SANS SECURITY AWARENESS

OUCH!

Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Prolećno čišćenje

Uvod

Većina nas veoma se raduje proleću! Priroda se budi, pejzaž menja, a mnogima se javlja želja za prolećnim čišćenjem. Potreba za uklanjanjem suvišnih stvari i raspremanjem u digitalnom svetu, za razliku od fizičkog, nije tako očigledna i teže se realizuje. U nastavku su navedeni saveti koji vam mogu pomoći da uspostavite nove digitalne navike i da dovedete u red i tu sferu svog života:

BEKAP: Dugoročno gledano, ovo je jedan od najvažnijih koraka i korak koji treba prvo da preduzmete pre nego što pređete na ostale. Ma koliko da ste bezbedni i zaštićeni, velika je verovatnoća da će vam u nekom trenutku biti potrebne rezervne kopije da povratite vaše važne podatke. U toj situaciji se možete naći iz brojnih razloga, od kojih su neki npr. kvar na hard disku, gubitak uređaja, ili zaraženost malverom poput ransomvera. Redovna izrada automatskog bekapa prema odgovarajućem planu osigurava da ćete, kada se javi potreba, moći da oporavite vaše najvažnije informacije.

BRISANJE: Sa vaših mobilnih uređaja i računara izbrišite sve programe ili aplikacije koje ne koristite. Pojedine aplikacije zahtevaju značajne resurse za smeštaj informacija, mogu uneti nove ranjivosti ili usporiti vaš uređaj. Što manje aplikacija imate, sistem i vaše informacije na njemu su bezbedniji. Mnogi uređaji prikazuju koliko vremena je prošlo otkad ste poslednji put koristili neku aplikaciju - ako je prošlo više od nekoliko meseci, ta aplikacija vam najverovatnije i ne treba!

AŽURIRANJE: Ažurirajte sve vaše uređaje i aplikacije i omogućite automatsko ažuriranje kad god je to moguće. Na ovaj način vaši uređaji i aplikacije ostaju ažurni, što ne samo da osigurava njihov brži rad, već i otežava njihovo hakovanje.

LOZINKE: Preispitajte svoje lozinke. Ako koristite iste lozinke za više naloga, promenite ih tako da svaki nalog ima jedinstvenu lozinku. Ne možete da se setite svih svojih jedinstvenih lozinki? Razmislite o korišćenju menadžera lozinki. Na kraju, omogućite dvofaktorsku autentifikaciju (2FA) kad god je to moguće, naročito za vaše naloge za elektronsku poštu i finansijske usluge.

FINANSIJSKI NALOZI: Proverite da li su vaši bankovni korisnički nalozi, računi za koje su vezane platne kartice i penzioni nalozi konfigurisani da vas obaveštavaju o svakoj transakciji, naročito za velike kupovine ili transfere novca. Što pre uočite prevarnu aktivnost, pre ćete je zaustaviti. Zavisno od toga u kojoj zemlji živite, zaštita vašeg izveštaja iz kreditnog biroa (credit freeze) može biti jedan od najefikasnijih načina zaštite vašeg identiteta.

PREGLEDAČ: Pregledajte sve dodatke (eng. add-ons, plugins) instalirane u vašem pregledaču (eng. browser). Pregledajte podešavanja dozvola i razmislite da li tim dodacima zaista treba pristup vašoj lokaciji, lozinkama ili spiskovima kontakata? Ako više ne koristite određene dodatke ili vas brinu njihova podešavanja u vezi sa vašom privatnošću, izbrišite ih.

DRUŠTVENE MREŽE: Proverite vaše prisustvo na internetu. Pregledajte svoja podešavanja privatnosti i izbrišite sve fotografije i video zapise kojima se više ne pristupa ili više nisu potrebni. Iskoristite pretraživač da proverite koje su sve informacije o vama dostupne na internetu. Ne zaboravite, sasvim je u redu da ograničite koliko informacija delite i sa kim ih delite.

RADNI STO: Očistite fioke vašeg stola, obrišite sve stare hard diskove i USB-ove, pa čak i uništite sve lepljive beleške koje sadrže previše informacija. Ako još uvek ne koristite šreder (uređaj za uništavanje papira), razmislite da ga nabavite.

ELEKTRONSKA POŠTA: Očistite vašu elektronsku poštu, obrišite ono što vam ne treba i organizujte ono na čemu radite. Posebno obratite pažnju na osetljive dokumente, poput onih sa vašim datumom rođenja ili drugim podacima o ličnosti, i uklonite ih iz vašeg prijemnog sandučeta (inboksa)!

Iako sve navedeno može delovati kao dosta zahtevan zadatak, budite uvereni da značajno doprinosi da vaši uređaji i informacije budu bezbedniji. Ako vam se čini da će vam za primenu svih saveta biti potrebno mnogo vremena, izaberite samo nekoliko stavki ili pokušajte da realizujete po jednu stavku dnevno ili nedeljno. Imajte u vidu da svaki mali korak u velikoj meri doprinosi vašoj zaštiti.

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

Kejti Nikls *(@LiketheCoins) je glavna analitičarka u kompaniji Red Canary i SANS instruktor za obuku FOR578: Cyber Threat Intelligence. Više od jedne decenije bavi se poslovima iz domena mrežne bezbednosti, reagovanja na incidente i obaveštavanja o bezbednosnim pretnjama.*

Dodatni materijal

Imate li bekap?:	http://www.sans.org/u/ZVr
Napravite lozinku na jednostavan način:	http://www.sans.org/u/ZVw
Potražite informacije o sebi na internetu:	http://www.sans.org/u/ZVB
Kako da se bezbedno rešite vašeg mobilnog uređaja:	http://www.sans.org/u/ZVG