OUCH! | August 2014

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- Ce este criptarea?
- Criptarea datelor stocate
- Criptarea datelor în tranzit

Criptarea

Ce este criptarea?

Probabil ați auzit multe persoane folosind termenul „criptare“ și cum ar trebui s-o folosiți pentru a vă proteja informațiile. Cu toate astea conceptul de criptare poate fi neclar. În plus, criptarea nu vă poate proteja de orice, având și ea limitări. În acest articol vom explica folosind termeni foarte simpli ce este criptarea, de ce ar trebui să o folosiți și cum s-o implementați corect.

Editor Invitat

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) este consultant, rezident în Washington, DC. Este instructor principal pentru cursul Institutului SANS despre Securitatea Dispozitivelor Mobile și Hacking Etic și autorul cursului Coordonarea Echipei de Gestiune a Incidentelor (MGT535).

Dețineți o cantitate enormă de informații confidențiale stocate pe dispozitivele personale, cum ar fi documente financiare, fotografii, mesaje email sau date medicale. Dacă se întâmplă să pierdeți unul dintre aceste dispozitive sau dacă vă este furat, toate aceste informații personale pot fi accesate de oricine a intrat în posesia lor. În plus, obișnuiți să faceți tranzacții online, accesând servicii bancare sau cumpărături. Dacă un răuvoitor v-ar urmări activitatea online, ar putea să fure toate informațiile, de exemplu contul bancar sau numerele cardurilor de credit. Criptarea protejează în astfel de împrejurări oferind siguranța că nicio persoană neautorizată nu vede sau modifică informațiile personale.

Atunci când nu este criptată, informația se cheamă text în clar. Aceasta înseamnă că oricine o poate accesa și citi cu ușurință. Criptarea transformă această informație într-un format ilizibil denumit text cifrat. Criptarea funcționează prin utilizarea unor operațiuni matematice complexe și a unei chei unice pentru convertirea informației în text cifrat. Cheia este ceea ce „încuie“ și „descuie“ informația, așa cum o cheie încuie și descuie o ușă. Un exemplu frecvent de cheie este o parolă, doar cei ce posedă acea parolă fiind capabili să decripteze și să acceseze informația. Pentru a proteja informația, trebuie să vă protejați cheia de criptare a acesteia. În mod uzual criptarea este folosită în două situații, mai precis puteți cripta datele stocate (cum ar fi cele înmagazinate în calculatorul portabil) sau datele în tranzit (cum ar fi transmiterea informațiilor online).

Criptarea informațiilor stocate

Scopul principal al criptării datelor stocate este acela de a proteja informația în cazul în care calculatorul portabil sau dispozitivul mobil este pierdut sau furat. Cu cincisprezece ani în urmă acesta nu era un motiv de îngrijorare, deoarece majoritatea calculatoarelor erau echipamente de birou mari și greoaie, ce erau dificil de mutat dintr-un loc într-altul. Astăzi majoritatea calculatoarelor portabile au 2-3 kilograme iar dispozitivele mobile pot cântări doar câteva zeci de grame. Aceste echipamente sunt foarte puternice și conțin o cantitate imensă de informație dar sunt și foarte ușor de pierdut. Pe lângă

Criptarea

acestea, multe alte medii de stocare, cum ar fi memoriile USB sau discurile CD-ROM, pot conține informații confidențiale. O tehnică uzuală pentru criptarea informației stocate pe astfel de dispozitive este Full Disk Encryption (FDE). Aceasta înseamnă că totul este criptat, nefiind necesar să alegeți ce anume este sau nu criptat. Majoritatea sistemelor de operare moderne au această funcționalitate încorporată, nefiind necesară decât activarea ei. De exemplu, MacOS X are FileVault, în timp ce unele versiuni de Windows includ BitLocker. Dacă sistemul pe care-l aveți are opțiunea Full Disk Encryption, recomandăm călduros activarea ei. De asemenea, multe dispozitive mobile suportă criptarea integrală a datelor stocate intern. De exemplu iOS, sistemul de operare pentru iPhone și iPad, criptează automat datele odată ce s-a activat un cod de acces pe dispozitiv. Pentru a afla dacă dispozitivul pe care-l aveți are funcționalitatea Full Disk Encryption, cereți detalii echipei Helpdesk sau supervizorului. În cazul calculatoarelor proprietate personală contactați producătorul sau consultați documentația disponibilă online.

