SANS SECURITY AWARENESS
Telekom Srbija
OUCH! | Januar 2018
Mesečni bilten za podizanje svesti o bezbednosti informacija

OUCH!

U OVOM BROJU...

Napravite digitalno bezbedan dom

Uvod

Pravljenje bezbednog digitalnog doma pre nekoliko godina bilo je jednostavno jer je većina kuća imala samo bežičnu mrežu i nekoliko računara. Danas je tehnologija postala mnogo složenija i integrisana u svaki deo naših života, od mobilnih uređaja i konzola za igru do kućnog termostata, pa čak i vašeg frižidera. U nastavku su opisana četiri jednostavna koraka kako da vaš dom učinite digitalno bezbednim.

Gost urednik

Met Bromili (Matt Bromiley) se bavi rešavanjem incidenata pomažući kompanijama svih veličina da se izbore sa ugrožavanjem bezbednosti svojih podataka. On je takođe SANS instruktor i drži kurs Napredna digitalna forenzika i rešavanje incidenata (FOR508, Advanced Digital Forensics and Incident Response). Pratite Meta na tviteru **@mbromileyDFIR**.

Vaša bežična mreža

Osnova gotovo svake kućne mreže je bežična (Wi-Fi) mreža. Ova mreža omogućuje svim vašim uređajima da se povežu na internet. Većinom kućnih bežičnih mreža se upravlja pomoću vašeg internet rutera ili bežične pristupne tačke (eng. wireless access point). Oba ova uređaja rade na isti način, tako što emituju bežične signale putem kojih se povezuju uređaji u vašoj kući. Ovo praktično znači da je zaštita vaše bežične mreže ključni deo u zaštiti vašeg doma. Zaštitite je primenom sledećih saveta:

- Promenite podrazumevanu administratorsku lozinku na vašem ruteru ili bežičnoj pristupnoj tački, u zavisnosti od toga koji od ovih uređaja kontroliše vašu bežičnu mrežu. Administratorski nalog vam omogućava da menjate podešavanja vaše bežične mreže.
- Osigurajte da samo osobe kojima verujete mogu da se povežu na vašu bežičnu mrežu tako što ćete postaviti jake mere zaštite. Trenutno najbolja opcija je da koristite bezbednosni mehanizam pod nazivom WPA2. Kada omogućite ovu opciju biće neophodna lozinka kako bi se drugi povezali na vašu kućnu mrežu, a dok su povezani njihove aktivnosti na mreži će biti šifrovane.
- Osigurajte da lozinka koja se koristi za povezivanje na vašu bežičnu mrežu bude kompleksna i da se razlikuje od administratorske lozinke. Takvu lozinku je samo jednom potrebno uneti na svaki vaš uređaj, budući da je oni čuvaju i pamte.
- Mnoge bežične mreže podržavaju kreiranje takozvane „Gost mreže“. Ova mreža omogućava posetiocima da se povežu na Internet, ali štiti vašu kućnu mrežu pošto se oni ne mogu povezati ni sa jednim drugim uređajem u

Napravite digitalno bezbedan dom

vašoj kućnoj mreži. Ako dodate mrežu za goste, obavezno i za nju uključite WPA2 i postavite jedinstvenu lozinku za povezivanje na ovu mrežu.

Niste sigurni kako da primenite ove savete? Pitajte vašeg internet provajdera ili potražite pomoć na njihovom veb sajtu, proverite dokumentaciju koju ste dobili uz vaš internet ruter ili bežičnu pristupnu tačku ili pogledajte njihove veb sajtove.

Sledite ova četiri jednostavna koraka za kreiranje bezbednog digitalnog doma: obezbedite svoju bežičnu mrežu, omogućite automatsko ažuriranje, koristite jedinstvene lozinke i izrađujte bekap.

Vaši uređaji

Sledeći korak je da znate koji su sve uređaji povezani na vašu kućnu bežičnu mrežu i da se postarate da su svi ti uređaji zaštićeni. Ovo je bilo jednostavno kada ste imali samo jedan ili dva računara. Međutim, danas se gotovo sve može povezati sa vašom kućnom mrežom, uključujući vaše pametne telefone, televizore, konzole za igrice, bebi alarme, zvučnike ili možda čak i vaš automobil. Kada ste identifikovali sve uređaje na vašoj kućnoj mreži, osigurajte da je svaki od njih zaštićen. Najbolji način da ovo sprovedete je da osigurate da automatsko ažuriranje na njima bude uključeno kad god je to moguće. Sajber napadači stalno pronalaze nove ranjivosti na različitim uređajima i operativnim sistemima. Omogućavanjem automatskog ažuriranja, vaš računar i uređaji će uvek koristiti najnoviji softver, što bilo koji pokušaj njihovog hakovanja čini mnogo težim.

Lozinke

Sledeći korak je da koristite jaku, jedinstvenu lozinku za svaki vaš uređaj i nalog na internetu. Ključne reči za lozinku su: jaka i jedinstvena. Umorni ste od kompleksnih lozinki koje se teško pamte i komplikovano unose? Niste jedini. Koristite frazu za pristup umesto lozinke. Ovo je vrsta lozinke koja koristi niz reči koje je lako zapamtiti, kao što su “Gde je moja kafa?” Ili “ Snežana i sedam patuljaka”. Što je vaša fraza duža, jača je. Jedinstvena lozinka podrazumeva korišćenje različite lozinke za svaki uređaj i nalog na internetu. Na ovaj način, ukoliko je jedna lozinka kompromitovana, ostali vaši nalozi i uređaji će i dalje biti bezbedni. Ne možete da zapamtite sve te jake, jedinstvene lozinke? Ne brinite, malo ko to i može. Zbog toga se preporučuje da koristite menadžer lozinke, posebnu aplikaciju koja za vas na bezbedan način čuva sve vaše lozinke u šifrovanom, virtuelnom sefu.

Konačno, omogućite verifikaciju u dva koraka kad god je to moguće, naročito za vaše naloge na internetu. Verifikacija u dva koraka pruža bolju zaštitu. Ona koristi vašu lozinku, ali takođe dodaje drugi korak, kao što je šifra poslata na vaš pametni

telefon ili aplikacija na pametnom telefonu koja generiše šifru za vas. Verifikacija u dva koraka je verovatno najvažniji korak koji možete preduzeti da biste se zaštitili na mreži i koristi se mnogo lakše nego što mislite.

Rezervne kopije

Ponekad, bez obzira koliko ste pažljivi, možete da budete hakovani. U tom slučaju je često jedini način na koji možete povratiti vaše lične informacije taj da ih oporavite iz bekapa. Postarajte se da redovno izrađujete rezervne kopije svih važnih informacija i proveravajte da li možete da ih oporavite. Većina mobilnih uređaja podržava automatsku izradu rezervnih kopija u Cloud-u. Za većinu računara možda ćete morati da kupite neku vrstu softvera ili servisa za bekap, koji su relativno jeftini i jednostavni za korišćenje.

Saznajte više

Prijavite se na OUCH! mesečni bilten za podizanje svesti o bezbednosti informacija namenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rešenjima za unapređenje svesti o bezbednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

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.

Dodatne informacije

Pristupne fraze:	https://securingthehuman.sans.org/ouch/2017#april2017
Menadžeri lozinki:	https://securingthehuman.sans.org/ouch/2017#september2017
Dvofaktorska autentifikacija:	https://securingthehuman.sans.org/ouch/2017#december2017
Rezervne kopije:	https://securingthehuman.sans.org/ouch/2017#august2017

Redakcija: Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley
Preveli: Dragan Ristić i Gordana Živanović