Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

- **Bežična mreža**
- **Uređaji**

Bezbednost vaše kućne mreže

Uvod

Pre ne tako mnogo godina kućne mreže su bile relativno jednostavne, uglavnom su podrazumevale uređaj za bežični pristup i jedan ili dva računara koji su se koristili za pretragu, kupovinu na Internetu, ili igranje. Međutim vremenom su kućne mreže postale sve složenije. Danas je na takve mreže priključeno daleko više uređaja koji se koriste za daleko složenije i osetljivije poslove nego što su jednostavna pretraga Interneta ili gledanje Internet sadržaja. U ovom izdanju objasnićemo kako da za vas i vašu porodicu kreirate bezbednu kućnu mrežu.

Gost urednik

Cheryl Conley je vođa tima za edukaciju vezanu za bezbednosti informacija u kompaniji Lockheed Martin i jedan od pionira iz oblasti edukacije zaposlenih u vezi bezbednosti informacija. Možete je pratiti na **@conleychera**.

Bežična mreža

Skoro svaka kućna mreža se zasniva na bežičnoj mreži (Wi-Fi mreža), koja vam omogućava da bežično povežete sve svoje uređaje na Internet, od laptopova i tableta do konzola za igranje ili televizora. Većina kućnih bežičnih mreža je omogućena preko Internet rutera, uređaja koji vaš Internet provajder instalira kod vas kući da bi vam omogućio pristup Internetu. Međutim, u nekim slučajevima bežična mreža može biti omogućena preko posebnog uređaja, uređajem za bežični pristup (Wireless Access Point), koji je povezan na vaš Internet ruter. Bez obzira kako je bežični pristup omogućen, uvek funkcioniše na isti način, tako što emituje bežične signale. Svi uređaji u vašoj kući se povezuju na bežičnu mrežu preko tih signala i onda pristupaju Internetu ili svim ostalim uređajima u vašoj kućnoj mreži. Na osnovu toga lako je zaključiti da je zaštita i bezbednost kućne bežične mreže ključni faktor u zaštiti vaše kućne mreže. Usled toga vam preporučujemo sledeće mere zaštite:

- Promenite fabričku (podrazumevanu) lozinku za administraciju rutera ili uređaja za bežični pristup, u zavisnosti koji uređaj omogućuje bežičnu mrežu. Nalog za administraciju omogućava konfiguraciju i podešavanja bežične mreže i stoga je od presudne važnosti za bezbednost kako vaše mreže, tako i svih vaših podataka. Problem leži u činjenici

Bezbednost vaše kućne mreže

da se većina rutera i uređaja za bežični pristup isporučuje sa fabričkim nalogom za administraciju i odgovarajućom lozinkom koja je dobro poznata i skoro uvek već odavno objavljena na Internetu. Obzirom na to, budite sigurni da se promenili lozinku za administraciju i da je nova jedinstvena, dovoljno kompleksna i da je smo vi znate.

- Promenite fabričko (podrazumevano) ime vaše bežične mreže (SSID). To je ime koje će te videti kada vašim uređajem tražite lokalne bežične mreže. Nazovite svoju mrežu jedinstvenim imenom tako da je možete jednostavno identifikovati, ali budite sigurni da naziv ne sadrži lične informacije. Ne postoji neka posebna prednost ako svoju mrežu podesite da bude sakrivena (ili da „ne emituje“) pošto se lako može otkriti bilo kakvim alatom za skeniranje.

Da bi ste zaštitili svoju kućnu mrežu, neophodno je da obezbedite svoju bežičnu mrežu i da redovno ažurirate i osigurate lozinkom sve svoje uređaje.

- Osigurajte da samo osobe kojima verujete mogu da se povežu i koriste vašu mrežu, i da je veza enkriptovana. To će te uraditi tako što ćete uključiti „jaku bezbednost“. Trenutno je najbolja opcija korišćenje bezbednosnog mehanizma pod nazivom WPA2. Na taj način, da bi se neko povezao na mrežu potrebno je da zna lozinku, i kada se jednom poveže razmena podataka je enkriptovana. Budite sigurni da ne koristite stare, prevaziđene bezbednosne mehanizme kao što je WEP, ili da uopšte ne koristite nikakvu zaštitu, da je vaše mreža potpuno otvorena. Otvorena mreža dozvoljava svakom de se poveže bez bilo kakve autentifikacije.
- Budite sigurni da je lozinka koja se koristi za povezivanje na vašu mrežu dovoljno jaka i da je različita od lozinke koja se koristi za administraciju. Imajte na umu da je najverovatnije potrebno da samo jednom unesete lozinku na svaki svoj uređaj, pošto će je oni nakon toga zapamtiti.
- Mnoge bežične mreže imaju opciju „mreže za goste“. Takva opcija omogućava da se posetioci povežu i koriste internet bez mogućnosti da se povežu sa vašim uređajima. Ako se odlučite za ovu opciju, budite sigurni da koristite WPA2 kao i jedinstvenu lozinku za takvu mrežu.
- Isključite „WiFi Protected Setup“ ili druge mehanizme koji dozvoljavaju novim uređajima da se povežu bez znanja lozinke i opcija podešavanja.
- Ako imate problema da zapamtite sve svoje lozinke, preporučujemo vam korišćenje menadžera lozinki.

Bezbednost vaše kućne mreže

Ako niste sigurni da možete samostalno da primenite ove savete, proverite sa svojim Internet provajderom, proverite dokumentaciju svog rutera ili proverite na Internet stranicama proizvođača opreme.

Uređaji

Sledeće je da znate šta je sve povezano na vašu kućnu mrežu i da su svi ti uređaji bezbedni. Nekada je to bilo jednostavno pošto se radilo samo o nekoliko uređaja. Međutim danas u „uvek povezanom“ svetu skoro svaki uređaj se može povezati na kućnu mrežu, uključujući TV, konzole za igranje, monitore za bebe, zvučnike, termostate ili možda vaš automobil. Jednostavan način da saznate šta je sve povezano na vašu mrežu je da je skenirate jednostavnim mrežnim skenerom kao što je Fing. Takve aplikacije možete instalirati na svoj računar ili mobini uređaj, pomoć u njih skenirati svoju mrežu i pronaći sve uređaje koji su povezani. Kada identifikujete sve uređaje potrebno je da ih osigurate. Najbolji način je da to postignete je da osigurate redovno (automatsko) ažuriranje kako operativnog sistema tako i aplikacija. Za svaki vaš uređaj, ako je neophodno, koristite jaku, jedinstvenu lozinku. Na kraju, proverite na Internet stranici svog Internet provajdera da li možda oni ne obezbeđuju besplatne alate za zaštitu kućne mreže svojih korisnika.

Saznaj Više

Prijavi se na OUCH! mesečni bilten bezbednosnih saveta za korisnike računara, pristupi prethodnim OUCH! izdanjima i saznaj više o SANS rešenjima u vezi svesnosti bezbednosti informacija na našoj internet prezentaciji http://www.securingthehuman.org.

Dodatne informacije

Propusne fraze:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_se.pdf
Menadžeri lozinki:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_se.pdf
Bezbednost vašeg novog tableta:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_se.pdf
Mapiranje vaše kućne mreže:	http://l.rud.is/home-network-mapping

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Preveo: Nenad Varinac