГц, гарантирует стабильный доступ в Сеть на всей территории квартиры и высокую скорость — до 100 Мбит/с даже при большом количестве подключенных устройств. Роутер оптимален для просмотра потокового HD-видео, сетевых игр, быстрых загрузок, работы по удаленному защищенному каналу. Частота 2.4 ГГц является наиболее используемой для передачи информации по Wi-Fi, а более свободная частота 5 ГГц обеспечивает передачу сигнала без помех и разрывов. Третий отличается от предыдущего большей скоростью доступа в Интернет — свыше 100 Мбит/с. Мы стараемся предложить каждому сегменту клиентов релевантное их потребностям оборудование.

Всегда ли возможно выявить все уязвимости устройства на этапе тестирования? Гарантирует ли отсутствие незадекларированных возможностей наличие российской сертификации?

Нет, как минимум, существуют уязвимости нулевого дня — 0day, против которых еще не разработаны защитные механизмы. Сертификация гарантирует только отсутствие незадекларированных возможностей в конкретной версии программного обеспечения. После его обновления потребуется новая сертификация. Более того, она необходима только для средств защиты информации (СЗИ), коими абонентские устройства не являются.

Ведете ли вы статистику того, как часто злоумышленники взламывают такие устройства? Обращаются ли с такими проблемами сами абоненты?

Если целью было совершение мошеннических действий со счетом клиента, то конечно. В этом случае абоненты сами к нам обращаются, а обстоятельства инцидентов расследуются. Если целью злоумышленника было создание бот-сети или, например, нелегальное подключение соседей к беспроводному Интернету, то, как правило, клиенты об этом даже не подозревают.

Оборудование «Дом.ru» позволяет использовать только те протоколы, которые обеспечивают надежное безопасное соединение. На всех наших устройствах изменены заводские данные для административного доступа, своевременно, централизованно и массово обновляются прошивки, в том числе с целью устранения новых уязвимостей в программном обеспечении. Если пользователи самостоятельно приобретают и устанавливают оборудование, в этом случае безопасность — своевременную смену паролей, установку обновлений, проведение диагностики — они должны обеспечивать самостоятельно.

Существует ли необходимость в разработке национальных стандартов информационной безопасности и выработки критериев доверенного оборудования?

Существует необходимость в разработке международных стандартов по обеспечению безопасности устройств Интернета вещей. Сейчас производители не уделяют должного внимания этим вопросам, поэтому самые большие бот-сети построены на IoT-устройствах и с их помощью проводятся масштабные DDoS-атаки.

На ваш взгляд, каковы должны быть основные критерии доверенного оборудования?

Их несколько. Во-первых, организация хранения идентификационных данных пользователя в закрытом, зашифрованном виде. Во-вторых, возможность своевременного обновления программного обеспечения только специалистами, ответственными за эксплуатацию оборудования. И в-третьих, наличие процедур, обеспечивающих безопасность обновления программного обеспечения.

В России проводится политика импортозамещения. Насколько это необходимо и возможно в отношении абонентского оборудования?

Большая часть оборудования и программного обеспечения на российском рынке связи — импортное. Основная доля приходится на производителей из Юго-Восточной Азии, которые не входят в список стран, применяющих экономические санкции в отношении нашей страны. Доля отечественных производителей небольшая, а линейка производимого ими оборудования недостаточно широкая. Несмотря на это, мы не только планируем внедрять новые решения, но уже используем продукты, представленные в реестре отечественного ПО, а также оборудование российских производителей. ■