Автор: Administrator
22.05.2015 14:19 -

Если действенный способ защиты своего дома? Быть может, есть какая-то новейшая система домашней безопасности, которая относится к классу «умных» из числа Интернет-решений? Конечно, есть, но специалисты утверждают, что обратившись к ним за помощью, можно быть менее защищенным и более уязвимым, чем до их установки. Почему же они делают такой вывод? Они опираются на выводы, сделанные разными компаниями во время тестирования устройств компьютерной безопасности! Оказывается, несмотря на широкую рекламу в массах, они не защищены от взломов хакеров…

Системы домашней безопасности сегодня подключены к Интернету, и могут соединяться через облако с мобильным устройством, web-браузером. Таким образом, каждый владелец может держать под контролем их работу. В составе такой системы очень много разных устройств, будь-то детекторы движения, видеокамеры, датчики утечки, присутствия, «умные замки» и т.д. Хоть они и должны способствовать тому, чтобы в дом никто не пробрался, но на деле у них очень много разного рода уязвимостей. В итоге держать дом под контролем может не только владелец системы, но и кто-то другой. Почему? Потому что отсутствуют установленные стандарты для защиты «умных» систем для дома.

Совсем недавно специалисты из компании «HP» опубликовали отчет, в котором провели анализ параметров защищенности систем на примере десяти самых популярных и делающих дом «умным». Специалисты попросту решили провести взлом всех 10 систем, выяснив ту или иную уязвимость. После этого они стали осуществлять сбор сведений о доме, в том числе и тех из них, которые касались видеокамер. Кол-во проблем испугало специалистов. Они были связаны с авторизацией, идентификацией, работой облачных и мобильных web-интерфейсов.

**Проблемы с защищенной аутентификацией и авторизацией**

- Использование простых паролей (опция, разрешенная самой системой);
- Нужда в механизме блокировки аккаунта, который позволяет проводить предотвращение автоматизированных атак;
- Отсутствие защиты от подбора аккаунта (угадывание данных, получение доступа);
- Получение видеодоступа к камерам, которые были установлены на четырех из семи систем;
- Две системы могли передавать видео без произведения операции по аутентификации;
- Одно устройство было оснащено 2-факторной аутентификацией.

**Вывод**

Чтобы обеспечить надежную защиту, производители должны правильно шифровать передачу данных. Правда, они почему-то не делают этого. 70% от предлагаемых на рынке устройств передавали данные аккаунта с задействованием незащищенного облачного интерфейса. При проведении обновления задействовали FTP (перехват сведений, получение доступа на сервер обновлений, запись на него).

Вот и выходит, что желая защититься, люди наоборот оказываются незащищенными, даже купив самое дорогое устройство из тех, которые есть на рынке.