SANS SECURING THE HUMAN Telekom Srbija

OUCH! | Oktobar 2016

Mesečni bilten za podizanje svesti o bezbednosti informacija

OUCH!

U OVOM BROJU...

Četiri koraka da ostanete bezbedni

Uvod

Tehnologija poprima sve značajniju ulogu u našim životima, a pri tom i njena složenost raste. Budući da se tehnološke promene događaju veoma brzo, ostajanje u toku sa bezbednosnim savetima može biti zbunjujuće. Deluje kao da se stalno pojavljuju novi saveti o tome šta treba, a šta ne treba da se radi. Međutim, iako se detalji vremenom mogu menjati, postoje osnovna pravila koja uvek možete primenjivati kako biste se zaštitili. Bez obzira koju tehnologiju koristite i gde je koristite, preporučujemo da primenjujete sledeća četiri koraka. Ako želite da naučite više o navedenim koracima, pogledajte deo Dodatni materijal na kraju ovog biltena.

Gost urednik

Ryan Johnson se primarno bavi pripremom organizacija da odgovore na neizbežne napade i upade u sistem, a takođe je i predavač na kursu Advanced Network Forensics pri SANS institutu. Na Tviteru je aktivan kao **@ForensicRJ**.

1. **Vi sami**: Na prvom mestu, najvažnije je da znate da sama tehnologija nikada neće moći u potpunosti da vas zaštiti. Napadači su naučili da napad na vas same predstavlja najlakši način da se zaobiđe i najnaprednija bezbednosna tehnologija. Ako žele vašu lozinku, kreditnu karticu ili lične podatke, najlakše im je da vas prevare da im te podatke date sami. Na primer, mogu vas pozvati telefonom pretvarajući se da su tehnička podrška iz Microsoft-a i tvrditi da je vaš računar zaražen, a zapravo su samo sajber kriminalci koji žele da im date pristup vašem računaru. Ili će vam možda poslati email sa objašnjenjem da vaša pošiljka ne može biti isporučena i molbom da kliknete na link kako biste potvrdili vašu adresu za dostavu, a taj klik će vas zapravo odvesti na maliciozni sajt sa koga će se izvršiti napad na vaš računar. Tako počinju napadi kao što su Ransomware ili CEO Fraud. Konačno, najveća zaštita od napadača ste vi sami. Budite uvek sumnjičavi. Korišćenjem zdravog razuma bićete u stanju da uočite i sprečite većinu napada.

2. **Lozinke**: Sledeći korak vaše zaštite se odnosi na upotrebu jakih/kompleksnih lozinki, jedinstvenih za svaki vaš uređaj i korisnički nalog. Ovde je naglasak na rečima “jaka/kompleksna” i “jedinstvena”. Jaka lozinka je ona koju hakeri ili automatizovani programi ne mogu lako da pogode. Da li ste umorni od kompleksnih lozinki koje se teško pamte, a teško i unose? Pokušajte da umesto njih koristite fraze. Umesto jedne reči koristite niz reči koje je lako zapamtiti, kao na primer “Gde je moja kafa?”. Što je vaša fraza duža, ona je jača. Lozinka je jedinstvena

Četiri koraka da ostanete bezbedni

ako za svaki uređaj ili korisnički nalog koristite drugačiju lozinku. Na taj način će i u slučaju da neka vaša lozinka bude otkrivena (kompromitovana), svi vaši drugi nalozi i uređaji ostati i dalje bezbedni. Ne možete da zapamtite sve te jake, jedinstvene lozinke? Ne brinite, ne možemo ni mi. Zato vam preporučujemo da koristite menadžere lozinki, specijalizovane aplikacije za pametne telefone ili računare koje omogućuju bezbedno čuvanje svih vaših lozinki u kriptovanoj formi.

Primenjujući ova četiri koraka dok koristite najnovije tehnologije doprinećete mnogo sopstvenoj zaštiti.

Konačno, jedan od najvažnijih koraka koji možete preduzeti da zaštitite nalog je da omogućite dvofaktorsku autentifikaciju. Lozinke same po sebi više nisu dovoljne da zaštite naloge, svima nam je potrebno nešto jače. Dvofaktorska autentifikacija je bolje rešenje. Ona koristi vašu lozinku, ali dodaje još jedan korak provere, bilo da je to nešto što vi jeste (biometrija), bilo da je nešto što imate (kao što je kod poslat na vaš telefon ili aplikacija na vašem telefonu koja generiše kod za vas). Omogućite ovu opciju na svakom nalogu za koji ova mogućnost postoji, uključujući i lozinku za pristup menadžeru lozinki. Dvofaktorska autentifikacija je verovatno jedini, najvažniji korak koji možete preduzeti da se zaštitite i to je mnogo lakše uraditi nego što mislite da jeste.

3. **Ažuriranje**: Postarajte se da vaši računari, mobilni uređaji, aplikacije i sve ostalo povezano na Internet koristi poslednju verziju softvera. Sajber kriminalci su u stalnoj potrazi za ranjivostima na softveru koji koriste vaši uređaji. Kada otkriju ranjivosti, oni koriste specijalne programe da ih iskoriste i hakuju uređaje koje koristite. A u međuvremenu, kompanije koje su napravile taj softver rade na ispravci ranjivosti koju objavljuju kao ažuriranje (update). Obezbedite li da vaši računari i mobilni uređaju preuzimaju i instaliraju ova ažuriranja, umnogome ćete otežati da vas neko hakuje. Da biste to postigli, jednostavno omogućite automatsko ažuriranje kad god je to moguće. Ovo pravilo važi za skoro sva tehnološka rešenja povezana na mrežu, uključujući televizore povezane na Internet, bebi monitore, kućne rutere, konzole za igrice, a jednog dana možda i vaš automobil. Ako su vaši operativni sistemi ili uređaji stari i više nisu podržani bezbednosnim ažuriranjima (ažuriranja se više ne objavljuju), predlažemo da ih zamenite novim koji će moći da se ažuriraju.

Četiri koraka da ostanete bezbedni

4. **Rezervne kopije i oporavak**: Ponekad se, ma koliko da ste pažljivi, može desiti da budete hakovani. Ako se to desi, potpuno brisanje i instalacija uređaja „od nule“ je često jedini način da budete sigurni da je vaš računar ili mobilni uređaj očišćen od malicioznog koda. U nekim slučajevima se dešava da vas napadač sprečava da pristupite vašim ličnim dokumentima, fotografijama i drugim informacijama na hakovanom sistemu. Često je povratak informacija iz rezervne kopije (bekapa) jedini način da im se ponovo pristupi. Postarajte se da dovoljno često kreirate bekap važnih informacija i da proveravate da je povratak informacija iz kreiranog bekapa moguć. Većina operativnih sistema i mobilnih uređaja omogućava automatsko kreiranje rezervnih kopija. Preporučujemo vam i da svoje rezervne kopije čuvate u Cloud-u ili fizički odvojene sa mreže kako biste ih dodatno zaštitili od sajber napada.

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

Sajber pecanje:	https://securingthehuman.sans.org/ouch/2015#december2015
Menadžeri lozinki:	https://securingthehuman.sans.org/ouch/2015#october2015
Verifikacija iz dva koraka:	https://securingthehuman.sans.org/ouch/2015#september2015
Propusne fraze:	https://securingthehuman.sans.org/ouch/2015#april2015
Rezervne kopije i oporavak:	https://securingthehuman.sans.org/ouch/2015#august2015

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis Cheryl Conley
Preveli: Dragan Ristić i Gordana Živanović