Buletini mujor për vetëdijësimin mbi sigurinë e përdoruesve të kompjuterëve

OUCH!

NË KËTË EDICION..

- Hyrje
- Pesë hapat kryesorë

Pesë hapat për të ruajtur sigurinë

Hyrje

Teknologjia po fiton një rol gjithmonë e më të rëndësishëm në jetët tona, por njëkohësisht po bëhet gjithmonë e më komplekse. Për shkak të shpejtësisë së ndryshimit të teknologjisë, përditësimi i këshillave mbi sigurinë mund të na hutojë. Duket sikur gjithmonë dalin udhëzime të reja se çfarë duhet të bëjmë apo të mos bëjmë. Megjithatë, edhe pse detajet në lidhje me të qenit të sigurt ndryshojnë gjatë gjithë kohës, ka disa gjëra themelore që mund të na ndihmojnë të mbrohemi. Pavarësisht teknologjisë që po përdorni apo ku po e përdorni, ne rekomandojmë këto pesë hapa kryesorë.

Botuesi i ftuar

Lenny Zeltser ka si fokus ruajtjen e sigurisë së operacioneve IT të klientëve të NCR Corp dhe jep mësim mbi luftimin e viruseve në SANS Institute. Lenny është aktiv në Twitter në **@lennyzeltser** dhe ka një blog mbi sigurinë në **blog.zeltser.com**.

Pesë hapat kryesorë

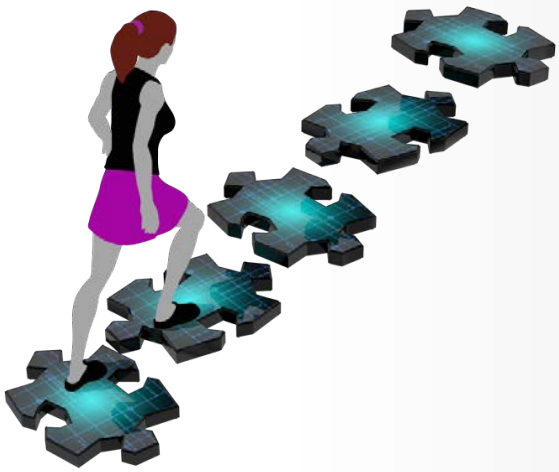
Secili prej pesë hapave më poshtë është një përmbledhje e thjeshtë. Për të mësuar rreth secilit prej tyre referojuni Burimeve në fund të buletinit.

1. **Ju**: Së pari dhe mbi të gjitha, kini parasysh se teknologjia nuk mund t'ju mbrojë e vetme. Sulmuesit kanë mësuar se mënyra më e lehtë për të shmangur teknologjinë e sigurisë është t'ju sulmojnë. Nëse ata duan të dinë fjalëkalimin apo numrin e kartës suaj të kreditit, rruga më e lehtë është që t'ju gënjejnë dhe ju t'ua jepni vetë këtë informacion. Për shembull, ata mund t'ju marrin në telefon duke thënë se marrin nga Microsoft-i dhe se kompjuteri juaj është infektuar, kur në fakt janë thjesht kriminelë kibernetikë që duan të marrin informacion nga ju. Ose mund t'ju dërgojnë një email ku shpjegojnë se pako juaj nuk është dërguar dhe ju kërkojnë të hapni një link për të konfirmuar adresën tuaj, kur në të vërtetë duan që ju të hapni një webiste me virus për të hyrë në kompjuterin tuaj. Përfundimisht, mbrojtja më e madhe nga sulmuesit jeni ju. Jini dyshues! Përdorni logjikën dhe mund të dalloni e ndaloni shumicën e sulmeve.

2. **Përditësimi**: Sigurohuni që kompjuterët, celularët, aplikacionet, dhe çdo gjë tjetër e lidhur me rrjetin përdorin software-in më të fundit. Kriminelët kibernetikë kërkojnë vazhdimisht pika të dobëta në teknologjinë që ju përdorni. Kur i zbulojnë, përdorin programe të veçanta për të shfrytëzuar këto pika të dobëta dhe hyjnë në çfarëdo teknologjie që po përdorni, duke përfshirë rrjetin, kompjuterin, dhe pajisjet elektronike të lëvizshme. Ndërkohë, kompanitë që kanë krijuar

Pesë hapat për të ruajtur sigurinë

teknologjinë që ju përdorni punojnë gjithë kohës për ta përditësuar atë. Pasi mësohet një pikë e dobët, ata krijojnë një përditësim (ang. patch) për ta rregulluar dhe e bëjnë publike atë. Nëse siguroheni që kompjuterët tuaj dhe pajisjet elektronike të lëvizshme i kanë këto përditësime, ulni numrin e pikave të dobëta të njohura dhe vështirësoni sulmet ndaj jush. Për të qëndruar të përditësuar, mundësoni përditësimin automatik sa herë të mundni. Ky rregull vlen për pothuajse çdo teknologji që lidhet me një rrjet, duke përfshirë edhe televizorët që kanë lidhje interneti, monitorët e vegjël, modemet, lojërat elektronike, ose ndonjë ditë edhe automjetin tuaj. Nëse sistemi operues i kompjuterit tuaj, pajisjes elektronike të lëvizshme, ose të ndonjë teknologjie tjetër që përdorni nuk mbështet më dhe nuk do të vazhdojë të përditësohet, ne ju rekomandojmë të merrni një version të ri që ka mbështetje.



