6 советов по повышению безопасности работы в сети Wi-Fi

СОВЕТ 1. ИСПОЛЬЗУЙТЕ НЕТРИВИАЛЬНЫЙ ПАРОЛЬ НА ДОСТУП К СЕТИ И СТАНДАРТ ШИФРОВАНИЯ ПАРОЛЯ WPA2

Вы только что установили Wi-Fi-роутер и подключили его к сети Интернет-провайдера (скорее всего, через проводной Ethernet-интерфейс). Первое, что вам нужно сделать, - установить пароль на доступ к сети и сменить стандарт шифрования паролей. Сам по себе пароль должен быть достаточно сложным (myWiFi, qwerty, 1111 и admin – не самые подходящие варианты) и не должен содержать в себе никакой информации, персонализирующей вас. То есть, ваши имя и фамилия, дата рождения, имя вашего домашнего питомца в качестве пароля – табу.

На текущий момент поддерживаются три беспроводных стандарта шифрования паролей. Это Wired Equivalent Protection (WEP), Wi-Fi Protected Access (WPA) и Wi-Fi Protected Access 2(WPA2).

В 2003 году Альянс Wi-Fi официально объявил о переходе с WEP на стандарт WPA ввиду его, WEP, высокой уязвимости. На самом деле, взлом WEP-защищенной Wi-Fi-сети – дело пары минут и элементарного в использовании программного обеспечения с набором таких утилит, как восстановление WEP-защищенного ключа, атаки по словарю и сниффер пакетов.

Wi-Fi Protected Access (WPA) был введен в эксплуатацию в 1999 году, и других приемлемых вариантов по шифрованию паролей в Wi-Fi не было вплоть до 2004 года, когда был представлен стандарт WPA2, улучшенная версия WPA. Все сертифицированные Wi-Fi-устройства, выпускаемые с 2006 года, поддерживают оба стандарта, WPA и WPA2.

Несмотря на то, что WPA – это ощутимый шаг вперед по защищенности в сравнении с WEP, существует ряд уязвимостей, которые делают этот стандарт открытым для атак. Самая примечательная из уязвимостей заключается в опции Wi-Fi Protected Setup (WPS), которой оснащается большинство новых моделей роутеров. Уязвимость WPS позволяет хакеру взломать пароль, в среднем, за 2 или 3 часа.

Если вы используете WPA или WPA2 для защиты вашей беспроводной сети, убедитесь, что опция WPS на вашем роутере выключена.

Wi-Fi Protected Access 2 (WPA2) на сегодня сильнейший из трех представленных здесь стандартов шифрования паролей в Wi-Fi, благодаря усовершенствованным методам шифрования и довольно жесткому тестированию перед вводом в эксплуатацию по инициативе Альянса Wi-Fi.

СОВЕТ 2. ИСПОЛЬЗУЙТЕ ФИЛЬТРАЦИЮ ПО MAC-АДРЕСУ

Одним из самых сильных инструментов роутера в плане безопасности и разграничения доступа является список подключаемых устройств, хранящийся в его памяти. Устройства, присутствующие в списке, пройдут успешную аутентификацию и получат доступ к беспроводной сети. Клиенты, пытающиеся подключиться к сети с устройств, в этом списке отсутствующих, - получат отказ в подключении. Другими словами, это опция фильтрации по MAC-адресу.

В теории, фильтрации по MAC-адресу должно быть достаточно для того, чтобы избежать любых несанкционированных подключений к вашей сети, кроме ситуации, когда злоумышленник получил доступ администратора к роутеру (как этого избежать, будет сказано далее) и может изменить содержимое таблицы MAC-адресов, добавив свой. Или другой вариант, когда тот же злоумышленник с помощью сниффера перехватывает данные о разрешенных в вашей сети MAC-адресах и подменяет свой MAC-адрес одним из них.

Каков вывод? Фильтрация по MAC-адресу – это действительно мощное оружие в вашем арсенале по защите беспроводной сети, оно способно остановить львиную долю хакерских атак «коврового» действия, однако может не устоять перед направленной атакой настойчивого взломщика, не пожалевшего времени на то, чтобы получить доступ к вашей сети.

