KYMENLAAKSON AMMATTIKORKEAKOULU
Liiketalous / Verkkoliiketoiminta

Kari-Pekka Niemi

YLEISKATSAUS TIETOTURVAAN JA TIETOTURVAKOULUTUKSEN JÄRJESTÄMINEN

Opinnäytetyö 2010

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Verkkoliiketoiminta

NIEMI, KARI-PEKKA	Yleiskatsaus tietoturvaan ja tietoturvakoulutuksen järjestäminen
Opinnäytetyö	42 sivua + 27 liitesivua
Työn ohjaaja	Lehtori Päivi Hurri
Toimeksiantaja	Kouvolan Lääkäriasema Ky
Huhtikuu 2010	
Avainsanat	tietoturva, tietoturvakoulutus, tietoturvauhka, tietoliikenne

Tietoturvasta huolehtiminen on tullut yhä ajankohtaisemmaksi viime vuosien aikana yhä useamman palvelun siirtyessä sähköiseen muotoon. Tietoturva pitää sisällään laajan kokonaisuuden, joka on hyvä jakaa eri osa-alueisiin tai sen hallitseminen muuttuu vaikeaksi. Näin voidaan hahmottaa lukuisat eri uhat ja niihin vaikuttavat tekijät.

Opinnäytetyön aiheena on luoda yleinen katsaus tietoturvaan sekä sen pohjalta laatia tietoturvakoulutus Kouvolan Lääkäriaseman henkilökunnalle. Tavoitteena ei ollut luoda tutkimusta kovin teknisestä näkökulmasta, vaan pikemminkin poimia aihealueesta tiedot, joita tavallinen peruskäyttäjä tarvitsisi hahmottaakseen, mitä tietoturva oikeastaan on.

Tietoturvasta löytyy suuri määrä tietoa eri lähteistä, kuten Internet-sivustoilta, kirjoista ja lehdistä. Opinnäytetyön tekemisen aikana on tutustuttu julkishallinnon, yritysten sekä yksittäisten henkilöiden luomiin tutkimuksiin ja oppaisiin. Myös kirjoittajan oma tietämys ja kokemus ovat toimineet lähteinä. Työssä on käsitelty tietoturvan eri käsitteitä ja osa-alueita sekä yleisiä keinoja, joita yksityiset käyttäjät ja eri organisaatiot hyödyntävät tietoturvariskien ehkäisemisessä. Sen lisäksi on tutkittu yleisiä tarpeita ja keinoja koulutuksen järjestämiseen.

Kerättyjen tietojen pohjalta laadittiin tietoturvakoulutus sekä siihen kuuluvat lisämateriaalit. Koulutus pidettiin Kouvolan Lääkäriaseman henkilökunnalle, jonka tuloksena osallistujat saivat tarvittavat perustason tiedot aiheesta.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Business Management

NIEMI, KARI-PEKKA	The Basics of Information Security and Organizing an Information Security Course
Bachelor's Thesis	42 pages + 27 pages of appendices
Supervisor	Päivi Hurri, Senior Lecturer
Commissioned by	Kouvolan Lääkäriasema Ky
April 2010	
Keywords	information security, information security training, information security threat, telecommunication

The role of information security has become more important especially during the last decade. Many different services are being transformed to an electronic format and more users are taking advantage of available online services. In order to properly manage the vast scheme of information security the subject has to be divided into smaller parts. In this way a bigger picture is created thus making it easy to perceive potential threats and their origins.

The purpose of the thesis was to make a general review of the basics of information security and to create a course based on the collected data. The course was created for the private health centre, Kouvolan Lääkäriasema. The idea behind the course was to teach the basics of information security to people who have only a little information of the subject matter.

The thesis was created by studying and gathering information from various books, webpage's, guides and news articles. The sources were created by public administration, private individuals with professional experience and different private companies. Also author's own experiences and knowledge on the matter contributed to the thesis. The thesis has divided the different areas of information security into their own sections and studied and explained them. In addition several threats or ways to prevent threats and increase the level of information security have been researched and studied. The thesis also discusses the need for information security training and documents the process of creating the course for the Kouvolan Lääkäriasema.

As a result an information security course was created and held for the staff members of Kouvolan Lääkäriasema. An extensive study material covering the entire thesis was created to support the course. The study material deals with the same topics as the thesis and it was given to all of the participants for home studying.

SISÄLLYS

1 JOHDANTO

Tietoturvan merkitys on tullut entistä tärkeämmäksi, koska valtava määrä palveluita on siirtynyt Internetiin ja yhä useampi käyttäjä hyödyntää verkon palveluita. Tietoturvasta huolehtiminen on olennaista niin yksityisille käyttäjille kuin yrityksille ja muille organisaatioille. Lainsäädännön on vaikea kulkea samaa tahtia kehityksen kanssa. Kehitys on niin nopeaa, että tietoturvasta huolehtiminen vaatii jatkuvia toimia, uudistuksia ja innovaatioita. Monet organisaatiot ovatkin laahanneet kehityksen perässä ja kokeneet suuria tappioita huonojen järjestelyjen ja riskeistä huolehtimisen laiminlyönnin vuoksi. Tietoturvauhat ovat verkostoituneet laajalti eri osa-alueisiin. Tämä tarkoittaa, ettei uhka ole vain virus tai hakkeri, vaan riskitekijöinä voivat olla esimerkiksi asiakas, organisaation henkilöstön jäsen tai laitevika. Tällöin jo peruskäyttäjän parempi tietämys aihepiiristä voi merkittävästi pienentää riskejä, minkä vuoksi tietoturvan jättäminen esimerkiksi pelkän hallinnon tai ATK-henkilöstön huolehdittavaksi ei ole järkevää.

Opinnäytetyö alkoi osana seminaarikurssia ja oli aluksi vain yleinen katsaus tietoturvaan, mutta myöhemmin aihepiiriä rajattiin ja muutettiin niin, että koottujen tietojen pohjalta laadittiin perustason käyttäjälle suunnattu tietoturvakoulutus. Myöhemmin päätettiin koulutuksen suuntaamisesta Kouvolan Lääkäriaseman työntekijöille. Opinnäytetyössä on pyritty ottamaan selvää, mitä tietoturva oikeastaan on, millaiset tekijät muodostavat tietoturvauhkia sekä on etsitty yleisiä keinoja, joilla tietoturvallisuutta voidaan parantaa ja tarkastella osa-alueittain. Tämän pohjalta laadittiin tietoturvakoulutus sekä lyhyehkö ja tiivistetty koulutusmateriaali. Työssä on pyritty käsittelemään aihetta myös eri näkökulmista, kuten organisaation hallinnon ja peruskäyttäjän. Tämän lisäksi on dokumentoitu koulutuksen järjestämistä ja sen tuloksia. Tarkoituksena ei ole ollut kuitenkaan tutkia aihetta liian yksityiskohtaisesta tai teknisestä näkökulmasta, koska koulutuksen kohderyhmänä ovat käyttäjät, joilla ei ole juuri aiempaa tietämystä aiheesta. Tietoturvasta on olemassa valtava määrä tutkimuksia ja ohjeistukset, säännökset ja toimitavat sen toteuttamisen suhteen vaihtelevat suuresti eri yhteisöjen välillä. Lähteitä on pyritty hakemaan julkishallinnon puolelta, erilaisten järjestöjen sivuilta, kirjallisuudesta sekä omasta kokemuksesta ja tietämyksestä. Ongelmallista oli rajata laajasta lähdeaineistosta aihepiirit, jotka ovat perustason käyttäjälle olennaisia.

Toimeksiantaja, Kouvolan Lääkäriasema, on vuonna 1975 perustettu yksityinen lääkäriasema, joka tarjoaa erilaisia työterveys-, erikoislääkäri-, röntgen- ja laboratoriopalveluita. Yrityksellä on Kouvolassa kaksi eri toimipistettä, ja asiakaskuntaan kuuluu yrityksiä sekä yksityisasiakkaita. Henkilökunta koostuu eri alojen lääkäreistä, psykologeista, terapeuteista, hoitajista, vastaanottosihteereistä ja kirjanpitäjästä. Yrityksen tavoitteena on tarjota asiantuntevaa ja oikein suunnattua hoitoa ja näin edistää alueen hyvinvointia. (Kouvolan Lääkäriasema 2010.)

2 YLEISTÄ TIETOTURVASTA

2.1 Mitä on tietoturva?

Tietoturva määritellään yleisesti englanninkielisellä lyhenteellä CIA (confidentiality, integrity, availability) eli tietoturvan pitäisi taata tietojen luottamuksellisuus, eheys ja käytettävyys (Järvinen 2002, 22). Tietojen eheyden pitäisi olla kunnossa, mikä tarkoittaa, että syötetty tai varastoitava data on sille tarkoitetussa muodossa, ilman että ulkopuolinen luvaton taho olisi päässyt muokkaamaan sitä. Tietojen pitäisi olla myös saatavilla ilman liiallisia toimenpiteitä niille henkilöille, joilla on tietoihin käyttöoikeus. Myös tietojen luottamuksellisuus on turvattava, niin etteivät asiattomat tahot pääse näkemään tai hyödyntämään niitä.

Edellä mainittujen käsitteiden lisäksi yhdistetään tietoturvaan myös todentaminen, pääsynvalvonta sekä kiistämättömyys. Todentamisella tarkoitetaan käyttäjän, palvelun, osoitteen tai muun vastaavan aitouden varmistamista. Kun esimerkiksi asiakas kirjautuu verkkopankkiin tunnuksillaan, on niiden lisäksi syötettävä vielä avainlukuja, joilla pyritään varmentamaan käyttäjän aitous. Pääsynvalvonnalla tarkoitetaan eri keinoja, joilla estetään asiattomien pääsy palveluun ja sallitaan käyttö todennetuille käyttäjille. Käytöstä pitää myös tallentua tietoja lokeihin, jotta esimerkiksi ongelmatilanteessa voidaan nähdä, mitä tietty käyttäjä on oikeasti palvelussa tehnyt. Kiistämättömyydellä tarkoitetaan, että tietty tapahtuma voidaan jälkikäteen todistaa sitovasti. Kiistämättömyys-käsite on erityisen tärkeä esimerkiksi verkon kautta tapahtuvassa kaupankäynnissä, jolloin ostotapahtumaan liittyvien eri vaiheiden kiistämättömyys on lähes välttämätöntä. (Järvinen 2002, 24.)

