SANS Telekom Srbija

OUCH! | Mart, 2017

Mesečni bilten za podizanje svesti o bezbednosti informacija

OUCH!

U OVOM BROJU...

- Uvod
- Dobavljanje mobilnih aplikacija
- Dozvole
- Ažuriranje aplikacija

Bezbedno korišćenje mobilnih aplikacija

Uvod

Mobilni uređaji poput tableta, pametnih telefona i satova su postali jedna od osnovnih tehnologija koju koristimo kako u privatnom tako i u profesionalnom životu. Ono što mobilne uređaje čini tako univerzalnim su milioni aplikacija koje za njih imamo na raspolaganju. Ove aplikacije nam omogućuju da budemo produktivniji, brže komuniciramo i razmenjujemo informacije sa drugima, da učimo i obrazujemo se ili samo da se više zabavljamo. Međutim, sa sve većim mogućnostima najrazličitijih mobilnih aplikacija dolaze i rizici. U nastavku vam predstavljamo neke korake koje možete preduzeti kako biste vaše mobilne aplikacije koristili na bezbedan način.

Gost urednik

Joshua Wright je tehnički direktor u kompaniji Counter Hack i instruktor u SANS institutu. On je autor kurseva SEC575: Mobile Device Security and Ethical Hacking, i Hacking Exposed: Wireless. Džoša možete pronaći i na tviteru na nalogu **@joswr1ght**.

Dobavljanje mobilnih aplikacija

Prvi korak je da osigurate da mobilne aplikacije uvek preuzimate sa bezbednih i pouzdanih lokacija. Sajber kriminalci su ovladali veštinama pravljenja i distribuiranja zaraženih mobilnih aplikacija koje izgledaju kao da su legitimne. Ako instalirate neku od ovih zaraženih aplikacija, kriminalci u potpunosti mogu preuzeti kontrolu nad vašim mobilnim uređajem. Preuzimanjem aplikacija samo od dobro poznatih, pouzdanih izvora umanjujete šansu da ćete instalirati zaraženu aplikaciju. Ono čega možda niste svesni je da brend mobilnog uređaja koji koristite određuje vaše opcije za preuzimanje aplikacija.

Za Apple-ove uređaja kao što su iPad ili iPhone, mobilne aplikacije preuzimajte samo iz Apple ove zvanične prodavnice (Apple App Store). Prednost ovoga je što Apple radi bezbednosnu proveru svih mobilnih aplikacija pre nego što ih učini dostupnim za preuzimanje. Iako Apple ne može da otkrije sve zaražene mobilne aplikacije, ovakvo kontrolisano okruženje pomaže da se značajno smanji rizik od instalacije zaražene aplikacije. Pored toga, ako Apple u svojoj prodavnici pronađe aplikaciju za koju veruje da je zaražena brzo će je ukloniti. Windows Phone koristi sličan pristup za upravljanje aplikacijama.

Mobilni uređaji sa Android operativnim sistemom su drugačiji. Android vam pruža veću fleksibilnost tako što ste u mogućnosti da preuzmete mobilnu aplikaciju sa bilo kog mesta na internetu. Ipak, sa ovom fleksibilnošću dolazi i više odgovornosti. Morate biti pažljiviji kada preuzimate i instalirate mobilne aplikacije pošto nisu sve proverene.

Bezbedno korišćenje mobilnih aplikacija

Gugl, takođe, ima svoju prodavnicu mobilnih aplikacija sličnu Apple-ovoj, koja se zove Google Play. Mobilne aplikacije koje preuzimate sa Google Play-a su prošle neke osnovne bezbednosne provere. Zato je preporuka da mobilne aplikacije za Android uređaje preuzimate samo sa Google Play-a. Izbegavajte preuzimanje Android mobilnih aplikacija sa drugih sajtova, pošto bilo ko, uključujući i sajber kriminalce, može lako da kreira i distribuira maliciozne mobilne aplikacije i navede vas da zarazite svoj mobilni uređaj. Kao dodatnu zaštitu, ukoliko je to moguće instalirajte antivirus na vaš mobilni uređaj.

