

KARELIA-AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

Jukka Suhonen

TIETOISKU PC:N TIETOTURVASTA

Opinnäytetyö
Huhtikuu 2014



OPINNÄYTETYÖ
Huhtikuu 2014
Tietotekniikan koulutusohjelma

Karjalankatu 3
FI 80200 JOENSUU
+358 50 260 6800

Tekijä
Jukka Suhonen

Nimeke
Tietoisuus PC:n tietoturvasta

Toimeksiantaja
Salainen

Tiivistelmä

Opinnäytetyön tutkimuksen kohteena olivat tietokoneiden tietoturva ja yrityksen tiedon suojaaminen. Tietoturva valittiin opinnäytetyön aiheeksi, koska hyvin suunniteltu tietoturva tulee olemaan tulevaisuudessa merkittävä turvallisuustekijä kotona, yrityksissä sekä maailmalla. Tämän pohjalta tietoturva oli ajankohtainen ja tulevaisuuden kannalta perusteltu opinnäytetyön aihevalinta.

Opinnäytetyössä evaluoitiin yleisimpiä tietokoneisiin kohdistuvia tietoturvauhkia ja esiteltiin suojaustoimenpiteitä näitä uhkia vastaan. Tietokoneiden suojaaminen ja tietoturvan toteuttaminen jaettiin teknisiin ratkaisuihin ja käyttäjän rooliin, jota tutkittiin tarkemmin toimeksiantajalle suunnatun kyselyn avulla. Myös pilvipalveluiden tietoturvaan tutustuttiin. Pilvipalveluita käsittelevässä osiossa keskityttiin selvittämään, miten palvelut tulisi toteuttaa, jotta yrityksen tiedot olisivat turvassa.

Opinnäytetyön osana suoritettiin toimeksiantajayritykselle tietoturvakysely, jonka tavoitteena oli tutkia henkilöstön toimintamalleja tietoturvaa uhkaavissa tilanteissa. Kysymyksissä tutkittiin esimerkiksi reagoitua sellaisiin sähköpostiviesteihin, jotka ovat uhka tietoturvalle. Kyselyn tuloksia analysoimalla voitiin havaita henkilöstön tietoturvalle riskialttiit toimintamallit. Henkilöstön toimintamallien kartoittamista perusteltiin sillä, että tietokoneiden käyttäjät muodostavat itsestään vakavimman tietoturvauhan.

Tuloksena opinnäytetyöstä saatiin toimeksiantaja yritykselle materiaali, jonka avulla yritys voi arvioida yrityksen tietokoneiden tietoturvan tasoa ja saada uutta näkökulmaa tietoturvaan. Tietoturvakyselyn tulokset tarjosivat konkreettista tietoa yrityksen henkilöstön toimintamalleista ja tietoturvan tuntemuksesta. Suurimmaksi uhaksi yritykselle kyselyn perusteella osoittautuivat sähköpostin välityksellä aloitettavat hyökkäykset tietoturvaa vastaan.

Kieli
Suomi

Sivuja 68
Liitteet 2
Liitesivumäärä 10

Asiasanat
tietoturva, yritysturvallisuus, pääsynvalvonta, haittaohjelma



THESIS
April 2014
Degree Programme in
Information Technology
Karjalankatu 3
FI 80200 JOENSUU
FINLAND
Tel. 358-13-260 6800

Author
Jukka Suhonen

Title
Fact sheet of the PC's IT-security

Commissioned by
Secret

Abstract

The focus of this thesis was the information security of the computers and securing the data of organizations. Well-designed cyber security will be a remarkable safety issue in the future at homes, organizations and global environments. Due to this, IT-security was a very topical and justified subject for the thesis.

In this thesis the most common types of computer threats were evaluated and the protection solutions presented to prevent these threats. The protection of the computers was divided into two factors which were the technical factors and the role of the user. The role of the user was investigated more specifically by performing a security inquiry. There is also a part for cloud services in the thesis which gives insight to the security solutions of cloud services.

As a part of the thesis there was the security inquiry for the company which commissioned this thesis. The objective of the inquiry was to investigate the behavior of the company's personnel in the situations where the IT-security is under possible threat. A part of the questions handled for example e-mail messages, which are one possibility to carry out an attack. The results of the inquiry were analyzed to find out if there was some behavior among the personnel that could be a threat for the company's IT-security.

The final result was the thesis which provides IT-security solutions for the company's computers and hopefully gives a new view towards IT-security issues. The inquiry results gave valuable information about the personnel's knowledge about IT-security threats and behavior against them. According to the results of the inquiry, the most notable threat for the company were the e-mail based attacks.

Language
Finnish

Pages 68
Appendices 2
Pages of Appendices 10

Keywords
information security, company safety, access control, malware

Sisältö

Käsitteet.....	6
1 Johdanto.....	11
2 Tietoturva.....	12
2.1 Tiedon määritelmä	12
2.2 Tiedon turvaluokitukset	13
2.3 Henkilöstön rooli	13
2.4 Tietoturva ja tietosuoja	14
2.5 Tietoturvan tavoitteet	15
3 Työasemien tietoturvat.....	18
3.1 Tietoturva.....	18
3.2 Haavoittuvuudet.....	19
3.3 Tietoturvaloukkaus	20
3.4 Haittaohjelmat	20
3.4.1 Haittaohjelmien tartuntamekanismit	20
3.4.2 Haittaohjelmien luokittelu	23
3.5 Phishing ja pharming	27
3.6 Man In The Middle- ja Browser-hyökkäykset	29
4 Työasemien tietoturvat.....	30
4.1 Fyysinen turvallisuus	30
4.2 Kiintolevyn ja tiedostojen salaaminen	32
4.3 Varmuuskopiointi	33
4.4 Virustorjuntaohjelma	33
4.5 Palomuri	34
4.5.1 Palomuriohjelma	37
4.5.2 Laitepalomuri	38
4.6 Päivitykset	39
4.7 Salasanat.....	40
4.7.1 Salasanojen suojaaminen verkkopalveluissa	41
4.7.2 Vahvan salasanan laatiminen	43
4.8 Käyttäjäoikeuksien rajoittaminen	45
4.9 Salausmenetelmät	46
4.10 Tiedonsiirron turvallisuuden varmistaminen	48
4.11 Internet-selaimen lisäosat.....	50
4.12 Sähköpostin turvallisuus	51
4.13 Langattomien verkkojen turvallinen käyttö	53

5	Pilvipalvelut	54
5.1	Pilvipalvelun määritelmä	54
5.2	Pilvipalveluntarjoajan toimenpiteet tietoturvan varmistamiseksi	54
5.3	Pilvipalveluiden turvallisuus yrityskäyttäjän näkökulmasta	56
6	Käyttäjän rooli.....	57
6.1	Yrityksen tietoturvakysely	57
6.2	Kyselyn tavoitteet	60
6.3	Kyselyn tulosten analysointi	60
7	Yhteenveto	61
	Lähteet.....	64

Liitteet

Liite 1 Tietoturva kysymykset

Liite 2 Tietoturva kyselyn oikeat vastaukset

Käsitteet

ADSL	Asymmetric Digital Subscriber Line on laajakaistaliittymän tyyppi, joka tarjoaa nopean tiedonsiirron palveluntarjoajalta asiakkaalle. ADSL:n vastaanottonopeus on nopeampi, kuin lähetysnopeus.
AES	Advanced Encryption Standard on symmetrisessä salauksessa tiedon salaamiseen käytettävä algoritmi.
APT	Advanced Persistent Threat eli kohdistettu hyökkäys on tapahtumaketju, jonka tavoitteena on hyökätä ja murtautua kohteeksi valitun organisaation tietojärjestelmiin.
Blowfish	Symmetrisessä salausjärjestelmässä käytettävä vahva salausalgoritmi.
DH	Diffie-Hellman on epäsymmetrisessä salausjärjestelmässä käytettävä algoritmi.
DMZ	Demilitarized Zone eli demilitarisoitu alue on palomuurien väliin sijoitettu vyöhyke. Vyöhykkeelle sijoitetaan julkiseen verkkoon tarjottavat yrityksen palvelut, kuten sähköpostipalvelimet tai www-palvelimet.
DNS	Domain Name System eli nimipalvelujärjestelmä, joka muuntaa verkkotunnukset IP-osoitteiksi, sekä huolehtii sähköpostin reitityksestä oikeisiin osoitteisiin.
DoS	Denial of Service eli palvelunestohyökkäys, jonka tarkoituksena on estää verkkosivuston käytettävyys kohdistamalla sivustolle suuria määriä tietoliikennettä.
DOS	Disk Operating System, levykäyttöjärjestelmä.
DSA	Digital Signature Algorithm eli digitaalinen allekirjoitusalgoritmi.

HTTP	Hypertext Transfer Protocol eli hypertekstin siirtoprotokolla on selaimen ja www-palvelimen tiedonsiirrossa käytettävä protokolla.
HTTPS	Hypertext Transfer Protocol Secure on suojattuun tiedonsiirtoon käytettävä protokolla. HTTPS käyttää TLS/SSL-protokollaa tiedon salaamiseen.
IDS	Intrusion Detection System eli tunkeilijan havaitsemisjärjestelmä on ohjelmoitu järjestelmä, jonka tehtävänä on tunnistaa organisaation verkkoon kohdistetut hyökkäykset.
IDPS	Intrusion Detection and Prevention System on tunkeilijan havaitsemis- ja estojärjestelmä, jonka tehtävänä on tunnistaa ja estää organisaation verkkoon kohdistunut hyökkäys.
Intranet	Lähiverkkoratkaisu jonka käyttöoikeus on rajoitettu tietyn ryhmän käyttöön. Organisaatioissa Intranet toimii esimerkiksi henkilöstön sisäisenä viestintäkanavana, jonka sisältöön vain yrityksen henkilöstöllä on oikeudet.
IMAP	Internet Message Access Protocol on protokolla, jota käytetään sähköpostiviestien hakemiseen sähköpostipalvelimelta. IMAP-protokolla säilyttää viestit sähköpostipalvelimella, joten sähköpostiviestit voidaan lukea usealla eri koneella.
IP-osoite	Numeerinen osoite, jonka tehtävänä on yksilöidä verkkoon kytketyt laitteet, kuten palvelimet, tietokoneet, verkkolaitteet ja tulostimet. IP-osoitteen avulla tietokone lähettää IP-paketit halutulle laitteelle.
IP-paketti	Internetissä liikennöivä tieto pakataan IP-paketteihin. IP-paketti sisältää esimerkiksi lähde- ja kohdeosoitteen, sekä osapuolten välillä siirrettävän datan.
MITM	Man In The Middle on kyberhyökkäys, jossa kahden osapuolen tiedonsiirron välittäjäksi asettuu tietoon oikeuttamaton ulkopuolinen henkilö.

NAT	Network Address Translation eli osoitteenmuunnos, jonka tehtävänä on muuttaa sisäverkon yksityiset IP-osoitteet ulkoverkkoon reititettäviksi julkiseksi IP-osoitteiksi. Osoitteenmuunnoksen avulla voidaan säästää rajallisesti saatavilla olevia julkisia IP-osoitteita, sekä lisätä organisaation sisäverkon tietoturvallisuutta.
PAT	Port Address Translation eli porttimuunnos on osoitteenmuunnostekniikka, jonka avulla yhden julkisen IP-osoitteen kautta voi liikennöidä ulkoverkkoon useita sisäverkon tietokoneita. Porttimuunnoksessa sisäverkon tietokoneiden yhteydet yksilöidään porttinumerolla, jonka avulla data ohjataan oikealle laitteelle.
PBKDF2	Password-Based Key Derivation Function 2 on salasanojen tiivistämiseen suunniteltu algoritmi. Algoritmia käyttämällä salasanoista lasketaan tietokantaan tallennettava tiiviste eli salasanaja ei tallenneta selväkielisinä.
POP3	Post Office Protocol 3 on protokolla, jota käytetään sähköpostiviestien hakemiseen sähköpostipalvelimelta. POP3-protokolla kopioi kaikki viestit palvelimelta tietokoneelle, jolla sähköpostiviestit luetaan. Tämän jälkeen viestejä ei säilytetä palvelimella, vaan ne poistetaan.
RSA	Rivest Shamir Adleman, julkiseen avaimen perustuva epäsymmetrinen kryptosysteemi. Systeemin kehittivät Ron Rivest, Adi Shamir ja Leonard Adleman.
SHA-1	Secure Hash Algorithm -1, Kryptografinen tiivistefunktio, jonka tehtävänä on varmistaa tiedon eheys.
SMTP	Simple Mail Transfer Protocol on protokolla jota käytetään sähköpostipalvelimien kesken sähköpostiviestien välittämiseen.
SSL	Secure Sockets Layer on tiedon salausprotokolla, jota HTTPS-protokolla käyttää tietoliikenteen salaamisessa. SSL tunnetaan TLS-protokollan edeltäjänä.

SQL	Structured Query Language on standardoitu kyselykieli. Kyselykielen avulla relaatiotietokantaan voidaan tehdä hakuja, kyselyjä sekä muutoksia.
TCP	Transmission Control Protocol, yhteydellinen kuljetusprotokolla, joka varmistaa IP-pakettien perille menon.
Tietokanta	Tallennettujen tietojen joukko, jotka ovat loogisesti yhteenkuuluvia. Tietokantaan voidaan tehdä kyselyjä SQL-kyselykieltä käyttämällä.
TLS	Transport Layer Security on salausprotokolla, jota HTTPS-protokolla käyttää tiedon salaamiseen.
UAC	User Account Control on Windows 7 -käyttöjärjestelmän turvaominaisuus, jonka tehtävänä on hallita tietokoneen käyttäjätilejä ja niiden oikeuksia.
UDP	User Datagram Protocol, yhteydetön kuljetusprotokolla. Yhteydetön kuljetusprotokolla ei varmista IP-pakettien perille menoa.
UPS	Uninterruptible power supply on laite, joka takaa virransyötön laitteistoille, kuten palvelimille vikatilanteissa.
URL	Uniform Resource Locator on yksilöity osoite Internetissä olevalle tiedostolle.
VPN	Virtual Private Network on virtuaalinen erillisverkko, jonka avulla yrityksen maantieteellisesti erillään olevat toimipisteet voidaan yhdistää ja mahdollistaa etätyö. VPN salaa kaiken virtuaalisessa verkossa siirrettävän tiedon.
WLAN	Wireless Local Area Network tarkoittaa langatonta lähiverkkotekniikkaa, jonka avulla laitteita voidaan yhdistää tietoverkkoon ilman kaapeleita.
WPA2	Wi-Fi Protected Access 2 on langattoman lähiverkon tiedonsalausprotokolla.

www-sivu Internetissä eli maailmanlaajuisessa verkossa julkaistu sivu.

XXS Cross site scripting (XXS) on www-sovelluksissa esiintyvä tietoturva-aukko, jota hyväksikäyttämällä hyökkääjä voi tunkeutua www-sivulle.

1 Johdanto

Hyvä tietoturva on viestintäverkoista riippuvaisessa tietoyhteiskunnassamme perustana sille, että tietojärjestelmien tarjoamien sähköisten palvelujen käyttäminen olisi mahdollisimman turvallista ja luotettavaa. Tietoturvaauhkien kehittyminen ja tietojärjestelmien lukuisat haavoittuvuudet asettavat tietokoneiden käyttäjille, tietoturvalle ja tietotekniikka alan-asiantuntijoille jatkuvasti uusia haasteita. Näin ollen ideaalia tilannetta, jossa tietoturva olisi täysin koskematon tietoturvauhille, on mahdotonta saavuttaa. Tietoturvaan liittyviä globaaleja uhkia, haavoittuvuuksia ja yritysten tietojärjestelmiin kohdistuneita ulkopuolisia hyökkäyksiä on julkaistu myös aktiivisesti eri medioissa lähiaikoina. Tämän johdosta tietoturva on opinnäytetyöaiheeksi hyvin ajankohtainen ja kiinnostava valinta.

Yrityksille ajan tasalla oleva tietoturvapoliitiikka on elintärkeä, oli kyseessä sitten pk-yrityksen tai suuren organisaation liiketoiminnassa käytettävät tietojärjestelmät. Mahdolliset tietoturvaloukkaukset vaikuttavat yritysten imagoon aina negatiivisesti varsinkin, jos sattuneet loukkaukset saavat laajempaa julkisuutta mediassa. Luonnollisesti tällaisissa tapauksissa yritysten nykyiset ja potentiaaliset uudet asiakkaat eivät ilahdu huonoista uutisista. Toimivat ja luotettavat tietojärjestelmät ovat siten yritysten toiminnan jatkuvuuden, kehityksen ja kilpailukyvyn edellytyksenä. Yritysten liiketoiminnalliset prosessit integroituvat osaksi toimivaa tietoteknistä infrastruktuuria, jota hyvän tietoturvapoliitiikan tehtävänä on tukea.

Tämän opinnäytetyön lähtökohtana on tutkia teoreettisesti yrityksissä käytettävän PC:n ja kannettavan työaseman haavoittuvuuksia sekä tietoturvaauhkia. Lisäksi lähtökohtana on selvittää, kuinka tietoturvauhkilta suojaudutaan käyttämällä teknisiä ratkaisuja ja hyviä käytäntöjä. Koska hyvästä ja riittävästä tietokoneen tietoturvasta on olemassa monenlaisia käsityksiä, päädytään tässä työssä käyttämään tietoturvan kannalta mahdollisimman turvallisia käytäntöjä. Näin voidaan varmistua, että käytännöt ovat riittävän tehokkaita täyttämään nykypäivän tietoturvan vaatimukset.

Opinnäytetyössä on myös oma osionsa pilvipalveluiden tietoturvasta. Halutessaan yritys voi siirtää tietojaan ulkopuolisten toimijoiden tarjoamiin pilvipalveluihin. Pilvipalveluiden avulla yritys voi säästää laitteisto- ja ylläpitokustannuksissa ja mahdollisesti myös

tietoturvan kustannuksissa. Tutkimuksen kohteena ovat pilvipalveluiden tietoturvaratkaisut, joiden perusteella yritys voi arvioida, parantavatko pilvipalvelut yrityksen tietoturvaa.

Opinnäytetyön tavoitteena on toimia tietoturvaa tukevana materiaalina toimeksiantaja yritykselle x, jonka nimi on muutettu tässä opinnäytetyössä. Lisäksi opinnäytetyöllä pyritään lisäämään yrityksen henkilöstön tietoturvan tuntemusta, oli kyseessä sitten yrityksen omien tietokoneiden tai ulkopuolisen tarjoamien pilvipalveluiden tietoturva. Osana opinnäytetyötä suoritetaan yritykselle tietoturvakysely, jonka tavoitteena on havainnollistaa yrityksen henkilöstön tämän hetkistä tietoturvan tuntemuksen tasoa. Kysymysten tarkoituksena on myös tutkia henkilöstön toimintamalleja erilaisissa PC:n tietoturvaa uhkaavissa tilanteissa, ja tunnistaa vastausten perusteella tietoturvalle vaaralliset toimintamallit.

2 Tietoturva

Suomen lainsäädännön mukaan tietoturva on osa organisaatioiden päivittäistä toimintaa ja se tulee hoitaa asianmukaisella tavalla [1, s.29]. Yritysmailmassa tietoturva tukee organisaation liiketoiminnan prosessien tarpeita ja täyttää sisäisiä sekä ulkoisia vaatimuksia. Organisaation tehokkuuden, toimivuuden ja kehityskyvyn määräävät tänä päivänä suurelta osin sen tietojärjestelmät ja niiden tietoturva. [2, s.19.] Tietoturva voidaan nähdä myös nykyajan kansalaistaitona, joka osaltaan takaa oman sekä muiden käyttäjien turvallisuuden tietoyhteiskunnassa.

2.1 Tiedon määritelmä

Tieto määritellään tämän opinnäytetyön tapauksessa eri muodoissa tallennettavaksi, käsiteltäväksi tai siirrettäväksi tiedoksi. Tiedon muotona voi olla asiakirja, tiedosto, ääni- tai kuvanauha, puhe, tietokanta, suoritettava ohjelma tai näyte. Tietoa tulisi tarkastella sen koko elinkaaren ajalta, jolloin tieto käy läpi sille ominaiset käsittelyvaiheet. Näitä tiedon käsittelyvaihteita ovat sen luonti, käyttäminen, muuttaminen, tallentaminen, siirtäminen jakelu, kopiointi, arkistointi ja tuhoaminen. [3, s.11.]

2.2 Tiedon turvaluokitukset

Tiedolle annetaan organisaatiossa tiedon turvaluokitus, jonka tarve on korostunut nykyaikaisessa sähköisessä asioinnissa ja sähköisessä arkistossa. Tiedot voidaan jakaa neljään turvaluokkaan seuraavasti:

- julkinen
- sisäinen
- luottamuksellinen
- salainen. [4.]

Julkinen tieto on luonteeltaan vapaasti kerrottavaa tietoa, kuten yrityksen www-sivuilla julkaistavaksi tarkoitettu tiedote. Julkinen tieto on siten kaikille nähtävissä, oli kyseessä sitten yrityksen oma henkilöstö tai täysin organisaation ulkopuolinen henkilö. Organisaation sisäinen tieto on tarkoitettu vain oman organisaation henkilökunnan tietoon ja kyseinen tieto on pidettävä ulkopuolisilta salassa. Sisäinen tieto voidaan julkaista esimerkiksi organisaation Intranet-sivuilla, joihin yrityksen ulkopuolisilla henkilöillä ei ole pääsyä. [4.]

Hallinnon tai työtehtävien näkökulmasta luottamuksellisia tietoja luokitellaan luottamuksellisen tiedon ryhmään. Tällainen luottamuksellinen tieto on pidettävä ulkopuolisilta salassa ja organisaation sisäisessä käytössä sen jakelu on rajoitettava tietoon oikeutetuille henkilöille. Salaista tietoa ovat asiakirjat, jotka sisältävät henkilötietoja ja asiakastietoja. Salainen tieto on henkilökohtaisesti salassa pidettävää tietoa. [4.]

2.3 Henkilöstön rooli

Yrityksen henkilöstö käsittelee ja tuottaa tietoa päivittäisessä työssään. Henkilöstön tietojenkäsittelyvälineillä prosessoima tieto sisältää yrityksen asiakkaiden ja mahdollisesti myös alihankkijoiden ja toimittajien asiakkaiden tietoja. Hyvää tietoturvaa voidaan pitää osana yrityksen organisaatiokulttuuria, jolloin henkilöstö ymmärtää tietoturvan merkityksen organisaatiolle. Tällöin yrityksen henkilöstö myös motivoituneesti työskentelee saavuttaakseen ja ylläpitääkseen organisaation hyvää tietoturvan tasoa. Hyvin toteutettu tietoturva tulisi nähdä yrityksessä kilpailuetuna, joka realisoituu liiketoiminnan jatkuvuudelle asetettujen edellytysten parantumisena. [1, s.12; 2, s.17-19.]

Lisäksi on huomioitava, että vastuu yrityksen tietojärjestelmien tietoturvasta koskettaa koko organisaation henkilöstöä. Näin ollen vastuu ei kuulu pelkästään vastuullisissa tehtävissä oleville henkilöille tai tietotekniikasta vastuussa olevalle osastolle. Organisaatiossa vaaditaankin jatkuvaa viestintää henkilöstön kesken ja koulutusta, jotta henkilöstö osaisi käsitellä tietoa vaaditulla huolellisuudella ja edistäisi tietoturvan toteutumista onnistuneesti. Organisaation tietoturvan voidaan sanoa olevan yhtä vahva, kuin sen heikoin lenkki. [1, s.12; 2, s.17-19.] Henkilöstön roolia ja tietoturvaan vaikuttavia toimintamalleja analysoidaan perusteellisemmin tämän opinnäytetyön kuudennessa luvussa.

2.4 Tietoturva ja tietosuoja

Tietoturva ja tietosuoja ovat tietoturvallisuuden keskeisiä termejä, jotka muistuttavat kieliasultaan hyvin paljon toisiaan. Samankaltaisen kieliasun johdosta nämä termit menevät ihmisiltä melko useasti sekaisin. Tietoturvan ja tietosuojan tavoite on sama eli tietojen suojaaminen, mutta suojattavan tiedon sisältö ja sen suojaamisen tarkoitus ovat molemmissa erilaiset. [5, s. 12.]

Tietoturvasta puhuttaessa tarkoitetaan tietojärjestelmien ja niissä sijaitsevan tiedon eli datan suojaamisesta. Tiedon suojaamisen lisäksi tietoturvan avulla varmistetaan tietojärjestelmien toiminta olosuhteista riippumatta, sekä niiden käytön turvallisuus. Näin saavutetaan tietoturvalle asetetut tavoitteet eli tiedon luottamuksellisuus, eheys ja käytettävyys. Tietoturvan tavoitteet on esitetty tarkemmin luvussa 2.5. [5, s. 12.]

