LAUREA AMMATTIKORKEAKOULU Uuden edellä

Tietoturvaopas Laurea-ammattikorkeakoulun kouluisännille

Mattsson, Thomas

Mäenpää, Minttu

2011 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Tietoturvaopas Laurea-ammattikorkeakoulun kouluisännille

Thomas Mattsson, Minttu Mäenpää
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kesäkuu, 2011

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Thomas Mattsson, Minttu Mäenpää

Tietoturvaopas Laurea-ammattikorkeakoulun kouluisännille

Vuosi 2011 Sivumäärä 45

Tämä opinnäytetyö käsittelee tietoturvaa yleisellä tasolla ja Laurea-ammattikorkeakoulun näkökulmasta. Opinnäytetyö on tehty Laurea-ammattikorkeakoulun kouluisännille. Laurea-ammattikorkeakoulun kouluisännillä ei ole ennen vastaavaa opasta ollut. Tietoturvaoppaan tarpeellisuudesta keskusteltiin kouluisäntien kanssa loppukesästä 2010, jonka jälkeen työskentely aloitettiin.

Oppaassa käydään läpi eri tietoturvallisuuden lajit, virukset, haittaohjelmat, sähköpostiturvallisuus ja sosiaalinen media. Oppaassa annetaan myös kuva siitä, miten mahdolliset uhat voidaan havainnoida ja tarvittaessa poistaa. Liian yksityiskohtaisiin ohjeisiin ei ole panostettu, sillä tietoturvan hoitaminen Laureassa ei ole kouluisäntien varsinainen työnkuva.

Tavoitteena oli luoda opas, josta kouluisännät saavat halutessaan yleiskuvan tietoturvasta ja siitä, miten tietoturvaan liittyvät asiat ovat Laureassa hoidettu tai ohjeistettu. Koska tietoturva kehittyy hurjaa vauhtia, on oppaassa kerrottu myös tietoturvan historiasta ja tulevaisuuden näkymistä.

Tiedonhankintamenetelminä käytettiin pääasiassa alan kirjallisuutta, oman koulun tietoturvaohjeita sekä verkosta löytyviä tietoturvajulkaisuja. Työstämme syntyi kouluisännille opas, jota he voivat käyttää tietoturvaan liittyvien asioiden opiskeluun ja kertaamiseen.

Asiasanat: tietoturva, palomuuri, virustorjunta, suojautumiskäytännöt, salasanat, sähköposti, sosiaaliset mediat

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Programme in Business Information Technology

Thomas Mattsson, Minttu Mäenpää

Data security guide for Laurea University of Applied Sciences facility caretakers

Year 2011 Pages 45

This thesis examines information security in general and from the perspective of Laurea University of Applied Sciences (UAS). The thesis has been completed for Laurea UAS facility caretakers, who have never had a similar guide. There was discussion about the necessity of a security guide with the caretakers in the late summer of 2010, after which work on the project began.

The guide describes the different types of information security areas, viruses, malware, email security and social media. The handbook also provides a picture of how potential threats can be detected and removed if necessary. Too detailed guidance is not included, as information security management at Laurea is not the caretakers' actual job description.

The purpose was to create a guide in which caretakers can receive an overview of information security and how security issues are handled at Laurea. Since information security is developing at a rapid pace, the guide also describes the history and future of information security.

Information security literature, Laurea's own guides and publications across the web were mainly used when gathering the information. The research resulted in a guide for Laurea's facility caretakers, which they can use to study and enhance their knowledge about information security.

Keywords: security, firewall, antivirus, protective practices, passwords, email, social media

SISÄLLYS

1 JOHDANTO

Tämä opas sisältää ohjeita ja informaatiota tietoturvasta Laurea-ammattikorkeakoulun kouluisännille. Ohjeet ja muu tieto on jaettu lukuihin niin, että ensiksi käsittelemme tietoturvauhkien havainnointia ja uhkia yleismaailmallisesta näkökulmasta. Yleisten termien ja ohjeistojen jälkeen siirrytään käsittelemään Laurean omia käytäntöjä ja sääntöjä aihetta koskien.

Olemme pyrkineet mahdollisimman selkeään ja helppokäyttöiseen oppaaseen, josta on hyötyä myös siinä tapauksessa, että teoksen käyttäjällä ei itsellään ole valmiiksi tietopohjaa aiheesta. Päätimme tehdä oppaan kun kuulimme, että Laurean kouluisäntien puoleen käännytään yhä useammin tietoturvaan liittyvissä asioissa. Kouluisäntien pyynnöstä keskitymme oppaassa erilaisiin teoreettisiin uhkiin, suojautumiskäytäntöihin, rutiinitarkistuksiin ja yleisimpiin ongelmiin sekä niistä selviytymiseen. Toivomme oppaan olevan eräänlainen tietoturvan perusohjeistus kouluisännille.

Opas ei sisällä ainoastaan ohjeita opiskelijoiden, vaan myös työntekijöiden ja koko kouluorganisaation tietoturvaongelmiin. Koska tietoturvaan liittyvät haasteet ja uhkat muuttuvat jatkuvasti, yritämme pureutua ongelmiin laaja-alaisesti. Esimerkkinä emme näytä, miten jokin tietty virus havaitaan tai poistetaan, vaan näytämme miten virukset havaitaan ja poistetaan nyt ja luultavasti ainakin lähitulevaisuudessa. Tällä pyritään siihen, että opas ei olisi aikansa elänyt jo vuoden päästä julkaisemisesta.

Koska tietoturva on käsitteenä erittäin laaja, yritämme pysyä oppaan tekstissä niissä aiheissa, jotka ovat Laurealle keskeisiä. Työssämme on konstruktiivinen tutkimusote, joka tarkoittaa käytännön ongelman ratkaisua luomalla uusi konstruktio. Meidän tapauksessa konstruktio on tämä tietoturvaopas ja ratkaistavana ongelmana toimi kouluisäntien lisääntynyt tarve tietoturvaosaamiseen.

2 TIETOTURVAN PERUSTEITA

Tietoturva on erittäin laaja käsite, joka voidaan jakaa kahdeksaan eri pääryhmään: tietoaineiston turvallisuuteen, ohjelmisto-, tietoliikenneturvallisuuteen, fyysiseen turvallisuuteen, laitteisto-, henkilö-, käyttöturvallisuuteen ja hallinnolliseen turvallisuuteen. (Ruohonen 2002, 2-7.)

Jotta tietoturva olisi toimivaa, tulisi tietokoneiden ja niissä olevien ohjelmien tehdä aina vain se, mitä pitääkin, eikä muuta. Tämä on toisin sanoen tietoturvan tavoite, joka on jaettu viiteen eri osioon:

- luottamuksellisuus
- autenttisuus, oikeellisuus
- kiistämättömyys
- eheys
- käytettävyys.

Autenttisuudella pyritään varmistamaan, että kaikki osat tietojärjestelmästä voidaan tunnistaa luotettavasti. Esimerkkinä voisi mainita Suomessa yleisesti käytettävät pankkitunnukset. Jos käyttäjä tai jokin muu taho pystyy kirjautumaan esimerkiksi pankkijärjestelmään, menetetään järjestelmän autenttisuus. Käyttäjän tunnistamisessa voidaan käyttää pankkilukujen sijasta esimerkiksi salasanaa, älykorttia tai biometristä tunnistusta. (Ruohonen 2002, 2-7.)

Luottamuksellisuuden tarkoitus on pystyä pitämään tiedot ja tiedostot vai niiden ihmisten tai tahojen käytettävissä, joille ne on määritetty kuuluvaksi. (Ruohonen 2002, 2-7.)

Kiistämättömyydellä tavoitellaan sitä, että kaikki tietojärjestelmässä tapahtuvat muutokset tai tapahtumat jättäisi jäljen esimerkiksi lokiin. Hyvänä esimerkkinä voisi mainita internetissä toimivan elektroniikkakaupan, josta käyttäjän onnistuu tilata tuote ja myöhemmin kiistää tilanneensa sitä. Kyseisessä tapauksessa olisi verkkokaupan kiistämättömyys mennyttä. (Ruohonen 2002, 2-7.)

Eheyden tavoitteena on pitää tietojärjestelmä sellaisessa tilassa, että tiedot tai tiedostot eivät pääse muuttumaan vahingossa tai tahallaan ilman, että oikeutettu käyttäjä tekee muutoksen. (Ruohonen 2002, 2-7.)

Käytettävyydellä pyritään pitämään tietojärjestelmä käyttäjien käytettävissä aina kun on tarkoituskin. Tämä on käyttäjän kannalta näkyvin tietoturvan palveluista. (Ruohonen 2002, 2-7.)

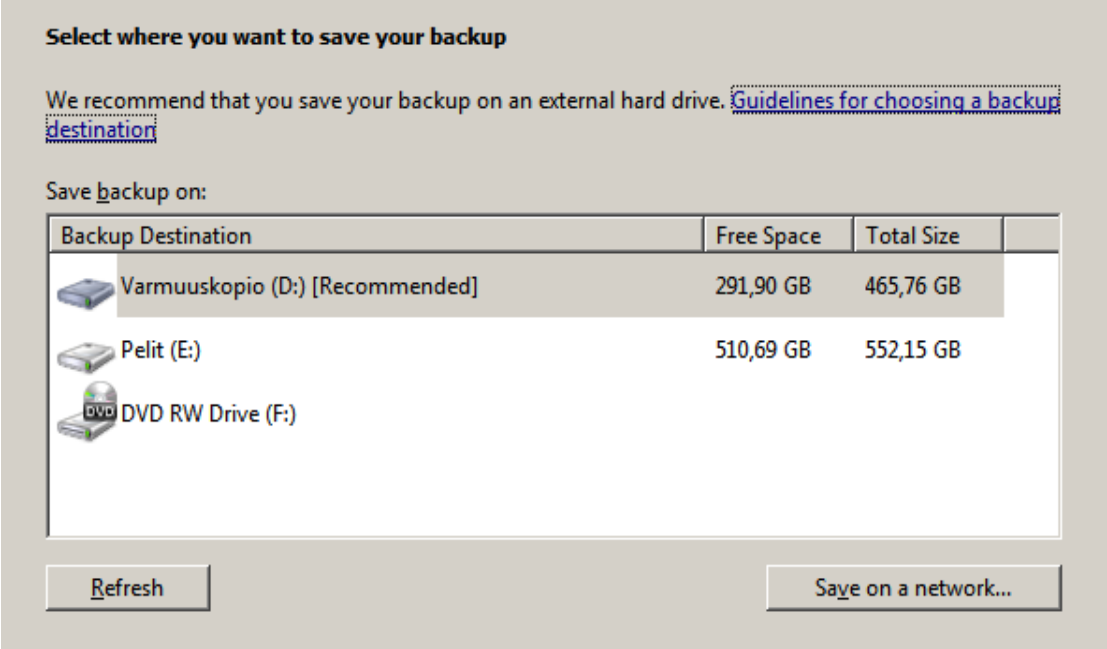
2.1 Tietoaineiston turvallisuus

Tärkein osa-alue tietoaineiston turvallisuudessa on tietojen suojaaminen. Myös käyttöoikeuksien määrittäminen, tiedostojen varmuuskopiointi ja palautus sekä tiedostojen turvallinen säilytys ja tuhoaminen ovat tärkeitä sektoreita. (Tietoaineiston-turvallisuus.)

Kun halutaan suojata tiedostoja, kannattaa aloittaa luokittelemalla informaatio esimerkiksi erittäin salaisiin tietoihin ja julkisiin tietoihin. Erittäin salaisia tietoja voivat olla ihmisten henkilötiedot tai yrityksen suunnitelmat tulevista projekteista. Julkista tietoa taas ovat esimerkiksi kaikille luettavissa olevat julkaistut artikkelit. On jokaisen organisaation itse päätettävissä, miten tiedot luokitellaan. Lainsäädännölliset asiat on syytä muistaa ja tarkistaa esimerkiksi henkilötietoja käsiteltäessä. (Tietoaineiston-turvallisuus.)

Kun osa-alueet on tarkasti jaoteltu, on helpompi ymmärtää ja käsitellä tietoaineistoja. Laureassa kaikki julkinen informaatio on hyvä olla esillä internet-sivuilla. Sieltä jokainen pääsee selaamaan haluamiaan tietoja. Salatuille alueille kirjaudutaan omilla opiskelijatunnuksilla. Opiskelijoita ja työntekijöitä on syytä ohjeistaa turvalliseen tietoaineistojen käyttämiseen. Materiaalien turvallinen säilytys ja varmuuskopioiminen ovat kaikille tärkeitä asioita opetella. Sillä tarkoitetaan, että käyttäjä ottaa kopiot työstään siltä varalta, että alkuperäinen kopio tuhoutuu esimerkiksi kovalevyn tuhoutuessa. Tiedostoja voi joku tahallisesti muuttaa tai ne voivat joutua tietomurron uhriksi ja tuhoutua. Kun on huolehdittu varmuuskopioinnista, tiedot voidaan palauttaa varmuuskopioilta ja työskentelyä voidaan jatkaa siitä mihin jäätiin. (Tietoaineiston turvallisuus.)

Seuraavassa kuvassa on esimerkki Windows 7-käyttöjärstelmän omasta varmuuskopiointi-ominaisuudesta.



Kuvio 1: Windows 7 – käyttöjärjestelmässä on helppo käyttöliittymä koko järjestelmän varmuuskopioimiseksi

On tärkeää muistaa säilyttää varmuuskopioita aina täysin eri paikassa kuin alkuperäiset tiedostot, jotta ne eivät vahingon sattuessa pääse tuhoutumaan samanaikaisesti. Erittäin tärkeästä tiedosta kannattaa ottaa monia kopioita eri paikkoihin esimerkiksi ulkoisille kovalevyille ja sijoittaa niitä eri paikkoihin. Näin ne eivät tuhoutuisi kaikki, esimerkiksi tulipalon sattuessa. Optisten tallennusmuotojen käyttö olisi tällöin suositeltavinta. Tällaisia ovat esimerkiksi cd- tai dvd-levyt. Magneettiset tallennusmediat, kuten levykkeet ja ulkoiset kovalevyt tuhoutuvat, jos ne joutuvat voimakkaaseen magneettikenttään liian pitkäksi ajaksi. Olisi siis syytä aina varmuuskopioita ottaessa miettiä, kuinka oleellista ja tärkeää tieto on ja miten se varmuuskopioidaan. (Tietoaineiston-turvallisuus; Ruohonen 2002, 209–211.)

On tärkeää muistaa, että kun tiedostoa halutaan poistaa, ei riitä, että se poistetaan muistitikulta tai tietokoneen kovalevyltä. Tällöin ainoastaan muistipaikka vapautuu, mutta tietoa ei ylikirjoiteta. Tiedostojen tuhoamiseen on olemassa monenlaisia vaihtoehtoja. Ylikirjoittamiseen kehitettyjä sovelluksia voidaan käyttää ja niihin löytyy ohjeita internetistä. On myös muistettava tuhota varmuuskopiot. (Tietoaineiston-turvallisuus.)

2.2 Ohjelmistoturvallisuus

Ohjelmistoturvallisuuden kannalta on tärkeää, että valitaan käyttöön sellaisia ohjelmistoja, joista aiheutuva tietoturvauhka on vähäinen. On myös tärkeää ottaa selvää kunkin ohjelmiston kannalta olennaisista säilytys- ja varmuuskopiointitavoista. Tämä käy helpoiten silloin, kun siihen kiinnitetään huomiota heti ohjelman käyttöönoton yhteydessä eikä vasta myöhemmin. Ohjelmistot muokataan yrityksen tarpeiden mukaisesti ja tässäkin tapauksessa on syytä muistaa lain asettamat vaatimukset. Jos ohjelmiston valmistaja on ulkomainen, voi lakiasetukset olla erilaiset. Ohjelmiston oletusasetuksia joudutaan siis muokkaamaan kunkin omiin tarpeisiin. (Laaksonen, Nevasalo & Tomula 2006, 67.)

