Buletini mujor për vetëdijësimin mbi sigurinë e përdoruesve të kompjuterëve

OUCH!

NË KËTË EDICION..

- Ç'është enkriptimi?
- Enkriptimi në qetësi
- Enkriptimi në lëvizje

Enkriptimi

Ç'është enkriptimi?

Ju mund të keni dëgjuar dikë të përdorë shprehjen "enkriptim" dhe si duhet ta përdorni atë për të ruajtur informatat tuaja. Por, koncepti i enkriptimit mund të duket pak i paqartë. Së pari, enkriptimi nuk mund t'ju mbrojë nga çdo rrezik, pra ka kufizimet e veta. Në këtë broshurë informative ne do të sqarojmë me fjalë të thjeshta se ç'është enkriptimi, pse duhet ta përdorni atë si dhe si ta zbatoni në mënyrë të saktë.

Botuesi i ftuar

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) është konsulent me qëndrim në Washington, DC. Ai është instruktor kryesor në Institutin SANS, në lëndët Mobile Device Security dhe Ethical Hacking (SEC575) si dhe autor për Incident Response Team Management (MGT535).

Ju ruani sasi të madhe të informatave në pajisjet tuaja, si p.sh. dokumente financiare, fotografi, emaile, ose të dhëna shëndetësore. Nëse ndodh të ju humbet ndonjë nga pajisjet tuaja, të gjitha ato informata të ndieshme mund të qasen nga dikush që e merr atë pajisje. Gjithashtu, ju mund të bëni blerje të ndieshme online, si p.sh. bankingu elektronik apo blerjet. Nëse një sulmues kibernetik provon të monitorojë aktivitetet tuaja online, ata mund t'i vjedhin të gjitha informatat tuaja, si p.sh. llogaritë bankare apo numrat e kartave të kreditit. Enkriptimi ju mbron nga këto situata duke u siguruar që njerëzit e paautorizuar nuk mund t'i qasen apo t'i modifikojnë informatat tuaja.

Kur informata nuk enkriptohet, quhet tekst i thjeshtë (ang. Plain-text). Kjo do të thotë që çdokush mund ta lexojë apo t'i qaset atij informacioni. Enkriptimi e ndryshon këtë informatë në një tekst të palexueshëm të quajtur tekst me shifër (ang. Cipher-text). Enkriptimi funksionon duke përdorur operacione komplekse matematikore dhe një çelës të veçantë për ta shndërruar informatën tuaj në "cipher-text". Çelësi (ang. Key) është ai që e mbyll apo e hap informatën tuaj për lexim, njësoj sikurse një çelës që e hap apo e mbyll një derë. Një shembull i zakonshëm i një çelësi është fjalëkalimi (ang. Password), pra vetëm personat që e kanë atë fjalëkalim mund ta dekriptojnë dhe t'i qasen informatës suaj. Për ta mbrojtur informatën tuaj të enkriptuar ju duhet ta mbroni çelësin tuaj. Në përgjithësi enkriptimi funksionon në dy mënyra, ju mund të enkriptoni të dhëna në qetësi (si p.sh. të dhënat tuaja në laptop) ose në lëvizje (gjatë levizjes së informatave tuaja online).

Enkriptimi i informatave në qetësi

Qëllimi kryesor i enkriptimit në qetësi është që të mbrojë informatat në raste kur kompjuteri apo pajisja juaj mobile vidhet nga dikush. Para rreth pesëmbëdhjetë vjetësh ky nuk ka qenë problem, sepse kompjuterët ishin të mëdhenj dhe të vështirë të lëvizen. Sot shumë laptopë peshojnë pak kilogramë, derisa pajisjet mobile pak gramë. Këto pajisje janë shumë të fuqishme

Enkriptimi

dhe përmbajnë sasi të madhe të informatave, por janë shumë të lehta që të humben. Gjithashtu, mediume tjera të lëvizshme mund të mbajnë të dhëna të ndjeshme, sikurse USB-të apo disqet kompakte (CD-ROM). Një teknikë e zakonshme e enkriptimit të informatave në këto mediume quhet Enkriptimi i Plotë i Diskut (ang. Full Disk Encryption – FDE). Kjo do të thotë se çdo gjë në sistem enkriptohet në mënyrë automatike, ju nuk keni nevojë të vendosni se çka të enkriptohet e çka jo. Shumica e sistemeve operative sot përmbajnë një FDE në vete, ju thjesht duhet ta aktivizoni. Për shembull, Mac OS e përfshin FileVault përderisa disa versione të Windows e kanë Bitlocker. Nëse kompjuteri juaj përkrah FDE, ne ju këshillojmë që ta aktivizoni. Gjithashtu shumica e pajisjeve mobile e përkrahin FDE për hapësirat e memorjes që kanë. P.sh. iOS, sistemi operativ për iPhone dhe iPad, automatikisht e aplikon FDE në momentin që ju vendosni një fjalëkalim. Që ta kuptoni nëse kompjuteri juaj apo pajisja mobile e përkrah FDE, pyesni njësinë përkrahëse apo mbikqyrësin tuaj. Për kompjuterët personalë, kontaktoni prodhuesin e kompjuterit tuaj apo lexoni dokumentacionin përcjellës.