Tietosuojan tavoitteena on suojata ihmisten henkilötietoja luvattomalta ulkopuoliselta käytöltä, jotta näitä mahdollisesti arkaluontoisiakin tietoja ei käytettäisi tarpeettomasti tai epäasiallisesti. Henkilötietoihin lukeutuvat ihmisten perustiedot, kuten nimi, osoite ja syntymäaika. Henkilötiedoiksi luetaan myös ihmisten ominaisuudet ja heidän toimintaansa kuvaavat merkinnät. Tietosuojan tehtävänä on varmistaa ihmisten oikeus yksityisyyteen. [1, s. 27; 5, s. 12.]

Lisäksi tietosuojaan kuuluu kansalaisten oikeus saada tietoa heitä koskevista rekisteritiedoista. Tietosuoja rajoittaa ja mahdollistaa luvanvaraiseksi yksilöstä kerättävien rekisterien ja tiedostojen ylläpitämisen ja tietojen luovutuksen niistä. Tietosuoja käsittää

sekä julkiset että salassa pidettävät henkilötiedot, joiden käsittelystä on säädetty laissa. Jokaisella kansalaisella on oikeus saada tietää ja tarkastaa henkilörekisterissä olevat itseään koskevat tiedot henkilötietolain 26. pykälän mukaan. Muutamat viranomaisten rekisterit eivät kuulu tämän tarkastusoikeuden piiriin, koska niiden tiedot voisivat vaarantaa yleistä turvallisuutta tai rikosten selvittämistä. [1, s.27; 5, s.254.]

Tietosuoja on ollut esillä mediassa tapauksissa, joissa virkamies on valtuuttamattomasti katsonut yksityishenkilön arkaluontoisia rekisteritietoja tietojärjestelmästä. Lisäksi on uutisoitu suurien organisaatioiden puutteellisesta tietoturvasta, joka on riski suuryritysten asiakkaiden tietosuojalle. Tietosuoja on myös puhuttanut ihmisiä sosiaalisen median palvelujen yleistyessä ja niiden saavuttaessa globaalin suosion. Tällaisia sosiaalisen median tarjoamia palveluja ovat esimerkiksi Facebook ja Instagram, joiden avulla käyttäjät voivat jakaa kuvamateriaalia ja tietoa. Tällaisissa sosiaalisen median palveluissa on riskinä, että käyttäjä itse paljastaa arkaluontoista tietoa.

Yhteenvetona tietoturvasta ja tietosuojasta voidaan sanoa, että tietoturvan tehtävänä on tarjota erilaisia keinoja tai toimintamalleja, joiden avulla tietosuojaa ylläpidetään. Tietoturvalla rakennetaan kuvainnollisesti muuri suojattavana olevan tiedon ympärille. Jos rakennettuna muurina toimiva tietoturva on heikko, ei se silloin riitä turvaamaan sellaisia tietoja, joita tietosuojalla on tavoitteena suojata. Tietojen suojaamisen tärkeys korostuu tapauksissa, joissa on kyse arkaluontoisista tiedoista, kuten henkilön terveydentilasta. [2, s.17.]

2.5 Tietoturvan tavoitteet

Tietoturvalle on asetettu tavoitteita, joiden saavuttamisen päämääränä on suojata yrityksen liiketoiminnalle tärkeät tietotekniset kohteet ja niissä sijaitseva tieto. Organisaation tietojärjestelmien ja tietoverkkojen tulee toimia keskeytymättömästi, tietojen ja tietojärjestelmien oikeudeton käyttö tulee estää ja tieto ei saa tuhoutua tai vääristyä. Tavoitteena on turvata tietoturvan kolme peruseriaa, jotka ovat tiedon:

- luottamuksellisuus (confidentiality)
- eheys (integrity)
- käytettävyys (availability). [1, s.29; 6, s.3.]

Tiedon on pysyttävä tarvittaessa luottamuksellisena eli tiedon näkyminen ulkopuolisille henkilöille, joilla ei ole oikeuksia nähdä sitä, täytyy estää. Tällaista tietoa yrityksissä ovat luottamukselliset sähköpostit, asiakirjat sekä palkka- ja henkilötiedot, jotka eivät saa vuotaa yrityksen tietojärjestelmistä julkisuuteen. Näiden tietojen tulee olla vain näihin kyseisiin tietoihin oikeutettujen ihmisten saatavilla. Luottamukselliseen tietoon pääsyä voidaan kontrolloida asettamalla käyttäjille salasanoja, rajoittamalla käyttäjäoikeuksia ja käyttämällä salausalgoritmeja. [5, s.10.]

Käytännön esimerkki tiedon luottamuksellisuudesta on henkilökohtainen tietokone, jonka kovalevyllä käyttäjä on tallentanut luottamuksellista tietoa asiakirjan muodossa. Vain järjestelmän pääsynvalvonnassa todennettu käyttäjä, jolla on tarvittavat käyttäjäoikeudet asiakirjaan, on oikeutettu lukemaan kovalevyllä tallennetussa asiakirjassa olevaa luottamuksellista tietoa. Käyttäjän henkilöllisyyden todentaminen tapahtuu tässä tapauksessa salasanalla, jonka järjestelmä vaatii tietokoneeseen kirjautumisen yhteydessä. Tiedon luottamuksellisena säilymiseen ei voida luottaa, jos oikeutetun henkilön salana paljastuu henkilölle, jolla ei ole oikeuksia nähdä asiakirjassa olevia tietoja.

Tietojen eheys edellyttää, että tietojen käsittelyn ja käytön aikana niihin kohdistuvat muutokset ovat oikeutettuja [5, s.10]. Tietoja eivät saa muuttaa valtuuttamattomat henkilöt tai prosessit, ja jos henkilöt ovat valtuutettuja, muutosten tulee olla luvallisia [6, s.3]. Konkreettinen esimerkki eheydestä ovat Internetin www-sivustot. Www-sivustoilla esitettyihin tietoihin voidaan tehdä oikeutettuja muutoksia, jolloin niiden tarjoama tieto sivustojen käyttäjille säilyy eheänä. Kun muutos tietoihin on oikeutettu, esitetty tieto on tällöin luotettavaa www-sivuston käyttäjille. Jos sivustoihin tehdään oikeudettomia muutoksia, esimerkiksi muutetaan jotain sivulla sijaitsevaa tietoa tahallisesti harhaanjohtavaksi, ei www-sivuston tarjoama tieto ole enää eheätä.

Tiedon eheys tulee varmistaa myös tiedonsiirron aikana, jolloin tieto siirtyy julkisessa verkossa. Julkisessa verkossa ulkopuolinen voi oikeudettomasti muokata siirtyvää dataa, jolloin tiedon eheys särkyä. Tiedon eheys voidaan varmistaa tiedonsiirron aikana tähän tarkoitukseen suunnitellulla tiiviste algoritmilla, jonka toimintaperiaate esitellään tämän opinnäytetyön luvussa 4.9.

Lisäksi tietojen tahaton tai tahallinen tuhoaminen vaarantaa tiedon eheyden. Tietokoneen tallennuspaikkana toimiva kovalevy voi hajota, tietoihin oikeutettu henkilö voi vahingossa poistaa tiedon tai tieto voidaan tuhota tahallisesti. Tiedon varmuuskopiointin avulla joko tahattomasti tai tahallisesti tuhoutunut tieto voidaan kuitenkin palauttaa.

Tietojen tulee myös olla käytettävissä, jotta käyttäjät voivat niitä tarvittaessa hyödyntää [5, s.10]. Tietojärjestelmien tarjoamat sähköiset palvelut ovat hyvä esimerkki käytettävyydestä. Käyttäjät kirjautuvat sähköisiin palveluihin saadakseen käyttöönsä niiden sisältämiä palveluja ja tietoja. Onnistuneella DoS-hyökkäyksellä eli palvelunestohyökkäyksellä voidaan estää jonkin sähköisen palvelun, kuten verkkopankin www-sivuston käytettävyys ja sen tietojen saatavuus asiakkaille. Tietojen käytettävyys estyy myös verkkolaitteiden, ohjelmistojen tai palvelimien vikaantuessa eli aina kyseessä ei ole ulkopuolinen hyökkäys vaan esimerkiksi palveluntarjoajan laitevika. Tietojen käytettävyyttä voidaan parantaa ottamalla tärkeistä tiedoista varmuuskopiot sekä huolehtimalla, että tietoverkoissa on laitevikojen varalta varalaitteita.

Näitä edellä esimerkein kuvattuja kolmea tietoturvan peruseriaa kutsutaan CIA-malliksi (confidentiality, integrity, availability). Vastakohtana tietoturvan tavoitteille ovat tiedon paljastuminen, muuttuminen ja tuhoutuminen (disclosure, alteration, destruction). [1, s.29; 6, s.3.] Tietoturvan kolmen peruseriaa lisäksi tietoturvan tavoitteisiin lasketaan myös kuuluvaksi:

- todennus (authentication)
- kiistämättömyys (non-repudiation)
- pääsynvalvonta (access control). [6, s.36.]

Todentamisen tarkoituksena on varmistaa, että käyttäjä on todella se henkilö, joka hän väittää olevansa [6, s.36]. Todentamisessa varmistetaan käyttäjän henkilöllisyys pyytämällä esimerkiksi salasanaa. Tapahtuman kiistämättömyyden tavoitteena on varmistaa, että esimerkiksi juridisesti sitova tapahtuma voidaan jälkeenpäin todistaa, ja henkilö ei voi kiistää suoritettua toimintaansa [3, s.8]. Kiistämättömyys saavutetaan siten, että tietojärjestelmän tapahtumista jää merkintä järjestelmän lokiin, josta tapahtumia voidaan etsiä ja jälkeenpäin todistaa. Pääsynvalvonta tarjoaa mekanismit, joiden avulla hallitaan käyttäjien todentamista ja sitä, mihin tietoon käyttäjillä on oikeudet. [7].

Pääsynvalvonta mekanismina tietokoneissa käytetään varsin yleisesti käyttäjätunnusta ja salasanaa, joiden avulla käyttäjän henkilöllisyys todennetaan. On olemassa myös muita käyttäjän todentamiseen tarkoitettuja pääsynvalvonta mekanismeja. Mobiilitodennus on yksinkertainen tapa, jossa käyttäjä palveluun rekisteröitymisen yhteydessä ilmoittaa puhelinnumerosa. Palvelusta lähetetään käyttäjän puhelimeen tekstiviesti, joka sisältää satunnaisen numerosarjan. Tekstiviestillä saapunut numerosarja syötetään kirjautumisikkunaan ja palvelu avautuu käyttäjälle. Puhelimeen voidaan myös asentaa mobiilivarmenne, jonka avulla käyttäjän todennus suoritetaan puhelimen sisällä. Varmenne avataan kirjoittamalla puhelimeen todentava pin-koodi ja näin todistetaan henkilöllisyys Internet-palvelulle. [5, s.143.]

Windows 8-käyttöjärjestelmässä on mahdollista suorittaa todentaminen käyttämällä tietokoneelle tallennettua valokuvaa. Käyttäjän tehtäväksi jää piirtää kuvan päälle kolmenlaisia merkkejä, kuten viivoja ympyröitä tai pisteitä. Käyttäjän todennus suoritetaan siten, että hän piirtää nämä merkit oikeisiin paikkoihin kuvassa. Luontevimmin merkeihin perustuva todennus onnistuu tablet-tietokoneilla. [5, s.150.]

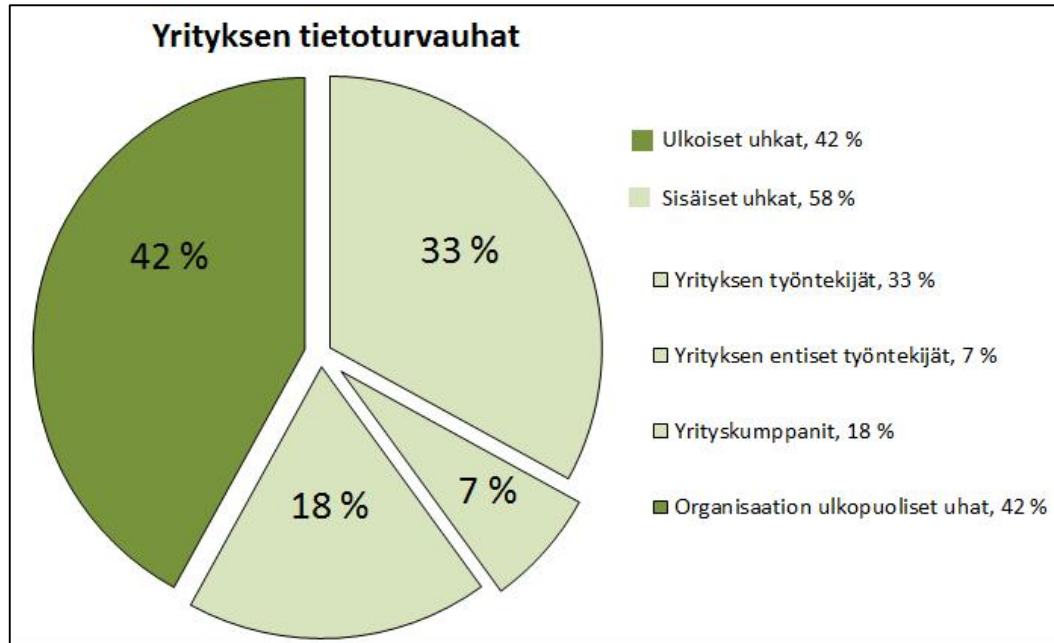
Biometrinen tunnistaminen perustuu ihmisten yksilöllisiin ominaisuuksiin. Näitä yksilöllisiä ominaisuuksia ovat henkilön sormenjäljet, puheääni, kasvonpiirteet ja silmän verkkokalvon rakenne. Biometrisessä tunnistuksessa etuna on, että käyttäjän ei tarvitse muistaa salasanaa. [5, s.153.]

3 Työasemien tietoturvaus

3.1 Tietoturvaus

Tietoturvauskalla tarkoitetaan tietoturvaan eli tiedon luottamuksellisuuden, eheyden ja käytettävyyden varmistaviin järjestelyihin kohdistuvaa uhkaa. Tietoturvaus voivat olla sisäisiä tai ulkoisia. Jos tietoturvaus muodostuu esimerkiksi organisaation oman henkilökunnan toiminnasta tai yrityksen suojaamattomista tietokoneista, tällöin puhutaan sisäisestä uhasta. Ulkopuolinen uhka kohdistuu organisaatioon sen ulkopuolelta esimerkiksi haittaohjelman, kuten tietokoneviruksen muodossa. Tietoturvaus toteutumisen todennäköisyyttä ja siitä seuraavan mahdollisen vahingon merkittävyyttä arvi-

oidaan tietoturvariskillä. Tietoturva-alan yritys Clearswift on tehnyt vuonna 2013 tutkimuksen, jonka tavoitteena oli selvittää ulkopuolisten uhkien ja sisäisten uhkien prosenttiosuudet yrityksissä (kuva 1). [8, s.13-14; 9.]



Kuva 1. Clearswiftin tekemän tutkimuksen tulokset. [9.]

3.2 Haavoittuvuudet

Haavoittuvuus tarkoittaa alttiutta tietoturvauhille. Haavoittuvuudeksi voidaan kutsua mitä tahansa heikkoutta, joka mahdollistaa vahingon toteutumisen. Tätä voidaan havainnollistaa ohjelmistolla, jossa oleva haavoittuvuus altistaa sen tietoturvauhille ja näin tekee mahdolliseksi tietojärjestelmän väärinkäytön. Tietojärjestelmien haavoittuvuudesta puhuttaessa voidaan myös toisinaan käyttää termiä tietoturva-aukko. [8, s.13-14.]

Nollapäivähaavoittuvuus on vaarallinen haavoittuvuuden ilmentymä, koska tässä tapauksessa tietoturva-aukko ei ole yleisesti tiedossa. Tästä johtuen kyseiseen tietoturva-aukkoon eli nollapäivähaavoittuvuuteen ei ole olemassa vielä korjaavaa päivitystä ja se on tietoturvauhkien hyväksikäytettävissä. Nollapäivähaavoittuvuuden arvo voi pimeillä markkinoilla olla lähemmäs miljoona euroa. Arvon ollessa näin korkea, pitää kyseessä olla jonkin uuden ja laajasti käytetyn ohjelman haavoittuvuus, kuten Flash-multimedialaajennuksen tai Office-sovelluksen. Nollapäivähaavoittuvuuden arvo putoaa luonnollisesti nolliin, kun tietoturva-aukko havaitaan ja siihen julkaistaan korjaava päivitys. [5, s.183.]

3.3 Tietoturvaloukkaus

Tietoturvaan kohdistuvaa oikeudetonta puuttumista kutsutaan tietoturvaloukkaukseksi. Esimerkiksi tietomurto yrityksen järjestelmiin on tietoturvaloukkaus. Tietovuoto tarkoittaa tietojen, kuten käyttäjien salasanojen, organisaation yrityssalaisuuksien tai yksilön arkaluontoisten tietojen vuotamista julkisuuteen esimerkiksi tietomurron yhteydessä. Tietomurto on rikos jossa tunkeudutaan tietojärjestelmään, kun taas tietosuojarikoksessa on kyseessä tietovuoto, jossa yksilön arkaluontoista tietoa leviää julkisuuteen. [1, s.172; 8, s.13-14.]

3.4 Haittaohjelmat

Haittaohjelmaksi (Malware) kutsutaan kaikkia niitä ohjelmia, jotka aiheuttavat tietokoneisiin päästyään vahinkoa tai haittaavat niiden normaalia toimintaa. Ensimmäiset haittaohjelmat, tietokonevirukset näkivät päivän valon jo 1980-luvulla, jolloin niiden kohteena toimivat Macintosh-koneet. Tekijöiden huomio kiinnittyi kuitenkin nopeasti yleistyvien PC-tietokoneiden DOS-käyttöjärjestelmiin. Koska tuolloin ei tietoverkkoyhteyksiä ollut, virusten leviäminen koneesta toiseen tapahtui levykkeiden mukana, joista ne tarttuivat edelleen ohjelmätiedostoihin. Käyttäjät eivät tienneet koneessa olleesta virus-tartunnasta, kunnes virus alkoi esittää ruudulla animaatiota tai soittamaan musiikkia koneen kaiuttimista. Tällaiset 1980-luvun virukset, kuten 1701, Ambulance tai Yankee Doodle olivat lähinnä kiusallisia tietokoneiden käyttäjille. Pahimmassa tapauksessa 80-luvun virukset, kuten Disk Killer ja Dark Avenger, saattoivat tuhota kiintolevyn ja sotkea tietokoneen tiedostoja. [5, s.177-178.]

Tänä päivänä haittaohjelmien luonne on täysin erilainen, kuin aikaisemmin 1980-luvulla. Modernissa yhteiskunnassa haittaohjelmien levittäjinä toimivat hakkerit ja näiden ohjelmien avulla on tarkoitus hakea taloudellista hyötyä. Tässä tapauksessa haittaohjelmasta on sitä enemmän hyötyä rikollisille, mitä kauemmin se tulee pysymään piilossa saastuneen tietokoneen käyttäjältä. [5, s.178.]

3.4.1 Haittaohjelmien tartuntamekanismit

Moderni murtautuja käyttää apunaan sosiaalista mediaa ja käyttäjän manipulointia (social engineering), tartuttaakseen yrityksen tietojärjestelmiin haittaohjelmia. Käyttäjän

manipuloinnilla tarkoitetaan tietojen luvaton hankkimista käyttäjää vakoilemalla tai harhauttamalla. Harhautuksessa käytetään perusmenetelmänä tekeytymistä eli esiinnyttään henkilönä tai tahona, jolla on oikeudet tietoihin. Manipuloinnin tavoite on saada ihmisen luottamus käyttämällä hänestä julkisesti saatavilla olevaa tietoa. [10;11]

Haaitaohjelmien levittämiseen ja käyttäjien manipulointiin sähköposti on erinomainen työkalu, koska se tuo tietoliikenneverkon välityksellä Internetistä tiedostoja käyttäjien tietokoneille. Haaitaohjelmia yritetään siten lähettää käyttäjille sähköpostien liitetiedostoina. Sähköpostien omat torjuntaohjelmat ovat kuitenkin nykyaikana hyviä tunnistamaan useimmat liitetiedostojen haaitaohjelmat. Tässä tapauksessa voidaan käyttää toista strategiaa eli sähköpostilla lähetetään tärkeältä vaikuttava linkki, jonka kautta käyttäjä huijataan lataamaan haaitaohjelma tietokoneelleen. [5, s.182.]

Haaitaohjelman voi saada tietokoneeseen myös miltä tahansa www-sivulta, jolloin puhutaan drive-by download -tartunnasta. Haaitaohjelma latautuu käyttäjän huomaamatta ja ilman, että käyttäjän tarvitsee itse tehdä mitään toimenpiteitä. Haaitaohjelma on tällaisessa tapauksessa istutettu tietomurron yhteydessä www-sivustolle. Osa haaitaohjelmista kykenee kokeilemaan erilaisia palvelinhaavoittuvuuksia ja siten levittämään itseään www-sivustoille. Haaitaohjelman voi saada tällaiselta murretulta www-sivustolta, jos oman Internet-selaimen tai siinä olevien laajennuksien eli lisäosien tietoturva-aukkoja ei ole paikattu. [5, s.183.]

Haaitaohjelma voi kytkeytyä osaksi selainta tietoturva-aukon sisältävän lisäosan avulla ja vaikuttaa selaimen normaaliin toimintaan. Selainta käytettäessä haaitaohjelma esimerkiksi kaappaa salasanoja, näyttää www-sivuilla mainoksia tai ohjaa käyttäjän väärin IP-osoitteisiin. Www-sivustolle istutettujen haaitaohjelmien todennäköisyys on suuri sivustoilla, joissa jaetaan sovellusten aktivointikoodeja tai muuten kyseenalaista sisältöä. Tällä mekanismilla saastuneissa tietokoneissa ei välttämättä ole mitään arvokasta tietoa mutta tietokoneita voidaankin hyödyntää esimerkiksi DoS-hyökkäyksien toteutuksessa ja haaitaohjelmien levityksessä. [5, s.183-184.]

Edellä mainittujen mekanismien lisäksi haaitaohjelmat käyttävät USB-muistitikkuja hyödyksi levitäkseen tietokoneisiin, kuten ne käyttivät levykkeitä 1990-luvulla. USB-muistitikkuja voidaankin pitää nykyajan levykkeinä. USB-muistitikkuja siirretään ko-

neesta toiseen ja samalla haittaohjelmat pääsevät leviämään tietokoneisiin. Haittaohjelmat tarttuvat USB-muistitikkujen lisäksi myös USB-kiintolevyihin ja digikameroiden muistikortteihin. Harvinaisen vaarallisen haittaohjelman sisältävästä USB-muistitikusta tekee sen mahdollisuus saastuttaa erityisen hyvin suojattuja kohteita. USB-muistitikkujen avulla haittaohjelma voidaan viedä julkisista verkoista erillään olevien tehtaiden ja voimalaitosten ohjauskoneisiin ja palomuuureilla suojattuihin yritysverkkoihin. Windows 7-käyttöjärjestelmästä on poistettu oletusarvoisesti autorun-toiminto, joka osaltaan auttaa suojautumaan ulkoisista muisteista automaattista käynnistystä hyödyntäviltä haittaohjelmilta. [5, s.188.]

Yrityksen tietojärjestelmiin haittaohjelmia tartutetaan käyttämällä asiantuntevasti tehtyjä kohdistettuja hyökkäyksiä (APT, Advanced Persistent Threat). Ensin hyökkääjät ottavat selvää, mitä virustorjuntaohjelmia ja muita suojauksia kohteena olevassa yrityksessä käytetään. Tämän perehtymisen jälkeen hyökkääjät suunnittelevat sellaisen haittaohjelman, joka ei aiheuta hälytystä organisaation virustorjuntaohjelmissa. Lisäksi hyökkääjät tutustuvat yrityksen organisaatiokaavioon ja henkilöstöön, käyttäen apunaan sosiaalista mediaa ja LinkedIn-palvelua tiedonhankinnassa. [5, s.183.]

