OUCH! | Ianuarie 2015

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- Generalități
- Obținerea aplicațiilor
- Drepturi de acces
- Actualizarea aplicațiilor

Utilizarea în siguranță a aplicațiilor de pe dispozitivele mobile

Generalități

Dispozitivele mobile, cum ar fi tabletele sau telefoanele inteligente au devenit una dintre principalele tehnologii pe care le folosim de o potrivă pentru nevoi personale și în activitatea profesională. Ce face dispozitivele mobile să fie atât de versatile este multitudinea de aplicații dintre care putem alege. Aceste aplicații ne ajută să fim mai productivi, să comunicăm și să partajăm informații instantaneu cu alții, să ne instruim sau pur și simplu să ne distrăm. Cu toate acestea, împreună cu versatilitatea lor aplicațiile mobile comportă și riscuri. Iată o serie de măsuri ce pot servi pentru securizarea și întreținerea aplicațiilor mobile folosite.

Editor Invitat

Chris Crowley este consultant independent, instructor și autor de cursuri certificat SANS. Este activ pe Twitter **@CCrowMontance** și pe Google plus: **+ChrisCrowley**.

Obținerea aplicațiilor

Primul pas este să vă asigurați că obțineți întotdeauna aplicațiile din surse sigure, de încredere. Rețineți că oricine poate crea o aplicație mobilă, așa că trebuie să fiți atenți de unde le luați. Infractorii și-au îmbunătățit măiestria de a crea și distribui aplicații mobile compromise ce par să fie în regulă. Dacă instalați o astfel de aplicație, răufăcătorii pot prelua controlul dispozitivului mobil, citindu-vă email-ul, ascultându-vă conversațiile sau copiind lista de contacte. Descărcând aplicațiile din surse populare, de încredere, reduceți astfel posibilitatea instalării unora infectate. Ceea ce poate nu sesizați este că marca dispozitivului mobil dictează opțiunile pe care le aveți.

Pentru produsele Apple, cum ar fi iPad sau iPhone, puteți obține aplicațiile dintr-un mediu controlat, portalul Apple app store. Avantajul acestei soluții este că Apple face verificări de securitate atât pentru aplicații cât și în privința autorilor acestora. Deși compania Apple nu poate identifica toți răufăcătorii și aplicațiile mobile infectate, acest mediu controlat reduce drastic riscul instalării de aplicații compromise. În plus, dacă Apple detectează o aplicație suspectă în portal, aceasta este imediat ștearsă. Platforma Windows Phone are o abordare similară pentru administrarea aplicațiilor.

Dispozitivele mobile bazate pe sistemul de operare Android sunt diferite. Android oferă mai multă flexibilitate permițând descărcarea de aplicații de oriunde din Internet. Implicit, această flexibilitate impune o responsabilitate crescută. Trebuie să fiți mult mai atenți cu aplicațiile pe care le descărcați și le instalați deoarece nu toate sunt verificate. Google oferă un mediu controlat pentru administrarea aplicațiilor similar celui de la Apple, numit Google Play. Aplicațiile mobile pe care le descărcați din portalul Google Play beneficiază de o serie de verificări de bază. Prin urmare, vă recomandăm să descărcați

Utilizarea în siguranță a aplicațiilor de pe dispozitivele mobile

aplicațiile pentru dispozitive Android numai din portalul Google Play. Evitați obținerea de aplicații mobile Android din alte surse, deoarece oricine și mai ales răufăcătorii pot crea și distribui aplicații compromise și vă pot păcăli infectându-vă dispozitivul mobil. Ca o măsură suplimentară de protecție, luați în calcul instalarea unui program antivirus pe mobil.

Pentru a reduce riscul și mai mult, evitați aplicațiile nou lansate, cu un număr redus de instalări sau care beneficiază de puține recenzii pozitive. Cu cât disponibilitatea unei aplicații este mai îndelungată și numărul de reacții pozitive de la utilizatorii ei este mai mare, cu-atât e mai probabil ca aplicația să fie sigură. De asemenea, instalați numai aplicațiile de care aveți nevoie. Întrebați-vă: chiar am nevoie de această aplicație? Fiecare aplicație aduce, potențial, nu numai vulnerabilități noi, dar și noi probleme legate de confidențialitate. Dacă nu mai folosiți o aplicație ștergeți-o de pe dispozitivul mobil (o puteți reinstala oricând mai târziu, dacă aveți nevoie de ea).

Esențial pentru folosirea în siguranță a aplicațiilor pe dispozitivele mobile este instalarea lor numai din surse sigure, actualizarea lor și verificarea drepturilor de acces cerute la instalare.

