VAASAN YLIOPISTO

TEKNILLINEN TIEDEKUNTA

TIETOTEKNIIKAN LAITOS

Susanna Ravantti

TIETOKONE RIKOKSENTEKOVÄLINEENÄ

Tietotekniikan pro gradu-tutkielma

VAASA 2008

SISÄLLYSLUETTELO

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Susanna Ravantti
Tutkielman nimi: Tietokone rikoksentekovälineenä
Ohjaajan nimi: Merja Wanne
Tutkinto: Kauppatieteiden maisteri
Laitos: Tietotekniikan laitos
Oppiaine: Tietotekniikka
Opintojen aloitusvuosi: 2002
Tutkielman valmistumisvuosi: 2008 **Sivumäärä:** 77

TIIVISTELMÄ:

Tutkielmani käsittelee teoriassa erilaiset tavat käyttää tietokonetta rikoksentekovälineenä. Lisäksi aihealuetta sivuten käsitellään esimerkiksi erilaiset suojautumiskeinot sekä keskeiset lait.
Tietokoneiden ja verkkojen yleistyminen sekä nopeuksien ja tehokkuuden nousu ovat positiivisen hyödyn lisäksi luoneet hedelmällisen maaperän myös rikolliselle toiminnalle. Monet yhteiskunnan kriittisistä toiminnoista ovat erilaisten verkkojen, tietokoneiden ja tietojärjestelmien varassa. Tämän tosiasian ollessa taustalla, muun muassa vandalismi, terrorismi sekä taloudelliset syyt ovat useimmiten motiivina tietokonerikokselle. Karkeasti yleistäen tekijänä sekä kohteena voi olla kuka tahansa.

Olen ryhmitellyt erilaiset tietokonerikokset seuraavasti:

- Sähköpostin ja tiedostojen kautta leviävät ilmentymät (esimerkiksi roskaposti, haittaohjelmat ja virukset)
- Internetissä esiintyvät rikokset kuten khalastelu ja väärät verkkosivustot
- Piratismi, jonka olennaisia piirteitä ovat vertaisverkot sekä niin kutsuttu warettaminen (laittomien tiedostojen imurointi Internetistä)
- Muut kuten identiteettirikokset ja laitevarkaudet

AVAINSANAT: Tietokonerikos, Tietoturva, Hakkeri, Virus, Piratismi

UNIVERSITY OF VAASA
Faculty of Technology
Author: Susanna Ravantti
Topic of the Master's thesis: Computer as a Tool of Crime
Instructor: Merja Wanne
Degree: Master of Science in Economics and Business Administration
Department: Department of Computer Science
Major subject: Computer Science
Year of Entering the University: 2002
Year of Completing the Master's Thesis: 2008 **Pages:** 77

ABSTRACT:

My master's thesis deals with different ways to use computer as a tool of crime in theory. In addition, this thesis contains related topics e.g. security issues and essential laws.
Computers and networks have become ubiquitous; also speed and effectiveness have created positive benefits but also a fertile ground to criminal activity. Most of society's critical functions depend on networks, computers and data systems. Vandalism, terrorism and economical issues are the most common motives to computer crime. If we generalize, anyone can be a criminal or a victim.

I've categorized different computer crimes as follows:

- The phenomena, which spread via email and files (e.g. spam, malware and viruses.)
- Crimes, which appear in Internet (e.g. phishing and fake www-sites.)
- Piracy, which include e.g. peer-to-peer networks and illegal downloading.
- Other crimes, like identity theft and stealing of hardware.

KEYWORDS: Computer crime, Data security, Hacker, Virus, Piracy

1. JOHDANTO

Jokainen tietokoneen käyttäjä on kuullut viruksista, piratismista tai hakkeroinnista. Nämä kaikki edellä mainitut asiat ovat ilmentymiä rikollisesta toiminnasta tietokonemaailmassa. On olemassa käyttäjäryhmiä, jotka järjestelmällisesti harjoittavat rikollista toimintaa mutta myös moni tavallinen käyttäjä syyllistyy siihen tietämättään. Kaikki eivät tiedä, että naapurin langattoman verkon käyttäminen on laitonta, vaikkakin siihen voi olla mahdollista puolivahingossa kirjautua. Tai että elokuvan sekä musiikin lataaminen vertaisverkkoa käyttäen rikkoo tekijänoikeuslakia. Nämä ovat tyypillisiä esimerkkejä tapauksista, joissa syyllistytään tietokonerikoksiin mutta niitä ei aina mielletä rikoksiksi menetelmien helppouden tai materiaalin saatavuuden vuoksi. Internetin leviäminen jokaisen käyttäjän ulottuville hyödyllisten ominaisuuksien lisäksi on luonut puitteet myös tietotekniikkarikollisuudelle.

Internetit, intranetit ja muut tietoverkot ovat kaikki alttiita ulkoisille tietoturvahyökkäyksille. Ulkoisia uhkia ovat muun muassa hakkerointi, vakoilu ja salakuuntelu, yhteyksien katkaiseminen sekä häiriköinti ja laitteisiin kohdistuva eriasteinen vahingonteko. Järjestelmiin voivat hyökätä kilpailijat, hakkerit, krakkerit tai muut, jotka haluavat päästä sisään organisaation tietojärjestelmään. Näistä tapauksista saadaan lukea päivittäin. Tämän lisäksi valitettava tosiasia on, että monet tietoturvarikkomukset tapahtuvat organisaation sisältä henkilökunnan, aikaisempien työtekijöiden ja joskus jopa vieraan työvoiman aiheuttamana. (Kerttula 1998; s. 37.)

Internet on verkkojen verkko. Tietoverkot kehitettiin Yhdysvalloissa 1960-luvun lopulla alun perin armeijan käyttöön. Puolustusvoimien lisäksi verkossa olivat

kiinnostuneet tiedeyhteisöt, niin tutkimuslaitokset kuin yliopistotkin. Näistä verkoista muodostui vähitellen Internet. Sen alkuversiota kutsuttiin ARPANETiksi, ja se oli luonteeltaan hajautettu. Verkkorakenne varmisti sen, ettei sotilaallinen isku olisi lamaannuttanut Internetin toimintaa, koska viestit olisivat etsineet aina vaihtoehtoisen reitin.
Internetiin kuului 1970-luvulla muutamia kymmeniä tietokoneita, 1980-luvun alkupuolella niitä oli noin tuhat ja vuosikymmentä myöhemmin Internetiin liittyneitä koneita oli jo satatuhatta. (Mäkinen 2006; s. 23.)

Verkon käyttäjät huomasivat varsin nopeasti, että se palveli muutakin kuin tieteellistä toimintaa. Internet soveltui hyvin erilaiseen kommunikaatioon, sekä keskusteluun ja sähköpostiviestintään mutta myös yleiseen tiedonvälitykseen. Varsinkin sähköpostin ja tietoliikenteen yleistyminen toi 1990-luvun alussa mukaan uusia käyttäjiä, sekä yrityksiä että yliopistojen ulkopuolisia yksityishenkilöitä. PC-tietokoneet ja graafinen Windows-käyttöliittymä tekivät Internetistä yhä enemmän jokamiehen välineen. (Mäkinen 2006; s. 23.)

Vuonna 2005 Internetiä käytti miltei neljä miljoonaa 15 – 74-vuotiasta suomalaista. Laajakaistaliittymien määrässä mentiin yli miljoonan jo kesäkuussa 2005, ja nyt ollaan jo 1,1 miljoonan paremmalla puolella. Laajakaistaa käyttää kahdeksan kymmenestä surffaajasta. Suomalainen käyttää Internetiä pääasiassa sähköpostiin, tiedon etsimiseen, pankkipalveluihin ja online-lehtien lukemiseen. Tilastokeskuksen mukaan eniten tietoa etsitään tuotteista ja palveluista sekä matkailusta ja majoituspalveluista. (Mikrobitti (1/06) 2006; s. 9.)

Vaikka voitaisiin puhua hakkerointitrendeistä, www-tihutöiden kasvavasta määrästä, valtion laitosten ja organisaatioiden ympärivuorokautisesta alttiudesta murtautumisille, yrityssalaisuuksien varkauksista, käsitellään asiaa hieman

maanläheisemmin. Ovatko organisaation tiedot arvokkaita? Henkilökuntaa koskevat tiedot, henkilötunnukset, luottokorttien numerot, palkkatiedot, yhteystiedot, markkinointistrategiat, tutkimus- ja tuotekehityshankkeet, henkinen omaisuus, tuloraportit ja talousennusteet - onko niillä arvoa? (Anonymous 2002; s. 4 – 5.)

Esimerkkejä järjestelmistä, joiden toiminta on nykyään riippuvaista tietokoneista:

- kuljetusjärjestelmät
- henkilökohtaiset ja yritysten rahatiedot ja -järjestelmät
- luottokorttien käsittelyjärjestelmät
- pankkiautomaatit
- julkinen puhelinverkko
- hätäpuhelut ja -tietoliikenne, esimerkiksi 112-puhelut
- lentoliikenteen ohjausjärjestelmät
- terveydenhoitotietojen säilytyksestä ja siirrosta vastaavat järjestelmät
- sähköjärjestelmät
- yleiset maksujen käsittelyjärjestelmät
- lippujärjestelmät. (Anonymous 2002; s. 4 – 5.)

2. TIETOKONERIKOLLISUUS

Uusi tekniikka on mahdollistanut uuden rikollisuuden haaran. Silti voidaan kysyä, kun kyse on tietokoneen varastamisesta, että onko kyseessä tietokonerikollisuutta vai yksinkertaisesti vain varkaus. Tietokonerikollisuus nimikkeen alla on lukematon määrä erilaisia rikosnimikkeitä mutta Lilleyn mukaan voidaan tietokonerikollisuus lokeroida kolmeen päähaaraan:

- Tietokone on *kohde.* Tämä sisältää hakkerointia, virukset sekä tietoliikennepalveluiden varastamisen
- Tietokone *rikoksentekovälineenä*, jolloin tekniikka korvaa perinteiset menetelmät. Tällaisia toimintoja ovat muun muassa petokset, rahanpesu ja esimerkiksi henkilön väijyminen
- Tietokone on *oheisvälineenä* rikoksessa. Esimerkiksi kirje on kirjoitettu anonyymisti tietokoneella käsinkirjoitetun sijasta. (Lilley 2002; s. 26.)

Kshetrin mukaan tietokonerikollisuudesta voidaan erottaa kolme uniikkia piirrettä verrattuna perinteiseen rikollisuuteen. 1) Teknisyys sekä niiden taitojen hallinta, 2) globaalisella tasolla ovat korkeammalla tasolla kuin perinteiset rikokset sekä 3) alana vielä varsin uusi ja tuore. (Kshetri 2006; s. 33.)

Teknologia tarjoaa oivallisen alustan rikokselle sillä, digitaalinen rikos voi olla anonyymi. Rikos voidaan suorittaa etänä ilman, että tarvitsee kohdata uhria. Digitaalinen rikos voidaan nähdä uhrittomana toimintana – mitä se ei tietenkään ole. Rikokset voidaan suorittaa nopeasti sekä melkein jälkiä jättämättä. Ei ole maantieteellisiä rajoja, ei asiakaskontrollia tai turvallisuustarkastuksia. Varastettavalla tavaralla ei ole massaa, varkaus voi olla yhdestä dollarista miljoo-

naan dollariin. Tekninen osaaminen ei myöskään välttämätöntä. Haluatko tehdä viruksen? Lataa ohjeet verkosta sen tekemiseen. (Lilley 2002; s. 28.)

”Hakkerointi”, ”krakkerointi” ja muu vahingollinen toiminta ovat todellisuutta nykyisissä dataverkoissa. Yleisesti käytetään nimitystä ”hakkerointi” kun puhutaan laittomista tunkeutumisista – nykypuhekielen mukaisesti ”krakkerointi” on varsinaisesti suojauksien murtamiseen tähtäävää toimintaa. ”Krakkeroinnilla” voi olla eri käyttötarkoituksia:

- Tunkeutuja voi saada verkko-oikeudet (käyttäjätunnukset ja salasanat) mutta ei halua tehdä muuta vahinkoa
- Tunkeutuja voi saada käyttöoikeudet ja pyrkiä niiden avulla tuhoamaan, vahingoittamaan ja muuttamaan tietoja
- Tunkeutuja voi saada käyttöoikeudet ja saa siten hallintaansa osan tai kokonaisuuden järjestelmästä ja voi esimerkiksi estää oikeutettujen käyttäjien pääsyn järjestelmään
- Tunkeutuja ei saa käyttöoikeuksia mutta voi lähettää väärennettyjä viestejä järjestelmän nimissä. Roskapostin lähettäminen on tyypillisin merkki tällaisesta toiminnasta
- Tunkeutuja ei saa käyttöoikeuksia mutta voi kehittää vahingollisia keinoja, jotka saavat verkon toimimaan virheellisesti. Tällaista toimintaa kutsutaan palvelunestohyökkäyksiksi. (Penttinen 2006; s. 186.)

Suurimmat menetykset ovat tietovarkauksissa sekä talous- ja tietoliikennepetoksissa. Tietovarkaus maksaa yritykselle siten keskimäärin miljoona dollaria (5,4 miljoonaa markkaa) (Kerttula 1998; s. 41.) Eli tämän päivän rahassa summa olisi likipitäen 900 000 euroa. Niin kutsuttu The Love Bug virus, joka on tällä hetkellä kaikista tuhoisin ja kallein virus, maksoi 8,7 miljoonaa dollaria mene-

tettynä tuotannonlaskuna sekä puhdistuskustannuksina (Lilley 2002; s. 80.)

2.1 Tietokonerikollisuus lisääntyy nopeasti

Tietokonerikollisuutta on selvitetty laajasti erityisesti USA:ssa. NCSA:n (National Center for Supercomputing Applications) mukaan tietokonerikollisuus kaksinkertaistuu aina 5,2 kuukauden välein (CTR 1997b). FBI:n (Federal Bureau of Investigation) ja CSI:n (Computer Security Institute) yhteisesti 1997 tekemässä laajassa tutkimuksessa tutkittiin 563 amerikkalaista organisaatiota. Kolmeen neljäsosaan niistä oli suoritettu sellainen tietoturvamurto, mistä oli ollut seurauksena taloudellisia menetyksiä. (Kerttula 1998; s. 39.)

Tunkeutumiset jaettiin kolmeen ryhmään: sisäisiin, Internetin kautta ja valintaverkon välityksellä tulleisiin. Tietoturvarikkomuksista yli 50 % tuli sisältäpäin ja 47 % Internetin kautta. Nämä molemmat tavat ovat kasvussa. (Kerttula 1998; s. 39.)

Mitä hakkerit tekevät, kun he hyökkäävät? Erään hakkeriyhteisössä tehdyn amerikkalaisen selvityksen mukaan 46 % on kertonut suorittaneensa jonkinasteista sabotaasia ja 18 % on väittänyt vahingoittaneensa Web-sivuja. Muita usein esiintyviä hyökkäyksiä ovat virusten levittäminen, aikapommin heittäminen (aktivoituu tiettynä ajanhetkenä), petokset, informaation käyttö rikolliseen tarkoitukseen ja luottamuksellisen informaation toimittaminen muille. Hakkereiden hyökkäysten kohteena on ennen kaikkea tietotekniikkayritykset (46 %) ja tietoliikenneyritykset (42 %). (Kerttula 1998; s. 40.)

Tietokonerikollisuuden uhreiksi joutuneiden yritysten haluttomuus raportoida viranomaisille rohkaisee kyberterroristien käyttäytymistä. Erään tutkimuksen mukaan vain 17 % tällaista rikollisuutta kohdanneista yrityksistä raportoi viranomaisille. Syitä tähän on muun muassa nolous, pelko asiakkaiden luottamuksen häviämisestä, mahdollisista vaikutuksista yrityksen luottokykyyn sekä mahdolliset vaikutukset osakkeisiin pörssissä. 70 % syynä on myös negatiivinen julkisuus yritykselle. (Kshetri 2006; s. 36.)

Verkkorikolliset verkostoituvat, mikä lisää rikollisuutta entisestään. Rikolliset tai rikollisorganisaatiot myyvät alamaailman palvelinten kautta varastettuja tietoja, kuten identiteettinumeroita, luotto- ja pankkikorttitietoa, pin-tunnuksia, käyttäjätilejä sekä sähköpostiosoitteita. 15 prosenttia näistä palvelimista löytyi Ruotsista, mikä on toiseksi eniten maailmassa. (Karkimo 2007; s. 13.)