Hyökkäys yrityksen tietojärjestelmiin käynnistetään lähettämällä muutamalle yrityksen avainhenkilölle sähköpostiviesti. Lähetetty viesti näyttää saapuvan toiselta työntekijältä tai tutulta yhteistyökumppanilta ja sisältää asialliselta näyttävän liitetiedoston, joka liittyy esimerkiksi työntekijöiden toimenkuviin. Tämän johdosta viestin saanut työntekijä avaa liitetiedoston ja sen seurauksena hänen tietokoneelleen pääsee nollapäivähaavoituvuutta hyväksi käyttävä haittaohjelma. [5, s.183.]

Haittaohjelman avulla hyökkääjät kuuntelevat näppäimistöä tai tietoverkkoa ja kaappaavat näin salasanoja. Kaapattuja salasanoja hyödyntäen hyökkääjät pystyvät eteneään yrityksen lähiverkon sisällä uusille tietokoneille ja lopuksi tavoittelemaansa tietoon. Kohdistetun hyökkäyksen prosessi voi kestää kuukausia, sillä hyökkääjillä ei ole kiirettä, heille vain tulokset ratkaisevat. Konkreettisia esimerkkejä kohdistettujen hyökkäyksien kykenevyydestä ovat Yhdysvaltojen puolustusvoimilta ja tietoturva-alan yhtiöiltä varastetut tiedot. Suomessakin sijaitseviin yrityksiin ja valtion virastoihin on hyökätty tällä periaatteella. [5, s.183.]

3.4.2 Haittaohjelmien luokittelu

Haittaohjelmia luokitellaan niiden ominaisuuksien ja toimintojen perusteella. Koska haittaohjelmia on hyvin paljon erilaisia ja niillä on samankaltaisia ominaisuuksia, niiden täsmällisen tarkka luokittelu on melko mahdotonta ja vaikeaa. Haittaohjelmat on kuitenkin tarkoitus aina luokitella ja yleensä ne kategorisoidaan seuraaviin yleisesti tunnetuihin ryhmiin:

- mato
- tietokonevirus
- troijalainen
- kiristysohjelma
- rootkit
- takaovi
- bottiverkot ja orjakoneet. [5, s.178;12;13.]

Mato (worm) on haittaohjelma, joka leviää tietoliikenneverkoissa tietokoneesta toiseen hyväksikäyttämällä tietokoneiden käyttöjärjestelmien ja sovelluksien haavoittuvuuksia. Levitessään madot käyttävät tietoliikenneverkkojen kaistanleveyttä ja kuormittavat työasemia, joka hidastaa tai pahimmassa tapauksessa kaataa tietojärjestelmiä. Tietokoneille voi myös aiheutua vahinkoa, jos mato sisältää haitallista suoritettavaa koodia (payload). Tällainen haitallinen suoritettava koodi on yleensä suunniteltu tietojen varastamiseen tai tiedostojen tuhoamiseen. [14.]

Madon tavoitteena on levitä saastuttamastaan tietokoneesta edelleen mahdollisimman moneen saastumattomaan tietokoneeseen. Madot pystyvät leviämään ja saastuttamaan tietokoneita automaattisesti ilman, että käyttäjän tarvitsee aktivoida niitä toiminnallaan millään tavalla. Madot leviävät myös hyvin nopeasti, koska ne pystyvät kopioimaan itseään. Jokainen kopio on itsenäinen mato, joka edelleen kopioi itseään eteenpäin. Mato ei toimiakseen lisää koodiaan tietokoneessa oleviin tiedostoihin tai ohjelmiin, vaan se toimii ja aiheuttaa vahinkoa itsenäisenä ohjelmana. [12;13;15.]

Madot hyödyntävät erilaisia keinoja, joiden avulla ne yrittävät levitä tietokoneesta toiseen. Madot voivat hyödyntää saastuneessa tietokoneessa jo olemassa olevia tietoli-

kenneverkkoyhteyksiä, joita ne käyttävät apunaan levitessään tietoverkoissa laajemmalle saastuttamaan uusia tietokoneita. Myös madon saastuttaman tietokoneen sähköpostiohjelmaa voidaan käyttää hyödyksi haittaohjelman levittämiseen. Tällaisessa tapauksessa mato käyttää apunaan sähköpostiohjelman osoitekirjaa, jonka avulla se lähettää itsestään kopioita kaikille osoitekirjasta löytyville henkilöille. Sosiaalisen median aikakaudella myös madot käyttävät sitä hyväkseen eli haittaohjelmaa voidaan yrittää levittää nykyään esimerkiksi Facebook-palvelun kautta. [15.]

Tietokonevirus (virus) on haittaohjelma, jonka tavoitteet ja vaikutukset saastuneessa järjestelmässä ovat samanlaisia kuin madolla. Tietokonevirukset on ohjelmoitu suorittamaan samankaltaisia haitallisia toimintoja, kuten tietojen tuhoamista tai sotkemista. Madolle ja tietokonevirukselle yhteistä on myös se, että ne pyrkivät leviämään saastuneelta tietokoneelta hyvin nopeasti mahdollisimman moneen toiseen tietokoneeseen. Virukset leviävät käyttämällä yleisiä haittaohjelmien tartuntamekanismeja, kuten sähköpostia, USB-muistitikkuja ja hyväksikäyttävät tietokoneiden käyttöjärjestelmien ja sovellusten haavoittuvuuksia. [12;14.]

Tietokonevirus vaatii levitäkseen ja toimiakseen, että käyttäjä aktivoi sen toiminnallaan suorittamalla jonkin ohjelman tai avaamalla haittaohjelman sisältävän sähköpostiviestin liitetiedoston. Virus voi siten olla uhkaavasti läsnä käyttäjän tietokoneella, mutta muodostua haitalliseksi vain käyttäjän toimesta. Toisin kuin itsenäisenä ohjelmana toimiva ja leviävä mato, tietokonevirus lisää aktivoituessaan haitallisen koodinsa tietokoneen tiedostoihin ja ohjelmiin. Virus tarvitsee siten aina isäntäohjelman, jonka avulla se voi suorittaa tietokoneelle haitallista koodia. Tällä tavalla virus myös leviää tietokoneessa. Mitä pidempään virus on tietokoneessa, sitä suuremman määrän tiedostoja se on saastuttanut haitallisella koodilla. [12;14.]

Trojalainen (Trojan) on haittaohjelma, joka suorittaa tietokoneessa oikeudettomia toimintoja lailliseksi ohjelmaksi tekeytyneenä. Toisin kuin tietokonevirukset ja madot, troijalaiset eivät pysty monistamaan itseään. Troijalaiset vaativat lisäksi käyttäjältä toimenpiteitä saastuttaakseen tietokoneen, joten ne yrittävät huijata käyttäjää. Troijalaiseksi määritellyn ohjelman on tavoitteena näyttää mahdollisimman hyödyllisestä ja harmittomalta sovellukselta. Käyttäjä huijataan lataamaan tämä sovellus mielenkiinnosta tietokoneelleen. Ladattava sovellus voi olla esimerkiksi www-sivuilta löytyvä peli, näy-

tönsäästäjä tai jopa virustorjuntaohjelma. Todellisuudessa tietokoneelle ladatun sovel-
luksen taustalla prosessoi käyttäjän huomaamatta troijalainen haittaohjelma, jonka ta-
voitteet ovat rikolliset. Troijalaisen haittaohjelman suorittamat toiminnot saastuneessa
järjestelmässä voivat olla yleisesti joitain seuraavista:

- tietojen tuhoaminen
- tietojen kopioiminen
- tietojen muokkaaminen
- takaoven lisääminen
- muiden haittaohjelmien, kuten virusten, aktivointi ja levittäminen
- tietoliikenneverkkojen ja tietokoneiden toiminnan häiritseminen. [16;17.]

Kiristysohjelma (ransomware) on haittaohjelma, jonka tavoitteena on kiristää rahaa tie-
tokoneen käyttäjältä. Haittaohjelma voi lukita tietokoneen näppäimistön, näytön tai jopa
koko tietokoneen siten, että käyttäjä ei voi avata lukitusta. Haittaohjelma esittää valheel-
lisiä ilmoituksia, joiden mukaan käyttäjä on ladannut tietokoneelleen piraattisovelluksia
tai katsonut laittomia videoita. Käyttäjää pyydetään tämän valheellisen tiedon perusteel-
la maksamaan sakko, jonka jälkeen varoitukset poistuisivat ja tietokonetta voisi taas
käyttää normaalisti. [13.] Kiristysohjelma voi lukita tietokoneen esimerkiksi poliisin
nimissä ja esittää tietokoneen ruudulla käyttäjään kohdistuvan syytteen ja rahalliset vaa-
timukset (kuva 2).



Kuva 2. Kiristysohjelma on lukinnut käyttäjän tietokoneen poliisin nimissä. [18.]

Rootkit-haittaohjelma (Rootkit) on suunniteltu olemaan mahdollisimman huomaamaton käyttäjälle ja olemassa oleville virustorjuntaohjelmistoille. Rootkit voi käynnistyä tietokoneessa ennen tietokoneen omaa käyttöjärjestelmää, jolloin sitä kutsutaan bootkit-haittaohjelmaksi. Rootkit myös piilottaa saastuneessa järjestelmässä olevia muita haittaohjelmia. Rootkit-haittaohjelman avulla voidaan esimerkiksi peittää troijalaisen haittaohjelman prosessointi tietokoneessa, jolloin käyttäjä tai virustorjuntaohjelmisto ei havaitse mitään normaalista poikkeavaa. [12;13.]

Takaovi (backdoor) on haittaohjelma, jonka kautta hyökkääjä pääsee käyttäjän saastuneeseen tietokoneeseen suorittamaan oikeudettomia toimia. Takaoven avulla hyökkääjä voi ohittaa saastuneen tietokoneen pääsynvalvontamekanismin ja ottaa siten saastuneen tietokoneen haltuunsa käyttämällä etäyhteyttä. Takaovi on yleensä lisätty salaa hyödylliseltä näyttävään troijalaiseen sovellukseen. Käyttäjä lataa tietokoneelleen sovelluksen mukana takaoven, jota hyödyntämällä ulkopuolinen hyökkääjä pääsee oikeudettomasti käyttäjän tietokoneelle. [5, s.179;13.]

Edellä kuvattujen haittaohjelmien lisäksi tietokoneen saastuttanut haittaohjelma voi myös ottaa haltuunsa tietokoneen tietoliikenneverkko-yhteyden. Tietokonetta kutsutaan tässä tapauksessa orjakoneeksi, koska se noudattaa ja toimii ulkopuoliselta hyökkääjältä tulevien ohjeiden mukaisesti. Bottiverkko (Botnet) tarkoittaa haittaohjelman saastuttamien orjakoneiden ryhmää, joita hyökkääjät ohjailevat tarkoituksiinsa soveltuen. Bottiverkoissa voi olla jopa kymmeniätuhansia haittaohjelman saastuttamia työasemia. Bottiverkon avulla tuotettuja palveluja voidaan myydä seuraaviin tarkoituksiin:

- lukuisten roskapostiviestien lähettäminen
- tietomurtojen jälkien peittäminen
- salasanojen murtaminen käyttämällä orjakoneiden laskentatehoa
- palvelunestohyökkäyksien toteuttaminen. [5, s.179.]

Tietokoneen käyttäjän on hyvin vaikeata huomata tietokoneensa muuttumista orjakoneeksi. Käyttäjä voi tosin huomata tietokoneen hidastumisen ja verkkoliikenteen kasvaneen määrän, mutta toisaalta tietokone voi käyttäytyä näin normaalistikin. Tietokoneen

luvaton käyttö orjakoneena paljastuu yleensä, kun operaattori ilmoittaa asiakkaalle havaitusta tartunnasta ja sulkee asiakkaan liittymän. [5, s.179.]

3.5 Phishing ja pharming

Luvussa 3.4.1 esiteltiin haittaohjelmien levittämisen työkaluna hyödynnettävä käyttäjän manipulointi (social engineering). Käyttäjän manipulointi voidaan jakaa phishing- ja pharming-hyökkäyksiin. Hyökkäysten tarkoituksena on saada käyttäjä luovuttamaan hyökkääjälle suoraan luottamuksellista tietoa, kuten verkkopankkien tunnuslukuja, tietokoneiden salasanoja ja henkilötietoja. [19.]

Phishing-hyökkäyksen toteuttamiseen voidaan käyttää sähköpostiviestiä, jonka on tarkoitus näyttää ulkoasultaan tunnetun yrityksen asiakaspalveluviestiltä. Sähköpostiviestiin on lisätty linkki, jota kautta käyttäjää pyydetään kirjautumaan palveluun esimerkiksi pankkitunnuksilla (kuva 3). Käyttäjän tietojen kyselyä voidaan viestissä perustella tunusten päivittämisellä tai tietojen tarkastamisella. Viestin linkistä avautuva sivusto voi näyttää täysin lailliselta sivulta, vaikka todellisuudessa kyseessä on rikollisten huijaussivusto. Kaikki tällaiselle huijaussivulle syötetyt tiedot päätyvät rikollisille. [19.]



Kuva 3. Esimerkki phishing-sähköpostiviestistä. [20.]

Pharming on vaikeampi sekä tehokkaampi tapa kalastella tietoja kuin edellä kuvattu phishing. Pharming-hyökkäyksen tarkoituksena on ohjata käyttäjä valesivustolle väärentämällä osoitetiedot, joita käyttäjän tietokone pyytää oikean sivuston löytämiseksi.

Valesivustolla käyttäjää pyydetään syöttämään esimerkiksi verkkopankin tunnuslukuja. Käyttäjä itse olettaa syöttävänsä tietoja oikealle ja lailliselle sivustolle. Pharming-hyökkäys voidaan toteuttaa kolmella eri tavalla:

- käyttäjän tietokoneen DNS-tietojen myrkytys
- sivustojenvälinen komentosarjahyökkäys (XSS-hyökkäys)
- palvelimen DNS-tietojen myrkyttäminen. [21.]

Käyttäjän tietokoneen DNS-tietojen myrkyttäminen tarkoittaa tietokoneen DNS-välimuistin oikeudetonta muokkaamista siten, että käyttäjä ohjataan valesivustolle, joka näyttää lailliselta sivustolta. Tietokoneet käyttävät DNS-välimuistia, johon on kopioituna aikaisemmin selattujen sivujen DNS-tietoja, jotta Internetin selaaminen olisi nopeampaa. Tietokoneen DNS-välimuistia voidaan muokata oikeudettomasti haittaohjelman, kuten troijalaisen avulla. [21.]

Sivustojenvälisen komentosarjahyökkäyksen tavoitteena on murtautua laillisten sivujen ohjelmistokoodiin. Yksinkertaisimmillaan se voidaan toteuttaa lisäämällä lailliselle sivustolle linkki, jota kautta käyttäjän ohjaus valesivustolle tapahtuu. Komentosarjan avulla voidaan myös selaimen tietoturva-aukkoa hyväksikäyttämällä saastuttaa käyttäjän tietokone. Komentosarjalla saastutettu tietokone ohjaa siten käyttäjän valesivustolle [21.]

Palvelimen DNS-tietojen myrkytyksellä tarkoitetaan Internet-palveluntarjoajan palvelimen DNS-välimuistin oikeudetonta muokkaamista. Internet-palveluntarjoajat käyttävät DNS-välimuistia, jotta käyttäjien tietokoneiden DNS-kyselyihin vastaaminen olisi nopeampaa. Palveluntarjoajan DNS-välimuistin oikeudettoman muokkaamisen jälkeen käyttäjät ohjataan valesivustoille, vaikka he kirjoittaisivat selaimen oikean sivuston URL-osoitteen. Palveluntarjoajien palvelimet ovat joka tapauksessa hyvin suojattuja, joten niiden DNS-tietojen myrkyttäminen on vaikeasti toteutettavissa, mutta käytännössä mahdollista. [21.]

3.6 Man In The Middle- ja Browser-hyökkäykset

Man In The Middle, eli MITM-hyökkäyksessä ulkopuolinen henkilö asettuu käyttäjän tietokoneen ja www-palvelimen, kuten verkkopankin- tai sähköpostipalvelimen tiedonsiirron väliin. Hyökkääjän tavoitteena on vakoilla käyttäjän tietokoneen ja www-palvelimen välillä siirtyvää luottamuksellista tietoa, kuten salasanoja tai verkkopankkitunnuksia. [22.]

Hyökkääjä voi toteuttaa MITM-hyökkäyksen kahdella erilaisella metodilla. Hyökkääjä voi pystyttää rikolliseen tarkoitukseen konfiguroidun reitittimen tai hyväksikäyttää laillisessa reitittimessä olevaa haavoittuvuutta. Reitittimellä tarkoitetaan verkkolaitetta, jonka avulla tietoliikennettä reititetään eri verkkojen välillä. Rikolliseen tarkoitukseen konfiguroidun reitittimen pystyttämiseen hyökkääjä käyttää omaa kannettavaa tietokonettaan tai verkkolaitetta, josta löytyy langaton verkkosovitin. Hyökkääjä asettaa laitteensa toimimaan langattomana tukiasemana ja nimeää langattoman verkon yleisesti julkisissa verkoissa käytetyllä nimellä, kuten ”kahvio” tai ”lentokenttä”. Käyttäjät muodostavat WLAN-yhteyden hyökkääjän pystyttämään tukiasemaan ja vierailevat sitä käyttäen Internetin www-sivuilla. Kaikki tietoliikenne käyttäjän tietokoneen ja Internetissä olevan www-palvelimen välillä kulkee rikollisen pystyttämän tukiaseman kautta. Hyökkääjä pystyy siten salakuuntelemaan eli kaappaamaan käyttäjien kirjaamia salasanoja ja muita arkaluontoisia tietoja, joita käyttäjät kirjoittavat www-sivuille. [22.]

Toinen vaihtoehto MITM-hyökkäykseen on käyttää laillista WLAN-tukiasemaa, jossa on hyväksikäytettävä haavoittuvuus. WLAN-tukiaseman haavoittuvuutta hyväksikäyttämällä hyökkääjän on mahdollista salakuunnella tukiaseman kautta kulkevaa verkkokäyttäjien tietoliikennettä. Tämä vaihtoehto on huomattavasti vaativampi toteutettava, mutta toteutuessaan se on tehokas tapa kaapata huomattavia määriä käyttäjien luottamuksellisia tietoja. [22.]

Man-In-The-Browser -hyökkäys on MITM-hyökkäyksen variantti, jossa hyökkääjän tavoitteena on saastuttaa käyttäjän Internet-selain haittaohjelmalla. Haittaohjelman avulla hyökkääjä kaappaa tietoja, kuten salasanoja, joita käyttäjän tietokoneen ja www-sivujen välillä siirretään.[22.]

4 Työasemien tietoturvauhkien torjunta ja ehkäisy

Hyvää tietoturvaa voidaan kuvailla vahvaksi muuriksi, jonka avulla tietoja suojataan tietoturva-uhilta. Organisaation työasemien tietoturvauhkien torjunta ja ehkäisy rakentuu monesta osa-alueesta, jotka toimivat kuvainnollisesti suojaavan muurin rakennuspalikoina. Jos näistä rakennuspalikoista puuttuu yksikin osa, tulee tietoa suojaavaan muuriin aukko, jota tietoturva-uhat voivat käyttää hyödykseen. Puolustus ulkoisia ja sisäisiä uhkia vastaan aloitetaan rakentamalla tietoturva osa-alueittain, jonka tuloksena tietoturva-uhkien hyväksikäyttämät tietoturva-aukot vähenevät.

4.1 Fyysinen turvallisuus

Fyysisen turvallisuuden tavoitteena on varmistaa organisaation prosesseille häiriötön ja turvallinen toimintaympäristö. Yrityksen toimitilojen ja niissä sijaitsevien laitteiden suojaaminen asianmukaisesti luo perustan tietoturvallisuuden ylläpitämiseen käytettäviin suojaustoimintoihin. Fyysisen turvallisuuden kannalta korkeaa suojausta vaativia kohteita ovat yrityksen omaan vahvuusalueisiin liittyvät toimitilat, kuten tuotekehitystilat, atk-laitetilat sekä hallinnolliset tilat. [2, s.125; 24, s.397.]

Organisaation tuotanto- ja toimitilojen fyysisellä suojaamisella estetään yrityksen tarvitsemien tietojen tuhoutuminen, vahingoittuminen tai joutuminen tietoon valtuuttamattoman henkilön haltuun. Yrityksen toimitilat tulisi suojata seuraavilta fyysistä turvallisuutta uhkaavilta tekijöiltä:

- varkaus
- tulipalo ja lämpötilan liiallinen kohoaminen
- vesivahinko ja kosteus
- sähköhäiriö
- pöly. [2, s.126.]

Kannettavilla tietokoneilla on erityisen suuri riski joutua varkauden kohteeksi, jos niitä säilytetään autoissa tai jätetään hetkeksikään vartioimatta. Käyttöjärjestelmän pääsynvalvonta suojaa tietokoneen oikeudettoman käytön, jolloin varastetun tietokoneen uusi käyttäjä ei voi kirjautua tietokoneeseen. Jos tietokoneen kovalevyä ei kuitenkaan ole

asianmukaisesti salattu, menettää pääsynvalvonta tällöin merkityksensä. Salaamattoman kovalevyn sisältämiä tietoja päästään lukemaan ja muokkaamaan ilman salasanaa, jos varastetun tietokoneen käyttöjärjestelmä asennetaan uudelleen. [24, 397-398; 25.]

Varkauksien kohteena ovat kannettavien tietokoneiden lisäksi yhä useammin tietokoneen sisällä olevat komponentit, kuten kovalevyt, muistipiirit ja kortit, sekä niiden sisältämät tiedot. Myös muut mobiililaitteet, kuten älypuhelimet ja tablet-tietokoneet ovat varkaiden kiinnostuksen kohteena [26.]. Varkaudet tapahtuvat usein keskellä päivää, jolloin toimitilojen hälytysjärjestelmät ovat kytketty pois päältä. Yrityksen laitetilaa ja muihin tietojenkäsittelytiloihin pääsyä tulisi seurata valvontalaitteistolla sekä varsinaisena työaikana, että toimitilojen ollessa suljettuna. Valvontalaitteisto ilmoittaa vartiointiliikkeeseen toimitiloihin luvattomasta tunkeutumisesta. [2, s.126; 24, 397.]

Organisaation tulee varautua sekä tulipaloihin, jotka voivat saada alkunsa hyvinkin monesta syystä, että tulipaloja yleisempiin vesivahinkoihin. On hyvä muistaa, että lapsikin voi tuhota kokonaisen talon tulen ja veden avulla. Laitetilan tulee siten olla eristettynä muusta tilasta paloturvallisesti ja tilaan ei saa päästä savua, joka voisi vahingoittaa tilassa olevia laitteita. Laitetilaan sijoitettavan ilmastoinnin avulla lämpötila pidetään sopivien raja-arvojen sisällä ja lämpötilojen kohoamista valvotaan lämpötila-antureilla, jotka ilmoittavat lämpötilan kriittisistä muutoksista. Vesivahinkoja taas aiheutuu rikkoutuvista putkista, joten laitetoissa ei tulisi olla vesiputkia, jotka voisivat aiheuttaa mahdollisen vesivahingon. Lisäksi on hyvä tietää, missä yrityksen toimitilojen yläpuolella olevien tilojen vesijohdot sijaitsevat. Vesivahingon vaikutusta voidaan ehkäistä myös siten, että tietoteknisiä laitteita ei säilytettäisi lattiatasossa. Pahimmassa tapauksessa tulipalo ja vesivahinko toteutuvat yrityksessä yhtä aikaa, jos tulipalon sammutusvedet valuvat kellaritiloihin, jossa sijaitsee organisaation tietoteknisiä laitteita. [2, s.127; 23, s.292.]

Lisäksi atk-laitteiston fyysistä turvallisuutta uhkaaviin tekijöihin liittyy olennaisesti sähköhäiriöt. Sähköhäiriöt voivat aiheuttaa käyttökatkoksia ja laiterikkoja. Tietotekniset laitteet voidaan suojata ylijännitesuojilla, jotka estävät esimerkiksi ukkoson aiheuttamista virtapiikeistä johtuvat laiterikot. Sähkökatkoihin voidaan varautua UPS-laitteilla, jotka varmistavat tasaisen sähkönsyötön laitteistolle vikatilanteissa. Myös staattinen sähkö on tietokoneille hyvin vahingollista. Staattista sähköä muodostuu helposti kotelolattiamatolla varustetuissa tiloissa. Varaus purkautuu kipinästä tietokoneeseen, kun käyttäjä kos-

kettaa sitä. Pahimmassa tapauksessa varauksen purkautumisesta aiheutuu ylijännite, joka tuhoaa jonkin tietokoneen komponentin. [2, s.127; 24, s.398.]

