SANS SECURING THE HUMAN Telekom Srbija

OUCH! | Decembar 2016

Mesečni bilten za podizanje svesti o bezbednosti informacija

OUCH!

U OVOM BROJU...

- **Vaše informacije**
- **Bezbedno brisanje vašeg uređaja (wiping)**
- **SIM / memorijske kartice**

Kako da se otarasite mobilnog uređaja na bezbedan način

Uvod

Mobilni uređaji (pametni telefoni, pametni satovi, tableti) nastavljaju da se razvijaju velikom brzinom i donose nove funkcionalnosti. Ovo za posledicu ima da ljudi često menjaju svoje mobilne uređaje, neretko jednom godišnje. Nažalost, česti su oni koji pri tome ne brinu mnogo o tome koliko njihovih ličnih podataka ostaje na uređajima koje su prestali da koriste. U ovom broju se bavimo tipovima ličnih informacija koje se mogu naći na vašem mobilnom uređaju i načinima da ih bezbedno obrišete pre nego što uređaj vratite, date nekom na korišćenje, poklonite ili odlučite da ga bacite. Ako vam je mobilni uređaj dao vaš poslodavac, ili se na njemu nalaze poslovni podaci, pre preduzimanja niže opisanih koraka obavezno se konsultujte sa vašim nadređenim i saznajte kakve su procedure za bekap podataka i rashodovanje uređaja u vašoj kompaniji.

Gost urednik

Heather Mahalik (**@HeatherMahalik**; **+HMahalik**) je glavna forenzičarka u ManTech CARD kompaniji. Ona je i glavna autorka SANS kursa Advanced Smartphone Forensics (FOR585) i instruktorka SANS kursa Windows Forensic Analysis (FOR408). Blogove objavljuje na **smarterforensics.com**.

Vaše informacije

Mobilni uređaji čuvaju mnogo više osetljivih podataka nego što ste vi toga svesni, često je to i nekoliko puta više nego što čuva vaš računar. Tipične sačuvane informacije su sledeće:

- Informacije o lokacijama na kojima živite i radite, kao i lokacije mesta koja često posećujete
- Kontakti, detalji o svim osobama iz vašeg imenika i aplikacija, uključujući članove porodice, prijatelje i kolege
- Istorija poziva koje ste inicirali, na koje ste odgovorili i koje ste propustili
- SMS poruke, govorne i multimedijalne poruke
- Čet sesije u okviru različitih aplikacija, igara i društvenih mreža
- Istorija o vašem kretanju na osnovu GPS koordinata ili podataka sa baznih stanica mobilne telefonije
- Istorija o stranama koje ste posetili na Internetu, pretragama koje ste vršili, kolačići (cookies) i keširane strane
- Lične fotografije, video i audio zapisi, elektronska pošta
- Sačuvane lozinke i pristup ličnim nalozima za elektronsko bankarstvo (online banking), elektronsku poštu ili druge servise
- Pristup fotografijama, fajlovima i informacijama koje čuvate u Cloud-u
- Informacije o vašem zdravstvenom stanju, uključujući vaše godine, puls, krvni pritisak, režim ishrane

Kako da se otarasite mobilnog uređaja na bezbedan način

Bezbedno brisanje vašeg uređaja (wiping)

Kao što sagledavate, na vašem mobilnom uređaju se najverovatnije nalazi ogromna količina osetljivih informacija. Bez obzira na način na koji ćete se rešiti svog mobilnog uređaja, bilo da ga poklanjate, menjate za novi, dajete drugom članu porodice, prodajete ili planirate da ga bacite, neophodno je da se prvo postarate da sve osetljive informacije na njemu budu obrisane. Možda toga niste svesni, ali obično brisanje podataka nije dovoljno jer se korišćenjem besplatnih alata koji se mogu naći na Internetu podaci lako mogu povratiti. Umesto toga potrebno je da bezbedno obrišete sve podatke na vašem uređaju, postupkom koji se popularno naziva wipe-ovanje. Ovim postupkom se zapravo vaše informacije prepisuju nizovima karaktera na način koji osigurava da se one ne mogu povratiti. Verovatno ćete pre nego što bezbedno obrišete vaš stari uređaj želeti da kreirate bekap kako biste lakše podesili vaš novi uređaj.

