Kotikone tietoturvalliseksi

Samuli Komokallio
Tietotekniikkaosasto

Kotikoneen tietoturvasta on syytä varmistua suorittamalla asianmukaiset päivitykset. Myös koneen käyttötottumuksia kannattaa tutkiskella.

Syksyn tullen atk-asemilla ja kotikoneilla tehdään taas opiskelutöitä. Atk-asemien ylläpidosta ei opiskelijan tarvitse huolehtia, mutta kotona pölyttyvä kannettava saattaa helposti jäädä kesän aikana huonolle huolenpidolle. Varmistamalla, että kotikone on toimiva ja turvallinen käyttää, voidaan ongelmilta välttyä jo etukäteen. Teknisten suojausten tarkastamisen aikana on myös hyvä punnita omia työskentelytapoja. Muistamalla muutaman perusasian välttyy monilta ikäviltä yllätyksiltä syksyn kiireissä.

Päivitä järjestelmä ja ohjelmat

Keskeinen asia tietokoneen turvaamisessa on sen päivittäminen. Pääsääntöisesti virukset käyttävät hyväkseen ohjelmistovirheitä. Näiden aukkojen tukkimiseksi ohjelmistovalmistajat toimittavat korjauksia eli päivityksiä. Tietokone kannattaa asettaa lataamaan ja asentamaan käyttöjärjestelmän päivitykset automaattisesti. Tärkeää on muistaa päivittää myös ohjelmat, joita koneella käytetään. WWW-selaimeen tai taulukkolaskentaohjelmaan on yhtälailla syytä olla asennettuna viimeisimmät turvapäivitykset. Osa ohjelmista ilmoittaa automaattisesti uusia versioita löytäessään, mutta parasta on varmistaa asia kunkin ohjelman osalta erikseen.

<kuva 1>

Windows Security Center -ikkunasta löytyy keskitetysti tieto käyttöjärjestelmän automaattisesta päivittymisestä, virustorjunnasta ja palomuurin tilasta. Ikkunaan pääsee avaamalla käynnistysvalikosta ohjauspaneelin (Control Panel).

</kuva>

<kuva 2>

Mozilla Firefox -selaimen uusimmat versiot osaavat ilmoittaa päivityksistä. Valikon kautta voi päivitystarpeen tarkastaa myös erikseen.

</kuva>

<kuva 3>

Microsoft Office päivitetään osoitteesta http://officeupdate.microsoft.com.

</kuva>

Virukset ja vakoilijat kuriin

Virustorjunta- ja palomuuriohjelma on oltava jokaisessa Windows-tietokoneessa. Ilman palomuuria Internetiin kytketty työasema saastuu muutamissa minuuteissa. Yliopiston opiskelijat ja työntekijät voivat hakea kotikoneelleen ohjelmistojakelusta ilmaiseksi F-Securen virustorjuntaohjelmiston. Ohjelma sisältää myös palomuurin. Mikäli virustorjuntaohjelman asentamisesta on kulunut aikaa, kannattaa käydä tarkastamassa, onko siitä ilmestynyt uudempia versioita. Uudemmassa versiossa on todennäköisesti mukana uusia ominaisuuksia tai se sisältää vähintään kehittyneemmät virustunnistusominaisuudet. Kun torjuntaohjelma ja siihen uusimmat viruskuvaukset on päivitetty, kannattaa tietokoneessa suorittaa virus- ja vakoiluohjelmien tarkastus. Vaikka torjuntaohjelma ei

uusista tartunnoista olisikaan ilmoittanut, saattaa kiintolevyllä majailla sinne aikanaan tallentuneita saastuneita tiedostoja ja vakoiluohjelmia.

<kuva 4>

F-Secure voidaan määrittää tarkastamaan haitta- ja vakoiluohjelmat koko tietokoneesta napsauttamalla ohjelman logoa hiiren oikealla painikkeella.