Tietoturvaa voidaan katsoa useasta näkökulmasta, mutta käytännössä se tarkoittaa esimerkiksi tietojärjestelmien ja laitteiden suojaamista erilaisia uhkia vastaan. Tieto-

turva sekoitetaan usein tietosuojaan, joka on ennemminkin yksilön tietojen ja yksityisyyden suojaamista, jonka periaatteet on tarkasti määritelty lainsäädännössä (Laaksonen - Nevasalo & Tomula 2006, 17). Tietoturvauhkia on monenlaisia, ja ne voidaan jakaa eri kategorioihin. Erilaiset järjestöt, yritykset, valtion elimet ja muut yhteisöt globaalilla tasolla ovat luoneet lukuisia eri ohjeistuksia, toimintatapoja ja sääntöjä, joilla on pyritty järjestelmien parempaan suojaamiseen. Käytännössä siis tietoturvauhkien määrittely ja siihen liittyvät toimenpiteet vaihtelevat suuresti jo pienissäkin yhteisöissä. Suomessa valtiovarainministeriö, joka on vastuussa valtion tietoturvallisuuden kehityksestä ja ohjeistuksesta, on laatinut muun muassa erilaisia ohjeita ja säännöksiä, joiden tarkoituksena on ylläpitää ja parantaa tietoturvaa kaikilla yhteiskunnan tasoilla (Tietoturvallisuus 2009). Toisaalta tarkkaa ja kattavaa lainsäädäntöä aiheesta ei ole luotu, vaan tietoturvallisuuden toteuttaminen yksityiskohtineen on pitkälti kiinni yrityksen tai muun sellaisen yhteisön ylläpitäjistä. Laki tietysti asettaa kuitenkin tietyt vähimmäisvaatimukset esimerkiksi rekisterinpitäjille.

Tietoturvaa uhkaavat monenlaiset tekijät. Järjestelmiin voidaan syöttää erilaisia haittaohjelmia ja viruksia, jotka voivat tuhota, kerätä tietoja tai esimerkiksi vain vakoilla järjestelmän käyttöä. Kohteita haittaohjelmille ja muille hyökkäyksille ovat esimerkiksi järjestelmissä tapahtuva tietoliikenne tai järjestelmän ylläpitämät palvelut. Myös järjestelmien käyttäjät luovat haavoittuvaisuuksia toiminnallaan, kuten käyttämällä helposti murrettavia salasanoja tai vuotamalla salasanoja, käyttäjätunnuksia ja muita tietoja eri teitse.

2.2 Tietoturvauhat

Tietoturvauhkia ovat muun muassa erilaiset järjestelmän virheet ja puutteet sekä haittaohjelmat. Järjestelmät ja eri ohjelmat voivat olla haavoittuvaisia, jos niiden ohjelmoinnissa on jätetty erilaisia tietoturva-aukkoja, joita mahdolliset tunkeutujat voivat hyödyntää. Lähes kaikki ohjelmat ja järjestelmät omaavat erisuuruisia määriä edellä mainittuja haavoittuvaisuuksia. Ohjelma ei ole välttämättä haavoittuvainen ainoastaan ohjelmointivirheiden vuoksi, vaan myös niitä käyttävät ihmiset voivat luoda toiminnallaan erilaisia riskejä. Näiden puutteellisuuksien kautta väärät tahot voivat vakoilla, varastaa tai tuhota tietoja. Motiiveina voivat olla tietojen myyminen eteenpäin, liiketoiminnan tai käyttäjän vakoilu tai vain puhdas vahingon tuottaminen. Tämän seurauksena järjestelmien toimivuus yleensä huononee, joka voi näkyä koneiden hidastelu-

na, palvelukatkoksina tai tietyt haittaohjelmat voivat jopa aiheuttaa niin suurta haittaa, että laitteistot muuttuvat käyttökelvottomiksi.

Lähes jokainen tietokoneen peruskäyttäjä on kuullut viruksista, haittaohjelmista, hakkereista ynnä muista sellaisista, vaikkei omaisikaan yksityiskohtaista tietoa niistä. Erilaisista haittaohjelmista tunnetuimpia ovat yleensä erilaiset virukset, madot, troijalaiset sekä botit. Virukset ovat ohjelmia, jotka pyrkivät tarttumaan eri tiedostoihin ja ohjelmiin ja sitä kautta leviämään muihin järjestelmiin. Virukset leviävät usein muiden tiedostojen mukana, kuten sähköpostiviesteissä tai Internetistä ladattavien ohjelmien kautta. Madot puolestaan ovat itsenäisiä ohjelmia, eli ne kopioivat ja levittävät itseään automaattisesti. Troijalaiset voivat taas olla viattoman näköisiä tiedostoja, jotka ovat todellisuudessa haittaohjelmia. Tavoitteena on saada käyttäjä uskomaan, että troijalainen tai ohjelma, johon se on liitetty, on turvallinen. (Haittaohjelma 2010.) Botit mahdollistavat käyttäjän koneen kaappauksen, jolloin ulkopuolinen taho voi käyttää sitä haluamillaan tavoilla. Käyttäjä ei monesti edes tiedä, että koneen hallinta on kaapattu. Useista kaapatuista koneista voidaan luoda suuria bottiverkkoja. Bottiverkkoja hallinnoivat tahot voivat valjastaa näin kaapatut koneet esimerkiksi lähettämään valtavia määriä roskapostia, tai useiden käyttäjien tiedot voidaan varastaa. Haluttu palvelu, kuten Internet-sivusto, voidaan lamauttaa palvelunestohyökkäyksellä, jossa kaapatut koneet lähettävät esimerkiksi tuhansia yhteydenottoja näin kaataen palvelun. (Botit ja bottiverkot – kasvava uhka 2010.)

Ihmiset luovuttavat huolimattomasti käyttäjätietojaan, käyvät vaarallisilla sivustoilla tai lataavat haitallisia ohjelmia huomaamattaan. Monet sivustot yrittävät huijata käyttäjiä rekisteröitymään tai antamaan itsestään tietoja, joita voidaan hyödyntää eri tavoin vilpillisessä mielessä. Sivustot voivat sisältää myös erilaisia tiedostoja, kuten viruksia tai muita haittaohjelmia, jotka käyttäjä saattaa vahingossa asentaa luullen niitä joksikin muuksi. Esimerkkitapauksena ovat väärennetyt virusohjelmat, joita Symantec-yhtiön mukaan on olemassa jo vähintään 250. Käyttäjiä pelotellaan tietoturvauhilla, jolloin ladataan ohjelma, josta saatetaan vielä maksaakin. Tämä puolestaan antaa väärentäjille kallisarvoisia ja arkaluonteisia tietoja käyttäjästä ja hänen tili- ja maksutiedoistaan. Samaan aikaan ladattu ohjelma altistaa käyttäjän koneen lukuisille vaaroille. (Väärät virustorjuntaohjelmat huijaavat ihmisiä netissä 2009.)

Erilaisia keinoja huijata käyttäjiltä maksutietoja, käyttäjätunnuksia, salasanoja ja muita sellaisia on lukemattomia. Tällaista toimintaa, jossa käyttäjiltä huijataan tietoja psykologisin menetelmin, kutsutaan sosiaaliseksi manipuloinniksi eli Social Engineering (Järvinen 2002, 307). Huijari voi esiintyä toisena henkilönä, vaikkapa tietyn palvelun ylläpitäjänä, joka soittaa asiakkaalle ja yrittää tiedustella arkaluonteisia tietoja. Käyttäjät saattavat myös luovuttaa arkaluonteisia tietoja epähuomiossa esimerkiksi käytettäessä erilaisia keskustelupalstoja tai yhteisöpalveluita, kuten Facebookia. Käyttäjä voi keskustelun lomassa kirjoittaa erittäin henkilökohtaisia tietoja ymmärtämättä, kuinka monelle käyttäjälle tiedot ovat saatavilla.

Monet haittaohjelmat saattavat vain hidastaa koneen käyttöä ja tuhota tiedostoja, mutta toisaalta tietoja voidaan käyttää myös markkinointiin. Markkinointiin käytettäviä haittaohjelmia kutsutaan mainosohjelmiksi (Adware). Ne pyrkivät esittämään käyttäjille erilaisia mainoksia, kuten avaamalla mainosikkunoita Internet-selaimessa käytön aikana. Erilaiset vakoiluohjelmat (Spyware) keräävät tietoja käyttäjästä ja järjestelmästä ilman lupaa. Niiden tarkoituksena voi olla vakoilu, tiedon varastaminen tai tietoja voidaan käyttää esimerkiksi mainontaan. Pahimmissa tapauksissa vakoiluohjelmat kykenevät tallentamaan näppäinpainalluksiakin, jolloin kaikki mitä käyttäjä kirjoittaa, voi mahdollisesti päätyä väärälle taholle. (Tietoturvaopas – Haittaohjelmat 2008.)

Suuri ongelma on roskaposti eli viestit, jotka ovat väärennöksiä tai muuten haitallisia ja tietoliikennettä haittaavia. Viestit sisältävät usein mainoksia tai yrityksiä saada käyttäjä avaamaan liitetiedostoja tai vierailemaan epäilyttävillä sivustoilla. Roskaposti kuormittaa valtavasti verkkoa, ja jopa suuri osuus kaikesta sähköpostiliikenteestä muodostuu roskapostista.

Näiltä uhilta suojautuminen on vaikeaa ja käytännössä melkein mahdotonta, koska haittaohjelmat ja keinot tunkeutua järjestelmiin kehittyvät käsi kädessä uusien tekniikoiden kanssa. Silti on toimintatapoja, joilla näitä riskejä voidaan pienentää. Tietoturvaohjelmistot kannattaa pitää ajan tasalla ja huolehtia, että koneet on suojattu asianmukaisesti. Tällaiseen tarvitaan yleensä palomuurit, virusohjelmat ja ajan tasalla olevat päivitetyt järjestelmät ja ohjelmistot. Kannattaa myös seurata tietoturva-alan julkaisuja, joita löytyy runsaasti verkosta sekä lehdistä. Käyttäjän oma tietämys tai organisaatiossa sovitut säännöt ja ohjeistukset ovat tärkeässä asemassa. Käyttäjän on myös oltava tarvittavan kriittinen ja yritettävä itse arvioida, onko esimerkiksi tietty sivusto,

tiedosto tai sähköpostiin saapunut viesti luotettava. Moni tietoturvaa uhkaava tekijä onkin vaarallinen, koska voidaan vedota käyttäjän tietämättömyyteen tai hyväuskoisuuteen hyödyntäen sosiaalista manipulointia, jolloin teknisillä keinoilla suojautuminen ei ole enää mahdollista.