4.2 Kiintolevyn ja tiedostojen salaaminen

Salasanalla suojatun tietokoneen salaamattoman kiintolevyn sisältöä voidaan lukea ja muokata helposti ulkopuolisen toimesta, jos tietokone varastetaan [25]. Kiintolevyn suojausta voidaan parantaa merkittävästi salaamalla koko kiintolevy. Vaikka varkaalle menetetään laite, salauksen ansiosta varas ei pääse näkemään sen sisältämiä sähköposteja, asiakirjoja tai muita yksityisiä ja luottamuksellisia tietoja. Salausprosessi tulee tehdä myös USB-muistitikuille ja ulkoisille kiintolevyille, jos niiden sisältämä tieto edellyttää luottamuksellisuutta. [27.]

Kiintolevyn salaamiseen voidaan käyttää esimerkiksi avoimen lähdekoodin TrueCrypt-salausohjelmistoa. Jos ohjelmalla salataan järjestelmäosio eli kiintolevyn osa jossa käyttöjärjestelmä sijaitsee, tietokoneeseen tulee käynnistettäessä TrueCryptin käynnistysvalikko, johon käyttäjä syöttää salasanansa. Järjestelmäosion salaus voi hidastaa tietokoneen prosessointia, koska tietokoneen käyttäminen vaatii salauksen purkamista ja käsittelyä. Nykyaikaiset koneet ovat kuitenkin varsin tehokkaita, joilla suorituskykyä riittää. [27.]

Vaihtoehtoisesti TrueCrypt-salausohjelmalla voidaan luoda erityinen salattu säiliö, johon siirretään kaikki luottamukselliset tiedot. Ohjelmalla luotu säiliö on yksi tiedosto, jolle käyttäjä valitsee nimen ja koon. Säiliön avaamisen jälkeen se näkyy tietokoneessa virtuaalisena levyasemana, johon käyttäjä voi siirtää salattavat tiedostot. Suljettuna ollessaan säiliö on ulkoasultaan kuin mikä tahansa tiedosto, joten tiedoston ulkoasusta ei voida päätellä että kyseessä on salattu tiedostosäiliö. Tiedostot pysyvät näin salaisina ja piilossa ulkopuoliselta käytöltä. [27.]

TrueCrypt-salausohjelmisto tukee useita salausalgoritmeja ja salausavaimien pituuden voi määritellä omatoimisesti. Jos käyttäjä ei ymmärrä algoritmien toimintaa, on hyvä käyttää oletusasetuksia, joita ohjelma ehdottaa. Tässä tutkielmassa salausta ja siihen liittyviä käsitteitä esitetään tarkemmin luvussa 4.9. [27.]

4.3 Varmuuskopiointi

Tärkeät tiedostot voidaan varmistaa käyttämällä tiedostojen varmuuskopiointia. Tieto voi tuhoutua odottamattomasti ja tulla käyttäjälle täysin yllätyksenä. Esimerkiksi virtapiikki voi rikkoa tietokoneen, jolloin menetetään sen sisältämät tiedot. Haittaohjelma taas voi salata tietokoneen tärkeät tiedostot siten, että käyttäjä ei voi hyödyntää tietoja. [28.]

Jos varmuuskopiointi suoritetaan paikallisesti, voidaan varmuuskopiot tallentaa ulkoiselle kiintolevylle, DVD- tai Blu-ray levyille tai USB-muistitikulle. Varmuuskopiointi voidaan suorittaa käyttämällä tähän tarkoitukseen suunniteltua ohjelmaa. Hyvässä varmuuskopiointiohjelmassa tulisi olla mahdollisuus aikatauluttaa varmuuskopiointi, jolloin kopiointi suoritetaan automaattisesti ja säännöllisesti tietokoneeseen liitetulle ulkoiselle kiintolevylle. Ohjelman tulisi myös tukea inkrementaalista varmuuskopiointia eli varmuuskopiointi suoritetaan vain tiedostoille, joihin on tehty muutoksia edellisen varmistuksen jälkeen. Windows 7-käyttöjärjestelmässä on käytävissä sen oma varmuuskopiointi ohjelma Windows Backup and Restore. [29.]

Varmuuskopiointi ohjelma voi sisältää ominaisuuden, jonka avulla voidaan suorittaa varmuuskopiointi koko kiintolevystä eli luodaan järjestelmän näköistiedosto (image). Järjestelmän näköistiedoston etuna on se, että esimerkiksi tietokoneen kovalevyn rikkoutuessa ei tarvitse asentaa uudestaan käyttöjärjestelmää ja käytössä olleita sovelluksia. Myös järjestelmäasetukset ja tiedostot palautetaan näköistiedoston avulla. [29.]

On myös tärkeää suunnitella varmuuskopioiden fyysinen säilytys. Varmuuskopioita tulee ottaa erillisille medioille, joita voidaan säilyttää eri tiloissa. Yksi varmuuskopio voidaan säilyttää esimerkiksi yrityksen tiloissa ja toinen kopioista yrityksen tilojen ulkopuolella, joka on todettu turvalliseksi paikaksi varmuuskopion säilytykseen. Näin varmistetaan, että esimerkiksi tulipalossa tai varkaudessa ei menetetä kaikkia varmuuskopioita. [29.]

4.4 Virustorjuntaohjelma

Virustorjuntaohjelma suojaa tietokonetta haittaohjelmilta ja tarvittaessa poistaa tai eristää tietokoneesta löytyneen haittaohjelman ennen kuin se aiheuttaa tietokoneelle huo-

mattavaa vahinkoa. Tietokoneeseen asennetun virustorjuntaohjelmiston toiminta perustuu säännöllisiin virustietokannan päivityksiin, jotka mahdollistavat sen tehokkaan toiminnan uusia haittaohjelmia vastaan. Virustorjuntaohjelmiston tietokannasta löytyvän haittaohjelman tunnisteen avulla voidaan havaita ja estää varsinaisen haittaohjelman toiminta. Jos virustorjuntaohjelman tietokanta ei ole ajan tasalla, on tietokone alttiina uusille haittaohjelmille. Uusia haittaohjelmia löydetään päivittäin, joten virustorjuntaohjelmistojen virustietokannat tulee päivittää useasti saman päivän aikana. Useimmat virustorjuntaohjelmistot tarkistavat ja asentavat saatavilla olevat uudet päivitykset automaattisesti. [30;31;32.]

Virustorjuntaohjelmia asennettaessa on kiinnitettävä huomiota, että asennettava torjuntaohjelmisto on luotettava. Käyttäjää voidaan huijata asentamaan Internetistä käyttäjälle haitalliseen tarkoitukseen suunniteltu virustorjuntaohjelmisto, joka näyttää täysin lailliselta sovellukselta. Esimerkiksi trojan-FakeAV-ohjelmat simuloivat virustorjuntaohjelmaa. Tällaiset laittomat virustorjuntaohjelmat huijaavat tietokoneesta löytyneestä haittaohjelmasta ja vaativat käyttäjää maksamaan rahaa, jotta löytynyt haittaohjelma voidaan poistaa. [16.]

4.5 Palomuuuri

Palomuurin (firewall) tehtävänä on suojata tietokonetta Internetistä, eli ulkoverkosta tulevalta ei-toivotulta tietoliikenteeltä. Käyttäjä ei voi itse vaikuttaa siihen, mitä tietoliikennettä sisäverkossa oleville tietokoneille saapuu pyytämättä ulkoverkosta jos palomuuria ei ole. Näin ollen palomuuria tarvitaan aina, sitä eivät riitä korvaamaan käyttäjän koulutus tai oma varovaisuus. Palomuuuri ei kuitenkaan yksistään riitä suojaamaan tietokonetta haittaohjelmilta ja siten tietokoneessa tulee olla palomuurin lisäksi myös luvussa 4.4 esitelty virustorjuntaohjelmisto. [1, s.24-25; 5, s.189.]

Palomuuuri voidaan havainnollistaa liikennepoliisinä, joka ohjaa liikennettä sisäverkossa olevien tietokoneiden ja Internetin välissä. Palomuuuri joko päästää liikenteen läpi tai pysäyttää sen, riippuen IP-pakettien sisällöstä ja palomuurin ohjaussäännöistä. Jos palomuuuri joutuu suorittamaan liikenteen eston, siitä jää aina merkintä palomuurin lokiin. [5, s.189.]

Palomuurissa on portteja 65535 kappaletta, joista tärkeimpiä portteja eli tunnettuja portteja ovat 1023 ensimmäistä. Portilla ei tässä yhteydessä tarkoiteta fyysistä liitäntää, vaan IP-paketin mukana olevaa numerokoodia. Tämän numerokoodin avulla IP-paketin vastaanottava tietokone tietää, mille sovellukselle tietoliikenne kuuluu. Esimerkiksi http-yhteyksissä käytetään porttinumeroa 80, jolloin IP-paketit ohjautuvat web-palvelimelle. Suojatuissa https-yhteyksissä web-palvelimeen yhteyttä otettaessa käytetään porttinumeroa 443. Sisäverkon tietokoneet taas käyttävät satunnaisia portteja, jotka ovat välillä 1024-65535. Sisäverkon tietokoneet lisäävät aina myös satunnaisen porttinumeron ulkoverkkoon lähetettävään IP-pakettiin. Satunnaisen porttinumeron avulla ulkoverkon palvelimet voivat lähettää IP-paketteja sisäverkon tietokoneille. Jos palomuurin portti on auki (open), tällöin tietokone vastaa kyseiseen porttiin ulkoverkosta saapuviin kyselyihin. Suljettu (closed) portti vastaa kysyjälle, että portti on suljettu. Näkymätön (stealth) portti ei vastaa mitään eli kysyjän kannalta näyttää, että porttia ei olisi olemassa. Näkymätön portin tila on siten kaikista tietoturvallisin vaihtoehto. [5, s.192-195.]

Erityisen kriittisiä portteja Windows-koneissa ovat NetBIOS-portit 135, 139 ja 445. NetBIOS-portteja käytetään esimerkiksi Windows-käyttöjärjestelmässä tiedostojen ja verkkotulostimien jakamisessa tietoverkon käyttäjien kesken. Ulkopuolinen henkilö voi kuitenkin oikeudettomasti hyödyntää kyseisiä portteja ja käyttäjän tiedot ovat siten vaarassa joutua ulkopuolisen haltuun. NetBIOS-porttien ollessa auki on hyvin todennäköistä, että tietokoneeseen murtaudutaan ulkoverkosta. [5, s.192-195;33.]

Palomuurit asetetaan yleensä toimimaan siten, että ne estävät ulkoverkosta sisäverkkoon pyrkivän tietoliikenteen, jota sisäverkon tietokoneilta ei ole pyydetty. Sisäverkosta ulkoverkkoon lähtevän tietoliikenteen palomuurit taas päästävät läpi. Konkreettiseksi esimerkiksi palomuurin teknisestä toiminnasta voidaan esittää Internet-selaimen käyttäminen www-sivuilla vieraillessa. Palomuuri päästää liikenteen lähtemään ulkoverkkoon, kun www-sivu pyyntö tulee sisäverkon tietokoneen selaimelta ja kohteena on ulkoverkossa olevan www-palvelimen IP-osoite. Sisäverkon tietokoneelta lähtevä IP-paketti sisältää tunnetun porttinumeron 80 eli tietoliikenne ohjataan ulkoverkossa olevaan www-palvelimeen. Lisäksi sisäverkon tietokoneelta ulkoverkkoon lähtevään IP-pakettiin lisätään satunnainen porttinumero väliltä 1024-65535. Satunnaisella porttinumerolla tarkoitetaan sisäverkon tietokoneen satunnaisesti valitsemaa porttinumeroa, jonka avulla sisäverkon tietokone tietää, mille sovellukselle ulkoverkosta saapuva tieto-

liikenne ohjataan. Sisäverkon tietokone voi esimerkiksi käyttää tässä tapauksessa porttinumeroa 1030, jolloin ulkoverkosta porttiin 1030 saapuva tietoliikenne ohjataan sisäverkon tietokoneen selainsovellukselle. Ulkoverkossa sijaitseva www-palvelin vastaa ja palauttaa selaimen pyytämän www-sivun sisäverkon palomuurin porttinumeroon 1030. Koska palomuri tietää ulkoverkosta porttiin 1030 saapuvan www-sivun liittyvän äskettäin selaimen tekemään pyyntöön, päästää se www-sivun käyttäjän koneelle ja selainsovelluksen käyttöön. [5, s.192-194.]

Yrityskäytössä myös sisäverkosta lähtevää liikennettä tulee suodattaa. Yrityksissä palomuri päästää läpi ulkoverkkoon vain tarpeellisia protokollia, kuten www-sivujen selaamiseen käytettävän http-protokollan. Tarvittaessa tarpeellisiakin protokollia estetään, jos kohde IP-osoite on palomuurin sulkulistalla. Tällä tavalla voidaan estää esimerkiksi henkilökunnan pääsy Internetin viihdepalveluihin. Lähtevän liikenteen rajoituksilla voidaan organisaatiossa havaita myös työasemille päässeet haittaohjelmat, joiden tavoitteena on siirtää tietoa ulos yrityksen sisäverkosta. [5, s.194.]

Isoissa organisaatioissa palomuurin avulla voidaan analysoida verkon kuormitusta ja käyttöastetta sekä suojata yrityksen sisäverkkoa palvelunestohyökkäyksiltä. Palomuri myös piilottaa sisäverkon koneet osoitteenmuunnostekniikoilla eli NAT-toiminnolla ja PAT-toiminnolla. NAT-toimintoa hyödyntämällä yrityksen sisäverkon tietokoneet näkyvät ulkoverkkoon julkisen IP-osoitteen kautta. Sisäverkossa sijaitsevien tietokoneiden IP-osoitteina käytetään yksityisiä IP-osoitteita, joita ei reititetä ulkoverkkoon. Liikennöinti yrityksen sisäverkosta ulkoverkkoon tapahtuu siten julkisten IP-osoitteiden välityksellä. NAT voidaan toteuttaa dynaamisena, jolloin yrityksellä on käytössään useampia julkisia IP-osoitteita. Jos yrityksellä on käytössään vain yksi julkinen IP-osoite, tällöin osoitteenmuunnoksessa käytetään porttimuunnosta eli PAT-toimintoa. Tietoliikenne ohjataan ulkoverkon ja sisäverkon välillä PAT-toiminossa käyttämällä yhtä julkista IP-osoitetta. PAT-toiminnossa jokainen julkinen IP-osoitetta käyttävä sisäverkon tietokone saa lisäksi ainutlaatuisen porttinumeron. Porttinumeron perusteella tietoliikenne voidaan siten ohjata oikeille sisäverkon tietokoneille eli sisäverkon tietokoneiden yhteydet erotellaan porttinumeroita hyödyntämällä. PAT-toiminon avulla useampi sisäverkon tietokone voi olla yhteydessä ulkoverkkoon vain yhden julkisen IP-osoitteen välityksellä. Osoitteenmuunnostekniikoiden ansiosta tietoturva paranee, sillä organisaation verkon ulkopuolelta ei tällöin tiedetä onko sisäverkossa yksi vai tuhat tietokonetta.

Yrityksen sisäverkon infrastruktuuri voidaan näin häivyttää ulkopuolisilta. [5, s.194; 24, s.404.]

Jos edellytetään että organisaation tietoverkkoon tulee päästä ulkoverkosta, käytetään tässä tapauksessa portin uudelleenohjausta. Esimerkiksi yrityksen sähköpostipalvelimet ja www-palvelimet ovat esimerkkejä palveluista, joihin sallitaan ulkoverkosta tulevat yhteyspyynnöt. Portin uudelleenohjauksella palomuuuri välittää tietoliikenteen eteenpäin, sallien sen vain esimerkiksi yrityksen www-palvelimelle. Kaikki tietoliikenne, joka saapuu ulkoverkkoon näkyvään julkiseen IP-osoitteeseen ja porttinumeroon 80, uudelleen ohjataan siten yrityksen web-palvelimelle. Lisäksi on huomioitava, että kaikki yrityksen palvelimet, joihin sallitaan tietoliikennettä ulkoverkosta, sijoitetaan demilitarisoidulle alueelle (DMZ). Demilitarisoitu alue voidaan rakentaa esimerkiksi kahdesta palomuurilaitteesta, jotka erottavat yrityksen sisäverkon ja ulkoverkon. Näiden kahden palomuurin väliin jäävää aluetta kutsutaan demilitarisoiduksi alueeksi.

4.5.1 Palomuuriohjelma

Tietoliikennettä suodattavan palomuurin toimintamalli voidaan toteuttaa usealla erilaisella tavalla. Palomuuuri voi olla sisäverkon tietokoneissa oleva ohjelma, jonka kautta ulkoverkosta saapuva tietoliikenne tarkastetaan ennen sen ohjaamista tietokoneissa olevien sovellusten käyttöön. Tällainen ohjelmallinen palomuuuri on yksinkertaisin ja helpoin ratkaisu. [5, s.190.]

Jos palomuuriohjelmassa on tietoturva-aukkoja, haittaohjelmat voivat siinä tapauksessa päästä palomuurista läpi. Käyttäjän koneeseen muuta kautta päässeet haittaohjelmat voivat myös sammuttaa palomuuriohjelman. Sähköpostiviestit tarjoavat haittaohjelmille tällaisen mahdollisuuden. Rajoitetuilla käyttäjäoikeuksilla voidaan varmistaa, että haittaohjelma tai tahattomasti käyttäjä itse eivät pysty sammuttamaan palomuuriohjelmaa. [5, s.190.]

Vuonna 2001 ilmestynyt Windows XP oli Microsoftin käyttöjärjestelmistä ensimmäinen, joka sisälsi valmiiksi ohjelmallisen palomuurin. Oletusarvona palomuuriohjelma oli kuitenkin pois käytöstä. Haittaohjelmat saastuttivat haavoittuvuuksia sisältäneen Windows XP:n muutamassa minuutissa, kun tietokone oli kytketty julkiseen verkkoon. Sitten palomuuriohjelma on aina ollut oletusarvona käytössä Microsoftin käyttöjär-

jestelmissä. Tietokoneen näytölle annetaan käyttäjälle myös toistuvia varoituksia, jos palomuuriohjelma sammutetaan. Palomuuriohjelma on myös vakiona Mac- ja linux-tietokoneissa. [5, s.190.]

Huomioitavaa on, että palomuuriohjelmia tietokoneessa saa olla vain yksi kerrallaan. Jos tietokoneessa on enemmän kuin yksi palomuuriohjelma, ne alkavat kilpailemaan keskenään tietoliikenteen hallinnasta ja ohjaamisesta. Tämän johdosta palomuuriohjelmistoihin tulee toimintahäiriöitä ja niiden suojaustoiminnot eivät enää toimi oikein, joka taas altistaa tietokoneen haitalliselle tietoliikenteelle. Jos tietokoneeseen hankittavassa tietoturvaohjelmistossa on oma palomuurisovellus, tällöin tietokoneessa oletusarvona käytössä oleva palomuuriohjelma on kytkettävä pois päältä. Tietokoneeseen asennettavat tietoturvaohjelmistot tekevät tämän toimenpiteen automaattisesti, joten käyttäjän ei tarvitse itse huolehtia palomuuriohjelman kytkemisestä pois päältä. [5, s.190.]

4.5.2 Laitepalomuuuri

Palomuurin toimintamalli voidaan toteuttaa myös fyysisenä laitteistona eli erillisenä laitepalomuurina. Tässä tapauksessa palomuuuri ei sijaitse sisäverkon tietokoneissa palomuurisovelluksena, vaan erillisenä fyysisenä laitteena sijoitettuna sisäverkon ja ulko-verkon väliin. Laitepalomuuuri on toiminnaltaan luotettavampi kuin palomuuriohjelma, koska se ei sisällä prosesseja, joita haittaohjelma voisi käyttää hyökkäyksen kohteena. Lisäksi laitepalomuuuri suojaa kaikkia sisäverkossa sijaitsevia tietokoneita, riippumatta siitä millaisia käyttöjärjestelmiä sisäverkon tietokoneissa käytetään. [5, s.190.]

Laitepalomuuuri ja palomuuriohjelma myös kykenevät toimimaan yhdessä hyvin, toisin kuin kaksi palomuuriohjelmaa samalla tietokoneella. Jos laitepalomuurista sattuu pääsemään läpi haitallista tietoliikennettä, tietokoneen oma palomuuriohjelma pysäyttää läpi päässeän haitallisen liikenteen. Erillisiä laitepalomuuureja implementoidaan vain isoimpien organisaatioiden sisäverkkoihin. Pienemmissä verkkoinfrastruktuureissa, kuten pienissä yrityksissä palomuurin ominaisuudet eli NAT- ja PAT-toiminnot, löytyvät reititin ominaisuudet sisältävästä ADSL-modeemista tai WLAN-tukiasemasta. [5, s.190.]

Laitepalomuuuri ei riitä korvaamaan tietokoneille asennettavaa palomuuriohjelmaa. Vaikka käytössä olisi laitepalomuuuri, tulee aina tietokoneilla olla myös palomuurioh-

jelma. Esimerkiksi haittaohjelma voi päästä yrityksen sisäverkkoon USB-muistitikun välityksellä, jolloin haittaohjelma ohittaa organisaation laitepalomuurin. Palomuuriohjelman avulla estetään sisäverkkoon päässeän haittaohjelman leviäminen muihin sisäverkon sisällä sijaitseviin tietokoneisiin.

4.6 Päivitykset

Tietokoneen käyttöjärjestelmän ja sovellusten säännöllisillä päivityksillä voidaan pienentää huomattavasti haittaohjelmien hyväksikäyttämiä haavoittuvuuksia tietokoneissa. Haittaohjelmat hyödyntävät tietokoneiden käyttöjärjestelmistä ja ohjelmistoista löytyviä tunnettuja haavoittuvuuksia eli tietoturva-aukkoja, joita hyväksikäyttäen ne saastuttavat käyttäjän tietokoneen. Haittaohjelmille on myös luonteenomaista, että ne kehittyvät tekniseltä rakenteeltaan hyvin nopeasti ja pyrkivät hyödyntämään tietokoneiden käyttöjärjestelmien ja sovellusten nollapäivähaavoittuvuuksia. Tällaisia kustomoituja haittaohjelmia suunnitellaan suosituimpiin käytössä oleviin käyttöjärjestelmiin ja ohjelmiin, kuten Windows-käyttöjärjestelmiin ja Adoben-sovelluksiin. Tämän kehityksen johdosta ohjelmistokehittäjät etsivät taukoamatta sovellusten nollapäivähaavoittuvuuksia, laativat näihin korjaavia päivityksiä ja saattavat päivitykset edelleen ohjelmistojen loppukäyttäjille. Loppukäyttäjien tietokoneisiin julkaistavien päivitysten tavoitteet ovat seuraavat:

- tietoturva-aukkojen korjaaminen tietoturvapäivitysten avulla
- käyttöjärjestelmän resurssien optimointi
- uusien tietoturvaominaisuuksien lisääminen ohjelmistoihin
- vanhojen ja haavoittuvien ominaisuuksien poistaminen
- ajureiden päivittäminen. [34.]

Windows-käyttöjärjestelmä on suositeltavaa päivittää automaattisesti, koska tällöin käyttäjän ei tarvitse etsiä päivityksiä verkosta. Windows-käyttöjärjestelmän päivitysasetukset määritetään Windows Update- hallintatyökalulla. Windows Update käyttää ohjelmistotyökaluja, jotka tutkivat käyttäjän tietokoneessa olevaa Windows-versiota sekä muita tietokoneesta löytyviä Microsoft-ohjelmistojen versioita. Näiden tietojen perusteella tietokoneeseen asennetaan Windows-käyttöjärjestelmän ja muiden Microsoft-ohjelmistojen, kuten Explorer-selaimen ja Word-tekstinkäsittelyohjelman päivitykset. [35.]

Käyttöjärjestelmän ja sen sisältämien sovellusten päivittäminen on vain yksi osa-alue tietokoneen tietoturvapäivityksistä. Yhtä tärkeää on päivittää tietokoneelle asennetut kolmannen osapuolen sovellukset eli ohjelmistot joita ei ole asennettu käyttöjärjestelmän asennuksen yhteydessä. Tällaisia sovelluksia ovat käyttäjän itse asentamat sovellukset, kuten Internet-selaimet Firefox ja Google Chrome ja pdf-lukuohjelma Adobe Reader sekä virustorjuntaohjelmat. Mitä suositumpi ja laajemmin käytössä oleva sovellus on kyseessä, sitä suurempi todennäköisyys on saada haittaohjelma tällaisen päivittämättömän sovelluksen tietoturva-aukon kautta. Päivittämättömällä Internet-selaimella on riski joutua haittaohjelman hyökkäyksen kohteeksi miltä tahansa www-sivulta, johon on onnistuttu murtautumaan ja upottamaan haittaohjelma. Web-sovellukset ovat erityisen alttiita haavoittuvuuksille. [36.]