Kun pohjatyö tehdään hyvin, sillä varmistetaan ohjelmien luvallisuus ja estetään laiton kopiointi ja käyttö. Käytetyt ohjelmat suojataan asianmukaisesti sekä huolehditaan lisenssien hallinnasta ja rekisteröinnistä. Lisenssien ylläpito on tärkeää, koska sillä pidetään ohjelmisto toiminnassa siihen asti, kun lisenssin käyttöaika loppuu. Ohjelmisto ei tällöin lopeta toimintaansa noin vain. Viranomaiset saattavat myös tutkia tietojärjestelmiä laittomien ohjelmien varalta, jolloin voimassaolevalla lisenssillä voidaan osoittaa siihen olevan käyttöoikeus. Ohjelmistoturvallisuudesta vastaa organisaation tietohallinto. (Ruohonen 2002, 4.)

2.3 Tietoliikenneturvallisuus

Tietoliikenneturvallisuutta tarvitaan, kun halutaan suojata tietojärjestelmän tietoliikenteen, sekä järjestelmän sisäisen, että ulkopuolisen verkon viestit. Tämä tarkoittaa esimerkiksi sitä, että eristetään omat verkot muista verkoista ja suojataan ne palomuureilla ja Proxy-palvelimilla. Järjestelmän ulkopuolella kulkeva tietoliikenne voidaan salakirjoittaa esimerkiksi käyttämällä VPN- verkkoja. Tällöin viestintäverkkojen avulla kirjoitettavat viestit eivät välity ja paljastu asiaankuulumattomille, eivätkä ulkopuoliset pääse muuttamaan tai tuhoamaan verkoissa välitettäviä viestejä. Mitä tehokkaampaa verkkojen salaus on, sitä vaikeampaa tiedon on päästä vääriin käsiin. Ongelmaksi liian hyvin salatun tiedoston välittämisessä voi muodostua se, että tiedon vastaanottaja ei osaa purkaa viestiä, tai hänellä ei ole riittäviä ohjelmia viestin lukemiseen. (Ruohonen 2002, 4; Laaksonen, Nevasalo & Tomula 2006, 66–67.)

Laurean opiskelijoille on tarjolla SSL-VPN tekniikka, joka takaa tietoturvallisen yhteyden kouluun verkon ulkopuolelta. SSL-VPN tekniikkaa voi käyttää osoitteessa gate.laurea.fi. (ssl-vpn ohje opiskelijoille.)

Tietoliikenteen turvallisuus vaatii jatkuvia toimenpiteitä verkon ylläpitäjältä, koska tietoliikenteen jatkuvuus pitää koko ajan turvata. Tiedon pitää myös pysyä salattuna ja sen eheys taata. (Järvinen 2002, 112.)

2.4 Fyysinen turvallisuus

Fyysinen turvallisuus on kaiken perusta ja pohja koko organisaation toiminnalle. Toimitilat suojaamalla luodaan perusta muille suojaustoimille, jolloin organisaatio voi toimia häiriöttömästi ja turvallisessa toimintaympäristössä. Ilman turvallista fyysistä ympäristöä ei voida olla varmoja, että itse tieto on luotettavissa käsissä. Fyysinen turvallisuus on erittäin laaja osa-alue tietoturvassa, jolloin tietenkään kaikki organisaation tilat eivät vaadi samantasoista suojausta kuin toiset. Esimerkkinä tuotekehittelytilat, atk-laitetilat sekä hallinnolliset tilat vaativat korkeaa suojaustasoa. Nyrkkisääntönä voidaan ajatella, että suojausta vaativat kaikki ne tilat, joissa käsitellään organisaation toiminnalle merkityksellistä tietoa. Jos toimitiloja organisaatiossa on paljon, olisi viisasta asettaa tilat tärkeysluokitukseen, jolloin fyysisen turvallisuuden suunnittelu helpottuu. Tällöin pystytään kartoittamaan selkeästi, mitkä tilat tarvitsevat enemmän suojausta kuin toiset. (Laaksonen, Nevasalo & Tomula 2006, 125.)

On olemassa eräänlaisia tarkistuslistoja, joista voidaan tarkastaa, miten fyysisiä tiloja kannattaa lähteä suojaamaan. Tällaisia ovat esimerkiksi ISO 27001 -standardi, joka sisältää omat vaatimuksensa. Viestintävirasto, VAHTI-ohjeet ja Suomen puolustusvoimat antavat myös omia määrityksiään. (Laaksonen, Nevasalo & Tomula 2006, 125–126.)

Fyysinen ympäristö tulee suojata monilta uhkatekijöiltä. Tällaisia ovat esimerkiksi vesivahingot, tulipalot, pölyn aiheuttamat haitat, sähköhäiriöt ja varkaudet. Haasteensa esimerkiksi varkaustapausten ehkäisyyn asettaa kannettavien tietokoneiden yleistyminen ja niiden varastamisen helppous. Varkaudet tapahtuvat yleensä päivisin, jolloin yrityksessä on hälytysjärjestelmät pois päältä. Tämän vuoksi kulkua tiloihin, jossa esimerkiksi tietokoneita säilytetään, tulisi jotenkin valvoa. Organisaation resurssien mukaan tämä voi olla videovalvontaa tai vaikkapa sähköisen kulkuluvan vaativien ovien käyttöönottoa. Sormenjälkitunnistimet ovat esimerkki hyvin varmasta tunnistusmenetelmästä, jolloin ulkopuolisten on hyvin vaikea päästä käsiksi arvokkaisiin tietoihin tai laitteisiin. (Laaksonen, Nevasalo & Tomula 2006, 126.)

Hyvin edullinen ja yksinkertainen tapa on pitää luetteloa henkilöistä, joilla on pääsy valvottuihin tiloihin. Tällöin tiedetään varmasti, ketkä huoneissa liikkuvat. Haasteellista Laurean kannalta tässä on se, että vaikka opettajat ja muu henkilökunta ovat tiedossa ja heillä on avain luokkiin, liikkuu koulussa niin paljon opiskelijoita ja muita ihmisiä, että täydellinen valvonta on hyvin vaikeaa. Usein opiskelijat työskentelevät luokissa ilman valvontaa, jolloin varkauksien mahdollisuus kasvaa. Turvakameroiden asentaminen luokkiin voisi olla hyvä idea, jos

varkauksia sattuu paljon, eikä niitä pystytä muuten kontrolloimaan. (Laaksonen, Nevasalo & Tomula 2006, 126.)

Laitetiloja suunniteltaessa on hyvä ottaa huomioon, että tiloihin ei saisi tulipalon uhatessa päästä savua, joka voisi vahingoittaa tallennusmediaa tai tallennuslaitteita. Tilat pitäisi olla eristetty muista tiloista paloturvallisesti. Tiloihin asennettavat lämpötila-anturit hälyttävät jo ennen kriittisen lämpötilan nousua, jolloin siihen ehditään reagoimaan. Tehokkaalla ilmastoinnilla saadaan aikaan se, että ilman lämpötila pysyy oikeana. Jo suunnitteluvaiheessa on hyvä huomioida, että laitteiden määrä huoneessa voi tulevaisuudessa kasvaa, jolloin ilmastoinnin pitää olla silloinkin riittävä. Ennakoimalla siis säästää paljon aikaa ja vaivaa, kun myöhemmin ei tarvitse ryhtyä remontoimaan tiloja aina uudelleen. Erityisesti palvelinhuoneisiin täytyy tarvittaessa asentaa erillinen koneellinen jäähdytys ja kostutusjärjestelmä. Nämä hoitavat myös epäpuhtaudet pois huoneen ilmasta. (Laaksonen, Nevasalo & Tomula 2006, 127; Hakala, Vainio & Vuorinen 2006, 305.)

Vesivahinko voi sattua koska tahansa, ja siihenkin on organisaation syytä varautua. Se on tulipalon ohella yleisin fyysistä turvallisuutta uhkaava ongelma. Laitetiloja suunniteltaessa otetaan huomioon, ettei tilassa, tai sen yläpuolella saisi olla vesiputkia joista vuoto voisi aiheutua. Rakentamalla välipohja laitetilaan, voidaan sillä suojata tilaa vesivahingolta. (Laaksonen, Nevasalo & Tomula 2006, 127; Hakala, Vainio & Vuorinen 2006, 305.)

Joskus laitetiloihin asennetaan ilmankostuttimia, jotka vaativat vesijohtoverkon. Silloin on tarkkaan suunniteltava mitä kautta vesi kulkeutuu pois, jos ilmankostutin rikkoutuu. Tällaisia ratkaisuja ovat esimerkiksi tulvimiselta suojatut lattiakaivot tai vuotoaltailla varustetut ilmankostuttimet. Vesivahinkoja torjuvat ratkaisut vaativat vuosittaista huoltoa jolloin niiden toimintakunto tarkastetaan säännöllisesti. On hyvä muistaa, että vuosittaiset huollon kustannukset ovat huomattavasti pienemmät, kuin vesivahingosta koituva haitta. (Laaksonen, Nevasalo & Tomula 2006, 127; Hakala, Vainio & Vuorinen 2006, 305.)

Pölyä on kaikkialla ja koko ajan, siihen auttaa vain säännöllinen siivous ja se, että rajoitetaan laitetilojen käyttöä. Jokainen kulkija tuo mukanaan pölyä joka sitten laskeutuu laitteiden päälle. Laitetiloja ei saisi käyttää samanaikaisesti tavaroiden varastointiin ja laitteet olisi hyvä nostaa pois lattioilta, jolloin siivoaminen helpottuu ja pölyä ei kerry laitteiden päälle niin paljoa. (Laaksonen, Nevasalo & Tomula 2006, 127.)

Sähkökatkokset voivat olla yleisiä ja niihinkin on syytä varautua. Se voi pahimmillaan aiheuttaa laiterikkoja, tietojen häviämistä tai ainakin käyttökatkoksia. UPS –laitteet *(Uninterruptible Power Supply)* ja varageneraattorit varmistavat laitteiden toiminnan pidemmänkin katkon aikana. UPS- laitteet antavat organisaation palvelimille ja työasemille, sekä aktiivilaitteille

virtaa niin kauan, että varageneraattorit ehtivät käynnistyä. UPS- laitteet on jaettu kahteen kategoriaan, online- ja offline-laitteisiin. Sähköurakoitsijat suunnittelevat organisaatioiden UPS-järjestelmät, ja tekevät oikeanlaiset ratkaisut kunkin organisaation tilojen mukaisesti. Näidenkin laitteiden ja varavoimakoneiden säännöllinen testaus ja huolto ovat tärkeitä asioita. Tällöin varmistetaan, että laitteet toimivat kun niitä tarvitaan. UPS- laitteet usein sammuttavat itse itsensä jos niiden sisäinen lämpötila nousee nopeasti, mutta oikosulun sattuessa yleensä seurauksena on tulipalo. Tällaisissa tilanteissa on erittäin tärkeää, että tilassa jossa UPS- laitteita säilytetään, on myös palovaroitin, joka on kytketty paloilmoitusjärjestelmään. (Hakala, Vainio & Vuorinen 2006, 309–314 ; Laaksonen, Nevasalo & Tomula 2006, 127.)

Edellä olevassa kuvassa on esimerkkinä Belkinin yksityiskäyttöön tarkoitettu UPS-laite.

Kuvio 2: UPS-laite, joka on tarkoitettu yksityiskäyttöön

Suomessa suuria ukkoskuuroja on harvemmin, jolloin organisaatioissa usein on unohdettu suojautua salamaniskuja vastaan. Kaapelien sijoittaminen maan alle ei estä ukkosta tuhoamasta kiinteistöjen sähkö- ja puhelinjärjestelmien kaapeleita. Organisaatioissa melkein kaikki laitteet ovat usein kytkettynä samaan lähiverkkoon. Tällöin riittää, että yhteen laitteeseen tulee salamanisku, ja pahimmassa tapauksessa kaikki koneet tuhoutuvat. Rakennuksen sähköjärjestelmä tulisi siis ylijännitesuojata. (Hakala, Vainio & Vuorinen 2006, 309–314.)

Kun tietokoneet olivat vielä suurkoneita, oli yleistä, että laiteongelmia aiheuttivat hyönteiset. Tämä on aivan mahdollinen uhka vielä tänäkin päivänä. Esimerkiksi jos laitteiden säilytystila on hyvin viileä ja rakennuksessa on muurahaisia, ne todennäköisesti hakeutuvat lämpimiin ATK-laitteisiin. Tällöin ne aiheuttavat toimintahäiriöitä. Halpa ja helppo keino on laittaa tiloihin muurahaisten torjumiseen tarkoitettuja muurahaisrasioita, jotka sisältävät myrkkyä. Muurahaiset menevät rasioihin ja vievät myrkkyä pesäänsä mennessään, jolloin pesä tuhoutuu. Myrkytyssuihkeiden käyttöä ei suositella, koska se voi aiheuttaa haittaa ATK-laitteille. (Hakala, Vainio & Vuorinen 2006, 306–307.)

Harva tulee ajatelleeksi, että jyrsijät ovat kiinnostuneita rasvasta, jota käytetään notkistamaan tele- ja verkkokaapeleita. Hiiret ja rotat siis voivat aiheuttaa mittavaa tuhoa jyrsiessään johtoja poikki. Hiiret mahtuvat niin pienistä koloista, että niitä vastaan suojautuminen voi joskus olla haastavaa. Esimerkiksi ilmastoinnin metallinen suojaverkko ei hiiriä välttämättä estele. (Hakala, Vainio & Vuorinen 2006, 306–307.)

2.5 Laitteistoturvallisuus

Laitteistoturvallisuuden perustana on se, että organisaatio ottaisi käyttöönsä vain sellaisia laitteita, joista aiheutuva tietoturvauhka olisi vähäinen. Tällöin organisaation laitteet eli tietokoneet, reitittimet ja palomuurit tulisi suojata hyvin. Laitteistojen turvallisuus on suorassa kytköksessä fyysiseen turvallisuuteen, koska kun fyysiset tilat joissa laitteet sijaitsevat, on suojattu hyvin, on laitteisiin ja niissä oleviin ohjelmiin käsiksi pääsy hankalampaa. (Ruohonen 2002, 5; Laaksonen, Nevasalo & Tomula 2006, 67.)

Tietoturvan kannalta olennaisia suojattavia laitteita organisaatiossa ovat esimerkiksi kannettavat tietokoneet, tulostimet, matkapuhelimet ja palvelimet. Organisaatiossa on syytä tehdä kartoitus, minkälaista suojausta mikäkin laite vaatii. Useat yritykset tarjoavat työntekijöilleen esimerkiksi oman kannettavan tietokoneen, jonka saa myös viedä kotiin. Tämä on myös tietoturvariski, koska kone poistuu yrityksen tiloista saattaen siellä olevat tiedot vaaraan joutua vääriin käsiin. (laitteistoturvallisuus.)

Asialla on myös kääntöpuolensa, mistä on vain hyötyä organisaatiolle. Jos työntekijällä on yrityksen omistama kannettava tietokone käytössään, hän ei tuo työpaikan tiloihin omaa tietokonettaan, joka myös olisi tietoturvariski. Kaikkien ylimääräisten koneiden tuominen yrityksen tiloihin lisää esimerkiksi uusien haittaohjelmien leviämistä organisaation tietoverkkoihin. Se, miten laitteet sijoitellaan, on tärkeää tietoturvan kannalta. Tässä löydetään taas yhteys fyysiseen tietoturvaan ja siihen, miten tilat joissa laitteita on, on suojattuna. Jos laitteita sijaitsee aivan poistumisteiden läheisyydessä, ne ovat helpoimmin poiskannettavissa. Varkaus

voi tapahtua keskellä kirkasta päivää, eikä muut työntekijät välttämättä edes huomaa varkautta. (laitteistoturvallisuus.)

