



Tietoturva SenioriPC-palvelussa

SenioriPC-tietokone perustuu Linux-käyttöjärjestelmään, jolle ei ole ainakaan toistaiseksi saatu aikaan vaarallisia haittaohjelmia. Windows-käyttöjärjestelmään näitä on olemassa jo yli 100 000 kappaletta, kun taas Linuxille niitä on muutama, ja nekin ovat ”harmittomia”.

Hyvin olennaista tietoturvan kannalta on pitää tietokoneiden ohjelmistot ajan tasalla, sillä tietoturvaa uhkaavia ohjelmistovirheitä löydetään kaiken aikaa. Henkilöstömme päivittää SenioriPC-tietokoneiden ohjelmistoja jatkuvasti, ja päivitykset asentuvat koneisiimme automaattisesti. SenioriPC:ssä on lisäksi otettu käyttöön tietoturvaa parantavia ratkaisuja, kuten vahvan salauksen sertifikaattiprosessit ja langattoman lähiverkon käyttämä suojattu aliverkko. SenioriPC-tietokoneeseen ei tarvitse hankkia erillistä virustorjuntaohjelmistoa.

Suomessa tietoturvasta tiedottavat useat alan yritykset, sekä Viestintävirastossa toimiva kansallinen tietoturvaviranomainen [CERT-FI](#).

Linux

Käyttöjärjestelmä on ohjausohjelma-kokonaisuus, joka toimii tulkkina käyttäjän ja tietokoneen välillä. 90-luvulla Suomalainen [Linus Torvalds](#) halusi luotettavan ja suorituskykyisen käyttöjärjestelmän. Koska sopivaa ei ollut tarjolla, alkoi hän kehittää omaa pääteohjelmaansa, josta myöhemmin kehittyikin Linux-käyttöjärjestelmän ydin.

Linuxin-käyttöjärjestelmä on suosittu erityisesti ammattilaiskäytössä korkean tietoturvan takia. Linux-ydintä käyttääkin suurin osa Internetin palvelun tarjoajista ja korkeinta turvallisuustasoa hakevat organisaatiot, kuten Suomen- sekä Yhdysvaltojen puolustusvoimat.

Virukset (Copyright Linux.fi sivusto)

Virus on vanhin PC-koneita vaivannut haittaohjelma, minkä takia sanaa käytetään usein tarkoittamaan kaikenlaisia haittaohjelmia. Oikeat virukset alkavat olla harvinaisia.

Oikea virus liittää itsensä tietokoneohjelman koodiin, eikä pysty leviämään kuin ohjelman mukana. Kun ohjelma ajetaan, viruskoodi kopioi itsensä muihin löytämiinsä ohjelmätiedostoihin, minkä ohella se saattaa tehdä muutakin, usein jotakin kohtuullisen harmitonta.

Linuxissa ”normaalikäyttäjillä” ei ole oikeuksia muuttaa järjestelmän ohjelmätiedostoja, joten ”normaalikäyttäjän” ajaman viruksen mahdollisuudet levitä ovat hyvin rajatut. Linux-virukset ovat erittäin harvinaisia, eikä tavallisen käyttäjän ole syytä vaivata niillä päätään.

SenioriPC pohjautuu Linux-käyttöjärjestelmään.

Verkkourkinta (Copyright: Wikipedia)

Verkkourkinta eli tietojenkalastelu on tietotekniikassa rikollista toimintaa, jolla pyritään saamaan haltuun luottamuksellisia tietoja, kuten henkilö- tai tilitietoja, esiintymällä tiedon saantiin oikeutettuna tahona. Haluttua tietoa ovat erityisesti salasana- tai luottokorttitiedot, joita käyttämällä hyökkääjä voi päästä huomattaviin taloudellisiin voittoihin; jo muutama lankaan mennyt uhri voi tehdä kalastelusta kannattavaa. Urkinta tapahtuu yleensä pikaviestin- tai sähköpostiviestin muodossa. Huijausviesti pyrkii näyttämään mahdollisimman aidolta ja luotettavan tahon lähettämältä.

Yksittäinen ihminen voi puolustautua tietokalastelua vastaan olemalla välittämättä epäilyttävistä sähköpostiviesteistä.

Vakoiluohjelmat (Copyright: Linux.fi sivusto ja Wikipedia)

Vakoiluohjelma eli spyware on ohjelma, joka kerää tietoja ohjelmaa suorittavasta tietokoneesta, ja tietokoneen käyttäjästä ilman käyttäjän suostumusta, ja välittää ne toiselle taholle. Tiedot voivat olla esimerkiksi käyttäjän selailemia Internet-osoitteita, sähköposti-osoitteita tai luottokorttitietoja. Tyypillisesti vakoiluohjelma asentuu tietokoneeseen jonkin ilmaisohjelman ohessa käyttäjän tietämättä. Tällainen ilmaisohjelma on tavallisesti myös mainosohjelma.

Myös maksulliset ohjelmat saattavat nykyään sisältää "vakoiluosan", jolla pyritään estämään ohjelman käyttöehtojen vastainen käyttö. Tästä "vakoilusta" yleensä kerrotaan käyttöehdoissa, mutta moni kuitenkin kokee tiedonkeruun arveluttavana.

