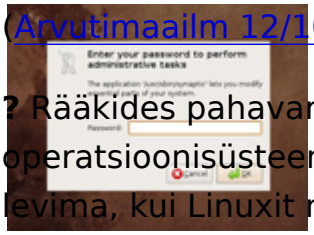
Miks pahavara Linuxis ei levi?

15 aastat tagasi - 18.03.2011 Autor: AM

(Arvutimaailm 12/10)



? Rääkides pahavarast tekib küsimus, kas see levib vaid populaarsetes operatsioonisüsteemides? Miks pahavara näiteks Linuxis ei levi ja kas hakkab levima, kui Linuxit rohkem kasutatakse?

! Julgen väita, et kui Linuxis jäädakse praeguse ülesehituse juurde, siis pahavara ei levi ka Linuxi populaarsuse kasvades. Kasutajaõigused on paigas, pahavara käivitamiseks peab kasutaja ise loa andma.

Kui Linuxist ei üritata Windowsit teha, siis ei teki ka probleeme pahavaraga (vt näiteks http://linux.oneandoneis2.org/LNW.htm). Kui aga üritatakse meeleheitlikult sarnaneda Windowsiga, siis loobutakse mugavuse nimel turvalisusest ja tulemuseks on kaos. Siiski areneb Linux distrotena ja säilivad ka nö Linuxi algupära säilitavad versioonid.

Pahavara tõrjumisest Linuxis aga siiski räägitakse ja aina enam. Põhiliselt seetõttu, et Windowsi maailmast tulnud dokumente tuleb puhastada, et mitte omakorda teisi Windowsi kasutajaid nakatada, kellele suure tõenäosusega neid dokumente edasi saadetakse. Lisaks failiserverid, kus Windowsi kasutajad oma faile hoiavad või e-posti serverid, mida nad loevad.

Mis siis Windowsis on halvemini?

Näiteks võib Windowsi nakatada vaid üksnes e-kirja avamisega, Linuxis samal ajal tuleks e-kirjaga kaasapandud fail salvestada, sellele käivitusõigus anda ja seejärel käivitada („soovitavalt“ juurkasutaja õigustes). On selge, et ükski kasutaja nii Linuxis tegema ei hakka ja seetõttu ka pahavara e-postiga Linuxis nii hästi ei levi.

Tõsi on ka fakt, et kui näiteks Windowsis tavakasutaja õigustes olla, siis ikkagi saab ka väljaspoole kodukataloogi kirjutada ja süsteemi rikkuda. Näiteks alati ei kontrollita, kes kirjutab Windowsi registrisse. Lisalugemist Windowsi registri osas leiab aadressilt http://msdn.microsoft.com/en-us/magazine/cc982153.aspx ja selle redigeerimisest - http://www.wikihow.com/Edit-the-Windows-Registry. Windowsi üks nõrku kohti ongi tema register. Kui selle turvalisust suudetakse muuta, siis on võimalik ka Windowsit ennast tunduvalt turvalisemaks muuta. Samas on teada ka

asjaolu, et Windowsis on nuhkimisprogrammid, mille abil kõlavate nimedega USA turvaorganisatsioonid inimestel silma peal hoiavad. Sellest on ka Arvutimaailma veergudel kirjutatud 2002. a.

Ubuntu nihkub Windowsi suunas

Tuleb öelda, et praegune Linuxite lipulaev Ubuntu on juba üks samm Windowsi suunas. Mis seal salata - kasutan isegi seda, kuna see on veel piiri peal ja samas saab selle sammu Windowsi suunas tagasi võtta. Nimelt on tavakasutajal õigus käivitada administraatori õiguses programme, kuid küsitakse veel salasõna. Samasugune lahendus on ka Mac OS-il. Tavakasutaja saab aga admin grupist välja võtta ja siis see õigus tal kaob.

Seetõttu ei ole siin tegelikult probleemi, kuna ühtegi administraatori õiguseid nõudvat tegevust siiski ilma salasõna sisestamata ära ei tehta. Samas on Ubuntu Linuxis näiteks juurkasutaja (root) lukus ja administraatori õigused on antud sellele kasutajale, kes paigalduse käigus loodi, kuid selle sisselogimiseks kasutatavat nime ei tea teised.

Windowsi suurim viga on, et ta ei küsi salasõna, kui tehakse mingit administraatori õigusi nõudvat tegevust - tuleb vaid kinnitust küsiv dialoogiaken, mida tavakasutaja ei loe ja klõpsitakse kiirelt "yes" või "ok" nuppu (see on UAC - User Account Control, mida Microsoft luges uueks tasemeks Windowsi turvalisuses). Kahjuks aga inimesed on endiselt hooletud ja klõpsivad huupi. Kuid ka Windowsis saab kasutaja administraatorite grupist välja võtta, aga paraku ei muuda see süsteemi eriti turvalisemaks, kuna ka tavakasutajana saab palju pahandust teha. Mõnevõrra parandab seda Group Policy kasutamine.

Pahalased kõrvaldatakse ruttu

Kuna Linuxi maailm areneb kiirelt, siis ka avastatud vead parandatakse kiirelt. Seetõttu kehtib taas lause - turvalisus ei ole seisund, vaid protsess, mille eest peab pidevalt hea seisma sõltumata operatsioonisüsteemist. Lihtsalt Linuxis on seda lihtsam teha tänu mugavale tarkvarahaldussüsteemile, mida nimetatakse veel pakihaldussüsteemiks (programmid kui tarkvarapakid, mõned nimetavad ka - paketid). Siin saab samuti lubada automaatse kriitiliste uuenduste paigalduse.

Mul on isiklik kogemus, kui andsin teada ühele programmipakkide pakendajale ühest veast ja 2 tunni pärast tuli teade, et nüüd on parandatud ja võin uue versiooni täiesti tasuta alla laadida.

Linuxit peetakse sageli kui sotsiaalabiks ja hädavahendiks, mida see tegelikult ei ole. Kui näiteks jõukas Chicago linnavalitsus Linuxile üle läks, siis ei olnud põhjuseks mitte raha, vaid oluliselt proosalisemad argumendid: töökindlus ja stabiilsus.

Rumaluse vastu ei aita miski

Kuid inimliku rumaluse vastu ei aita ka kõige turvalisemad operatsioonisüsteemid. Linuxis kehtivad üldiselt samad tõed, mis mujalgi: tulemüüri kasutamine, ülearused teenused kinni ja mittevajalikud programmid maha, olemasolevad turvata, üle võrgu sisselogimine lubada vaid tavakasutaja õiguses olevale kasutajale (sudo või su abil võetakse hiljem peale sisselogimist alles juurkasutaja õigused), salasõnade regulaarne vahetamine ning tugevate salasõnade kasutamine, peale teatud arvu üritamisi lukustada kasutajakonto või ka blokeerida IP-aadressid, kui üle võrgu üritati siseneda, regulaarne tarkvarauuendus jne.

Väike paranoia on kasulik mistahes operatsioonisüsteemis.

EDMUND LAUGASSON
Zeroconf OÜ tegevjuht

- Lahendused

- Tarkvara
- Turvalisus