Verkon kautta yritetään monella tavalla petkuttaa ihmisiä. Monet muutoin järkevästikin käyttäytyvät ihmiset ovat menettäneet paljon rahaa, kun eivät ole osanneet varoa. Huijareita on vähän, mutta verkko antaa heille keinoja yrittää miljoonien ihmisten huijaamista joka päivä. (Korpela 2005; s. 157.)

2.2 Tietotekniikkarikollisuus Suomessa

Erään suppean tutkimuksen mukaan Suomessa 18 % vastanneista yrityksistä tai organisaatioista oli joutunut hakkeroinnin kohteeksi. Näistä noin 40 % oli joutunut hakkeroinnin kohteeksi yli 10 kertaa. Havaituista hakkereista 51 % oli ollut kotimaisia, 31 % ulkomaisia ja 14 % oman yrityksen sisältä. Yleisimmät hakkeroinnin aiheuttamat vahingot ovat olleet tiedostojen anastaminen (22 %),

tietoliikenneyhteyksien häirintä (21 %), ohjelmien anastaminen (16 %), järjestelmän käytön estäminen (9 %). Loput ovat muita vahinkoja. Tutkimus perustui 102 henkilön vastaukseen eri toimialoilta. Tutkimus on suppea ja sen tuloksiin tulee suhtautua yleisyydessään kriittisesti. Mutta tutkimus osoitti kuitenkin hakkerointiongelman vakavuuden Suomessakin eri toimialoilla. (Kerttula 1998; s. 40.)

3. TIETOKONERIKOLLISUUDEN TEKIJÄT

Tietokonerikollisuuden tekijät voidaan lokeroida erilaisin perustein. Hyökkääjä voi olla sisäinen tai ulkoinen, riippuen hänen suhteestaan hyökättävään kohteeseen. Hyökkääjät voidaan jakaa myös amatööreihin tai ammattilaisiin. Useimmiten amatöörit syyllistyvät esimerkiksi vandalismiin tai virusten levittämiseen, niin ammattilaiset suorittavat rikoksen järjestäytyneen rikollisuuden piirissä ja heitä ajaa taloudelliset edut. Usein hyökkäykset tässä tapauksessa liittyvät hallituksiin, sotilasoperaatioihin tai teollisuusvakoiluun. (Chen & Davis 2006; s. 2.)

Aikanaan viruksia ja matoja kirjoittivat lähinnä nuoret, joita viehätti luvattoman toiminnan houkutus ja sen harrastajapiireissä tuottama kunnia. Tänään harrastajien tilalle ovat tulleet ammattilaiset, jotka tavoittelevat taloudellista hyötyä. Haittaohjelmien levittäjinä toimivat yhä useammin kansainväliset liigat ja järjestäytynyt rikollisuus. (Järvinen 2006; s. 77.)

Useimmiten tietomurtautuja on nuori henkilö, koska he nopeasti omaksuvat asioita. Varsin tyypillistä on myös se, että on paljon aikaa mutta vähän rahaa. (Järvinen 2002; s. 293.) Erään tutkimuksen mukaan nuorista henkilöistä voidaan vielä erottaa yksi erottuva ryhmä eli opiskelijat. Miespuoliset henkilöt sortuvat piratismiin ja muihin väärinkäytöksiin naispuolista henkilöä helpommin. Eniten väärinkäyttäjiä on 20 – 30 vuotiaissa. (Cronan, Foltz & Jones 2006; s. 89.)

3.1 Hakkeri ja krakkeri

Alun perin hakkereilla tarkoitettiin Internetin pioneerikauden tietokoneharrastajia, jotka tempuillaan (hack about = peukaloida tekstiä) pyrkivät muuttamaan tietokoneiden ohjelmia ja halusivat saada ne toimimaan paremmin. Alkuaikojen hakkeri oli innostunut harrastelija, eikä toiminta pitänyt sisällään taloudellisen hyödyn tavoittelua. Hakkerointi oli leikkiä, tapa päteä ja esimerkiksi Yhdysvalloissa se kriminalisoitiin vuonna 1986 (Computer Fraus and Abuse Act.) (Mäkinen 2006; s. 197.)

Odom määrittelee seuraavasti hakkerin ja krakkerin eroavaisuudet. Termi krakkeri tarkoittaa henkilöä, joka yrittää tarkoituksellisesti aiheuttaa ongelmia verkon laitteille. Hakkeri puolestaan tarkoittaa henkilöä, joka yrittää murtautua verkkoon, mutta ei pyri aiheuttamaan vahinkoa. (Odom 2005; s. 385.)

Kun krakkeri-iskulla on jokin aatteellinen motiivi, käytetään termiä haktivisti (hakkeri + aktivisti). Haktivistit osoittavat mieltään sotkemalla globalisaatioon tai turkistarhaukseen liittyviä www-sivuja tai kuormittavat palveluita niin, että ne menevät tukkoon. (Järvinen 2002; s. 295.)

3.2 Tavallinen käyttäjä

Kuinka tavallinen kansalainen erehtyy laittomuuksien puolelle tietämättään? Esimerkiksi kopioidessaan musiikkia verkosta siihen erikoistuneilta palvelimilta ja nettisivuilta. Tai ”lainatessaan” naapurin suojaamatonta wlan-verkkoa surffatakseen Internetissä. Useimmiten tällaisissa tapauksissa on kyse tietämät-

tömyydestä tai mahdollisuuden helppoudesta. Monet ajattelevat, että jos teksti tai dokumentti on Internetissä, se on kaikkien vapaasti käytettävissä. Mutta tekijänoikeus pätee myös netissä, tähän aiheeseen palataan myöhemmin luvussa ”Tietokonerikollisuutta koskevat keskeiset lait”.

Hämäläisen mukaan pahin vihollinen istuu kuitenkin usein yrityksen sisällä: petollinen tai huolimaton työntekijä. Hänellä on pääsy liiketoiminnan kannalta keskeiseen tietoon, joten hän voi saattaa liikesalaisuuksia tai muuta luottamuksellista tietoa vääriin käsiin. (Hämäläinen 2007; s. 57.)

3.3 Muita tekijäryhmiä

Script kiddie on halventava nimitys nuorille, jotka käyttävät varsinaisten hakkerien tekemiä helppokäyttöisiä työkaluja tai valmiita komentosarjoja (skriptejä) murtoyrityksiin. Teollisuusvakooja on tietomurtojen ammattilainen ja hänellä on käytössään parhaat välineet sekä runsaasti osaamista. Häntä kiinnostavat yritysten tuotekehitys ja tuotteiden tekniset tiedot. Vieraiden valtioiden tiedustelupalveluista ei ole tarkkaa tietoa mutta on varmaa, että kansainvälistä dataliikennettä seurataan ja että myös sotilastiedustelut ovat kiinnostuneita hakkereiden menetelmistä. (Järvinen 2002; s. 296 – 297.) Esimerkiksi Neuvostoliiton avaruussukkulaohjelma perustui amerikkalaiseen teknologiaan, jota varastettiin Internetin kautta. Suunnitelmia haettiin monien teknisten yliopistojen koneista. (Anonymous 2002; s. 97.)

Myös järjestäytynyt rikollisuus on yksi tekijäryhmä. Esimerkiksi on näyttöä siitä, että suurien virusepidemioiden tai tietojen khalastelujen (Phishing) takana

on ollut joissakin tapauksissa yhteyksiä järjestäytyneeseen rikollisuuteen. Hyvien ohjelmoijien ei kannata kirjoittaa viruksia ja riskeerata kiinnijäämistä, kun taidoilla voi ansaita rahaakin. Rikolliset ostavat kehittyneitä haittaohjelmia omiin tarkoituksiinsa ja maksavat niistä hyvin. Erityisen kysyttyjä ovat nollapäiväaukkoja käyttävät haittaohjelmat, koska niitä on helpointa levittää. (Järvinen 2006; s. 77.)

4. MOTIIVI

Tyypillinen hyökkääjän motiivi on yksinkertaisesti halu näyttää kykynsä ja aiheuttaa tavallisuudesta poikkeavia ilmiöitä verkon toiminnassa tai sen tarjoamissa palveluissa. Toisessa ääripäässä hyökkääjän motiivina voi olla paikallisen tietoyhteiskunnan toimintojen lamauttaminen eli eräänlainen terrorismi. Laajasti ajateltuna nykyinen tietoyhteiskunta on jo niin riippuvainen tietoliikenneyhteyksistä, erityisesti Internetistä, että tietoverkon lamautuminen saattaa aiheuttaa ennalta arvaamattomia katastrofaalisia kerrannaisvaikutuksia. Terrorismin uhka on siten otettava yhä vahvemmin huomioon myös tietoliikennerat-kaisujen suojaamisessa. Yhtä lailla elektronisen sodankäynnin merkitys poikkeus- ja kriisitilanteissa on tulossa yhä tärkeämmäksi. (Penttinen 2006; s. 187.)

Seuraavassa on listattu tyypillisimmät motivaation aiheuttajat:

- Maine
  Halu kasvattaa mainetta esim. krakkeriyhteisössä.
- Vahingon tuottaminen
  Vahingonteko viattomaan kohteeseen tai tyytymättömät työntekijät.
- Poliittisen ilmaisun tekeminen
  Palestiina vs. Israel.
- Rahallinen hyöty ja varkaus
  Varkaus tai luvaton varainsiirto, henkisen omaisuuden varkaudet ja yritysvakoilu tai luottokorttivarkaudet.
- Osaaminen
  Halu ymmärtää järjestelmää ja oppia, jännityksen hakeminen.

(Jenkins 2002; s. 189 – 195.)

Yksi tyypillisimpiä syitä on poikamainen näyttämisen halu. Ilmiö on ikivanha, muodot vain ovat nykyaikaiset. Taitavien tietokoneharrastajien joukon lisäksi on olemassa suurempi joukko jäljittelijöitä. Taitavimmat ovat tehneet ohjelmia, joilla voi tehdä tietomurtoja ja häiritä verkon toimintaa, ja he ovat laittaneet niitä Internetiin jakeluun - ei välttämättä avoimeen jakeluun, mutta melko helposti saataville. Niinpä jäljittelijät voivat usein ilman mainittavaa teknistä osaamista tehdä samanlaisia tekoja kuin heidän ihailemansa taiturit. Aivan tavallinen suomalainen lapsi tai nuori saattaa siis olla tietomurtaja vanhempiensa tietämättä. Ei tunneta lakia ja muiden ihmisten oikeuksia, tai ei välitetä niistä. Ei ymmärretä, että pelkkä yritys päästä sisään tietokoneeseen tai palveluun salasanoja arvailemalla on rikos. Ei myöskään tiedetä, mitä seuraamuksia rikoksista ja pahanteosta voi olla. Verkossa toimiminen voi luoda harhakuvan siitä, että toimijaa ei voida saada kiinni. Tietokonealan ammattilainen saattaa olla turhautunut esimerkiksi siksi, että hänen omassa maassaan ei ole töitä hänelle tai palkka on naurettavan pieni (esimerkiksi Kiina ja Venäjä). Tästä tai jostakin muusta oman elämän tilanteesta voi johtua halu kostaa. Tietomurron syy voi olla taloudellinen. Silloin kyse on yleensä pyrkimyksestä saada selville kilpailijan liikesalaisuuksia tai muuten hankkia rahanarvoista tietoa. Tietotekniikka voidaan käyttää myös aseena. Nykymaailmassa hyvin paljon riippuu tietotekniikasta, myös sotilaallisella alalla. Siksi voi saavuttaa paljon häiritsemällä vihollisen tietojärjestelmiä, vakoilemalla niistä tietoja ja syöttämällä niihin väärää tietoa. Voidaan myös pyrkiä häirintään ilman sotilaallistyyppistä tarkoitusta. Tavoitteena voi olla vain julkisuuden saavuttaminen jollekin asialle. (Korpela 2005; s. 194 – 196.)

Kuten kaikissa rikoksissa, hyökkääjä täyttää omia tarpeitaan, joiden syy ja motiivit voivat olla monenlaisia. Muiden ihmisten tietokonejärjestelmiin murtau-

tuminen ja niiden hallinnan saaminen on epäilemättä hyvin jännittävää. Kiinni jäävät kertovat usein, että yksin tämä tunneryöppy riittää motiiviksi. (Anonymous 2002; s. 189.)

Jos pohditaan syitä niin kutsuttuun warettamiseen (laittomien tiedostojen lataaminen Internetistä), niin pääsyynä on äänitteiden sekä muiden tallenteiden hinta sekä saatavuus. Lempisarjan uudet jaksot imuroidaan netistä hdtv-resoluutiolla heti, kun jaksot ovat esitetty Yhdysvalloissa. Osa sarjoista ei päädy suomalaisille tv-kanaville tai edes dvd-versioiksi.

5. KUKA ON YLEISIN KOHDE?

Koti- ja pienyrityskäyttäjät ovat yhtä alttiita hyökkäyksille kuin suuren mittakaavan dot.com-yritykset. Suurin ero on se, että he kärsivät todennäköisemmin palvelunesto- ja virustyyppisistä hyökkäyksistä. Tällä käyttäjäryhmälle Internet- tai järjestelmäturvallisuus ei aina ole itsestäänselvyys. Useimmissa pienyrityksissä ei ole järjestelmien ylläpitäjää eikä niillä ole varaa palkata tietoturva-ammattilaista näiden asioiden hoitoon. Kotikäyttäjät voidaan yleisesti ottaen luokitella huolettomien tietokonekäyttäjien kategoriaan, jossa tietoturvakokemus on vähäistä tai puuttuu tyystin. Muun muassa Yahoo!, eBay, Nike ja Microsoft ovat kokeneet tunkeutumisia, palvelunestoja, www-töhrintää ja asiakas- ja luottokortitietojen varkauksia. Myös useisiin tunnettuihin verkkoturvayrityksiin on hyökätty vaihtelevalla menestyksellä. (Anonymous 2002; s. 188.)

Näillä järjestelmillä on korkea profiili, minkä vuoksi niitä tavoitteleva hyökkääjä ottaa huomattavat riskin. Yhdysvalloissa hallituksen tai sotilaallisten tietojärjestelmien peukalointi tai käyttöyritys on liittovaltiollinen rikos. Nämä järjestelmät kuuluvat myös planeetan parhaiten suojattujen järjestelmien joukkoon. Kiinnostavaa kyllä, osa näistä hyökkäyksistä todella onnistuu ja jäävät havaitsematta, ja joissakin tapauksissa salaista tietoa on varastettu tai hallituksen www-sivuja on töhritty. (Anonymous 2002; s. 188.)

Jos kohteen valintaa mietitään, rahalaitoksen valinta tuntuu järkevämmältä kuin useimmat muut tavoitteet. Se, että joku haluaa hyötyä murtotyöstä, on paljon ymmärrettävämpää kuin se, että joku haluaisi saada etäkäyttäjän yhteyden katkaistua. Pankit ja muut rahalaitokset käyttävät usein maailman parhaita verkkoturvatekniikoita. Rahalaitokset ovat vahvasti riippuvaisia tietokonelait-

teista ja verkosta raha-asioiden hoitamisessa, ja ne siirtävät rahaa sähköisesti laitoksesta toiseen. (Anonymous 2002; s. 188.)

6. ERILAISET TIETOKONERIKOLLISUUDEN LAJIT

Tietokonerikosten kirjo on suuri ja niiden luokittelu ei ole yksinkertaista. Rikoksessa saattaa olla usean kategorian piirteitä. Esimerkiksi khalastelu on usein verkkosivustoilla esiintyvää huijaamista, mutta se voi myös lähestyä käyttäjää sähköpostin, viruksen tai niin kutsutun social engineeringin keinoin.

6.1 Sähköpostin tai tiedostojen kautta leviävät ilmentymät

Vaarattomaan päähän kuuluvat ketjukirjeet, joissa kehotetaan levittämään sähköpostiviestiä omille ystäville. Toista ääripäätä edustavat nigerialaiskirjeet, joihin mukaan lähtevä voi menettää rahansa – ja jos lähtee selvittelemään rahojensa kohtaloa, henkikin voi olla vaarassa. (Järvinen 2006; s. 53.) Lisäksi sähköposti on oiva virusten tai muiden haittaohjelmien jakelukanava. Sähköposti ei ole ainoa väylä, vaan myös muut kommunikaatiovälineet kuten matkapuhelin sekä pikaviestimet kuten esimerkiksi Messenger-ohjelma ovat tällaisten pöpöjen sikiämispaikkoja.

6.1.1 Roskaposti

Roskaposti eli spammi (spämmi) tarkoittaa sähköpostia, joka

- on lähetetty hyvin suurelle määrälle vastaanottajia
- ei ole vastaanottajien tilaamaa tai edes heidän suostumuksellaan lähetettyä
- sisältää tyypillisesti mainoksen tai huijausyrityksen. (Korpela 2005; s.

149.)

Sähköpostitse tulleissa huijausyrityksissä on usein seuraavia piirteitä. Jos viestissä on seuraavista ominaisuuksista kolme tai useampia, se on todennäköisesti huijausta tai roskapostia.

1. Viesti tulee taholta, johon ei ole ollut missään yhteydessä
2. Sinua puhutellaan hyvin tuttavallisesti, vaikka lähettäjä ei ole tuttu
3. Viestistä ei mitenkään ilmene, miksi tarjous tehdään juuri sinulle
4. Viesti on ilmeisesti massajakeluna lähetetty, esimerkiksi vastaanottajakentässä lukee vain "Undisclosed recipients", ja tieto käytetystä osoitetietojen lähteestä puuttuu
5. Viesti on jotakin maailmassa yleisesti käytettyä kieltä, esimerkiksi englantia tai kiinaa, eikä sellaista kieltä, jolle sinulle yleensä kirjoitetaan
6. Viestissä käytetään paljon ulkonaisia tehokeinoja, esimerkiksi isolla kirjaimilla kirjoittamista tai erikoisia fontteja ja värejä
7. Viestissä vedotaan ihmisten myötätuntoon ja sääliin taikka helpon rikastumisen haluun. Usein mainitaan iso rahasumma
8. Sinua vaaditaan toimimaan nopeasti, muuten tilaisuus menee ohi
9. Sinua vaaditaan pitämään asia salassa
10. Viesti tarjoaa jotakin, jonka laillisuutta on syytä epäillä. Jos viestissä erityisesti vakuutellaan, että tarjottu asia on täysin laillinen, se yleensä on laiton
11. Tiedot lähettäjästä ovat epämääräisiä, esimerkiksi pelkkä sähköpostiosoite tai nimi
12. Viesti on lähetetty jonkun tunnetun tahon nimissä tai sellaisen tukee vedoten. (Korpela 2005; s. 157 – 158.)

Usein huijauksella pyritään samaan rahaa, vieläpä niin, että huijattu joutuu kierteeseen ja joutuu maksamaan yhä lisää. Huijari ei suinkaan aina ensimmäiseksi vaadi rahaa. Hän saattaa päinvastoin kirjoittaa tarjoavansa rahaa tai muita etuja. Vasta myöhemmin sinulle kerrotaan, että sinun pitäisi maksaa muutama sata tai muutama tuhat euroa "pankkikuluihin" ja tämä voi tuntua pikkuasialta, koska luvassa on miljoonia. Huijari saattaa myös olla vain keräämässä tietoja, tavallisesti aikomuksena myöhemmin käyttää niitä hyväksi tai myydä niitä eteenpäin (esim. kehotus käydä annetulla verkkosivulla). Huijarin tarkoituksena voi olla myös pelkkä vahingoittaminen, esimerkiksi viruksen istuttaminen uhrin tietokoneeseen (esim. sähköpostin liitetiedosto). Jotkut huijarit yrittävät saada uhrinsa toimimaan halutulla tavalla, esimerkiksi alistumaan seksuaaliseen hyväksikäyttöön. Tällöin kyseessä on yleensä huijari, joka lähestyy uhrejaan yksilöllisesti ja on hankkinut heistä tietoa verkon kautta tai muutoin. (Korpela 2005; s. 158.)

Hoancan mukaan tulevaisuudessa spämmi tulee turhauttamaan käyttäjiä siinä määrin, että sähköpostin käyttö loppuu tyystin. Arvion mukaan vuonna 2015 spämmiä on 95 % kaikesta sähköpostiliikenteestä. Lisäksi spämmi aiheuttaa useita kuluja, kuten ei-toivotun postin on laskettu laskevan käyttäjien tuottavuutta 1.4 – 3.1 %. Lisäksi turha tietoliikenne maksaa niin palvelujentarjoajille ja loppukäyttäjille. Koska sähköposti on tällä hetkellä oivallinen virusten kuljetuskanava, tehokkaiden estojen ja suodatuksen vuoksi voidaan menettää muun muassa tärkeää tietoa ja näin ollen käyttäjien usko sähköpostin luotettavuutta kohtaan laskee. (Hoanca 2006; s.23.)

6.1.2 Ketjukirjeet

Kiinnostavannäköisiä juttuja levitetään usein ketjukirjeinä. Kun saat viestin, jossa sinua kehotetaan lukemaan viesti huolella ja sitten lähettämään se edelleen 5 tai 10 ystävällesi, hävitä viesti. Jos tunnet lähettäjän, voit ehkä sopivan tilaisuuden tullen ystävällisesti valistaa häntä vastaisen varalle. Ketjukirjeet ovat väärä tapa levittää tietoa, eivätkä ne useimmiten tietoa levitäkään vaan valhetta, huijausta tai huhua. Ketjukirjeet kuluttavat tietoliikenteen käsittelytehoa ja ärsyttävät monia vastaanottajia. (Korpela 2005; s. 159 – 161.)

6.1.3 Nigerialaiskirjeet

Oman lukunsa muodostavat ns. nigerialaishuijaukset, joita on liikkunut eri muodoissaan aina 1980-luvun lopusta lähtien. Aluksi huijauksia lähetettiin kirjeinä ja fakseina, mutta vuonna 2000 nigerialaisetkin (tai kuka siten huijauksen takana onkaan) keksivät siirtyä sähköpostiin. (Järvinen 2002; s. 190 – 192.) Nyt nigerialaiskirjeitä eli 419-huijauksia tulee arviolta 40 prosenttia Nigeriasta ja yhteenlaskettuna Afrikan eri maista noin 80 prosenttia. Vuonna 2002 Yhdysvaltain oikeusministeriö sai luvan avata kaiken Nigeriasta tulevan kirjepostin. 70 prosenttia kirjeistä osoittautui 419-huijauksiksi. (Virta 2006; s.15.)

Perustarina on aina sama, vaikka siitä onkin monia variaatioita: joku kenraali, merkittävässä asemassa valtion virkamies tai tämän puoliso on saanut haltuunsa suuren määrän rahaa, joka pitäisi siirtää huomiota herättämättä ulkomaille. Kirjeen lähettäjä pyytää vastaanottajan apua, koska on kuullut tämän olevan luotettava henkilö. Kyse on kymmenistä miljoonista dollareista (jopa 62 miljoonaa dollaria), joista muutama kymmenen prosenttia luvataan palkaksi siitä, että

vastaanottaja osallistuu varojen siirtämisen ilmoittamalla yhteystietonsa ja pankkitilin numeronsa. Uhri, joka lähtee huijaukseen mukaan, menettää ainakin rahansa. Niitä tarvitaan paikallisten viranomaisten lahjomiseen tai rahansiirron käytännön järjestelyihin. Uhri saatetaan myös houkutella paikan päälle rahojen siirtoa valvomaan. Tällöin on vaarassa rahojen lisäksi myös oma henki. (Järvinen 2002; s. 190 – 192.)

Sähköpostilla kerrottava tarina tuntuu hyvin uskottavalta, mutta silti on hämmästyttävää, että vielä monien varoitusten ja vuosia jatkuneen tiedottamisen jälkeen kokeneet ja koulutetut ihmiset lankeavat tällaiseen ansaan. Ahneus tai taloudellisen ahdingon synnyttämä herkkäuskoisuus ovat vahvoja motiiveja. Vuonna 2001 keskusrikospoliisi arvioi, että yksin suomalaisilta oli nigerialaiskirjeillä huijattu ainakin pari miljoonaa euroa. Australialainen kriminologian instituutti arvioi, että vuosien 1989 - 1996 välillä oli huijattu maailmanlaajuisesti yli viisi miljardia dollaria. Rahat päätyvät järjestäytyneelle rikollisuudelle ja huumekaupan pyörittämiseen. (Järvinen 2002; s. 190 – 192.)

Taistelu nigerialaiskirjeitä vastaan on muuttunut harrastukseksi. Vastahuijarit eli ”scambaittaajat” pyrkivät siihen, etteivät huijausviestin lähettäjät ehdi saada saamaan hyväuskoisia ansaan. Vastahuijari vastaa nigerialaiskirjeeseen ja näyttelee lankaan menevää aloittelijaa. Penniäkään ei luonnollisesta lähetetä ja parhaimmat scambaittaajat pitävät uhriksi muuttunutta huijaria koukussa kuukausien ajan. (Virta 2006; s. 15.)

6.1.4 Hoaxit

Hoaxit ovat pelkkää huuhaata olevia virusvaroituksia, jotka kiertävät käyttäjiltä

toisille esimerkiksi sähköposteina tai uutisryhmien välityksellä. Niissä tyypillisesti kerrotaan jostakin uudentyyppisestä tuhoisasta viruksesta, jota ei mikään torjuntaohjelma pysty havaitsemaan. Nämä huhut viruksista loppujen lopuksi toimivat itse eräänlaisina viruksina, joita pelästyneet käyttäjät sitten levittävät ympäriinsä. Verkottuminen on lisännyt merkittävästi tällaisten juttujen määrää. (Kerttula 1998; s. 402.)

6.1.5 Haittaohjelmat

Sana haittaohjelma (malware) viittaa kaikkiin niihin ohjelmiin, jotka asentuvat koneelle salaa tai lupaa kysymättä ja tuottavat käyttäjälle haittaa. Vielä 1990-luvulla tähän ryhmää kuuluivat vain virukset ja muutama harvinainen troijalainen, mutta nopeiden verkkoyhteyksien myötä haittaohjelmien määrä ja uhkapotentiaali ovat nousseet aivan uudelle tasolle. (Järvinen 2006; s. 77.)

Kerttula määrittelee haittaohjelman seuraavasti: Malware on yleinen nimike kaikille vahinkoa tuottaville ohjelmille - viruksille, troijalaisille, madoille, loogisille pommeille sekä muille vastaaville ohjelmille. Virukset, jotka eivät sisällä mitään varsinaista tuhoa aiheuttavaa aktivoitumisrutiinia, kuuluvat nekin malware-termin piiriin. (Kerttula 1998; s. 402.)

Symantecin kahdesti vuodessa julkaiseman Internet Security Threat-raportin mukaan 50 yleisimmästä haittakoodista 66 prosenttia oli tarkoitettu salassa pidettävän tiedon varastamiseen. Kasvua edelliseen raportointikauteen oli 48 prosenttia. (Karkimo 2007; s. 13.)

Haittaohjelmat voivat:

- hidastaa ja häiritä koneen toimintaa esimerkiksi sammuttamalla koneen kesken työskentelyn
- varastaa koneelta tiedostoja
- seurata, mitä käyttäjä tekee koneella. Ohjelma voi esimerkiksi kopioida kaikki näppäinpainallukset ja välittää tiedon haittaohjelman lähettäjälle, jolloin lähettäjä saattaa saada haltuunsa käyttäjän tunnuksia ja salasanoja
- ohjata verkkopankkia käyttävän asiakkaan maksut väärille tileille ilman, että asiakas huomaa asiaa. (Salmi 2006; s. 5.)

6.1.6 Nollapäiväaukot

Välineenä on haittaohjelma, joka ujutetaan organisaation viattomalta näyttävän Microsoft Office-dokumentin sisällä. Hyökkääjä hyödyntää ennalta tuntematonta, niin sanottua nollapäivähaavoittuvuutta, joka mahdollistaa vihamielisen koodin ajamisen työasemassa, kun Office-dokumentti avataan. Tietoja urkkiva haittaohjelma on tarkoitusta varten laadittu, joten virustorjuntaohjelman sormenjälkipohjainen tunnistus ei tunne sitä. Suojautumisen tekee haasteelliseksi se, että yhtä turva-aukkoa käytetään yleensä vain yhteen hyökkäykseen. Teoriassa siis Office-ympäristön ahkera päivittäminen ei suojaa hyökkäyksiltä, koska tulevissa tietomurroissa ei samaa haavoittuvuutta enää hyödynnetä. Yleensä kohteena ovat vanhat eli Office 2000-versiot. Hyökkäysväline on lähes aina Office-dokumentti eli Word-, Excel- tai PowerPoint-liite, joka lähetetään organisaatioon sähköpostin liitteenä. Sähköpostisuodatusta tarjoava Messagelabs kertoi huhtikuussa (2007) löytäneensä 592 sähköpostia, joilla oli toteutettu 249 erillistä hyökkäystä. Hyökkäysten koteina on ollut muun muassa elektroniikkateollisuuden, puolustusteknologia- ja ydinvoima-alan toimijoita, asianajotoimistoja ja oppilaitoksia. Hyökkäyksissä käytettyjä sähköpostiotsikoita ja liitetiedostojen

nimiä ei yleensä anneta julkisuuteen. (Laurio 2007; s. 31 – 32.)

6.1.7 Virukset

Vahingontekijä asentaa tietokoneeseen ohjelman pyrkien vahingoittamaan tietokonetta tai varastamaan sillä olevia tietoja. Tällaisia asentuvia ohjelmia kutsutaan viruksiksi. (Odom 2005; s. 385.)

Ensimmäinen PC-virus havaittiin Pakistanissa tammikuussa 1986. Nimellä Brain kutsutun viruksen kirjoittivat parikymppiset veljekset Basil ja Amjad Alvi, ja heidän oli helppo jäljittää, sillä he ikuistivat nimensä, osoitteensa ja puhelinnumeron viruksen ohjelmakoodiin. Nimi Brain on peräisin poikien tietokonealan yrityksestä Brain Computer Services. Alkuperäinen virus tarttui 360 kilotavun levykkeiden välityksellä. Seuraava virus havaittiin vuonna 1988, joka oli nimeltään Ping-Pong sen aikaisen tv-pelin mukaan. Tämä italialainen virus aktivoituessaan sai pienen pallon liikkumaan kuvaruudun poikki. Koko virusongelmaa pidettiin ohimenevänä ilmiönä. Koska tietoliikenneyhteyksiä ei harrastajien BBS-järjestelmiä lukuun ottamatta ollut, virukset saattoivat levitä vain levykkeiden välityksellä ja se oli hidasta. Suomessa ensimmäiset virukset havaittiin vasta vuonna 1988 ja aluksi ne olivat vain Macintosh-käyttäjien ongelma. PC-virukset tekivät maihin nousun vuonna 1989, myös Suomeen. (Järvinen 2002; s. 250.) Sitä mukaa, kun uusia laitteistoja ja käyttöjärjestelmiä kehitetään, viruksenkirjoittajat kehittelevät niille uusia viruksia. Lisäksi nopeiden tietoliikenneyhteyksien yleistyminen on kasvattanut räjähdysmäisesti erilaisten virusten lukumäärää. Tänään virukset ovat jokapäiväinen riesa ja tuttu käsite jokaiselle käyttäjälle. Tunnetuimpia viruksia ovat CIH, LoveLetter, Anna Kournikova ja Nimda.

Haittaohjelmista ikävimpiä torjuttavia ovat itseään muuntelevat eli polymorfiset virukset. Tällainen virus saattaa näyttää ennen suoritusta täysin vaarattomalta, mutta suorituksen aikana ohjelmakoodia tai rekisterin sisältöä muutetaan siten, että ohjelmasta hypätään toisaalle muistiin tallennettuun haittaohjelmaan. (Ahonen 2006; s. 8.)

Joka viides eurooppalainen on menettänyt tietokoneeseen tallennettuja henkilökohtaisia tiedostoja, kuten valokuvia, musiikkia ja osoitetietoja, tietokoneviruksen takia. Tietoturvayhtiö McAfeen teettämän tutkimuksen mukaan kaksi kolmasosaa tallentaa valokuvat vain digitaalisessa muodossa. Arvioiden mukaan eurooppalaisilla on koneillaan pelkästään musiikkitiedostoja yhteensä yli 15 miljardin euron arvosta. (Mikrobitti (1/06) 2006; s. 9.)

6.1.8 Troijan hevoset

Troijan hevonen on ohjelma, joka tekee jotakin muuta kuin mitä käyttäjä odottaa. Kyseinen toiminto tulee olla rakennettu ohjelmaan tarkoituksella. Troijan hevoset lähes poikkeuksetta sekoitetaan viruksiin. Näillä kahdella on kuitenkin yksi merkittävä ero - troijalaiset eivät levitä itse kopioita itsestään, toisin kuin virukset. Troijan hevoset kykenevät leviämään vain käyttäjän avustuksella. Tästä syystä troijalaiset ovat merkittävästi viruksia harvinaisempia. (Kerttula 1998; s. 402.)

6.1.9 Verkkomadot

Verkkomadot ovat pieniä ohjelmia, jotka leviävät netin välityksellä koneesta toiseen. Madot poikkeavat viruksista kahdella tavalla:

- ne eivät tarvitse isäntäohjelmaa, vaan levittävät itse itseään kopioimalla
- mato aktivoituu täysin automaattisesti, joten omalla varovaisuudella ei voi juurikaan vaikuttaa asiaan. (Järvinen 2002; s. 255.)

6.1.10 Bottiverkot

Bottiverkoiksi (botnet) kutsutaan joukkoa koneita, jotka on valjastettu ulkopuoliset tahon käyttöön uhrien itsensä tietämättä. Termi on peräisin alun perin IRC-kanavilla käytetyistä bot-ohjelmista, jotka suorittivat automatisoituja tehtäviä.(Järvinen 2002; s. 255.)

Botnetit eli lähinnä kaapatuista kotikoneista muodostetut hyökkäysverkot ovat nostaneet voimakkaasti päätään etenkin viime vuoden loppupuolella. Iso-Britannia on nykyisin suuri botnet-alusta, koska laajakaistayhteydet ovat lisääntyneet. Kärkimaat ovat USA, Kiina ja Iso-Britannia. (Karkimo 2006; s. 17.)

6.1.11 Näppäimistökaapparit

Näppäimistökaapparit (keyboard loggers) ovat salasanojen ja käyttäjätunnusten kaappaamiseen erikoistuneita ohjelmia. Ne jäävät muistiin ja heräävät, kun uhri menee vaikkapa verkkopankin sivuille. Ohjelma nappaa syötetyt tunnukset muistiin ja lähettää ne isännälleen IRC-kanavalla tai sähköpostiviestinä. (Järvinen 2002; s. 256.)

6.1.12 Modeemikaapparit

Uhrin koneeseen lähetetään haittaohjelma, joka ohjelmoi modeemin tai ISDN-kortin soittamaan ulkomaiseen palvelunumeroon. Sieltä yhteys kiertää normaalisti Internetiin, mutta käyttö voi maksaa jopa useita euroja minuutilta. (Järvinen 2002; s. 257.)

6.1.13 Rootkitit

Rootkittien historia ulottuu Unix-aikaan asti. Nimensä mukaisesti rootkit oli ohjelmakokoelma, jotka istutettiin murrettuun tietokoneeseen. Paketti sisälsi joukon Unix-apuohjelmia, joilla korvattiin käyttöjärjestelmän alkuperäiset komennot. (Järvinen 2002; s. 258.)

Näillä ohjelmilla hyökkääjä voi hallinnoida konetta Administrator-tason oikeuksilla. Rootkitit ovat entistä suositumpia, sillä niiden olemassaolo voidaan piilottaa järjestelmässä ja niiden löytäminen on vaikeaa. Ne voivat korvata kokonaisia tiedostoja, komentoja tai ominaisuuksia (esimerkiksi Windows Task Manager) omilla saastuneilla versioillaan. Niiden suosiota lisää myös se, että ne tekevät viruksista sekä muita hyökkäyksistä entistä tehokkaampia ja niiden avulla voidaan varastaa arvokasta informaatiota. Näitä käytetään esimerkiksi khalastelussa. (Geer 2006; s. 17 – 18.)

6.1.14 Valeturvaohjelmat

Netti on tulvillaan hyödyllisiä apuohjelmia, mutta valitettavasti kaikki eivät ole sitä miltä näyttävät. Ne poistavat näön vuoksi levyltä haittaohjelmia, mutta asentavat samalla omat haittaohjelmansa tilalle.

6.2 Internetin vaarat

Sähköisessä ympäristössä liikkuu vastuullisten ja asiallisesti toimivien yritysten lisäksi myös huijareita. Huijausten tarkoituksena on houkutella kuluttajia maksamaan tavaroista ja palveluista, joita ei ole olemassa tai jotka eivät toimi. Kohteeksi voi joutua kuka tahansa iästä tai koulutuksesta riippumatta. (Salmi 2006; s. 9.)

Yleisimpiä huijausmenetelmiä ovat:

- Ennakko- tai liittymismaksut

  Kuluttajaa houkutellaan arpajais- tai lottovoitolla, muulla palkkiolla tai mahdollisuudella ansaita suuria summia kotona työskentelemällä. Enne rahojen saamista kuluttajan on kuitenkin maksettava ennakko- tai liittymismaksu. Luvattua palkkiota ei koskaan tule eikä ennakkoon maksettuja rahoja saa koskaan takaisin.
- Sijoitushuijaukset

  Kuluttajalle tarjotaan osake-, kiinnelaina- tai kiinteistösijoituksia, optioiden kauppa tai valuuttakauppaa, jolle luvataan korkeita tuottoja. Sijoitukset ovat kuitenkin yleensä täysin arvottomia.
- Pyramidimarkkinointi

  Pyramidimarkkinointi muistuttaa verkostomarkkinointia, mutta siinä jä-

senen tulot eivät kerry tuotteiden myynnistä, vaan uusien jäsenten hankinnasta. Käytännössä kaikki pyramidijärjestelmät hajoavat jossain vaiheessa ja alatasoilla olevat menettävät sijoittamansa rahat. pyramidimarkkinointi on Suomessa laitonta.

- Maksulliset palvelunumerot

  Kuluttaja ohjataan esimerkiksi ilmaisen matkan tai arpajaisvoiton lunastamiseksi soittamaan palvelunumeroon. Kuluttajalle ei välttämättä kerrota, että palvelunumero on maksullinen. Yleensä numerossa vastaa automaatti, joka yrittää venyttää puhelua mahdollisimman pitkään ja kerryttää näin soittajan puhelinlaskua.

- Ihmetuotteet

  Kuluttajalle annetaan tuotteen ominaisuuksista katteettomia lupauksia. Tyypillisiä esimerkkejä ovat laihdutustuotteet, joiden luvataan pudottavan painoa ilman, että tarvitsee tehdä mitään muutoksia elämäntapoihin. (Salmi 2006; s. 9.)

Huijausten onnistumista lisää se, että niissä hyödynnetään usein tehokkaasti psykologisia keinoja:

- Vedotaan ihmisten toiveisiin nopeasta rikastumisesta, elämän kohentumisesta tai laihtumisesta
- Vedotaan palvelun tai tuotteen laajaan suosioon
- Vedotaan auktoriteettiin
- Kerrotaan, että tarjous on voimassa vain hyvin lyhyen aikaa tai että tuotetta on tarjolla vain rajoitetusti
- Annetaan joku nimellinen lahja, jonka jälkeen kuluttaja tuntee olevansa vastapalveluksen velkaa ja tarjouksesta kieltäytyminen on vaikeampaa.

(Salmi 2006; s. 10.)

6.2.1 Phishing eli Khalastelu

Termi phishing on yhdistelmä sanoista password ja fishing. Khalastelu tarkoittaa tietojen urkkimista pahaa-aavistamattomilta käyttäjiltä. Huijarit keräävät tietoja, joista on heille taloudellista hyötyä: pankkitilien numeroita, pin-koodeja, salasanoja ja käyttäjätunnuksia. (Järvinen 2006; s. 273 – 274.)

Khalastelu on sikäli erikoinen tietoturvauhka, että koska se perustuu käyttäjien huijaamiseen, käyttöjärjestelmällä tai turva-aukoilla ei ole mitään merkitystä. Kyse on social engineering – hyökkäyksestä, jossa uhri huijataan luovuttamaan luottamuksellista tietoa. (Järvinen 2006, s. 274.)

Phishing-hyökkäysten määrä on jatkanut kasvuaan. Viime vuonna niiden määrä kasvoi 2,99 miljoonasta 5,7 miljoonaan viestiin päivässä. (Mikrobitti (1/06) 2006, s. 9.)

6.2.2 Kaikki verkkokaupat eivät ole aitoja

Sähköinen kaupankäynti nostaa päätään entisestään. Sen vuotuiset myyntiluvut ovat kaksinkertaistuneet viimeisen vuoden aikana Pohjoismaissa. Suurin este verkkokaupan räjähdysmäiselle kasvulle lienee huoli tietoturvasta. Esimerkiksi 70 prosenttia niistä suomalaisista, jotka eivät tee Internet-ostoksia, sanoo ostamatta jättämisen syyksi huolen tietoturvasta. He eivät halua paljastaa luottokorttinsa numeroa Internetissä. (Mikrobitti (1/06) 2006, s. 9.)

Epäilyttävän verkkokaupan tai arveluttavan palvelun voi joskus tunnistaa maalaisjärkeä käyttämällä. Monilla aloilla Internet mahdollistaa uudenlaisen, hyvin kevyen ja edullisen toimintamallin, jonka ansiosta hintataso saadaan alhaiseksi. Silti ero perinteiseen kauppaan ei voi olla kovin suuri. Jos sivusto lupaa tuotteita tai palveluita puoleen hintaan, jossain on koira haudattuna. Luottokortin käyttö netissä on turvallista, kunhan noudattaa normaalia kortin haltijalta edellytettävää huolellisuutta ja varovaisuutta. Luottokorttiyhtiöt ovat tarkkoja korteistaan. Jos jonkin verkkokaupan toiminnasta tulee jatkuvasti reklamaatioita ja veloitusten oikeellisuus kiistetään, korttiyhtiö sanoo sopimuksensa kauppiaan kanssa irti. Kansainvälisessä kaupassa kaikki ennakkomaksut ja tilisiirrot ovat varottavia. Luotettavalla nettipalvelulla pitäisi aina olla fyysinen katuosoite. Ei herätä luottamusta, jos www-sivulla mainitaan vain sähköpostiosoite ja mahdollisesti puhelinnumero. Tosin www-sivuilla ilmoitettu osoitekaan ei välttämättä ole todellinen, ja sen tarkistaminen ulkomailta on liki mahdotonta. Kieliasu korreloi jossain määrin luotettavuuden kanssa. Vakavasti otettavan palvelun sivuilla ei ole kirjoitusvirheitä. (Järvinen 2006; s. 54 – 55.)

6.2.3 Domain-nimien luotettavuus ja sivujen väärentäminen

Verkkosivut eivät aina ole sitä, miltä näyttävät. Kansainvälisten domain-nimien varaaminen on vapaata, eikä hakijan tarvitse etukäteen todistaa oikeuttaan nimeen. Päällekkäisyydet ja suoranaiset riidatkin ovat väistämättömiä; niitä ratkotaan jälkikäteen oikeudessa tai joskus ostamalla nimi rahalla. YK:n alaisuudessa toimiva WIPO on toiminut sovitteluelimenä kansainvälisissä tapauksissa. (Järvinen 2002; s. 207.)

Oman lukunsa muodostavat ne kaapparit, jotka väijyvät tunnetuilta yrityksiltä

vapautuvia nimiä ja kaappaavat ne itselleen. Nimestä saattaa tulla vapaata riistaa, jos yritys unohtaa uusia sen ajoissa tai rahaliikenteessä on jokin sekaannus, eikä uusimismaksu mene perille. Sen jälkeen osoitetta yritetään myydä takaisin yritykselle rahaa vastaan tai sen osoitteeseen perustetaan kyseenalainen aikuisviihdepalvelu. (Järvinen 2002; s. 208.)

Sivujen kopiointi käy hetkessä ja tulos on täysin alkuperäisen kaltainen. Osoitteiden ja muiden turvamekanismien kiertäminen ei sitten enää onnistukaan yhtä helposti. Mutta aika pitkälle voi päästä, ja kokemattomaan käyttäjään kömpelökin huijaus menee täydestä. (Järvinen 2006; s. 59.)

1. Harhaanjohtava linkki

   Linkissä näkyy osoite www.pankki.fi, mutta todellinen osoite vie hakkerin omaan palveluun. JavaScript-koodilla on mahdollista poistaa selaimen osoiterivi näkyvistä, joten käyttäjän voi olla vaikea havaita päätyneensä väärälle sivustolle.

2. Harhaanjohtava domain-nimi

   Käytetään alkuperäistä muistuttavaa, mutta siitä hieman poikkeava domain-nimeä. Suomen domain-nimiä jakava Viestintävirasto tuskin hyväksyisi ilmiselvästi huijaustarkoituksissa varattuja domain-nimiä, mutta kansainvälisissä net-, com- ja org-alueissa mitään kontrollia ei ole.

3. Osoitteen väärentäminen grafiikalla

   Joissakin selaimissa on mahdollista kikkailla niin, että osoiterivin päälle piirrettävällä kuvalla peitetään todellinen osoite ja näytetään sen tilalla huijarin haluama osoite.

4. DNS-palvelun manipulointi

   Jos huijari pääsee manipuloimaan DNS-palvelua, hän voi ohjata osoitepyyntöjä haluamiinsa osoitteisiin. Esimerkiksi huijari voi yrittää napata

kerrostalon taloverkossa liikkuvaa DHCP-kyselyä, jolla käyttäjän kone pyytää IP-osoitetta ja DNS-palvelinten osoitteita.

5. Hosts-tiedoston muokkaus

   Kun Windowsin pitää selvittää verkkonimeä (joko Internet-nimi tai lähiverkon sisäinen Netbios-nimi) vastaava laiteosoite, se tarkistaa ensimmäiseksi, löytyykö nimi hosts-tiedostosta. Jos tieto löytyy, sitä käytetään eikä enempiä selvityksiä tehdä. Hosts on tavallinen tekstitiedosto, joten sitä voi muokata vaikka Notepadilla.

6. Selaimen turva-aukot

   Viimeinen keino on hyödyntää selaimessa olevaa turva-aukkoa eli haavoittuvuutta, joka mahdollistaa osoitetiedon väärentämisen. Näin vakavat aukot harvinaisia, esiintyvät vain tietyissä selaimen versioissa ja ne paikataan nopeasti. (Järvinen 2006; s. 60 – 66.)

6.2.4 Varmenteet merkki aitoudesta

Varmenne eli sertifikaatti on sähköinen todistus. Se sisältää joukon tietoja, jotka varmenteen myöntäjä on tarkistanut ja todennut oikeiksi. Sen jälkeen hän on laskenut tiedoista tiivisteen ja allekirjoittanut sen digitaalisesti. Henkilö, jolle varmenne esitetään, tarvitsee myöntäjän julkisen avaimen purkaakseen tiivisteen ja verratakseen sitä itse laskemaansa. Jos tulokset täsmäävät, varmenteessa kerrottua tietoa voidaan pitää uskottavana. (Järvinen 2003; s. 160.)

Parhaana takeena www-sivuston aitoudesta toimii SSL-varmenne. Miljoonat ihmiset käyttävät SSL-salausta päivittäin. SSL:n yleisesti käytetty 128-bittinen versio on nykytietämyksellä täysin turvallinen, eikä sitä pystytä murtamaan. SSL on lyhenne sanoista Secure Sockets Layer. Kyse on salaustekniikkaan perustavasta protokollasta, joka estää ulkopuolisia näkemästä nettiliikenteen sisäl-

töä. Selain erottaa aidon palvelun varmenteilla. Varmenne, josta suomenkielinen Windows käyttää nimitystä sertifikaatto, on sähköinen henkilöllisyystodistus. Jokin taho on ensin tarkistanut palvelun aitouden ja myöntänyt sille todistuksen, jonka selain surffauksen aikana tarkistaa ja hyväksyy. Jos varmenne havaitaan väärennetyksi tai se ei jostain syystä kelpaa, selain antaa varoituksen. Varmenteita myöntävästä tahosta käytetään nimitystä Certificate Authority ali CA. (Järvinen 2006; s. 67.)

Erilaisia varmenteita:

1. Sähköposti. Hankkimalla toistensa varmenteet kaksi henkilöä voi lähettää toisilleen salattua sähköpostia, vaikka eivät olisi ikinä tavanneet toisiaan. Niin ikään osapuolet voivat olla varmoja siitä, että sähköpostiviestit todella tulevat oikealta henkilöltä.
2. Palvelinvarmenteet. Internet-palvelimelle asennettava varmenne todistaa, mikä palvelin on kyseessä. Käyttäjän selain tarkistaa palvelimelta saamansa varmenteen tiedot ja varoittaa, jos ne eivät täsmää. Näin estetään hyökkääjää ohjaamasta selainta omalle valesivulleen.
3. VPN-varmenne. Yrityksen palomuuri saattaa vaatia tietokoneita todentamaan itsensä varmenteella, ennen kuin VPN-yhteys sisäverkkoon avataan.
4. HST-varmenne. HST-kortti sisältää Väestörekisterikeskuksen kansalaiselle myöntämän varmenteen tämän henkilöllisyyden todistamiseksi.
5. Omien tiedostojen salausvarmenne. Käytettäessä Windows 2000:sta alkaen tarjolla olevaa EFS-tiedostojärjestelmää (Encrypted File System) Windows luo automaattisesti 100 vuotta voimassa olevan varmenteen ja siihen liittyvät avaimet, joita tiedostojen salaukseen käytetään.

6. Ohjelmien päivitysvarmenne. Windowsin automaattinen päivitystoiminto (Update) varmentaa ladattavat päivitykset ja niitä jakavan palvelimen varmenteella, jotta kukaan ulkopuolinen ei pysty ujuttamaan koneeseen viruksia tai takaportteja kaappaamalla itselleen Windows päivityksen aikana kulkevaa datavirtaa.
7. ActiveX-varmenne. Varmenne, joka takaa www-sivuilta ladattavien ActiveX-ohjelmien aitouden. Varmenne ei kuitenkaan takaa ohjelmien tekijän tarkoitusperiä – ohjelma saattaa aiheuttaa käyttäjälle vahinkoa tarkoituksellisesti tai ohjelmointivirheen seurauksena. (Järvinen 2003; s. 162.)

6.3 Piratismi

Sisältöteollisuus on onnistuessaan hyvä bisnes, mutta siinä on myös ongelmansa. Niistä merkittävin kopiointi. Se on kiusannut aina niin musiikin, elokuvien, kirjojen kuin tietokoneohjelmienkin tekijöitä. Koska kyse on immateriaalisesta hyödykkeestä, tuottaja ei voi suojata teosta ja rajoittaa sen käyttöä samalla tavalla kuin esimerkiksi lypsykarjatilan isäntä voi määrätä maidostaan. (Järvinen 2003; s. 346.)

6.3.1 Plagiointi ja piratismi

Plagioinnilla tarkoitetaan toisen tekstin tai taideteoksen (esim. sävellyksen) esittämistä omanaan - toisin sanoen varastamista. Plagiaatti on kirjallinen tai taiteellinen varkaus tai sellaiseen perustuva teos.
Piratismi on sen sijaan ohjelmistojen laitonta kopiointia, osapuilleen samaa kuin plagiointi. Piraattikopio on luvaton alkuperäisestä tai sen jäljennöksestä tehty tietokoneohjelman tai esimerkiksi musiikkiäänitteen kopio. Laitonta kopiointia

on esiintynyt yhtä kauan kuin mikrotietokoneet ovat olleet olemassa. BSA:n (Business Software Alliance) arvioiden mukaan jopa joka toinen Suomessa käytetty ohjelma olisi laiton kopio. Italiassa ja Espanjassa tämä luku on vielä korkeampi, arviolta 75 %. Vaikka tekijänoikeuksien valvonta onkin tehostunut, ovat uudet Itä-Euroopan valtiot osoittautuneet ongelmallisiksi, sillä laillisuuden valvonta ei ole kehittynyt niissä samalle tasolle kuin Yhdysvalloissa ja vanhoissa EU-maissa. Plagioinnin ja piratismin erona voisi pitää sitä, että piratismi on kaupallisempaa ja järjestelmällisempää toimintaa, ja digiaika on tehnyt siitä liiketoimintaa. (Mäkinen 2006; s. 191.)

Laajakaistaisten Internet-yhteyksien yleistyessä 1990-luvun lopulla alkoi uusi aikakausi piratismissa. Lisäksi Napsterin ilmaantuminen miljooniin koneisiin ympäri maailmaa vuonna 1999 räjäytti mp3:ten suosion. Helmikuussa 2001 palvelulla mitattiin olevan yli 25 miljoonaa käyttäjää mutta artistit ja levy-yhtiöt eivät arvostaneet musiikin ilmaisjakelua ja Metallica sekä Dr. Dre käynnistivät paljon julkisuutta saaneet oikeusjutut yhtiötä vastaan. Napster on jälleen elossa maksullisena palveluna. Mutta P2P-ohjelmat (vertaisverkko-ohjelmat) täyttivät Napsterin jättämän aukon. (Komonen 2006; s. 38.)

Nuoriso kopioi musiikkituotteita varmaan sen kummemmin ajattelematta, ja usein syyksi ilmoitetaan äänitteiden korkea hinta. Suuria monikansallisia mediataloja syytetään rahastamisesta ja kopioiden tekemistä pidetään eräänlaisena Robin Hood-toimintana. Tekijänoikeuslain mukaan kopioiminen omaan käyttöön ei olekaan kiellettyä - ja niin kauan kuin se pysyy oman perheen sisällä ja kyseessä on yksityiskäyttö, laittomuuksiin ei ole syyllistytty. Vasta kun toiminta muuttuu järjestelmälliseksi ja kaupalliseksi, on se kiellettyä.
Piratismi rikkoo siis tekijänoikeuksia, joka puolestaan suojaa luovaa työtä ja sen

tekijöitä. Aina kun toiminta on ammattimaista, se on kiellettyä. Piratismia on myös tuotteiden maahantuonti ja niiden levittäminen verkossa. Joskus piratismi liittyy kansainväliseen talousrikollisuuteen, joka on hyvin johdettua ja organisoitua. (Mäkinen 2006; s. 196.)

Suomen piraattiherkkyyteen - onhan se kaksinkertainen muihin Pohjoismaihin, vaikuttaa todennäköisesti Venäjän läheisyys. Vaikka Suomessa piratismi on yleistä, melkein samalla tasolla eteläeurooppalaisten maiden kanssa (uudet EU-maat ovat asia erikseen), ei Suomi onneksi joudu IFPI:n "mustalle listalle" (International Federation of the Phonographic Industry). Sinne ovat päässeet Brasilia, Kiina, Meksiko, Paraguay, Venäjä, Espanja, Taiwan, Thaimaa, Ukraina ja uutena maana Pakistan. Verkossa tapahtuva piratismi lisääntyi Suomessa vuonna 2004; tähän on muun muassa vaikuttanut laajakaistayhteyksien yleistyminen. (Mäkinen 2006; s. 197.)

Kopiointia ei voi suoraan rinnastaa varastamiseen, koska immateriaalinen hyödyke ei vähene teon seurauksena. Kopiointi aiheuttaa varkauteen verrattavia taloudellisia tappioita vain siltä osin, kuin se vähentää muutoin tapahtuvaa myyntiä. Ääritapauksessa se voi jopa lisätä myyntiä, kun tieto hyvästä musiikista leviää. Jonkinlaisen sisällön vapaa saatavuus on aina kuulunut asiaan. Tekijänoikeuslaki menee jopa niin pitkälle, että se nimenomaisesti turvaa kansalaisen oikeuden kopioida sisältöä yksityiseen käyttöön. Digitaalitekniikka on muuttanut kopioinnin olemusta. Kertaalleen ostetusta CD-levystä on mahdollista tehdä rajattomasti kopioita, jotka ovat laadultaan täsmälleen alkuperäisen kaltaisia. Voikin väittää, ettei kyse ole enää kopioinnista, vaan luvattoman kappaleen valmistuksesta. Juuri tämä on saanut levy-yhtiöt huolestumaan. Niiden omien tehtaiden lisäksi levyjä valmistetaan nyt myös kodeissa. (Järvinen 2003;

s. 347.)

6.3.2 Vertaisverkot

Vuonna 2002 ohjelmoija Bram Cohen esitteli uuden bittorrent-protokollan ja asiakasohjelman, joka yhdisti ja paranteli edeltäjiensä ominaisuuksia. Bittorrent-verkossa tiedostojen jakaminen toimii hyvin nopeasti käyttäjien kesken ilman minkäänlaista keskuspalvelinta. Ainoastaan niin sanotun trackerin säilytykseen tarvitaan palvelin. Tutkimusten mukaan noin kymmenen prosenttia kaikesta tietoliikenteestä on P2P-liikennettä. (Komonen 2006; s. 39.)

Vertaisverkko-ohjelmia ovat muun muassa Kazaa, BitTorrent, eMule ja DC++. Vertaisverkko tarkoittaa verkkoa, jossa koneet ovat keskenään samassa asemassa, samanvertaisina. Vertaisverkossa jokainen kone toimii myös palvelimena. Perusajatus on, että kukin vertaisverkkoon liittyvä käyttäjä asentaa koneeseensa erityisen ohjelmiston, joka sekä ottaa vastaan aineistoa vertaisverkosta että lähettää aineistoa siihen. Tämä mahdollistaa sen, että suositun tiedoston levitessä kukin vastaanottaja samalla myös jakaa sitä eteenpäin. Näin vältetään yhden tai muutaman palvelimen järjestelmästä johtuva ruuhkaisuus. Käytännössä vertaisverkkoon liittyminen edellyttää kiinteää ja suhteellisen nopeaa Internet-yhteyttä. (Korpela 2005; s. 147.)

Se, mikä oikeasti on muuttunut, ei olekaan kopiointi vaan jakelu. Internet on synnyttänyt peer-to-peer – verkostoja, joissa miljoonat ihmiset voivat napin painalluksella kopioida ”kavereilleen” sisältöjä maasta toiseen, nimiä paljastamatta. Tämä on aidosti uusi ja levy-yhtiöiden kannalta vaarallinen tilanne, eikä enää vastaa lainsäätäjän alkuperäistä ajatusta yksityisestä kopioinnista. P2P-

verkosta saa melkein minkä tahansa musiikkiesityksen ja videon omalle koneelleen nappia painamalla. Kuka voisi vastustaa tällaista helppoutta ja edullisuutta? Vastaavaa laillista kanavaa ei ole. (Järvinen 2003; s. 347.)

Vertaisverkot ovat yleistyneet muun muassa siksi, että niitä on vaikea valvoa. Internetin vertaisverkot eivät sinänsä ole laittomia, mutta hyvin suuri osa niissä tehdystä kopioinnista rikkoo lakia. Niihin liittyy myös tietoturvaongelmia. Jos asentaminen tehdään huonosti, ohjelma saattaa jakaa koko kovalevysi sisällön kaikkien saataville vertaisverkossa. (Korpela 2005; s. 148.)

6.4 Muita tietotekniikkarikollisuuden alalajeja

On erilaisia tekniikoita varastaa tietoa tai haitata muulla tavoin yrityksen toimintaa verkon läpi. Lisäksi vanhanaikainen tapa suorittaa varkaus on varastaa fyysisesti laite. Nykyisyydessä ja varsinkin tulevaisuudessa suuri rikollisuuden laji on identiteettivarkaudet, jotka ovat jo varsin yleisiä Yhdysvalloissa tällä hetkellä.

6.4.1 Palvelunestohyökkäys

Vahingontekijä voi tehdä asioita, joiden seurauksena palvelin vikaantuu. Tällaista tekoa kutsutaan palvelunestohyökkäykseksi (engl. Denial of Service attack eli DoS). (Odom 2005; s. 385.)

Niin sanotut palvelunestohyökkäykset tehdään useimmiten hyödyntämällä ohjelmistojen virheitä tai puutteita. Palvelunestohyökkäykset toimivat siten,

että ne aiheuttavat verkkokapasiteetin ylimääräistä kulutusta, kyllästävät resursseja tai kaatavat järjestelmiä tai sovelluksia ja estävät tai hidastavat palveluita. (Penttinen 2006; s. 188.)

Palvelunestohyökkäys kuuluu niiden hyökkäysten ryhmään, jotka aiheuttavat palvelun saannin katkeamisen tai estävät palvelun toiminnan. Palvelunestohyökkäyksiä on monenlaisia ja niillä voidaan iskeä monenlaisiin kohteisiin. Iskun seuraukset voivat kestää minuutteja, tunteja tai päiviä ja voivat vaikuttaa verkon suorituskykyyn, datan eheyteen ja järjestelmän toimintaan. (Anonymous 2002; s. 324.)

6.4.2 Tiedustelu ja sosiaalinen tekniikka

Tiedustelu on prosessi, jossa kerätään tietoa tietystä kohteesta tai kohteista. Sosiaaliseen tekniikkaan kuuluvat juonet, puijaukset ja ihmisten manipulointi niin, että he antavat tietoja, joista on haittaa yritykselle, organisaatiolle tai henkilölle. Tällaisista tiedoista voi olla apua hyökkäyksen suunnittelussa, organisoinnissa tai toteuttamisessa. (Anonymous 2002; s. 74 – 75.)

Järvinen määrittelen saman termin seuraavasti: Social engineering kuvaa toimintaa, jossa teknisiä suojakeinoja kierretään psykologisin keinoin. Hyökkääjän tavoitteena on saada työntekijä paljastamaan tietoja verkon suojauksista tai jopa oma käyttäjätunnus ja salasana. (Järvinen 2002; s. 307.)

Social engineering-tekniikan variaatioita ovat shoulder surfing ("olan yli surffaus"), jossa kurkitaan käyttäjän kirjoittamia salasanoja sekä dumpster diving ("roskisdyykkaus"), jossa tietoturvaan liittyviä dokumentteja ja pois heitettyä

atk-materiaalia kaivetaan roskalaatikoista. (Järvinen 2002; s. 308.)

6.4.3 Porttiskannerit ja passiivinen käyttöjärjestelmän tunnistus

Porttiskannerit ovat ohjelmia, jotka tarkistavat, onko tietokoneen TCP/IP-pinossa kuuntelutilassa olevia portteja. TCP/IP yhdistää monia protokollia ja mahdollistaa Internetissä tapahtuvan tiedostonsiirron. Ohjelmoijat voivat kirjoittaa ohjelmia, jotka selvittävät, mitkä portit ovat avoinna ja mitkä suljettuja. (Anonymous 2002; s. 76.)

6.4.4 Turva-aukot

Seuraava vaihe on varsinainen murtautuminen tietokoneverkkoon. Sen krakkerit tekevät käyttämällä hyväksi käyttöjärjestelmien palvelujen heikkoja kohtia. On olemassa paljon turva-aukkoja; oikean aukon löytäminen voi olla vaivalloista. Kaikkia aukkoja ei ole luotu samanarvoisiksi eli useimmat aukot ovat käyttöjärjestelmästä riippuvaisia. (Anonymous 2002; s. 86.) Turva-aukkoa hyödyntävää ohjelmaa kutsutaan eksploitiksi (exploit). (Järvinen 2006; s. 25.)

6.4.5 Henkilöllisyysvarkaudet

Henkilöllisyysvarkauksia on ollut aina, mutta todellinen epidemia niistä on tullut vasta Internetin myötä. Aiemmin varkaiden piti kaivaa tiedot roskalaatikoista, murtautua uhrien postilaatikoihin ja varastaa lompakoita tai käsilaukkuja, mutta nyt henkilötiedot löytyvät helpommin netistä. Kun varas on selvittänyt uhrin syntymäajan, osoitteen ja sosiaaliturvatunnuksen, sen on helppo esiintyä tämän puolesta. Varas saattaa tilata tavaraa esiintymällä uhrin nimissä tai avata

uuden luotollisen tilin ja kirjoittaa katteettomia shekkejä. Varas voi jopa ilmoittaa luottokorttiyhtiölle ja pankille osoitteenmuutoksen, jotta uhri ei tiliotteista ja karhukirjeistä huomaisi, mitä on tekeillä.
Varastetun henkilöllisyyden valtaaminen takaisin sekä oman nimen ja luottohistorian puhdistaminen on iso urakka.
Internetistä henkilötietojen varastaminen on helppoa ja tavaroiden tilaus, osoitteenmuutokset ja muu asiointi onnistuu sähköpostilla ilman, että henkilöllisyyttä varmistetaan riittävästi. Jos yhteydenpito kulkee webmail-sähköpostin kautta, toisen nimissä voi esiintyä pitkäänkin paljastumatta. (Järvinen 2002; s.189.) 54 prosenttia identiteettivarkauden mahdollistamista tietovuodoista johtui tietokoneen tai tallennusmedian, kuten usb-tikun, häviämisestä. (Karkimo 2007; s. 13.)

Pääasiassa identiteettivarkauden uhri on nuori henkilö, joilla on tapana antaa itsestään tietojaan verkossa. Tyypillisesti tällaisella henkilöllä on tapana muuttaa usein kotipaikkaansa. Tutkimusten mukaan vielä useiden vuosien jälkeen, uhrilla on vaikeuksia ajoittain saada lainaa tai työtä, joitakin henkilöitä on jopa pidätetty rikoksista, joissa eivät olleet osallisina. (Sweeney 2006; s. 75.)

Tätä taustaa vasten on hyvä miettiä virtuaalisten kohtaamispaikkojen turvallisuutta. Tällaisia paikkoja verkossa on muun muassa MySpace ja Facebook. Liian usein törmää sellaiseen profiiliin, josta käy ilmi käyttäjän esimerkiksi syntymäaika, koti-osoite ja matkapuhelimen numero. Kuinka helppoa onkaan identiteettivarkaan valita uhrinsa?

6.4.6 Laite varastetaan

Matkamikrot ovat varkaiden mielikohteita. Mutta myös pöytäkoneita varastetaan, ja vieläpä keskellä kirkasta päivää. Mitä röyhkeämpi ja uskottavampi suunnitelma on, sitä todennäköisemmin se onnistuu, koska epätavallista suunnitelmaa vastaan ei osata varautua. Erityisen tarkkana on oltava silloin, kun talossa remontin tai muuton vuoksi liikkuu paljon vieraita ihmisiä kantamuksia mukanaan. (Järvinen 2002; s. 307.)

Tietokoneiden varkaudet yllättävän yleisiä Suomessa. Kolmasosa varkauksista tapahtuu Helsingissä, loput ympäri maata. Suomessa tehdään vuosittain kaksi tuhatta ilmoitusta rikoksista, johon liittyy yhden tai useamman tietokoneen varkaus. Noin puolet varkauksista kohdistuu kannettaviin tietokoneisiin, joista melkein joka viiden viedään autosta. (Hämäläinen 2007; s.67.)

7. KUINKA SUOJAUTUA?

Tietoturva on tietojen, tietokoneiden, tietojenkäsittelyn ja tietoliikenteen suojaamista erilaisia uhkia vastaan. Uhkia aiheuttavat esimerkiksi laiteviat, ohjelmistojen virheet ja tietovälineiden turmeltuminen, mutta myös ilkivalta ja rikollisuus. (Korpela 2005; s. 10.)

Tietoturva on myös suojautumista sellaisia ihmisiä vastaan, jotka ahneuttaan, ilkeyttään tai ymmärtämättömyyttään aiheuttavat uhkia, esimerkiksi tekevät viruksia tai yrittävät tietomurtoa. Juuri koskaan he eivät näytä roistoilta – senkään takia, että emme yleensä näe heitä. Lisäksi he saattavat esiintyä miellyttävästi ja kohteliaasti viesteissään. (Korpela 2005; s. 19.)

Yksittäisiä tietoturvallisuuteen kohdistuvia uhkia on rajattomasti ja siksi niitä kaikkia ei ole mahdollista tai edes järkevää pyrkiä selvittämään ja esittämään. Uusia uhkia syntyy koko ajan ja osa vanhoista poistuu, joten niiden seuraaminen voi olla yritykselle työläs, turhauttava ja aikaa vaativa tehtävä. Koska yksittäisten uhkien kattava esittely on käytännössä mahdotonta, on niitä syytä tarkastella suurempina kokonaisuuksina. Tämä lähtökohtana voidaan tietoturvallisuuden uhat jaotella esimerkiksi seuraavasti:

- vahingossa syntyneet ja tarkoituksella aiheutetut uhat
- passiiviset ja aktiiviset uhat
- sisäiset ja ulkoiset uhat
- ihmisen aiheuttamat ja luonnosta johtuvat uhat. (Miettinen 1999; s. 34.)

Vahingossa syntyneet uhat seuraavat yleensä ihmisen tekemää virhettä tai teknisen järjestelmän toimintahäiriöitä. Ihmisen tahallisesta toiminnasta voi syntyä

tarkoituksella aiheutettu uhka. Tämä ei tapahdu vahingossa tai sattumalta, vaan ihmisellä on jokin tietty tarkoitus teolleen. Jos uhka ei aiheuta yrityksen toiminnalle välitöntä vahinkoa, kutsutaan sitä yleensä passiiviseksi uhaksi. Sen vastakohta on aktiivinen uhka, joka aiheuttaa yleensä välitöntä vahinkoa yrityksen toiminnalle. Sisäiset uhat kohdistuvat tietoturvallisuuteen yrityksen sisältä ja niiden aiheuttaja on yleensä työntekijä tai joku muu sisäiseen toimintaan vaikuttava henkilö. Ulkoisten uhkien aiheuttaja ei yleensä kuulu yrityksen henkilökuntaan tai muuhun lähipiiriin. Ulkoisen uhkan aiheuttaja voi olla esimerkiksi yrityksen tietoverkkoon pyrkivä luvaton tunkeutuja, kilpaileva yritys tai valtiollinen tiedustelupalvelu. Ihmisen aiheuttamat uhat ovat ihmisen toimintaa mikä voi olla tarkoituksellista tai vahingossa syntynyttä. Luonnosta aiheutuvat uhat ovat yleensä vaikeasti ennakoitavissa. Tavallisia tällaisia uhkia ovat suuret luonnonmullistukset: tulvat, metsäpalot, maanjäristykset, hirmumyrskyt ja tulivuoren purkaukset.
(Miettinen 1999; s. 34 – 37.)

Ennalta estävillä suojauskeinoilla yritys pyrkii suojautumaan erilaisia riskejä vastaan ennen niiden toteutumista. Havaitsevat suojauskeinot auttavat tunnistamaan syntyviä tai jo toteutuneita uhkatilanteita, tietoturvallisuusongelmia ja väärinkäytön mahdollisuuksia. Korjaavia suojauskeinoja tarvitaan silloin, kun uhkatilanne on jo toteutunut ja siitä on aiheutunut vahinkoja. (Miettinen 1999; s. 144.)

Yleisiä tietoturvauhkia voivat olla esimerkiksi:

- Salakuuntelu tai dataliikenteen seuraaminen muiden huomaamatta.
- Oman identiteetin naamioiminen, jolloin väärinkäyttäjä hämää tilaajaa esimerkiksi uskottelemalla väärennetyn verkon kautta olevansa todelli-

nen operaattori saadakseen luottamuksellista tietoa käyttäjältä. Väärinkäyttäjä voi myös uskotella järjestelmälle olevansa luvallinen käyttäjä saadakseen järjestelmäkohtaista luottamuksellista tietoa.

- Luvaton liikenneanalyysi. Vaikka itse viestin sisältöä ei saisikaan selvitetyksi, väärinkäyttäjä voi tutkia viestiin liittyviä ominaisuuksia, kuten viestin pituutta, lähettäjän ja vastaanottajan osoitetta, lähetysaikaa ja viestien tiheyttä, saadakseen selville käyttäjän sijainnin tai tiedon siitä, minkä asian vuoksi viesti lähetettiin.
- Luvaton tietokantojen selailu, jonka avulla väärinkäyttäjä voi löytää tilaajia koskevia arkaluonteisia tietoja joko verkkoon jääneiden tietoturva-aukkojen kautta (tietovuoto), tai häiritsemällä verkon toimintaa (verkko reagoi jollakin tavalla käyttäjän lähettämään merkinantoon.) Jälkimäisessä tapauksessa käyttäjä voi esimerkiksi pyrkiä aktiivisesti alustamaan tietoliikenneyhteyttä saadakseen tietoa siihen liittyvästä verkon signaloinnista (viestien pituudesta, ajoituksista, datanopeuksista sekä lähetys- ja vastaanotto-osoitteista).
- Tietosisällön manipulointi, jolla hyökkääjä saattaa muokata, lisätä, toistaa tai poistaa viestejä.
- Häirintä ja väärinkäyttö, joilla hyökkääjä voi estää luvallisten käyttäjien liikennettä tai merkinantoa. Hyökkääjä voi myös ylikuormittaa järjestelmää ja siten estää luvallisia käyttäjiä pääsemästä järjestelmään. Edelleen hyökkääjä (väärinkäyttäjä tai toinen verkko)voi myös pyrkiä lisäämään omia oikeuksiaan päästäkseen käsiksi arkaluonteiseen tietoon. Häirintään voidaan käyttää myös erillistä erikoissovellusta.
- Hylkäys, jolla käyttäjä tai toinen verkko voivat olla välittämättä jonkun verkon toiminnosta tai käskystä.

- Luvaton pääsy palveluihin, jolla väärinkäyttäjä voi naamioitua luvalliseksi käyttäjäksi, tai väärinkäyttämällä luvallisia oikeuksiaan. (Penttinen 2006; s. 191 – 192.)

Tietoturvalla tarkoitetaan myös hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Määritelmä tarkoittaa tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamista hallinnollisin ja teknisin toimin. Näitä tietoturvatoimia ovat esimerkiksi laitteille ja järjestelmiin pääsynvalvonta, tietojen ja järjestelmien luvattoman käytön esto, käsittelytapahtumien kirjaaminen, tietoliikenteen alkuperä valvonta ja reititysvalvonta, järjestelmien käyttöoikeuksien määrittely, ylläpitotoimien asianmukainen järjestäminen ja tietojen sekä järjestelmien suojaaminen tietoturvaa vaarantavilta teoilta tai tapahtumilta, kuten viruksilta tai muilta haittaohjelmilta. Lisäksi tietoturvatoimia ovat tietoliikenteen häirinnän valvonta ja sen estäminen. (Helopuro, Perttula & Ristola 2004, s. 38.)

Palvelun ja käsittelyn tietoturvasta huolehtiminen tarkoittaa toimia toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi. (Helopuro ym. 2004, s. 39.)

Toiminnan turvallisuudella tarkoitetaan muun muassa sitä, että ylläpidetään kirjallisia ohjeita siitä, miten tietoturvavaatimukset toteutetaan, oman tietoturvan tasoa seurataan säännöllisesti, varmistetaan tietoturvavaatimusten toteutuminen käytettäessä alihankkijoita ja suojataan laitteet ja tiedostot luvatonta pääsyä ja käyttöä vastaan. Lisäksi toiminnan turvallisuudella tarkoitetaan sitä,

että pidetään rekisteriä kunkin järjestelmän osalta siitä, kenellä on järjestelmän käyttäjätunnuksia ja mitä oikeuksia milläkin käyttäjätunnuksella on ja valvotaan tietojen, asiakirjojen, viestintäverkkojen, laitteistojen, palvelujen ja tiedostojen tietoturvaan vaikuttavia tapahtumia niin, että tietoturvan kannalta merkittävät tapahtumat havaitaan. Tietoliikenneturvallisuudella tarkoitetaan muun muassa sitä, että viestintäverkkojen avulla välitettävät viestit ja tunnistamistiedot eivät paljastu asiaankuulumattomille ja asiaankuulumattomat eivät pääse muuttamaan tai tuhoamaan viestintäverkoissa välitettäviä viestejä. Lisäksi tietoliikenneturvallisuudella tarkoitetaan sitä, että viestintäverkoissa on toiminaan kannalta riittävät todentamismenettelyt, ja että asiaankuulumattomat eivät pääse tunnistamistietoihin tai käsittelyä koskeviin tietoihin. Laitteistoturvallisuudella ja ohjelmistoturvallisuudella tarkoitetaan muun muassa sitä, että käytetään sellaisia laitteistoja, tietojärjestelmiä ja ohjelmistoja, joista aiheutuva tietoturvauhka on vähäinen sekä järjestetään toiminnan kannalta tärkeiden ohjelmistojen varmuuskopiointi ja turvallinen säilytys. (Helopuro ym. 2004, s. 40.)

Tiedon varjeleminen sen koko elinkaaren ajan on kuitenkin kertaluokkaa vaikeampi tehtävä kuin vaikkapa Internetin kautta verkkoon pyrkivien haittaohjelmien torjunta. Vähäisin este eivät ole asenteet: IT ponnistelee tuodakseen tiedot mahdollisimman esteettömästi kaikille niitä tarvitseville, ja ylimääräisten suojausten pelätään alentavan käyttäjätyytyväisyyttä. Ongelmia ovat myös apuvälineiden hajanaisuus ja kokonaisvaltaisen lähestymistavan puute. Myös se että missä tieto on, missä se sijaitsee ja liikkuu. Kaikkea tietoa ei voi suojata, mutta luottamuksellinen tieto on suojattava kaikkialla. Tiedolla on myös taipumus monistua yrityksen prosesseissa ja sovelluksissa (esimerkiksi sähköpostit ja omat verkkolevyt). Mutta näin luottamuksellinen tieto voi joutua suojaamattomalle alueelle. (Hämäläinen 2007; s. 58.)

Yhtenä ulkoisena uhkana voidaan nähdä informaatiosodankäynti. Viimeaikaiset tutkimukset viittaavat siihen, että ensimmäinen todellinen informaatiosodan hyökkäys tapahtuu 20 vuoden sisällä. PCCIP (Yhdysvaltain haavoittuvaisuutta tutkiva ryhmä) on tunnistanut keskeisiä resursseja, joihin on mahdollista hyökätä Internetin kautta. Tässä on niistä muutamia:

- informaatio ja tietoliikenne
- sähköenergiajärjestelmät
- bensiinin ja öljyn kuljetus ja varastointi
- pankit ja rahalaitokset
- kuljetusvälineet
- vedenjakelujärjestelmät
- hälytyspalvelut
- valtion palvelut.

  (Anonymous 2002; s. 98 – 99.)

7.1 Käyttäjän tasolla

Palvelinten käytön edellytyksenä on useimmiten, että siihen on annettu nimenomainen oikeus. Käyttäjä tarvitsee käyttäjätunnuksen ja salasanan. Käyttäjätunnus on yhtä kuin käyttäjän verkkonimi ja salasana on salainen merkkijono, jonka ainoastaan käyttäjä tuntee. (Odom 2005; s. 356.)

Tietoa voidaan suojata soveltamalla Windowsin ryhmäkäytäntöjä, joiden käyttäminen perustuu käyttäjäryhmien perustamiseen ja hallinnoimalla niiden pääsyä eri resursseihin ja antamalla niille erilaisia käyttöoikeuksia.

Kaikkein turvallisimmassakin salaustekniikassa on merkittävä ongelma: sen käyttäjiä ovat tavalliset ihmiset. Jos järjestelmä edellyttää käyttäjän määrittelemää salasanaa, pitkästä avaimesta ja turvallisesta tekniikasta saadaan vain rajoitetusti hyötyä, sillä hyvän salasanan keksiminen on vaikeaa. Lisäksi keksimisen pitäisi olla jatkuvaa, sillä salasanoja tulisi vaihtaa säännöllisesti.

Mukavuudenhaluisella käyttäjällä on houkutus valita lyhyt, helposti muistettava salasana. Sen estämiseksi järjestelmä saattaa vaatia salasanalta tiettyä minimipituutta ja jopa pakottaa käyttämään sekaisin pieniä ja isoja kirjaimia. On myös kehitetty muistisääntöjä, jotka auttavat hyvän salasanan määrittelyssä. Yksittäisen salasanan (password) sijaan voidaan myös käyttää salalausetta (passphrase). Silloin edellä kuvattu lause kirjoitetaan salasanan paikalle kokonaisuudessaan. Kokonainen lause on periaatteessa turvallisempi kuin yksittäinen sanan, mutta sen kirjoittaminen on työlästä ja virhealtista – etenkin jos kentässä näkyy kirjoituksen aikana vaan tähtiä. (Järvinen 2003; s. 244.)

Salasana ei saisi olla mikään yksittäinen kielen sana. Käytännössä luonnollisen kielen sanat ja erilaiset nimet ovat kuitenkin suosittuja valintoja salasanoiksi. Eri kielillä on saatavissa tuhansien sanojen mittaisia listoja, joita hyökkääjä voi kokeilla. Tekniikkaa kutsutaan osuvasti sanakirjahyökkäykseksi (dictionary attack). Menetelmä edellyttää, että hyökkääjä pääsee kokeilemaan sanoja kaikessa rauhassa. Toimikortti tai verkkopalvelu, joka lukitsee itsensä kolmesta väärästä yrityksestä, on immuuni sanakirjahyökkäystä vastaan. Salatut työtiedostot tai kaapatut viestit eivät ole. (Järvinen 2003; s. 246.)

Yksi ratkaisu salasanojen ongelmaan ja käyttäjien tunnistamiseen on biometriikan käyttö. Siinä käyttäjä tunnistetaan jonkin henkilökohtaisen ominaisuuden perusteella (esimerkiksi sormenjälki, käsi, kasvot, ääni, iiris tai verkkokalvo).

Biometriikalla on monia hyviä puolia. Käyttäjän muistiparkaa ei rasiteta, koska muistettavaa yhteistä salaisuutta ei ole. Kyse ei ole liioin avaimesta tai kortista, joka voitaisiin hukata tai varastaa.
(Järvinen 2002; s. 357 – 358.)

Tietokoneiden käyttäjille voidaan antaa toisistaan poikkeavia käyttöoikeuksia. Työasemalla työskenneltäessä käyttäjälle pyritään antamaan ne oikeudet, joilla työskentely onnistuu sujuvasti. Yleisesti ottaen käyttäjälle annetaan ensin peruskäyttäjäoikeudet, sitten tarpeen mukaan annetaan mahdollisesti muita lisäoikeuksia. Lisäoikeuksia voidaan tarvita sovellusten ja laitteiden käytössä.

Jos käyttäjätunnusten ja salasanojen lähettämiseen käytetyt protokollat lähettävät ne selkokielisinä, salasanat voi saada selville nuuskimen avulla. Nuuskin on yleisesti käytössä oleva synonyymi analyysi- ja sieppaustyökalulle, joita voi ladata ilmaiseksi Internetistä ja joilla voi tehdä tavallisesta PC:stä nuuskimen. (Odom 2005; s. 365.)

7.2 Salaus

Salauksiin ja niiden purkamiseen erikoistunut tieteenala, kryptologia on saanut nimensä kreikan kielen sanoista kryptos (salainen, piilotettu) sekä logos (sana). (Järvinen 2003; s. 19.)

Salauksessa tietokone soveltaa dataan tiettyä algoritmia ja lähettää verkkoon sen tuloksen. Vastaanottava tietokone voi sitten muodostaa alkuperäisen datan uudestaan purkamalla salauksen. Salattua dataa ei voida lukea, vaan se näyttää täysin satunnaiselta bittien ja tavujen joukolta. Data voidaan saada lukukelpoi-

seksi ainoastaan purkamalla salaus, jota varten tarvitaan salausavain. Datan yksityisyys voidaan säilyttää, koska salausavainta ei anneta kenellekään ulkopuoliselle. (Odom 2005; s. 368.)

7.3 Fyysinen tunkeutuminen verkkoon

Jos yrityksessä on tiloissaan lähiverkko, eikä fyysinen tietoturva ole kunnossa, on verkko altis sille, että kuka tahansa voi kävellä yritykseen, kytkeytyä lähiverkkoon ja yrittää pääsyä verkon palvelimiin. Jos fyysisestä tietoturvasta on huolehdittu kunnolla, kenelle tahansa voidaan sallia tietokoneen liittäminen RJ-45-seinärasiaan ja lähiverkkoon. Vaikka useimmiten yrityksissä sallitaan nykyisin yritysverkossa olevan PC:n yritys muodostaa palvelinyhteys, monet lisäävät tietoturvaansa vaiheen, jossa laitteet todennetaan, ennen kuin ne voivat lähettää ensimmäistäkään pakettia palvelimelle. (Odom 2005; s.359.)

Verkoissa käytetään tunkeutumisen havaitsemisjärjestelmiä eli IDS-järjestelmiä etsimään vakoojan lailla toimivia, luvallista liikennettä jäljittteleviä tapahtumia, IDS valvoo palomuurin läpi päästämiä paketteja ja etsii niistä seikkoja, jotka voisivat osoittaa, että joku yrittää huiputtaa palomuuria, saada pakettinsa sen läpi ja aiheuttaa vahinkoa verkon palvelimille ja isännille. Jotkin IDS-järjestelmät ovat verkkoon sijoitettuja laitteita, jotka valvovat lähiverkossa liikkuvia paketteja, toiset taas palvelimilla olevia ohjelmistoja. Edellisiä kutsutaan verkkopohjaisiksi ja jälkimmäisiä isäntäpohjaisiksi IDS-järjestelmiksi. (Odom 2005; s. 385.)

Langattomat 802.11 – lähiverkot soveltuvat täydentämään yrityksen lähiverkkoa, jakamaan kodin nettiyhteyttä ja toteuttamaan Internet-yhteyden paikallisoperaattorin tilaajajohdosta riippumattomasti. Langattomuus ja liikkuvuus mahdollistavat uudentyyppisten päätelaitteiden ja sovellusten käyttöönoton, tilapäisten verkkojen toteuttamisen nopeasti ja erikoiskohteiden verkottamisen ilman kaapelia. IEEE:n 802.11 – standardien mukaiset laitteet hyödyntävät vapaasti käytettäviä taajuusalueita eivätkä tarvitse käyttölupaa. 802.11 – standardit eivät tarjoa riittävää tietoturvaa, ja ongelma korostuu radioaaltojen edetessä myös rakennuksen ja tontin ulkopuolella. Langattoman verkon suorituskyky on lähiverkkoa huonompi ja jaetun median toimintaperiaatteen vuoksi vaikeasti ennakoitavissa. (Puska 2005; s. 13.)

WLAN-verkkojen vakavia passiivisia uhkia ovat seuraavat:

- Liikenteen salakuuntelu, myös rakennuksen ulkopuolelta. Tarkoituksena kerätä tietoa, joka auttaa verkkoon tunkeutumista. WLAN-verkon passiivinen kuuntelu ja liikenteen kerääminen onnistuu suunta-antennilla pitkänkin matkan päästä. Salakuuntelua on vaikea estää ja mahdoton havaita.
- Liikenteen analysointi, jolloin verkon liikenne voi paljastaa luottamuksellista tietoa. Kerättyä tietoa voidaan analysoida myös jälkeenpäin. Salakuunteluun ja analysointiin on saatavilla monia valmiita ohjelmia, jotka myös ilmoittavat löydetyn verkon turva-asetukset, jopa salausavaimet.

Aktiivisessa tapauksessa tunkeutuja lähettää kohdeverkkoon dataan tai signaalia. Tällaisia uhkia ovat mm. seuraavat:

- Siirtomedia häirintä, joka voidaan toteuttaa vapaasti käytettävillä taajuuksilla toimivalla radiolähettimellä tai ylikuormittamalla WLAN-yhteyspisteitä tai muita laitteita turhilla liityntä- tai palvelupyynnöillä. Häirintään ja palveluestohyökkäyksiin voi varautua eristämällä verkko ulkopuolisilta häiriöiltä tai rajoittamalla palvelupyyntöjen määrää.
- Langattomassa verkossa liikkuvat datan muokkaaminen tahallisesti tai tahattomasti. Tahallinen muokkaus perustuu usein yhteysosapuolten väissä toimimiseen (man in the middle). Tahaton datan korruptoiminen havaitaan tarkistussummasta, ja kyseinen kehys hylätään virheellisenä. Sopivilla järjestelyillä suurin osa datan muokkaamisesta voidaan havaita.
- Usein lopullinen päämäärä on tietojärjestelmään tunkeutuminen ja muita keinoja käytetään tämän päämäärän takia. Koska langaton verkko syöttää liikennettä yrityksen tietoverkkoon, voi murtautuja päästä käsiksi yrityksen sisäisiin palvelimiin ja työasemiin. Palvelimet on usein vahvasti suojattuja ja ammattimaisesti hoidettuja, mutta työasemien tietoturvapäivitykset, -asetukset ja turvajärjestelyt saattavat olla huonosti hoidettuja. Murtautumisyritys kriittiseen palvelimeen havaitaan yleensä, mutta samaa ei voi sanoa työasemaan tunkeutumisesta. (Puska 2005; s. 70.)

7.4 Päivitykset

Kaikkien käyttöjärjestelmien turvallisuus perustuu nykyisin päivityksiin. Säännöllinen päivittäminen on tietoturvan ensimmäinen edellytys. Päivittäminen on tarpeen, koska laitteet tuodaan myyntiin keskeneräisinä. Kiireen vuoksi niihin jää virheitä, joita joudutaan sitten paikkailemaan jälkikäteen. Käyttöjärjestelmän lisäksi sovelluksiakin pitää päivittää säännöllisesti. Sovellukset tarvitsevat

myös turvapäivityksiä, sillä työtiedostot voivat laukaista ohjelmissa virhetoimintoja ja pahimmassa tapauksessa ladata netistä jonkin haittaohjelman. Virhetoimintoja voidaan käyttää tietoturvahyökkäyksiin jakamalla työtiedostoa, joka aiheuttaa sovelluksessa puskurin ylivuodon. Joissakin tapauksissa hyökkääjä voi saada koneen täysin hallintaansa yhden ainoan työtiedoston avulla. (Järvinen 2006; s. 15 – 17.)

7.5 Viruksentorjuntaohjelmistot

Viruksia vastaan voidaan taistella asentamalla käyttäjien koneisiin ja palvelimiin virustorjuntaohjelmistot. Ne tutkivat tietokoneen tiedostot ja vertaavat niitä tunnettujen virusten luetteloon. Sähköpostit sisältävät usein liitetiedostoja. Virusohjelmisto tutkii tiedostot ja vertaa niiden sisältöä tunnettujen virusten luetteloon. Jos tiedosto sisältää viruksen, ohjelmisto joko tuhoaa sen tai siirtää sen eristyksiin. (Odom 2005; s. 387.)

Ensimmäinen virustorjuntaohjelmisto valmistettiin Indonesiassa vuonna 1988. Kaksi vuotta myöhemmin Symantec julkaisi ohjelman nimeltä Norton AntiVirus. (Lilley 2002; s. 14.)

Symantecin tekemän tutkimuksen mukaan yli 92 prosenttia kotikoneista on suojattu tietoturvaohjelmistolla. Se on hyvää kehitystä, sillä kaikista tietoturvahyökkäyksistä peräti 86 prosenttia yrittää iskeä kotikäyttäjän koneisiin. Mutta huolestuttavan suuri osa, peräti 40 prosenttia suomalaisista, ei kuitenkaan varmuuskopioi tiedostojaan lainkaan. (Jalovaara 2006; s. 11.)

7.6 Palomuuri

Palomuuri (Firewall) konfiguroidaan säännöin, jotka kertovat, mikä verkossa on sallittua ja mikä ei. Sääntöjen mukaan palomuuri sallii tiettyjen pakettien kulkevan lävitseen ja hylkää toiset. (Odom 2005; s. 378.)

Korpela määrittelee palomuurin seuraavasti: ohjelma tai laite, joka valvoo ja rajoittaa tietokoneen ja muun maailman välistä verkkoliikennettä. Erityisesti sillä pyritään estämään, että joku voi näkymättömästi käyttää konettasi verkon kautta. Se saattaa myös estää koneeseen päässeitä viruksia ottamasta yhteyttä ulospäin. (Korpela 2005; s. 86.)

Palomuuri ei enää riitä suojaamaan yritystä, koska palomuurin ohi on muita reittejä. Oma henkilökunta ja vieraat tuovat yritykseen kannettavia tietokoneita, jotka liitetään yrityksen sisäverkkoon. Silloin koneissa mahdollisesti olevat haittaohjelmat pääsevät leviämään suoraan lähiverkkoon. Yrityksen tiloissa olevat WLAN-tukiasemat saattavat päästää liikennettä sekä ulos ja sisään palomuurin ohi. Pahin epäkohta on portti 80, jonka pitää olla auki surffausta varten. Siksi monet muutkin ohjelmat ovat alkaneet käyttää sitä. Esimerkiksi vakoiluohjelmat välittävät havaintonsa isännälleen yleensä juuri 80-portin kautta, koska silloin niiden aiheuttama liikenne ei erotu muusta surffauksesta. (Järvinen 2006; s. 105.)

Palomuuri on jopa tärkeämpi kuin virustentorjuntaohjelma, sillä palomuuri suojaa uhkilta, joihin käyttäjä ei voi omilla toimillaan vaikuttaa. Virustorjunnassa käyttäjän omalla varovaisuudella on keskeinen rooli. Kun ei avaa tiedostoliitteitä ja pitää selaimen, käyttöjärjestelmän ja sähköpostiohjelman ajantasalle päi-

vitettynä, välttyy kaikilta viruksilta. Palomuuri suojelee niin sisäverkkoa kuin yksittäistä kotikäyttäjän työasemaa hyökkäyksiltä. Suoja liittyy lähinnä turva-aukkoihin, joita ei ole päivitetty tai vielä edes löydetty. Mikäli ohjelmat toimisivat oikein, palomuurisuojausta ei tarvittaisi – ohjelmat ottaisivat vastaan vain sen liikenteen, mikä pitääkin. (Järvinen 2006; s. 107.)

Palomuurin toimintaa on mahdollista yrittää horjuttaa monin tavoin. Yksi tapa on lähettää tietokoneeseen todellisia tai valepaketteja niin runsaasti, että liian kevyesti suojattu palomuuri saturoituu liikenteestä. Tämän jälkeen ohjelmistoon ja käyttöjärjestelmään voidaan pyrkiä hyökkäämään. Toinen tapa on lähettää liian isoja paketteja, jolloin saatetaan päästä FW:n käyttöjärjestelmään ja voidaan siten tehdä virtual server – määrityksiä. Palomuuri on hyökkääjälle ensisijainen kohde, koska sen horjuttaminen helpottaa järjestelmään pääsemistä. (Penttinen 2006; s. 188 – 189.)

7.7 Maalaisjärki

Kaikista ratkaisevin keino suojautumiseen tietotekniikkarikollisuuteen löytyy näytön ja tuolin välistä. Käyttäjä voi omilla toimillaan vaikuttaa asioihin. Tuntemattomilta lähettäjiltä tulleet sähköpostiliitteet voi jättää avaamatta tai muistaa olla jättämättä matkatietokonetta auton takapenkille kauppareissun ajaksi.

Henkilöllisyysvarkauden riskiä voi minimoida seuraavasti:

- älä ilmoita henkilötietojasi turhaan äläkä kirjoita niitä julkisille www-sivuille tai keskustelualueille.
- henkilötunnus (hetu, entinen sosiaalitunnus) ei ole valtionsalaisuus,

mutta sen kysymiseen tulee olla hyvät perustelut. Elleivät perustelut vakuuta, älä ilmoita tunnusta.

- tarkkaile postiasi (sitä perinteistä!): jos laskut tai tiliotteet lakkaavat, ota yhteyttä pankkiisi.
- älä säilytä pankkikortin tunnusnumeroa lompakossa.
- älä säilytä lompakossa tarpeettomia luottokortteja.

(Järvinen 2002; s. 189 – 190.)

Teoriassa khalastelu-huijaukset on helppo torjua: riittää, kun ei koskaan luovuta salasanoja, pin-koodeja tai käyttäjätunnuksia tuntemattomille tahoille. Huijarit eivät kysy tunnuksia suoraan, vaan lähettävät käyttäjälle viestin, jossa pyydetään kirjautumaan palveluun ja päivittämään omia yhteystietojaan. Viesti voi myös varoittaa, että käyttäjän tunnuksella on tehty vääriä tilauksia. Olipa houkuttelukeino mikä tahansa, osa vastaanottajista menee lankaan ja kirjautuu palveluun, jolloin he tulevat huomaamattaan antaneeksi tunnuksensa. (Järvinen 2006; s. 283 – 284.)

Suomalainen käyttäjä voi tuhota empimättä valtaosan khalastelu-viesteistä, sillä ne on usein lähetetty suurten kansainvälisten pankkien nimissä. Lisäksi paras suoja huijauksia vastaan on suomi itse. Suomen kieli on vaikeaa, eikä sitä juurikaan osata maamme rajojen ulkopuolella. Koneellinen kielenkäännös tuottaa niin huonoa suomea, että ainakin syntyperäiselle suomalaiselle huijaus paljastuu heti. Toisaalta se, että viestissä onkin virheetöntä ja hyvää suomea, lisää viestin uskottavuutta ja aitouden vaikutelmaa. (Järvinen 2006; s. 286 – 287.)

8. TIETOKONERIKOLLISUUTTA KOSKEVAT KESKEISET LAIT

Koska tietokonerikollisuus on varsin uusi rikollisuuden ala ja se on luonteeltaan kansainvälinen mm. verkoissa tapahtuvat rötöstelyn vuoksi, se asettaa vaatimuksia laille, sillä niissä on eroja eri maiden välillä. Tämä on haaste mm. silloin kun on kyseessä sellaisesta rikoksesta, joka on tapahtunut monessa maassa ja myös tekijöitä saattaa olla mukana eri puolilta maailmaa. Yhteistyötä viranomaisten välillä löytyy mutta mm. Kiina ja Venäjä eivät tunnista tietokonerikollisuutta, jollei se vaikuta negatiivisesti kansallisiin intresseihin. Teollisuusmaat tekevät kansainvälistä yhteistyötä, mutta kehitysmaat eivät ole näihin osallistuneet. (Kshetri 2006; s. 33 – 35.)

Tietosuoja on vakiintunut nimitys henkilötietojen suojalle. Se siis tarkoittaa nimenomaan yksityistä ihmistä koskevia tietoja, kuten vaikkapa ihmisen nimeä, puhelinnumeroa, perhesuhteita, mieliruokaa, tulojen määrää ja terveystietoja. Osa henkilötiedoista on hyvin arkaluonteisia, osa taas on sellaisia, joita joudumme kertomaan hyvin usein. (Korpela 2005; s. 173.)