Kad prelazite na korišćenje novog mobilnog uređaja ne zaboravite da na starom uradite „factory reset“ i iz njega uklonite SIM i sve eventualne SD kartice.

Najlakši način da bezbedno obrišete vaš uređaj je da upotrebite njegovu funkcionalnost za povratak na fabrička podešavanja (factory reset). Ovim se vaš uređaj vraća na stanje u kojem je bio kada je kupljen. “Factory reset” predstavlja najbezbedniju i najjednostavniju metodu za uklanjanje podataka sa vaših mobilnih uređaja. Ova funkcionalnost se na različitim uređajima pokreće na različite načine, a koraci za pokretanje na najpopularnijim uređajima su:

- Apple iOS uređaji: Settings | General | Reset | Erase All Content and Settings
- Android uređaji: Settings | Privacy | Factory Data Reset

Nažalost, uklanjanje ličnih podataka sa Windows Phone uređaja nije tako jednostavno kao „factory reset“. Istraživanja metoda za bezbedno brisanje vaših ličnih podataka sa uređaja su u toku. Ako su vam potrebna dodatna objašnjenja o tome kako da bezbedno obrišete vaš uređaj, proverite korisničko uputstvo ili veb sajt proizvođača vašeg uređaja. Ne zaboravite, jednostavno brisanje vaših ličnih podataka nije dovoljno jer se tako obrisani podaci mogu povratiti na lak način.

SIM i memorijske kartice

Uz staranje o podacima koji se čuvaju na vašem uređaju, trebalo bi da razmotrite i šta ćete učiniti sa vašom SIM (Subscriber Identity Module) karticom. SIM kartica omogućava da mobilni uređaj uspostavi konekciju sa mrežom mobilne telefonije. Kada sprovodite „factory reset“ vašeg uređaja, SIM kartica zadržava informacije o vašem nalogu i vezana je za vas kao korisnika. Ako zadržavate broj telefona, možda će biti potrebno da sa vašim provajderom mobilne telefonije dogovorite

Kako da se otarasite mobilnog uređaja na bezbedan način

prenos SIM kartice na novi uređaj. Ako je potrebno da se izda nova SIM kartica drugačije veličine, sačuvajte i fizički uništite staru SIM karticu.

Na kraju, neki mobilni uređaji koriste posebne SD (Secure Digital) memorijske kartice za dodatni smeštaj podataka. Ove kartice često sadrže fotografije, aplikacije za pametne telefone i drugi osetljivi sadržaj. Ne zaboravite da pre odlaganja vašeg mobilnog uređaja uklonite sve eksterne memorijske kartice (kod nekih uređaja, SD kartice mogu biti sakrivene u odeljku u kom se nalazi baterija, verovatno ispod nje). Ove kartice se najčešće mogu koristiti i u novim mobilnim uređajima ili kao dodatni memorijski prostor na vašem računaru uz korišćenje odgovarajućeg USB adaptera. Ako dalje korišćenje SD kartice više nije moguće savetujemo da je, baš kao i vašu staru SIM karticu, fizički uništite.

Ako imate još nedoumica u vezi sa ovde navedenim koracima vaš mobilni uređaj možete odneti u prodavnicu u kojoj ste ga kupili i potražiti pomoć od obučenog tehničara. Na kraju, ako vam se čini da je vaš mobilni uređaj za otpad, razmislite još jednom da li ga nekome možete donirati.

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

Bezbednost vašeg novog tableta:	https://securingthehuman.sans.org/ouch/2016#january2016
Rezervne kopije i oporavak:	https://securingthehuman.sans.org/ouch/2015#august2015
Obuka Advanced Smartphone Forensics:	https://sans.org/for585
Arhive OUCH biltena:	https://securingthehuman.sans.org/ouch/archives

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