2.3 Verkon suojaus ja valvonta

Verkkojen ja laitteiden suojauksesta tulee huolehtia asianmukaisesti. Tämä ei ole ainoastaan kannattavaa yleisen turvallisuuden kannalta, vaan henkilötietolaki velvoittaa rekisterinpitäjät huolehtimaan järjestelmiensä turvallisuudesta. Käytännössä käyttäjän ei pidä päästä verkkoon ja saada oikeuksia muokata tai saada tietoja vahingossa tai vilpillisessä mielessä. (22.4.1999/523,32§.) Haavoittuvaisuuksien korjaamisen ja tunkeutumisyritysten lisäksi on hyvä muistaa, että verkossa saattaa olla jo valmiina luvattomia käyttäjiä, jotka ovat onnistuneet muilla tavoilla ohittamaan suojauksen. Verkon käyttöä voidaan seurata, ja onkin tärkeää kiinnittää huomiota siihen, miten paljon dataa liikkuu ja minne ja kuormittaako se turhaan verkkoa. Esimerkiksi, jos huomataan, että työasemalta, jota käytetään pääasiassa arkipäiväisiin toimistotehtäviin, lähetetään huomattavia määriä dataa kuormittaen verkkoa, voi kyseessä olla jonkinlainen tietomurto tai asiaton käyttö.

Erilaisten tietokantojen ylläpito, joihin varastoidaan lokeja tietomurroista tai murtoyrityksistä, on hyvä keino tietoturvan parantamiseksi. Kun on tiedossa ja kirjattuna kaikki paljastuneet yritykset, murrot ja niihin liittyvät yksityiskohdat, voidaan analysoida verkon vahvuuksia, haavoittuvaisuuksia ja etsiä tapoja ja parannuksia, joilla vastaavia tapauksia voidaan estää tulevaisuudessa. Mahdollisen tunkeutujan on myös vaikeampi yrittää kiistää tapahtuma, jos tunkeutumisesta on tallennettu luotettavat tiedot. Lokitiedot tulee tallentaa erillisille palvelimelle ja suojata se myös asianmukaisesti, jottei järjestelmiin tunkeutuva osapuoli muuta myös lokitietoja, esimerkiksi peittääkseen tunkeutumisesta tallentuneet tiedot (Laaksonen - Nevasalo & Tomula 2006, 192). Vaikka tietomurrot huomattaisiinkin ja tiedot niistä tallennettaisiin, on oltava olemassa myös erilaisia hälytysjärjestelmiä, jotka ilmoittavat tietomurroista, jotta asialle voidaan tehdä jotain. On tapauskohtaista, minkälainen järjestely on tarpeen riippuen organisaatiosta. Jos kyseessä on tärkeitä luottamuksellisia tietoja tai verkko, jonka jatkuva toiminta ja ylläpito ovat välttämättömiä, voidaan tietoliikennettä valvoa vuoro-

kauden ympäri, jolloin on mahdollista puuttua rikkeisiin reaaliajassa hälytyksen tullessa. Tällaiset järjestelyt vaativat kuitenkin jo paljon resursseja ja varoja.

Eri työasemien käyttöä ja verkon liikennettä pitää seurata, mutta se vaatii usein tunnistamistietojen käsittelyä sekä viesteihin puuttumista. Perustuslain yksityiselämän suoja suojelee yksilön oikeuksia niin, että henkilötiedot sekä viestintä ovat luottamuksellisia, mutta viestintään saa kajota käyttäjän luvalla tai jos epäillään, että viestintävälineitä tai verkkoa käytetään vilpillisessä mielessä (Tietosuojavaltuutetun toimisto 2009,5). Tällainen tapaus voi olla esimerkiksi, jos yhteyksiä käytetään laittoman materiaalin lataamiseen tai jos pyrkimyksenä on verkon häirintä tai yleisten organisaation toimintaohjeiden rikkominen. Erilaiset piratismiin käytettävät ohjelmat voivat kuormittaa huomattavasti verkkoja ja niillä ladattavien tiedostojen sisältö voi olla arveluttavaa. Työnantajalla on siis oikeus puuttua tapauksiin tiettyjen kriteerien pohjalta, tarkkailla käytettäviä ohjelmia ja estää väärinkäytöksiä. (Laaksonen - Nevasalo & Tomula 2006, 193.) Operaattorit ilmoittavat asiakkaan kanssa tehdyissä liittymäsopimuksissa erilaisista rikkeistä, kuten laittoman sisällön lataamisesta, jolloin rikkeestä jääneet tunnistamistiedot voidaan välittää eteenpäin viranomaisten pyynnöstä. Tämä vaatii jo usein painavan syyn ja tarkat järjestelyt. Esimerkiksi yritykset ja kunnat ovatkin yleensä laatineet työntekijöilleen eritasoisia ohjeita, joissa määritetään, mitä koneilla saa tehdä. Työntekijöiltä voi olla kokonaan rajoitettu ohjelmien lataus ja asennus koneille ja mahdollisesti jopa kielletty kaikenlainen Internetin selaaminen työajalla. Näillä toimilla on pyritty pienentämään riskejä verkon väärinkäytöstä, mutta yksilötason viestintää on hankala valvoa. Moni käyttäjä ei noudata sääntöjä, joten onkin parempi teknisin keinoin esimerkiksi rajoittaa pääsyä tietyille sivustoille tai estää eri ohjelmien käyttö.

2.4 Tietoturvan suunnittelu ja järjestäminen

Uhkien torjuntaa suunnitellessa ja toteuttaessa täytyy huomioida, mitä kaikkea erilaisiin hankintoihin sisältyy ja minkälaiset ratkaisut sopivat tietylle organisaatiolle. Tietoturvan järjestämisestä on hyvä huolehtia jo ennen minkäänlaisia hankintoja, koska jälkikäteen toteutettuna voi tulla esille monenlaisia yhteensopivuusongelmia jo käytössä olevien ohjelmien kanssa. On valikoitava tarkkaan myös toimittajat ja keinot, joilla tietoturvaratkaisut hankitaan ja tutustutaan tulevaan yhteistyökumppaniin ja sen ratkaisuihin. On myös mietittävä, kuka asentaa ohjelmistot, miten, milloin ja millä ai-

kataululla. Hankinnat eivät lopu asennukseen, vaan usein tarvitaan myös jatkuvaa teknistä tukea tai apua päivityksiin ja mahdollisiin muutostilanteisiin, joissa järjestelmiä joudutaan muokkaamaan. Tietoturvaratkaisuja tarjoavan yrityksen rooli voi olla siis hyvinkin erilainen, yritys voi vain toimittaa tietyn ohjelmistopaketin tai muuttua jatkuvaksi yhteistyökumppaniksi, joka valvoo tietyn organisaation verkkoja ja toimintaa ja vastaa niiden ylläpidosta.

Ohjelmien hankinnoissa ja suunnittelussa on huomioitava myös palvelimet, Internet ja selainliikenne tai muut yhteydet, jotka täytyy myös suojata (Laaksonen - Nevasalo & Tomula 2006, 204). Kotikoneen suojaus on yleensä kiinni sen käyttäjästä, mutta toisaalta, jos kone on yhteydessä esimerkiksi yrityksen tietokantoihin ja tehdään etätyötä, voi kotikoneen saastuminen altistaa myös yrityksen verkon. Tietokoneiden lisäksi Internet-yhteyksiä luovat myös puhelimet tai muut koneet, joiden tietoturvapuolta saatetaan usein laiminlyödä. Kännykät, kannettavat tietokoneet ja muut sellaiset kannattaakin suojata ajantasaisilla tietoturvaohjelmistoilla ja käyttää erilaisia salausmenetelmiä. Riskit ovat silti suuremmat, kun laitteet ottavat yhteyttä tietokantoihin vieraiden verkkojen kautta tai jos koneet ovat vapaa-ajan käytössä, jolloin saatetaan käsitellä sopimatonta tai muuten riskialtista aineistoa. Riskejä luovat myös laitteet, jotka ovat pitkään poissa verkosta. Tällöin tietoturvaohjelmistot saattavat vanhentua ja järjestelmä muuttuu haavoittuvaiseksi, kun ohjelmistot eivät kykene hakemaan ajantasaisia päivityksiä (Hakala – Vainio &Vuorinen 2006, 137). Jokaisen organisaation onkin hyvä tehdä perinpohjainen riskikartoitus ennen hankintoja ja dokumentoida koko hankintaprosessiketju.

Monet ohjelmistoratkaisut, kuten F-Securen tietoturvaohjelmistot, voivat vaatia myös paljon tehoja koneilta ja järjestelmiltä hidastaen käyttöä varsinkin vanhemmissa laitteissa. Tämä voi johtaa uusiin laitehankintoihin tai päivityksiin, jotka voivat luoda jo suuria menoeriä. Organisaation onkin hyvä etukäteen tehdä tarkka suunnitelma tarvittavista hankinnoista ja etsiä juuri omiin tarpeisiin räätälöity ohjelmistokokonaisuus. Hankinnoissa onkin muistettava yksi tietoturvallisuuden kulmakivistä eli tietojen pitää olla käytettävissä. Jos tiedot on täydellisesti turvattu, mutta niihin käsiksi pääsy oikeilta tahoilta on liian työlästä tai resursseja vievää, ei tietoturvallisuus enää aja asiaansa oikealla tavalla. Esimerkiksi asiakaspalvelua hoitavissa toimipisteissä tietojenkäsittelyn nopeus voi olla ensiarvoista, jolloin hidastelevat järjestelmät voivat helposti muodostua kompastuskiveksi.

Jos halutaan huolehtia tietojen pysymisestä mahdollisimman turvassa, on turvauduttava salausmenetelmiin, koska tärkeitä tietoja voi vuotaa tai päästä väärin käsiin monilla eri tavoilla. Jos tiedostot tai laitteet on salattu, mahdollinen tunkeutuja ei pysty välttämättä pääsemään käsiksi tietoihin. Erityisesti salattavia kohteita ovat kiintolevyt, etäyhteydet, muistitikut, sähköpostiviestit, liitetiedostot ja muut tärkeitä tietoja sisältävät laitteet tai viestintään käytettävät järjestelmät ja menetelmät (Laaksonen - Nevasalo & Tomula 2006, 195). Tiedostojen salaamiseen ja suojaukseen on useita erilaisia menetelmiä, esimerkiksi julkisten ja yksityisten salausavainten käyttö, digitaaliset allekirjoitukset sekä holvaus. On kuitenkin arvioitava salauksen tarve, koska läheskään kaikkea tietoa ei ole järkevä salata, sillä erilaisten salausmenetelmien hallinnasta voi tulla vaikeaa ja aikaa vievää. (Salausmenetelmät 2009.)

