Kuidas kaitsta Mäkki?

14 aastat tagasi - 14.01.2011 Autor: AM

(Arvutimaailm 10/10)

? Olles Windowsikasutaja ja minnes üle OS X-ile ehk Mac-ile arvavad paljud, et on lõplikult vabanenud viirustest ja igasugusest pahavarast. See on nii ja ei ole ka.

! Hoidkem kätt sündmuste pulsil. Kõik kasutajad, sõltumata platvormist, peavad mingil määral end siiski kaitsma ja kaitsmiseks lihtsaid asju teadma.

Jah, Macil ei ole nii palju viiruseid kui Windowsil, kuid see ei ole tingitud sellest, et Windows on „paha“. Ei ole see ka tingitud sellest, et Windows on levinum ning OS X-i all ei ole need viirused nö nii „lahedad“ häkkeri vaatenurgast.

Mac OS X esimene viirus avastati SophosLabsi poolt 16. veebruaril 2006. See levis läbi Macintosh Messenger iChati. Viirus oli tehtud nii, et paistis olevat täiesti süütu JPEG faili ikoon. Viirus levitas iseennast failina, mis sisaldas nakatunud kontakte. Kasutaja võttis faili vastu ja oligi nakatunud. Midagi kurja see ei teinud, arvatavasti oli eesmärk näidata, et OS X kasutajad ei ole alati kaitstud.

Praeguseks on Maci kasutajaid rünnanud umbkaudselt 60-80 erinevat viirust. Praegu valitseb küll taas viirusemaastikul suhteline vaikus, kuid olgem ausad, me ei tea ju, millal võib mingi viirus taas välja tulla. Näiteks võivad need tulla läbi .doc formaadis dokumendi makrode. Jutt käib viirustest, siin hulgas ei ole reklaam- ega nuhkvara ja turvaaugud - ärge unustage ka neid.

OS X all näevad kõik programmid välja ühe failina, mida nimetatakse Bundle arhitektuuriks. Üks fail hoiab enda sees teisi faile ja installimisel OS X ei viska erinevaid kaustu ja faile süsteemi laiali. See on nii pluss kui ka miinus. Hea ja mugav on kasutajal ja arendajal, kuid hea on ka häkkeril. Viirus võib teha nii, et ta paistab välja näiteks kui iTunes. Kasutaja käivitab selle, mille järel avanebki iTunes, et kasutaja ei hakkaks midagi kahtlustama. Sellega koos aga käivitub ka mingi kood, mis juba teeb oma inetuid asju.

Suuremad sorti turvaaugud on olemas nii OS Xis (praegu näiteks Apple´i QuickTime´is) kui ka kolmanda osapoole tarkvaral (näiteks Adobe´i toodetel). Viimane iPhone tarkvara lahtimuukimine käiski läbi PDF-i.
Varsti me jõuamegi nii kaugele, et ei ole vahet, millist operatsioonisüsteemi kasutame. See aga tähendab, et kaitsta tuleb end samuti vaatamata kasutatavale operatsioonisüsteemile.

Kõige lihtsamad turvalisuse punktid, mida inimesed tavaliselt unustavad üle minnes Windowsiga arvutilt Mac-ile, on siin.

15 turvalisuse alustala

1. Mõtle juba antiviiruse peale! Jah, praegu on kõik roosiline ja ilus, kuid vaevalt, et see kestab väga kaua. Kes ei soovi kulutada, võib kasutada avatud lähtekoodiga tasuta antiviirust ClamXav. Tasulise tarkvara valik on üpriski suur: Avast! Antivirus, iAntiVirus, MacScan, Norton AntiVirus, Sophos Anti-Virus, VirusBarrier X5, VirusScan, ProtectMac. Tasulistest soovitan näiteks VirusBarrier X5te. Skanni arvutit ning tarkvara, mida tahad paigaldada ja uuenda antiviirust. See oleks juba hea esimene samm.
2. Alati installi Apple´i enda uuendusi, see jutt käib eriti turvauuenduste kohta. Need parandavad suuremad turvaaugud.
3. Open source ja vabalt kättesaadavate failide puhul kontrolli nende allikaid. Nendes programmides võivad peituda ka trooja hobused. Ära installi kahtlaseid lisandeid oma tarkvarale. Nagu esimene viiruski, mis oli Mac-il esmapilgul tavaline pilt, võib osutuda see lisand hoopis miskiks muuks.
4. Ole ettevaatlik Office´i dokumentidega. Office´i makrotes võivad peituda skriptid, mis võivad pahandust teha. Office muidugi teatab, kui dokument sisaldab makrot, nii et kontrolli taas allikaid ja ära igaks juhuks neid makrosid ava.
5. Lihtne põhireegel: ära kasuta administraatori kontot. Tee endale tavaline konto igapäevaseks kasutamiseks.
6. OS Xil on olemas programm „Keychain“, mis hoiab enda sees veebilehekülgede, rakenduste ja serverite paroole. Juhul, kui kasutad Safari AutoFill funktsiooni, siis ka kõik konto andmed on seal. Vaikimisi on Keychaini parool sama, mis sinu kontol. Juhul, kui oled sisse loginud, saab ka keychaini lahti. Et seda vältida, määra Keychainile teine parool. Samuti seadista, et Keychain paneks end lukku mingi aja vältel, kui Mac läheb unerežiimi.
7. Krüpteeri oma ketas. Samuti kasuta FileVaulti, mis lukustab ja krüpteerib sinu kasutaja kausta ja küsib alati parooli.
8. Kogu ketta krüpteerimine tundub absurdne? Kasutada Disk Utilityt ja loo endale disk image, mis käitub kui tavaline kaust, kuid mis ei ole paigaldatud (mountitud) senikaua, kuni on sisestatud õige parool.
9. Kasuta tulemüüri. Seda juhul, kui sa ei kasuta antiviirust, millel juba on oma tulemüür. Õnneks see on vaikimisi sisse lülitatud, kuid igaks juhuks kontrolli üle.
10. Lülita igasugused Sharing ehk andmete jagamise funktsioonid välja, kaasa arvatud Bluetooth, juhul kui sa seda ei kasuta.
11. Krüpteeri oma võrgusessioon ja kasuta üle Intyerneti turvalist kanalit ehk VPNi.
12. Ära kasuta piraattarkvara. Suurem osa igasugust pahavara ja muud kahtlast sodi liigub just piraattarkvaras. Tuntud on juhud, kus trooja hobused saabusid arvutisse koos iWorki ja Adobe CS4ga.
13. Kui sul on installitud BootKampi abil Windows või muu operatsioonisüsteem, siis kindlusta ka selle turvalisus. Ühte kaitstes kaitse ka teist.
14. Nakatanud Mac võib nakatada ka iPhone´i, iPodi ja iPadi ning vastupidi, juhul kui on kasutusel näiteks Jailbroken ehk võrgulukust lahti murtud iPhone vms.
15. Tee varukoopiaid. OS Xle ei ole vaja mingit lisatarkvara, muretse vaid varuketas ja lase TimeMachine käima, mis teeb regulaarselt varukoopiaid.

EVGENI NIKOLAEVSKI
Riigi Infosüsteemide Arenduskeskus, kasutajatoe spetsialist

- Lahendused

- Tarkvara
- Turvalisus