Kannettavien tietokoneiden yleistyessä on syytä harkita niiden lukitsemista kaapelilukolla johonkin kiinteään esineeseen, esimerkiksi pöytään kiinni. Useimmissa kannettavien malleissa on valmiina erillinen paikka kaapelilukolle. (laitteistoturvallisuus.)

Kun laitteet huolletaan asianmukaisesti ja pidetään muutenkin kunnossa, vältytään usein ongelmilta. Organisaation kannattaa tehdä huoltosopimuksia sekä ylläpitosopimuksia käyttämiensä laitteiden osalta. Tällöin varmistutaan siitä, että ne huolletaan säännöllisesti ja että laitteet toimivat moitteettomasti. Kun organisaatiolla on kaikki laitteet dokumentoituina, niiden ylläpito helpottuu. Laitteet kannattaa myös merkitä, jolloin ne voidaan tunnistaa organisaatiolle kuuluvaksi. Rikki menneet laitteet tulee hävittää asianmukaisella tavalla. (laitteistoturvallisuus.)

2.6 Henkilöturvallisuus

Tietojärjestelmien käyttäjät itsessään aiheuttavat melkoisia tietoturvauhkia organisaatiolle. Tärkein asia uhkien ehkäisyssä on käyttäjien kunnollinen opastus tietojärjestelmien käytössä. Joskus käyttäjät aiheuttavat tahallisesti vahinkoa tietojärjestelmille. Tähän auttaa käyttöoikeuksien tarkka määrittely, ettei henkilölle anneta enempää valtaa organisaation tietojärjestelmiin pääsemiseen, kuin hänen katsotaan tarvitsevan. Useat yritykset tarkistavat työntekijöidensä taustoja, varmistaakseen ettei henkilö ole syyllistynyt esimerkiksi petoksiin tai kavalluksiin. Kunnollinen henkilöturvallisuus on siis henkilöstöstä aiheutuvien tietoturvauhkien hallintaa. (Ruohonen 2002, 5; Laaksonen, Nevasalo & Tomula 2006, 138.)

Organisaation tulee määrittää kullekin työntekijälle selkeästi tämän tehtävä- ja vastuualueet, jolloin vaarallisia työyhdistelmiä ei pääsisi syntymään. Henkilöturvallisuus on prosessi, joka siis alkaa työntekijän palkkaamisesta. Näihin tilanteisiin liittyy henkilöstörekisterejä. On esimiesten tehtävä hoitaa tämä selvitystyö ennen työntekijän rekrytoimista. Kaikki yritykset eivät suinkaan käytä taustatietojen selvitystä rekrytoidessaan, mutta tietomurtojen ja rikkomusten yleistyessä, myös taustatietojen selvitykset ovat luonnollisesti lisääntyneet. (Laaksonen, Nevasalo & Tomula 2006, 138–139.)

On monia tapoja tarkastella ihmisten taustoja. Helpointa voi olla vaikka vain hakea hakusanalla henkilön nimi. Hakukoneet voivat tarjota yllättävääkin tietoa. On silti syytä pitää mielessä, että internetistä löytyvä tieto pitää aina kyseenalaistaa ja siihen tulee suhtautua tietyllä kritiikillä. Luotettavaa on esimerkiksi soittaa työnhakijan suosittelijoille ja haastatella heitä henkilöstä. Silloin saa jo melko kattavan kuvan henkilöstä. Ansioluettelokin on helppo vää-

rentää, joten rekrytoijan on hyvä ottaa selvää, onko työnhakija todella ollut kyseisissä yrityksissä aiemmin töissä. Työtodistukset kertovat työntekijän ansioista edellisissä työpaikoissa. Jos hänellä ei ole näitä esittää, on mietittävä miksi hän ei ole hoitanut itselleen suosittelijoita tai työtodistuksia. (Laaksonen, Nevasalo & Tomula 2006, 139–140.)

Jotkut työnantajat suorittavat luottotietojen ja rikostaustojen selvitystä. Tällaiset palvelut ovat maksullisia ja ne suoritetaan suojeluspoliisin kautta. Turvallisuusselvitys on mahdollista tehdä vain, jos se oleellisesti vaikuttaa haettavaan virkaan, eli selvityksiä ei voi tehdä vain silkasta mielenkiinnosta henkilön taustoja kohtaan. Henkilön pitää lisäksi antaa suostumuksensa tietojensa selvittämiseen. Luottotiedot kertovat henkilön taloudellisesta asemasta, sitoumuksen hoitokyvystä ja luotettavuudesta. Näitä tietoja yritys voi tarvita silloin, kun tehtävään palkattavalta henkilöltä vaaditaan erityistä luottamusta tai taloudellista vastuuta tehtävässään. Henkilöllä on aina oikeus saada tietää kuka hänen luottotietojaan on kysellyt ja mihin tarkoitukseen tietoja on haettu. (Laaksonen, Nevasalo & Tomula 2006, 139–140.)

Työsopimuksessa oleellista tietoturvan kannalta on se, että siihen laaditaan tarkasti, mitä työntekijä tulee yrityksessä tekemään ja mitkä ovat hänen vastuualueensa. Työntekijällä pitää olla selkeys siitä, kuka on hänen esimiehensä ja kuka vastaa hänen koulutuksestaan ja perehdytyksestään työtehtäviin. Usein yrityksissä, joissa käsitellään salaisia tietoja, työntekijä allekirjoittaa salassapitosopimuksen. Tämä sopimus suojaa organisaatiota siltä, että luottamuksellista tietoa kulkeutuu eteenpäin. Jos työntekijä rikkoo salassapitosopimusta, on rangaistuksena yleensä rahamääräinen vahingonkorvaus. Kun henkilö on palkattu organisaatioon töihin, on hänen kanssaan käytävä läpi organisaation tietoturvapolitiikka ja tietojenkäsittelyn ja tietoturvallisuuden periaatteet. (Laaksonen, Nevasalo & Tomula 2006, 141–142.)

Työntekijän toimenkuva voi organisaatiossa muuttua. Tällöin voi aiheutua tietoturvariskejä, jos toimenkuvaa ei ole määritelty kunnolla alkuvaiheessa. Toimenkuva nimittäin kertoo sen, minkälaista tietoa työntekijä tarvitsee työssään ja mitä tietoa hän muokkaa. Toimenkuvaan liittyy siis oleellisesti kaikki käyttöoikeudet eri ohjelmiin, järjestelmiin ja lähiverkkoihin. Jos toimenkuva muuttuu, voi työntekijän aluevastuu esimerkiksi supistua, eikä hänellä ole enää lupa kaikkiin samoihin alueisiin kuin ennen. Ristiriitojen välttämiseksi on hyvä siis tarkistaa, että työntekijällä on oikeudet vain hänen tarpeidensa mukaisesti. Ennen kuin uudet oikeudet kirjataan, kaikki työntekijän vanhat oikeudet poistetaan, jotta ei synny vaarallista työyhdistelmää tai turhia käyttöoikeuksia. (Laaksonen, Nevasalo & Tomula 2006, 141–142.)

Työsuhteen päättyminen on usein työnantajalle hankala tilanne, koska työntekijän mukana poistuu usein salaistakin tietoa. Vaikka tietokoneet ja muut laitteet jäisivätkin työnantajalle työsuhteen päätyttyä, on työntekijä voinut kopioida tiedostoja ja kertoa informaatiota

eteenpäin. Hänen päänsä sisällä olevaa informaatiota ei kukaan voi nähdä eikä lukea. (Laaksonen, Nevasalo & Tomula 2006, 143–144.)

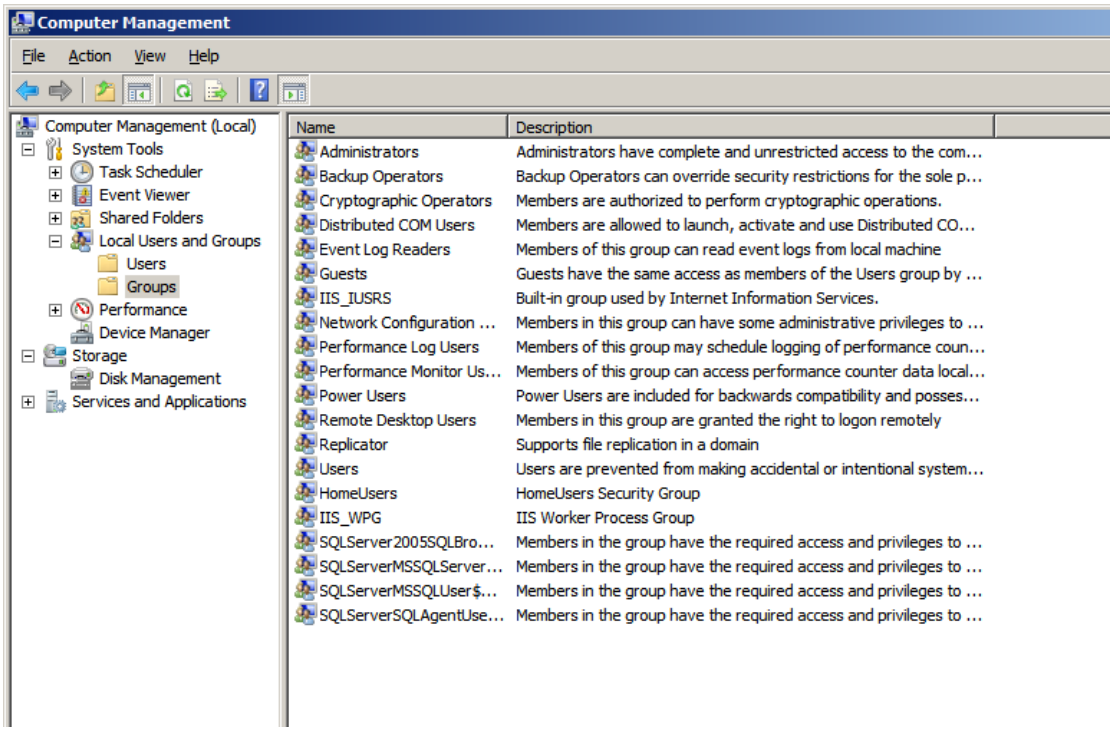
Joissain yrityksissä on voimassa kilpailukielto, mikä tarkoittaa sitä, ettei työntekijä irtisanoutuessaan saa tiettynä aikana rekrytoitua saman alan yritykseen töihin. Organisaation esimiesten on hyvä muistaa, että irtisanoutuvankaan työntekijän henkilön tietosuoja ei saa vaarantua, mikä tarkoittaa ettei henkilön tietoja saa käsitellä huolimattomasti vaikka työntekijä olisikin jo lähtenyt pois yrityksestä. Suomessa on tarkka laki, joka määrittelee yksityisyyden suojan työelämässä. (Laaksonen, Nevasalo & Tomula 2006, 143–144.)

2.7 Käyttöturvallisuus

Tietojärjestelmiä on aina syytä käyttää turvallisesti ja tätä tarkoittaa käyttöturvallisuus. Jälleen kerran löydetään yhteys toiseen osa-alueeseen eli henkilöstöturvallisuuteen. Henkilöt voivat aiheuttaa tietoturvariskejä, jos he eivät piittaa turvallisuusasioista, tai heillä ei ole riittävää osaamista turvallisuusasioihin. (Ruohonen 2002, 5.)

Käyttöturvallisuuteen liittyy oleellisena osana esimerkiksi käyttöoikeuksien hallinta ja erilaiset tunnistus- ja todentamismenetelmät. Näillä saavutetaan turvallisuutta tietojärjestelmien käyttöön, koska niitä voivat käyttää ainoastaan valtuutetut henkilöt. Usein käyttäjät tahattomasti ja huolimattomuuttaan aiheuttavat tietojärjestelmiin turvallisuusriskejä, jolloin taas korostuu henkilökunnan koulutuksen tärkeys. Tekijöiden pitää tietää mitä he tekevät, jotta vältyttäisiin turvallisuutta uhkaavilta tekijöiltä. (Käyttöturvallisuus.)

Kuvassa voi nähdä Windowsille ominaisen käyttäjäryhmien hallintaan tarkoitetun perusnäkymän.



Kuvio 3: Windows 7 – Käyttöjärjestelmän käyttäjäryhmiä

On myös tärkeää, että testi- ja ohjelmistoympäristö eivät sijaitse samassa ympäristössä käyttöympäristön kanssa. Näin ollen niiden toiminta ei pääse häiritsemään toisiaan. Käyttöturvallisuuden parantamiseksi organisaatiossa tulisi sallia tietokoneiden käyttäjiltä vain sellaisten tietojärjestelmien käyttö, jota he työssään tarvitsevat. Esimerkiksi turha internetsivujen selailu aiheuttaa aina riskejä käyttöturvallisuuteen.(Käyttöturvallisuus.)

2.8 Hallinnollinen turvallisuus

Koska tietoturvallisuus on niin laaja alue, sen hallinnointiin on syytä kiinnittää huomiota. Jotta kaikki osa-alueet pysyisivät hallinnassa, niitä pitää johtaa. Tätä kutsutaan hallinnolliseksi turvallisuudeksi. Tämä osa-alue varmistaa muiden osa-alueiden toimivuuden ja turvallisuuden, suunnittelee tulevaisuuden ratkaisuja ja luo kehittävän tietoturvasuunnitelman organisaatiolle. (Ruohonen 2002, 5; Hakala, Vainio & Vuorinen 2006,10.)

Hallinto pitää yhteyttä muihin turvallisuudesta vastaaviin organisaatioihin sekä viranomaisiin. Tällaiset tehtävät kuuluvat yleensä organisaation tietohallinnolle. He ovat myös selvillä lakisääteisistä asioista, sekä erilaisista lisenssi- ja palvelusopimuksista. (Ruohonen 2002,5; Hakala, Vainio & Vuorinen 2006,10.)

3 VIRUKSET JA MUUT HAITTAOHJELMAT

Nykypäivän tietoturvassa keskeinen ongelma on virukset, ja niiden torjuminen onkin arkipäivää. On hyvä muistaa, että viruksen leviävät aina koneiden käyttäjien toiminnan seurauksena. Ne eivät yksinään hyökkää koneisiin ja laitteisiin, vaan tarvitsevat aina käyttäjän joka aktivoi viruksen, joko vahingossa tai tahallaan. On tärkeää ymmärtää, mitä virukset ovat ja miten ne toimivat, jolloin niiden torjuminenkin helpottuu. (Järvinen 2002, 249; Ruohonen 2006, 345–346.)

3.1 Yleistä viruksista

Virukset ovat siis erilaisia tietokoneohjelmia, jotka on ohjelmoitu siten, että ne leviävät koneesta toiseen, joka tapahtuu usein täysin käyttäjän huomaamatta. Virusten skaala on laaja, toiset virukset tekevät mittavia tuhoja, toiset taas vahingoittavat vain joitain osia koneessa. Yhtenäistä kaikille viruksille on se, että ne tavalla tai toisella aina haittaavat koneen toimintaa. (Järvinen 2002, 249; Ruohonen 2006, 345–346.)

Virukset kopioivat itse itseään, jolloin ne leviävät laajalle tietoverkkojen välityksellä. Niille tyypillinen ominaisuus on se, että ne toimivat jonkin toisen ohjelman sisällä. Näin ollen käyttäjä voi avatessaan toiseksi luulemansa ohjelman, saada samalla riesakseen viruksen, joka alkaa levitä hänen koneessaan. Virus voi tarttua mihin tahansa ohjelmatiedostoon, eli mihin tahansa tiedostoon, joka sisältää ajettavaa koodia. (Järvinen 2002, 249; Ruohonen 2006, 345–346.)

