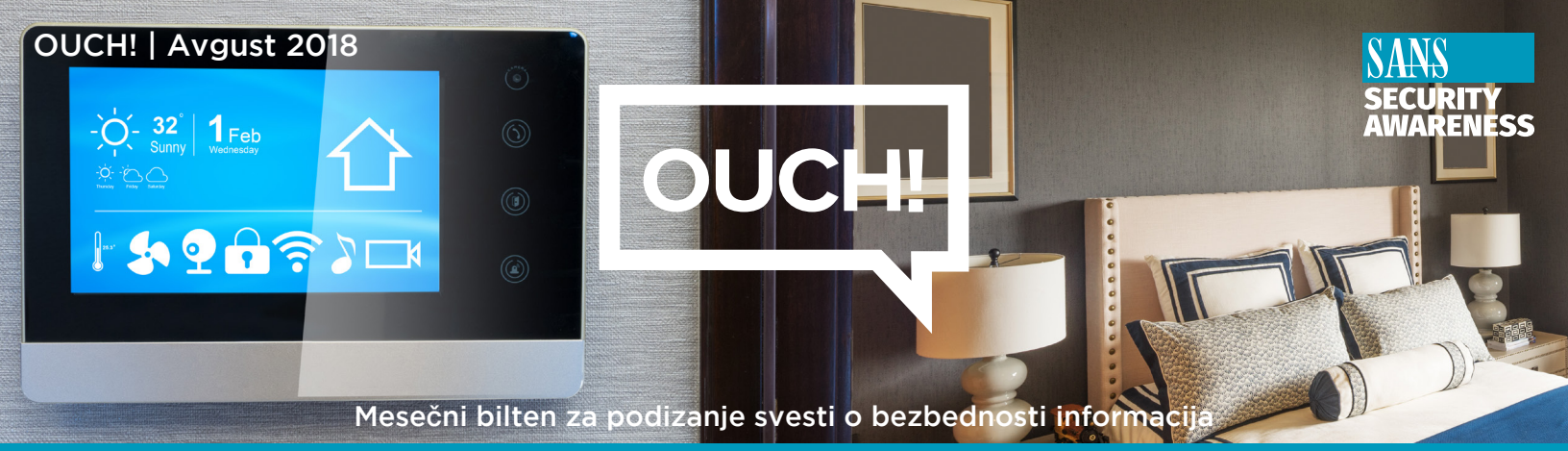
OUCH! | Avgust 2018



SANS SECURITY AWARENESS

OUCH!

Mesečni bilten za podizanje svesti o bezbednosti informacija

Pametni kućni uređaji

Šta su pametni kućni uređaji?

Do skora je bilo uobičajeno da su samo pojedini uređaji koje imate kod kuće (laptop, pametni telefon ili konzola za igru) mogli da se povežu na internet. Međutim, danas se sve više i više vaših uređaja, počev od sijalica i zvučnika na televizoru do brave na ulaznim vratima pa čak i automobila, povezuje na internet. Uskoro će skoro svaki uređaj u vašoj kući imati mogućnost povezivanja na internet. Ovi povezani uređaji često se nazivaju Internet stvari (eng. Internet of Things, IoT) ili pametni kućni uređaji. Iako ovi povezani uređaji unose velike pogodnosti u svakodnevni život, oni donose i sebi svojstvene opasnosti.

U čemu je problem?

Što je više uređaja koji su povezani na vašu kućnu mrežu, to su veće šanse da nešto krene po zlu. Hakeri mogu programirati vaše uređaje da napadaju druge, proizvođači mogu prikupljati detaljne informacije o vašim aktivnostima ili se vaši uređaji mogu zaraziti i zaključati vas. Mnoge kompanije koje proizvode ove uređaje nemaju iskustva sa sajber bezbednošću i vide bezbednost kao dodatni trošak. Kao posledica toga, brojni uređaji koje kupujete imaju malo ili nimalo ugrađenih bezbednosnih komponenti. Na primer, neki uređaji imaju predefinisane (unapred postavljene) lozinke koje su dobro poznate i ne mogu se promeniti.

