SANS SECURITY AWARENESS

OUCH! | Януари, 2018 г.

Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

Създаване на кибер-сигурен дом

Преглед

Преди няколко години създаването на кибер-сигурен дом беше просто; повечето домове нямаха повече от една безжична мрежа и няколко компютъра. Днес технологията е станала много по-сложна и е интегрирана във всяка част от нашия живот, от мобилни устройства и конзоли за игри до домашния термостат и дори може би хладилника. Ето четири прости стъпки за създаване на кибер-сигурен дом.

Гост-редактор

Мат Бромили през деня работи в екип по реагиране при инциденти, където помага на клиенти от всякакъв мащаб да се справят при изтичане на данни. Той също така е инструктор на SANS и води курс FOR508 - Advanced Digital Forensics, Incident Response, and Threat Hunting. Следвайте Matt на **@mbromileyDFIR**.

Вашата безжична мрежа

Почти всяка домашна мрежа започва с безжична (или Wi-Fi) мрежа. Това позволява на всичките ви устройства да се свързват с интернет. Повечето домашни безжични мрежи се управляват от вашия интернет рутер или отделна безжична точка за достъп. И двете устройства работят по един и същи начин чрез излъчване на безжични сигнали, а устройствата във вашия дом се свързват чрез тези сигнали. Това означава, че защитата на безжичната ви мрежа е ключова част от сигурността на вашия дом. Препоръчваме ви следните стъпки, за да я защитите.

- Променете администраторската парола по подразбиране в интернет рутера или в безжичната точка за достъп, което от двете устройства контролира вашата безжична мрежа. Администраторският акаунт е това, което ви позволява да конфигурирате настройките за вашата безжична мрежа.
- Уверете се, че само хора, на които имате доверие, могат да се свържат с вашата безжична мрежа. Направете това, като осигурите добра сигурност. Понастоящем най-добрият вариант е да използвате защитния механизъм, наречен WPA2. С въвеждането на това е необходима парола, за да могат хората да се свързват с вашата домашна мрежа и след като свържат, онлайн действията са криптирани.
- Уверете се, че паролата, използвана за свързване с вашата безжична мрежа е достатъчно добра и че е различна от паролата за администратора. Не забравяйте, че трябва да въведете паролата само веднъж за всяко от устройствата, тъй като те съхраняват и запомнят паролата.
- Много безжични мрежи поддържат мрежа за гости - Guest Network. Това позволява на посетителите в дома да се свързват с интернет, но защитават вашата домашна мрежа, тъй като не могат да се свързват с някое от другите устройства във вашата домашна мрежа. Ако добавите мрежа за гости, не забравяйте да

Създаване на кибер-сигурен дом

активирате WPA2, както и уникална парола за тази мрежа.

Не сте сигурни как да направите тези стъпки? Обърнете се към вашия доставчик на интернет услуги или проверете техния уебсайт, проверете документацията, предоставена с интернет рутера или безжичната точка за достъп, или се обърнете към съответния уебсайт.

Следвайте тези четири прости стъпки, за да създадете кибер-сигурен дом -подсигурете Wi-Fi мрежата, активирйате автоматично актуализиране, използвайте уникални пароли и правете резервни копия.

Вашите устройства

Следващата стъпка е да знаете какви устройства са свързани към безжичната домашна мрежа и да се уверите, че всички тези устройства са в безопасност. Това беше просто, когато имаше само един или два компютъра. Днес обаче почти всичко може да се свърже с вашата домашна мрежа, включително смартфоните, телевизорите, конзолите за игра, бебефоните, високоговорителите или дори колата. След като идентифицирате всички устройства във вашата домашна мрежа, уверете се, че всяко от тях е защитено. Най-добрият начин да направите това е да сте сигурни, че има възможност за автоматично актуализиране, когато това е възможно. Кибер-атакуващите постоянно намират нови слабости в различните устройства и операционни системи. С активирането на автоматичните актуализации компютърът и устройствата винаги използват най-актуалния софтуер, което ги прави много по-трудни за проникване.

Пароли

Следващата стъпка е да използвате силна уникална парола за всяко от вашите устройства и онлайн профили. Ключовите думи тук са силна и уникална. Писнало ви е от сложни пароли, които трудно се запомнят и трудно се пишат? И ние сме така. Вместо това, използвайте фраза за достъп. Това е вид парола, която използва серия от думи, които лесно се запомнят, като например „Къде ми е кафето?“ или „слънце-поничк-щастие“. Колкото по-дълга е вашата парола, толкова по-силна е тя. Уникална парола означава използването на различна парола за всяко устройство и онлайн акаунт. По този начин, ако една парола е компрометирана, всички останали профили и устройства са все още обезопасени. Не можете да помните всички тези силни, уникални пароли? Не се притеснявайте, и ние не можем. Ето защо ви препоръчваме да използвате мениджър за пароли - специална програма за сигурност, която съхранява сигурно всичките ви пароли в криптиран виртуален сейф.

И накрая, активирайте удостоверяване в две стъпки, когато е възможно, особено за онлайн профилите си. Удостоверяването в две стъпки е много по-силно. То използва паролата ви, но също така добавя и втора стъпка,

като например код, изпратен на вашия смартфон или приложение на вашия смартфон, което генерира кода. Удостоверяването в две стъпки е може би най-важното нещо, която можете да предприемете, за да се защитите онлайн и е много по-лесно, отколкото сте предполагали.

Архивиране

Понякога, без значение колко сте предпазливи, може да ви хакнат. Ако случаят е такъв, често единственият начин да си възвърнете личната информация е да я възстановите от резервно копие - архив. Правете редовно архивиране на всяка важна информация и проверете дали успявате да възстановите информацията от него. Повечето мобилни устройства поддържат автоматично архивиране в облака. За повечето компютри може да се наложи да закупите някакъв вид софтуер или услуга, които са на сравнително ниски цени и са лесни за използване.

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 securingthehuman.sans.org/ouch/archives.

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

Фрази за достъп:	https://securingthehuman.sans.org/ouch/2017#april2017
Мениджър на паролите:	https://securingthehuman.sans.org/ouch/2017#september2017
Удостоверяване в две стъпки:	https://securingthehuman.sans.org/ouch/2017#december2017
Архивиране:	https://securingthehuman.sans.org/ouch/2017#august2017

Редакторски колектив: Уолт Scrivens, Фил Хофман, Кати Кликнете, Черил Конли
Превод: Николай Дачев и Радослава Несторова