Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

- Uvod
- Pribavljanje aplikacija
- Prava pristupa
- Ažuriranje aplikacija

Bezbedno korišćenje aplikacija na mobilnim uređajima

Uvod

Mobilni uređaji kao što su tableti i pametni telefoni postali su jedna od primarnih tehnologija koje koristimo kako u privatne, tako i u poslovne svrhe. Ono što čini mobilne uređaje tako svestranim su svakako milioni aplikacija koje su nam na raspolaganju. Aplikacije nam omogućavaju da budemo produktivniji, trenutnu komunikaciju ili deljenje sa drugima, trening i edukaciju ili samo više zabave. Ipak, tolike prednosti sa sobom nose i određene rizike. Upoznajte se sa koracima koje možete preduzeti u cilju bezbednog korišćenja i održavanje vaših mobilnih aplikacija.

Gost urednik

Chris Crowley je nezavisni konsultant, sertifikovani SANS instruktor i autor kurseva. Aktivan je na Twitteru, **@CCrowMontance**, i na Google plus-u, **+ChrisCrowley**.

Pribavljanje aplikacija

Prvi korak svakako predstavlja preuzimanje aplikacija iz pouzdanih izvora. Imajte na umu da skoro svako može da napravi aplikaciju za mobilne uređaje, tako da je izuzetno važno gde ste je nabavili. Sajber kriminalci su usavršili svoje veštine pravljenja i distribuiranja inficiranih aplikacija koje izgledaju baš kao i legitimne. Ako instalirate neku od inficiranih aplikacija, moguće je da kriminalci preuzmu kontrolu nad vašim uređajem, a to može da uključi i čitanje vaše el. pošte, slušanje vaših razgovora i preuzimanje podataka o vašim kontaktima. Preuzimanjem aplikacija iz poznatog, pouzdanog izvora drastično smanjujete mogućnost da instalirate inficiranu aplikaciju. Ono čega možda niste svesni je da tip uređaja koji koristite određuje opcije koje imate na raspolaganju.

Kod Apple uređaja, kao što su iPad ili iPhone, aplikacije je moguće samo pribaviti iz uređene i održavane sredine, „Apple App Store“. Prednosti ovakvog pristupa je da sam Apple brine o bezbednosnoj proveri aplikacija i samih autora. Mada Apple ne može da identifikuje sve „loše momke“ i sve inficirane aplikacije, takva uređena sredina drastično redukuje rizik instalacije inficiranih aplikacija. Pored toga, ako Apple pronađe u svojoj „prodavnici“ aplikaciju za koju veruje da je maliciozna, brzo će je ukloniti. Windows Phone koristi sličan pristup upravljanja aplikacijama.

Android mobilni uređaji su drugačiji. Android obezbeđuje veću fleksibilnost tako što dozvoljava preuzimanje aplikacija sa bilo koje lokacije na Internetu. Veća fleksibilnost podrazumeva i veću odgovornost. Usled toga, prilikom preuzimanja i

Bezbedno korišćenje aplikacija na mobilnim uređajima

instaliranja aplikacija potrebno je biti veoma obazriv sami tim što niko ne garantuje da su aplikacije proverene. Google održava i upravlja prodavnicom mobilnih aplikacija sličnoj Apple-ovoj, nazvanoj „Google Play“. Aplikacije koje preuzimate sa „Google Play-a“ su prošle kroz proces osnovne bezbednosne provere. Usled toga, za Android uređaje preporučljivo je da aplikacije preuzimate samo sa „Google Play-a“. Izbegavajte da aplikacije preuzimate sa dugih Internet stranica, pošto svako, uključujući i sajber kriminalce, može lako da kreira i distribuira maliciozne aplikacije, i da vas na taj način navede da inficirate svoj mobilni uređaj. Kao dodatnu zaštitu, uzmite u obzir instalaciju anti-virus softvera.

Ključ bezbednog korišćenja aplikacija za mobilne uređaje leži u instalaciji aplikacija iz pouzdanih izvora, redovnom ažuriranju i proveri prava pristupa.