Ensimmäisiä viruksia alkoi ilmaantua tietokoneisiin 1980-luvun puolivälissä. Mikrotietokoneiden yleistyminen aiheutti myös virusten kehittymisen ja leviämisen, koska näissä koneissa ohjelmat pystyivät itse monistamaan itseään ja näin leviämään koneesta toiseen. Ensimmäisen viruksen kehittäjät jäivät heti kiinni, koska he olivat ikuistaneet nimensä, osoitteensa ja puhelinnumeronsa viruksen ohjelmakoodiin. Tämä tapahtui Pakistanissa vuonna 1986. Tapaus aiheutti maailmanluokan uutisen, sillä olihan luotu jotain ihan uutta ja ihmeellistä. Tämän viruksen nimi oli Brain, tekijöidensä yrityksen nimen mukaisesti. Viruksia pidettiin alussa vain ohimenevänä ilmiönä ja se olikin aluksi vain Macintosheissa esiintyvä ongelma. PC-käyttäjät olivat tyytyväisiä kun heidän koneissaan ei ollut viruksia, kunnes vuonna 1989 pc-virukset valtasivat jo Suomenkin. Tästä virusten määrä lähti kohisten nousuun. (Järvinen 2002, 250–251.)

Alussa virukset olivat yksinkertaisia, muutaman koodinpätkän kokoisia ja ne voitiin jakaa kahteen ryhmään, lohkoviruksiin ja ohjelmaviruksiin. Levykkeitä käytettiin ja lohkovirukset levisivät niiden välityksellä. Virustyyppi levisi ja tarttui tämän jälkeen jokaiseen levykkeeseen,

joka kyseisen koneen A-asemaan laitettiin. Ohjelmavirukset levisivät ohjelmien välityksellä. Kun koneessa oli ohjelmavirus, se levisi sen jälkeen kaikkiin muihinkin ohjelmiin jotka koneeseen asennettiin viruksen tarttumisen jälkeen. Vuonna 1992 nousi suuri kohu Michelangelo-viruksesta, jota tutkittaessa selvisi, että 6.3 päivämääränä se tuhoaa kaikki kirjanpitotiedostot, jota koneissa on. Tämä aiheutti maailmanlaajuisen huolen, koska virus oli levinnyt laajalle. (Järvinen 2002, 251–252.)

Koska kyseessä oli ensimmäinen laaja ja vakava virusepidemia, kaikki olivat huolissaan seurauksista. Kun maaliskuun kuudes päivä koitti, osoittautui, että virus ei ollutkaan niin mahtipontinen, kuin oli annettu ymmärtää. Se kuitenkin aiheutti tuhoa muutamiin tuhansiin koneisiin ja niiden tiedostoihin. Michelangelo-virus sai yritykset kiinnostumaan virustorjunnasta, jonka johdosta torjuntaohjelmille alkoi olla yhä enemmän kysyntää. Microsoftin 1990-luvun alussa julistama Windows 3.0 oli jymymenestys, koska useimmat DOS -virukset eivät voineet levitä siihen. Luultiin jo, että virusongelmista oli päästy eroon, mutta toisin kävi. (Järvinen 2002, 251–252.)

Windows 95:n julkistaminen toi mukanaan myös ensimmäisen makroviruksen. Tästä lähtien piti varoa myös tiedostoja entisen levykkeiden ja ohjelmatiedostojen lisäksi. Makrovirukset levisivät nopeasti ja niitä tuli jatkuvasti yhä uusia ja erilaisia. Makrovirusten valmistamiseen ei välttämättä tarvita edes kummoisia ohjelmointitaitoja, koska nykyään internetissä on saatavilla ohjeita näiden virusten luomiseen. Niiden ohjelmoimisen helppouden vuoksi niiden määrä kasvaa jatkuvasti. (Järvinen 2002, 253–254; Ruohonen 2006, 350.)

Sähköpostien yleistyessä alkoi levitä myös sähköpostivirukset. Melissa-virus oli ensimmäinen sähköpostivirus, joka levisi kulovalkean tavoin hetkessä maailmanlaajuisesti. Se ehti levitä noin miljoonaan tietokoneeseen aiheuttaen 80 miljoonan dollarin kustannukset, kun sitä puhdistettiin pois koneista. Sähköpostivirukset leviävät nopeasti sen takia, että ne lähettävät itse itseään postina osoitekirjassa oleviin osoitteisiin. Virus aktivoituu, kun sähköposti aukaistaan. Virusta ei tarvitse myöskään tehdä enää niin pieneksi, koska se leviää sähköpostin liitteissä, eikä piilossa niin kuin muut virukset. (Järvinen 2002, 254–255; Ruohonen 2006, 350–351.)

Madot ovat erilaisia haittaohjelmia siksi, että ne tarvitsevat aina isännän itselleen ja leviävät tämän mukana. Isäntä voi olla levyke tai ohjelmatiedosto tai vaikkapa dokumentti. Toinen ero virukseen on myös se, että se leviää itsenäisesti kirjoittamalla itsestään kopion paikkaan, josta se pääsee suoraan ajettavaksi. Se toimii siis itsenäisesti, eikä toisen ohjelman sisällä, niin kuin virus. Mato myös saattaa monistaa itseään useaan kertaan saman järjestelmän sisällä. Madot eivät välttämättä ole niin haitallisia kuin virukset, niiden haitta lähinnä on se, että ne ylikuormittavat koneen kapasiteettia vieden tilaa ja suorittamalla kopioita itsestään. Tämä aiheuttaa sen, että koneet menevät helposti jumiin tai toimivat hitaasti. Yleensä madot pyr-

kivät vain leviämään, mutta ne voivat myös sisältää tuhoa aiheuttavaa koodia. (Järvinen 2002, 255–256; Ruohonen 2006, 353–354.)

Erittäin haitallinen ja vaikea havaita on haittaohjelma nimeltä troijan hevonen eli troijalainen. Se naamioituu hyödylliseksi ohjelmaksi, mutta sen taakse kätkeytyykin esimerkiksi vakoiluohjelma. Troijalainen voi olla tutusta osoitteesta tulleesta sähköpostista, jossa on jouluterveh dys tai muu hauska viesti. Kun viesti avataan, troijalainen asentaa tietokoneelle takaoven tai muun vakoiluohjelman käyttäjän huomaamatta. Tällaiset troijalaiset ovat erittäin vaarallisia, kun niitä käytetään esimerkiksi yrityksiä vastaan. Käyttäjä ei välttämättä osaa edes epäillä joutuneensa troijalaisen hyökkäyksen uhriksi, koska sähköposti usein tulee oikeasta osoitteesta, sisältäen oikeanlaisen tervehdyksen tai viestin. Troijan hevonen ei siis leviä itsestään, vaan se pitää klikata auki ja tämän tekee aina käyttäjä itse. (Järvinen 2002, 256–257; Ruohonen 2006, 354.)

Edellä olevassa kuvassa on Beast – nimisen troijan hevosen käyttöliittymä.

Kuvio 4: Beast on Windows-pohjainen troijan hevonen, joka avaa tietoturva-aukkoja kohteen koneelle

Niin oudolta kuin se kuulostaakin, on olemassa myös hyviä viruksia. Niiden tarkoitus on koneen vahingoittamisen sijaan aiheuttaa hyötyä koneeseen, johon on tarttunut jo virus. Tällaisia hyviä viruksia ovat muun muassa Anti-virus-virukset, tiedostonpakkausvirukset ja huoltovirukset. Anti-virus-virukset poistavat muita viruksia koneelta. Huoltovirukset toimivat koneessa ikään kuin huoltomiehinä korjaten tietoturva-aukkoja ja poistaen väliaikaistiedostoja. (Ruohonen 2006, 352–353.)

Tiedostonpakkausvirusten hyöty on siinä, että ne pakkaavat tartuttamansa ohjelmatiedoston, jolloin se kuluttaa vähemmän tilaa koneen kovalevyllä. Näiden hyvien virusten kääntöpuolena kuitenkin on, että ne saattavat olla yhtä haitallisia kuin huonot virukset. Ne voivat esimerkiksi sisältää ohjelmointivirheitä, jolloin ne eivät toimi oikein. Tämä taas aiheuttaa sen, että virukset leviävät tietojärjestelmiin, joihin niitä ei ole tarkoitettu. Myös hyvä virus kuluttaa tietokoneen kapasiteettia. (Ruohonen 2006, 352–353.)

Haittaohjelmia ovat siis kaikki ne ohjelmat, jotka käyttäjältä lupaa kysymättä asentuvat koneelle salaa, aiheuttaen tuhoa. Nykyään ongelmana eivät ole enää vain viruksia levittävät teinit jotka kokeilevat osaamistaan, vaan haittaohjelmia levittävät ennen kaikkea kansainväliset liigat ja järjestäytynyt rikollisuus. Rikolliset ostavat itselleen hyödyllisiä haittaohjelmia ja tekevät niillä bisnestä. Vakoiluohjelmien käyttö on lisääntynyt ja huijausviestejä lähetellään yhä enemmän. Roskapostit ovat sähköpostikäyttäjien harmina, tukkien postilaatikot ja levittäen viruksia. Roskapostittajat saavat helposti käsiinsä toimivia sähköpostiosoitteita ja näin ollen levittävät yhä laajemmalle roskapostejaan. (Järvinen 2006, 77–79.)

Nettikauppiaat keräävät käyttäjiensä surffaustietoja, käyttäen niitä hyväkseen, kun he miettivät mihin kohdistaa mainontaansa. Haittaohjelmien pääsy koneisiin pitäisi siis estää, jotta esimerkiksi netissä surffailu olisi turvallista. Käyttöjärjestelmässä ei saisi olla tietoturva-aukkoja, koska niiden kautta leviävät helposti madot ja muut haittaohjelmat. Käyttöjärjestelmän säännöllinen päivitys, käyttäjien oikeuksien rajoittaminen ja palomuurit suojaavat näiltä aukoilta. (Järvinen 2006, 77–79.)

Seuraavassa kuvassa on esimerkki huijausilmoituksesta, jossa ihmisiä houkutellaan ilmaisella kannettavalla tietokoneella.

Kuvio 5: Hyvin tyypillinen huijausilmoitus, jossa käyttäjää pyydetään osallistumaan ilmaisen kannettavan tietokoneen arvontaan

Haittaohjelmien yleisimpiä merkkejä ovat:

- netissä surffattaessa avautuu mainosikkunoita, jotka eivät liity itse sivun tuotteisiin tai palveluihin
- kone ”tahmaa” ja toimii selkeästi aiempaa hitaammin
- työpöydälle ilmestyy tuntemattomiin verkkopalveluihin osoittavia kuvakkeita ja selaimessa näkyy uusia työkalupalkkeja
- selaimen aloitussivu vaihtuu toiseen palveluun eikä sitä pysty muuttamaan takaisin
- prosessorin kuormitusaste, joka näkyy Task Managerin näytössä, pysyy jatkuvasti lähellä 100 prosenttia
- selain kaatuilee joko heti käynnistäessä tai satunnaisesti selailun aikana
- verkkoliikenteen määrä kasvaa oleellisesti, mikä näkyy verkkopäätelaitteen merkkivalojen tasaisena palamisena
- levyltä löytyy erikoisesti nimettyjä tiedostoja, joissa on usein välilyöntejä ja numeroita; on myös tyypillistä että nimet vaihtuvat koko ajan.

(Järvinen 2006, 85.)

Tietokoneiden jatkuva kehitys, sekä käyttäjiensä osaamisen kasvaminen luovat yhtälön, jolla saadaan jatkossa aikaan vaarallisempia ja enemmän tuhoa aiheuttavia viruksia ja haittaohjelmia. Datayhteyksien nopeudet kasvavat koko ajan, ja tämä mahdollistaa uusien virusten leviämisen yhä nopeammin ja tehokkaammin. Uusissa viruksissa yhdistellään yhä enemmän eri

tekniikoita ja ne ovat myös monimutkaisempia ja kehittyneempiä. Mitä nopeampi datayhteys, sitä enemmän tietoa saadaan siirrettyä kerralla. Virusten oma koodi kasvaa samalla mitalla jopa satoihin kilotavuihin. Virusten tunnistus tulee koko ajan vain vaikeutumaan, kun ne oppivat paremmin piiloutumaan ja muuntelemaan omaa koodiaan. (Järvinen 2002, 265.)

Virukset alkavat käyttää yhä enemmän ääntä ja kuvaa tietokoneissa. Ne voivat tulevaisuudessa esimerkiksi kopioida kotikoneilta ääntä ja levittää sitä internetin www-sivuille. Tällöin perheen sisäiset keskustelut voisivat päätyä koko maailman kuultaviksi. Tällainen aiheuttaisi mittavia tuhoja esimerkiksi yrityksille, joiden salaisia tietoja vuotaisi yhä enemmän julkisuuteen. Virukset osaavat myös käyttää mobiilipalveluita hyödykseen ja voivat lähettää netin kautta tuhansia tekstiviestejä, tai tilata kännyköihin maksullisia palveluita, jotka käyttäjä joutuu maksamaan. Vaaraksi voisi muodostua esimerkkinä tilanne, jossa virukset soittelisivat hätänumeroihin ja tukkisivat linjat näillä turhilla puheluillaan. Haittaohjelmia tullaan varmasti käyttämään yhä enemmän jopa sodankäynnin välineenä, sillä virusten takana on koko ajan yhä isompia organisaatioita ja jopa valtioita. Kyse ei ole enää mistään pienen porukan osaamasta leikistä, vaan pelottavasta tulevaisuudesta jota kukaan ei pysty ennustamaan. (Järvinen 2002, 265.)

3.2 Viruksien havainnointi

Etsintäohjelmat auttavat haittaohjelmien havainnoinnissa. Koska käyttäjä ei voi aina luottaa omaan harkintakykyynsä sataprosenttisesti, nämä skannerit auttavat haittaohjelmien havainnoinnissa käymällä levyn tiedostoja läpi. Havaitessaan haittaohjelman, ne ilmoittavat siitä ja käyttäjä voi yrittää poistaa ohjelman koneelta. Usein skannerit ovat turhankin innokkaita ja ilmoittavat kaikesta mahdollisesta joka saattaisi olla haittaohjelma. Tällaisia tilanteita syntyy esimerkiksi silloin, jos joku tiedosto on pakattu useaan kertaan. Erityisesti etsintäohjelmat keskittyvät vakoiluohjelmien etsintään ja luulevat löytävänsä niitä jatkuvasti www-sivuilta. (Järvinen 2006, 85–87.)

Seuraavassa kuvassa näkyy haittaohjelmien poistoon tarkoitetun Ad-Aware ohjelman käyttöliittymä.

Kuvio 6: Lavasoftin kehittämä haittaohjelmien etsintätyökalu Ad-Aware

Nettisivusto virusscan.jotti.org on hyödyllinen käyttäjälleen, sillä sinne voi syöttää epäilyttäviltä vaikuttavia ohjelmatietoja, joita käyttäjä on löytänyt levyltään. Sivusto käyttää useita skannereita, jotka tutkivat näitä tiedostoja. (Järvinen 2006, 85–87.)

Kun virus tai muu haittaohjelma on havaittu, on tietokone heti syytä irrottaa verkosta. Sen jälkeen tietokoneen uudelleenkäynnistyksen voi suorittaa esimerkiksi käynnistys cd:llä, johon virus ei ole vielä tarttunut. Viruksen poistamiseen voi kokeilla uusimman päivityksen saanutta virustorjuntaohjelmaa. Jos viruksen poisto onnistuu tällä virustutkalla, voidaan kone käynnistää uudelleen ja suorittaa uusi virustentarkastus siltä varalta, että virus varmasti on poistettu. (Ruohonen 2002, 228.)