</kuva>

Selaimen käyttöön järkeä

WWW-selain on yksi tärkeimpiä kotikoneen ohjelmia. Se on myös ehkä koneen haavoittuvin osa. Siksi päivitykset ja asetukset on syytä olla kunnossa kaiken aikaa. Selain tallentaa oletuksena valtavan määrän tietoa Internetin käytöstä ja käyttäjän syöttämistä tiedoista. Asetuksien avulla tiedon määrää kannattaa karsia, sillä myös haittaohjelmat etsivät tietoja. Kannattaa vähintään asettaa pois käytöstä tunnusten tai salasanojen tallentaminen. Joissakin selaimista on mahdollisuus helposti tyhjentää kaikki selaamisesta tallennetut jäljet. Poisto kannattaa ottaa tavaksi myös kotikoneella. Vierailla tietokoneilla toimenpide on välttämätön selailun jälkeen. Aiemmasta käyttäjästä ja hänen toimistaan koneella ei koskaan voi mennä takuuseen. WWW-selailun teknisiä suojauksia olennaisempaa ovat kuitenkin käyttäjän omat toimet. Maltti ja maalaisjärki ovat parhaita turvavälineitä. Jos sivusto haluaa asentaa selaimeen lisukkeita tai suorittaa ohjelmia koneellasi, harkinta on aina paikallaan. Älä suostu kaikkeen, mitä verkosta sinulle tarjotaan.

<kuva 5>

Selailun paikalliset jäljet voi helposti tyhjentää Mozilla Firefox -selaimessa valikon kautta tai Ctrl+Shift+Del-näppäinyhdistelmällä.

</kuva>

Oikeudet ja salasanat kuntoon

Kotikoneen päivittämisen ja asetusten tarkistelun lomassa on hyvä huomioida myös laitteen käyttäjäoikeudet. Tietokonetta tulee käyttää peruskäyttäjän oikeuksilla. Vain asentaminen ja muu ylläpito tehdään ylläpitotunnuksin, näin vaikeutetaan haittaohjelmien leviämistä. Tarttuessaan useat haittaohjelmat perivät sen käyttäjäoikeuden, millä konetta parhaillaan käytetään. Jos koneessa ollaan ylläpitäjänä, myös haittaohjelmalla on asentumiseen hyvät edellytykset. Kotikoneeseen tulisi siis luoda erityinen ylläpitäjän tunnus ja peruskäytössä oleva käyttäjätunnus alentaa tavalliseksi käyttäjäksi. Ohjelmien asentamista tai muuta ylläpitoa varten ei tietokoneesta tarvitse kirjautua ulos, useimmat toiminnot voidaan suorittaa napsauttamalla ohjelman kuvaketta hiiren oikealla painikkeella ja valitsemalla avautuvasta valikosta suorittajaksi ylläpitäjätunnuksen.

<kuva 6>

Useimmat ylläpitotyöt, kuten ohjelmien asentaminen onnistuu myös tavallisena käyttäjänä Run as… (Suorita…) -toiminnon avulla napsautettaessa suoritettavaa ohjelmaa hiiren oikealla painikkeella.

</kuva>

Kotikoneissa saattaa olla myös tilanne, ettei salasanaa ole asetettu käyttöön. Tämä luonnollisesti kannattaa asettaa ja viimeistään tässä vaiheessa voidaan samalla vaihtaa muiden käytettyjen järjestelmien salasanat niin erilaisten verkkopalveluiden kuin yliopiston järjestelmienkin osalta.

Samojen salasanojen käyttämistä näissä on vältettävä ehdottomasti. Jos jonkin nettifoorumin salasana vuotaa muille vaikkapa kirjaston koneen tallentaessa sen automaattisesti, on huomattavasti

pienempi huoli esimerkiksi Weboodin tai sähköpostin salasanojen joutumisesta samalla vieraisiin käsiin. On myös olemassa paljon asialliseltakin näyttäviä WWW-sivustoja, jotka on luotu ainoastaan tunnusten ja salasanojen varastamista varten. Yliopiston käyttösääntöjen mukaan tunnuksen haltija on vastuussa kaikesta tunnuksilla tehtävistä toimista, niistä siis todella kannattaa pitää huoli.

