Ежемесячный журнал по вопросам компьютерной безопасности

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Ваша беспроводная сеть
- OpenDNS
- Ваши устройства

Защита Домашней Сети

Обзор

Ещё несколько лет назад домашний интернет был предельно простым и представлял собой одну или две точки входа в Интернет или онлайн игры. Однако теперь домашние сети намного сложней. Мы не только подключаем к сети большее количество устройств, но и с их помощью совершаем гораздо больше операций. В этом выпуске мы поговорим о базовых шагах создания безопасной домашней сети.

Об авторе

Кевин Джонсон – CEO компании Secure Ideas, владеет сервисом **MySecurityScanner.com**, является ведущим инструктором SANS Institute. Больше информации о Кевине на сайте: **www.secureideas.com**

Ваша беспроводная сеть

Почти в каждом доме есть так называемая беспроводная сеть (или WiFi сеть). Это позволяет подключить к сети Интернет любое устройство, начиная от ноутбуков и игровых приставок до телевизоров, без проводов. Для этого нужна беспроводная точка доступа. Подключение к ней осуществляется с помощью устройства под названием раутер (он может быть встроенным в модем), который посылает беспроводной сигнал для подключения устройств к сети. Как только ваши устройства соединятся с точкой доступа, они могут соединяться и с другими устройствами домашней сети. Таким образом, беспроводная точка доступа является одной из ключевых частей домашней сети, и мы рекомендуем следующие шаги для её защиты.

- Для большинства точек доступа используется по умолчанию логин и пароль администратора, который многие знают или даже можно найти в Интернет. Прежде всего, нужно поменять логин и пароль администратора на ваш собственный, который будете знать только вы. Убедитесь, что используете уникальный пароль, а не пароль от других аккаунтов.
- Следующее, что вы должны сделать, сконфигурировать имя вашей сети (его ещё называют SSID). Это имя будут видеть ваши устройства при поиске домашней сети. Имя следует выбрать уникальное, чтобы сеть было легко идентифицировать, но не используйте никаких персональных данных. Также нет смысла конфигурировать вашу сеть как скрытую или

Защита Домашней Сети

невидимую. Все детали скрытой сети легко можно узнать с помощью специальных сканирующих программ и для опытных злоумышленников это не будет преградой.

для защиты домашней сети убедитесь, что вы используете защищенную беспроводную сеть, пользуетесь Open DNS или подобным сервисом и регулярно обновляете все устройства домашней сети

- Необходимо обеспечить доступ к сети только узкому кругу людей. Убедитесь, что соседи не могут подключаться к вашей сети или мониторить её. Вы можете легко уменьшить эти риски, разрешив усиленную защиту вашей беспроводной точки доступа. В настоящее время лучшим способом защиты является механизм безопасности WPA2. Эта система запрашивает пароль у всех желающих подключиться к вашей домашней сети. После аутентификации эти соединения зашифрованы. Убедитесь, что вы не пользуетесь устаревшими способами защиты, например, WEP, или защиты нет вообще – это называется открытой сетью. Любой может подключиться к вашей открытой сети без аутентификации.

- Убедитесь, что используете сильный пароль, его сложно подобрать, и он отличается от пароля администратора. Помните, для большинства устройств нужно ввести его однажды. Устройства его запомнят, и будут хранить.

- Большинство беспроводных точек доступа поддерживают режим гостевой сети. Гостевая сеть позволяет гостям подключиться к вашей беспроводной точке доступа и получить доступ в интернет, но они не могут подключаться к устройствам вашей домашней сети. Если вы используете гостевую сеть, необходимо включить защиту WPA2 и использовать новый пароль к ней.

- Если вам сложно запомнить многочисленные пароли, используйте менеджер паролей.

Open DNS

После того, как вы сконфигурируете беспроводную сеть, мы рекомендуем использовать Open DNS в качестве DNS серверов вашей домашней сети. Также вы можете воспользоваться услугой Norton ConnectSafe for Home. Когда вы вводите имя веб сайта в браузере, DNS подсказывает браузеру

Защита Домашней Сети

адрес сервера, к которому нужно подключиться. Такие сервисы, как Open DNS, определяют инфицированные веб сайты и блокируют доступ к ним с любого устройства домашней сети. Эти серверы дают дополнительную возможность фильтровать и блокировать веб сайты с нежелательным содержанием. Этот подход особенно эффективен тем, что не требует дополнительной установки программного обеспечения на ваших устройствах: вы просто конфигурируете беспроводную точку доступа.

Ваши устройства

Следующий шаг - определение того, что подключено к вашей домашней сети и проверка безопасности подключённых устройств. Раньше это было проще, так как устройств было немного. Но в наши дни почти любой прибор можно подключить к домашней сети, включая телевизоры, игровые консоли, детские мониторы, колонки, домашнюю систему отопления и даже автомобиль. Как только вы определили все устройства домашней сети, их количество может вас удивить. Для обеспечения безопасности данных устройств используйте последнюю версию их операционной системы. При любой возможности подключите функцию автоматического обновления. Если такой функции нет, то проверяйте обновления и делайте это ежемесячно. Проверяйте сайт вашего интернет провайдера – он может предоставить бесплатные инструменты и сервисы для безопасности домашней сети.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

Ресурсы

OpenDNS
http://www.opendns.org
Norton ConnectSafe:
http://dns.norton.com/dnsweb/dnsForHome.do
Network security scanner:
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
Менеджер паролей:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова