Tietoturvallisuus

Mikko Vestola
AT2-kurssin itsenäinen harjoitustyö
Koulun nimi
20.5.2002
Arvosana: Erinomainen

Sisällysluettelo

1 Johdanto

Tietoturvalla tarkoitetaan yleensä tietojen suojaamista mm. rikoksia ja tallennuslaitteiden vaurioitumista vastaan. Kotikäyttäjän kannalta tärkeimpiä toimenpiteitä ovat viruksilta suojautuminen ja varmuuskopioiden tekeminen. Yrityskäytössä taas täytyy vielä luoda menetelmät, jolla tärkeät tiedot suojataan ulkopuolisilta.

Tietokoneiden avulla luodaan valtavia määriä informaatiota, joka tallennetaan tietokoneen massamuisteihin. Yrityskäytössä tietokoneeseen saattaa parissa viikossa kertyä tietomäärä, jonka arvo voi olla jopa suurempi kuin itse tietokoneen. Myös kotikäytössä viikkojen tai jopa muutamien vuosien työn katoaminen tietovahingon seurauksena olisi lähes katastrofi.

Internetin käytön nopean kasvun myötä tietoturvalla on tärkeä merkitys nyky-yhteiskunnassa. Internet kattaa lähes kaikki yhteiskunnan toiminta-alueet. Esimerkiksi kaupankäynnin ja pankkipalvelujen siirtyminen verkkoon lisäävät tietoturvan merkitystä.

Lähde: (Tietokoneen käyttötaito 1 s. 40)

2 Internetin vaarat

2.1 Tietokonevirukset

Tietokonevirus on ilkivaltainen ohjelma, joka on ohjelmoitu levittämään itseään tietokoneesta toiseen mahdollisimman huomaamattomasti levykkeiden tai netin välityksellä. Joskus virus ilmoittaa olemassaolostaan näyttämällä ruudulla outoja viestejä tai kuvia tai sitten virus vain pysyy piilossa. Tavallisesti virus on ohjelmoitu aktivoitumaan tietystä tapahtumasta, esim. päivämäärästä tai tietokoneen riittävän monen käynnistyskerran jälkeen.

Aktivoituessa virukset tekevät monenlaisia asioita. Harmittomimmat kirjoittelevat ruudulle pilaviestejä tai tekevät hauskaksi tarkoitettuja temppuja, mutta pahimmat virukset voivat hävittää tiedostoja tai sotkea koko kiintolevyn käyttökelvottomaksi. Tietokoneviruksen voi saada netin, sähköpostin tai esim. levykkeen välityksellä yleensä avaamalla exe-päätteisen tiedoston ja näin virus käynnistyy. Sähköpostiviruksen leviäminen vaatii liitetiedoston klikkaamista, mutta jotkut virukset kuten Nimda hyödyntävät esim. Microsoft Outlookin bugeja, jossa virus muuttaa päivittämättömän sähköpostiohjelman asetuksia siten, että liitetiedostot avautuvat automaattisesti.

Virukset voivat tarttua myös vain netissä surffatessa esim. Java-sovelmien tai ActiveX-komponenttien kautta. Saastuneen ActiveX-koodin voi kuka tahansa asentaa www-sivulleen ja kun käyttäjä on sallinut selaimensa käyttää ActiveX-komponentteja niin kun sivut ladataan selain lataa koodin sisältävän ohjelman koneeseen ja seuraavalla käynnistyskerralla virus asentaa itsensä kiintolevylle.

Lähde: (Tietokoneen käyttötaito 1 s. 40, Tekniikan Maailma 7/1999 s.60-61)

2.1.1 Ensimmäiset virukset 1980-luvun lopulla

Tietokoneviruksen tekijä on aina ihminen. Ensimmäiset pc-virukset havaittiin vuonna 1986 ja sen jälkeen virushavaintoja on tehty melko tiuhaan tahtiin. Ensimmäinen kuuluisa Internet-virus syntyi vuonna 1988 kun yhdysvaltalainen Robert Morris kirjoitti yksinkertainen ns. madon, saadakseen selville montako konetta Internetiin oli tuolloin kytketty. Väärään paikkaa ajautuneen desimaalipilkun takia ohjelma kuitenkin kopioi itsensä tuhansia kertoja jokaiselle palvelimelle, kaataen kymmenen prosenttia Internetin palvelimista.