Käyttäjän ei tarvitse välttämättä omata yksityiskohtaista tietoa tietoturvauhista tai saada erityiskoulutusta, jos käytettävät ohjelmat ovat tarpeeksi kehittyneitä ja automatisoitu. Tällainen järjestely onkin yleensä oivallinen arkipäiväisessä työympäristössä, jossa tavallisen työtekijän ei ole suotavaa päästä tekemään itsenäisiä päätöksiä tietoturvasta, jos esimerkiksi palomuuri kysyy, sallitaanko tietyn ohjelman pääsy verkkoon. Käyttäjä voi tällöin tehdä tahattomasti huonoja päätöksiä ja sallia tunkeutujalle pääsyn järjestelmiin tai vaihtoehtoisesti estää tietyltä ohjelmalta mahdollisuuden päivitysten hakuun. On siis parempi, että ohjelma tekee itse jonkinlaisen toiminnon tai hälytyksen tai ilmoittaa käyttäjälle, joka ottaa yhteyttä tietoturvasta vastaavaan henkilöön. Ohjelmat keräävät lokeja, jonka perusteella voidaan myöhemmin tutkia tapahtuneita vaaratilanteita tai tunkeutumisyrityksiä ja nähdä mitä tapahtui, milloin ja kenen toimesta. Toisaalta käyttäjän oma tietämys mahdollisista riskeistä tuo aina enemmän lisäturvaa, koska mikään järjestelmä ei ole täydellisesti suojattu. Eri ohjelmistoratkaisut tuovat myös paljon muutoksia käyttöjärjestelmiin tai voivat vaatia erityistoimenpiteitä, jotka saattavat usein hämmentää käyttäjää. Onkin tärkeää huolehtia, että henkilökunta on tietoinen muutoksista tai uusista ohjelmista, jolloin voidaan välttyä monelta teknistä tukea vaativalta tilanteelta. Hankintojen yhteydessä on huomioitava, onko olemassa tarve antaa henkilökunnalle koulutusta aiheesta. Arkipäiväisissä toimistotöissä jo perustasonkin ohjeistus tai tiedottaminen voi olla riittävää, mutta tietyissä organisaatioissa, joissa toteutetaan monimutkaisia prosesseja tietokoneilla, voi tulla kyseeseen jo hyvinkin syvälaatuinen koulutus.

Onkin hyvä varautua, miten toimitaan tilanteessa, jossa on jo tapahtunut jonkinlainen tietomurto tai vastaava. Varmuuskopiointi toki säilyttää vanhat tiedot, mutta jos on kyseessä esimerkiksi yrityksen kotisivu, jonka kautta asiakkaat hoitavat toimintaansa, voi palvelun äkkinäinen lakkautuminen olla katastrofi. Varmuuskopioitujen tietojen tai järjestelmien uudelleen asentaminen vie myös aikaa ja resursseja. On kartoitettava, mitä kautta, kenelle ja kuinka nopeasti tieto palvelun lakkautumisesta kulkee ja miten minimoidaan välittömät vahingot. Esimerkiksi, jos havaitaan tunkeutuminen tietokantaan, niin ilmoitus tunkeutumisesta lähtee vastuuhenkilölle, joka sulkee järjestelmän tai pääsyn tunkeutujalta estäen näin tietojen varastamisen tai tuhoamisen. On luotava myös toimintasuunnitelma pidemmän aikavälin vahingoille. Esimerkiksi yrityksen verkkosivujen alasajo voi aiheuttaa pitkäaikaista vahinkoa, kuten Sampo-pankin tapauksessa, jossa palvelun katkeaminen aiheutti suuria kustannuksia asiakkaiden tehdessä reklamaatioita ja vaihtaessa palveluntarjoajaa (Sampo Pankin asiakkaat äänestävät jaloillaan 2008). Varautumissuunnitelmat koskettavat myös yrityksen budjettia, johon on varattava resursseja eri riskitilanteiden hoitoon ja niiden aiheuttamien vahinkojen korjaamiseen, koska toimintakyvyn äkkinäinen heikkeneminen voi helposti aiheuttaa varojen loppumisen kriittisellä hetkellä (Hakala – Vainio & Vuorinen 2006, 31). Onnistunut riskienkartoitus ja varotoimenpiteiden oikea toimeenpano ovat kriittisessä asemassa, jotta voidaan toipua toteutuneesta uhkatilanteesta mahdollisimman pienillä vahingoilla.

2.5 Lainsäädäntö

Suomessa ei ole tällä hetkellä olemassa tarkkaa ja yhtenäistä tietoturvaa koskevaa lainsäädäntöä, vaan eri säännökset tulevat useista eri laeista ja asetuksista. Tällaisia ovat esimerkiksi perustuslaki, sähköisen viestinnän tietosuojalaki, henkilötietolaki ja laki sananvapauden käyttämisestä joukkoviestinnässä. (Sähköisen viestinnän tietoturva ja –suoja 2010.)

Yleiset lait pätevät myös Internetissä tapahtuvassa toiminnassa ja on myös säädetty uusia lakeja, jotka erityisesti koskettavat Internetin käyttöä. Kunnianloukkaus ja yksityiselämää koskettavien tietojen levittäminen on kiellettyä. Tämä on tullut erityisesti esille, kun poliisille on tehty tutkintapyyntöjä erilaisista palstakirjoituksista tai erilaisissa yhteisöpalveluissa tapahtuneista rikkeistä. Moni käyttäjä ei välttämättä kykene tiedostamaan, että keskustelupalstalla toisen nimittely, uhkailu tai rasismi otetaan va-

kavasti. Erilaisissa palveluissa, kuten chateissa ja Facebookissa levitetään myös paljon yksityiskohtaisia henkilötietoja, joita myös lainsäädäntö suojaa. On mietittävä tarkkaan, mitä haluaa kertoa itsestään tai muista ihmisistä julkisissa profiileissa, jotka ovat kaikkien saatavilla. Viestintäsalaisuus suojelee viestintää, kuten sähköpostia, puheluita ja kirjeitä. Onkin muistettava, ettei toisen käyttäjän sähköpostia saa avata sen enempää kuin kirjettäkään. Ilmeisimpiä tietoturvauhkia ovat yleensä erilaiset virukset, järjestelmiin tunkeutumiset ja muut vastaavat. Erikseen kiellettyjä laissa ovat virusten tekeminen ja levitys, tietoverkkojen häirintä, järjestelmiin tunkeutuminen tai sen yrittäminen sekä niiden luvaton käyttö. Suurena ongelmana on yleensä roskapostitus, jota on hankala rajoittaa, ja laissa onkin kielletty markkinointi ilman lupaa ja käyttäjän on saatava päättää, voidaanko hänen tietojaan hyödyntää markkinoinnissa. Varsinaiset hankaluudet syntyvät yleensä, kun roskapostittajat käyttävät useita eri osoitteita ja heitä ei saada helposti henkilökohtaiseen vastuuseen. Monet tahot keräävät, levittävät ja myyvät luvattomasti sähköpostilistoja, joiden sisältämiä yhteystietoja hyödynnetään roskapostituksessa. Toisaalta monet käyttäjät eivät myöskään usein lue tietyn palvelun käyttöehtoja ja saattavat huolimattomuuttaan rekisteröityä palveluun, jonka kautta käyttäjätiedot päätyvät roskapostittajille. (Lainsäädäntö ja internet 2008.)

Tekijänoikeuslaki on ollut paljon puhuttu aihe vuosien ajan, koska piratismia on pyritty karsimaan ympäri maailman mitä erilaisimmilla keinoilla heikolla menestyksellä. Yleensä tekijänoikeuskiistat koskettavat Internetissä laittomasti jaettavaa musiikkia, pelejä ja elokuvia sekä tahoja, jotka ylläpitävät edellä mainittujen jakamiseen käytettäviä palveluita. Samat lait koskevat myös esimerkiksi toisen tekemän kuvan tai tekstin käyttöä omilla kotisivuilla ilman lupaa, jota moni käyttäjä ei tiedosta. Tietoturvan kannalta piratismi on ongelmallista, koska sen mukana leviää paljon haittaohjelmia, laitonta materiaalia sekä se kuormittaa valtavasti verkkoa. Myös tavat, joilla piratismi on pyritty kitkemään, ovat olleet kyseenalaisia, koska niihin liittyy paljon lainsäädännöllisiä ongelmia. Viranomaisten on puututtava yksilötason viestintään ja tarkistettava koneita, joka on monesti ongelmallista, ja myös tuomioiden kovuus vaihtelee suuresti valtiokohtaisesti. Eri organisaatioille tuottaa myös kuluja kehittää keinoja, joilla estetään tai valvotaan, etteivät työntekijät käytä verkkoa väärin.

3 TIETOTURVAN ERI OSA-ALUEET

3.1 Osa-alueiden määrittely

Tietoturvasta huolehtiminen pitää sisällään valtavan kokonaisuuden, joten onkin järkevää jakaa ja lajitella se eri osa-alueisiin. Tässä opinnäytetyössä on käytetty valtionhallinnon VAHTI-tietoturvaohjeiden määrittelemiä kategorioita: hallinnollinen tietoturva, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus. Nämä kategoriat tai niitä läheisesti muistuttavat muut samankaltaiset määrittelyt ovat yleisesti käytettyjä. Määrittely antaa mahdollisuuden suunnitella paremmin, mihin voimavaroja käytetään ja miten jakaa esimerkiksi vastuualueita eri henkilöille tai yksiköille. Osa-alueiden jakaminen helpottaa myös kokonaiskuvan saamista tietoturvan rakenteesta tietyssä organisaatiossa, koska voidaan muun muassa helposti nähdä, mitä kautta riskitekijöitä ilmaantuu tiettyjä järjestelmiä kohtaan ja mihin muihin järjestelmiin saattaa vaikuttaa yhden osa-alueen altistuminen, esimerkiksi hyökkäykselle. Määrittely antaa myös paremman kuvan organisaatiosta, kun nähdään selkeästi esimerkiksi, tehdäänkö etätöitä, jolloin tietoturvariskit voivat iskeä käyttäjän omalta koneelta, tai käytetäänkö yrityksessä paljon mobiililaitteita, joiden suojaustaso voi olla alhaisempi. Nämä esimerkit ovat alueita, joita voidaan helposti sivuuttaa, jos organisaatiossa ei ole selkeää kuvaa ja luokittelua kokonaisuudesta.

3.2 Hallinnollinen tietoturva

Hallinnollisella tietoturvalla tarkoitetaan johdon tai muun hallinnollisen elimen laatimia yleisiä periaatteita, ohjeistuksia ja ajatuksia tietoturvasta ja eri tavoista, joilla sitä tullaan ylläpitämään tietyn organisaation sisällä. Tähän sisältyvät myös vastuualueiden ja resurssien jako sekä riskien arviointi. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003,40.)