Criptarea este o metodă puternică de securizare a informației, dar este atât de puternică pe cât de complexă este cheia de criptare folosită.

Criptarea informației în tranzit

Informația este vulnerabilă, de asemenea, și atunci când este în tranzit. Dacă datele nu sunt criptate, pot fi urmărite și capturate online. Acesta este motivul pentru care vreți să vă asigurați că orice comunicare confidențială online, cum ar fi accesarea serviciilor bancare, trimiterea de mesaje electronice sau poate chiar accesarea rețelelor sociale este criptată. Cel mai răspândit mecanism de criptare online este protocolul de transfer de date HTTPS. Aceasta înseamnă că tot traficul dintre programul de navigare și un site Web este criptat. Căutați așadar https:// în adresă, un lacăt desenat alături de aceasta sau evidențierea adresei în culoarea verde în programul de navigare online. Toate acestea sunt semne care confirmă că transferul de date online este criptat. În funcție de programul de navigare online folosit și de site-ul vizitat, puteți să vedeți toate aceste indicii simultan. De asemenea, atunci când vă conectați la o rețea wireless cu acces public, asigurați-vă că este folosită criptarea, pe cât posibil. Nu în ultimul rând, ori de câte ori trimiteți un mesaj email, asigurați-vă că programul de mesagerie electronică folosit este configurat să transmită datele printr-un canal criptat. Majoritatea acestor programe oferă posibilitatea criptării și, în plus, furnizorul de servicii de acces Internet vă poate oferi asistența necesară configurării criptării în clientul de email folosit.

Implementarea corectă a criptării

Indiferent ce tip de criptare folosiți sau cum o folosiți, majoritatea formelor pe care le ia criptarea au în comun o serie de pași ce trebuie urmați pentru o utilizare adecvată:

Criptarea

- Criptarea pe care o folosiți este atât de puternică pe cât de puternică este cheia folosită. Dacă cineva ghicește sau modifică această cheie, va obține acces la datele Dumneavoastră. Trebuie să vă protejați cheia de criptare.
- Dacă folosiți un cod de acces sau o parolă pentru cheia de criptare, asigurați-vă că este suficient de lungă și complexă, n-o pierdeți și n-o uitați. Dacă o uitați nu mai puteți accesa propriile date personale.
- Criptarea pe care o folosiți este la fel de puternică pe cât de puternică este securitatea calculatorului folosit. Dacă aceasta a fost compromisă de un atac informatic atunci răuvoitorii pot ocoli criptarea. În consecință, fiți siguri că ați securizat calculatorul personal și dispozitivul mobil folosit.
- Aveți la dispoziție mai multe variante de criptate; alegeți întotdeauna cea mai puternică metodă.

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

Cegeka este o companie de servicii IT integrate cu peste 2100 de angajați, prezentă în Benelux, Franța, Polonia și România. Clienții beneficiază de consultanță, dezvoltare de software și aplicații Web, administrarea infrastructurii IT la distanță sau la sediile proprii, sau servicii de externalizare complexe. Având propriile centre de date moderne, Cegeka deține expertiza și tehnologiile ce garantează agilitatea și inovația necesare rezolvării celor mai complexe cerințe ale clienților. Pentru mai multe informații accesați www.cegeka.com sau urmăriți-ne pe Twitter @cegeka

Resurse

Mac OS X Filevault:	http://support.apple.com/kb/ht4790
Despre criptare în iOS:	http://support.apple.com/kb/ht4175
Despre criptare pe Android:	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
Criptarea în Windows:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
Securizarea calculatorului personal:	http://www.securingthehuman.org/ouch/2012#december2012
Programe de gestionare a parolelor:	http://www.securingthehuman.org/ouch/2013#october2013

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