Enkriptimi është një mënyrë e fuqishme e mbrojtjes së të dhënave tuaja, por është poaq i fortë sa është çelësi juaj enkriptues.

Enkriptimi i informatave në lëvizje

Informata është e cënueshme edhe kur është në lëvizje. Nëse informacioni nuk është i enkriptuar, ai mund të monitorohet dhe të kapet gjatë lëvizjes online. Kjo është arsyeja pse duhet të sigurohuni që çdo informatë e ndjeshme në komunikimet online, si bankingu elektronik, dërgimi i emaileve ose ndoshta edhe qasja në mediume sociale është e enkriptuar. Enkriptimi më i shpeshtë online është HTTPS. Kjo do të thotë që është enkriptuar i tërë trafiku në mes të shfletuesit tuaj të internetit (ang. Browser) dhe faqes që vizitoni. Kërkoni pjesën që fillon me https:// në rreshtin që shkruani në shfletues, apo ikonën e drynit në një cep të faqes, ose vëreni kur rreshti bëhet me ngjyrë të gjelbër. Këto janë shenja që komunikimi është i enkriptuar. Varësisht nga shfletuesi që keni apo faqja e internetit, ju mund t'i shihni të tri këto shenja njëkohësisht. Gjithashtu, sa herë që lidheni në vende publike me Wi-Fi (rrjet pa tel), sigurohuni që përdorni enkriptim nëse është e mundur. Në fund, kur dërgoni apo pranoni emaile sigurohuni që klienti i emailit që përdorni është i konfiguruar që të transmetojë email nëpër kanale të sigurta. Shumica e klientëve ofrojnë enkriptim, gjithashtu edhe ISP i juaj mund t'ju ndihmojë të aktivizoni enkriptimin në klientin tuaj të emailit.

Zbatimi i drejtë i enkriptimit

Pa marrë parasysh llojin e enkriptimit që përdorni apo si e përdorni, gati të gjithë format e enkriptimit ndajnë diçka të përbashket në hapat që duhet ndjekur që të përdoret drejt.

Enkriptimi

- Enkriptimi juaj është poaq i fortë sa çelësi juaj. Nëse dikush e qëllon apo e komprometon çelësin tuaj, ata do të kenë qasje në të dhënat tuaja. Ju duhet ta mbroni çelësin tuaj.
- Nëse përdorni një fjalëkalim apo kod si çelës, sigurohuni që ai të jetë i gjatë dhe i sigurt dhe të mos e humbisni apo harroni atë. Nëse e harroni atë, ju do të kyçni përgjithmonë të dhënat tuaja.
- Enkriptimi juaj është poaq i fortë sa siguria e kompjuterit tuaj. Nëse kompjuteri juaj është manipuluar apo infektuar atëherë sulmuesit kibernetikë mund të anashkalojnë enkriptimin tuaj. Prandaj sigurohuni që kompjuteri apo pajisja juaj mobile janë të sigurt poashtu.
- Nëse ju jepen disa mundësi për enkriptim, gjithmonë zgjidhni mënyrën më të sigurt.

Mëso më shumë

Regjistrohuni në buletinin tonë mujor për vetëdijësimin mbi sigurinë OUCH!, qasuni në arkivat e OUCH!, dhe mësoni më shumë mbi zgjidhjet për ngritjen e vetëdijes mbi sigurinë të ofruara nga SANS duke na vizituar në faqen http://www.securingthehuman.org.

Edicioni në shqip

Edicioni në shqip i OUCH! është përkthyer nga gjuha angleze nga Ilir Bytyçi dhe Jorida Nano. Iliri është magjistër i shkencave në administrimin e rrjetave dhe sistemeve kompjuterike, është ligjërues në universitet për lëndë të ndryshme nga fusha e TI, dhe është përgjegjës për sigurinë e teknologjise informative në bankë. Jorida është përkthyese profesioniste e gjuhës angleze në OSBE.

Burimet

Mac OS X Filevault:	http://support.apple.com/kb/ht4790
Enkriptimi i iOS:	http://support.apple.com/kb/ht4175
Enkriptimi në Android:	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
Enkriptimi në Windows:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
Sigurimi i kompjuterit tuaj:	http://www.securingthehuman.org/ouch/2012#december2012
Menaxhuesit e fjalëkalimeve:	http://www.securingthehuman.org/ouch/2013#october2013

Bordi editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Përkthyer nga: Ilir Bytyçi dhe Jorida Nano