Yksi keskeinen laki käsittelee tekijänoikeutta. Sitä käsiteltiin aiemmin pintapuolisesti piratismia koskevassa luvussa. Seuraavassa muita keskeisiä lakeja, jotka sivuavat tavalla tai toisella tietokonerikollisuutta.

8.1 Viestintäsalaisuus

Kansalaisen oikeus yksityiseen viestintään on turvattu perustuslailla. Yksityiselämän suojaa käsittelevä perustuslain 10. pykälä sanoo ykskantaan ”Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.”

Aiemmin käytössä ollut kirjesalaisuus on tekniikan kehittyessä muutettu yleiseksi viestintäsalaisuudeksi, joka ei tee eroa viestinnän toteutustapojen välillä. Lähettäjän tarkoitus ratkaisee. Jos viesti on tarkoitettu yksityiseksi, se saa automaattisesti lain tarkoittaman suojan. Viestintäsalaisuus turvaa niin puheluiden, sähköpostin, tekstiviestien kuin muidenkin vastaavien luottamuksellisuuden. (Järvinen 2003; s. 250.)

Tieto- ja viestintärikoksia käsittelevä rikoslain 38 luku määrittelee viestintäsalaisuuden loukkauksen seuraavasti:

Joka oikeudettomasti

1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin vaikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka
2) hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta, on tuomittava viestintäsalaisuuden loukkauksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Yritys on rangaistava. (Järvinen 2003; s. 250.)

Viestintäsalaisuuden loukkauksesta voi saada sakkoja tai enintään vuoden vankeutta. Jos teko kohdistuu erityisen luottamukselliseen viestintään, se tehdään teknistä apuvälinettä tai ohjelmaa käyttäen, tai jos hyödynnetään luottamusasemaa, teko saattaa täyttää törkeän viestintäsalaisuuden loukkauksen tunnusmerkistöön ja silloin rangaistusmaksimi on kolme vuotta vankeutta. Kuten rikoslaki sanoo, jo yrityskin on rangaistava. (Järvinen 2003; s. 252.)

Laki turvaa viestintäsalaisuuden myös kotioloissa. Lain mukaan puoliso ei saa lukea toisen sähköposteja, tekstiviestejä tai puhelimen soittotietoja. Käytännössä näin tapahtuu jatkuvasti. Puhelin on houkuttelevasti tyrkyllä, eikä sitä lukita kotioloissa. Pahaa-aavistamattoman puolison nukkuessa on helppo selvittää ja tutkia puhelut, osoitekirja ja tekstiviestit. (Järvinen 2003; s. 253 – 254.)

8.2 Tietoliikenteen häirintä

Tietoverkon, tiedonsiirron tai sähköpostin toiminnan tarkoituksellinen häirintä tai ylikuormitus on kiellettyä. Tästä säädetään rikoslaissa, se 38. luvussa, jossa sanotaan:

5§ Tietoliikenteen häirintä
Joka puuttumalla postiliikenteessä taikka tele- tai radioviestinnässä käytettävän laitteen toimintaan, lähettämällä ilkivaltaisessa tarkoituksessa radiolaitteella tai televerkossa häiritseviä viestejä tai muulla vastaavalla tavalla oikeudettomasti estää tai häiritsee postiliikennettä taikka tele- ja radioviestintää, on tuomittava tietoliikenteen häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi. (Mäkinen 2006; s. 120.)

Esimerkiksi spammaus eli roskapostin lähettäminenkin on tietoliikenteen häirintää. Samaa voidaan sanoa keskustelupalstan häiriköinnistä. (Mäkinen 2006; s. 121.)

8.3 Tietomurto

Vieraaseen tietojärjestelmään tunkeutuminen tai järjestelmän luvaton käyttö - jopa pelkkä sen yrityskin - on rikos, josta voi seurata vankeutta. (Mäkinen 2006; s. 121.)

Myös toisen käyttäjän tunnusten ja salasanojen arvailu ja kokeileminen on kiellettyä. Hakkerointia kutsutaan rikoslaissa tietomurroksi. Rikoslaki sanoo 38. luvussa tietomurrosta seuraavaa:

8§ Tietomurto

Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1. momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta.

(Mäkinen 2006; s. 122.)

8.4 Vaaran aiheuttaminen tietojenkäsittelylle

Haitallisten virusten kirjoittaminen ja niiden tarkoituksellinen levittäminen on kiellettyä. Rikoslain 34. luvun osastoon, jossa luetellaan "yleisvaarallisia rikoksia" kuten tulipalojen, räjäytysten ja tulvien aiheuttaminen. Tietokonevirusten levittämisestä on määräykset luvun 9. pykälässä.

9 a § Vaaran aiheuttaminen tietojenkäsittelylle

Joka, aiheuttaakseen haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle.

1) valmistaa tai asettaa saataville sellaisen tietokoneohjelman tai ohjelmakäskyjen sarjan, joka on suunniteltu vaarantamaan tietojenkäsittelyä tai tieto- tai telejärjestelmän toimintaa taikka vahingoittamaan sellaisen järjestelmän sisältämiä tietoja tai ohjelmistoja, tai levittää sellaista tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka 2) asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseen tai levittää sellaista ohjetta, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, vaaran aiheuttamisesta tietojenkäsittelylle sakkoon tai vankeuteen enintään kahdeksi vuodeksi. (Mäkinen 2006; s. 124.)

8.5 Lapsiporno

Lapsipornon levittäminen ja hallussapito on kielletty riippumatta siitä, missä muodossa aineisto on. Rikoslain 17. luvun 18. pykälässä puhutaan "törkeä sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan levittämisestä". Kyse on kaikista kuvista ja kuvatallenteista, joissa sukupuolisiveellisyyttä loukkaavasti esitetään lasta tai väkivaltaa tai eläimeen sekaantumista. Raskauttavaa on myös se, jos rikos "tehdään erityisen suunnitelmallisesti".

Rikoslain seuraavassa pykälässä (RL 17: 19) säädetään lapsipornon hallussapidosta. Sillä pyritään suojaamaan lapsia, jotta he eivät joutuisi seksuaalisen hyväksikäytön kohteiksi. Siksi lapsia esittävien sukupuolisiveellisyyttä loukkaavien kuvien "oikeudeton" hallussapito on kielletty. Tutkijalla ja esim. journalistilla

on tietenkin oikeus pitää epäsiveellistä materiaalia - mutta vain tutkimustarkoituksessa. Lapsiporno ja pedofilia ja etenkin niihin liittyvien materiaalien levitys on helpottunut ja tehostunut Internetin myötä. (Mäkinen 2006; s. 129.)

Verkon reaaliaikaiset keskustelualueet ovat nuorten suosiossa, onhan se vaivaton ja halpa tapa pitää yhteyttä kavereihin sekä tutustua uusiin ihmisiin. Koskaan ei voi silti tietää varmasti, onko keskustelija juuri se, joka väittää olevansa. 14-vuotiaana tyttönä esiintyvä henkilö saattaa olla todellisuudessa 50-vuotias mies. Tekstillä on helppo hämätä, eikä mahdollinen valokuvakaan aina esitä oikeaa henkilöä.
Siksi on tärkeää varoittaa lapsia keskustelualueiden vaaroista ja varmistaa, että nämä eivät lähde omin päin tapaamaan verkossa tutustumiinsa ihmisiin.
(Järvinen 2002; s. 181 – 182.)

9. YHTEENVETO

Tietotekniikan ulottuessa entistä enemmän eri osa-alueille niin yksityisen käyttäjän elämässä kuin yritysmaailmassakin, on varmaa, ettei tietotekniikkarikollisuus tule vähenemään. Tämä rikollisuuden ala tulee löytämään uusia tekniikoita sekä tapoja. Lisäksi on huomattava, kuinka paljon yhteiskunnan kriittisiä toimintoja on tietokoneiden ja verkkojen varassa. Niiden turvaaminen nyt ja tulevaisuudessa on todellinen haaste sekä elinehto. Jokainen on potentiaalinen kohde, joten uhka on myös entistä enemmän henkilökohtainen jokaisen käyttäjän kohdalla.

F-Securen tutkimusjohtajan, Mikko Hyppösen mukaan rahaliikenteeseen, luottokorttiliikenteeseen ja verkkopankkiliikenteeseen liittyvät huijaukset tulevat olemaan ykkösongelma lähitulevaisuudessa. Syitä tähän on muun muassa raha, sillä puhutaan sadoista miljoonista euroista vuodessa. Lisäksi kiinnijääneitä tapauksia on vähän, kyseessä on lähes täydellinen rikos. Harvoin rikoksista tehdään rikosilmoitusta ja vaikka tehdään, niin yleensä poliisi ei tutki kunnolla. Ja vaikka tutkii, eivät löydä syyllisiä tai jos löytävät, he eivät joudu syytteeseen. Tai sitten löytyy joku välikäsi tai mennään niin monen maan kautta, ettei löydy enää viranomaisia tai lainsäädäntöä. (Kotilainen 2007; s.49.)

Esimerkiksi virukset tulevat leviämään muihinkin viestimiin kuin vain sähköpostiin. Vuonna 2004 tulivat ilmi ensimmäiset matkapuhelimiin tarttuvat virukset. Kyseessä oli bluetooth-yhteyden kautta siirtyvä koodi, joka vielä tuolloin oli varsin harmiton otus. Mutta matkapuhelimet saattavat sisältää tärkeätä tietoa, sillä nykyisillä puhelimilla on mahdollista tehdä paljon samankaltaisia toimintoja kuin tietokoneella.

Biometrinen tunnistus saattaa olla yksi tulevaisuuden ratkaisu käyttäjien autentikointiin. Mutta tällä hetkellä tekniikka on vielä lapsenkengissään, sillä se ei ole vielä tarpeeksi tarkka ja luotettava menetelmä. Yllättävää kyllä, jo noin 375 hengen joukossa tahattoman parin syntymisen todennäköisyys on yli 50 prosenttia. Kuinka tällainen konflikti-tilanne järjestelmässä voi erottaa kaksi käyttäjää toisistaan? Mutta biometrinen tunnistus saattaa olla ratkaisuna identiteettivarkauksiin, sillä esimerkiksi luottokortti ei toimisi enää perinteisellä PIN-koodilla vaan vaikkapa käyttäjänsä sormenjäljellä.

Lainsäädännöllä on haasteena pysyä koko ajan muuntautuvan tietokonerikollisuuden perässä. Lisäksi viranomaisten yhtenäistettävä rintamaansa maiden maantieteellisistä rajoista huolimatta. Jatkuvasti uusiutuva It-ala haastaa myös jatkuvaan osaamisen kehittämiseen sekä uusien menetelmien ja tekniikoiden luomista.

LÄHDELUETTELO

Ahonen, Paavo (2006). Hunajapurkit pyydystävät haittaohjelmia. MicroPc-lehti. 8/2006. s. 10.

Anonymous (2002). *Hakkerin käsikirja*. Sams Publishing, IT Press, Edita Publishing Oy, Helsinki. 920 s. ISBN 951-826-224-1

Chen, Thomas M. & Chris Davis (2006). Digital Crime and Forencsic Science in Cyberspace. [online] Hersey, PA, USA. Idea Group Publishing. s. 1- 23. Saatavana World Wide Webistä (28.3.2008): <URL:http://site.ebrary.com/lib/tritonia/Doc?id=1012456&ppg=8 >.

Cronan, Timothy Paul, Bryan C. Foltz & Thomas W. Jones (2006). Piracy, Computer Crime, And Is Misuse at the University. Communications of the ACM. June 2006/Vol. 49, No. 6. s. 85 – 90.

Geer, David (2006). Hackers Get to the Root of the Problem. [online] The IEEE Computer Society. s. 17 – 19. May 2006. Saatavana World Wide Webistä (28.3.2008): <URL: http://www.computer.org/security/>.

Helopuro, Sanna, Juha Perttula & Juhapekka Ristola (2004). *Sähköisen viestinnän tietosuoja*. 1. painos. Jyväskylä: Telentum Media Oy. 320 s. ISBN 952-14-0755-7.

Hoanca, Bodgan (2006). How Good Are Our Weapons in the Spam Wars? [online] The IEEE Computer Society. s. 22 – 30. Spring 2006. Saatavana World Wide Webistä (28.3.2008): <URL: http://www.computer.org/>.

Hämäläinen, Pertti (2007). Palomuuri ei tuki tietovuotoa. Tietokone-lehti. 5/2007. s. 57 - 58.

Hämäläinen, Pertti (2007). 5 pahinta uhkaa. Tietokone-lehti. 10/2007. s. 62 – 69.

Jalovaara, Veli-Matti (2006). Verkkorikollisuus vaatii uusia vastakeinoja. MicroPc-lehti. 14/2006. s. 11.

Järvinen, Petteri (2002). *Tietoturva & yksityisyys*. 1. painos. Jyväskylä: Docendo Finland Oy. 452 s. ISBN 951-846-152-X

Järvinen, Petteri (2003). *Salausmenetelmät.* 1. painos. Jyväskylä: Docendo Finland Oy. 385 s. ISBN 951-846-183-X

Järvinen Petteri (2006). *Paranna tietoturvaasi.* Docendo Finland Oy, Jyväskylä. 352 s. ISBN 951-846-289-5.

Karkimo, Ari (2006). Symantec valvoo asiakkaiden puolesta. Tietokone-lehti. 1/2006. s. 16 – 17.

Karkimo, Ari (2007). Nettimafian lonkeroita Ruotsissakin. Tietokone-lehti. 5/2007. s. 13.

Kerttula, Esa (1998). *Tietoverkkojen tietoturva.* 1. painos. Oy Edita Ab, Liikenneministeriö, Helsinki. 510 s. ISBN 951-37-2672-x

Komonen, Olli-Pekka (2006). Piratismi ei kuole. Tietokone-lehti. 6&7/2006. s. 38 – 40.

Korpela, Jukka K. (2005). Turvallisesti netissä – Kodin tietoturvaopas. 1. painos. Jyväskylä. Docendo Finland Oy. 208 s. ISBN 951-846-248-8.

Kotilainen, Samuli (2007). Tietoturvan haasteet kasvavat edelleen. Tietokone-lehti. 4/2007. s. 47 – 49.

Kshetri, Nir (2006). The Simple Economics of Cybercrimes. [online]. The IEEE Computer Society. s. 33 – 39. January/February 2006. Saatavana World Wide Webistä (28.2.2008): <URL: http://www.computer.org/security/>.

Laurio, Juha-Matti (2007). Täsmähyökkääjä iskee ovelasti. MicroPc-lehti. 9/2007. s. 30 – 33.

Lilley, Peter (2002). Hacked, Attacked and Abused: Digital Crime Exposed. [online]. Milford, CT, USA. Kogan Page, Limited. Saatavana World Wide Webistä (28.3.2008):
<URL: http://site.ebrary.com/lib/tritonia/Doc?id=10023728&ppg=30 >.

Miettinen, Juha E. (1999). *Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan.* Kauppakaari Oyj. Gummerus Kirjapaino Oy, Jyväskylä. 318 s. ISBN 952-14-0229-6.

Mäkinen, Olli (2006). *Internet ja etiikka.* BJT Kirjastopalvelu Oy, Helsinki Gummerus Kirjapaino Oy, Vaajakoski. 1. painos. 251 s. ISBN 951-692-621-5

Odom Wendell (2005). *Tietoverkot – perusteet.* Edita Prima Oy, Helsinki. s. 507. ISBN 951-826-788-X.

Penttinen, Jyrki (2006). *Tietoliikennetekniikka – 3 G ja erityisverkot*. 1. painos. Helsinki: Werner Söderström Osakeyhtiö. 246 s. ISBN 951-0-31255-X.

Puska, Matti (2005). *Langattomat lähiverkot*. Jyväskylä: Gummerus Kirjapaino Oy. 294 s. ISBN 952-14-0934-7.

Salmi, Laura (2006). Kuluttajan opas – Luotettavat ja turvalliset sähköiset palvelut. Luoti-julkaisuja 7/2006, Liikenne- ja viestintäministeriö sekä Kuluttajavirasto. Ollut saatavana World Wide Webistä (31.5.2007): <URL:http://www.luoti.fi>.

Sweeney, Latanya (2006). Protecting Job Seekers from Identity Theft. The IEEE Computer Society. [online] s. 74 – 78. March/April 2006. Saatavana World Wide Webistä (28.3.2008): <URL: Http://www.computer.org/internet/>.

Mikrobitti (2006). *Tietoturvaa vuonna 2006*. Mikrobitti. 1/2006. S. 9.

Virta, Toni (2006). Vieraskirja vetää nettihuijareita. MikroPc-lehti. 5/2006. s. 15.