Virus saattaa kuitenkin pompata koneelle heti kun se käynnistetään uudelleen ja tämä onkin merkki siitä, että virus on ehtinyt kopioida itseään jonnekin, mistä virustutkat eivät sitä ole löytäneet. Tällaisia paikkoja voivat olla esimerkiksi tietokoneen keskusmuisti tai kovalevyn käynnistyssektori. Tietokoneen keskusmuistin tyhjennys voi auttaa poistamaan viruksen. Jos

virus on päässyt tietokoneen paristovarmennettuun keskusmuistiin, tulee emolevyllä oleva paristo poistaa hetkeksi ja laittaa se sitten takaisin paikoilleen. Jos paristovarmennettu muisti tyhjennetään, merkitsee se sitä, että tietokoneen BIOS-asetukset palautuvat oletusasetuksiksi. Jotta tiedetään koneessa käytetyt BIOS-asetukset, kannattaa ne merkitä itselleen muistiin ennen kuin paristo irrotetaan. Näin asetukset saadaan heti pariston palauttamisen jälkeen laitettua takaisin niin kuin ne olivatkin. (Ruohonen 2002, 228.)

Kovalevyn käynnistyssektorille ennättänyt virus poistetaan siten, että käynnistyssektori ylikirjoitetaan alkuperäisellä käynnistyssektorilla. Tällöin tietokone käynnistetään oikean käyttöjärjestelmän levykkeellä ja annetaan komento fdisk/mbr. Tämä voi olla riskialtis toimenpide silloin, kun siihen todella on tarttunut käynnistyslohkovirus. Jos virustorjuntaohjelma ei pysty virusta poistamaan, voi tämä olla ainoa keino saada virus poistetuksi. Ennen tämän komennon suorittamista kannattaa ottaa kaikista tiedostoista varmuuskopiot, sillä tiedot saattavat pahimmassa tapauksessa kadota kokonaan. (Ruohonen 2002, 228–229.)

Kun kaikki voitava viruksen poistamiseksi on kokeiltu (virustorjuntaohjelma, tietokoneen keskusmuistin ja paristovarmennetun muistin tyhjennys, kovalevyn käynnistyssektori uusittu), eikä virus siltikään katoa koneelta, kannattaa vielä varmistaa, ettei virus tartu koneelle joka kerta uudestaan esimerkiksi toiselta tietokoneelta, virustorjuntaohjelmasta tai käynnistyslevykkeeltä. (Ruohonen 2002, 228–229.)

Varmuuskopioiden ollessa varmassa tallessa, voidaan koko kovalevy tyhjentää ja näin ollen palauttaa tietokone samaan tilaan kuin se oli varmuuskopioita otettaessa. Jos verkossa on useampia koneita, on ne syytä käydä myös läpi viruksen hyökkäyksen varalta ja suorittaa tarvittavat toimenpiteet. (Ruohonen 2002, 228–229.)

3.3 Viruksien torjunta

Käyttöjärjestelmässä ei saisi olla tietoturva-aukkoja, koska niiden kautta leviävät helposti madot ja muut haittaohjelmat. Käyttöjärjestelmän säännöllinen päivitys, käyttäjien oikeuksien rajoittaminen ja palomuurit suojaavat näiltä aukoilta. Jos taas selaimessa on turva-aukkoja, ovat ne mutkikkaampia, koska palomuuri on voimaton niitä vastaan. Selaimen säännöllinen päivitys on perusasia, joka pitäisi aina muistaa. Käyttäjille pitäisi myös olla itsestään selvää, ettei epämääräisiä www-sivuja tule selata ja turhaan klikkailla. Joskus se ei riitä, koska myös ”hyvämaineisilta” nettisivuilta leviää haittaohjelmia. Joku on voinut murtautua kyseiselle sivulle ja istuttanut haittaohjelman sinne, tai haittaohjelma saattaa levitä sinne sivuilla käytettyjen mainosten välityksellä. (Järvinen 2006, 79–83.)

Koska yksikin klikkaus jollekin sivulle voi olla kohtalokas ja tuhota koko koneen, on terveen järjen ja harkintakyvyn käyttö erittäin suotavaa selailtaessa internetsivuja. Koneen puhdistaminen voi olla jopa mahdotonta, koska vaikka haittaohjelman saisikin poistettua, se ilmestyy takaisin uudella nimellä. Jos haittaohjelmia on paljon päällekkäin, kone ei enää voi toimia kunnolla. Joskus ainoa keino on formatoida koko kovalevy ja asentaa kaikki uudelleen. Tätä tietenkin pyritään välttämään kaikilla mahdollisilla haittaohjelmien torjuntaan pystyvillä keinoilla. (Järvinen 2006, 79–83.)

Vuonna 2005 kuusi kymmenestä yleisimmästä viruksesta oli sähköpostin välityksellä leviäviä viruksia. Kaikki nämä kymmenen virusta olivat levinneet Windows-käyttöjärjestelmien kautta. (Laaksonen, Nevasalo & Tomula 2006, 202–205.)

Suomessa yritysten virustorjunta on verraten muuhun maailmaan melko hyvällä mallilla. Ongelmia voi aiheutua silloin, kun organisaation tietokoneita käytetään kotona ja etäyhteyksillä. Tällöin torjuntana voidaan käyttää esimerkiksi sellaista menetelmää, että etäyhteyksiä käytetään vain yrityksen omalta kannettavalta tietokoneelta. Näin voidaan olla varmoja, että virustorjunta on ajan tasalla. Työntekijä ei saisi ottaa yhteyttä yrityksen verkkoihin omilla henkilökohtaisilla tietojenkäsittelylaitteillaan. Vaikka työasemat olisikin virustorjuttu, se ei riitä. Torjunta pitää järjestää myös palvelinympäristöön, mobiililaitteille ja internetympäristöön. Joskus virustorjunta ulkoistetaan, ja se edellyttää sitä, että palveluntarjoaja tarjoaa riittävästi raportointia ja tiedotusta jo torjutuista viruksista ja mahdollisista uusista uhista. (Laaksonen, Nevasalo & Tomula 2006, 202–205.)

Palomuuri suojaa viruksilta. Se tarkastaa kaiken saapuvan dataliikenteen, ennen kuin se saapuu yrityksen lähiverkkoon. Se ei tarkista ainoastaan www-sivustoja, vaan kaikki muutkin ohjelmat ja data joutuvat sen syyniin. Usein esimerkiksi sähköpostien liitetiedostot on pakattu, jotta siirto olisi nopeampaa. Tällöin palomuurin työ vaikeutuu ja verkkoliikenne samalla hidastuu.

Tärkeintä olisi muistaa välttää turhia tiedostoliitteitä. Näppärä tapa on kirjoittaa teksti leikepöydälle ja kopioida se siitä sähköpostiin ja lähettää. Tällöin tosin logot ja grafiikat poistuvat, mutta jos tarkoitus on lähettää vain tekstiä, sillä ei ole merkitystä. Tekstin lähettäminen pelkästään ilman dokumenttia poistaa työtiedostojen mukana leviävät virukset. Viestejä, jotka tulevat chat-kanavilta, pikaviestiohjelmista tai news- keskusteluryhmistä ei tulisi koskaan avata. (Järvinen 2002, 275–280.)

Koska virukset aktivoituvat vasta tiedostoa avattaessa, olisi hyvä käyttää hyödykseen liitetiedostojen esikatselumahdollisuutta, joka on useimmissa sähköpostiohjelmissa valmiina. Klikkaamalla hiiren kakkospainikkeella kuvakkeen kohdalla, quick view -vaihtoehto näyttää pie-

nessä ikkunassa millaista tietoa tiedosto sisältää. Sisällöstä saa käsityksen ja jos se osoittautuukin virukseksi, se ei aktivoidu koska tiedostoa ei ole vielä avattu. (Järvinen 2002, 275–280.)

WordPad on yksinkertainen ohjelma, jolla voi avata Word-liitteitä. Koska se ei sisällä makrokieltä, virukset eivät voi aktivoitua, jos liitteet avataan sen kautta. Tämä on siis suositeltavan yksinkertainen keino lukea turvallisesti saatuja Word-tiedostoja. Sovelluksessa voi olla käytettävissä toiminto, joka estää automaattisesti käynnistyvien makrojen toiminnan. Aina kannattaisi tarkistaa, löytyykö se omalta koneelta ja asettaa se toimintaan. (Järvinen 2002, 275–280.)

Opettelemalla tunnistamaan epäilyttävät viestit ja rajoittamalla jakelulistojen käyttöä, voidaan torjua monia viruksia. Usein myös käytämme turhaan lähiverkkoyhteyksiä, joissa eräät virukset leviävät. Kannattaa siis sulkea kaikki NET USE –yhteydet, joita ei tarvita ja välttää turhaan jakamasta oman levyn tiedostoja. (Järvinen 2002, 275–280.)

Virustutkat, eli virustentorjuntaohjelmat ovat ohjelmia, joilla pyritään löytämään ja tuhoamaan kaikki koneella olevat virukset. Tutka voi etsiä viruksia esimerkiksi tutkimalla jokaisen tiedoston tietokoneelta, tai se voi skannata tietokoneen keskusmuistia läpi. Useimmat virustentorjuntaohjelmat tekevät näitä molempia asioita samaan aikaan. Ohjelmat osaavat etsiä tunnettuja viruksia, etsiä viruksen toimintaa muistuttavia piirteitä, tai ne voivat seurata ohjelmien toimintaa ja pysäyttää sen toiminnan, jos ne epäilevät kyseessä olevan virus. Näissä ohjelmissa on taas tämä sama ongelma siitä, että kun ne etsivät viitteitä virustyyppisistä ohjelmista, ne antavat usein vääriä hälytyksiä. (Ruohonen 2002, 226–227.)

Virustentorjuntaohjelmien päivityksestä tulisi huolehtia äärimäisen tarkasti, jopa päivittäin. Ongelmaksi muodostuu se, että päivitykset väistämättä laahaavat hieman virusten jäljessä, koska virusten kehittäjillä on aina ”varaslähtö”. Uusista viruksista saadaan tietoa aikaisintaan vasta sen jälkeen, kun ensimmäinen kone on saastunut. Jos virustorjuntaohjelman päivitys aiheuttaa käyttökatkoja tietokoneelle, on syytä arvioida tarkkaan, kuinka usein päivitys on oleellista organisaation koneille. Usein päivitystoiminto on automaattinen, kun taas joskus päivitykset tulee käyttäjän hakea itse. Suurissa verkoissa, kuten esimerkiksi Laurean verkossa, olisi varmasti viisainta olla automaattinen päivitysjärjestelmä. (Ruohonen 2002, 226–227.)

Kuvassa Suomalaisen F-Securen kehittämä virustorjuntaohjelman päänäkymä.

Kuvio 7: F-Secure on suomalaisten kehittämä ohjelma virustorjuntaan

Seuraavassa on lista asioista, jotka virustorjunnan onnistumisen kannalta on syytä ottaa huomioon:

- työasemien virustorjunta
- etä- ja mobiililaitteiden virustorjunta, mukaan lukien kotikoneet
- palvelimien virustorjunta
- tuotannollisten järjestelmien virustorjunta
- sähköpostin, selaimen ja internet-liikkeen virustorjunta
- kaikkien virustorjuntakomponenttien automaattinen ja riittävän tiheä päivitys
- siirrettävien medioiden kuten usb-muistien, ipod-soittimien, cd-levyjen käsittely ja suojaus
- tietoturvavaatimukset (virustorjuntavaatimukset) laite- ja järjestelmätoimittajille
- sopimukset ja raportointikäytännöt sekä seuranta
- toiminta virustapauksissa.

(Laaksonen, Nevasalo & Tomula 2006, 205.)

Kaksitoista tärkeää muistisääntöä virusten ja muiden haittaohjelmien torjuntaan:

- vältä tiedostoliitteitä
- käytä liitetiedostojen esikatselua
- avaa dokumentit WordPadilla
- estä makrojen aktivoituminen
- tunnista epäilyttävät viestit
- älä avaa viestiä heti
- päivitä ohjelmat uusimpiin versioihin
- harkitse ohjelman vaihtoa
- rajoita jakelulistojen käyttöä
- sulje tarpeettomat lähiverkkoyhteydet
- poista Windows Scripting Host käytöstä
- käytä torjuntaohjelmaa ja päivitä sitä säännöllisesti.

(Järvinen 2002, 273.)

4 LAUREAN VIESTINTÄVÄLINEIDEN TIETOTURVA

4.1 Sähköpostin tietoturva

Olemme saaneet viime vuosikymmeninä elää dataliikenteen kehityksen ja mullistuksen aikaa. Sähköposti on yksi niistä useista keksinnöistä, jotka ovat muuttaneet asioita helpompaan suuntaan. Sähköpostilla käyttäjä lähettää postia minne tahansa maailmassa vain muutamassa sekunnissa ja täysin ilmaiseksi. Mikä voisikaan olla helpompi tapa hoitaa asioita nykypäivänä? Melkein jokaisella ihmisellä on oma henkilökohtainen sähköpostiosoite, tai jopa useita. Lisäksi on olemassa työpaikkojen ja koulujen sähköpostiosoitteita. Ihminen on siis käytännössä katsoen aina tavoitettavissa jonkun osoitteen kautta. Ihmiset lähettävät yksityisiä sähköposteja luottaen siihen, että kukaan ulkopuolinen ei pääse niihin käsiksi. (Järvinen 2002, 215.)

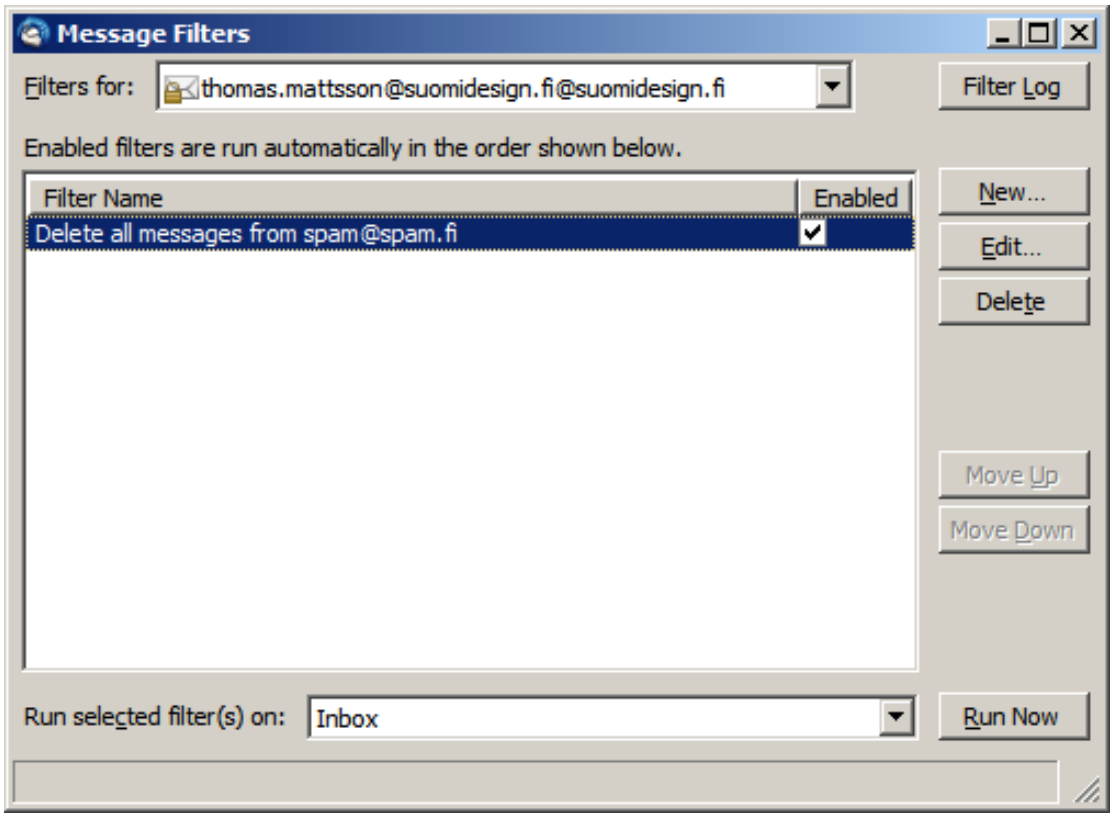
Sähköpostijärjestelmä koostuu kolmesta osasta. Näitä ovat itse verkko, postitoimisto ja käyttäjän postiohjelma. Postitoimisto toimii palvelimena joka ottaa posteja vastaan, jakaen ne edelleen käyttäjien postilaatikoihin. Jos käyttäjä on tuntematon, postitoimisto palauttaa viestin lähettäjälleen ja lähettäjä saa virheilmoituksen ”tuntematon käyttäjä”. Itse postilaatikko sijaitsee käyttäjän omalla palvelimella. Täältä käyttäjä pystyy lukemaan postinsa. Yrityksen postipalvelin voi sijaita esimerkiksi organisaation omassa verkossa, mutta usein nämä palvelimet ovat ulkoistettuja internet-operaattoreille. Yksityisen käyttäjän sähköpostit tulevat aina operaattorin kautta, josta ne haetaan luettavaksi omalle koneelle. (Järvinen 2002, 216–247.)