Troijan hevoset (Copyright: Linux.fi sivusto ja Wikipedia)

Troijan hevonen on nykyään tärkein haittaohjelman muoto. Haittaohjelma on naamioitu muotoon, joka houkuttelee käyttäjän itse asentamaan, tai ajamaan sen. Tavallisesti ne tekee jonkin yksinkertaisen hyödyllisen toiminnon, mutta samalla käynnistää viruksen, madon, tekee tuhoja tai perinteisimmillään avaa takaportin tai muun haavoittuvuuden tietojärjestelmään. Se voi myös tehdä tiedonhakua, tietojen tuhoamista tai vastaavaa, jättämättä mitään jälkiä.

Jos käyttöjärjestelmä ja sen ohjelmat on säädetty niin, että ohjelmia ei pääse ajamaan vahingossa, troijan hevosten välttämiseksi riittää olla ajamatta muualta kuin luotetuista lähteistä saatuja ohjelmia. Ohjelmat kannattaa itse hankkia suoraan tekijältä tai tietoturvaa ymmärtävän välikäden kautta, ei satunnaisen www-sivun linkistä tai kaverin lähettämästä sähköpostista.

Troijan hevoset eivät ole Linuxissa varsinainen ongelma. Linuxissa ajettaviksi suunnitellut troijan hevoset ovat erittäin harvinaisia, eivätkä esimerkiksi sähköpostin tai satunnaisen web-sivun kautta saadut haitta-ohjelmat juuri koskaan toimi. Lisäturvaa tuo se, että Linux-ohjelmalla on aina oltava suoritusoikeudet, ennen kuin ne voidaan ajaa. SenioriPC pohjautuu Linux-käyttöjärjestelmään.

Takaovet (Copyright: Linux.fi sivusto ja Wikipedia)

Takaovi mahdollistaa ulkopuolisen henkilön luvattoman pääsyn tietokoneeseen tietoverkon välityksellä, ohittaen näin käyttäjän todennuksen.

Takaovi muodostetaan asentamalla käyttäjän tietämättä muun ohjelman mukana tai tietoturva-aukon kautta palvelin (esimerkiksi troijalainen), joka kuuntelee ennalta sovittua porttia. Kun krakkeri skannaa verkkoja ja havaitsee, että jossain koneessa sovittua porttia kuuntelee sovellus, hän yrittää ottaa koneeseen yhteyden soveltuvalla asiakasohjelmalla. Jos osoittautuu, että sovellus oli troijalainen, krakkeri muodostaa yhteyden palvelimeen ja näin pystyy hallitsemaan konetta riippuen troijalaisen ominaisuuksista. Useat madot sisältävät takaoven.

Takaovi-haittaohjelman tarkoitus voi olla pelkästään levitä mahdollisimman tehokkaasti, mutta usein tekijä haluaa myöhemmin käyttää koneita, joille haittaohjelma on päässyt ns. "bottiverkkona".

Makrovirukset (Copyright: Linux.fi sivusto ja Wikipedia)

Makrovirus on tietokonevirus, joka on kirjoitettu makro-kielellä. Jotkin tietokoneohjelmat, erityisesti Microsoft Windows Office-paketin ohjelmat sallivat makrovirusten lisäämisen tiedostoihin, jotta tiettyjä toimintoja voitaisiin suorittaa automaattisesti ohjelman käytön yhteydessä. Tämä mahdollistaa erityisen väylän virusten leviämiseksi. Juuri tästä syystä on vaarallista avata odottamattomia liitetiedostoja sähköpostia käytettäessä.

SenioriPC:ssä käytetään OpenOffice toimisto-ohjelmia, jotka tukevat tai tulee tukemaan Microsoft Windows Office-paketille kirjoitettuja makroja, joten Windowsille kirjoitetut makrovirukset saattavat toimia Linuxissakin. Vaikka toimisto-ohjelmien makrokieltä hyödyntäviä haittaohjelmia ei juurikaan ole nähty Linuxissa, ensimmäinen toimiva sellainen voi levitä hyvin tehokkaasti, jos makroja on totuttu käyttämään varomattomasti. SenioriPC pohjautuu Linux-käyttöjärjestelmään. SenioriPC:ssä käytetään OpenOffice toimisto-ohjelmia.



Madot (Copyright: Linux.fi sivusto ja Wikipedia)

Mato on samantapainen haitallinen tietokoneohjelma kuin virus. Mato on suunniteltu leviämään tietokoneesta toiseen automaattisesti. Mato käyttää tietokoneiden verkkoon näkyvien osien haavoittuvuuksia ja pystyy siten leviämään koneiden käyttäjien tekemättä mitään. Leviäminen edellyttää ohjelmointivirhettä käyttöjärjestelmän matalan tason verkkopakettien käsittelyssä, tai virhettä verkkoa kuuntelevassa palvelussa.

Ei ole havaittu, että modernit madot olisivat levinneet maailmanlaajuisesti muissa kuin Microsoft Windows käyttöjärjestelmissä.

SenioriPC pohjautuu Linux-käyttöjärjestelmään.