Kako da se zaštitite

Šta možete da učinite kako biste povezane uređaje koristili na bezbedan i siguran način? Ovi uređaji mogu da pruže izvanredne funkcije koje olakšavaju svakodnevni život. Pored toga, kako tehnologija brzo napreduje, možda jednostavno nećete imati izbora osim da koristite pametne uređaje. U nastavku navodimo ključne korake koje možete preduzeti da biste se zaštitili.

Povežite samo ono što je potrebno: Najjednostavniji način obezbeđivanja uređaja jeste da ga ne povežete sa internetom. Ako nije neophodno da vaš uređaj bude dostupan sa interneta, nemojte ga ni povezivati na vašu Wi-Fi mrežu. Da li je zaista neophodno da vam toster šalje obaveštenja na telefon?

Znajte šta ste povezali: Koji uređaji su vam povezani sa kućnom mrežom? Niste sigurni ili ne možete da se setite? Isključite vašu bežičnu mrežu i proverite šta više ne radi. Možda na ovaj način nećete otkriti sve uređaje, ali ćete se iznenaditi za koliko ste uređaja zaboravili da su uopšte povezani.

Ažurirajte uređaje: Važi isto što i za vaš računar i mobilne uređaje, od ključnog je značaja da ažurirate sve vaše uređaje. Ako uređaj poseduje mogućnost automatskog ažuriranja, uključite je.

Lozinke: Zamenite lozinke na vašim uređajima sa jedinstvenim i jakim pristupnim frazama koje samo vi znate. Nove lozinke ćete najverovatnije morati da unesete samo jednom. Ne možete da se setite svih vaših lozinki ili fraza za pristup? Ne brinite, ne možemo ni mi. Razmislite o korišćenju menadžera lozinki da biste ih čuvali na bezbedan način.

Postavke privatnosti: Ako vaš uređaj dozvoljava da konfigurišete opcije vezane za privatnost, iskoristite ih da ograničite količinu informacija koje uređaj prikuplja ili deli. Jedna od opcija je i da onemogućite bilo kakvo deljenje informacija.

Proizvođač: Kupujte uređaje od kompanije koju poznajete i kojoj verujete. Potražite proizvode koje imaju opcije vezane za bezbednost, kao što su mogućnost automatskog ažuriranja, izmena podrazumevane lozinke i promena postavki privatnosti.

Stalno slušanje: Ako uređaj može da prima vaše glasovne komande, on neprestano sluša. Zato budite svesni da vaši Aleksa i Google Home uređaji mogu snimati osetljive razgovore, uzmite to u obzir kada odlučujete gde ćete u vašem domu postaviti uređaje i obavezno preispitajte njihove postavke privatnosti.

Gost mreža: Razmislite o tome da svoje pametne kućne uređaje smestite u zasebnu „Gost“ Wi-Fi mrežu umesto na osnovnu Wi-Fi mrežu koju koristite za računare i mobilne uređaje. Na ovaj način, u slučaju da neki pametni uređaj bude zaražen malverom, računari ili mobilni uređaji na vašoj glavnoj mreži će ostati zaštićeni.

Nema razloga za strah od novih tehnologija, ali budite svesni rizika koji njihovo korišćenje nosi sa sobom. Primena ovih nekoliko jednostavnih saveta može vam pomoći da napravite daleko bezbedniji digitalni dom.

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Gost urednik

Robert M. Li *(@RobertMLee) je SANS-ov sertifikovani predavač i autor kurseva o sajber pretnjama i odgovoru na incidente, „FOR578 - Cyber Threat Intelligence“ i „ICS515 - ICS Active Defense and Incident Response“. Robert je, takođe, direktor i osnivač kompanije Dragos koja se bavi sajber bezbednošću u industrijskim sistemima.*

Dodatni materijal

Pristupne fraze:	https://www.sans.org/u/GEB
Menadžeri lozinki:	https://www.sans.org/u/GEG
Bezbednost vaše kućne mreže:	https://www.sans.org/u/GEL