Hyvin hoidettu hallinnollinen tietoturva on erittäin tärkeä tekijä varsinkin suurissa organisaatioissa, joissa se luo yhtenäisen perustan sekä ajattelutavan. Jotta hallinnon ajamat arvot ja päätökset saavuttavat myös työntekijät, on luotava ohjeistuksia, järjestettävä koulutuksia sekä huolehdittava henkilökunnan hyvästä tiedottamisesta. Laaksonen - Nevasalo & Tomulan (2006, 128) mukaan lähes kaikissa organisaatioissa on tarpeellista määritellä erilaiset roolit ja vastuut liittyen tietoturvanhallintaan. Kun mää-

rittely on tehty ja valittu esimerkiksi eri osastoille tietoturvavastuuhenkilöt, on turvallisuuskysymyksistä huolehtiminen organisaation sisällä paljon selkeämpää ja valvonta tehokkaampaa. Tämä helpottaa resurssien jakamista sekä antaa realistisen kuvan organisaation tilasta, mikä puolestaan helpottaa johdon päätöksiä ja toimintaa. Näin hallinnosta vastaavilla on ajantasainen ja selkeä käsitys organisaation tarpeista.

Organisaatiosta ja sen koosta riippuen on kyseenalaista, tarvitaanko tietoturvavastaavia, koska esimerkiksi pienemmissä yrityksissä tilannetta on paljon helpompi seurata ja tietoturvapäätökset saattavat olla hyvin vähäpätöisiä. Henkilökunnan ja muiden käyttäjien ohjeistuksen tarve voi myös olla hyvin vaihtelevaa. Hallinnollisen tietoturvan tärkeys korostuu sitä enemmän, mitä toiminta perustuu tietotekniikan käyttöön, tietojen turvalliseen käsittelyyn ja mitä suurempi organisaatio on.

Jotta johdon asettamat linjaukset olisivat oikeasti sisäistetty ja vaikuttamassa työntekijöiden keskuudessa, pitää huolehtia tietyistä perusasioista, joista Opas julkishallinnon tietoturvan järjestämisestä (2003,41) listaa seuraavia: organisaation tietoturvapolitiikka ja - periaatteet, tietoturvavastuiden jako työjärjestyksissä ja tehtäväkuvauksissa, tietoturvaohjeiden laatu, kattavuus sekä koulutus ja allekirjoitetut vakuutukset turvaohjeiden lukemisesta ja noudattamisesta. Käytännössä tämä tarkoittaa, että työntekijät ovat tietoisia ja ymmärtävät organisaationsa kannan tietoturva-asioihin ja eri tapoihin, joilla sitä toteutetaan, ja ovat sitoutuneet siihen. Samaan aikaan itse organisaatio on järjestänyt työntekijöilleen ohjeistukset ja mahdollisuuden koulutukseen sekä huolehtinut, että työpaikalta löytyy vastuuhenkilöitä, joiden työnkuvassa on selkeästi määritelty tietoturvavastuualueet.

Tarpeen vaatiessa käyttäjät tulisi hyvissä ajoin perehdyttää asioihin ja ohjeisiin, jotka olennaisesti vaikuttavat heidän työtehtäviinsä (Opas julkishallinnon tietoturvan järjestämisestä 2003,41). Esimerkiksi salassapidettäviä tietoja käsittelevät työntekijät, jotka joutuvat käyttämään paljon sähköpostia ja muita viestintävälineitä, kuten sairaanhoidon piirissä toimivat ihmiset, tarvitsevat yksityiskohtaiset ohjeet tietoturvakäytännöistä hyvissä ajoin.

Ilman suunniteltua tai hyvin toteutettua hallinnollista tietoturvaa vastuu jääkin yleensä käyttäjälle itselleen, jonka oma tieto- ja osaamistaso voi olla hyvin vaihtelevaa. Tällöin olisikin hyvä, että käyttäjä pyrkii välttämään selkeitä riskitekijöitä, kuten henkilökohtaisten palvelujen käyttöä tai surffailua Internetissä. Vaikka hallinnollista tietotur-

vaa laiminlyötäisiin tai sitä ei pidettäisi tärkeänä, pitäisi työntekijällä tästä huolimatta olla jonkinlainen perusohjeistus.

3.3 Henkilöstöturvallisuus

Valtionhallinto määrittelee henkilöstöturvan seuraavasti: *Henkilöstöön liittyvien tietoturvariskien hallinta henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta* (Valtionhallinnon tietoturvakäsitteistö 2003, 13). Henkilöstöturvallisuus onkin siis avainasemassa tietoturvan suhteen, koska heikoin lenkki on yleensä työntekijä itse. Johtoporras voi antaa sääntöjä, kieltoja, kannusteita ja ohjeita, mutta työntekijästä itsestään riippuu, kuinka hyvin ohjeet sisäistetään ja noudatetaanko niitä. Tietoturvallisuutta parantaa myös, kun huolehditaan sijaisuuksista, varahenkilöistä ja eri käyttäjien vastuualueista, jolloin tiedot ja palvelut ovat todennäköisemmin saatavilla ja käytettävissä myös ongelmatilanteiden aikana.

Henkilöstöturvallisuus pitää huomioida jo työhönottovaiheessa. On tärkeää, että työhön otettava henkilö on tehtävään sopiva ja häneen ei liity riskitekijöitä. Valintaprosessia voidaan myös tukea erilaisilla taustaselvityksillä ja testeillä lain puitteissa. Nykyaikana työntekijöistä voi löytyä suuria määriä henkilökohtaisia tietoja erilaisten yhteisöpalveluiden, kuten Facebookin kautta, mutta näitä tietoja ei saisi käyttää työhönottovalinnassa. Henkilöstöturvallisuus ei rajoitu ainoastaan organisaation omiin työntekijöihin, vaan myös yhteistyökumppaneihin. Monilla sidosryhmillä on asemastaan riippuen erisuuruisia oikeuksia päästä käsiksi laitteisiin, tietoihin tai muuttamaan järjestelmien asetuksia. Ulkopuolisia tahoja tai yhteistyökumppaneiden edustajia voivat olla esimerkiksi asiakkaat, siivoojat, huoltomiehet tai muut vastaavat. Näiltä tahoilta voi ollakin vaikea tai mahdotonta vaatia tai odottaa tietämystä tietoturvan suhteen. (Laaksonen - Nevasalo & Tomula 2006, 139.)

Irtisanottaessa työtekijöitä, liiketoimintaa harjoittaessa ja muissa toiminnoissa vaihdetaan usein organisaatiolle tärkeitä ja salassa pidettäviä tietoja, jolloin tietoja voi vuotaa ulkopuolisille tahoille. Tätä voidaan estää erilaisilla sopimuksilla, kuten salassapitosopimuksilla tai lisensseillä (Laaksonen - Nevasalo & Tomula 2006, 141). Kaikkia asioita ei ole kuitenkaan mahdollista tai järkevää saada paperille sopimusmuotoon tai ylläpitää pelkillä kielloilla ja säännöillä. Henkilöstöä on koulutettava ja motivoitava niin, että tietoturvasta huolehtiminen olisi oma-aloitteista eikä sääntöjen sanelemaa. On

laadittava tarvittavat seurantajärjestelmät, koulutukset, ohjeistukset ja toimitavat sekä varmistettava, että ne ymmärretään ja niitä noudatetaan. Tämä auttaa muun muassa työhönotossa, yhteistyökumppaneiden valinnassa, työtehtävien jaossa, vastuuhenkilöiden valinnoissa sekä henkilöstöturvan ylläpidossa. On myös ensiarvoisen tärkeää, että ohjeistukset ja toimitavat on laadittu lain puitteissa ja etteivät ne riko työntekijän tai yhteiskumppanin oikeuksia.

Organisaatiot kokevat myös muutoksia, jolloin työroolit voivat muuttua. Tämä voi merkitä olennaista muutosta esimerkiksi työntekijän käyttöoikeuksista erilaisiin tietoihin tai palveluihin, kuten tilanteessa, jossa työntekijä ei ole enää jäsenenä organisaatiossa tai tietyssä projektissa, mutta jolla on silti niihin tarvittavat käyttäjätunnukset, salasanat tai pääsy organisaation sähköposteihin ja intranetiin. On siis pyrittävä karsimaan turhat ja ylimääräiset käyttöoikeudet sekä välttämään ristiriitoja vanhojen ja uusien oikeuksien kesken (Laaksonen - Nevasalo & Tomula 2006, 142). Eri työtehtävissä ja oikeuksissa on huomioitava myös erilaiset vaaralliset yhdistelmät. Yksi ja sama henkilö ei saisi olla asemassa, joka antaa mahdollisuuden oikeuksien väärinkäyttöön itsensä tai läheisten tahojen hyväksi. (Opas julkishallinnon tietoturvan järjestämisestä 2003,41).

3.4 Fyysinen turvallisuus

Mahdollinen tietoturvauhka ei aina tule ulkopuolelta verkon kautta tai aiheudu käyttäjän tekemästä virheestä. Laitteistot voivat olla fyysisessä vaarassa. Laaksonen - Nevasalo & Tomula (2006, 125) listaa seuraavia vaaratekijöitä: varkaus, tulipalo tai väärä lämpötila, kosteuden aiheuttamat vahingot, sähköhäiriöt ja pöly. Varsinkin varkaudet ovat suurempi ongelma, koska työpaikoilla ja yhteisöissä käytetään paljon kannettavia tietokoneita ja muistitikkuja, joiden varastaminen tai hävittäminen vahingossa on huomattavasti helpompaa kuin perinteisten pöytäkoneiden kohdalla. Kulunvalvonta on tärkeää, jotta voidaan estää ei-haluttujen henkilöiden liikkuminen esimerkiksi toimitiloissa näin pienentäen varkauden tai muun rikkeen riskiä. Toimitiloissa olevat tietokoneet ja muut laitteet tulee myös lukita ja asettaa tarvittavat käyttäjätunnukset esimerkiksi tietokoneisiin ja puhelimiin. Muita lueteltuja fyysisiä uhkia kannattaa ehkäistä toimitiloissa jo muistakin syistä, mutta ne antavat hyvän syyn myös huolehtia tietojen varmuuskopioinnista tai oikeista laitehankinnoista. Pienetkin investoinnit tilojen yleiseen turvallisuuteen ja varmuuskopiointiin voivat säästää organisaation suurilta

menetyksiltä. Kadonnut tai tuhoutunut tieto voi olla korvaamatonta ja aiheuttaa suuria odottamattomia haittoja toiminnalle, joten varmuuskopioinnista ja muusta suojauksesta huolehtiminen on tärkeää.