Vastaanottaja löytyy sen osoitteessa olevan Windows-toimialue-nimen kautta ja lähettävän ja vastaanottavan postitoimiston välillä on ainoastaan reitittimiä, jotka ohjaavat kaikkea ip-paketeista koostuvaa internet-liikennettä. Reitittimien tehtävä ei ole suodattaa millaista tietoa eteenpäin välitetään, ne vain kuljettavat kaiken mahdolliset mahdollisimman nopeasti eteenpäin. Välitettävä ip-paketti ei myöskään tallennu reitittimelle. Siirtoyhteyden ollessa näin mahdollisimman suora, parantaa se tietoturvaa, koska postia on vaikea napata sen liikkuessa nopeasti reitittimen välityksellä vastaanottajalleen. (Järvinen 2002, 216–217.)

On hyvä muistaa, että sähköpostin käyttöön liittyy nykyään erittäin paljon tietoturvariskejä. Emme voi esimerkiksi ikinä olla varmoja siitä, että viesti jonka lähetämme jollekin, tulee todella luetuksi. Tärkeät viestit voivat jäädä lukematta jo pelkästään sen takia, että ne saattavat hukkua postien sekaan, jos käyttäjälle saapuu jatkuvasti uutta postia. Luotamme nykyään liikaa sähköpostin toimivuuteen ja siihen, että kun sähköposti on lähetetty eteenpäin, tärkeäkin asia on saatu näin hoidetuksi. Näin ei silti välttämättä ole, vaikka voimme olla siinä luulossa, että vastaanottaja on saanut viestimme. Vastaanottajaa kannattaa aina pyytää kuittaamaan tärkeät viestit, jolloin tiedämme niiden todella menneen perille. Useat postiohjelmat tarjoavat esimerkiksi automaattisia kuittausmekanismeja, joka lähettää viestin lähettäjälleen kun viesti on luettu. Jos ihminen on poissa esimerkiksi työpaikaltaan pidemmän aikaa, hän usein laittaa itselleen poissaoloviestin. Tämä viesti välittyy heti kaikille häntä tavoittaneille ilmoittaen, ettei hän ole tavoitettavissa tiettynä aikana. Näin lähettäjä tietää, ettei vastaanottaja ole ainakaan vielä lukenut hänen lähettämäänsä sähköpostia. (Järvinen 2002, 218–219.)

Useissa sähköposteissa on automaattinen roskapostifiltteri. Se suodattaa tulevaa postiliikennettä laittaen roskakoriin suoraan sellaiset viestit, joiden se tulkitsee olevan mainospostia tai muuta turhaa postia. Se havaitsee roskapostin erilaisten avainsanojen tai muiden tunnusmerkkien avulla. Ongelmia syntyy, jos seula on liian tiukka ja tärkeää postia päätyy vahingossa roskakoriin käyttäjän huomaamatta. Kannattaa siis silloin tällöin käydä katsomassa, mitä postia filtteri onkaan sinne roskalaatikkoon suodattanut. (Järvinen 2002, 218–219.)

Oheisessa kuvassa näkyy Mozilla Thunderbird – ohjelman sähköpostifiltteri.



Kuvio 8: Sähköpostin manuaalinen suodatus Mozilla Thunderbird -ohjelmassa

Sähköpostiviestit voivat myös päätyä vääriin käsiin esimerkiksi käyttäjän huolimattomuuden seurauksena. Kiireessä lähetetyt viestit voidaan vahingossa lähettää väärälle henkilölle ja arkaluontoistakin asiaa voi päätyä vääriin käsiin. Jos viesti on jo lähetetty, sitä ei voida kutsua takaisin. Ainoa tapa ehkäistä tätä, on lukea viesti ja sen vastaanottaja huolella ennen sen lähettämistä. On myös oltava huolellinen osoitteita kirjoittaessa, sillä sähköposti ei tiedä mihin osoitteeseen sen pitäisi mennä. Lähettäjällä voi mennä esimerkiksi .com- ja .fi-päätteet sekaisin, jolloin posti menee väärälle henkilölle. (Järvinen 2002, 219–221.)

Koska lähettäjä-kentän oikeellisuutta ei missään vaiheessa tarkisteta, emme voi varmalla tietää lähettäjän oikeaa henkilöllisyyttä. Varsinkin roskapostien lähettäjät käyttävät jatkuvasti toisten henkilöiden nimiä lähetellessään postejaan. Jos vastaajanottajaa haluaa lähettää vastauksen saamaansa huijauspostiin, se menee perille sille henkilölle, jolta vastaanottaja luuli alun perin viestin tulleen. Alkuperäisen viestin lähettäjä ei siis pysty kaappaamaan vastausviestiä itselleen. Jos epäilee lähettäjän aitoutta, on syytä kysyä asiaa ihan suoraan henkilöltä itseltään. Sähköpostiosoitteita pystyy rekisteröimään omaan käyttöönsä mielin määrin ja millä nimillä tahansa. Siksi on helppoa teeskennellä olevansa joku aivan toinen henkilö ja lähetellä viestejä tämän nimissä. (Järvinen 2002, 224–227.)

Sähköpostia itseään voidaan pitää suhteellisen luotettavana välineenä. Tieto kulkee valon nopeudella internetin runkoverkossa, jolloin siihen on lähes mahdotonta tarttua. Poikkeuksen muodostavat runkoverkkoa ylläpitävät operaattorit ja heidän kanssaan yhteistyötä tekevät tiedustelupalvelimet. Jos tiedustelupalvelua ei oteta huomioon, sähköpostin sisältä voi paljastua ulkopuolisille ainoastaan lähettäjän tai vastaanottajan päässä. Onkin tärkeää määritellä, kuka pääsee lukemaan mitäkin sähköposteja, jos sama osoite on käytössä usealla taholla. Myös tietenkin lähettäjän näppäilyvirhe voi vahingossa lähettää viestin vääriin käsiin. Tekniset ongelmat voivat myös vaarantaa sähköpostin luotettavuuden. Postijärjestelmiin voi tulla ohjelmavirheitä, jolloin postit menevät vääriin osoitteisiin. On myös syytä muistaa, että sähköposti ei katoa laatikosta vain klikkaamalla ”poista”. Roskakori pitää usein tyhjentää vielä erikseen ohjelmasta ja asetuksista riippuen. Yleensä roskakorinkaan tyhjentäminen ei poista viestejä tietokoneen kovalevyltä. (Järvinen 2002, 228–230.)

Sähköpostin turvaohjeita:

- lähettäjän nimitietoon ei voi luottaa. Tarkista lähettäjänimen aloitus, jos on vähäistäkään syytä epäillä sitä
- viesti on varmuudella mennyt perille vasta kun vastaanottaja kuittaa sen
- lähetä tärkeät viestit salattuina
- seisotko sanojesi takana? Kerran lähetetty posti voi kummitella vielä vuosienkin päästä, harkitse siis mitä lähetät
- ohjaa yksityiset viestit johonkin webmail- palveluun, niin ne pysyvät erillään työpaikan posteista eivätkä paljastu vahingossa
- salaamaton sähköposti on turvatonta viestintää. Mutta niin ovat faksit, kirjeet ja tekstiviestitkin.

(Järvinen 2002, 217.)

Sähköpostin käytön yleistyessä jatkuvasti, kasvaa samaa tahtia niin virusten kuin roskapostienkin määrä. Organisaatioissa olisi hyvä, että roskapostin suodatus olisi saanut työntekijöiden suostumuksen jopa työsopimuksessa, jolloin säännöt sähköpostiin liittyvistä turvallisuusasioista olisi kaikille samat ja muutenkin selkeät. Roskapostien levitessä niistä koituvat kustannukset maksaa aina viestin vastaanottaja, jolloin maksut esimerkiksi yrityksille voivat olla mittaviakin. Suuremmissa organisaatioissa roskapostin kappalemäärä nousee todella suureksi, jos postia tulee paljon. Ja varsinkin tällöin roskapostin suodattamiseen joudutaan käyttämään mittavia resursseja. Rahan lisäksi se vaatii ennen kaikkea aikaa, vaivannäköä, ohjelmistoja ja laitteita. (Laaksonen, Nevasalo & Tomula 2006, 206–209.)

Koska on vaarana, että roskapostinsuodatusohjelmat poistavat tärkeitä viestejä, kannattaa järjestää viestit niin, ettei ohjelma heti välittömästi poista niitä. Paras tapa on laittaa viestit

vaikka erilliseen kansioon kuin saapuneet viestit. Näin voidaan käydä tarkistamassa, ettei tärkeitä viestejä ole joutunut suodatusohjelman poistamaksi. (Laaksonen, Nevasalo & Tomula 2006, 209.)

Helpoin tapa torjua roskapostit, on estää osoitteen päätyminen roskapostilistalle. Jos osoite on sinne kerran joutunut, sitä ei saa sieltä enää poistettua. Roskapostiviesteihin ei saisi ikinä vastata vaikka niissä kysyttäisiin mitä tahansa. Jos ne lupaavat poistaa osoitteen listalta ja käyttäjä vastaa viestiin, roskapostin lähettäjä saa tiedon, että osoite on toiminnassa ja lähettää siihen yhä enemmän roskapostia. Joskus roskaviesteissä voi olla jopa puhelinnumeroita, joihin soittamalla muka pääsee eroon roskaposteista. Jos käyttäjä soittaa tällaiseen numeroon, voi luvassa olla mielettömän iso puhelinlasku. (Laaksonen, Nevasalo & Tomula 2006, 209.)

Yritysten olisi hyvä muistaa, ettei sähköpostiosoitteita kannattaisi suoraan ilmoittaa sen www-sivustoilla. Osoitteet kannattaa aina ilmoittaa muodossa etunimi.sukunimi@yritys.fi, etunimi.sukunimi [a] esimerkki.fi, tai laittaa se kuvatiedostona www-sivulle, koska sähköpostiosoitteiden etsintäohjelmat eivät osaa lukea kuvamuodossa olevaa tekstiä. Yritysten sähköpostiosoitetta tulisi käyttää vain yritystoiminnassa, ei käyttäjän henkilökohtaisten asioiden hoidossa. Organisaation sähköpostin käyttäjiä tulisi ohjeistaa ja kouluttaa riittävästi, jotta he saisivat tietoa turvallisesta sähköpostin käytöstä. (Laaksonen, Nevasalo & Tomula 2006, 209–210.)

Koska roskapostia ei voi varotoimista huolimatta kokonaan estää tulemasta sähköpostilaatikkoon, sitä pitäisi pystyä torjumaan mahdollisimman tehokkaasti. Useat sovellukset sisältävät kattavia listoja roskapostin lähettäjien osoitteista, jolloin nämä tietämällä voidaan estää postin tulo kyseisistä osoitteista. Roskapostien lähettäjät kuitenkin muuntelevat osoitteitaan, jolloin kattavan listan ylläpitäminen muuttuu mahdottomaksi. Roskapostinsuodatusohjelmat toimivat siten, että ne antavat pisteitä roskapostiin viittaavista elementeistä ja kun tietty pistemäärä ylittyy, se määrittelee tulleen postin roskapostiksi. Ne arvioivat otsikkoa, lähettäjää ja viestin sisältöä. Varsinkin yrityksille suositellaan käyttöönotettaviksi roskapostin suodatukseen tarkoitettuja sovelluksia. Suomen yritysmaailmassa suosituimpia sovelluksia ovat BorderWare, ChipherTrust, SpamKiller, IronPortSystems ja Symantec. Nämä kaikki ovat erittäin tehokkaita roskapostin torjumisessa. (Laaksonen, Nevasalo & Tomula 2006, 210–211)

Käyttäjät eivät voi luottaa täysin suodatusohjelmiin, jolloin heidän on itse myös oltava aktiivisia torjumaan ei-toivottua postia. Sähköpostiohjelmissa kannattaa:

- käyttää toimittajan tarjoamaa suodinta ja säätää sen taso riittävän korkealle

- käyttää suodattimen automaattista tai manuaalista päivitystä ohjelmistotoimittajan sivuilta tai yrityksen omalta päivityspalvelimelta
- käyttää sallittujen osoitteiden tai Windows-toimialueiden listaa tarpeellisten viestien poistamisen riskin minimoimiseksi
- käyttää ei-sallittujen lähettäjien listaa tunnettujen roskapostinlähettäjien torjumiseksi
- käyttää sallittujen osoitteiden listan automaattista päivitystä niiden osoitteiden osalta, joille käyttäjä lähettää viestin
- mahdollisesti estää muista kuin tietyistä maatunnuksista (esim.fi ja .com) tulevien viestien vastaanottaminen
- estää tarpeetonta koodausta ja merkistöä sisältävien viestien vastaanotto.

(Laaksonen, Nevasalo & Tomula 2006, 213.)

4.2 Sosiaalisen median tietoturva

Tietoverkkoja ja tietotekniikkaa yleisesti hyödyntävä sosiaalinen media on viestinnän muoto, johon liittyy tiedostojen, kuvien, videoiden ja muun digitaalisen sisällön jakaminen. Laurea näkee sosiaalisessa mediassa hyötyä esimerkiksi verkostoitumisessa, osaamisen kehittämisessä ja markkinoinnissa. Sosiaaliset mediat sisältävät paljon erilaisia työkaluja, joita käyttäjät voivat yleisesti hyödyntää niin ammatillisessa, kuin yleishyödyllisessä mielessä. Suurin osa sosiaalisten medioiden työkaluista on ilmaisia ja kaikkien saatavilla, mutta rajattujakin sovelluksia löytyy. Tällaiset ovat yleensä tietylle käyttäjäryhmälle rajattuja. (Sosiaalinen media.)

Sosiaalisen median tulevaisuutta ei voi kukaan ennustaa, mutta yritykset ja organisaatiot ovat jo löytäneet uusia jakelumalleja ja ansaintalogiikoita sieltä. Sosiaalisen median käyttäminen edellyttää, että käyttäjällä on hallussaan myös tietoturvapuoli. Edellä lista hyvistä vinkeistä:

- huolehdi, että sinulla on voimassaoleva haittaohjelmien suojaus tietokoneessa ja kännykässä
- valitse yksilöllinen ja monimutkainen salasana, joka ei ole ulkopuolisten arvattavissa
- älä käytä Laurean tietoverkon käyttäjätunnus/salasana – yhdistelmää sosiaalisen median välineissä
- älä hyväksy verkostoon tuntemattomia henkilöitä
- älä avaa epäilyttäviä linkkejä tai viestejä
- huolehdi omasta ja muiden yksityisyyden suojasta.

(Sosiaalinen media.)