Lähde: (Tietokoneen käyttötaito 1 s. 40, MikroBitti 3/2002 s.54)

2.2 Erityyppisiä tietokoneviruksia

2.2.1 Tiedostovirus

Tiedostovirukset aktivoituvat ja kopioivat itseään aina käynnistyttyään. Virus jää tietokoneen keskusmuistiin ja kiinnittää itsensä muihinkin käynnistettäviin ohjelmiin. Ilkeimmät tiedostovirukset tuhoavat jokaisen saastuttamansa tiedoston, jolloin virustutkastakaan ei ole apua. Tämänlainen virus leviää todella nopeasti esim. ohjelmakopioiden välityksellä.

Lähde: (Tietokoneen käyttötaito 1 s. 41, MikroBitti 2/2002 s. 36-39)

2.2.2 Käynnistyslohkovirus

Käynnistyslohkovirus tallentaa itsensä kiintolevyn tai levykkeen käynnistyslohkoon, tällöin virus aktivoituu jo ennen käyttöjärjestelmää ja mahdollista virustutkaa. Käynnistyslohkovirus voi tartuttaa koneeseen esimerkiksi silloin, kun tietokoneen levykeasemaan on jäänyt viruksen saastuttama levyke. Jos tietokone on määritelty käynnistymään ensin a-asemalta, virus pääsee automaattisesti levykkeen käynnistyslohkolta tietokoneen kiintolevylle.

Lähde: (MikroBitti 2/2002 s. 36-39)

2.2.3 Makrovirus

Makrovirus on toteutettu sovellusten omilla makro-ohjelmointikielillä kuten Microsoftin Wordin tai Excelin. Makrovirus käynnistyy esim. tekstinkäsittelyohjelmassa makroja ajaessa. Makroviruksen tekee erityisen vaaralliseksi se, että ne toimivat kaikissa niissä käyttöjärjestelmissä, jossa kyseessä olevaa ohjelmaa voidaan käyttää. Makrovirukset leviävät usein sähköpostin liitetiedostojen välityksellä ja ne kiusaavat lähinnä Microsoftin toimisto-ohjelmien käyttäjiä.

Lähde: (Tietokoneen käyttötaito 1 s. 41, Tekniikan Maailma 6/2000 s. 38-44)

2.2.4 Mato

Viruksista madot ovat aiheuttaneet viime aikoina huolta eri puolilla maailmaa. Mato on virusohjelma, joka kopioi itseään automaattisesti ja siirtyy tietokoneesta toiseen verkkoyhteyksien välityksellä. Mato hakeutuu yleensä mikron keskusmuistissa tai kiintolevyllä oleviin tyhjiin kohtiin ja alkaa täyttää niitä. Lopulta mato voi pysäyttää koko tietokoneen toiminnan. Madot eivät itse tuhoa tiedostoja. Ne leviävät yleensä sähköpostin liitetiedostojen välityksellä.

Lähde: (Tietokoneen käyttötaito 1 s. 41, MikroBitti 2/2002 s. 37)

2.2.5 Troijan hevonen

Troijan hevosta ei yleensä luokitella tietokonevirukseksi, mutta sekin voi saada pahaa jälkeä aikaan. Troijan hevonen on vaarattomaksi ohjelmaksi naamioitu virus, joka voi olla naamioitunut muun muassa näytönsäästäjäksi tai peliksi. Kun ohjelma käynnistetään, virus alkaa esim. formatoimaan kovalevyä. Troijan hevonen ei lisäänny itsekseen vaan leviää kopioidun ohjelmatiedoston välityksellä yleensä Internetin kautta.

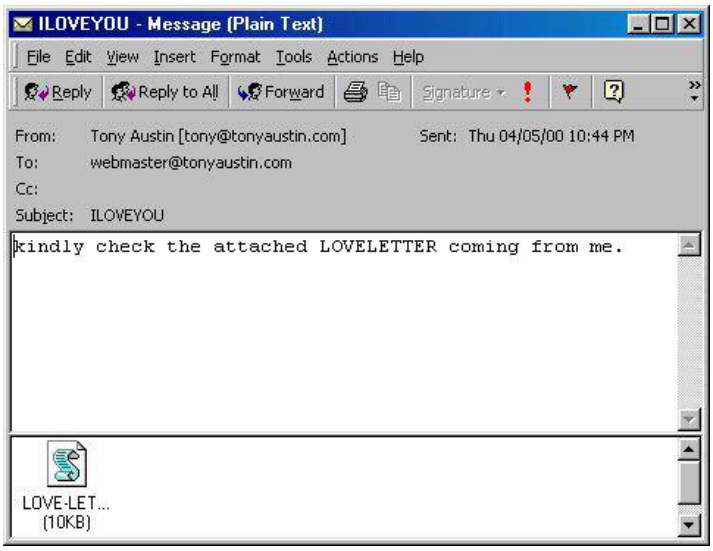
Lähde: (Tietokoneen käyttötaito 1 s. 41, MikroBitti 1/2002 s. 32-34)

2.3 Erityisen harmilliset tietokonevirukset

Kaikkien aikojen pahimpia tietokoneviruksia ovat olleet: **LoveLetter** (löydetty 4.5.2000), **Melissa** (26.3.1999), **Nimda** (18.9.2001), **Code Red** (heinäkuu 2001) ja **CIH** (elokuu 1998). Seuraavassa on esitelty pari tunnetuimpaa tietokonevirusta.

2.3.1 Maailman laajimmin levinnyt virus: LoveLetter

Vuonna 2000 räjähdysmäisesti 15 miljoonaan koneeseen levinnyt LoveLetter –viruksen voisi kuvitella jo herättäneen tietokoneen käyttäjät sähköpostiviruksien varalta, mutta yhä monet lankeavat ansaan ja saavat koneeseensa LoveLetter –viruksen. LoveLetter levisi sähköpostin vbs-päätteisen liitetiedoston välityksellä. Asiaa pahensi se, että LoveLetter osasi hyödyntää Outlookin osoitteistoa lähettämällä kopion itsestään jokaiseen sähköpostiohjelman osoitekirjan osoitteeseen. Joten aina kun joku sai LoveLetterin, se näytti tulevan tutun ihmisen sähköpostiosoitteesta, eikä kukaan osannut epäillä mitään.



LoveLetter kiusasi mm. nimeämällä tiedostoja uudestaan ja piilottamalla tiedostoja. Alkuperäinen LoveLetter uhkasi kuva- ja äänitiedostoja. Jotkut LoveLetterin variaatiot yrittivät estää tietokoneen käynnistymistä sotkemalla ini-asetustiedostoja. LoveLetterin vahingot ovat kuitenkin onneksi jääneet melko pieniksi, mutta pientä harmia se sai aikaan sitäkin enemmän. Yleensäkin nämä ns. hittivirukset leviävät nopeasti ja unohtuvat sitten.

Lähde: (MikroBitti 3/2002 s. 56-57, Tekniikan Maailma 11/2000 s.58-59)

Tällainen on LoveLetterin sähköpostiviesti ja liitetiedostoa klikkaamalla saa koneeseen viruksen.

2.3.2 Monimutkainen Nimda -tietokonevirus

Hyvä esimerkki pahaa jälkeä saaneesta viruksesta on vähän aikaa sitten ympäri maailmaa riehunut Nimda-virus. Nimda levisi yleisesti sähköpostiliitteiden välityksellä, mutta se käytti myös muiden hyökkäysohjelmien jättämiä takaportteja. Kohteena olivat päivittämättömät palvelimet.

Saastuneilta palvelimilta käyttäjälle saatettiin esittää www-sivu, jossa pyydettiin lataamaan Nimdan sisältämä Outlook-tiedosto. Näin käyttäjä saattoi siirtää viruksen itselleen ajattelemattomuuttaan. Virus yritti myös lisätä palvelimen www-sivulle JavaScript-koodia, joka taasen tartuttaisi tietoturva-aukkoja sisältävän selaimen. Näin virus hyödynsi palvelinten bugeja, käyttäjien hyväuskoisuutta sekä käyttäjän ja ylläpitäjän laiskuutta ohjelmistojen päivityksessä.

Nimda oli leviämisteholtaan poikkeuksellisen tehokas ja tämän madon kehittämiseen oli uhrattu paljon aikaa. Nimda yhdisti monta toimintoa ja se häiritsi vakavasti useiden yhtiöiden verkkoliikennettä ja aiheutti taloudellista vahinkoa pitkin maailmaa. Ja Nimdan nopeuskin oli aivan uskomaton: se tartutti viruksen kolmessa päivässä 500 000:n tietokoneeseen.

Nimda-viruksen tausta on tuntematon. Sen tekijää ei tiedetä, mutta viruksien asiantuntijat arvelevat, että se on selvästi ammattimaista tasoa ja tekijällä on ollut selvä tavoite. Koodia on testattu laboratorioympäristössä, joka vaatii rahaa. Herää väkisinkin kysymyksiä: kuka/ketkä, miksi ja minkä takia?

Lähde: (MikroBitti 3/2002 s. 54-55)

2.4 Hakkerit

Internet on levitessään ja laajetessaan tuonut hyötyjen lisäksi myös lieveilmiöitä. Internetistä on tullut erilaisten hakkerien temmellyskenttä. Laajakaistaisten internet-yhteyksien yleistyminen on runsaasti Internetiä käyttävien ihmisten mieleen. Kiinteän kuukausimaksun turvin konetta voi pitää verkkoon liitettynä ympäri vuorokauden, jolloin esim. satunnaisen sähköpostin tarkasteluun ei aina tarvitse käynnistää koko konetta.

Jatkuvasti auki olevalla yhteydellä on kuitenkin myös haittapuolensa: Tietoliikenneyhteys on samalla koko ajan avoin myös toiseen suuntaan. Tätä yhteyttä pitkin voi joku pahanilkinen sielu täysin huomaamatta murtautua käyttäjän koneelle tekemään tuhojaan. Hakkerit tunkeutuvat muiden tietokoneisiin yleensä hyödyntämällä Windowsin tai www-selaimen tietoturva-aukkoja.

Modeemikäyttäjät jäävät yleensä hakkereilta rauhaan, sillä modeemiyhteys on hidas ja ei ole aina auki. Hakkerit voivat kuitenkin saada pahaa jälkeä aikaan, erityisesti yrityksille. Käyttäjän koneelle tunkeutunut vieras voi vaikka tutkailla tiedostojasi, ujuttaa koneellesi virus tai poistaa tärkeimpiä tiedostoja. Tunkeutuja voi saada koneeltasi tietoonsa myös käyttäjätunnuksia ja salasanoja. Varastettujen tunnuksien avulla hakkeri voi jatkaa hankaluuksien aiheuttamista ja sillä kertaa jäljet johtavat käyttäjään, jolta salasanat varastettiin.

Hakkeri voi myös tehdä käyttäjän koneesta huomaamatta maailmanlaajuisen nettihyökkäyksen välikappaleen. Ns. palvelunestohyökkäyksissä murtautuja ujuttaa tuhansiin koneisiin ympäri maailmaa pienen huomaamattoman ohjelman, joka sitten tiettynä aikana alkaa pommittaa yleensä jotain suurta julkista palvelinta turhalla liikenteellä. Riittävän monen koneen voimin suurinkin palvelu saattaa kaatua ylivoimaisen liikennemäärän edessä.

Lähde: (MikroBitti 5/2002 s.44-47)

3 Suojautuminen

3.1 Viruksilta suojautuminen

Eräs tärkeimmistä toimenpiteistä virustartunnan varalta on ottaa varmuuskopiot tärkeistä tiedostoista. Jos tiedostot ovat isoja, kannattaa ne kopioida CD:lle tai ZIP-levylle. Varmuuskopiot tulisi ottaa säännöllisesti ja säilyttää muualla kuin omalla koneella. Tuhoisimmat virukset kun voivat tehdä koko kiintolevyn käyttökelvottomaksi.

Varmuuskopioita kannattaa ottaa myös jo saastuneista tiedostoista, sillä jälkikäteen niitä voi yrittää puhdistaa yksi kerrallaan. Makroviruksilta voi suojautua estämällä esim. Microsoft Wordia käyttämästä makroja. Vieraita Wordin doc-tiedostoja ei kannata avata elleivät ne tule varmasta lähteestä. Doc-tiedostot kannattaakin tallentaa rtf-muotoon, joka ei sisällä makroviruksia.

Ehkä paras tapa suojautua viruksilta on käyttää hyvää virustorjuntaohjelmaa. Hyviä virustorjuntaohjelmia saa myös ilmaiseksi netistä. Kuten esimerkiksi AntiVir, joka on helppokäyttöinen ja ilmainen.

Viruksen löytyminen koneelta näkyy esim. tällaisena ilmoituksena.

Virustorjuntaohjelma on ohjelma, joka tutkii kiintolevyn tiedostot kun käyttäjä haluaa tai sitten ajastetusti esim. kerran viikossa. Torjuntaohjelma etsii ohjelmista virusten ns. sormenjälkiä eli ohjelmakoodia, jonka perusteella virus sitten tunnistetaan. Joissakin virustentorjuntaohjelmissa on ns. heuristinen tarkistus, jolloin tiedostoista etsitään piirteitä, jotka viittaisivat viruksiin, mutta tämän menetelmän huonona puolena on se, että ohjelma voi antaa usein vääriäkin hälytyksiä.

Kun virustorjuntaohjelma löytää viruksen, annetaan käyttäjän yleensä valita, mitä viruksen saastuttamalle tiedostolle tehdään. Yksi vaihtoehto on tiedoston puhdistaminen, jolloin torjuntaohjelma yrittää irrottaa tiedostosta viruskoodin. Jotkut virukset kuitenkin osaavat tuhota osan saastuttamastaan tiedostosta, jolloin puhdistaminen ei välttämättä onnistu. Tällöin ainoaksi vaihtoehdoksi jää tiedoston poistaminen.

Jotkut virustorjuntaohjelmat tarjoavat jopa sellaista vaihtoehtoa, että saastunut tiedosto lähetetään torjuntaohjelman valmistajalle tutkittavaksi, jolloin tiedoston voi saada takaisin ehjänä jo muutamassa tunnissa.

Torjuntaohjelma tunnistaa viruksen käyttämänsä tietokannan perusteella, jossa on tiedot kaikista ohjelman tuntemista viruksista. Jos tietokanta on vanha, voi viruksen saastuttama tiedosto jäädä kokonaan havaitsematta. Tämän takia onkin tärkeää, että virustorjuntaohjelmaa päivitettäisiinkin ainakin kerran viikossa. Päivityksen voi yleensä tehdä helposti netin kautta ja sen saa toimimaan myös automaattisesti. Uusi viruksia tulee kuitenkin koko ajan lisää ja ne ovat entistä tehokkaampia.

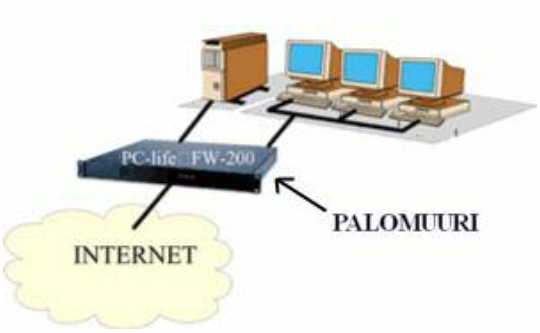
Lähde: (MikroBitti 4/2002 s.38-39, MikroBitti 1/2002 s. 32-34)

3.2 Hakkereilta suojautuminen

3.2.1 Palomuurit

Internetissä kaikki tieto kulkee porttien kautta. Näitä tietoliikenneportteja on kaiken kaikkiaan 65 536 kappaletta, joista esim. http-liikenne kulkee porttiin numero 80. Tietokonevirusten lisäksi on olemassa uhka, että joku ulkopuolinen hakkeri pääsee tunkeutumaan Internetin kautta tietokoneeseesi auki olevista porteista. Näiden hakkereiden tunkeutumisyritykset voi kuitenkin hyvin estää käyttämällä palomuuria.

Palomuuri on laite tai ohjelma, jonka tarkoituksena on toimia eräänlaisena tietokoneen portsarina. Se pitää ainoastaan käyttäjän kannalta välttämättömät portit auki, kuten http:n käyttämän portin 80. Näin kukaan ei pääse koneellesi muiden porttien kautta. Kaikki koneelta lähtevä tai sinne saapuva liikenne joutuu kulkemaan palomuurin kautta.



Palomuurit voidaan jakaa kahteen pääryhmään: laitteisiin ja ohjelmiin. Hyviä palomuuriohjelmia saa ilmaiseksi Internetistä. Palomuurilaitteiden etuna on niiden parempi toimintavarmuus, mutta ne ovat myös kalliita (n.100 €-200 €). Suojattavassa tietokoneessa pyörivät muut ohjelmat eivät kuitenkaan pääse sotkemaan erillisen palomuurilaitteen toimintaa.