3.5 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan verkoissa tapahtuvan tietoliikenteen suojaamista eri keinoilla. Näin pyritään turvaamaan tietoliikenteen jatkuvuus ja samaan aikaan huolehditaan sen salaamisesta, jolloin tietojen eheys on turvattu (Järvinen 2002, s.112). Verkoissa liikkuu suuria määriä tietoja monilla eri tavoilla ja useissa eri muodoissa. Esimerkiksi yrityksen sisäisessä verkossa olevat koneet lähettävät tietoja omassa ja ulkopuolisessa verkossa oleviin koneisiin. Tietoliikennettä voidaan suojata esimerkiksi palomuureilla tai erilaisilla salausmenetelmillä, jotka estävät tai vaikeuttavat ulkopuolisten tahojen pääsyä tietoihin. Tietoliikenteen suojaaminen on tärkeää, koska sitä koskettavat tietoturvauhat eivät rajoitu ainoastaan siihen, että tietty palvelu lakkaisi toimimasta tai häiriintyisi, vaan myös tietojen luottamuksellisuus ja eheys voivat vaarantua.

Lähes kaikki tietoturvauhat voivat tavalla tai toisella vaikuttaa tietoliikenneturvallisuuteen, ja näin ollen pelkät tekniset suojausmenetelmät, kuten yleiset koneisiin asennettavat tietoturvaohjelmistot, eivät ole välttämättä riittäviä. Onkin huomioitava erityistarpeita ja -riskejä, jotka liittyvät eri laitteisto- tai ohjelmistoratkaisuihin tai ohjeistuksiin. Käyttäjät luovat omalla toiminnallaan riskejä, joita organisaatiot voivat ehkäistä ohjeistuksilla ja säännöillä. Tietoliikenneturvallisuuden kannalta on erityisesti huomioitava sähköpostiin, Internetin käyttöön ja etäyhteyksiin liittyviä tekijöitä, kuten henkilökohtaisen käytön rajoittamista työaikana tai Internetistä ladattavien ohjelmien asennuskieltoja (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003,43).

3.5.1 Sähköposti

Sähköpostin oikeanlainen käyttö ja suojaus ovat olennaisia tietoturvan kannalta. Sähköpostia käytetään kotona sekä töissä, mutta todennäköisesti käyttöpaikasta riippumatta postissa liikkuu sekä työasioita että henkilökohtaisia viestejä. Sähköpostilaatikot voivat sisältää monenlaista tietoa, kuten tunnuksia, salasanoja, yhteystietoja, salassapidettävää tietoa ynnä muuta sellaista. Sähköpostiviestit kulkevat usein myös suojaamattomina, jolloin ne voidaan helposti kaapata ja lukea. Hyvänä nyrkkisääntönä on-

kin, ettei sähköpostin kautta pidä lähettää arkaluonteisia tietoja ja jos mahdollista, suojata viestit. Työsähköposteja käytetään myös henkilökohtaiseen viestintään, ja niillä saatetaan rekisteröityä erilaisiin vapaa-ajanpalveluihin, kuten keskustelufoorumeille. Tämä tuo riskejä, koska sähköpostiosoitteet päätyvät monille eri tahoille, jotka voivat käyttää tietoja mm. roskapostitukseen. Roskapostituksesta on puhuttu ja uutisoitu paljon viime vuosina, ja sitä on yritetty estää erilaisilla tekniikoilla ja lainsäädännöllä. Roskapostitus ei ole uhka vain sen aiheuttamien tietoturvariskien vuoksi, vaan se luo myös valtavia kustannuksia eri organisaatioille. Toisaalta itse roskapostin lähettäjälle kustannuksia ei juuri synny, koska viestien lähetys on ilmaista ja tarvitaan ainoastaan lista osoitteista ja postitusohjelma (Järvinen 2002, 236). Sähköpostiohjelmiin on rakennettu suodattimia, jotka hakevat viesteistä tiettyjä piirteitä, lähettäjiä tai sanoja, joiden perusteella määritellään, onko kyseessä aito viesti vai roskaposti. Vaikka suodattimet ovat hyvin kehittyneitä, pääsee paljon vääriä viestejä silti läpi. Organisaatioiden on hyvä pitää sähköpostiosoitteensa mahdollisimman piilossa, välttää ketjukirjeitä, ohjeistaa työntekijöitä ja huolehtia, että sähköpostiosoitteet ovat oikeassa käytössä, eikä niitä ole rekisteröity muihin palveluihin. (Laaksonen - Nevasalo & Tomula 2006, 206.)

Erilaiset ketjukirjeet, jotka yleensä sisältävät vitsejä tai runoja ovat suosittuja ja niiden mukana kulkee linkkejä, kuvia ja muita tiedostoja. Tämä tuo suuria riskejä, varsinkin kun viestien perässä monesti vielä on merkintä ”lähetä tämä myös ystävillesi”. Tämä on hyvä keino levittää haittaohjelmia, koska käyttäjät lähettävät viestit eteenpäin itse ja yleensä viestin turvallisuutta ei epäillä, jos se saapuu tuttavalta. Viestit voivat myös kuormittaa tietoliikennettä, jos ne sisältävät suuria liitetiedostoja ja niitä lähetetään paljon samanaikaisesti.

Käyttäjän oma tietämys on ehkä tärkein tietoturvaa parantava tekijä sähköpostin käytössä. Käyttäjän on itse kyettävä tunnistamaan epätavalliset ja epäilyttävät viestit ja mahdolliset huijausyritykset, kuten salasanojen kalasteluyritykset. Näitä uhkia ei pystytä tehokkaasti poistamaan minkäänlaisella teknisellä suojauksella, koska ainoastaan käyttäjä itse voi tehdä päätöksen, haluaako hän avata viestin vai ei. F-Securen vuoden 2005 yleisimpien virusten listauksessa kaikista yleisimmät virukset käyttivät useimmiten sähköpostia levityskeinona (Laaksonen - Nevasalo & Tomula 2006, 202). Jos viesti on epäilyttävä, kuten kirjoitusasussa on omituisuuksia tai pahoja virheitä, lähettäjä on tuntematon, otsikko viittaa mainontaan tai on muuten epäilyttävä, ei viestiä

kannata avata. Liitetiedostoja ei myöskään pidä avata, jos epäilee viestin aitoutta, ja liitetiedostot on hyvä aina tarkistaa virusohjelmalla. Vaikka viesti olisi saapunut läheiseltä tuttavalta tai työtoverilta, se ei takaa viestin aitoutta, koska on mahdollista, että itse lähettäjän kone on saastunut. (Muista sähköpostin käytössä 2008.) Sähköpostilaatikossa ei kannatta säilyttää viestejä, joissa on tunnuksia ja salasanoja, ja on hyvä varmistaa, että roskapostinsuodatustoiminnot ovat päällä. Käyttäjän on aina myös muistettava kirjautua ulos postista ja myös huolehdittava, ettei ohjelma ole tallentanut käyttäjätunnuksia ja salasanoja automaattista kirjautumista varten. Erilaisten yritysten ja organisaatioiden on hyvä hankkia turvalliset sähköpostiohjelmat, joiden virustorjunnasta on huolehdittu, eikä turvautua ilmaisiin tai kokeiluversioina tarjottaviin sähköpostipalveluihin.

3.5.2 Etätyö, kannettavat laitteet ja mobiililaitteiden tietoturva

Tavallisten pöytäkoneiden lisäksi on suuri määrä erilaisia laitteita, jotka mahdollistavat työnteon myös työpisteen ulkopuolella. Puhelimet ovat kehittyneet laitteiksi, jotka mahdollistavat surffauksen Internetissä altistaen näin ne samoille vaaroille kuin tietokoneetkin. Esimerkiksi puhelimet, jotka käyttävät Bluetooth-yhteyksiä ,ovat samalla lailla alttiita viruksille kuin tavalliset verkossa olevat tietokoneetkin. Langattomiin Internet-yhteyksiin kykenevien laitteiden määrä ja markkinat ovat kasvaneet. Tästä koituvat riskit on huomattu, josta kertoo muun muassa F-Securen myyntitilastot. F-Securen mukaan yritysten mobiilitietoturvaohjelmistojen myynti kasvoi jopa 80 % vuonna 2009 (F-Secure: Mobiilitietoturva kasvussa 2010). Tämän lisäksi kannettavia tietokoneita ja muita laitteita käytetään työn ulkopuolella ja yleisillä paikoilla, jolloin ulkopuoliset saattavat nähdä tärkeitäkin tietoja tai esimerkiksi perheenjäsenet saattavat hyödyntää työkonetta henkilökohtaisessa käytössä. Pieniä laitteita ja kannettavia on helppo hukata, varastaa tai särkeä ja ne ovat alttiita lukuisille fyysisille vaaroille, kuten kylmyydelle, kosteudelle, pudottamiselle, huonoille säilytystiloille ynnä muille sellaisille.

Puhelimille, muistitikuille, MP3-soittimille ja muille vastaaville voidaan myös tallentaa suuria määriä tietoa ja ne voidaan kytkeä koneisiin käytännössä missä tahansa. Riskialteinta on, että nämä laitteet ovat arkipäiväistyneet ja ovat jokaisen käytettävissä, ja valvonta ja riskienhallinta ovat vaikeita ja vaativat usein teknisiä keinoja.

Organisaatiot voivat käyttää paljon resursseja toimitilojensa koneiden ja verkkojen suojaukseen, mutta ponnistelut valuvat helposti hukkaan, jos verkkoon pääseekin viruksia työntekijän saastuneelta kotikoneelta tai työntekijä hukkaa tärkeitä tietoja sisältävän muistitikun tai kannettavan. Tietokoneet ja kännykät voidaan lukita eri keinoilla, kuten käyttäjätunnuksilla, salasanoilla, PIN-koodeilla sekä laitteisiin voidaan tehdä erilaisia merkintöjä, jotta niiden omistaja voidaan varmentaa tarvittaessa. Tallennettuja tietoja ja kokonaisia laitteita voidaan myös salata käyttäen erilaisia ohjelmistoratkaisuja.

Tietoliikenne tapahtuu monesti langattomien etäyhteyksien kautta, joiden suojauksesta ja oikeanlaisesta käyttötavasta on huolehdittava. Etätyö ja mukana kulkevat laitteet tuovat siis paljon mahdollisuuksia, mutta samaan aikaan myös paljon riskejä. Vaikka etätyömahdollisuuksia ei tietoisesti hyödynnettäisikään, käyttää moni työntekijä esimerkiksi yrityksensä sähköpostia tai muita palveluita kotoa tai muualta käsin, ja organisaation sisäinenkin tietoliikenne voi tapahtua langattomien yhteyksien kautta.