Laurean tietoverkon ja – järjestelmien käyttösääntöjä tulee noudattaa, varsinkin Laurean verkossa, tai kun käytössäsi on Laurean omia työkaluja. Tietoturvasyistä voi myös olla mahdollista, että jotkin sosiaalisen median sivustot estetään it-palveluiden toimesta. Ennen sosiaali-

seen mediaan rekisteröitymistä, tulee käyttäjän ottaa selvää käyttöehdoista. Joissain sosiaalisen median palveluissa voi esimerkiksi oman kuvan tekijänoikeuden menettää sivustolle. Myös muiden ihmisten tekemien kuvien ja tekstien liittäminen sivustolle vaatii yleensä tekijän ja lähteen mainintaa. (Sosiaalinen media.)

5 SUOJAUTUMISKÄYTÄNNÖT

5.1 Päivitykset

Kaiken tietoturvan peruskivi on käyttöjärjestelmien säännönmukainen päivitys. Se, että päivitykset hoidetaan säännöllisesti, on kaiken muun turvallisen toiminnan edellytys. Päivittäminen pidentää tuotteen käyttöikää, ollen näin haitallinen palvelun valmistajalle. Usein valmistajilla on tapana jossain vaiheessa lopettaa kokonaan uusien päivitysten tarjoaminen tiettyyn ohjelmaan, jolloin asiakas joutuu ostamaan kokonaan uuden tuotteen. Joskus päivittäminen voi muodostua kuluttajalle jopa ongelmaksi, koska kaikkia laitteita ei voi päivittää itse ja laite saatetaan joutua viemään huoltoon. (Järvinen 2006, 15.)

Koko tietojärjestelmän kriittisin osa on käyttöjärjestelmä. Koska käyttöjärjestelmä sisältää kymmeniä miljoonia rivejä koodia, on mahdotonta, että se olisi ikinä kerralla kunnolla toimiva ilman yhtäkään turva-aukkoa tai ohjelmointivirhettä. Tämän vuoksi päivityksistä on tullut tietotekniikan arkipäivää jo aivan kaikille ”tavallisillekin” tietokoneen käyttäjille. Ennen Microsoftin tuloa päivityksistä vastasi vain alan ammattilaiset, nykyään jokainen voi päivittää oman Windowsinsa miten haluaa. (Järvinen 2006, 16.)

On hyvä ymmärtää ero päivittämisen ja versioiden vaihtamisen välillä. Tuotteen päivitys ei siis tarkoita, että koko versio vaihdetaan uuteen, vaan päinvastoin. Jos vaihdetaan kokonaan uuteen versioon, se johtaa usein siihen, että koko päivitysrumba kyseisen ohjelman ympärillä alkaa kokonaan alusta. Tämän vuoksi versiopäivityksiä on syytä välttää ja asentaa mieluummin ilmaisia, version sisäisiä päivityksiä. Kun tuotteen versio vaihdetaan uuteen, se myös luonnollisesti maksaa asiakkaalle. (Järvinen 2002, 75.)

Koska lähes jokainen tietokonetta käyttävä ihminen käyttää nykyään sähköpostia ja internetiä muutenkin, on ennen kaikkea huolehdittava niiden päivityksistä. Jatkuvaa päivitystä vaatii myös esimerkiksi sivulle upotettuja animaatiota toistava Flash Player-ohjelma. (Järvinen 2006, 16.)

Windowsin päivitys on oleellinen monelle käyttäjälle. Päivitystoiminnot ovat luonnollisesti muuttuneet eri Windows-versioissa. Ensimmäiset itse tehtävät päivitysominaisuudet tulivat Windows 98- version myötä. Sitä ennen päivitys hoitui vain ostamalla uuden version. Alussa

käyttäjän piti itse olla hyvin aktiivinen päivitysten suhteen, sillä ne eivät olleet automaattisia. Windowsilla huomattiin, että ihmiset olivat laiskoja päivittämään ohjelmiaan omaaloitteisesti, joten markkinoille tuli ohjelma joka tarkisti ajankohtaiset päivitykset automaattisesti ja tarjosi niitä asiakkaille. Näin ihmisten oli helpompi huomata uudet päivitykset ja asentaa ne omalle koneelleen. Tästä eteenpäin päivitykset ovat kehittyneet hurjaa vauhtia. Jo Windows 2000-versio tarkisti kaikki päivitykset automaattisesti ja jopa latasi ne automaattisesti kiintolevylle odottamaan käyttäjän itse tekemää asennusta. Päivityksistä, joita ei ollut asennettu, ei tietenkään ollut mitään hyötyä käyttäjälle. Tässäkin siis tarvittiin käyttäjän omaa aktiivisuutta. (Järvinen 2006, 18–20.)

Windows XP:n myötä päivitys tuli pakolliseksi ja käyttäjästä riippumattomaksi, koska oli huomattu, että käyttäjän aktiivisuuteen nojaavat päivitykset eivät yksinkertaisesti toimi. Päivitysohjelma ohjelmoitiin hakemaan itse uudet päivitykset ja asentamaan ne automaattisesti koneeseen. Ohjelma jopa tarvittaessa käynnistää tietokoneen uudestaan, jotta päivitykset saadaan toimimaan. Windows lähettää aktiivisesti viestejä käyttäjilleen, jolloin päivitysasennukset eivät voi jäädä huomioimatta. (Järvinen 2006, 20.)

Vaikka päivitykset ovat nykyään niin helpoksi tehtyjä ja automaattisia kuin mahdollista, niihin liittyy silti ongelmallisuuksia. Koska päivitykset ovat kooltaan suuria, jopa kymmeniä megatavuja, ne tarvitsevat toimiakseen nopeita yhteyksiä. Useimmat ohjelmat vaativat koneen uudelleenkäynnistyksen, joka saattaa muodostua ongelmalliseksi. Esimerkiksi käytettäessä samanaikaisesti joitain laskelmointi- tai tilastointiohjelmia, jotka voivat katketa kesken kaiken kun kone käynnistyy uudestaan. (Järvinen 2006, 20.)

5.2 Palomuurit

Organisaatioiden internet-suojaukset pohjautuivat alun perin kokonaan palomuurien toimintaan. Palomuurien ollessa edelleen tärkeässä asemassa, on niiden osa tietoturvan kokonaiskuvassa pienentynyt. Tilanne on muuttunut vuosien myötä. Nykyään palomuurien ohi on myös muita väyliä yrityksen tietoverkoissa. Esimerkiksi vieraan tuoma kannettava tietokone ottaa yhteyden langattomaan verkkoon, voi sen kautta päästää liikennettä ohi palomuurin. (Järvinen 2006, 105.)

Aikoinaan protokollat olivat porttikohtaisia, jolloin tietty portti sulkemalla saatiin koko palvelun käyttö estettyä. Nykyään porttia on helppo vaihtaa, eikä palveluiden sulkeminen ole niin yksinkertaista. Pahimpana epäkohtana voidaan pitää porttia numero 80, jota käytetään yleisesti internetin surffausta varten. Haitta- ja vakoiluohjelmat pystyvät näin ollen lähettämään tietonsa 80-porttia hyödyntäen. Tämä johtaa siihen, ettei palomuuri pysty erottamaan haittaohjelman lähettämää dataa normaalista verkkoliikenteestä. Jotta palomuuri voisi tunnistaa

datan, pitäisi jokainen ip-paketti erotella ja tutkia, onko se http-protokollan mukaista. (Järvinen 2006, 105.)

Kuva havainnollistaa, missä kohdassa palomuuri erottaa yrityksen verkon ja internetin.

Kuvio 9: Palomuuri erottaa yrityksen verkon ja internetin

Nykypäivänä palomuuri torjuu lähinnä hakkereita. Kun kyse on haittaohjelmista, on kyse yleensä käyttäjän tekemästä latauksesta, jolloin palomuurin on mahdotonta selvittää, onko kyseessä vahingossa vai tahallaan avattu yhteys. Aikoinaan palomuureilla oli helppoa rajoittaa työntekijöiden netin käyttöä, mutta ongelmaksi on koitunut se, että palomuuri pystyy tulkitsemaan ainoastaan salaamatonta liikennettä. Jos työntekijä ottaa esimerkiksi salatun yhteyden (https) välityspalvelimeen, ei palomuuri pysty mitenkään selvittämään, missä sivustoilla käyttäjä liikkuu. Https-portti voidaan sulkea, mutta samalla häviäisi todella moni hyödyllinen palvelu, esimerkiksi nettipankit. (Järvinen 2006, 106.)

5.2.1 Koneen suojaaminen palomuurilla

Palomuurilla voidaan suojata kokonaista sisäverkkoa tai ainoastaan yhtä kotikäyttäjän konetta. Palomuureilla saatava suoja liittyy lähinnä päivittämättömiin, tai löytämättömiin tietoturva-aukkoihin. Palomuuri suojaa myös inhimillisiltä konfigurointivirheiltä. Esimerkiksi tahatto-

masti auki jätetyt palvelut, tai jaetut kansiot on estetty verkon ulkopuolisilta palomuurin avulla. (Järvinen 2006, 109.)

Palomuurit voivat olla kokonaan erillisiä laitteita (rautapalomuuri), tai käyttöjärjestelmän sisällä toimivia sovellusmuureja (softapalomuureja). Molemmissa on hyötynsä ja haittansa. Paras malli hyödyntää sekä rauta- että softapalomuuria. (Järvinen 2006, 109.)

5.2.1.1 Rautapalomuuri

Rautapalomuurin etuihin kuuluu muun muassa luotettavuus. Palomuuri toimii piittaamatta tietokoneongelmista, eikä niihin pysty murtautumaan. Fyysistä palomuuria ei myöskään pysty kiertämään, eikä sammuttamaan ohjelmallisilla komennoilla. Hyötyihin kuuluu myös se, että ainoastaan yksi laite pystyy suojaamaan kokonaisen sisäverkon, jolloin säästytään myös konekohtaisilta konfiguroinneilta. (Järvinen 2006, 109–110.)

Kuvassa Juniper networksin SSG5 fyysinen palomuuri pienyrityksille.

Kuvio 10: Juniper SSG5, Rautapalomuuri pienyrityksille

Rautapalomuurin ominaisuuksiin kuuluu myös se, että se pysyy päällä myös silloin, kun kone vasta käynnistelee käyttöjärjestelmäänsä. Tällaisesta palomuuriasennuksesta saa myös helposti organisaatiota kiinnostavia lokitiedostoja ja muita kehitystrendejä. (Järvinen 2006, 109–110.)

Rautapalomuurin haittoihinkin lukeutuu monia asioita. Ensimmäisenä voisi mainita säätöjen ja käyttöönoton vaikeuden. Tämä johtaa siihen, että rautapalomuuri tarvitsee osaavan ylläpitohenkilön toimiakseen. Vaikka asetukset olisivat kerran saatu kohdilleen ja toimiviksi, voi kaiken joutua tekemään alusta palomuurin päivityksen jälkeen. (Järvinen 2006, 109–110.)

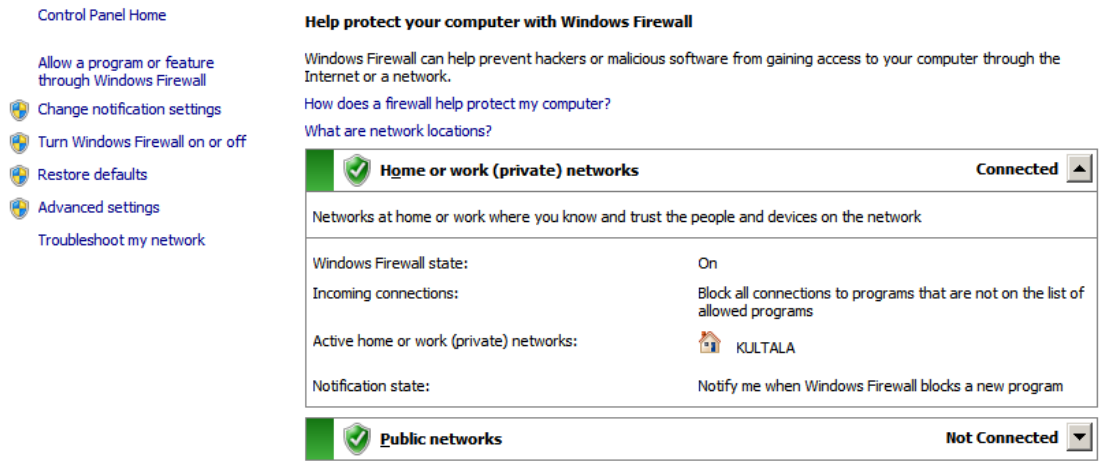
Rautapalomuurit ovat myös kalliita, joten yksityishenkilöille tai pienyrityksille niitä ei voi suositella. Tällaisissa tilanteissa voisi ajatella käyttöön wlan- ja adsl- ym. päätelaitteiden mukana tulevaa palomuuria. Näitä palomuuritoimintoja on lähes kaikissa kyseisissä laitteissa, ne pitää vain osata ottaa käyttöön. Rautapalomuuri ei anna myöskään minkäänlaista ilmoitusta itse käyttäjälle, vaan virheet ja ilmoitukset kerääntyvät lokiin, jota it-ylläpito voi tarkastella. (Järvinen 2006, 109–110.)

5.2.1.2 Softapalomuuri

Sovelluspohjaisiin palomuureihin liittyy monia etuja. Ne on muun muassa helppo ottaa käyttöön, ja käyttöjärjestelmissä onkin yleensä valmiina palomuuriominaisuus. Nämä pitää vain aktivoida ja konfiguroida toimiviksi. Softapalomuurit antavat myös välittömästi ilmoitukset epäilyttävästä liikenteestä. Näin ollen käyttäjän on helppo selvittää, mistä dataliikenteestä on kysymys. Esimerkiksi jatkuvat yhteydenotot samalta sovellukselta viittaavat päivityskutsuihin. (Järvinen 2006, 109–110.)

Haittojakin softapalomuureista löytyy. Esimerkkinä mainittakoon se, että ne ovat haavoittuvampia kuin fyysiset palomuurit. Softapalomuurit ovat normaaleita tietokonesovelluksia ohjelmointivirheineen. Palomuurin asetuksia voi näin ollen muuttaa ohjelmallisesti ja haittaohjelma saattaa avatakin itselleen aukon käyttäjän huomaamatta. Toinen haittapuoli on softapalomuurien liiallinen teknisyys peruskäyttäjälle. Kaikki eivät pysty päättelemään, ollaanko tilanteessa antamassa oikeutta sallitulle vai haittaohjelmalle. (Järvinen 2006, 109–110.)

Kuvassa on yleisesti Windowseista löytyvä softapalomuuri kotikäyttäjille.



Kuvio 11: Windows firewall, softapalomuuri kotikäyttäjälle

Sovelluspohjaiset palomuurit kuluttavat prosessoritehoja ja muistia, hidasten näin koko konetta. Palomuuri myös käynnistyy normaalisti muiden ohjelmien mukana, joten kone on suojaamaton ennen sitä. (Järvinen 2006, 109–110.)

5.3 Salasanakäytännöt

Salasana on yleisin tunnistamiskeino, koska se on halpa ja helppo toteuttaa. Muut tunnistamiskeinot ovat jo paljon kalliimpia. Salasanoissa on paljon epäkohtia, joista ehkä merkittävin on se, että jos käyttäjä unohtaa salasanansa, jonka jälkeen hän ei voi enää todentaa itseään järjestelmälle. Salasanatunnistus ei siis ole kovin luotettava tekniikka. (Järvinen 2002, 339–340.)

Salasanoja on hyviä ja huonoja, ja käyttäjien pitäisikin opetella millainen oikeastaan on hyvä salasana. Sellaisen keksiminen ei ole niin helppoa, kun voisi kuvitella. Useimmat laittavat salasanaksi esimerkiksi lemmikkinsä tai lapsensa nimen, tai oman syntymäaikansa. Se ei todellakaan ole kannattavaa, sillä salasana ei saisi sisältää mitään tuttua informaatiota kyseisestä henkilöstä. Myöskään käyttäjätunnus, eikä salasana saa missään nimessä olla samat. (Järvinen 2002, 339–340.)

