Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

- **Безжичната мрежа**
- **Устройствата**

Защита на домашната мрежа

Преглед

Допреди няколко години домашните мрежи бяха сравнително прости, обикновено нищо повече от безжична точка за достъп и един или два компютъра за сърфиране, онлайн пазаруване или игри. Оттогава домашните мрежи станаха значително по-сложни. Днес свързваме далеч повече устройства към тези мрежи и ги използваме за доста повече неща от просто сърфиране и ползване на онлайн медии. В този бюлетин ще обясним как да изградите сигурна домашна мрежа за вас и вашето семейство.

Гост-редактор

Черил Конли е начело на звено „Обучение и информираност в сигурността" в Локхийд Мартин, работеща усилено по кампанията The I Campaign™, която обхваща над 100 000 служители. Това включва работни групи в цялата компания в допълнение към глобална фишинг програма. Можете да последвате Черил на **@conleychera**.

Безжичната мрежа

Почти всяка домашна мрежа започва с безжична мрежа (наричана понякога Wi-Fi мрежа). Това е което ви дава възможността да свържете безжично устройствата си с Интернет, от лаптопи и таблети до игрови конзоли и телевизори. Повечето домашни безжични мрежи се управляват от вашият Интернет рутер, който е устройството инсталирано в дома ви от Интернет доставчика, за да ви свърже с Интернет. В някой случаи безжичната ви мрежа може да се управлява от отделна система, наричана безжична точка за достъп, която е свързана към Интернет рутера. Който и от двата варианта да е налице, начинът на работа е един и същ – излъчване на безжичен сигнал. Различните устройства в дома ви се свързват с безжичната мрежа чрез този сигнал. От там тези устройства се свързват с Интернет и с другите устройства в домашната ви мрежа. Това означава, че защитата на безжичната мрежа е много важна част от защитата на вашия дом. Препоръчваме следните стъпки, за да я защитите.

- Сменете заводската администраторска парола за Интернет рутера или безжичната точка, в зависимост от това кое управлява безжичната мрежа. Администраторският достъп е това, което позволява да се променят настройките на безжичната мрежа. Проблемът тук е, че много рутери или безжични точки се доставят със заводски потребител и парола, които са общоизвестни и често публикувани в Интернет. Това налага да се смени администраторската парола със сложна и уникална такава, известна само на вас.
- Сменете заводското име на безжичната мрежа (наричано понякога SSID). Това е името виждано от устройствата, когато те търсят безжична мрежа наоколо. Дайте на мрежата си уникално име, така че лесно да я разпознавате, но се уверете, че в името няма никаква лична информация. Има много малко

Защита на домашната мрежа

полза от настройването на мрежата като скрита (т.е. без да излъчва името си), тъй като повечето програми за безжично сканиране и повечето злосторници много лесно откриват скритите мрежи.

- Уверете се, че само доверени хора могат да се свържат към безжичната ви мрежа и че връзката е криптирана. Това се прави като активирате силна защита. В момента най-добрият вариант е да се използва механизъм наречен WPA2. В този случай ще се изисква парола за достъп до домашната ви мрежа и връзката ще бъде криптирана след като веднъж е установена. Уверете се, че не използвате по-старите, отживели методи, като WEP, или не сте изобщо без механизъм за сигурност, което се нарича отворена мрежа. Отворените мрежи позволяват на всеки да се свърже към безжичната ви мрежа без каквато и да е оторизация.

За да предпазите домашната си мрежа, защитете безжичната мрежа и обновете и защитете с парола всички устройства в мрежата.

- Уверете се, че паролата, използвана за достъп до безжичната ви мрежа е сложна и е различна от администраторската. Помнете, че най-вероятно ще се налага да въвеждате паролата само по веднъж за всяко устройство, тъй като устройствата могат да съхраняват и помнят паролата.
- Много безжични мрежи поддържат т.нар. Мрежа за гости (Guest Network). Това позволява посетители да се свързват към Интернет, но защитава домашната ви мрежа, тъй като те не могат да се свързват към другите ви свързани устройства. Ако създадете мрежа за гости, уверете се, че сте включили WPA2 и че паролата за тази мрежа е уникална.
- Изключете т.нар. Wi-Fi Protected Setup или други механизми позволяващи нови устройства да се свързват към мрежата без да знаят паролата или настройките.
- Ако се затруднявате да помните всичките тези различни пароли, препоръчваме ви да ползвате софтуер за управление на пароли, за да ги съхранявате по сигурен начин.

Не сте сигурни как да направите тези стъпки? Обърнете се към Интернет доставчика си, проверете документацията, с която идва Интернет рутера ви или безжичната точка, или посетете уебсайта на производителя им.

Устройствата

Следващата стъпка е да знаете какво е свързано към домашната ви мрежа и да проверите дали всички тези устройства са защитени. Някога това беше просто, когато биваха свързвани само няколко устройства. В днешния

Защита на домашната мрежа

„винаги свързан" свят почти всичко може да се свърже към домашната ви мрежа, включително телевизори, игрови конзоли, бебефони, тонколони, термостатът на парното и може би дори колата ви. Един лесен начин да откриете какво е свързано към домашната ви мрежа е да използвате прост мрежов скенер, например Fing. Тези програми, които можете да инсталирате на компютъра или мобилното си устройство, сканират безжичната ви мрежа и докладват за всяко свързано устройство. Веднъж като идентифицирате всички устройства в домашната си мрежа, трябва да се убедите, че всяко едно от тях е защитено. Най-добрият начин да направите това е да се погрижите те винаги да ползват най-новата версия на операционната система/фърмуер. Където е възможно, включете автоматичното обновление. Ако някое устройство изисква парола, винаги използвайте уникална и сложна парола. И накрая, погледнете уебсайта на Интернет доставчика си, тъй като той може да предлага безплатни инструменти, с които да си помогнете в защитата на домашната мрежа.

НАУЧЕТЕ ПОВЕЧЕ

Абонирайте се за месечния бюлетин за информационна сигурност OUCH!, разгледайте архивните броеве на OUCH! и научете повече за решенията за информационна сигурност на SANS като ни посетите на http://www.securingthehuman.org.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:
https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962
https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b

Ресурси

Пароли:	https://securingthehuman.sans.org/ouch/2015#april2015
Мениджъри на пароли:	https://securingthehuman.sans.org/ouch/2015#october2015
Защитете своя нов таблет:	https://securingthehuman.sans.org/ouch/2016#january2016
Карта на домашната ви мрежа:	http://l.rud.is/home-network-mapping

Редакторски колектив: Бил Уайман, Уолт Скривенс, Фил Хофман, Боб Рудис
Превод: Николай Дачев и Радослава Несторова