Jos mahdollista, etäyhteyksiä käyttäville laitteille on hyvä asettaa tietyt vähimmäisasetukset. Käytännössä, kun toinen laite yrittää muodostaa yhteyttä, tarkistetaan esimerkiksi, onko yhteyttä ottava laite päivitetty ja suojattu asetuksien vaatimilla tavoilla. (Laaksonen - Nevasalo & Tomula 2006, 226.)

Langattomia verkkoja ylläpitävät tukiasemat eivät ole välttämättä suojattuja, jolloin ulkopuoliset tahot voivat teoriassa seurata kaikkea koneella tapahtuvaa tietoliikennettä. Useilla paikoilla, varsinkin kaupunkialueilla, voi suojaamattomia yhteyksiä olla saatavilla runsaasti, ja kuka tahansa voi käyttää niitä. Moni käyttäjä ei ole tästä tietoinen tai ei välitä, jos hänen omistamaansa verkkoa käyttää ulkopuolinen. Vaarana on aina, että ulkopuolinen taho käyttää verkkoa laittomuuksiin. Verkkojen ja tietoliikenteen suojauksesta ja salauksesta pitää huolehtia. Voidaan käyttää esimerkiksi salausavainta, jota kysytään aina, kun kone ottaa yhteyden langattomaan tukiasemaan. Jos ulkopuolinen taho ei tiedä oikeaa avainta, ei yhteyttä pystytä avaamaan. (Langattoman verkon tietoturva kuntoon 2009.)

3.6 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan tietojenkäsittelyyn käytettävien laitteiden toimintakyvyn varmistamista sekä varautumista mahdollisiin uhkatekijöihin, jotka voivat

heikentää laitteiston toimivuutta (Järvinen 2002, 112). Laitteistoturvallisuudesta huolehtiminen alkaa jo hankintavaiheessa, jolloin on huomioitava takuuajat, huoltosopimukset sekä laadunvarmistus. Jotta käytettävyys ja toimivuus voidaan turvata, on ylläpidon lisäksi hyvä ohjeistaa käyttäjiä laitteiden oikeanlaiseen käsittelyyn ja toiminnan seuraamiseen. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003,47.)

Käyttäjien on hyvä huolehtia tietyistä perusasioista. Tietokoneet ja muu elektroniikka on hyvä pitää poissa pölyisistä tai kosteista paikoista ja säilyttää lukituissa tiloissa. Laitteita on käsiteltävä oikein, kuten vältettävä turhaa virran päälle jättämistä tai huolimatonta käsittelyä. Koneet ja muut laitteet on myös aseteltava oikein, kuten ottamalla huomioon koneiden kuumeneminen ja tuuletustarpeet. Monet käyttäjät tuovat mukanaan lukuisia henkilökohtaisia laitteita, kuten kännyköitä, MP3-soittimia tai muistitikkuja, jotka voidaan liittää organisaation koneisiin. Mahdollisten haittaohjelmien lisäksi henkilökohtaiset laitteet voivat aiheuttaa muitakin ongelmia, jos ne ovat esimerkiksi vaurioituneita, asentavat omia ohjelmistojaan tai sisältävät haittaohjelmia. Jos laitteissa alkaa ilmetä erilaisia vikoja, kuten sähköongelmia tai omituisia ääniä tai muita vastaavia, on laitteiden huollosta vastaavia tahoja informoitava. Pieni helposti korjattavissa oleva vika voi tulla kalliiksi, jos siitä ei ilmoiteta ajoissa. Laitteistoturvallisuus on olennainen tietoturvan osa-alue jokaisessa organisaatiossa, koska tietojen käytettävyys sekä eheys voivat vaarantua toimintakatkosten tai hajoamisten yhteydessä.

3.7 Ohjelmistoturvallisuus

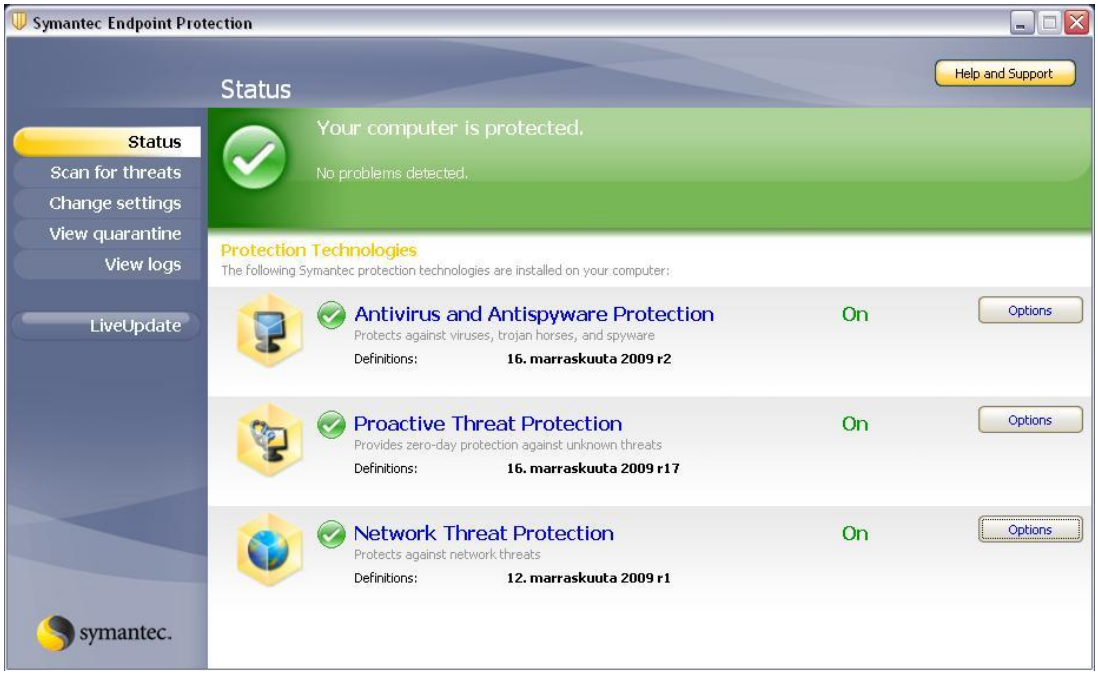
Ohjelmistoturvallisuudella tarkoitetaan tietojenkäsittelyyn käytettävien laitteiden ohjelmistojen suojaamista. Tähän liitetään myös ohjelmistojen käytettävyyteen liittyviä seikkoja, kuten ohjelmistojen yhteensopivuus, päivitys, rekisteröinti tai mahdolliset käyttölisenssit. Näitä tekijöitä huomioimalla voidaan ehkäistä laittomien ohjelmistojen käyttöä ja levitystä sekä saada parempi varmuus ohjelmistojen laatutasosta ja toimivuudesta. (Järvinen 2002, 113.)

Hankittavien ohjelmien tulee olla luotettavia eli organisaatioiden kannattaa käyttää maksullisia ja laadukkaita ohjelmia ja välttää ilmaisversioiden tai Internetistä saatavien vähemmän tunnettujen tai laittomasti ladattujen ohjelmien käyttöä. Monet ilmaisversiot voivat olla tarkoitettuja ainoastaan yksityisille käyttäjille tai kokeiluversioiksi

ja voivat sisältää haittaohjelmia. Esiin voi nousta myös yhteensopivuusongelmia, jos tietyt ohjelmat eivät osaa toimia yhteiskäytössä muiden tai vanhempien ohjelmien kanssa. Monella työpaikalla voi esimerkiksi olla ongelmallista, kun uudella Wordilla tuotetut asiakirjat eivät välttämättä avaudukaan vanhemmissa versioissa uusien ominaisuuksien vuoksi. Erityisen tärkeää on huolehtia, että ohjelmat päivitetään ja mikään toinen ohjelma ei estä tai häiritse päivitysprosessia. Huolestuttavaa on, että monet ohjelmat saatetaan julkaista nykyään lähes keskeneräisinä ja puuttuvat ominaisuudet ja haavoittuvaisuudet korjataan päivityksillä myöhemmin. Ohjelmistoturvallisuutta pitääkin jo ajatella hankintavaiheessa, jolloin on hyvä huomioida yhteensopivuus, lisenssit, ohjelmistojen päivitettävyys ja mahdollinen tekninen tuki (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003,47). Esimerkiksi yrityksen hankkiessa uuden taloushallinto-ohjelman on hyvä varmistaa, että se on yhteensopiva nykyisten ohjelmien kanssa, ohjelmalle löytyy mahdollisuus tekniseen tukeen ja ohjelma voidaan tarvittaessa päivittää tai sen sisältämät tiedot siirtää seuraavaan ohjelmaan.

Ajan tasalla olevat virustorjuntaohjelmat ovat elintärkeitä niin tavalliselle yksityiselle käyttäjälle kuin mille tahansa organisaatiollekin. Virustorjuntaohjelmat pyrkivät etsimään erilaisia tunnettuja haittaohjelmia, jolloin niiden toiminta voidaan estää eri tavoilla, kuten tunnistamalla virus tiedostosta ennen kuin käyttäjä edes avaa itse tiedoston tai etsimällä jo olemassa olevia viruksia laitteilta tai muilta talletusvälineiltä. Virus voidaan tällöin poistaa, asettaa karanteeniin tai havainnosta voidaan vain informoida käyttäjää. Virusohjelmia löytyy suuri valikoima eri tarpeisiin. Yksityiset käyttäjät löytävät todennäköisesti toimivia ilmaisversioitakin, jotka antavat riittävän tietoturvan tason, jos niiden lisäksi järjestelmä on muuten ajan tasalla ja suojattu käyttäen esimerkiksi turvallisia selaimia, sähköpostiohjelmia ja haittaohjelmien poisto- ja havaitsemistyökaluja. Tavallisen käyttäjälle on vaivaton vaihtoehto ostaa tietoturvapaketti, joka sisältää kaikki tarvittavat ohjelmat ja on helppo asentaa ja hallinnoida. Ohjelmien käyttölisenssit on yleensä uusittava maksullisesti tietyin väliajoin, jonka vuoksi moni käyttäjä tukeutuukin heikkoihin ilmaisohjelmiin tai käyttää järjestelmiä ilman suojausta. Yrityksille virusohjelmat ovat käytännössä pakkohankinta, ja monet tarjoajat myyvät omia yrityksille suunnattuja pakettejaan. Kaikki virustorjuntaohjelmat eivät ole ainoastaan virusten havaitsemista ja poistoa varten, vaan ne osaavat myös etsiä muita haittaohjelmia, suodattaa sähköpostia tai niihin on rakennettu oma palomuurinsa. Palomuurien tarkoitus on hallinnoida koneiden välistä tietoliikennettä estäen ei-haluttuja yhteydenottoja ja tunkeutumisyrityksiä.