Kolmannen osapuolen sovellusten asetuksista on tapauskohtaisesti katsottava, miten niiden päivityspolitiikka toimii. Suositeltavaa on, että sovellukset asetettaisiin huolehtimaan päivitysten tarkastamisesta automaattisesti. Useat sovellukset ilmoittavat näin saatavilla olevista päivityksistä, jonka jälkeen käyttäjä voi itse ladata ja asentaa ne. Ohjelman ilmoittaessa uudesta saatavalla olevasta päivityksestä, tulee päivitys ladata ja asentaa välittömästi. [36.]

Huomion arvoista on myös se, että mitä vähemmän tietokoneessa on sovelluksia, sitä vähemmän haittaohjelmilla on mahdollisia sovellusten tietoturva-aukkoja hyödynnettävään. Tästä johtuen kaikki käyttäjälle tarpeettomat sovellukset, joita ei enää käytetä ja päivitetä, on suositeltavaa poistaa tietokoneesta. Ennen sovellusten poistamista on hyvä ottaa varmuuskopiot tärkeistä tiedostoista ja varmistua poistettavan sovelluksen tarpeellisuudesta järjestelmän toimivuuden kannalta. Myös turhat Internet-selaimen lisäosat on hyvä poistaa käytöstä. Mitä vähemmän selaimessa käytetään lisäosia, sitä vähemmän on olemassa mahdollisia haittaohjelmien hyödyntämiä tietoturva-aukkoja [5, s.183-184; 37; 38.]

4.7 Salasanat

Tietokoneissa ja verkkopalveluissa käytetään yleisesti käyttäjätunnukseen ja salasanaan perustuvaa pääsynvalvontamekanismia. Käyttäjätunnuksen avulla käyttäjät yksilöidään ja yksilöityjen käyttäjien henkilöllisyys todennetaan salasanan avulla. Salasanan tarkoi-

tuksena on estää tietokoneiden, tietoverkkojen, sovellusten ja luottamuksellisen tiedon oikeudeton käyttö, jolloin tieto on käytettävissä vain siihen oikeutetuille henkilöille. [39.]

Käyttäjää manipuloimalla salasanoja voidaan kysyä yrityksen työntekijöiltä hyödyntämällä sähköpostia tai jotain toista viestintäkanavaa kuten puhelinta. Käyttäjälle voidaan lähettää sähköpostiviesti tietohallinnon nimissä ja ilmoittaa, että käyttäjän salasana tulisi vahvistaa. Salasan vahvistaminen tapahtuu viestissä olevasta linkistä, joka todellisuudessa johtaa rikolliselle sivustolle, jota kautta salasana päättyy rikollisille. [10;11]

Teknisesti salasanoihin voidaan kohdistaa Brute-force- ja sanakirjahyökkäyksiä (dictionary attack), joiden tavoitteena on murtaa käyttäjien laatimia salasanoja. Brute-force-hyökkäys perustuu lukemattomien mahdollisten salasana vaihtoehtojen kokeilemiseen, kunnes kohdalle sattuu oikea salasana. Tällainen hyökkäys toteutetaan ohjelmallisilla työkaluilla käyttämällä apuna nykyaikaisten tietokoneiden nopeaa laskentatehoa. Sanakirjahyökkäys toteutetaan samalla periaatteella, mutta sen tapauksessa ei kokeilla kaikkia mahdollisia salasana kombinaatioita. Sanakirjahyökkäykseen tarkoitettu ohjelmisto käyttää apunaan eri maiden sanakirjoista löytyviä selväkielisiä sanoja. [40.]

Edellä kuvattujen hyökkäyksien toteuttaminen verkkopalveluihin on vaikeaa. Verkkopalvelut sallivat rajoitetun määrän vääriä salasana yrityksiä, esimerkiksi kolme yritystä, kunnes ne estävät IP -osoitteet, jotka yrittävät kirjautua väärillä salasanilla. Tilanne on kuitenkin toinen, jos hyökkääjä saa käyttöönsä salasanalla suojatun tiedoston tai fyysisen laitteiston, kuten varastetun tietokoneen. Tällaisessa tilanteessa hyökkääjä voi kokeilla ohjelmistotyökaluja hyväksikäyttäen lukemattoman määrän salasanoja, kunnes hän onnistuu murtautumaan suojattuun tiedostoon tai tietokoneeseen. [40.]

4.7.1 Salasanojen suojaaminen verkkopalveluissa

Mediassa on kerrottu useasti tietomurtojen kohteeksi joutuneista verkkosivustoista, joilta on onnistuttu julkaisemaan miljoonia käyttäjätilejä ja salasanoja. Monet verkkosivujen käyttäjät olivat valinneet salasanaksi huonon ja heikon salasan, joka olisi arvattavissa ilman ohjelmallisiakin työkaluja. Käyttäjien kymmenen yleisintä salasanaa vuoden 2013 aikana, jotka tulivat julki tietomurtojen yhteydessä, olivat seuraavat:

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123 [41;42.]

Verkkopalveluihin kohdistuneissa hyökkäyksissä käyttäjien laatimia salasanoja on joissain tapauksissa säilytetty vastuuttomasti tietokannoissa selväkielisinä. Näin verkkopalveluiden ei pitäisi ikinä tehdä, sillä verkkopalveluun tietomurtautunut voi SQL-injektiohyökkäyksellä listata selväkielisenä kaikkien käyttäjien salasanat. SQL-injektiohyökkäys on mahdollinen jos verkkopalvelun SQL-tietokannassa on tietoturva-aukko. SQL-injektiohyökkäyksellä tarkoitetaan, että ulkopuolinen henkilö voi tehdä verkkopalvelun SQL-tietokantaan sellaisia kyselyjä, joihin hänellä ei tulisi olla oikeuksia. Ulkopuolinen henkilö voi esimerkiksi tehdä SQL-tietokantaan kyselyn, joka tulostaa näytölle kaikkien verkkopalvelun käyttäjien käyttäjänimet ja käyttäjänimiä vastaavat salasanat. Selväkielisessä salasanojen säilytysratkaisussa vahvojen salasanojen laatimisella ei ole siten mitään merkitystä jos esimerkiksi SQL-injektiohyökkäys on mahdollista toteuttaa tietoturva-aukon sisältämään salasanatietokantaan. Verkkopalveluiden tulisi tallentaa käyttäjien salasanat kolmea perussääntöä noudattaen:

1. Salasanan salaus yhdensuuntaisella tiivistefunktiolla
2. Satunnaisten bittien lisääminen eli suolauksen käyttäminen salauksessa
3. Tallennetaan ainoastaan salasanan salattu versio. [43;44;45.]

Yhdensuuntaisella salauksella tarkoitetaan salausta, jossa käytetään matemaattista funktiota, kuten nykyisin suositeltavia hitaita tiivistefunktioita nimeltä PBKDF2 (Password-Based Key Derivation Function 2) tai Blowfish. Yhdensuuntaisessa salauksessa matemaattiselle funktiolle on tyypillistä, että se pystytään helposti laskemaan toiseen suun-

taan, mutta sen käänteisfunktion laskeminen on hyvin vaikeaa ja hidasta. Käytännössä tämä tarkoittaa, että salatusta tekstistä ei siten voida selvittää, minkälainen alkuperäinen salaamaton teksti on. [44;45.]

Jos käytetään pelkästään yhdensuuntaista salausta, voidaan yhden salasanan salakielistä versiota verrata salasanatietokannan kaikkiin salasanoihin. Vertailu estetään menetelmällä, jossa jokaiseen salasanaan lisätään yksilöidysti satunnaisia bittejä. Tätä menetelmää kutsutaan salasanojen suolaukseksi ja tämän menetelmän avulla kahden samankin salasanan salatut versiot ovat erilaiset. Lisäksi salasanaan lisätyt satunnaiset bitit lisäävät salasanan efektiivistä pituutta. [43;44;45.]

Salasanasta tallennetaan siten salasanatietokantaan vain edellä kuvatulla tavalla salattu versio. Kun käyttäjä kirjautuu verkkopalveluun, hänen järjestelmään kirjoittamansa salasana salataan käyttämällä matemaattista funktiota ja lisätään salasanalle yksilöity suola eli satunnaiset bitit. Tämän jälkeen salattua salasanaa verrataan verkkopalvelun salasanatietokannassa olevaan salattuun salasanaan. [45.]

4.7.2 Vahvan salasanan laatiminen

Salasanan laatimiseen käyttäjille on annettu tarkkoja ohjeita, joiden avulla voidaan tunnistaa heikot salasanat ja luoda vahvoja, vaikeasti arvattavia ja murrettavia salasanoja. Seuraavassa on luettelo tunnusmerkeistä, jotka ovat heikkoja salasanoja ja joita murtautajat suurella todennäköisyydellä kokeilevat ensimmäisenä:

- nimet ja numerot, jotka liittyvät salasanan laatijaan, kuten syntymäpäivä tai lempinimi
- käyttäjänimi missään muodossa
- oman nimen, perheenjäsenen nimen tai lemmikin nimen johdannaiset
- millä tahansa kielellä kirjoitetut kokonaiset sanat
- numerosarja tai helppo kirjainyhdistelmä, kuten 12345678 tai qwerty
- käyttäjää koskeva ja helposti saatavilla oleva tieto, kuten puhelinnumero.

[41;46.]

Vahvalla salasanalla tietokone voidaan suojata tietomurroilta ja haittaohjelmilta. Vahvan salasanan tulee sisältää seuraavat kriteerit:

- salasanan pituus on vähintään kahdeksan merkkiä pitkä. Mitä enemmän salasanassa on merkkejä, sitä vahvempi salasana on
- salasana sisältää isoja kirjaimia
- salasana sisältää pieniä kirjaimia
- salasana sisältää numeroita
- ei sisällä enempää, kuin kaksi samaa kirjainta peräkkäin
- salasana sisältää merkkejä, jotka eivät ole kirjaimia tai numeroita. [39;46.]

Edellä lueteltuja kriteerejä käyttämällä salasana voi edelleen olla heikko, jos siinä käytetään heikon salasanan tunnusmerkkejä. Salasana Hello2U! sisältää kaikki vahvan salasanan kriteerit mutta se luokitellaan heikoksi, koska se sisältää kokonaisen sanan. [46.]

Vahvan salasanan rakentaminen voidaan aloittaa valitsemalla helposti muistettava virke, josta on mahdollista luoda lyhenne. Esimerkkinä voidaan käyttää virkettä ”*matkustin afrikkaan kesällä 2002*”. Tämän jälkeen osa virkkeen kirjaimista muutetaan isoiksi kirjaimiksi ja virkettä lyhennetään poistamalla haluttuja kirjaimia. Lisäksi kirjaimia korvataan numeroilla ja symboleilla. Siten virkkeestä ”*matkustin afrikkaan kesällä 2002*” saadaan muodostettua vahva salasana, joka on esimerkiksi muotoa ”*maT@frK3s2()02*”.

Salasanat tulee myös vaihtaa säännöllisesti ja käyttäjän omistamilla eri tileillä tulee käyttää eri salasanoja. Jos samaa salasanaa käytetään kaikilla käyttäjän omistamilla tileillä, tällöin yhdellä salasanalla voidaan murtautua kaikkiin käyttäjän tileihin, kuten sähköpostitiliin ja tietokoneisiin. Salasanan vaihtoväliin vaikuttaa merkittävästi salasanan pituus. Salasanan pituutta lisäämällä, vaikka kymmeneen merkkiin, voidaan lisätä salasanan vahvuutta ja siten sen vaihtoväliä. [39;43.]

Käyttäjiä ohjeistetaan säilyttämään salasanansa siten, että kukaan ulkopuolinen ei voi saada niitä tietoonsa. On kohtuutonta olettaa, että käyttäjät muistaisivat lukuisat eri tiliensä salasanat. Salasanojen säilytykseen suunnitellun Keepass-ohjelman avulla käyttäjän tulee muistaa vain yksi salasana. Ohjelma salaa kaikki käyttäjän salasanat keskite-

tysti tietokantaansa AES-algoritmillä ja käyttäjä voi purkaa tämän salauksen yhdellä laatimallaan salasanalla. [46.] Myös LastPass-ohjelma on suunniteltu salasanojen turvalliseen säilyttämiseen. [48.]

4.8 Käyttäjäoikeuksien rajoittaminen

Asettamalla tietokoneen eri käyttäjätileille erilaisia käyttöoikeuksia, voidaan tietokoneen tietoturvaa parantaa merkittävästi. Käyttöoikeuksien rajoittamisen avulla estetään haittaohjelmien asentaminen sekä niiden aiheuttamien oikeudettomien muutosten tekeminen tietokoneeseen. Tietokoneen saastuttaman haittaohjelman oikeudet järjestelmässä ovat suoraan verrannollisia kirjautuneena olevan käyttäjätilin oikeuksiin. Käytännössä tämä tarkoittaa, että haittaohjelmalla on oikeudet vain niihin toimenpiteisiin, mitkä käyttäjätilille kirjautuneelle käyttäjälle on sallittu. [49;50.]

Tietokoneiden käyttäjätilit voidaan jakaa kahteen ryhmään eli peruskäyttäjätileihin ja järjestelmänvalvojien tileihin. Peruskäyttäjälle annetaan järjestelmässä matalamman tason oikeudet, jotka oikeuttavat käyttäjän normaaliin työskentelyyn, kuten sähköpostin lähettämiseen, Internetin selaamiseen ja tekstinkäsittelyohjelman käyttämiseen. Peruskäyttäjä ei saa esimerkiksi oikeuksia muuttaa tietokoneen tietoturva-asetuksia, jolloin estetään käyttäjän tahaton tietoturvan vaarantaminen tai tahallisen haittaohjelman mahdollisuus muokata asetuksia. [49;50.]

Järjestelmänvalvojalla taas on järjestelmään täydet hallinnolliset oikeudet, jotka oikeuttavat asetusten muuttamiseen, ohjelmien asentamiseen ja muiden käyttäjätilien hallintaan. Monet haittaohjelmat vaativatkin toimiakseen tietokoneissa järjestelmänvalvojan oikeudet. Haittaohjelmat saavat paljon enemmän vahinkoa aikaiseksi, jos käyttäjä on kirjautuneena tietokoneeseen järjestelmänvalvojan oikeuksilla haittaohjelman tartunta hetkellä. Tämän johdosta tietokoneeseen kirjaudutaan aina peruskäyttäjän tilillä, jolloin työskentely on merkittävästi turvallisempaa ja mahdollisen haittaohjelman toiminta mahdollisuudet rajataan olemattomaksi. Järjestelmänvalvojan tehtäviä voidaan tarvittaessa suorittaa peruskäyttäjän tilillä kirjautuneena, jos käyttäjä todentaa henkilöllisyytensä järjestelmänvalvojan salasanalla. [49;50.]

Windows 7- ja 8-käyttöjärjestelmässä käyttöoikeuksia valvoo ja hallitsee käyttäjätilien hallintatyökalu UAC (User Account Control). UAC-hallintatyökalun avulla voidaan

rajoittaa, mitä muutoksia ohjelmat voivat tehdä tietokoneeseen. UAC informoi aina käyttäjää ilmoituksella, jos jokin ohjelma on tekemässä tietokoneeseen muutosta, missä vaaditaan järjestelmänvalvojan oikeudet. [49.]

Hallintatyökalun avulla saavutettava vakaampi tietoturvallisuus perustuu sen kykyyn säädellä käyttäjätilin oikeustasoa tilanteen vaatimalla tavalla. UAC-hallintatyökalu varmistaa, että tietokoneeseen ei tehdä mitään muutoksia käyttäjän tietämättä ja käyttöoikeudet eivät ole tarpeettomasti korkeimmalla tasolla. Järjestelmänvalvojallakin on tässä tapauksessa käytössään vain peruskäyttäjänoikeudet ja väliaikaisesti hänelle voidaan myöntää järjestelmänvalvojan valtuudet suorittaa hallinnollisia tehtäviä. Jos järjestelmänvalvojan valtuudet omaava käyttäjä saa hallintatyökalulta ilmoituksen, että tietokoneeseen ollaan tekemässä muutoksia, voi hän halutessaan antaa oikeuden tehdä muutokset. Siten hänelle annetaan salasana todennuksen jälkeen väliaikaisesti järjestelmänvalvojan oikeudet tehtävän suorittamiseen ja tämän jälkeen oikeudet palautetaan takaisin peruskäyttäjän tasolle. Käyttäjät, joilla ei ole järjestelmänvalvojan salasanaa, eivät voi suorittaa mitään UAC-työkalun ilmoittamia toimenpiteitä. Näiden käyttäjien oikeudet pysyvät siten aina peruskäyttäjien oikeuksina. [49.]

4.9 Salausmenetelmät

Tieto määritellään tietotekniikassa selväkieliseksi, jos sitä voidaan ymmärtää ja lukea ilman, että sen tulkitsemiseen tarvitaan laskennallisia toimenpiteitä. Tapaa, jolla selväkielisen tiedon sisältö salataan siten, että sitä ei voida ymmärtää tai lukea, kutsutaan salaukseksi. Tiedon salauksen avulla voidaan saavuttaa tiedon luottamuksellisuus, eheys, todennus ja kiistämättömyys. Tiedon salaamisessa ja salauksen purkamisessa käytetään salausavaimia, jotka perustuvat matemaattisiin funktioihin eli salausalgoritmeihin. Salausavaimen pituus ja käytettävä salausalgoritmi vaikuttavat merkittävästi tiedon salauksen vahvuuteen, koska nykyaikaisen tietokoneen laskentatehoa hyödyntäen voidaan murtaa helposti lyhyet salausavaimet. Riittävän vahvoilla avaimilla ja salausalgoritmeilla ei pystytä murtamaan salausta. Salauksen purkaminen veisi äärettömän pitkän ajan, vaikka käytössä olisi useamman tietokoneen laskentateho. [51;52.]

Symmetrisessä salausjärjestelmässä tiedon salaaminen ja salauksen purkaminen suoritetaan samalla salausavaimella. Tietoturvan näkökulmasta ongelmalliseksi muodostuu salausavaimen toimittaminen toiselle osapuolelle, jonka avulla hän voi purkaa salauk-

sen. Jos ulkopuolinen pystyy kaappaamaan salaisen avaimen tiedonsiirron aikana, hän voi lukea ja muuttaa tietoa ennen kuin tieto saavuttaa siihen oikeutetun osapuolen. Symmetrisessä salauksessa on suositeltavaa käyttää nykyaikana AES-salausalgoritmia, jossa salausavaimen pituus on vähintään 128-bittiä. Erittäin luottamuksellisen tiedon salauksessa suositellaan AES-salausalgoritmia käytettäessä avaimen pituudeksi 256-bittiä. [51;52;53.]

Epäsymmetrinen tiedonsalausjärjestelmä hyödyntää avainparia, joista yhtä käytetään tiedon salaukseen ja toista salauksen purkamiseen. Avainpari muodostuu julkisesta avaimesta, joka salaa tiedon ja salassa pidettävästä yksityisestä avaimesta, jonka avulla tiedon salaus puretaan. Julkisen avaimen avulla kuka tahansa voi salata tiedon, mutta salauksen purkaminen onnistuu vain julkisesta avaimesta johdetulla yksityisellä avaimella. Yksityinen avain on siten vain sen omistajan tiedossa eli tietoon oikeutetulla osapuolella on oma ainutlaatuinen salainen avaimensa. Tietoon oikeutetut osapuolet jakavat keskenään vain julkisen avaimen. Jos ulkopuolinen kaappaa tiedonsiirron aikana julkisen avaimen, ei hän kykene purkamaan salausta, koska hänellä ei ole siihen tarvittavaa yksityistä avainta. Lisäksi julkisesta avaimesta ei voida helposti johtaa tietoon oikeutetun osapuolen yksityistä avainta, sillä se on hidasta ja miltei mahdotonta. Salausalgoritmina epäsymmetrisessä salauksessa käytetään DH (Diffie-Hellman), DSA (Digital Signature Algorithm) ja RSA (Rivest, Shamir, Adleman) -algoritmeja joissa avaimen pituutena tulee olla 2048-bittiä. [51;52;53.]

Lisäksi tietoon oikeutettujen osapuolten tulee varmistua, ettei tiedonsiirron aikana kukaan ole muuttanut tietoa, eli tiedon on pysyttävä eheänä. Tämä ratkaistaan käyttämällä tiivistefunktiota, jonka avulla voidaan varmistua tiedon eheydestä sen tiedonsiirron aikana. Tiivistefunktiota käyttämällä lähetettävä tieto myös allekirjoitetaan digitaalisesti lähettäjän toimesta. Lähetettävästä tiedosta lasketaan ensin tiiviste käyttämällä yksisuuntaista funktiota. Lähettäjä koodaa tiivistetyn tiedon yksityisellä avaimellaan, jonka jälkeen tieto lähetetään vastaanottajalle. Tiedon vastaanottaja laskee vastaanotetusta tiedosta myös tiiviste. Lopuksi vastaanottaja vertaa laskettua tiivistettä koodattuun lähettäjän tiivisteeseen, avaamalla koodatun tiivisteeseen lähettäjän julkisella avaimella. Jos vastaanottajan laskema tiiviste on sama kuin lähettäjän salattu tiiviste, on viesti tällöin eheä, muussa tapauksessa viestiä on muokattu sen tiedonsiirron aikana. SHA-1 (Secure Hash Algorithm -1) tiivistefunktio on riittävän vahva varmistamaan tiedon ehey-

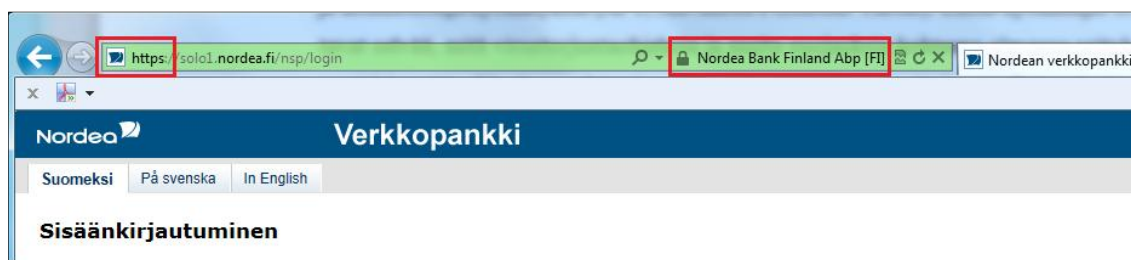
den. Tarvittaessa esimerkiksi verkkopankissa voidaan käyttää myös vahvempia tiiviste-funktioita, jolloin käytössä voi olla SHA-256 tai SHA-384. [51;53.]

4.10 Tiedonsiirron turvallisuuden varmistaminen

Tiedonsiirto käyttäjän tietokoneen Internet-selaimen ja Internetissä sijaitsevan www-palvelimen välillä tapahtuu käyttämällä hyperteaksin siirtoprotokollaa, eli http-protokollaa. Http-protokollaa käytettäessä kaikki tiedonsiirto käyttäjän selaimen ja www-palvelimen välillä tapahtuu selväkielisenä. Tiedon siirtyessä käyttäjän selaimelta ulkoverkkoon, se liikkuu julkisessa verkossa usean eri verkkolaitteen kautta, kunnes saavuttaa määränpäänsä, eli www-palvelimen. Tämän matkan aikana http-protokollalla siirretty tieto on luettavissa ja muokattavissa oikeudettomasti ulkopuolisen toimesta. [54.]

Http-protokollan tietoturvasempi vaihtoehto on https-protokolla, joka salaa käyttäjän selaimen ja ulkoverkossa sijaitsevan www-palvelimen välillä siirrettävän tietoliikenteen. Https-protokolla suojaa tietoliikenteen käyttämällä salausprotokollana TLS-protokollaa, jonka edeltäjä tunnettiin nimellä SSL-protokolla. Salausprotokollan avulla selaimen ja www-palvelimen välillä siirtyvät tiedot on salattu siten, ettei niitä ei voida ulkopuolisen toimesta lukea selväkielisinä. [54.]

Tietoturvan näkökulmasta on tärkeää, että käytössä on aina suojattu https-protokolla, kun selaimeen kirjoitetaan luottamuksellisia tietoja. Sähköpostitilin käyttäminen, tileihin kirjautuminen ja verkkopankissa asiointi ovat kaikki tilanteita, joissa tiedonsiirto tulee tapahtua käyttämällä https-protokollaa. Tietokoneen käyttäjä voi aina halutessaan tarkistaa selaimen osoiteriviltä, onko käytössä http-protokolla vai tiedon suojaava https-protokolla. Käytettävästä selaimesta riippumatta (Chrome, Explorer, Firefox, Safari, Opera) osoiteriville ilmestyy https-alkuinen osoite sekä lukon kuva, kun käytössä on https-protokolla (kuva 4). [54.]