Ključ bezbednog korišćenja mobilnih aplikacija je u instalaciji aplikacija samo iz proverenih izvora, u instalaciji ažuriranja čim se ona pojave i odobravanju samo neophodnih privilegija aplikacijama.

Bez obzira koji mobilni uređaj koristite, dodatni korak koji možete preduzeti je izbegavanje potpuno novih aplikacija, zatim aplikacija koje je preuzeo mali broj korisnika ili imaju vrlo mali broj pozitivnih komentara. Što duže je aplikacija dostupna, što je više ljudi koji su je koristili i što je veći broj pozitivnih komentara o njoj to je veća verovatnoća da se aplikacija može smatrati bezbednom. Pored toga, instalirajte samo aplikacije koje su vam neophodne i koje koristite. Zapitajte se, da li vam je stvarno potrebna aplikacija koju instalirate? Ne samo da svaka aplikacija potencijalno donosi nove ranjivosti, već ona nosi i nove probleme kada je privatnost u pitanju. Ako prestanete da koristite aplikaciju uklonite je sa svog mobilnog uređaja (uvek je možete dodati kasnije ako vam bude potrebna). Na kraju, nikad ne radite tzv. „jailbreak“ ili „root“ vašeg mobilnog uređaja. Ovim postupcima se uređaj hakuje i instaliraju se neodobrene aplikacije ili menjaju postojeće ugrađene funkcionalnosti. Na ovaj način, ne samo da se zaobilaze i premošćavaju mnoge bezbednosne kontrole ugrađene u vaš mobilni uređaj, već se često poništava garancija i ugovor o podršci.

Dozvole

Kada ste instalirali mobilnu aplikaciju iz pouzdanog izvora, proverite da li je ona bezbedno konfigurisana i da štiti vašu privatnost. Uvek razmislite pre nego što mobilnoj aplikaciji dozvolite pristup: da li želite da aplikaciji odobrite prava koja zahteva i da li su joj zaista neophodna? Na primer, neke aplikacije koriste geo-lokacijske servise. Ako aplikaciji dozvolite da uvek zna vašu lokaciju, na taj način njenom kreatoru možete omogućiti da prati vaše kretanje, a čak i da te informacije prodaje drugima. Ako ne želite da date dozvolu, odbijte zahtev koji vam postavlja aplikacija ili pronađite drugu aplikaciju koja zadovoljava vaše potrebe. Zapamtite, imate puno drugih aplikacija na raspolaganju.

Bezbedno korišćenje mobilnih aplikacija

Ažuriranje aplikacija

Mobilne aplikacije, kao i vaš računar i operativni sistem mobilnog uređaja, moraju da se ažuriraju da bi bile bezbedne. Kriminalci stalno traže i pronalaze slabosti u aplikacijama. Oni zatim razvijaju napade kako bi eksploatisali ove ranjivosti. Programeri koji su kreirali vašu aplikaciju takođe kreiraju i objavljuju ažuriranja (updates) kako bi ispravili ove ranjivosti i zaštitili vaše uređaje. Što češće proveravate i instalirate ažuriranja, to bolje. Većina uređaja vam omogućava da konfigurišete sistem tako da se mobilne aplikacije ažuriraju automatski. Ovo podešavanje se preporučuje. Ukoliko ovo nije moguće, preporučuje se da bar jednom u dve nedelje proveravate da li je postoje ažuriranja za vaše mobilne aplikacije. Na kraju, kada se vaše aplikacije ažuriraju uvek proverite svaku novu dozvolu koju aplikacije zahtevaju.

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

Socijalni inženjering:	https://securingthehuman.sans.org/ouch/2017#january2017
Kako da se otarasite mobilnog uređaja na bezbedan način:	https://securingthehuman.sans.org/ouch/2016#december2016
Bezbednost vašeg novog tableta:	https://securingthehuman.sans.org/ouch/2016#january2016
Arhive OUCH biltena:	https://securingthehuman.sans.org/ouch/archives
Kurs: Mobile Device Security:	https://sans.org/sec575

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