Duke ndjekur këto pesë hapa kryesorë ju mund të jeni të mbrojtur për shumë kohë ndërsa përdorni teknologjinë më të fundit.

3. **Fjalëkalimet**: Hapi tjetër është përdorimi i një fjalëkalimi të vështirë e të veçantë për secilën nga pajisjet tuaja, llogaritë online, apo aplikacionet. Fjalët kyçe këtu janë i vështirë dhe i veçantë. Një fjalëkalim i vështirë do të thotë që nuk mund të gjendet lehtë nga hacker-at apo nga programet e tyre të automatizuara. Në vend të një fjale të vetme, përdorni një frazë të gjatë ose disa fjalë të kombinuara me simbole dhe numra. I veçantë do të thotë të përdorni nga një fjalëkalim të ndryshëm për çdo pajisje dhe llogari online. Në këtë mënyrë, nëse kompromentohet një nga fjalëkalimet, llogaritë dhe pajisjet e tjera janë ende të sigurta. Nuk i mbani mend gjithë ato fjalëkalime të vështira dhe të veçanta? Mos u shqetësoni, as ne nuk i mbajmë mend. Kjo është arsyeja pse ju rekomandojmë të përdorni një menaxher fjalëkalimesh – një aplikacion i specializuar për smartphone-in ose kompjuterin tuaj që mund të ruajë në mënyrë të sigurt të gjithë fjalëkalimet tuaja në format të koduar. Së fundi, nëse ndonjë nga llogaritë tuaja pranon verifikimin me dy hapa, ne rekomandojmë që ta aktivizoni gjithmonë sepse kjo është një nga mënyrat më të fuqishme për ta mbrojtur.

4. **Enkriptimi**: Një hap i tretë që rekomandojmë është enkriptimi që siguron se vetëm ju ose njerëzit tuaj të besuar mund të kenë qasje në informacionin tuaj. Të dhënat mund të enkriptohen në dy vende: në qetësi dhe në lëvizje. Enkriptimi i të dhënave në qetësi do të thotë t'i mbrosh kur janë të ruajtura si dosje si p.sh në hard drive apo në USB. Shumica e sistemeve operative ju lejojnë t'i enkriptoni automatikisht të gjithë të dhënat tuaja duke përdorur instrumente të tilla si Full Disk Encryption. Ne ju rekomandojmë që ta aktivizoni sa herë të jetë e mundur. Enkriptimi i të dhënave në lëvizje do të thotë që enkriptohen ndërsa transferohen nga kompjuteri apo pajisja juaj në pajisje të tjera, si p.sh kur

Pesë hapat për të ruajtur sigurinë

përdorni e-banking. Një mënyrë e thjeshtë për të verifikuar që enkriptimi është i aktivizuar kur ju navigoni në internet është të filloni kërkimin e adresës me “https:” e cila ka pranë imazhin e një kyçi.

5. **Backup**: Ndonjëherë, pavarësisht sa të kujdesshëm jeni, një nga pajisjet apo llogaritë tuaja mund të kompromentohen. Nëse ndodh, mënyra më e shpeshtë për të siguruar që kompjuteri apo pajisja juaj nuk ka marrë virus është ta formatoni nga fillimi. Sulmuesi mund të mos ju lejojë që të shihni dosjet tuaja personale, fotot, apo ndonjë informacion tjetër të ruajtur në sistemin e kompromentuar. E vetmja mundësi mund të jetë t’i rimerrni informacionet tuaja personale nga backup-i. Sigurohuni që po bëni back-up (ruajtje e të dhënave diku tjetër) vazhdimisht dhe verifikoni që mund t’i rimerrni të dhënat nga backup-i. Shumica e sistemeve operative dhe pajisjet elektronike të lëvizshme lejojnë backup-in automatik.

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

Sulmet me viruse ndaj email-it:	http://www.securingthehuman.org/ouch/2013#february2013
Të mbani kompjuterin të sigurt:	http://www.securingthehuman.org/ouch/2013#december2013
Fjalëkalime të vështira:	http://www.securingthehuman.org/ouch/2013#may2013
Menaxherët e fjalëkalimeve:	http://www.securingthehuman.org/ouch/2013#october2013
Verifikimi me dy hapa:	http://www.securingthehuman.org/ouch/2013#august2013
Enkriptimi:	http://www.securingthehuman.org/ouch/2014#august2014
Backup:	http://www.securingthehuman.org/ouch/2013#september2013

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