Palomuuriohjelmien ongelmana on se, että ne toimivat käyttäjän koneessa eivätkä erillisessä palomuurilaitteessa. Ei-toivottu tietoliikenne joudutaan siis ottamaan vastaan käyttäjän koneelle ja käännyttämään vasta sitten pois. Tämä luo pienoisen turvallisuusriskin, sillä murtautumista yrittävät hakkerit voivat olla niin taitavia, että softapalomuurit saadaan taipumaan murtautujan tahtoon ja on myös olemassa sellaisia viruksia, jotka hyökkäävät palomuuriohjelmaa vastaan ja jos palomuuriohjelma lakkaa toimimasta, jää kone suojattomaksi.

Varsinaiset palomuurilaitteet sijoitetaan tietokoneen ja internetin väliin, jonka avulla ei-toivottu liikenne saadaan karsittua pois jo ennen kuin se pääsee tietokoneeseen asti. Kohdatessaan mielestään epätavallista liikennettä palomuuri ilmoittaa siitä käyttäjälle. Palomuurit ovat kuitenkin melko vainoharhaisia ja voivat pitää tavallista internet-liikennettäkin hyökkäyksenä.

Jos palomuuri havaitsee samasta osoitteesta tulevia hyökkäyksiä tiheään tahtiin tai jos hyökkäykset kohdistuvat samaan tietoliikenneporttiin, yrittää hakkeri todennäköisesti koneellesi. Palomuuri voi pysäyttää hyökkäyksen estämällä kaiken epäilyttävästä osoitteesta tulevan tiedon saapumisen koneellesi, mutta silti itse voi jatkaa netin selailua. Varmin tapa on kytkeä kone täysin irti Internetistä.

Lähde: (MikroBitti 2/2002 s. 54-56, MikroBitti 5/2002 s. 44-47)

3.2.2 WWW-liikenteen salaus: SSL-salaus

Internetissä liikkuminen on yleensä aika turvatonta. Kun asiakas kirjautuu esim. jonkun verkkokaupan tai vaikkapa pankin sivuille kotikoneellaan käyttäen www-selainta, joku taitava hakkeri voi hyvinkin onnistua varastamaan esimerkiksi luottokortin numeron. Tätä tietoliikennettä voidaan kuitenkin turvata esimerkiksi kryptaamalla liikenne www-selaimen ja www-palvelimen välillä.

Yksi yleisin vaihtoehto tähän on Netscapen kehittämä Internetin salausprotokolla SSL (Security Sockets Layer). SSL on protokolla, joka on suunniteltu parantamaan www-selaimen ja palvelimen välistä tietoturvaa. Netscapen ja Microsoftin selaimet tukevat kumpikin SSL:ää ja sitä käytetäänkin nykyisin yleisesti pankkipääteyhteyksien suojausmenetelmä.

Lähde: (Tietoliikenteen perusteet s. 91, http://www.tpu.fi/~comima/tietoturva.htm)

3.3 Tietovarkaudet

Yksi uhka on myös tiedostojen tai koko tietokoneen joutuminen vääriin käsiin esim. varkauden yhteydessä. Tällöin tietokoneen täytyisi olla kiinni ja salasanan täytyisi olla sellainen, ettei sitä helvillä arvaa. Hyvä salasana on sellainen, joka on helppo muistaa itse, mutta muiden mahdollisimman vaikea arvata. Lisäksi se on oltava riittävän pitkä.

Tänä päivänä lähdetään siitä, että kunnollisen salasanan tulisi olla vähintään 13 merkkiä pitkän. Lisäksi se ei saisi olla mikään yksittäinen sanakirjasta löytyvä sana ja siinä tulisi olla myös muita merkkejä kuin kirjaimia. Salasanat tulisi vielä vaihtaa riittävän usein jos on mahdollista.

Usein yrityksen työntekijöillä voi olla kannettavat tietokoneet. Tällöin kannattaisi hankkia kannettaviin erilliset Kensington-lukot, joilla kannettavan saa vaijerilukolla kiinni johonkin, mistä sitä ei niin vain oteta mukaan. Myös tärkeimmät koneen tiedostot kannattaisi laittaa salasanojen taakse tai kryptata eli salakirjoittaa erillisellä salausohjelmalla. Tällaisia ovat esim. Pretty Good Privacy -salausohjelma, joka on yksityiskäytössä ilmainen.