Kuva 4. Https-alkuinen osoite sekä lukon kuva Explorer-selaimen osoiterivillä.

TLS/SSL protokolla hyödyntää sekä symmetristä salausjärjestelmää, että epäsymmetristä salausjärjestelmää. Epäsymmetristä salausta käytetään vain, kun käyttäjä muodostaa yhteyden www-palvelimeen. Yhteyden muodostamisen jälkeen tiedonsalaaminen suoritetaan käyttämällä symmetristä salausta, joka on mahdollistaa nopeamman tiedonsiirron selaimen ja www-palvelimen välillä. [55.]

Selaimen ja www-palvelimen välisen tiedonsiirron suojaamisen lisäksi luottamuksellisissa toimenpiteissä on tärkeää, että selaimeen yhteydessä olevan www-palvelimen identiteetti voidaan todentaa. Palvelimien todentamisessa hyödynnetään digitaalisia sertifikaatteja eli varmenteita, jotka todistavat, että www-sivusto tai palvelu on se, mikä se väittää olevansa. Www-palvelimelle sijoitettavassa sertifikaatissa on salattuun https-yhteyteen vaadittava julkinen salausavain. Sertifikaattien tehtävänä on siten varmistaa, että https-protokollan avulla siirrettävä luottamuksellinen tieto menee tietoon oikeutetulle www-palvelimelle. [54;56.]

Digitaalisia sertifikaatteja www-palvelimille myöntävät kolmannen osapuolen roolissa olevat varmentajat, kuten luotettu virallinen autentikoija VeriSign. Autentikoivan organisaation myöntäessä sertifikaatin, se vakuuttaa sertifikaattiin lisätyllä digitaalisella allekirjoituksella, että kyseessä on esimerkiksi valtuutetun verkkopankin www-palvelin. Internet-selaimissa on sisäänrakennettuna tunnettujen ja luotettujen sertifikaattien myöntämät sertifikaatit. Digitaaliseen sertifikaattiin sisällytetään seuraavat tiedot:

- sertifikaatin omistajan julkinen avain
- informaatio organisaatiosta, jolle sertifikaatti on myönnetty
- informaatio sertifikaatin varmentajasta ja varmentajan digitaalinen allekirjoitus
- päiväys milloin sertifikaatti on myönnetty ja sen voimassaolo-aika
- sertifikaatin sarjanumero [54.]

Https-yhteyden alussa www-palvelin lähettää sertifikaattinsa käyttäjän selaimelle. Selain varoittaa käyttäjää, mikäli https-yhteyttä muodostetaan www-palvelimelle, jonka sertifikaatti ei ole myönnetty luotettavalta varmentajalta tai sertifikaattiin liittyy muita ongelmia. Jos www-palvelimen sertifikaatti on luotettu, käyttäjän selain luo kertakäyttöisen istuntoavaimen, jonka se salaa käyttämällä www-palvelimen sertifikaatin mukana lähetettyä julkista avainta. Tämän johdosta vain www-palvelin voi purkaa istuntoavaimen yksityisellä avaimellaan ja siten selaimen ja www-palvelimen välille muodostuu salattu https-yhteys. Tiedonsiirron salaamiseen käytetään selaimen ja www-palvelimen välillä istuntoavainta, kunnes yhteys palvelimeen katkaistaan. [54;56.]

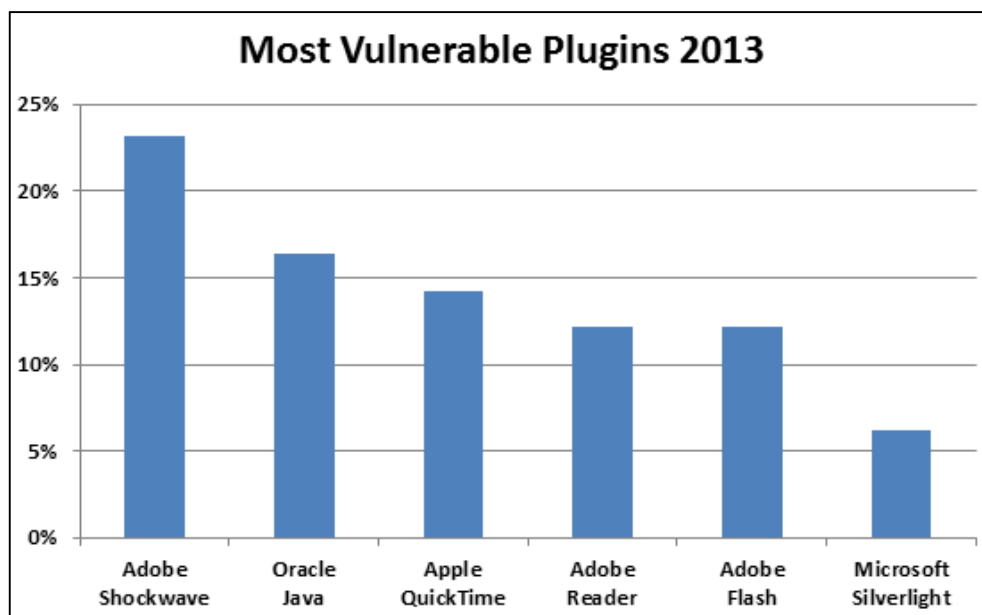
4.11 Internet-selaimen lisäosat

Internet-selaimen lisäosat eli selainlaajennukset ovat ohjelmia, joita käyttäjä voi asentaa tietokoneelle asentamaansa internet-selaimen. Käyttäjät voivat lisäosien avulla muokata selaimestaan omaan käyttöön sopivan kokonaisuuden ja lisätä selaimen lisäominaisuuksia. Lisäosien avulla selaimen toiminnallisuutta voidaan parantaa mutta samalla tietoturvariskit kasvavat, sillä lisäosien sisältämät haavoittuvuudet ovat tietoturvaohjelmien hyväksikäytettävissä. [57;58.]

Säännöllisten tietoturvapäivitysten ansiosta selainten tietoturvaongelmia on onnistuttu hillitsemään. Selaimen jälkeenpäin asennetut lisäosat taas eivät päivitty yhtä tiheästi tai säännöllisesti, kuin selain. Jokainen erillinen selaimen asennettava lisäosa sisältää sille ainutlaatuiset haavoittuvuutensa, joiden korjaavista päivityksistä käyttäjän tulee itse huolehtia. Kaikki selaimen lisäosat eivät osaa hakea automaattisesti päivityksiä, joten käyttäjän on etsittävä ja ladattava päivitykset omatoimisesti. Siten turhat lisäosat, joilla ei ole käyttöä, on hyvä poistaa selaimesta. Lisäosat ovat kolmannen osapuolen kehittämiä ohjelmia, joten käyttäjän selaimen itse asentamat lisäosat eivät päivitty selaimen päivitysten yhteydessä. Huomioitavaa on kuitenkin, että joissain selaimissa tulee valmiina tärkeimmät lisäosat. Tällaisessa tapauksessa selaimen päivitys päivittää myös selaimen mukana valmiina tulleet lisäosat. [57;58.]

Selaimen lisäosia asennettaessa on ensin hyvä varmistua, onko lisäosan asentaminen tarpeellista eli tuleeko käyttäjä tarvitsemaan lisäosaa ja sen toimintoja selaimessa. Jos lisäosa nähdään tarpeelliseksi, asennettava lisäosa tulee ladata tunnetulta ja luotettavalta

sivustolta eli valmistajan sivulta. Esimerkiksi Flash-multimedialaajennus tulee aina ladata Adoben sivuilta. Adobe on kehittänyt kyseisen videoiden katseluun suunnitellun multimedialaajennuksen. On tärkeää asentaa lisäosat aina luotettavasta lähteestä koska muualta asennettava lisäosa voi olla haittaohjelma, joka vaikuttaa haitallisesti selaimen toimintaan. Lisäosan asentamisen jälkeen käyttäjän tulee huolehtia, että lisäosa päivitetään säännöllisesti. [58.]



Kuva 5. Haavoittuvimmat selaimen lisäosat vuoden 2013 aikana. [59.]

4.12 Sähköpostin turvallisuus

Sähköpostin käyttäminen on osa organisaatioiden päivittäistä toimintaa. Sähköpostia käytettäessä on hyvä tunnistaa sen käyttöön liittyvät tietoturvariskit. Oletuksena sähköpostiviestit kulkevat julkisessa verkossa eli Internetissä salaamattomana ja viestien avulla voidaan tuoda käyttäjien tietokoneelle haitallisia tiedostoja. Sähköpostin käyttö vaatii tämän johdosta käyttäjiltä tietoa, miten tunnistaa haitalliset sähköpostiviestit sekä miten suojata lähetettävät viestit.

Organisaatioon saapuviin sähköpostiviesteihin tulee suhtautua varauksella, koska sähköpostia voidaan käyttää välillisesti tartuttamaan haittaohjelmia organisaatioiden tietokoneisiin. Sähköpostiviestit voivat sisältää linkkejä phishing-sivustoille ja viestien liitteinä voidaan lähettää haittaohjelmia. Ennen kuin sähköpostiviestin turvallisuuteen voi luottaa, on hyvä toimia seuraavien vaiheiden mukaisesti:

- Varmista että tietokoneessa on ajan tasalla oleva virustorjuntaohjelma. Virustorjuntaohjelmassa tulisi myös olla ominaisuus, jonka avulla voi tarkistaa sähköpostiviestien liitteet.
- Sähköpostiviestin lähettäjän osoite tulee tarkistaa ja varmistua siitä, että tunnet henkilön tai organisaation, joka viestin on lähettänyt. Tuntematon lähettäjä tai osoite ei välttämättä merkitse vaarallista viestiä mutta tällaisen viestin avaamisessa tulee noudattaa varovaisuutta.
- Viestin aiherivi on hyvä tarkistaa epäilyttävän kielenkäytön varalta. Esimerkiksi epäselvä kieli ja liitteen avaamisen tai linkin avaamisen kehoitus aiherivillä viestivät vaarasta. Virukset voivat tekeytyä eli matkia kelpollisia sähköpostiosoitteita, jolloin epäilyttävä aiherivi osoittaa viestin olevan petollinen. Linkkien avaaminen voi johtaa saastuneille verkkosivuille, joista tietokoneelle ladataan haittaohjelma.
- Jos sähköpostiviesti sisältää liitteen, tarkista liite tietokoneessa olevalla virustorjuntaohjelmistolla. Jos liitteenä on suoritustiedosto, jota et ole odottanut saavasi, viesti on tällöin hyvä poistaa avaamatta siinä olevaa liitettä. PDF-liitetiedostojen avaaminen on myös vaarallista, jos tietokoneen Adobe- reader –apuohjelma ei ole ajan tasalla.
- Jos viesti on saapunut tuntemaltasi henkilöltä mutta epäilet sen olevan huijausta, lähetä tuntemallesi henkilölle sähköpostiviesti ja varmista viestin kelpoisuus. [60;61.]

Lisäksi sähköpostin efektiivinen tietoturva edellyttää toteutuakseen, että muodostetaan salattu yhteys palveluntarjoajan sähköpostipalvelimeen ja lähetettävät ja tallennettavat sähköpostiviestit salataan. Yhteyden salaamiseen käyttäjän tietokoneen ja palveluntarjoajan sähköpostipalvelimen välillä käytetään TLS/SSL-salausta. Jos sähköpostin lukemiseen käytetään selainpohjaista asiakasohjelmaa, tulee selaimen osoiterivillä olevan www-osoitteen alkaa https-protokollalla. Tällöin yhteys sähköpostipalvelimen ja selaimen välillä todennetaan ja salataan käyttämällä TLS/SSL-salausta. Käytettäessä työpöytäsovellusta sähköpostin lukemiseen, tulee TLS/SSL-salaus asettaa käyttäjän tiliasetuksista. [62.]

Lähetettävät sähköpostiviestit voidaan salata käyttämällä OpenPGP-sähköpostiviestien salausprotokollaa. OpenPGP käyttää salauksessa symmetristä- ja epäsymmetristä salausta. Sähköpostiviesti salataan käyttämällä kertakäyttöistä symmetristä avainta, joka on

pituudeltaan merkittävästi lyhyempi, kuin julkinen avain. Kertakäyttöinen symmetrinen avain mahdollistaa nopeamman salausprosessin. Kertakäyttöinen avain liitetään viestin mukaan ja salataan käyttämällä viestin vastaanottajan julkista avainta. Viestin vastaanottaja purkaa kertakäyttöisen symmetrisen avaimen salauksen käyttämällä omaa salaista avaintaan. Tämän jälkeen hän voi purkaa kertakäyttöistä avainta hyödyntämällä sähköpostiviestin salauksen ja lukea viestin selväkielisenä. [62.]

4.13 Langattomien verkkojen turvallinen käyttö

Julkiset langattomat verkot mahdollistavat verkkoyhteydet myös työmatkan aikana esimerkiksi hotelleissa, lentoasemilla ja kahviloissa. Langaton verkko tarjoaa kantoalueen, joka mahdollistaa jaetun pääsyn Internetiin. Kaikki langattoman verkon kantoalueen sisällä olevat langatonta verkkokorttia tukevat tietokoneet voidaan siten liittää verkkoon. [63.]

Langattoman verkon tarjoajat ovat useimmissa tapauksissa mahdollistaneet langattoman verkon nopean ja helpon käytön asiakkailleen, mikä tarkoittaa esimerkiksi salauksen puuttumista. Langattomissa verkoissa tieto kulkee ilman halki radiosignaalien välityksellä ja kuka tahansa voi kaapata signaalit tähän tarkoitukseen suunnitellulla työkalulla. Salaamaton langaton tietoliikenne voidaan siten helposti signaalin kaappauksen jälkeen lukea, oli kyseessä sitten käyttäjätunnukset tai sähköpostiviestit. [63.]

Julkisen langattoman verkon käyttäminen edellyttää käyttäjältä tietoturvallisuuden tuntemusta, jotta verkon käyttöön saataisiin lisäturvaa. Ensin on hyvä varmistua, että yhteys muodostetaan oikeaan langattomaan verkkoon esimerkiksi hotellissa, eikä tietojen kaappaamiseen suunniteltuun verkkoon. Hotelli voi esimerkiksi antaa salasanan, joka vaaditaan yhteyden muodostamiseen langattomaan verkkoon. Web-sivuja selatessa tulee käyttää aina salattua yhteyttä, jonka voi varmistaa selaimen osoiterivin https-alkuisesta osoitteesta. Tarvittaessa voidaan käyttää myös VPN-sovellusta salaamaan tiedonsiirto. Kirjautuminen sähköpostitileihin ja sähköpostiviestien luku tulee suorittaa käyttämällä salattua https-yhteyttä, jos sähköpostiohjelma on web-pohjainen. Jos sähköpostiviestit luetaan työpöytäsovelluksella, POP3-, IMAP-, SMTP-tileistä tulee ottaa käyttöön salaus. Tietokoneen langaton verkkokortti kytketään aina lopuksi pois käytöstä, kun sitä ei enää käytetä. [64;65.]

Myös yksityisiä langattomia verkkoja uhkaavat samankaltaiset vaarat kuin avoimia julkisia langattomia verkkoja. Ulkopuolinen voi kaapata yrityksen yksityistä langatonta tietoliikennettä ja lukea salaamattoman tiedon. Yrityksen langattomiin verkkoihin voidaan turvallisesti liittyä, kun niissä käytetään asianmukaista salausta. WPA2-protokollaa käyttämällä voidaan salata kaikki langaton tietoliikenne luotettavan varmasti yrityksen yksityisissä langattomissa verkoissa. [65.]

5 Pilvipalvelut

5.1 Pilvipalvelun määritelmä

Pilvipalvelut (cloud computing) tarkoittavat käyttöön suhteutuvia, internetissä käytettäviä tietotekniikkaratkaisuja, kuten ohjelmistoja, palveluita, levykapasiteettia ja laskentatehoa. Pilvipalveluiden avulla voidaan korvata tai täydentää organisaation omia ydinjärjestelmiä. Palveluiden veloittaminen asiakkaalta suoritetaan tietoliikennekapasiteetin ja ohjelmistojen käytön mukaan. Tämän johdosta pilvipalveluiden tarjoama joustavuus ja kustannustehokkuus johtavat niiden merkittävään yleistymiseen. [1, s.26.]

5.2 Pilvipalveluntarjoajan toimenpiteet tietoturvan varmistamiseksi

Pilvipalveluita käytettäessä yritys siirtää tietojaan yrityksen oman verkon ja hallinnan ulkopuolelle. Tämä on aiheuttanut useimmissa tietohallinto- ja tietoturvasiantuntijoissa huolen yritysten tietoturvallisuudesta ja pakottanut organisaatiot miettimään tietoturvakäytäntöjään ja sopimustekstiensä sisältöjä. Pilvipalveluihin liittyvät keskeisimmät kysymykset tietoturvan näkökulmasta, joita sopimuksia tehdessä tulisi selvittää, ovat seuraavat:

- missä tietoja säilytetään?
- miten tiedot suojataan?
- kenellä on oikeudet käsitellä tietoja ja kuinka niiden käyttöä valvotaan?
- täyttääkö palvelujen tietoturva asiakkaan vaatimukset?
- onko riskianalyysit laadittu?
- onko sopimuksissa huomioitu riittävässä määrin tietoturva-asiat?
- mitä mahdollisuuksia on siirtyä pois käyttöön otetusta palvelusta? [1, s.26.]

Asiakkaalle pilvipalveluissa tarjottu tekninen ympäristö suojataan tietoturvaohjelmilla käyttämällä useita tietoliikenne- ja palvelintekniikan menetelmiä. Pilvipalvelukoneistoa suojaa palveluntarjoajan omistama ja ylläpitämä palomuuuri sekä tunkeutujan havaitsemisjärjestelmä. Tunkeutujan havaitsemisjärjestelmästä käytetään termiä Intrusion Detection System (IDS) tai Intrusion Detection and Prevention System (IDPS). IDS/IDPS-järjestelmä, joka voi olla erillinen laitteisto tai palvelimessa oleva ohjelma, reagoi hyökkäystilanteessa katkaisemalla havaitun hyökkääjän yhteydet. [66, s.93.]

Pilvipalveluiden käyttäjämäärät ovat suuria, mikä tekee niistä mielenkiintoisia kohteita yritys- tai muita salaisuuksia etsiville ulkopuolisille. Tieto tulee suojata myös sisäisiltä uhkilta eli pilvipalveluntarjoajan omalta henkilökunnalta sekä verkostokumppaneilta. Koska asiakkaan pilvipalveluun siirrettävät tiedot salataan, ei ulkopuolinen hyökkääjä onnistu lukemaan tietoja, vaikka hän pääsisikin tunkeutumaan pilvipalvelun tietoihin. Asiakas tarvitsee tiedon salaamiseen tarkoitetun ohjelman ja menettelyn salaustavaimien tallentamiseen. Salaustavaimien tulisi olla vain asiakkaan tiedossa, joten usein pilvipalveluntarjoaja ei salaa tietoja asiakkaan puolesta. Lisäksi useimmat palveluntarjoajat varmentavat asiakkaidensa tiedot tallentamalla ne kolminkertaisesti. Esimerkiksi kahden tallennuspaikan ongelmat eivät johda katastrofiin, sillä asiakkaan hävinnyt tai tuhoutunut tieto voidaan palauttaa kolmannesta tallennuspaikasta. Pilvipalveluntarjoajan tulisi myös kyetä suorittamaan tiedon hävittäminen aukottomasti jos yritys haluaa hävittää palveluun tallentamansa tiedot. [66, s.93; 67 s.110.]

Lisäksi pilvipalvelukoneiston palvelimia kovennetaan, eli palvelimista poistetaan kaikki järjestelmäpalvelut, jotka eivät ole välttämättömiä. Hyökkääjät voivat hyväksikäyttää tarpeettomien järjestelmäpalveluiden UDP/TCP-portteja päästäkseen kiinni pilvipalveluiden tietoihin tai käyttäjätunnuksiin. Koventamisen ansiosta palvelimen hyökkäysvektori saadaan pieneksi, jolloin verkossa olevalle hyökkääjälle palvelin on vähemmän näkyvä. [66, s.93-94.]

Pilvipalveluissa tietoturvan vastuut siirtyvät asiakkaalta palveluntarjoajalle. Keskimääräinen kotikäyttäjä on asiakas, joka hyötyy pilvitoimintamallin lisäämästä tietoturvasta. Yrityksissä on kuitenkin tehty panostuksia tietoturvallisuuden suhteen. Tämän johdosta

tietoturvan parantamiseen pilvipalvelun kautta ei ole välttämättä tarvetta tai taloudellisia kannusteita. [66, s.94.]

5.3 Pilvipalveluiden turvallisuus yrityskäyttäjän näkökulmasta

Yrityksen tulisi ottaa huomioon tietoturvaan liittyvät riskit jos yritys harkitsee pilvipalveluiden käyttöä tai käyttää niitä. Ulkoisten pilvipalveluiden osalta on selvitetty, millaisia tietoturvaan liittyviä turvallisuusriskejä pilvipalveluiden käyttöön liittyy. Ensimmäisenä riskinä voidaan pitää ulkopuolisten henkilöiden, palveluntarjoajan oman henkilöstön tai palveluntarjoajan mahdollisten kumppaneiden pääsyä yrityksen tietoihin. Palveluntarjoajan omalla henkilöstöllä on pääsy pilvipalvelulaitteistoon ja sen tietoliikenteeseen. Palveluntarjoajan henkilöstö voi olla tietoturvauhka tietoisesti tai tiedostamattaan. Henkilöstön joukosta löytyvän yksilön intressit voivat johtaa tahallisiin väärinkäytöksiin tai tietoturva voi vaarantua henkilöstön tietämättömyyden tai huolimattomuuden seurauksena. Esimerkkinä ihmisen erehtyväisyydestä on tapaus vuodelta 2008, jolloin Flexiscalen työntekijä poisti muutostöiden yhteydessä vahingossa osan asiakkaiden pilvipalveluun tallentamat tiedot. Lisäksi palvelu oli poissa toiminnasta useamman päivän eli palvelun käytettävyys asiakkaille estyi kyseisen vahingon seurauksena. [67, s.104.]

Vastuu tallennetusta tiedosta sekä tallennetun tiedon sijainti pilvipalveluissa tulee myös ottaa huomioon yhtenä turvallisuusriskinä. Yrityksellä on edelleen vastuu huolehtia tietojensa säilytyksen turvallisuudesta ja luotettavuudesta eli pilvipalveluiden käyttäminen ei vapauta yritystä näistä vastuista. Kartoitukset pilvipalveluntarjoajan tiloihin voivat kuitenkin olla mahdottomia toteuttaa. Asiakkaalla ei ole pääsyä pilvipalveluntarjoajan tiloihin ja palvelua tuottavasta infrastruktuurista ei anneta tarkempaa tietoa. Koska asiakkaan ei anneta tutustua paikan päällä pilvikoneistoon tai palveluntarjoajan henkilöstöön, luottamus pyritään rakentamaan muulla tavoin. On myös mahdotonta selvittää, missä tiedot sijaitsevat ja miten hyvin tietojen turvallisuudesta huolehditaan. Tiedot voivat sijaita esimerkiksi eri maassa, jolloin tulisi huomioida maakohtaiset erot tietosuojalaissa ja muussa tietoliikenteeseen vaikuttavassa sääntelyssä. Tämän johdosta yrityksen on vaikea arvioida palveluntarjoajan toimintaan liittyvät riskit sekä miten se on varautunut niihin. [67, s.105-111.]

Pilvipalveluntarjoajan tulee pystyä erottamaan yrityksen tiedot muiden pilvipalveluissa olevien yritysten tiedoista. Pilvipalveluntarjoajan tulee kyetä takaamaan yritykselle,

etteivät toiset palveluntarjoajan asiakkaat pääse yrityksen tietoihin käsiksi. Lisäksi tulisi varmistaa, etteivät turvatoimina käytetyt toimenpiteet, kuten salaus hidasta liiaksi palvelua. [67, s.105-111.]

Yrityksen on selvitettävä, miten pilvipalveluntarjoaja on varautunut odottamattomiin ongelmiin ja virheistä toipumiseen. Yrityksen tulee selvittää, miten ongelmatilanteista tiedotetaan asiakkaalle eli yritykselle, sekä miten kauan pilvipalveluntarjoajan poikkeustilanteesta palautuminen kestää normaaliin tilanteeseen. [67, s.105-111.]

