Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Četiri jednostavna koraka da ostanete bezbedni

Uvod

Korišćenje najnovijih tehnologija na bezbedan način često može izgledati naporno i zbunjujuće. Međutim, bez obzira koju tehnologiju koristite i kako je koristite, sledeća četiri jednostavna koraka će vam pomoći da ostanete bezbedni.

1. Vi sami: Na prvom mestu, najvažnije je da znate da tehnologija sama po sebi nikada neće moći u potpunosti da vas zaštiti, i da ste vi sami vaša najbolja zaštita. Napadači su naučili da će ciljanjem vas samih, umesto vašeg računara ili drugih uređaja, najlakše doći do onoga što žele. Ako žele vašu lozinku, podatke o platnoj kartici ili kontrolu nad vašim računarom, najlakše im je da vas prevare da im to date, što često čine kreirajući lažni osećaj hitnosti. Na primer, mogu vas pozvati telefonom pretvarajući se da su tehnička podrška iz Majkrosofta 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 mejl sa upozorenjem da vaša pošiljka ne može biti isporučena i pokušati da vas nateraju 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. Najveća zaštita od napadača ste vi sami. Korišćenjem zdravog razuma bićete u stanju da uočite i sprečite većinu napada.

2. Fraze kao lozinke: Današnje procesorske brzine dovele su do toga da uobičajena lozinka dužine 8 karaktera postane zastarela i ranjiva. Kada vam neki sajt zatraži da kreirate lozinku, upotrebite jaku i jedinstvenu frazu. Fraza je vrsta lozinke koju čini niz reči koje je lako zapamtiti, kao na primer „Ne treba se bojati Treba živeti“. Što je vaša fraza duža, ona je jača. Lozinka je jedinstvena ako za svaki uređaj ili korisnički nalog koristite drugačiju lozinku. Na ovaj način će i u slučaju da neka vaša lozinka bude otkrivena (kompromitovana), svi vaši drugi nalozi i uređaji i dalje ostati bezbedni. Ne možete da zapamtite sve te jake, jedinstvene lozinke? Koristite menadžere lozinki, specijalizovane aplikacije koje omogućavaju bezbedno čuvanje svih vaših lozinki u kriptovanoj formi, a nude i druge korisne funkcije.

Konačno, omogućite dvofaktorsku autentifikaciju (poznatu i pod nazivom verifikacija u dva koraka ili multifaktorska autentifikacija). Ona koristi vašu lozinku, ali dodaje još jedan korak provere, bilo da je to kod

poslat na vaš telefon ili aplikacija na vašem telefonu koja generiše kod za vas. Dvofaktorska autentifikacija je verovatno najvažniji korak koji možete preduzeti da zaštitite vaše naloge na internetu i to je mnogo lakše uraditi nego što izgleda.

3. Ažuriranje: Postarajte se da svi vaši računari, mobilni uređaji, programi i aplikacije koriste najnoviju verziju softvera. Sajber kriminalci su u stalnoj potrazi za ranjivostima softvera koji koriste vaši uređaji. Kada otkriju ranjivosti, oni koriste posebne programe da ih iskoriste i hakuju uređaje koje koristite. U međuvremenu, kompanije koje su napravile softver za te uređaje vredno rade na ispravci ranjivosti koju objavljuju kao ažuriranje softvera (eng. update). Obezbedite li da vaši računari i mobilni uređaju odmah 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 sve uređaje povezane na mrežu, uključujući televizore povezane na internet, bebi monitore, kamere za video nadzor, kućne rutere, konzole za igrice, a uskoro možda i vaš automobil.

4. Rezervne kopije i oporavak: Ponekad se, ma koliko da ste pažljivi, može desiti da budete hakovani. U tom slučaju oporavak iz bekapa često je jedini način da vratite sve vaše lične informacije. Postarajte se da dovoljno često kreirate bekap važnih informacija i da proveravate da je povratak vaših informacija iz bekapa moguć. Većina operativnih sistema i mobilnih uređaja omogućava automatsko kreiranje rezervnih kopija, bilo na eksterne diskove ili na klaud.

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

***Stiv Anson**, sertifikovani instruktor SANS instituta, daje smernice za poboljšanje stanja bezbednosti timovima koji se bave IT zaštitom i vladama širom sveta. Stiv je autor knjige „Applied Incident Response" koja će uskoro biti izdata, kao i sajta www.AppliedIncidentResponse.com na kome objavljuje besplatne resurse u vezi sa praktičnom primenom IT bezbednosti i zaštite.*

Dodatni materijal

Socijalni inženjering:	https://www.sans.org/u/W3G
Personalizovane prevare:	https://www.sans.org/u/W3Q
Napravite lozinku na jednostavan način:	https://www.sans.org/u/W3V
Imate li bekap:	https://www.sans.org/u/W40