Roskaposti suodatukseen

Mikäli hermot eivät vielä ole menneet roskapostien vuoksi, on hyvin todennäköistä että syksyn kiireisinä hetkinä näin tapahtuu. Suojautuminen siis kannattaa aloittaa etukäteen. Yliopiston sähköpostijärjestelmissä on mahdollisuus käyttää keskitettyä roskapostin tunnistusta ja suodatusta. Tunnistus toimii tietotekniikkaosaston palvelimella, joten se ei ole riippuvainen postinlukuohjelmasta. Suodatus täytyy kuitenkin jokaisen itse aktivoida. Lisäksi kannattaa harkita suodatukseen pystyvän postiohjelman käyttöä kotikoneella. Esimerkiksi Microsoft Outlook ja Mozilla Thunderbird -ohjelmissa on suodatusominaisuudet. Kaiken kaikkiaan roskapostista pääsee huomattavasti vähemmällä, jos jakaa sähköpostiosoitettaan harkitusti eikä avaa, saati vastaa roskaviesteihin. Erilaisissa verkkorekisteröitymisissä on suositeltavaa käyttää jotain niitä varten tehtyä osoitetta. Ilmaisia sähköpostiosoitteita tarjoavia palveluita löytyy helposti.

<box>

Ohjeet keskitetyn roskapostitunnistuksen käyttöönottoon löytyy osoitteesta *http://www.helsinki.fi/atk/posti/spamtunnistus.html*

</box>

Muita toimenpiteitä

Langattomassa verkossa on yksinkertaista seurata viereisen surffailijan liikennöintiä ja salaamatonta sähköpostinvaihtoa. Käytettäessä kotikannettavaa yliopistolla, kannattaakin siihen asentaa tietoliikenteen salaamiseen tarkoitettu OpenVPN-asiakasohjelma. Ohjelma on haettavissa ohjelmistojakelusta ja sen avulla myös HUPnet-verkkoon tarvitsee kirjautua vain kerran, ei kahden tunnin välein kuten normaalisti. Ohjelma salaa tietoliikenteen kotikoneen ja yliopiston verkon välillä.

Tekijänoikeusasiat on hyvä pitää mielessä saatettaessa tietokonetta toimintakuntoiseksi. Tekijänoikeuksin suojattujen musiikkikappaleiden, videoiden tai ohjelmistojen luvaton lataaminen on laitonta. Luvattomasti ladatut ohjelmat usein sisältävät myös kylkiäisinä takaportteja, joiden kautta murtautujan on mahdollista saada kotikone haltuunsa. Myös ohjelmistopäivitysten saaminen laittomiin versioihin voi olla hankalaa tai mahdotonta. On muistettava, että useimmissa vertaisverkko-ohjelmissa on haavoittuvuuksia, lisäksi osassa on itsessään vakoiluominaisuuksia. Opiskelijan kukkarolle löytyy järkevämpiäkin vaihtoehtoja saada ohjelmia. Tietotekniikkaosaston atk-neuvonnasta annetaan mielellään lisätietoja mahdollisista halvoista kampuslisenssiohjelmista sekä ilmaisohjelmistoista, jotka ovat monasti täysin yhteensopivia ja ominaisuuksiltaan verrattavissa kaupallisiin.

Viimeinen, muttei vähäisin asia, on saattaa varmistukset kuntoon. Tallentamalla opiskelutyöt, valokuvat ja muut tärkeät tiedostot säännöllisin väliajoin esimerkiksi ulkoiselle kiintolevylle tai CD-ROM-levylle vältytään ikäviltä yllätyksiltä, jos tietokone lakkaa toimimasta tai muuta yllättävää tapahtuu. Varmistamisesta kannattaa luoda tapa, esimerkiksi kopioimalla kotikoneen tärkeiden tiedostojen kansio joka perjantai ulkoiselle levylle. Tärkeää on testata myös etukäteen, että tietojen palauttaminen onnistuu tarpeen tullen!