Yrityksen tulee myös selvittää, miten pilvipalveluntarjoaja kykenee selvittämään rikollisen tai muuten sopimattoman toiminnan. Myös tällaisiin tilanteisiin liittyvät vastuukysymykset tulee selvittää pilvipalveluntarjoajan kanssa. Pilvipalveluntarjoajan kykyvyys rikollisen toiminnan tutkinnan suorittamiseen sekä siihen liittyvät vastuukysymykset on myös selvitettävä etukäteen palveluntarjoajan kanssa. Jälkikäteen vastuukysymysten selvittäminen voi olla hankalaa. [67, s.105-111.]

6 Käyttäjän rooli

Edellisissä luvuissa esiteltiin teknisiä käytäntöjä, joiden avulla voidaan suojata tietokoneita tietoturvauhilta. Teknisen suojauksen lisäksi on tärkeää, että tietokoneen käyttäjät ovat valveutuneita ja tunnollisia tietoturvan suhteen. Voidaankin sanoa, että tietokoneiden käyttäjien rooli on kiistämättä tietoturvan tärkein tekijä.

6.1 Yrityksen tietoturvakysely

Opinnäytetyön osana suoritettiin toimeksiantajayritykselle tietoturvakysely. Kyselyn tavoitteena oli kartoittaa yrityksen henkilöstön tuntemusta tietokoneisiin kohdistuviin tietoturvauxhiin. Kysymyksissä organisaatioon kohdistettiin ulkoisia sekä sisäisiä tietoturvauxhia. Tietoturva kysymykset löytyvät tämän opinnäytetyön liitteestä yksi (liite 1) ja oikeat vastaukset liitteestä kaksi (liite 2).

Kysely toteutettiin jakamalla yrityksessä työskenteleville henkilöille kysymyslomakkeet, joihin he vastasivat itsenäisesti. Erityistä teknistä osaamista ei vaadittu kysymysten ymmärtämiseen eli kysely oli suunnattu peruskäyttäjille. Kysymykset laadittiin si-

ten, että niihin voisi vastata kuka tahansa henkilö, joka käyttää tietotekniikkaa työssään. Tähän ratkaisuun päädyttiin sen johdosta, että kysely voitaisiin toistaa mille tahansa yritykselle, jossa työntekijät käyttävät tietotekniikkaa työnsä suorittamiseen. Kysymyksiin annettiin valmiit vaihtoehdot, joista vastaajien tuli valita mielestään sopivin vaihtoehto. Ennen varsinaista kysymyslomakkeiden jakoa yrityksen henkilöstölle, kysymysten toimivuus testattiin ulkopuolisilla henkilöillä, jonka jälkeen niihin tehtiin tarvittavia muutoksia.

Kysymyksissä esiintyvät tietoturvaohat käsittelivät arkipäivän tilanteita, joissa yrityksen tietoturva on uhattuna, joko ulkopuolisen hyökkääjän toimesta tai yrityksen työntekijän tietämättömyyden johdosta. Uhkaavat tilanteet syntyvät usein käyttäjien tietämättömyydestä, jota hyökkääjät käyttävät hyväkseen esimerkiksi lähettämällä huijausviestejä sähköpostin välityksellä. Äärimmäisissä tapauksissa myös käyttäjien välinpitämättömyys ja tietoturvan laiminlyönti voivat olla vakava uhka yrityksen tietoturvalle.

Lomakkeen kysymykset laadittiin edellä kuvattujen perustelujen pohjalta. Ensin henkilöstöltä kysyttiin salasanoista. Kysymyksessä tuli valita uudelle työntekijälle salasana annetuista vaihtoehdoista, joista yksi salasana vaihtoehto oli tietoturvan kannalta vahva. Loput salasana vaihtoehdot olivat heikkoja, kuten suoria numero- tai kirjainyhdistelmiä. Kysymyksen pohjalta voitiin tutkia, ymmärtääkö henkilöstö valita tietoturvan kannalta riittävän kompleksisen eli vahvan salasanan. Kysymys lomakkeen myöhemmässä vaiheessa tiedusteltiin, miten henkilöstö muistaisi lukuisat eri salasanat tietokoneisiin ja verkkopalveluihin. Tarkoituksena oli selvittää, käytettäisiinkö esimerkiksi salasanojen säilytysohjelmaa vai samoja salasanoja kaikissa verkkopalveluissa, jotta salasanojen muistaminen olisi helpompaa.

Seuraavaksi tutkittiin tietokoneen fyysiseen turvallisuuteen suhtautumista. Kysymyksessä kannettava tietokone oli jäänyt yrityksen logolla varustetun auton takapenkille, jonka työntekijä huomasi ajaessaan autolla kauppaan. Kysymyksen tavoitteena oli selvittää, jättävätkö vastaajat kannettavan tietokoneen autoon vai ottavatko he sen mukanaan kauppaan.

Tämän jälkeen kyselyn tärkeimpänä osana tutkittiin kahdella kysymyksellä henkilöstön reagointia huijausviesteihin. Ensimmäisessä kysymyksessä ylläpito pyytää käyttäjää

asentamaan tietokoneeseen käyttöjärjestelmän kriittisen haavoittuvuuden korjaavan tietoturvapäivityksen, jonka latauslinkki löytyy viestistä. Toisessa kysymyksessä tietohallinto ilmoittaa sähköpostiviestillä, että käyttäjän sähköpostitili on kaapattu ja tietohallinnolle tulisi tämän perusteella luovuttaa käyttäjän sähköpostitilin salasana. Näissä kahdessa kysymyksessä on tärkeätä huomata, että viestien sisältö voi sisältää henkilöstölle täysin vierasta teknistä kieltä. Tilanne on silti realistinen, sillä tällä tavalla hyökkääjät toimivat todellisuudessaakin. Tärkeintä oli tutkia ymmärretäänkö yrityksessä, että sähköpostiviestien linkkien kautta ei ladata päivityksiä tai kysellä salasanvoja, vaikka lähettäjänä olisikin luotettava taho.

Henkilöstön mielipidettä kysyttiin myös siitä, miten työntekijä voisi vaikuttaa toiminnallaan tietoturvan toteutumiseen. Tämä kysymys kartoitti sitä, että henkilöstö ymmärtäisi työntekijän roolin tietoturvan edistämiseksi ja että sitä ei voida korvata teknisesti esimerkiksi virustorjuntaohjelmistolla. Kysymyksen tavoitteena oli myös tutkia, että työntekijää osataan ohjata toimimaan esimerkillisellä tavalla tietoturvaa edistäen.

Kysymyslomakkeen yhdessä kysymyksessä pyydettiin henkilöstöä valitsemaan parhaiten nykyaikaisen haittaohjelman luonnetta kuvaava vaihtoehto. Kysymyksessä selvitettiin lyhyesti, mitä haittaohjelmalla tarkoitetaan, jotta vastaajat ymmärtäisivät kysymyksen. Tarkoituksena oli selvittää, miten vakavana uhkana henkilöstö ymmärtää haittaohjelmat.

Kyselyssä tuli huomioida myös yleisesti käytössä olevat USB-muistitikut, joiden avulla on onnistuttu saastuttamaan jopa ydinvoimaloiden järjestelmiä. USB-muistitikkuä käsittelevässä kysymyksessä oli kyseessä yrityksen pihalle hylätty muistitikku. Kysymyksen avulla saatiin tietoa henkilöstön toimintamalleista tällaisessa tilanteessa.

Kysymyslomakkeen viimeinen kysymys koostui useammasta kohdasta. Jokainen kohta oli oma väittämänsä, johon vastaajien tuli vastata, ovatko he samaa vai eri mieltä väittämän kanssa. Väittämät käsittelivät samoja asioita, kuin aiemmin esitetyt kysymykset ja niiden oli tarkoitus varmistaa vastaajien tietoturva osaaminen.

6.2 Kyselyn tavoitteet

Yrityksen henkilöstölle jaetun tietoturvakyselyn tavoitteena oli havainnollistaa henkilöstön toimintamalleja erilaisissa tietoturvaa uhkaavissa tilanteissa. Tulosten perusteella voitiin arvioida, miten valveutuneita työntekijät ovat kohdatessaan erilaisia tietoturva-uhkia. Tärkeimpänä tavoitteena oli löytää tietoturvalle riskialttiit henkilöstön toimintamallit, jotka edesauttavat yrityksen tietoturvauhkien, kuten kohdistettujen hyökkäyksien toteutumista. On hyvä muistaa se tosiasia, että yhdenkin työntekijän vääränlainen toimintamalli voi mahdollistaa koko yritystä koskevan tietoturvaloukkauksen toteutumisen.

6.3 Kyselyn tulosten analysointi

Kyselyn tulosten perusteella voitiin todeta, että henkilöstö ymmärsi kompleksien, eli tietoturvan kannalta riittävän vahvojen salasanojen turvallisuuden ja tunnisti heikot salasanat. Yksikään vastaaja ei erehtynyt valitsemaan salasanaksi heikkoa salasanaa, eli numero- tai kirjainyhdistelmää, kuten *qwerty* tai *1234567890*. Myös käyttäjätunnuksen hyödyntämistä takaperin salasanana vastustettiin. Parhaaksi vaihtoehdoksi lukuisten eri salasanojen muistamiseen vastaajat valitsivat salasanojen säilytysohjelman. Tältä osin vastaajat ymmärsivät, että salasanoja ei tarvitse muistaa ulkoa.

Kysymyksissä tutkittiin henkilöstön reaktiota USB-muistitikkuun, joka löytyy yrityksen pihalta hylättynä. Tällaiseen hylättyyn muistitikkuun liittyy tietoturvariski, koska se voi sisältää haittaohjelman, joka voi saastuttaa yrityksen sisäverkon. Yksi vastaajista ei olisi kieltänyt liittämästä USB-muistitikkuja yrityksen työasemiin. USB-muistitikussa mahdollisesti ollut haittaohjelma olisi pahimmassa tapauksessa saastuttanut yrityksen työaseman ja edennyt edelleen uusiin sisäverkon tietokoneisiin.

Yksikään vastaajista ei mennyt avaamaan tuntemattoman sähköpostin liitteenä tulevia tiedostoja, vaikka ne vaikuttivat hyödyllisiltäkin. Siten voitiin tehdä päätelmä, että tällaisten liitetiedostojen vaarallisuus tietokoneille ymmärrettiin yrityksessä erinomaisesti. Tämä estää osaltaan haittaohjelmien asentamisen työasemille. Lisäksi kaikki vastaajat ymmärsivät tietokoneen lukitsemisen tärkeyden, jos työasemalta poistutaan esimerkiksi tauon ajaksi. Näin varmistetaan luottamuksellisten tietojen tai tietokoneen oikeudeton käyttö. Tuntemattomien sähköpostiviestien liitetiedostojen vaarallisuuden tunteminen ja

työaseman lukitseminen ovat tietoturvallisuuden perusasioita, jotka jokaisen tietokoneen käyttäjän tulisi tietää.

Kyselyn perusteella merkittävin tietoturvauhka muodostuu yritykselle käyttäjän manipuloinnista ja phishing-yrityksistä. Henkilöstö oli yhtä mieltä siitä, että ei ole normaalia toimintaa tiedustella sähköpostilla työntekijöiden salasanoja. Osa henkilöstöstä erehtyi kuitenkin lataamaan sähköpostilinkin kautta päivityksiä tai antamaan salasanaan, jos viestin lähettäjänä olisi ollut tietohallinto tai ylläpito. Luotettavan lähettäjän lisäksi huijausviestit oli laadittu käyttämällä teknistä sanastoa, joka osaltaan erehdytti tarkoituksenmukaisesti vastaajia. Yksi vastaajista ymmärsi, että viestit olivat huijausta, eikä reagoinut viesteihin mitenkään. Tästä voidaan myös tehdä päätelmä, että myös suurissa yrityksissä on aina henkilöstöä, jotka voivat erehtyä uskomaan taitavasti laadittuja huijausviestejä. Tietoturva huijausviestien aiheena on myös tehokas manipuloinnin väline. Mitä kriittisemmältä viesti näyttää, sitä varmemmin joku erehtyy tulemaan huijatuksi.

Tietokoneen fyysistä turvallisuutta koskevassa kysymyksessä yrityksen työntekijä oli huomannut kauppaan ajaessaan, että yrityksen kannettava tietokone oli jäänyt auton takapenkille. Vastaajat olisivat jättäneet kannettavan tietokoneen autoon lukkojen taakse, joko takakonttiin tai takapenkille. Tietoturvalisin vaihtoehto olisi kuitenkin ottaa kannettava tietokone kauppaan mukaan. Murtautuminen autoon on aina mahdollista ja kannettava tietokone on helppo varastaa. Rikollisia kiinnostaa kaikki irtaimisto, mitä he mukaansa saavat, oli se sitten lukkojen takana takakontissa tai takapenkillä.

Kaikki vastaajat ymmärsivät työntekijän roolin tärkeyden tietoturvalle. Vastaajat olivat eri mieltä väittämän kanssa, jonka mukaan työntekijä ei voisi vaikuttaa tietoturvaan toiminnallaan. Lisäksi vastaajat ymmärsivät, että tekniset ratkaisut kuten salasanat ja virustorjuntaohjelmistot eivät korvaa käyttäjän varovaisuutta.

7 Yhteenveto

Toimiva ja efektiivinen tietokoneiden tietoturva rakentuu monesta eri osa-alueesta. Tietoturvaan liittyvässä opinnäytetyössä voisi tutkia tarkasti jotain yksittäistä tietoturvaan vaikuttavaa tekijää, kuten palomuurilaitteita tai haittaohjelmien torjuntaohjelmistojä. Tällaisessa tapauksessa aihe rajautuisi suppeaksi mutta syvälliseksi tutkielmaksi, keskit-

tyen tarkasti valittuun osa-alueeseensa. Päätin kuitenkin käsitellä useita eri tekijöitä, jotka vaikuttavat tietokoneiden tietoturvaan, jotta toimeksiantajayritys saisi mahdollisimman hyvän näkemyksen tietokoneiden suojaustoimenpiteistä. Tietoturvasta olisi tullut liian suppea vaikutelma ja mahdollisesti vääärnlainen kuva toimeksiantajalle, jos olisi tutkittu pelkästään esimerkiksi erilaisia virustorjuntaohjelmistoja. Myös oma mielenkiintoni aiheeseen vaikutti osaltaan siihen, että tutkin aihetta laajemmasta näkökulmasta. Tavoitteeni oli selvittää kaikki sellaiset tietokoneiden tietoturvaa tukevat toimenpiteet, joita käyttäjät voisivat omilla toiminnoillaan toteuttaa käytännössä. Lisäksi tutkin toimeksiantajayrityksen tietokoneiden käyttäjien toimintamalleja.

Toisaalta tietoturva on kuitenkin niin laaja, että kaikkea mahdollista siihen liittyvää tietoa ei voida käsitellä yhdessä opinnäytetyössä. Varsinkin edellä mainittu syvälinen tutkiminen vaatii keskittymisen vain yhteen osa-alueeseen. Tällöinkin voi olla, että aihetta joudutaan rajaamaan suppeammaksi. Siten tämän opinnäytetyön tarkoituksena ei ole olla kaiken kattava opas tietoturvaan, vaan lähinnä valistava opinnäytetyö. Opinnäytetyö auttaa ymmärtämään tietoturvauhat ja niiden merkittävimmät torjuntaan tarvittavat suojaavat toimenpiteet ja parhaimmassa tapauksessa motivoi tutkimaan lisää aihetta.

Tutkielmassa esitetyt tietoturvauhat tulevat pysymään luonteeltaan samankaltaisina, vaikkakin ne tulevat kehittymään tekniseltä rakenteeltaan ohjelmistojen ja käyttöjärjestelmien rinnalla. Uhkien kehittymistä taas tulee seurata siinä määrin, että niihin voidaan vastata ajan tasalla olevilla suojaustoimenpiteillä. Tietoturva-uhat kuten haittaohjelmat ja käyttäjien manipulointi eivät varmasti katoa mihinkään, vaan ovat aina läsnä tietoteknisessä ympäristössä. Tekniikka mahdollistaa nykyaikana entistä tehokkaammat torjuntamenetelmät ulkopuolisia hyökkäyksiä vastaan. Asia ei ole kuitenkaan näin yksinkertainen, sillä tekniikalla ei voida yksinomaan ratkaista tietoturvaa. Tietoturvasta 20 prosenttia on tekniikkaa ja 80 prosenttia psykologiaa [68.]. Tärkein vaikuttaja tietoturvan kannalta on siten tietokoneen käyttäjä, joka toiminnallaan edesauttaa hyvän tietoturvan toteutumista. Edes tekniikka, jonka tarkoituksena on paikata ihmisen heikkouksia, ei auta kaikissa tilanteissa, joissa tietokoneen käyttäjä muodostaa itsestään pahimman tietoturvauhan.

Yritykselle suunnatun kyselyn tavoitteena olikin löytää henkilöstön toimintamalleista tietoturvaa uhkaavat toimintamallit. Vaikka nyky-yhteiskunnassa ollaan melko tietoisia

tietojärjestelmiin kohdistuvista uhkista, voi loppukäyttäjän yllättää melko helposti kii-reisenä päivänä esimerkiksi käyttäjän manipuloinnilla. Tämä ilmeni esitettyjen kysy-mysten valossa, koska osa vastaajista asensi huijaus sähköpostien tarjoamia päivityksiä ja luovutti salasanansa keksityn tietohallinnon viestin perusteella. Käyttäjien manipu-lointiin on myös melko vaikea puuttua teknisillä apuvälineillä, koska manipulointi tapa-uksissa ollaan suoraan yhteydessä huijauksen uhriin esimerkiksi puhelimella.

Laatimalla opinnäytetyön tietoturvasta, olen pystynyt sisäistämään paremmin tietoko-neiden tietoturvaan vaikuttavia tekijöitä ja tutustunut erilaisiin näkökulmiin aiheeseen liittyen. Perehtyminen erilaisiin toimenpiteisiin, joiden avulla varustautuminen tietotur-vauhkia vastaan aloitetaan, on opettanut hahmottamaan suojaavien toimenpiteiden laa-ajan skaalan. Oma mielipiteeni on, että osa-alueiden asiantuntijuus vaatii syventymisen vain tiettyyn osa-alueeseen ja käytännön kokemuksen erilaisista vaihtoehdoista.

Mielenkiintoisinta oli huomata aineiston etsinnän yhteydessä, miten erilaisia mielipiteitä tietoturvan ratkaisemiseksi on olemassa. Esimerkiksi virustorjuntaohjelmiston tarpeelli-suus saatettiin kyseenalaistaa, koska jotkin virustorjuntaohjelmistot vievät paljon resurs-seja ja siten saattavat hidastaa tietokoneen toimintaa. Tällaiset toimenpiteet sopivat mie-lestäni vain kokeneille käyttäjille ja esimerkiksi yrityksissä on aina oltava ajan tasalla olevat tietoturvaohjelmistot. Yrityksillä ei myöskään mahdollisesti ole intressejä koulut-taa henkilöstöä siinä mittakaavassa, että esimerkiksi virustorjuntaohjelmistot voitaisiin korvata koulutuksella. Henkilöstön koulutus jossain määrin on kuitenkin tärkeää, jotta henkilöstö osaa tunnistaa tietoturva-uhat ja omat toimintamallit, jotka ovat uhaksi yri-tyksen tietoturvalle.

Tulevaisuuden kannalta tietoturvaan joudutaan kiinnittämään entistä enemmän huomio-ta, koska yhteiskunta tulee olemaan yhä enemmän riippuvainen toimivista tietojärjes-telmistä. Jokaisen yksilön, organisaation ja valtion tulee omalta osaltaan tunnistaa vel-vollisuutensa ja tehdä tarvittavat toimenpiteet tietoturvan toteuttamiseksi. Vain yhdessä vastuullisesti toteutettu tietoturva tulee edistämään Suomen tietoverkkojen turvallista hyödyntämistä niin yksityishenkilöille kuin organisaatioille. Välinpitämätön suhtautu-minen taas johtaa siihen, että saastuneiden järjestelmien osuus kasvaa ja tietojärjestel-mien käyttämisestä tulee entistäkin turvattomampaa.

Lähteet

1. Andreasson, Ari & Koivisto, Juha. 2013. Tietoturvaa toteuttamassa. Helsinki. Tietosanoma Oy
2. Laaksonen, Mika & Nevasalo, Terho & Tomula, Karri. 2006. Yrityksen tietoturvakäsikirja. Helsinki. Edita Publishing Oy
3. Valtionhallinnon tietoturvallisuuden johtoryhmä. 2003. Käyttäjän tietoturvaohje. [Viitattu 9.1.2014.] Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/51027/51024_fi.pdf
4. Eläketurvakeskus. 2010. Asiakirjaturvallisuus. [Viitattu 9.1.2014.] Saatavissa: <http://tyoelakelakipalvelu.etk.fi/se/soveltamisohje/index.php?asiakirjanumero=17390>
5. Järvinen, Petteri. 2012. Arjen tietoturva. Jyväskylä. Docendo
6. Ronald, L. Krutz & Russel, Dean Vines. 2003. Tietoturvasertifikaatti-CIISP. Helsinki. Edita Publishing Oy.
7. CSC – Tieteen tietotekniikan keskus. 2010. Keskeiset käsitteet. [Viitattu 9.1.2014.] Saatavissa: <http://www.tdata.fi/fi/keskeiset-kasitteet>
8. Sanastokeskus TSK.2004. Tiivis tietoturvasanasto. [Viitattu 10.1.2014.] Saatavissa: <http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf>
9. Clearswift. Then enemy within: an emerging threat. 2013. [Viitattu 25.4.2014.] Saatavissa: <http://www.clearswift.com/blog/2013/05/02/enemy-within-emerging-threat>
10. Laitila, T. 2013. Maailman tunnetuin hakkeri: tämä on yrityksen pahin tietoturvauhka. Tietoviikko. [Viitattu 22.1.2014.] Saatavissa: http://www.tietoviikko.fi/kaikki_uutiset/maailman+tunnetuin+hakkeri+tama+on+yritysten+pahin+tietoturvauhka/a939422
11. Pietarién, I. 2004. Käyttäjän manipulointi. Tietotekniikan liitto ry.[Viitattu 22.1.2014.] Saatavissa: http://www.ttlry.fi/viikon_sana/k%C3%A4ytt%C3%A4j%C3%A4n-manipulointi
12. Kaspersky lab. Internet security FAQs. [Viitattu 15.1.2014.] Saatavissa: <http://www.kaspersky.com/internet-security-center/internet-safety/faq>
13. Bodnar, C. 2013 .A Malware Clasification. Kaspersky lab. [Viitattu 26.1.2014.] Saatavissa: <http://blog.kaspersky.com/a-malware-classification/>
14. Veracode. Computer worm. [Viitattu 15.1.2014.] Saatavissa: <http://www.veracode.com/security/computer-worm>
15. Trend Micro. As the worm turns. [Viitattu 16.1.2014.] Saatavissa: <http://www.antivirus.com/security-software/definition/computer-worms/index.html>
16. Kaspersky lab. What is a Trojan? [Viitattu 17.1.2014.] Saatavissa: <http://www.kaspersky.com/internet-security-center/threats/trojans>
17. Trend Micro. Trojan horse or Trojan: It's Not All a Myth. [Viitattu 17.1.2014.] Saatavissa: <http://www.antivirus.com/security-software/definition/trojan-horse/index.html>
18. Isokoski, Janne. 2012. ”Poliisi haittaohjelma” ja sen poistaminen koneelta. IT-Webpalvelut. [Viitattu 16.4.2014.] Saatavissa: <http://it-webpalvelut.com/wp-content/uploads/2012/10/poliisiherja.png>