СОВЕТ 3. СВЕДИТЕ К МИНИМУМУ УРОВЕНЬ И ОБЛАСТЬ ПОКРЫТИЯ СИГНАЛА

Некоторые модели роутеров позволяют настраивать силу и область покрытия сигнала. Такая настройка очень актуальна, если вы точно знаете, что максимальное покрытие, в котором вы нуждаетесь, ограничено пределами только вашей квартиры и никогда не превысит, к примеру, 30 метров. А если ваш роутер в стандартных условиях «держит» 50-100 метров покрытия, то считайте, что остальные 20-70 метров вы отпускаете в «свободное плавание», давая возможность вашим любознательным соседям с хакерскими наклонностями попытаться подключиться к вашей сети.

Следует заметить, что большинство беспроводных роутеров не предоставляют эту функцию в чистом виде, а позволяют манипулировать уровнем мощности передачи. А это не совсем то, что нам нужно, так как изменение уровня мощности передачи на низкий (например, на 20/100) приведет к ухудшению сигнала на всей области покрытия.

СОВЕТ 4. НЕ ИСПОЛЬЗУЙТЕ НА РОУТЕРЕ НАСТРОЙКИ SSID ПО УМОЛЧАНИЮ

Смена настроек SSID по умолчанию сама по себе мало в чем поможет против атаки продвинутого и заинтересованного во взломе именно вашей сети хакера. Однако, это неплохой психологический ход, который может отбить охоту у хакеров низкого и среднего пошиба атаковать вашу сеть. Смена SSID явно указывает на то, что вы в курсе комплекса мер по обеспечению безопасности беспроводной сети и, что вполне логично, реализовали их у себя. Взлом вашей сети превращается из банальной в более продвинутую задачу, требующую дополнительных временных затрат и, возможно, другого уровня знаний. А это не всегда интересно. Чаще хакеру средней руки просто хочется получить доступ к бесплатному Интернету, и сделать это поскорее, так что хакер переключится на сеть «попроще».

Какие именно настройки SSID имеются в виду? Это, во-первых, SSID-имя (имя вашей сети, которое будет выводиться в списке доступных сетей устройства, пытающегося подключиться). Можно задавить хакера своим авторитетом, используя в качестве SSID какой-то технический термин в тему. С первого взгляда убедившись в вашей технической продвинутости, хакер наверняка переключит свое внимание на сеть соседа с SSID Vasya95.

Вторая опция настроек SSID – это широковещательная рассылка SSID. Отключив возможность широковещательной рассылки SSID на вашем роутере, вы сильно усложните хакеру (помним, что речь все еще о хакерах низкого и среднего пошиба) процесс обнаружения вашей сети, если он пользуется стандартными утилитами операционной системы. Тем не менее, невозможность решения этой задачи сводится на нет с помощью нехитрых манипуляций с такими утилитами, как inSSIDer или NetStumbler. Так что не расслабляемся.

СОВЕТ 5. ВСЕГДА МЕНЯЙТЕ IP-АДРЕС И ПАРОЛЬ АДМИНИСТРАТОРА НА ДОСТУП К WEB-ИНТЕРФЕЙСУ РОУТЕРА

Забавно наблюдать, когда, скорее всего по невнимательности или забывчивости, беспроводной роутер, настроенный по всем правилам обеспечения безопасности, вдруг впускает в свою панель настройки по стандартному набору вида 192.168.1.50/admin:admin. Такая забывчивость может дорого обойтись, пример уже приводился в этой статье выше. Да и хакер повеселится, осматривая ваши трехметровые бронированные ворота без намека на забор.

СОВЕТ 6. ВСЕГДА ОТКЛЮЧАЙТЕ ФУНКЦИЮ НАСТРОЙКИ РОУТЕРА ЧЕРЕЗ БЕСПРОВОДНОЕ СОЕДИНЕНИЕ

Данный совет – в продолжение предыдущему. Отключение данной функции означает, что настройку роутера можно осуществить только через физическое проводное подключение, а значит, требует включения хакера в проводную сеть, а значит… А зачем?