Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

Pet ključnih pravila za vašu bezbednost

Uvod

Kako tehnologija ima sve veću ulogu u vašem životu, takođe se povećava i njena kompleksnost. Uzimajući u obzir brze tehnološke promene, aktuelnost bezbednosnih saveta se može dovesti u pitanje. Čini se, kao da se konstantno uvode nove smernice - šta činiti, a šta ne. Međutim i pored toga što se detalji tokom vremena menjaju, osnovne stvari koje možete da uradite da bi se zaštitili ostaju iste. Bez obzira koje tehnologije koristite, preporučujemo sledećih pet ključnih pravila

Gost urednik

Lenny Zeltser je odgovoran za zaštitu IT operacija klijenata u NCR Corp i predaje zaštitu od štetnog softvera pri SANS Institutu. Lenny je aktivan na Twitter-u kao **@lennyzeltser** i piše za bezbednosni blog **blog.zeltser.com**.

Pet ključnih pravila

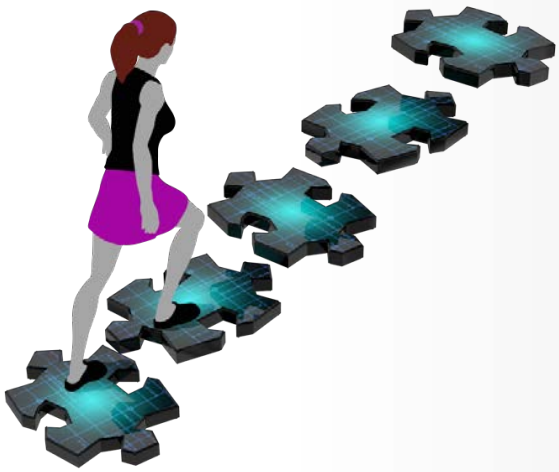
Dole navedena pravila su samo površan pregled, za detaljnija objašnjenja svakog pravila, pročitajte zasebne biltene prikazane u odeljku Dodatne informacije na kraju ovog biltena.

1. **Ti**: Prvo i pre svega, imajte na umu da tehnologija samo po sebi ne može da vas zaštiti. Sajber kriminalci su do sada naučili da je najlakši način da zaobiđu bezbednosne tehnologije da direktno napadnu vas. Ako žele vašu lozinku ili kreditnu karticu najlakše za njih je da prevare vas da im tu informaciju sami otkrijete. Na primer, mogu vas pozvati predstavljajući se kao tehnička podrška Microsoft-a, sa tvrdnjom da je vaš računar inficiran virusom, i na taj način pokušati da od vas dobiju informacije koje će im omogućiti pristup vašem računaru. Ili će vam možda poslati el. poštu koja tvrdi da paketi koji ste naručili ne može biti isporučen i da je potrebno da kliknete na „link“ i potvrdite adresu, a u stvari žele da vas preusmere na malicioznu internet stranu koja će inficirati vaš računar. Na kraju krajeva, vi ste najbolja zaštita protiv sajber kriminalaca. Budite sumnjičavi, koristeći zdrav razum moguće je prepoznati i zaustaviti većinu sajber napada.

2. **Ažuriranje**: Uverite se da vaši računari, mobilni uređaji, aplikacije i sve ostalo rade sa najnovijim verzijama softvera. Sajber kriminalci neprestano tragaju za slabostima i propustima u tehnologijama koje se koriste. Kada pronađu propuste, onda upotrebe posebne programe da bi hakovali uređaje koji koristite, uključujući računare,

Pet ključnih pravila za vašu bezbednost

mrežne i mobilne uređaje. U međuvremenu, kompanije koje su napravile tehnologije koje koristite, naporno rade da bi ih održale aktuelnim. Kada su slabosti ili propusti poznati, oni kreiraju zakrpe ili popravke, koje zatim objavljuju. Redovnim ažuriranjem vaših uređaja, smanjujete broj poznatih slabosti i propusta i time u mnogome otežavate njihovo hakovanje. Da bi ste smanjili rizik, uključite automatsko ažuriranje kad god je to moguće. Ovo pravilo važi za sve tehnologije povezane na Internet, uključujući i najnoviju generaciju televizora, monitore za bebe, kućne rutere, konzole za igranje ili čak automobile. Ako operativni sistem vašeg mobilnog uređaja ili druge tehnologije koju koristite nije više podržan od strane proizvođača i niste u mogućnosti da ga više ažurirate, preporučujemo da nabavite novu verziju uređaja za koji je podrška obezbeđena.



Poštovanjem ovih pet pravila, učinićete mnogo za svoju ličnu bezbednost ne gubeći korak sa najnovijim tehnologijama.

3. **Lozinke**: Sledeće pravilo podrazumeva korišćenje jake, jedinstvene lozinke za svaki od vaših uređaja, „on-line“ računa ili aplikacija. Ključne stvari su jake i jedinstvene. Jaka lozinka podrazumeva onu koju nije lako pogoditi, kako od strane sajber kriminalca, tako i od strane automatskog programa. Umesto jedne reči, koristite duge propusne fraze od više reči uključujući i simbole i brojeve. Jedinstvene podrazumeva korišćenje posebne lozinke za svaki od uređaja ili „on-line“ računa. Takav pristup omogućava da ako je jedan od računa kompromitovan ostali računi i uređaji budu bezbedni. Ne možete da pamtite toliko jakih, jedinstvenih lozinki? Ne brinite ne može skoro niko? Zbog toga vam preporučujemo da koristite menadžere lozinki, specijalizovane aplikacije za računare ili telefone, koje na bezbedan način čuvaju sve lozinke u šifrovanom (enkriptovanom) formatu. Na kraju, ako neki od vaših „on-line“ računa koristi verifikaciju iz dva koraka, preporučujemo vam da je aktivirate pošto predstavlja jedan od najboljih načina za zaštitu autentifikacije.

4. **Encripcija (šifrovanje)**: Četvrto pravilo koje preporučujemo je enkripcija i ona obezbeđuje da samo vi ili neko kome vi verujete može da pristupi vašim informacijama. Podaci se mogu enkriptovati na dva načina, u mirovanju ili u kretanju. Enkripcija u mirovanju podrazumeva zaštitu dok su podaci uskladišteni kao fajlovi na vešem tvrdom disku ili USB stiku. Većina operativnih sistema omogućava automatsku enkripciju svih vaših podataka korišćenjem funkcija kao što je Potpuna Enkripcija Diska (Full Disk Encryption). Preporučujemo

Pet ključnih pravila za vašu bezbednost

da je aktivirate kad god je to moguće. Enkripcija u kretanju podrazumeva da su podaci enkriptovani kada se razmenjuju između uređaja, na primer elektronsko bankarstvo. Jednostavan način da proverite da li je ovakva enkripcija uključena dok koristite Internet je da se uverite da adresa internet strane koju posećujete počinje sa „https“ i pored sebe ima ikonu katanca.

5. **Rezervne kopije (bekap-i)**: Ponekad, bez obzira koliko se pažljivi, neki od vaših uređaja ili „on-line“ računa može biti kompromitovan. U tom slučaju, često je jedina opcija koja može da osigura da je računar ili mobilni uređaj bez štetnog softvera ili virusa, potpuno brisanje i ponovno instaliranje od početka. Sajber kriminalci vas čak mogu i onemogućiti da pristupite svojim fajlovima, fotografijama ili drugim informacijama uskladištenim na kompromitovanim uređajima. Vaša jedina opcija može da bude oporavak svih fajlova iz rezervnih kopija (bekap-a). Potrudite se da redovno pravite rezervne kopije svih vaših važnih podataka i uverite se da ih možete povratiti kada su vam potrebni. Većina operativnih sistema i mobilnih uređaja sada omogućava automatsko pravljenje rezervnih kopija.

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

Napadi „Pecanjem“ putem el. pošte:	http://www.securingthehuman.org/ouch/2013#february2013
Bezbednost tvog novog tableta:	http://www.securingthehuman.org/ouch/2013#december2013
Lozinke:	http://www.securingthehuman.org/ouch/2013#may2013
Menadžeri lozinke:	http://www.securingthehuman.org/ouch/2013#october2013
Verifikacija iz dva koraka:	http://www.securingthehuman.org/ouch/2013#august2013
Enkripcija (Šifrovanje):	http://www.securingthehuman.org/ouch/2014#august2014
Rezervne kopije:	http://www.securingthehuman.org/ouch/2013#september2013

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