Da bi ste dodatno umanjili rizik, izbegavajte potpuno nove aplikacije, one koje je relativno malo ljudi preuzelo ili one koje imaju malo pozitivnih komentara. Što je duže aplikacija dostupna ili što više pozitivnih komentara ima, to je verovatnije da je aplikacija pouzdana. Osim toga, instalirajte samo aplikacije koje su vam potrebne ili koje koristite. Uvek postavite sebi pitanje, da li mi je ta aplikacija stvarno neophodna? Ne samo da svaka aplikacija sa sobom nosi potencijalne nove slabosti, nego i nove izazove u vezi privatnosti. Ako neku aplikaciju prestanete da koristite, uklonite je sa vašeg uređaja (uvek kasnije, ako vam bude potrebna, možete da je ponovo instalirate).

Konačno, možete doći u iskušenje da „jailbreak-ujete“ ili „root-ujete“ vaš mobilni uređaj. To je proces hakovanja uređaja, koji omogućava instalaciju aplikacija koje nisu odobrene ili menjanje postojećih, fabrički ugrađenih funkcionalnosti. Take postupke vam ne preporučujemo, pošto oni ne samo da zaobilaze i eliminišu ugrađene bezbednosne kontrole, nego i često mogu da ugroze garanciju ili servisnu podršku.

Prava pristupa

Kada jednom instalirate aplikaciju iz pouzdanog izvora, sledeće što treba da imate na umu je da bezbedno konfigurisana i da je privatnost osigurana. Instalacija i/ili konfiguracija aplikacije često zahteva da dozvolite određena prava pristupa. Uvek dobro razmislite pre nego što dozvolite pristup, da li su aplikaciji za posao koji obavlja stvarno potrebno prava pristupa koja zahteva? Na primer, neke aplikacije koristi servis geo-lokacije. Ako dozvolite aplikaciji da uvek zna vašu lokaciju, možda dozvoljavate autoru aplikacije da prati vaše kretanje, samim tim i mogućnost da tu informaciju proda nekom ko će

Bezbedno korišćenje aplikacija na mobilnim uređajima

je iskoristiti na neki način koji vi ne odobravate. Ako ne želite da dodelite prava pristupa koje aplikacija zahteva, nabavite ili kupite drugu aplikaciju koje zadovoljava vaše potrebe. Imajte na umu da je izbor ogroman. Kod Apple uređaja je dozvoljeno da se neka prava pristupa menjaju u Postavkama („Settings“) ili u toku rada palikacije, na primer pristup geo-lokaciskim informacijama. Kod Windows i Android uređaja je drugačije, princip je sve ili ništa. Ako ne dozvolite pristup svemu što je zatraženo, nemoguće je instalirati aplikaciju.

Ažuriranje aplikacija

Aplikacije za mobilne uređaje, kao i operativni sistem vašeg računara ili mobilnog uređaja, moraju biti ažurirane da bi bile aktuelne. Kriminalci konstantno tragaju i nalaze nove slabosti u aplikacijama. Na osnovu toga razvijaju napade koji za cilj imaju eksploataciju uočenih slabosti. Autori aplikacija takođe kreiraju i objavljuju ispravke za uočene sigurnosne propuste i time štite vaš uređaj. Što češće proveravate i instalirate ispravke, to bolje. Većina platformi dozvoljavaju da konfigurišete vaš sistem da automatski ažurira aplikacije. To je pristup koji preporučujemo. Ako to nije moguće, preporučujemo da na svake dve nedelje proverite da li postoje nova ažuriranja za vaše aplikacije. U svakom slučaju, kada se aplikacije ažuriraju, budite sigurni da ste proverili da li su prava pristupa izmenjena.

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

Društveni inženjering:	http://www.securingthehuman.org/ouch/2014#november2014
Odlaganje vašeg mobilnog uređaja:	http://www.securingthehuman.org/ouch/2014#june2014
Bezbednost vašeg novog tableta:	http://www.securingthehuman.org/ouch/2013#december2013
Opšti bezbednosni termini:	http://www.securingthehuman.org/resources/security-terms
SEC575: Bezbednost mobilnog uređaja - kurs:	http://www.sans.org/sec575

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