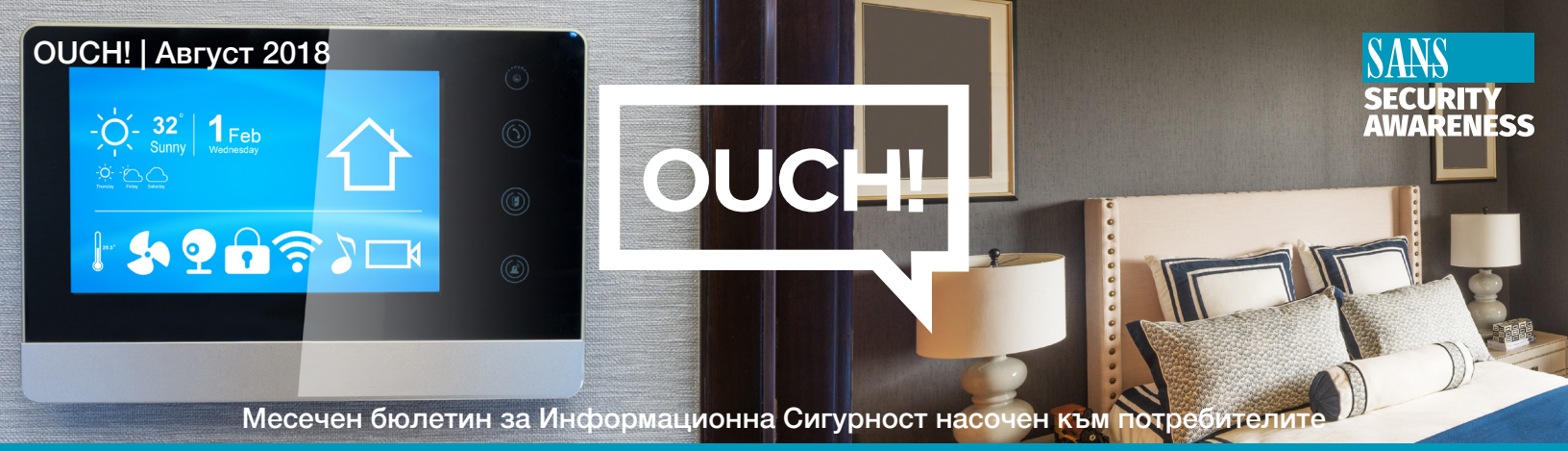
OUCH! | Август 2018



SANS SECURITY AWARENESS

OUCH!

Месечен бюлетин за Информационна Сигурност насочен към потребителите

Умни домашни устройства

Какво са умните домашни устройства?

Доскоро много малко от устройствата ви у дома можеха да се свържат с Интернет, като лаптоп, смартфон, или игрова конзола. В наши дни обаче, все повече устройства се свързват с Интернет, от електрически крушки и говорители до телевизори, ключалки и дори автомобилите. Скоро почти всяко устройство в дома ви би могло да е свързано с Интернет. Тези свързани устройства често биват наричани Интернет на Нещата (Internet of Things - IoT) или умни домашни устройства. Освен удобствата, които тези свързани устройства предлагат, с тях идват и някой уникални опасности.

Какъв е проблемът?

Колкото повече устройства са свързани с домашната ви мрежа, толкова повече неща могат да се объркат. Хакери могат да програмират тези устройства да атакуват други, търговците могат да събират значително количество информация за дейностите ви, или устройствата могат да се заразят и да изгубите достъпа до тях. Много от компаниите произвеждащи тези устройства нямат никакъв опит с кибер сигурността и за тях сигурността е разход. В резултат много от устройствата налични на пазара имат предвидена малко или никаква сигурност.Например, някой устройства имат фабрични пароли, която са добре известни или няма начин да бъдат сменени.

Как да се защитя

Какво може да се направи? Ние определено искаме да се възползвате от свързаните устройства, сигурно и безопасно. Тези устройства предоставят прекрасни възможности и правят живота по-лесен. Освен това, с разрастването на технологиите е възможно да нямате друг избор освен умните устройства. Ето няколко ключови стъпки, които да предприемете, за да се защитите:

Свържете само нужното: Най-простият начин да подсигурите устройство е да не го свързвате с Интернет. Ако едно устройство не ви е нужно онлайн, не го свързвайте с безжичната си мрежа. Наистина ли имате нужда от това тостерът да ви праща съобщения на телефона?

Знайте какво е свързано: Какви устройства имате свързани към домашната си мрежа? Не сте сигурни или не помните? Изключете безжичната мрежа и вижте какво ще спре да работи. Може да не намерите всичко, но ще се изненадате за колко устройства сте забравили.

Обновявайте: Точно както компютрите и мобилните устройства, изключително важно е да поддържате обновени абсолютно всичките си устройства. Ако устройството има възможност за автоматично обновяване – включете я.

Пароли: Сменете паролите на устройствата си с уникални, сложни фрази известни само на вас. Най-вероятно ще ви се наложи да ги въвеждате само веднъж. Не можете да помните пароли? Не се тревожете, и ние не можем. Съветваме ви да ползвате софтуер за управление на пароли, където да ги съхранявате.

Поверителност: Ако устройствата ви имат настройки за поверителност, намалете до минимум информацията която събират и споделят. Най-добре е напълно да спрете всяка функционалност за споделяне.

Търговец: Купувайте устройства на компания която познавате и на която можете да се доверите. Търсете продукти поддържащи сигурност, като например поддръжка на автоматични обновявания, възможност да се смени фабричната парола и опции за поверителност.

Винаги слушащи: Ако едно устройство поддържа гласови команди, то постоянно слуша. Например, Алекса и Google Home биха могли да запишат поверителни разговори. Имайте това предвид, когато избирате мястото на такова устройство в дома си, и прегледайте опциите за поверителност.

Мрежа за гости: Обмислете дали да не включите умните си устройства към отделна безжична мрежа вместо към основната такава, където са всичките ви компютри и мобилни устройства. Така ако някое от умните ви устройства бъде инфектирано, компютрите и мобилните ви устройства ще са в отделени безопасно в главната мрежа.

Няма причина да се страхуваме от новите технологии, но трябва да сме запознати с рисковете идващи с тях. Дадените тук прости стъпки ще помогнат за един по сигурен дом в умни устройства.

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

Гост-редактор

Робърт М. Лий *(@RobertMLee) е SANS сертифициран инструктор и автор на FOR578 - Cyber Threat Intelligence и ICS515 - ICS Active Defense and Incident Response. Робърт е също така изпълнителен директор и основател на фирмата Dragos, специализираща в индустриалната киберсигурност.*

Ресурси

Фрази-пароли:	https://www.sans.org/u/GEB
Управление на пароли:	https://www.sans.org/u/GEG
Защита на домашна мрежа:	https://www.sans.org/u/GEL

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