OUCH! | Martie, 2017

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 pe dispozitivele mobile

Generalități

Dispozitivele mobile, cum ar fi tabletele, telefoanele sau ceasurile inteligente au devenit una dintre principalele tehnologii pe care le folosim de o potrivă pentru nevoi personale cât și în activitatea profesională. Ce face dispozitivele mobile să fie atât de versatile e multitudinea de aplicații dintre care putem alege. Aceste aplicații ne permit să fim mai productivi, să comunicăm și să partajăm instantaneu informații 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 maximum de beneficii din utilizarea aplicațiilor mobile.

Editor Invitat

Joshua Wright este director tehnic la Counter Hack și instructor senior la Institutul SANS. Este autorul cursurilor SEC575: Securitatea Dispozitivelor Mobile, Ethical Hacking, și Hacking Exposed: Wireless. Josh poate fi contactat pe Twitter la **@joswr1ght**.

Obținerea aplicațiilor

Primul pas este să vă asigurați că obțineți întotdeauna aplicațiile din surse sigure, de încredere. Infractorii și-au îmbunătățit măiestria de a crea și distribui aplicații mobile compromise ce par să fie în regulă. Descărcând aplicațiile din surse populare, de încredere, reduceți astfel posibilitatea instalării unora infectate. Ceea ce poate nu sesizați este că marca dispozitivului mobil folosit dictează opțiunile pe care le aveți la descărcarea de aplicații. Pentru produsele Apple, cum ar fi iPad sau iPhone, descărcați aplicațiile numai din portalul Apple App Store. Avantajul acestei soluții este că Apple face o verificare de securitate pentru toate aplicațiile, înainte să le facă disponibile. Deși compania Apple nu poate identifica toate aplicațiile mobile infectate, acest mediu controlat reduce dramatic 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. Însă, 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 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 cu ușurință aplicații compromise și vă pot păcăli infectându-vă dispozitivul mobil. Ca o măsură suplimentară de protecție, atunci când e posibil, instalați un program antivirus pe mobil.

Esențialul în utilizarea securizată a aplicațiilor pe dispozitivele mobile este instalarea lor numai din surse sigure, actualizarea lor și acordarea drepturilor de acces strict necesare.

Indiferent de tipul de dispozitiv folosit, o măsură suplimentară pe care o puteți lua este să 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, cu cât numărul celor ce au folosit-o a crescut și numărul de reacții pozitive de la utilizatorii ei este mai mare, cu-atât e mai probabil ca aplicația să fie sigură. Mai mult, 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). În final, nu înlăturați protecția sistemului de operare de pe dispozitivul mobil, procedură denumită uzual *jailbreaking* sau *rooting*. Acesta este procedeul prin care obțineți accesul neîngrădit la sistemul dispozitivului și instalați aplicații neautorizate sau schimbați funcționalitatea standard a acestuia. Aceste metode nu numai că ocolesc sau dezactivează marea majoritate a controalelor de securitate ce au fost configurate pe dispozitivul mobil, dar invalidează garanția și asistența de care beneficiați pentru acesta.

Drepturi de acces

Odată ce ați instalat o aplicație dintr-o sursă de încredere, asigurați-vă că este corespunzător configurată și că vă protejează informațiile personale. Gândiți-vă de fiecare dată înainte să autorizați orice fel de acces: vreți să acordați aplicației drepturile de acces solicitate, are aplicația neapărat nevoie de acele drepturi? Dacă permiteți unei aplicații să știe permanent unde vă aflați, s-ar putea să dați posibilitatea autorului aplicației să vă urmărească deplasările, eventual chiar să vândă aceste informații altcuiva. Dacă nu vreți să acordați drepturile de acces pe care o anumită aplicație le cere, blocați cererea de acces și mai căutați până găsiți o aplicația similară care să vă satisfacă necesitățile. Rețineți că aveți o mulțime de opțiuni la îndemână.

Utilizarea în siguranță a aplicațiilor pe dispozitivele mobile

Actualizarea aplicațiilor

Aplicațiile mobile, la fel ca sistemul de operare de pe calculatorul personal sau dispozitivul mobil, trebuie actualizate pentru a fi la zi. Răufăcătorii caută permanent și identifică vulnerabilitățile aplicațiilor. Apoi concep atacuri ce se bazează pe aceste vulnerabilități. Autorii aplicațiilor creează și publică de asemenea actualizări ale aplicațiilor pentru a rezolva aceste vulnerabilități și pentru a vă proteja dispozitivele. Cu cât verificați mai des și instalați actualizările aplicațiilor, cu-atât mai bine. Majoritatea dispozitivelor 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. În sfârșit, atunci când aplicațiile sunt actualizate asigurați-vă că 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 securingthehuman.sans.org/ouch/archives

Versiunea în limba română

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Resurse

Ingineria socială:	https://securingthehuman.sans.org/ouch/2017#january2017
Casarea dispozitivelor mobile:	https://securingthehuman.sans.org/ouch/2016#december2016
Securizarea tabletei noi:	https://securingthehuman.sans.org/ouch/2016#january2016
Arhiva buletinelor OUCH și a traducerilor lor:	https://securingthehuman.sans.org/ouch/archives
Curs despre securitatea dispozitivelor mobile:	https://sans.org/sec575

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