19. Kilpailu ja kuluttajavirasto. Huijaukset. [Viitattu 27.1.2014.] Saatavissa: <http://www.kuluttajavirasto.fi/fi-FI/huijaukset/tili-ja-luottokorttitietojen-kalastelu/>
20. Taloussanomat. OP-Pohjolan nimissä lähetetty huijausviestejä. 2011.[Viitattu 17.4.2014.] Saatavissa: <http://www.taloussanomat.fi/kotimaa/2011/08/12/op-pohjolan-nimissa-lahetetty-huijausviesteja/201111242/12>
21. Norton. 2006. Pharming on phishing-huijausta kehittyneempi ja vaikeammin havaittava hyökkäysmuoto. [Viitattu 27.1.2014.] Saatavissa: http://securityresponse.symantec.com/fi/fi/norton/library/familyresource/article.jsp?aid=article1_08_06
22. Fisher, D. 2013. What is a Man-in-the-middle Attack? [Viitattu 12.2.2014.] Saatavissa: <http://blog.kaspersky.com/man-in-the-middle-attack/>
23. Järvinen, Petteri. 2009. Digi arkistointi. Jyväskylä. WSOYpro OY.
24. Paananen, Juha. 2005. Tietotekniikan peruskirja. Jyväskylä. Docendo Finland Oy.
25. Suoranta, Lauri. 2008. Levynsalaus turvaa selustan. Tietokone. [Viitattu 28.2.2014.] Saatavissa: http://www.tietokone.fi/artikkelit/levynsalaus_turvaa_selustan
26. Norton. Nortonin tutkimus paljastaa: Mobiililaitteet Euroopassa usein suojaamattomia. 2013. [Viitattu 29.4.2014.] Saatavissa: <http://news.cision.com/fi/pilgrim/r/nortonin-tutkimus-paljastaa--mobiililaitteet-euroopassa-usein-suojaamattomia,c9395444>
27. Kekäläinen, Otto. 2009. Turvallisuus-lehti. [Viitattu 10.3.2014.] Saatavissa: <http://www.valo-cd.fi/oppaat/truecrypt-opas.pdf>
28. Bowen, David. 2013. 6 Tips to Keep Your Home Computer Safe and Secure. Kaspersky lab. [Viitattu 11.3.2014.] Saatavissa: <http://blog.kaspersky.com/6-tips-to-keep-your-home-computer-safe-and-secure/>
29. Bedford, Mike. 2012. How to back up your PC and laptop. PC advisor. [Viitattu 12.3.2014.] Saatavissa: <http://www.pcadvisor.co.uk/how-to/software/3356160/how-backup-your-pc-laptop/>
30. Tietokoneen suojaus ja turvallinen käyttö. Microsoft. [Viitattu 20.2.2014.] Saatavissa: <http://windows.microsoft.com/fi-fi/windows/understanding-security-safe-computing#1TC=windows-7>
31. Bolshakova, M. Tip of the week: How to Schedule Antivirus Databases Update. Kaspersky lab. 2013. [Viitattu 18.2.2014.] Saatavissa: <https://blog.kaspersky.com/tip-of-the-week-how-to-schedule-anti-virus-databases-update/>
32. Update your antivirus software. Microsoft. [Viitattu 18.2.2014.] Saatavissa: <http://windows.microsoft.com/en-us/windows/update-antivirus-software#1TC=windows-7>
33. NetBIOS and special ports blocked. Office Of Information Technology. 2009. [Viitattu 13.5.2014.] Saatavissa: <http://www.oit.uci.edu/security/netbios.html>
34. Goodrich, R. PC Security and the Importance of Patch Update. TopTen Reviews. [Viitattu 18.2.2014.] Saatavissa: <http://anti-virus-software-review.toptenreviews.com/pc-security-and-the-importance-of-patch-updates.html>

35. Lue tietoja Windowsin automaattisista päivityksistä. Microsoft. [Viitattu 18.2.2014.] Saatavissa: <http://windows.microsoft.com/fi-fi/windows/understanding-windows-automatic-updating#1TC=windows-7>
36. Ludlow, D. When Windows XP support ends, here's how to keep your PC secure. Expert reviews. 2014. [Viitattu 18.2.2014.] Saatavissa: <http://www.expertreviews.co.uk/software/1304965/when-windows-xp-support-ends-heres-how-to-keep-your-pc-secure>
37. Dahanayke, Nadeeka. Ten Ways to Improve the Security of a New Computer. 2012.TechCERT. [Viitattu 22.2.2014.] Saatavissa: <http://www.techcert.lk/index.php/en/component/content/article/9-alerts/97-ten-ways-to-improve-the-security-of-a-new-computer->
38. Kent, Jennifer. Steiner, Katie. Ten Ways to Improve the Security of a New Computer. 2012. US-CERT. 2012. [Viitattu 22.2.2014.] Saatavissa: <http://www.us-cert.gov/sites/default/files/publications/TenWaystoImproveNewComputerSecurity.pdf>
39. Chaplin, M. & Creasey, J. CF6.4 Access Control Mechanisms –Password. Information Security Forum. 2011.
40. Hoffman, C. Brute-Force Attacks Explained: How All Encryption is Vulnerable. How-To Geek. 2013. [Viitattu 11.2.2014.] Saatavissa: <http://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable/>
41. Merritt, M. Hyvät ja huonot salasanat. Norton. [Viitattu 11.2.2014.] Saatavissa: <http://fi.norton.com/dos-donts-passwords/article>
42. Worst passwords of 2013. Splashdata. [Viitattu 11.2.2014.] Saatavissa: <http://splashdata.com/press/worstpasswords2013.htm>
43. Järvinen, Petteri. 2011. Hyvällä salasanalla on harvoin merkitystä. [Viitattu: 28.2.2014.] Saatavana: <http://pjarvinen.blogspot.fi/2011/07/hyvalla-salasanalla-on-harvoin.htm>
44. Laakkonen, C. Salasanat talteen turvallisesti. Sofokus. 2013. [viitattu 11.2.2014.] Saatavissa:<http://www.sofokus.com/blogi/salasanat-talteen-turvallisesti/>
45. Tallenna salasanat oikein. Gelo Oy. [Viitattu 11.2.2014.] Saatavissa:<http://www.gelo.fi/tallenna-salasanat-oikein/>
46. Vihjeitä vahvan salasanan luomiseen. Microsoft. [Viitattu 11.2.2014.] Saatavissa: <http://windows.microsoft.com/fi-fi/windows-vista/tips-for-creating-a-strong-password>
47. Keepass Password Safe. [Viitattu 20.2.2014.] Saatavissa: <http://keepass.info/>
48. Rubenking, Neil. Six great password managers. PCMag. 2011. [Viitattu 28.4.2014.] Saatavissa: <http://www.pcmag.com/article2/0,2817,2381432,00.asp>
49. Help prevent malware infection on your pc. Microsoft. [Viitattu 12.2.2014.] Saatavissa: <http://www.microsoft.com/security/portal/mmpc/shared/prevention.aspx>

50. Mikä on käyttäjätilien valvonta ? Microsoft. [Viitattu 12.2.2014.] Saatavissa: <http://windows.microsoft.com/fi-fi/windows/what-is-user-account-control#1TC=windows-7>
51. Introduction to Cryptography. How PGP works. [Viitattu 13.2.2014.] Saatavissa: <http://www.pgpi.org/doc/pgpintro/>
52. Next Generation Encryption. Cisco. 2013. [Viitattu 13.2.2014.] Saatavissa: http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html
53. Salausmenetelmät. Secmeter. [Viitattu 13.2.2014.] Saatavissa: <http://www.secmeter.com/salausmenetelmat.html>
54. Donohue, B. Digital Certificates and HTTPS. Kaspersky lab. 2013. [Viitattu 10.2.2014.] Saatavissa: <http://blog.kaspersky.com/digital-certificates-https/>
55. Hartley, B. How HTTPS Secures Connections: What every Web Dev Should Know. 2013. [Viitattu 19.2.2014.] Saatavissa: <http://blog.hartleybrody.com/https-certificates/>
56. How SSL Works. Symantec. [Viitattu 10.2.2014.] Saatavissa: <http://www.symantec.com/page.jsp?id=how-ssl-works>
57. Moisio, Aleks. Nettiselaimen lisäosa on tietoturvariski. Digitoday. 2008. [Viitattu 22.4.2014.] Saatavissa: <http://www.digitoday.fi/tietoturva/2008/01/16/nettselaimen-lisaosa-on-tietoturvariski/20081430/66>
58. Poor, Mike. Browser security and privacy. SANS. 2011. [Viitattu 22.4.2014.] Saatavissa: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201111_en.pdf
59. Kandek, Wolfgang. Secure your browser before shopping online. Qualys Community. 2013. [Viitattu 22.4.2014.] Saatavissa: <https://community.qualys.com/blogs/laws-of-vulnerabilities/2013/11/27/secure-your-browser-before-shopping-online>
60. Sähköpostiviesteihin luottaminen. Microsoft. [Viitattu 9.3.2014.] Saatavissa: <http://windows.microsoft.com/fi-fi/windows/when-trust-email-message#1TC=windows-7>
61. Kärkkäinen, Henrik. Tietomurtoja sähköpostin voimin –olenko vaarassa? Digitoday. 2010. [Viitattu 9.3.2014.] Saatavissa: <http://www.digitoday.fi/tietoturva/2012/11/06/tietomurtoja-sahkopostin-voimin--olenko-vaarassa/201241468/66>
62. Geier, E. How to Encrypt Your Email. PC World. 2012. [Viitattu 12.2.2014.] Saatavissa: http://www.pcworld.com/article/254338/how_to_encrypt_your_email.html
63. Langattomat Wi-Fi-alueet: yhteydet matkoilla. Norton. [Viitattu 17.3.2014.] Saatavissa: <http://fi.norton.com/travel-hotspot-security/article>
64. Boatman, Kim. Onko turvallista käyttää hotellin ilmaista langatonta Internet-yhteyttä? Norton. 2010. [Viitattu 17.3.2014.] Saatavissa: http://fi.norton.com/yoursecurityresource/detail.jsp?aid=free_wifi
65. Geier, Eric. Here's what an eavesdropper sees when you use an unsecured Wi-fi hotspot. PC World. 2013. [Viitattu 14.3.2014.] Saatavissa:

<http://www.pcworld.com/article/2043095/heres-what-an-eavesdropper-sees-when-you-use-an-unsecured-wi-fi-hotspot.html>

- 66. Heino, Petteri. 2010. Pilvipalvelut. Hämeenlinna. Kariston Kirjapaino Oy
- 67. Salo, Immo. 2010. Cloud computing, palvelut verkossa. Docendo. Jyväskylä.
- 68. Harju, Emmi. Tietoturvasta huolehtiminen on elinehto. Varsinais-Suomen yrittäjä. 2010. [Viitattu 22.4.2014.] Saatavissa: <http://www.y-lehti.fi/arkisto/artikkeli/3192/Tietoturvasta+huolehtiminen+on+elinehto+>

1.

Yrityksen työntekijä miettii tietokoneelleen salasanaa. Minkälaista salasanaa sinä suosittelisit käytettäväksi, jos työntekijän käyttäjätunnus on matti?

- ☐ abc123
- ☐ 1234567890
- ☐ qwerty
- ☐ eqT@R12!
- ☐ Suosittelisin häntä käyttämään salasanaan hänen omaa käyttäjätunnustaan takaperin.
- ☐ password1

2.

Lähdet ostamaan toimistotarvikkeita firman logolla varustetulla autolla ja matkalla kauppaan huomaat, että yrityksen kannettava tietokone on jäänyt näkyville auton takapenkille. Miten toimit tietokoneen kanssa saavuttuasi kaupan pihaan?

- ☐ Siirrän tietokoneen auton lukolliseen takakonttiin, josta varkaat eivät näe sitä.
- ☐ Otan tietokoneen mukaani kauppaan.
- ☐ Jätän tietokoneen takapenkille kun käyn kaupassa, sillä kukaan ei ehdi varastaa sitä.
- ☐ Kaupan läheisyydessä ei näy yhtään varkaalta näyttävää henkilöä. Käyn nopeasti kaupassa ja jätän kannettavan tietokoneen auton takapenkille.

3.

Saat englanninkielisen sähköpostiviestin Ylläpidosta (Helpdesk), eli luotettavalta taholta. Viestissä ilmoitetaan että sinun tulisi asentaa tietokoneellesi välittömästi käyttöjärjestelmän kriittisen haavoittuvuuden korjaava tietoturvapäivitys. Tietoturvapäivityksen latauslinkki löytyy sähköpostiviestin lopusta. Kuinka toimit tässä tapauksessa?

- ☐ Koska päivitykset keskeyttävät aina työnteon, säilytän viestin ja asennan päivityksen myöhemmin iltapäivällä.
- ☐ En reagoi viestiin ja poistan sen.
- ☐ Siirryn latauslinkkiin ja lataan sieltä löytyvän Microsoft päivityksen välittömästi.
- ☐ Viesti vaikuttaa tärkeältä mutta asennan päivityksen huomenna, koska kyseessä voi olla aikaa vievä prosessi.

4.

Haittaohjelma on yleisnimitys ohjelmille (esimerkiksi tietokonevirus), jotka aiheuttavat ei-toivottuja tapahtumia tietokoneessa. Mikä seuraavista vaihtoehdoista kuvaa parhaiten nykyaikaista haittaohjelmaa?

- ☐ Ne ovat nuorten harrastelijoiden kirjoittamia, piloiksi tarkoitettuja ja eivät ole tietokoneille kovin vahingollisia.
- ☐ Työntekijän on helppo havaita työaseman saastuttanut taloudellista hyötyä tavoitteleva haittaohjelma.
- ☐ Ne ovat ammattimaisia ja niillä on tarkoitus saada taloudellista hyötyä.
- ☐ Virustorjuntaohjelmistot tunnistavat ja pysäyttävät kaikki haittaohjelmat.

5.

Työntekijä miettii, miten hän voisi toiminnallaan estää tietokonevirusten ja muiden haittaohjelmien pääsyn yrityksen työasemiin. Minkä neuvon sinä antaisit hänelle?

- ☐ Suojaa työasemasi mahdollisimman vaikealla salasanalla.
- ☐ Katkaise tietokoneestasi virta, aina kun et käytä sitä pitkään aikaan.
- ☐ Työntekijänä et voi vaikuttaa asiaan, se on virustorjuntaohjelmiston tehtävä.
- ☐ Tuntemattoman sähköpostiviestin liitteenä tulevia, hyödyllisiltäkin vaikuttavia tiedostoja ei saa avata.

6.

Työntekijä tuo yritykseen mukanaan USB-muistitikun, jonka hän kertoo löytäneensä aamulla yrityksen pihalta? Hän on liittämässä USB-muistitikkua yhteen yrityksen työasemista, jotta hän näkisi onko siihen tallennettuna mitään. Miten reagoisit tähän?

- ☐ Yrityksen työasemiin on turvallista liittää USB-muistitikkuja, joten en reagoi mitenkään.
- ☐ Pyydän häntä liittämään USB-muistitikun yrityksen työasemaan, joka ei ole kytketty ikinä Internetiin.
- ☐ Muistutan häntä ennen työasemaan liittämistä, kuinka USB-muistitikku poistetaan työasemasta turvallisesti käytön jälkeen.
- ☐ Kiellän työntekijää liittämästä kyseistä USB-muistitikkua mihinkään yrityksen työasemista.

7.

Työsähköpostiisi ilmestyy hyvällä ja sujuvalla suomenkielellä kirjoitettu viesti. Viestin lähettäjänä on tietohallinto, joka ilmoittaa että sähköpostitilisi on kaapatu ja sitä käytetään roskapostin lähetykseen. Viestissä pyydetään vahvistamaan sähköpostitilisi salasana viestissä olevan linkin kautta, jotta sinulle voidaan tehdä uusi tili ja käyttäjätunnus. Miten toimitisit tässä tilanteessa?

- ☐ Poistan viestin, enkä reagoi siihen.
- ☐ Toimin vastuullisesti. Siirryn välittömästi sähköpostin osoittamaan linkkiin ja syötän salasanani sitä kysyttäessä.
- ☐ Kiireisen aikataulun vuoksi toimin viestissä annettujen ohjeiden mukaisesti vasta iltopäivällä.
- ☐ En reagoi viestiin heti, koska työt keskeytyisivät. Seuraavana päivänä saan saman sähköpostiviestin ja nyt toimin, kuten viestissä käsketään.

8.

Yrityksen työntekijänä tarkastelet tietokoneellasi luottamuksellista dokumenttia. Päättät pitää tauon ja poistua työpisteeltäsi. Minkä toimenpiteen teet ennen lähtöäsi?

- ☐ Tallennan dokumentin ja Lukitsen työaseman esimerkiksi ctrl+alt+del näppäinyhdistelmän avulla.
- ☐ Irrotan Ethernet tietoliikennekaapelin, jotta tietokoneelle ei sillä välin tulisi tietokoneviruksia.
- ☐ Minun ei tarvitse tehdä mitään. Dokumentti jää tietokoneen näytölle sopivasti odottamaan paluutani tauolta.
- ☐ Tallennan dokumentin, koska tauon aikana voi tulla sähkökatko.

9.

Mikä on sinun mielestäsi paras tapa muistaa/säilyttää lukuisat eri salasanat tietokoneisiin ja verkkopalveluihin?

- ☐ Käytän samaa salasanaa kaikissa tietokoneissa ja verkkopalveluissa.
- ☐ Kirjoitan tietokoneen salasanat paperille ja kiinnitän paperin tietokoneen näppäimistön pohjaan.
- ☐ Käytän salasanojen säilytysohjelmaa.
- ☐ Käytän mahdollisimman yksinkertaisia ja selkokielisiä salasanoja, kuten *salasana*, *auto*, *koira* yms.

10.

Seuraavassa on esitettynä väittämiä. Valitse oletko niistä **samaa mieltä** tai **eri mieltä**.

1. Vaihdan tietokoneideni salasanat säännöllisesti

- ☐ **Samaa mieltä** ☐ **Eri mieltä**

2. Otan tärkeistä tiedostoista aina varmuuskopiot

- ☐ **Samaa mieltä** ☐ **Eri mieltä**

3. Numerosarja 12345678 on heikko salasana

- ☐ **Samaa mieltä** ☐ **Eri mieltä**

4. On normaalia toimintaa, että sähköpostiviestillä tiedustellaan työntekijöiden salasanoja

- ☐ **Samaa mieltä** ☐ **Eri mieltä**

5. Yrityksen työntekijät eivät voi toiminnallaan vaikuttaa tietoturvallisuuteen

- ☐ **Samaa mieltä** ☐ **Eri mieltä**

6. Tuntemattoman sähköpostin liitetiedostot eivät ole vaarallisia

- ☐ **Samaa mieltä** ☐ **Eri mieltä**

7. Kirjainyhdistelmä qwerty on vahva salasana

- ☐ **Samaa mieltä** ☐ **Eri mieltä**

1.

Yrityksen työntekijä miettii tietokoneelleen salasanaa. Minkälaista salasanaa sinä suosittelet käyttäväksi, jos työntekijän käyttäjätunnus on matti?

☐ abc123

☐ 1234567890

☐ qwerty

☒ **eqT@R12!**

☐ Suositteaisin häntä käyttämään salasanaan hänen omaa käyttäjätunnustaan takaperin.

☐ password1

2.

Lähdet ostamaan toimistotarvikkeita firman logolla varustetulla autolla ja matkalla kauppaan huomaat, että yrityksen kannettava tietokone on jäänyt näkyville auton takapenkille. Miten toimit tietokoneen kanssa saavuttuasi kaupan pihaan?

☐ Siirrän tietokoneen auton lukolliseen takakonttiin, josta varkaat eivät näe sitä.

☒ **Otan tietokoneen mukaani kauppaan.**

☐ Jätän tietokoneen takapenkille kun käyn kaupassa, sillä kukaan ei ehdi varastaa sitä.

☐ Kaupan läheisyydessä ei näy yhtään varkaalta näyttävää henkilöä. Käyn nopeasti kaupassa ja jätän kannettavan tietokoneen auton takapenkille.

3.

Saat englanninkielisen sähköpostiviestin Ylläpidosta (Helpdesk), eli luotettavalta taholta. Viestissä ilmoitetaan että sinun tulisi asentaa tietokoneellesi välittömästi käyttöjärjestelmän kriittisen haavoittuvuuden korjaava tietoturvapäivitys. Tietoturvapäivityksen latauslinkki löytyy sähköpostiviestin lopusta. Kuinka toimit tässä tapauksessa?

- ☐ Koska päivitykset keskeyttävät aina työnteon, säilytän viestin ja asennan päivityksen myöhemmin iltapäivällä.

☒ **En reagoi viestiin ja poistan sen.**

- ☐ Siirryn latauslinkkiin ja lataan sieltä löytyvän Microsoft päivityksen välittömästi.
- ☐ Viesti vaikuttaa tärkeältä mutta asennan päivityksen huomenna, koska kyseessä voi olla aikaa vievä prosessi.

4.

Haittaohjelma on yleisnimitys ohjelmille (esimerkiksi tietokonevirus), jotka aiheuttavat ei-toivottuja tapahtumia tietokoneessa. Mikä seuraavista vaihtoehdoista kuvaa parhaiten nykyaikaista haittaohjelmaa?

- ☐ Ne ovat nuorten harrastelijoiden kirjoittamia, piloiksi tarkoitettuja ja eivät ole tietokoneille kovin vahingollisia.
- ☐ Työntekijän on helppo havaita työaseman saastuttanut taloudellista hyötyä tavoitteleva haittaohjelma.

☒ **Ne ovat ammattimaisia ja niillä on tarkoitus saada taloudellista hyötyä.**

- ☐ Virustorjuntaohjelmistot tunnistavat ja pysäyttävät kaikki haittaohjelmat.

5.

Työntekijä miettii, miten hän voisi toiminnallaan estää tietokonevirusten ja muiden haittaohjelmien pääsyn yrityksen työasemiin. Minkä neuvon sinä antaisit hänelle?

- ☐ Suojaa työasemasi mahdollisimman vaikealla salasanalla.
- ☐ Katkaise tietokoneestasi virta, aina kun et käytä sitä pitkään aikaan.
- ☐ Työntekijänä et voi vaikuttaa asiaan, se on virustorjuntaohjelmiston tehtävä.
- ☒ **Tuntemattoman sähköpostiviestin liitteenä tulevia, hyödyllisiltäkin vaikuttavia tiedostoja ei saa avata.**

6.

Työntekijä tuo yritykseen mukanaan USB-muistitikun, jonka hän kertoo löytäneensä aamulla yrityksen pihalta? Hän on liittämässä USB-muistitikkua yhteen yrityksen työasemista, jotta hän näkisi onko siihen tallennettuna mitään. Miten reagoisit tähän?

- ☐ Yrityksen työasemiin on turvallista liittää USB-muistitikkuja, joten en reagoi mitenkään.
- ☐ Pyydän häntä liittämään USB-muistitikun yrityksen työasemaan, joka ei ole kytketty ikinä Internetiin.
- ☐ Muistutan häntä ennen työasemaan liittämistä, kuinka USB-muistitikku poistetaan työasemasta turvallisesti käytön jälkeen.
- ☒ **Kiellän työntekijää liittämästä kyseistä USB-muistitikkua mihinkään yrityksen työasemista.**

7.

Työsähköpostiisi ilmestyy hyvällä ja sujuvalla suomenkielellä kirjoitettu viesti. Viestin lähettäjänä on tietohallinto, joka ilmoittaa että sähköpostitilisi on kaapatu ja sitä käytetään roskapostin lähetykseen. Viestissä pyydetään vahvistamaan sähköpostitilisi salasana viestissä olevan linkin kautta, jotta sinulle voidaan tehdä uusi tili ja käyttäjätunnus. Miten toimitisit tässä tilanteessa?

☒ **Poistan viestin, enkä reagoi siihen.**

- ☐ Toimin vastuullisesti. Siirryn välittömästi sähköpostin osoittamaan linkkiin ja syötän salasananani sitä kysyttäessä.
- ☐ Kiireisen aikataulun vuoksi toimin viestissä annettujen ohjeiden mukaisesti vasta iltopäivällä.
- ☐ En reagoi viestiin heti, koska työt keskeytyisivät. Seuraavana päivänä saan saman sähköpostiviestin ja nyt toimin, kuten viestissä käsketään.

8.

Yrityksen työntekijänä tarkastelet tietokoneellasi luottamuksellista dokumenttia. Päättät pitää tauon ja poistua työpisteeltäsi. Minkä toimenpiteen teet ennen lähtöäsi?

☒ **Tallennan dokumentin ja Lukitsen työaseman esimerkiksi ctrl+alt+del näppäinyhdistelmän avulla.**

- ☐ Irrotan Ethernet tietoliikennekaapelin, jotta tietokoneelle ei sillä välin tulisi tietokoneviruksia.
- ☐ Minun ei tarvitse tehdä mitään. Dokumentti jää tietokoneen näytölle sopivasti odottamaan paluutani tauolta.
- ☐ Tallennan dokumentin, koska tauon aikana voi tulla sähkökatko.

9.

Mikä on sinun mielestäsi paras tapa muistaa/säilyttää lukuisat eri salasanat tietokoneisiin ja verkkopalveluihin?

- ☐ Käytän samaa salasanaa kaikissa tietokoneissa ja verkkopalveluissa.
- ☐ Kirjoitan tietokoneen salasanan paperille ja kiinnitän paperin tietokoneen näppäimistön pohjaan.
- ☒ **Käytän salasanojen säilytysohjelmaa.**
- ☐ Käytän mahdollisimman yksinkertaisia ja selkokielisiä salasanoja, kuten *salasana*, *auto*, *koira* yms.