Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

- **Kućna bežična mreža**
- **„OpenDNS“**
- **Uređaji**

Kako obezbediti kućnu mrežu

Uvod

Do pre nekoliko godina kućne mreže su bile relativno jednostavne, ne više od bežičnog pristupnog uređaja („wireless access point“) i jednog ili dva računara, uglavnom za pretraživanje interneta ili „on-line“ igranje. Međutim kućne mreže vremenom postaju sve složenije. Danas, ne samo da se povezuje više uređaja, nego se i upotrebljavaju za mnogo kompleksnije poslove. U ovom izdanju objasnićemo osnove kreiranja sigurnije kućne mreže.

Gost urednik

Gost urednik ovog OUCH! izdanja je Kevin Johnson, CEO u „Secure Ideas“, u čijem vlasništvu je „**MySecurityScanner.com**“, i viši instruktor pri SANS Institutu. Više informacija na **www.secureideas.com**.

Bežična mreža

Skoro svaka kućna mreža podrazumeva bežičnu mrežu (Wi-Fi mrežu). Pomoću nje je moguće da sve svoje uređaje bežično povežeš na Internet, od laptop računara, pametnog telefona i tableta do konzola za igranje i televizora. Da bi to bilo moguće, tvojoj bežičnoj mreži je potreban uređaj za bežični pristup. To je fizički uređaj koji je povezan sa Internet ruterom (često ugrađen u Internet ruter) koji emituje bežični signal pomoć u kojeg se uređaji povezuju. Kada se jednom na takav način uređaj poveže, može se povezati sa ostalim uređajima u okviru iste kućne mreže i sa Internetom. Obzirom da je uređaj za bežični pristup jedan od ključnih uređaja svake kućne mreže, preporučljivo je obezbediti ga na sledeći način:

- Kod većine uređaja za bežični pristup podrazumevani (default) administratorski „login“ i lozinka su opšte poznata stvar i lako ih je naći na Internetu. Usled toga ih je neophodno promeniti u nešto što je samo tebi poznato. Vodi računa da se radi o jedinstvenoj lozinci koju ne koristiš za bilo koji drugi svoj račun.

- Sledeća stvar koju je potrebno konfigurisati je ime bežične mreže (SSID). To je ime koje uređaji vide kada traže bežičnu mrežu. Nazovi svoju mrežu nekim jedinstvenim imenom tako da možeš lako da je identifikuješ, ali vodi računa da ne sadrži bilo kakve lične informacije. Takođe postoji

Kako obezbediti kućnu mrežu

mogućnost da se mreža konfiguriše kao skrivena („hidden“) ali u tome nema neke posebne prednosti, obzirom da većina alata za skeniranje bežičnih mreža i veštijih hakera mogu bez problema da ih identifikuju.

Da bi tvoja kućna mreža bila bezbedna, potrebno je da obezbediš bežičnu mrežu, koristiš „OpenDNS“ ili sličan servis, i da svi uređaji koje koristiš budu ažurirani.

- Vodi računa da samo osobe kojima veruješ i koje znaš mogu da se povežu i koriste tvoju mrežu, i da koristiš neki tip ekripcije, osim ako ne želiš da i tvoje komšije i druge nepoznate osobe mogu da koriste i nadgledaju tvoju mrežu. Rizik da se to desi možeš jednostavno da rešiš tako što ćeš koristiti „jaku“ enkripciju, trenutno je najbolja opcija WPA2. Aktiviranje ove opcije, prilikom svakog pokušaja povezivanja sa tvojom mrežom, biće potrebno da se unese odgovarajuća lozinka, i ako je odgovarajuća enkriptovana veze će biti uspostavljena. Vodi računa da ne koristiš zastarele metode kao što je WEP ili da uopšte ne koristiš enkripciju (otvorena mreža). Otvorena mreža omogućava povezivanje bez ikakve autentifikacije, tako da svako može da se poveže.

- Vodi računa da je lozinka koja se koristi za pristup „jaka“, teška da se pogodi i da je drugačija od one koju koristiš za administraciju. Imaj na umu da će lozinku verovatno morati da uneseš samo jednom za svaki od uređaja koji koristiš, pošto će je oni zapamtiti i nakon toga automatski koristiti kada je potrebno.

- Većina uređaja za bežični pristup podržavaju nešto što se zove Mreža za goste („Guest Network“). Takve mreža omogućava posetiocima da se povežu na mrežu i da pristupaju Internetu ali im ne dozvoljava da se povežu druge uređaje u kućnoj mreži. Ako aktiviraš Mrežu za goste, vodi računa da je WPA2 uključen i da se za nju koristi drugačija lozinka.

- Ako ne možeš da zapamtiš sve lozinke, najbolje je da koristiš „menadžer lozinke“.

Kako obezbediti kućnu mrežu

„OpenDNS“

Kada je bežična mreža konfigurisana, preporučljivo je konfigurisati „OpenDNS“ kao DNS server (ili sličan servis kao na primer „Norton ConnectSafe for Home“). DNS je servis pomoć u koga tvoj pretraživač zna kom serveru na Internetu treba da pristupi. Servisi kao što je „OpenDNS“ identifikuju poznate, inficirane vebsjatove i onemogućavaju uređaje da im pristupe. Pored toga, ovi servisi često dozvoljavaju da i sam filtriraš ili blokiraš problematične vebsajtove. Ono što je jako dobro kod ovih servisa je to što nije potrebno da se instalira dodatni softver, potrebno je samo da se konfiguriše uređaj za bežični pristup.

Uređaji

Veoma je bitno da znaš koji uređaji su povezani na tvoju mrežu, i da su ti uređaji pouzdani. Nekada je to bilo jednostavno pošto je samo nekoliko uređaja i bilo povezano. Danas skoro svaki uređaj može da bude povezan, uključujući i TV, konzolu za igranje, alarm za bebe ili kućni termometar. Jednom kada identifikuješ sve uređaje možda budeš iznenađen koliko ih je. Najbolji način da tvoji uređaji budu bezbedni je da koriste najnoviju verziju operativnog sistema. Zato je najbolje da ako je to moguće uključiš opciju automatskog ažuriranja. Ako to nije moguće proveri jednom mesečno da li je moguće ažurirati ih. Takođe, jednom mesečno poseti vebsajt Internet provajdera, pošto ponekad oni obezbede besplatne alate i servise za proveru sigurnosti.

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

OpenDNS:
http://www.opendns.org
Norton ConnectSafe:
http://dns.norton.com/dnsweb/dnsForHome.do
Network security scanner:
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
Password Managers:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

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