Lähde: (Tekniikan Maailma 6/2000 s. 38-44, http://www.tietokone.fi/lukusali/artikkelit/2001tk02/tietotur.htm, http://www.teli.stadia.fi/~kuivanen/tietoturva/)

4 Sähköpostin tietoturvallisuus

Sähköpostin tietoturvallisuus ei ole nykyään mitä parhain. Vähän aikaa sitten riehuneet Melissa ja LoveLetter levisivät kummatkin sähköpostin kautta. Erityisesti Microsoftin Outlook sähköpostiohjelmassa on isoja turvallisuusriskejä. Maailma lukemattomat internet-palveluntarjoajatkaan eivät yleensä tarkasta välittämiään sähköposteja virusten varalta, mutta on poikkeuksiakin kuten MikroBitin tarjoaman sähköpostipalvelun välittämät kaikki sähköpostit, jotka menevät virusseulan läpi, joka päivitetään tarpeeksi usein.

Sähköpostin turvallisuus on kuitenkin pitkälti kiinni Internetin turvallisuudesta. Kun lähetät sähköpostin, joku voi siepata viestin ja lukea sen jos salausta ei ole hoidettu kunnolla. Tietoturvaongelmia syntyy myös jos tärkeä sähköposti menee väärään osoitteeseen. Tämä voi tapahtua helposti, sillä pienikin kirjoitusvirhe osoitteessa, niin viesti menee minne sattuu. Tavallisissa kirjeissähän ei kirjoitusvirhe osoitteessa yleensä haitta juuri mitään.

Kaikesta huolimatta sähköposti ei ole sen turvattomampi kuin perinteisin keinoin lähetetty kirje. Tietoturvallisuutta voidaan parantaa käyttämällä sähköposteissa salakirjoitusta tai digitaalista allekirjoitusta varmennukseen keneltä sähköposti tulee. Paras tapa välttyä sähköpostitse liikkuvilta viruksilta on yksinkertaisesti jättää avaamatta kaikki liitetiedostot jos ei ole liitetiedostoa odottanut saavansa.

Lähde: (http://www.student.oulu.fi/~salaine/essee.html, MikroBitti 3/2002 s. 57)

5 Omat kokemukset

Itselläni ei ole kokemuksia viruksista ja hakkereista, mutta tiedostojen tuhoutumisesta kyllä on ja olen huomannut varmuuskopioinnin erittäin tarpeelliseksi. Kerran minulle kävi niin, että tietokoneeni meni tilttiin, jostain ihmeen syystä, ja kaikki tiedostot hävisivät. En ollut silloin varmuuskopioita ottanut, mutta onneksi minulla ei juurikaan tärkeitä tiedostoja siellä ollut.

Onneksi sen jälkeen aloin ottamaan varmuuskopioita, sillä muutama vuosi tapahtuman jälkeen jollain mystisellä tavalla kaikki esitelmät, jotka olen tallentanut tietokoneelleni hävisivät. Saatoin kuitenkin huokaista helpotuksestani kun olin muutama päivä ennen tiedostojen häviämistä ottanut niistä varmuuskopiot, eikä siinä kauaa kestänyt kun sain kaikki tiedostot takaisin.
Varmuuskopiointi on todellakin tärkeää, eikä ollenkaan turhaa.

6 Lähdeluettelo

Tapio Hämeen-Anttila, **Tietoliikenteen perusteet**, 2000, Teknolit, 1. painos, s. 91
Lammi, Karhula, Simola, **Tietokoneen käyttötaito 1**, Teknolit, 2000, 1.painos, s.40-41
Tekniikan Maailma 7/1999, Yhtyneet kuvalehdet Oy, s. 60-61
Tekniikan Maailma 6/2000, Yhtyneet kuvalehdet Oy, s. 38-44
Tekniikan Maailma 11/2000, Yhtyneet kuvalehdet Oy, s. 58-59
MikroBitti 1/2002, Sanoma Magazines Finland, s. 32-34
MikroBitti 2/2002, Sanoma Magazines Finland, s. 36-39, 54-57
MikroBitti 3/2002, Sanoma Magazines Finland, s. 54-57
MikroBitti 4/2002, Sanoma Magazines Finland, s. 38-46
MikroBitti 5/2002, Sanoma Magazines Finland, s. 44-50
Internet: http://www.tietokone.fi/lukusali/artikkelit/2001tk02/tietotur.htm
Internet: http://www.teli.stadia.fi/~kuivanen/tietoturva/
Internet: http://www.tpu.fi/~comima/tietoturva.htm
Internet: http://www.tieke.fi/

Kuvalähteet:

LoveLetter: http://www.tonyaustin.com/viruzlist/loveletter.html
Virus alert: Internet
Palomuuri: http://www.pclife.fi/fw200.html