În ultimă instanță ați putea fi tentați să înlăturați protecția sistemului de operare de pe dispozitivul mobil, procedură denumită uzual jailbreaking sau rooting. Această procedură permite instalarea de aplicații ce nu au fost aprobate sau modificarea parametrilor de funcționare și a configurației sistemul de operare a dispozitivului mobil. Recomandăm insistent să evitați jailbreaking-ul sau rooting-ul, deoarece aceste metode ocolesc sau dezactivează marea majoritate a controalelor de securitate ce au fost configurate pe dispozitivul mobil și, în plus, invalidează contractele de garanție și asistență de care beneficiați pentru acesta.

Drepturi de acces

Odată ce ați instalat o aplicație dintr-o sursă de încredere, următorul pas este să vă asigurați că este corespunzător configurată și că vă protejează informațiile personale. Instalarea și configurare aplicațiilor mobile impune cel mai adesea acordarea unor anumite drepturi de acces. Gândiți-vă de fiecare dată înainte să autorizați orice fel de acces dacă aplicația are neapărat nevoie de acele drepturi pentru a funcționa corect. De exemplu, unele aplicații folosesc serviciile de geo-locație. Dacă permiteți unei aplicații să știe permanent unde vă aflați, s-ar putea să dați posibilitatea autorului aplicației să vă urmărească deplasările, eventual să vândă aceste informații altcuiva. Dacă nu vreți să acordați drepturile de acces pe care o anumită aplicație le cere, mai căutați până găsiți o aplicația similară care să vă satisfacă necesitățile. Rețineți că aveți o mulțime de opțiuni la îndemână. Dispozitivele Apple dau posibilitatea modificării anumitor drepturi de acces la execuția unei aplicații, cum ar fi informațiile de geo-locație. Dispozitivele bazate pe Windows sau Android sunt diferite, oferind o abordare de tip *totul sau nimic*. Dacă nu autorizați drepturile de acces specificate nu veți putea instala aplicația.

Utilizarea în siguranță a aplicațiilor de pe dispozitivele mobile

Actualizarea aplicațiilor

Aplicațiile mobile trebuie actualizate, la fel ca sistemul de operare de pe calculatorul personal sau dispozitivul mobil. Infractorii cercetează permanent și identifică vulnerabilitățile aplicațiilor. Ei orchestrează apoi atacuri ce se bazează pe aceste vulnerabilități. Autorii aplicațiilor creează și publică actualizări ale aplicațiilor pentru a rezolva aceste vulnerabilități și pentru a vă proteja dispozitivele mobile. Cu cât verificați mai des și instalați actualizările aplicațiilor, cu-atât mai bine. Bună parte din platformele folosite permit configurarea sistemului pentru actualizarea automată a aplicațiilor. Recomandăm să folosiți această opțiune. Dacă nu este posibil, atunci vă recomandăm să verificați cel puțin la două săptămâni dacă sunt disponibile versiuni actualizate ale aplicațiilor mobile. Chiar și așa, atunci când aplicațiile sunt actualizate verificați orice drepturi de acces suplimentare pe care acestea le pot cere.

Aflați mai multe

Abonați-vă la buletinul informativ lunar OUCH!, accesați arhiva și aflați mai multe despre programele de instruire asupra domeniului securității informației vizitând pagina web SANS http://www.securingthehuman.org

Versiunea în limba română

Grupul Cegeka este un furnizor privat de servicii IT&C fondat în 1992. Având sediul central în Belgia, Cegeka este prezentă în Austria, Republica Cehă, Franța, Germania, Italia, Luxemburg, Olanda, România și Republica Slovacă. Compania furnizează servicii clienților din întreaga Europă: soluții Cloud pentru companii, servicii de securitate, dezvoltare de aplicații folosind tehnicile Agile, mentorat în metodologii Agile și externalizarea infrastructurii IT&C. Cegeka are 3200 de angajați și a realizat o cifră de afaceri combinată de 330 milioane euro în 2013. Pentru mai multe informații vizitați www.cegeka.com.

Resurse

Ingineria socială:	http://www.securingthehuman.org/ouch/2014#november2014
Înlocuirea și casarea dispozitivelor mobile:	http://www.securingthehuman.org/ouch/2014#june2014
Securizarea tabletei nou cumpărate:	http://www.securingthehuman.org/ouch/2013#december2013
Dicționar de termeni uzuali:	http://www.securingthehuman.org/resources/security-terms
SEC575: Curs despre securitatea dispozitivelor mobile:	http://www.sans.org/sec575

Echipa editorială: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducere: Cosmin Hănulescu