OUCH! | Iunie 2016

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Ce este criptarea?**
- **Ce se poate cripta?**
- **Cum se face corect**

Criptarea

Ce este criptarea?

Puteți auzi oamenii folosind termenul criptare și vorbind despre modul în care o puteți folosi pentru a vă proteja propria persoană sau informațiile pe care le dețineți. Criptarea poate însă crea confuzii și ar trebui să îi puteți înțelege limitele. În acest număr explicăm în termeni simpli ce este criptarea, modul în care aceasta vă poate proteja și modul în care puteți să o aplicați corect.

Editor Invitat

Francesca Bosco (**@francibosco**) este cercetător și administrator de proiect pentru proiecte din sfera infracțiunii cibernetice, securității cibernetice și folosirea necorespunzătoare a tehnologiei. Lucrează la United Nations Interregional Crime and Justice Research Institute și este co-fondator al Tech and Law Center.

Dețineți o cantitate semnificativă de informații sensibile pe calculatoare sau telefoane, cum ar fi documente personale, poze și email-uri. Dacă v-ați pierde sau vi s-ar fura unul dintre aceste dispozitive, toate informațiile sensibile ar putea fi accesate de oricine este în posesia acelui dispozitiv în acel moment. Mai mult, poate că, de regulă, faceți o serie de operațiuni sensibile online cum ar fi tranzacții bancare sau cumpărături. Dacă cineva v-ar monitoriza aceste activități, v-ar putea fura informații referitoare la numerele conturilor și ale cardurilor de credit. Procedeul de criptare vă protejează în aceste situații prin a se asigura că nicio persoană neautorizată nu vă poate accesa sau modifica informațiile.

Criptarea există de mii de ani. În prezent criptarea este mult mai sofisticată dar servește aceluiași scop – acela de a transmite un mesaj secret dintr-un loc în altul, cu asigurarea faptului că doar cei autorizați îl pot citi și accesa. Atunci când informația nu este criptată aceasta se numește *plain text* sau text simplu. Aceasta înseamnă că oricine o poate citi sau accesa. Criptarea convertește această informație într-un format neinteligibil numit *cipher-text* sau text-cifrat. Procedeele de criptare din prezent folosesc operații matematice complexe și o cheie unică pentru convertirea informației în text-cifrat. Cheia este cea care ascunde sau arată informația. În majoritatea cazurilor cheia este parola de acces sau codul de acces.

Ce se poate cripta?

În general există două tipuri de date care se criptează: date în stare de repaus (cum ar fi datele stocate pe telefonul mobil) și date în mișcare (cum ar fi descărcarea email-urilor și schimbul de mesaje instant cu un prieten).

Criptarea datelor în stare de repaus este vitală pentru protejarea informațiilor în cazul în care computerul sau telefonul mobil este pierdut sau furat. Aparatele din ziua de azi sunt extrem de puternice și dețin o cantitate impresionantă de informații dar

Criptarea

sunt, de asemenea, și foarte ușor de pierdut. În plus, există și alte tipuri de unități mobile care pot conține informații sensibile, precum memorii USB flash sau hard discuri externe. Full Disk Encryption (Criptarea Intregului Disc) (FDE) este o tehnică de criptare folosită pe scară largă, care criptează întregul disc în cadrul sistemului. Aceasta înseamnă că tot ce există în sistem este automat criptat și dumneavoastră nu trebuie să decideți ce să criptați și ce să nu criptați. În prezent, majoritatea computerelor sunt livrate cu sistemul FDE dar pot exista situații în care trebuie să porniți / activați manual acest sistem. Pe computerele Mac acesta se numește FileVault iar pe computerele Windows, în funcție de versiune, puteți folosi Bitlocker sau Device Encryption. Majoritatea telefoanelor mobile dețin FDE. iOS, pe iPhone și iPad, activează automat FDE odată ce a fost setat un cod de acces. Începând cu versiunile Android 6.0 (Marshmallow), Google solicită activarea implicită a sistemului FDE, cu condiția ca sistemul hardware să îndeplinească anumite standarde minime.

Criptarea este o metodă puternică de a vă securiza informațiile dar puterea ei depinde direct de cea a cheii.

Informația mai este vulnerabilă atunci când se află în tranzit. Dacă datele nu sunt criptate, acestea pot fi monitorizate, modificate și capturate online. De aceea, ar trebui să vă asigurați că orice tranzacții și comunicări online sensibile sunt criptate. Un mod comun de criptare este HTTPS. Aceasta înseamnă că tot traficul între programul de navigare online și site-ul web este criptat. Uitați-vă după https:// în adresa URL, un simbol cu lacăt sau colorarea în verde a adresei URL. Un alt exemplu este momentul în care trimiteți sau primiți un email. Majoritatea clienților de email furnizează capabilități de criptate pe care ar putea fi nevoie să le activați. Un al treilea exemplu de criptare a datelor aflate în tranzit este între doi utilizatori care schimbă mesaje instant prin aplicații de tip iMessage, Wickr, Signal, WhatsApp, sau Telegram. Aplicațiile de acest fel folosesc criptare *end-to-end*, care previne accesarea datelor de către o terță parte, în timp ce acestea sunt transferate de la un sistem către altul. Aceasta înseamnă că doar dumneavoastră și cel cu care comunicați puteți citi ceea ce se trimite.

Cum se face în mod corect

Pentru a fi sigur că sunteți protejat când folosiți criptarea este de importanță capitală să folosiți corect acest procedeu.

- Puterea criptării este direct proporțională cu cheia. Dacă cineva ghicește sau intră în posesia cheii, această persoană va avea acces la date. Protejați-vă cheia. Dacă folosiți un cod de acces sau o parolă de acces drept

Criptarea

cheie, asigurați-vă că aceasta este o parolă puternică, unică. Cu cât aceasta este mai lungă, cu atât îi va fi mai greu unui atacator să o ghicească sau să o forțeze. Nu uitați parola, fără cheie nu vă mai puteți decripta informațiile. Dacă nu vă puteți aminti toate parolele, vă recomandăm un program de gestiune a parolelor.

- Puterea criptării depinde de securitatea dispozitivelor pe care le dețineți. Dacă computerul sau telefonul au fost compromise sau infectate cu programe malware, atacatorii cibernetici vă pot ocoli criptarea. De aceea este foarte important să luați alte măsuri pentru a vă proteja sistemul, printre care folosirea unui program anti-virus, parole puternice și actualizarea în permanență a sistemului.
- Multe aplicații de mobil sau computer oferă acum criptări puternice pentru a vă proteja datele și comunicarea. Dacă aplicația pe care vă gândiți să o instalați nu suportă criptarea, atunci gândiți-vă la o alternativă.

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

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

Criptarea explicată:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Propoziții-parolă:	https://securingthehuman.sans.org/ouch/2015#april2015
Programe de gestiune a parolelor:	https://securingthehuman.sans.org/ouch/2015#october2015
Ce sunt programele malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Securizarea tabletei:	https://securingthehuman.sans.org/ouch/2016#january2016

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