Egg-pankin vuonna 2002 tekemän tutkimuksen mukaan vain 3 prosenttia käyttäjistä oli valinnut itselleen salasanan, joka ei kuulunut helposti arvattaviin kategorioihin. Näitä tutkimuksessa olivat esimerkiksi lasten nimet, käyttäjän oma syntymäpäivä, tai kumppanin nimi. Usein salasanat ovat myös liian lyhyitä. Mitä pidempi salasana on, sitä vaikeampaa sitä on kenenkään arvata. Usein ohjelmat, joihin salasanoja luodaan, ovatkin asettaneet salasanoille minimimerkki- ja formaattivaatimukset. (Järvinen 2002, 340–341.)

Nykyään salasanoja on joka paikassa niin paljon, että niiden muistaminen ja keksiminen voi olla hankalaa. Tällöin turvaudutaan usein yhteen salasanaan ja käyttäjätunnukseen, joita käytetään joka paikassa. Aina pitäisi pyrkiä käyttämään eri salasanoja ja myös vaihtamaan niitä riittävän usein. Useimmat lähiverkon salasanat on asennettu niin, että ne vanhenevat määrätyn ajan päätyttyä, jonka jälkeen salasana on pakko uusia. Usein vaihtoon on myös liitetty muisti, joka tallentaa edelliset salasanat, eikä hyväksy niitä enää uudelleenkäytettäväksi. Salasanan kuuluisi myös sisältää sekä isoja, että pieniä kirjaimia, sillä se moninkertaistaa ajan jonka Brute force-haku käyttää salasanan etsimiseen. Tätä tekniikkaa käyttävät ohjelmat kokeilevat jokaisen vaihtoehdon yksi kerrallaan, kunnes oikea salasana löytyy. Tällöin on lisäksi merkitystä sillä, että salasana on mahdollisimman pitkä. Niin ikään erikoismerkkien käyttö on suositeltavaa salasanoissa. (Järvinen 2002, 341.)

Me suomalaiset käytämme mielellämme ääkkösiä ja miksei niitä voisi myös käyttää salasanoissa. Ongelmaksi voi muodostua silloin se, että ohjelma ei pidä ääkköstä aakkosmerkkinä, eikä tästä syystä hyväksy sitä salasanaksi. Lisäksi koneessa pitää olla asennettuna suomenkielinen näppäimistöajuri, jolloin ääkkösiä voidaan kyseisellä näppäimistöllä edes kirjoittaa. (Järvinen 2002, 341–342.)

Organisaatioissa ja yrityksissä salasanojen kanssa törmätään ongelmaan, kun tärkeimpiä tietoja sisältävät tiedostot ovat salasanojen takana, jolloin salasana ei voi olla vain yhden ihmisen tiedossa. Niin sanottua jaettua salasanaa voidaan käyttää, jolloin lähiverkossa luodaan useita tunnuksia joihin ylläpidolla on täydet käyttöoikeudet. Jos kaksi tai useampi varaylläpitäjää syöttää osan salasanasta tietämättä toistensa valitsemia sanoja, he voivat ylläpitäjän ollessa estynyt, muodostaa yhteisesti omista sanoistaan salasanan ja päästä näin ylläpitäjäksi ja saada tämän oikeudet. (Järvinen 2002, 343.)

Salasanoihin siis liittyy paljon riskejä. Vaikka on koetettu valita mahdollisimman pitkä ja hyvä salasana, voi se kääntyä käyttäjän kohtaloksi tämän unohtaessa sen. Salasanan voi toki kirjoittaa itselleen jonnekin muistiin, mutta paikka pitää vähintään olla erillään tietokoneesta. Tämä ei kuitenkaan poista sitä riskiä, että salasana joutuu vääriin käsiin. Harva tulee myöskään ajatelleeksi, että joku voi katsoa vierestä sillä välin, kun käyttäjä kirjautuu järjestelmään. Salasana muodostuu kenttään yleensä tähtinä juuri sen takia, ettei sitä kukaan näe suoraan näytöltä. (Järvinen 2002, 344.)

Troijalaiset virukset voivat asentaa koneisiin takaportteja tai vakoiluohjelmia, jotka tallentavat itseensä jokaisen koneella tehdyn näppäilyn. Tämä paljastaa kirjoitetun salasanan suoraan vakoilijalle. Tämän vuoksi vierailla koneilla omien salasanojen käyttäminen on aina riski. (Järvinen 2002, 344.)

Meille kaikille on varmasti tuttu myös pankkien käyttämä salasanajärjestelmä, jossa salasanat ovat kertakäyttöisiä. Ei siis ole haittaa, jos salasana paljastuu, koska sitä ei enää ikinä käytetä uudelleen. Kertakäyttöinen salasana siis vanhenee välittömästi, kun se on näppäilty järjestelmään. Tällöin salasanakenttää ei tarvitse edes peittää tähdillä siinä pelossa, että joku näkee näppäillyn salasanan. Salasana ei toimi yksinään, vaan siihen pitää aina yhdistää käyttäjätunnus. Nämä yhdessä avaavat lukon, jolla käyttäjä pääsee käsiksi pankkipalveluihinsa. Aina vaihtuvan salasanan lisäksi kysytään vielä käyttäjän omaa henkilökohtaista salasanaa. Tämä käytäntö on siis melko turvallinen, mutta vain silloin, kun käyttäjätunnusta ja salasanoja ei säilytetä samassa paikassa. (Järvinen 2002, 345–346.)

Vakiosalasana tai käyttäjätunnus olisi hyvä olla vain käyttäjänsä päässä, eikä missään ylhäällä kirjoitettuna. Kertakäyttösalasanojen miinuspuolena on muun muassa se, että listaa pitää

aina kantaa mukanaan, jos haluaa mennä verkkopankkiinsa muualta kuin kotikoneelta. Salasanalistat luonnollisesti myös kuluvat loppuun, koska salasanat ovat kertakäyttöisiä. Tällöin niitä pitää tilata pankilta lisää. (Järvinen 2002, 345–346.)

Laurea käyttämät salasanakäytännöt ovat normaalia monimutkaisemmat. Keskitetyt salasanat täytyy olla vähintään 8 merkkiä pitkiä ja enenintään 14 merkkiä pitkiä. Salasanan tulee myös sisältää kolme seuraavasta neljästä kohdasta:

- pieniä kirjaimia (esim. a, b, c..)
- isoja kirjaimia (esim. A, B, C..)
- numeroita (1, 2, 3...)
- jotain seuraavista erikoismerkeistä (@ # $ % & / *).

(Salasanat.)

Salasana ei Laurean tapauksessa saa sisältää ääkkösiä, eikä erikoismerkkejä joita ei löydy yllä olevasta listasta. (Salasanat.)

6 OHJEITA VERKON TURVALLISEEN KÄYTTÖÖN

Yrityksissä ja organisaatioissa olisi syytä laatia selkeät säännöt ja käytännöt siitä, miten verkkopalveluja käytetään ja minkä palveluiden käyttöä on rajoitettu. Jos selaamista halutaan rajoittaa merkittävästi, organisaation tulee osoittaa selkeästi, mitkä palvelut ja sivut ovat kiellettyjä ja huolehtia käyttäjien informoimisesta. Yksityisen henkilön selaamia internetsivuja ei saa lain mukaan tutkia. Joten jos yritys haluaa rajoittaa internetsivuilla käyntiä, on se mahdollista määrittelemällä ne sivut, joilla ei saa kyseisellä koneella surffata. Henkilökuntaa olisi hyvä opastaa selkeästi siitä, minkälainen käyttö ei ole sallittua. Lakipykälät tulee ottaa huomioon ja muistaa, että tiedostojen laiton jako tai laittoman materiaalin hallussapito ovat laissakin kiellettyä. Olisi myös hyvä muistaa, että työpaikan koneet ovat työn tekemistä varten, eikä henkilökohtaisten asioiden hoitamista varten. Organisaatiossa voidaan siis rajoittaa käyttäjiensä käyttöoikeuksia säännöillä. Esimerkiksi omilla henkilökohtaisilla sivuilla ei saa vierailla työajalla. Aina on vaarana, että näiltä sivuilta tarttuu koneelle jokin haittaohjelma, josta voi olla haittaa yrityksen tietokoneelle. (Laaksonen, Nevasalo & Tomula 2006, 163–165.)

On olemassa laki yksityisyyden suojasta työelämässä, joka määrittelee esimerkiksi työnantajan oikeudet ja mahdollisuudet työntekijän sähköpostin avaamiseen. Usein yrityksissä suositellaan, että yrityspostia saa käyttää vain työasioiden hoitoon. On suotavaa, että omat henkilökohtaiset asiat hoidettaisiin käyttäen muita viestintämahdollisuuksia kuin yrityksen sähköpostia. (Laaksonen, Nevasalo & Tomula 2006, 165–166.)

Sähköpostin käyttöohjeistuksessa olisi hyvä huomioida seuraavia asioita:

- sähköpostiosoitteiden julkaiseminen ja esitystapa esimerkiksi yrityksen www-sivulla
- menettelytavat työntekijän sairastuessa
- menettelytavat työntekijän ollessa poissa töistä pidempään esimerkiksi äitiysloman tai vuorotteluvapaan takia
- toiminta henkilön irtisanoutuessa
- henkilökohtaisten sähköpostiviestien käsittely
- väärään osoitteeseen saapuneen sähköpostiviestin käsittely
- perille menemättömän sähköpostin käsittely
- sähköpostin salaus
- sähköpostin liitetiedostojen käsittely
- roskapostin käsittely.

(Laaksonen, Nevasalo & Tomula 2006, 166.)

Salasanoihin liittyvät ohjeistukset tulee olla niin selkeitä ja lyhyitä, että ne on helppo ymmärtää. On syytä pohtia miten käyttäjät saadaan noudattamaan annettuja ohjeita. Salasanaohjeistuksessa olisi hyvä ottaa huomioon muun muassa seuraavia asioita:

- ohje turvallisen salasanan muodostamiseksi
- oletussalasanojen muuttaminen välittömästi sovellusta käyttöönotettaessa
- salasanan vaihtaminen ja siihen liittyvät käyttäjän huoleksi jäävät toimenpiteet
- ohje, miten tulee toimia tilanteessa kun salasana katoaa, joutuu vääriin käsiin tai se syötetään väärin liian monta kertaa.

(Laaksonen, Nevasalo & Tomula 2006, 167.)

Organisaatioissa olisi hyvä muistaa niin sanottu puhtaan pöydän periaate. Jokaisen vastuulla on siivota työpisteensä päivän päätteeksi. Se tarkoittaa papereiden pois keräämistä, tulosteiden ja muiden dokumenttien huolehtimista omille paikoilleen. Yrityksissä ja organisaatioissa liikkuu monenlaista väkeä, aina siivoojista oppilaisiin ja työntekijöihin. Kun jokainen huolehtii omien tavaroidensa poisviemisestä, niin riski tietojen päätymisestä vääriin käsiin minimoituu. Esimerkiksi siivoojat voivat nähdä vahingossa sellaista tietoa, mitä ei ole tarkoitettu heidän silmilleen. Kun tiedostot on asianmukaisesti dokumentoitu, myös työnteko on kaikin puolin mukavampaa ja sujuvampaa. Yrityksissä on myös hyvä muistaa se tosiasia, että jos salaisia papereita pidetään arvattavissa paikoissa työpaikoilla, se voi vaarantaa koko yrityksen salassapidon. (Laaksonen, Nevasalo & Tomula 2006, 169–170.)

Organisaatioissa on syytä varautua siihen, että tulee jokin onnettomuus, jolloin tärkeää tietoa voi kadota. Tällöin on syytä panostaa tietojen varmistamiseen. Helpoimmin tämä onnistuu,

jos kaikki ohjelmat ja tiedostot on ohjelmoitu oletusarvoisesti tallentumaan varmistettaville verkkokovalevyille, joissa tietenkin tulee olla riittävä tallennuskapasiteetti. Koska kaikkea tietoa ei voi mitenkään varastoida, on syytä määritellä, mikä tieto on tärkeää säilyttää ja mikä ei. (Laaksonen, Nevasalo & Tomula 2006, 170–171.)

7 YHTEENVETO

Alun perin tarkoituksenamme oli tehdä tietoturvaa käsittelevä kirja. Aihetta enemmän pohdittuamme ja opinnäytteen ohjaajien kanssa keskusteltuamme, totesimme aiheen olevan liian laaja. Halusimme myös sisällyttää työhön jonkinlaisen tutkimusmenetelmän. Idea tietoturvaoppaasta kouluisännille syntyi, kun ohjaajamme sitä ehdottivat. Kävi ilmi, ettei isännillä vastaavanlaista opasta ollut. Saimme myös tietää, että isänniltä kyseltiin usein tietoturvaan liittyviä kysymyksiä, vaikka kyseisiin aiheisiin vastaaminen ei kuulukaan heidän työnkuvaansa. Syntyi siis idea tehdä selkeälukuinen opas, josta saisi vinkkejä yleisimpiin ongelmiin ja kysymyksiin. Aiheen laajuuden vuoksi oppaassa käsitellään asioita melko pintapuolisesti ja olemme yrittäneet käsitellä sellaisia aiheita, jotka laurean kannalta ovat oleellisia. Kouluisännät antoivat vapaat kädet oppaan tekoon, joten saimme itse päättää oppaan sisältämät aiheet.

Oppaan teko oli erittäin haastavaa ajanpuutteen vuoksi, sekä ajankohtaisten ilmaisten kirjallisten lähteiden löytäminen vaikeaa. Halusimme käyttää enemmän kirjoja lähteinä, kuin esimerkiksi verkkojulkaisuja koska mielsimme ne luotettavammiksi. Työ kattaa meidän mielestämme tärkeimmät sektorit tietoturvasta kouluisäntien kannalta katsottuna.

Kun alkuperäisenä ongelmana pidetään sitä, että kouluisännät tarvitsevat lisää informaatiota tietoturvasta, niin opas ei korjaa asiaa kokonaan. Tämä opas on vain pintaraapaisu tietoturvan maailmaan, joten kouluisäntien olisi syytä saada perehdytystä tietoturvaan myös jatkuvan koulutuksen muodossa. Pidämme opasta kuitenkin selkeälukuisena ohjenuorana kouluisäntien yleiseen käyttöön. Tekstiä on helppo ymmärtää ja halutessaan lisätietoa aiheista voi etsiä alan kirjallisuudesta tai internetistä.

LÄHTEET

Hakala, M & Vainio, M & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland.

Henkilöstöturvallisuus
Viitattu 9.2.2011
http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html

Järvinen, P. 2006. Paranna tietoturvaasi. Jyväskylä: Docendo Finland.

Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä: Docendo Finland.

Laaksonen, M & Nevasalo, T & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing.

Laitteistoturvallisuus
Viitattu 28.2.2011
http://www.tietojesiturvaksi.fi/content/laitteistoturvallisuus

Ruohonen, M. 2002. Tietoturva. Jyväskylä: Docendo Finland.

Salasanat
Viitattu 1.3.2011
https://intra.laurea.fi/intra/fi/05_it_palvelut/04_ohjeet/02_it_ohjeet/Opiskelijoiden_SSL-VPN_Ohjeistus/index.jsp

Sosiaalinen media
Viitattu 1.2.2011
https://intra.laurea.fi/intra/fi/01_laurea/05_laurea_osio5/01_Verkkotyovalineet/04_some/index.jsp

Ssl-vpn ohje opiskelijoille
Viitattu 10.3.2011
https://intra.laurea.fi/intra/fi/05_it_palvelut/04_ohjeet/02_it_ohjeet/Opiskelijoiden_SSL-VPN_Ohjeistus/index.jsp

Tietoaineiston turvallisuus.
Viitattu 18.2.2011.
http://www.tietojesiturvaksi.fi/content/tietoaineiston-turvallisuus.

KUVAT