Onkin siis pyritty sitomaan ohjelmistopaketit yhdeksi kokonaisuudeksi, joka pienentää kuluja ja vähentää riskejä eri ohjelmien yhteiskäytöstä aiheutuvista ristiriitatilanteista. Ohjelmat on rakennettu erittäin käyttäjäystävällisiksi ja suurin osa toiminnoista on automatisoitu. Tämä tarkoittaa, että ohjelmat osaavat yleensä pitää omat tietonsa ajan tasalla eli ne päivittävät jatkuvasti tietokantojaan tunnetuista uhista sekä haavoittuvaisuuksista. Kehittyneemmät ja usein myös maksulliset versiot eivät vaivaa käyttäjää, vaan pyörivät taustalla älykkäästi valikoiden esimerkiksi sallittavat ja estettävät yhteydenotot eri ohjelmien kesken tai verkossa. Yksityiset käyttäjät, jotka turvautuvat ilmaisversioihin, joutuvat yleensä hakemaan erikseen virusohjelmat, palomuurit ja muut tietoturvaohjelmistot, joiden taso voi olla kyseenalainen. Monet eri Internetissä toimivat palvelut voivat tarjota eritasoisia virustestejä omilla palvelimillaan. Esimerkiksi Hotmail-sähköposti palvelu tarkistaa posteja ja liitetiedostoja haittaohjelmien varalle, mutta on täysin eri asia, riittääkö ilmaisen palvelun tarjoama tietoturvan taso yrityskäyttöön.



Kuva 1. Symantec Endpoint tietoturvaohjelmiston päävalikko. Valikko on myös tavalliselle käyttäjälle helppolukuinen ja -käyttöinen sekä ohjelma sisältää virustorjunnan lisäksi palomuurin ja muita ominaisuuksia.

Virustorjuntaohjelmistot eivät anna täydellistä suojaa, koska aina löytyy tapoja ohittaa suojaukset tai hyödyntää järjestelmien heikkouksia. Viat eivät ole vain virusohjelmissa, vaan käyttöjärjestelmissä. Käyttöjärjestelmistä, kuten Windowsista, löytyy lukuisia haavoittuvaisuuksia. Suurin osa koneista käyttää sen valmistajan, Microsoftin, ohjel-

mistoja, jonka vuoksi suurin osa haittaohjelmista on suunniteltu nimenomaan Windows-käyttöjärjestelmiin. Muut järjestelmät voivat sisältää yhtä lailla haavoittuvaisuuksia, mutta käyttäjämäärät ovat huomattavasti pienemmät, jonka vuoksi heikkouksien hyödyntäminen ei ole yhtä kannattavaa.

3.8 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan tietoja ja niitä sisältävien järjestelmien tunnistusta, luokittelua ja valvontaa käsittelyn eri vaiheissa. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003, 49.) Tiedot on hyvä luokitella esimerkiksi julkisiksi, organisaation sisäisiksi, luottamuksellisiksi tai salaisiksi (Järvinen 2002, 113). Ilman minkäänlaista luokittelua suurten tietomäärien hallinta muuttuu erittäin vaikeaksi ja epäluotettavaksi. Luokittelun avulla tiedot voidaan tunnistaa ja niiden käsittelyyn voidaan laatia selkeät toimintaohjeet.

Tietoja liikkuu tulosteina, sähköpostitse, viesteinä, muistitikuilla, levykkeillä ja muilla tavoilla. Kun organisaatiossa käsitellään arkaluonteisia tietoja, on tärkeää huolehtia, että niitä käsitellään asianmukaisesti, jotta tietojen eheys ja luottamuksellisuus säilyvät. Oikeanlaisella käsittelyllä voidaan ehkäistä tahattomia tietovuotoja tai estää ulkopuolisten asiaton pääsy tietoihin. Erilaisia käsittelyn vaiheita voivat olla uusien tietojen luominen, tallennus, tietojen arkistointi tai tuhoaminen. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003, 49.) On tärkeää huomioida myös eri tavat, joilla tietoa tallennetaan ja miten tietoa lähetetään. Esimerkiksi sähköpostilla ei kannatta lähettää salaisia asiakirjoja ja luottamuksellisia tietoja ei pidä tallentaa suojaamattomille laitteille.

3.8.1 Varmuuskopiointi

Tietojen varmuuskopiointi on ensiarvoisen tärkeää. Jos verkonsuojaus pettää tavalla tai toisella, voi tärkeitä ja jopa korvaamattomia tietoja vuotaa, tuhoutua tai joutua väärien tahojen käsittelyyn. F-Securen teettämän kyselyn mukaan, joka toteutettiin yli 40 eri maassa, paljastui että ainoastaan 5 % vastanneista teki varmuuskopioita, vaikka samaan aikaan yli 40 % vastaajista ilmoitti menettäneensä tärkeitä tiedostoja tai muuta aineistoa erilaisten ongelmatapausten yhteydessä (Varmuuskopioi tiedostosi 2009). Varmuuskopioinnissa voivat peruskäyttäjät turvautua muistitikkuihin, DVD-levyihin, erillisiin kiintolevyihin, verkkoasemiin ynnä muihin sellaisiin. Tapoja tietojen säilyt-

tämiseen on lukuisia. Muistitikut, levyt, kannettavat kovalevyt ja muut sellaiset voivat kuitenkin helposti hukkua ja ne voidaan varastaa, hukata tai ne vaurioituvat helposti. Hyvä keino onkin tallentaa tietoja toiselle kiintolevylle, esimerkiksi toiselle tietokoneelle. Organisaatioiden suuremmat tietokannat vaativat yleensä erityistoimenpiteitä ja -keinoja sekä varmuuskopioinnin automatisointia. Varmuuskopiot on järkevä myös säilyttää turvallisessa paikassa minimoiden riskit esimerkiksi varkauksista tai muista fyysisistä uhista. Yrityksissä ja organisaatioissa, joiden koko toimeentulo saattaa perustua esimerkiksi asiakastietokantoihin tai luottamuksellisten tietojenkäsittelyyn, ei ole yleensä varaa hukata tietoja. Säännöllisen varmuuskopioinnin lisäksi on myös testattava, että kopioidut tiedostot ovat käyttökelpoisia ja noudettavissa, koska tiedostot voivat korruptoitua tallennuksen aikana tai tiedostot ovat muista syistä palauttamattomissa. Asennetuista ohjelmista kannattaa myös pitää palautuslevyjä, koska niiden asentaminen tyhjältä pohjalta voi olla hyvinkin vaikea prosessi, jossa vaaditaan ulkopuolista apua.

Tietoja voidaan myös varmuuskopioida erillisille palvelimille tietyin väliajoin ja palvelimien ylläpito ulkoistetaan tai hoidetaan itse. Omien varmuuskopiopalvelimien ylläpito voi olla kallista ja vaatia erityisosaamista ja niiden säilytystiloista on huolehdittava aiemmin lueteltujen fyysisten uhkien vuoksi. Esimerkiksi F-Secure tarjoa omaa Backup-palveluaan, jossa yritys tai muu organisaatio lähettää verkon kautta varmuuskopioitavia tietoja F-Securen tietokantaan, ja näin varmuuskopioiden ylläpito on ulkoistettu (Varmuuskopioi tiedostosi 2009).

3.8.2 Tietojen tuhoaminen

Tietoja tallennetaan monenlaisiin laitteisiin, kuten CD- ja DVD-levyille, muistitikuille, kiintolevyille, magneettinauhoille ja muille sellaisille. Tallennukseen käytettyjä laitteita saatetaan myydä tai hävittää monista eri syistä, jolloin ne voivat päätyä monille eri tahoille, kuten uudelle omistajalle, jälleenmyyjälle tai hävityspalvelulle. Laitteita yleensä myydään ja hävitetään, kun tekniikka alkaa vanhentua ja tehdään uusia hankintoja. Monesti myös tallennukseen käytettävät laitteet tai muut välineet ovat saavuttaneet täyden käyttöikänsä, kuten DVD-levy tai kiintolevy joka on hajonnut tai jota on käytetty niin paljon, ettei sen toimivuuteen enää voida luottaa. (Securely Removing Data 2010.) Tärkeää on, ettei laitteen haltuunsa saava taho pysty noutamaan vanhoja

tietoja laitteista. Tämän vuoksi on tärkeää huolehtia, että tallennusvälineet tuhotaan tai puhdistetaan.

Jos halutaan huolehtia, että tiedot tuhoutuvat varmasti, kannattaa CD- ja DVD-levyt, levykkeet, muistitikut ja kiintolevyt tuhota huolellisesti esimerkiksi vaurioittaen DVD-levy lukukelvottomaksi. Vaikka laite olisi jo valmiiksi hajonnut, kannattaa se silti tuhota kunnolla, koska ei ole takeita, ettei toinen taho pystyisi halutessaan noutamaan tietoja eri keinoin. Ei pidä unohtaa, että koneilta yleensä myös printataan tietoja paperimuotoon, joiden oikeanlainen hävitys on yhtä tärkeää. Tapauksissa, joissa laitteita myydään eteenpäin tai tallennusvälineitä tullaan käyttämään uudelleen, kannattaa turvautua ohjelmiin, jotka on suunniteltu datan oikeaan poistamiseen, jolloin tiedot hävitetään, niin ettei niitä voida enää noutaa uudelleen. Erilaisten organisaatioiden ja yritysten kannattaakin turvautua ulkopuolisiin yrityksiin, jotka ovat erikoistuneet tietojen hävitykseen ja laitteiden puhdistamiseen. Moni käyttäjä ei välttämättä ymmärrä, että tiedot ovat yhä noudettavissa, vaikka ne olisikin poistettu roskakorista tai tietokone on formatoitu. Poistetut tiedostot muuttuvat vain käyttämättömäksi tilaksi, kunnes niiden yli kirjoitetaan.

Tietojen ja laitteiden oikeanlaisesta hävityksestä ja tyhjentämisestä huolehtiminen on oleellinen osa tietoturvaa. Esimerkiksi jos yritys myy vanhoja koneitaan eteenpäin ja ei huolehdi niiden tyhjentämisestä, voi ostaja päästä käsiksi hyvinkin arkaluonteisiin tai salassapidettäviin tietoihin. Tämä on huomioitava varsinkin julkishallinnossa tai muissa organisaatioissa, joissa käsitellään henkilötietoja, ja tietokoneet ja muut laitteet voivat olla useiden eri ihmisten ja osastojen käytössä.

Monet eri ohjelmat, kuten Internet-selaimet, tallentavat tietoja käytön yhteydessä. Kun ohjelma lataa koneen muistiin esimerkiksi kuvia, evästeitä tai muita tiedostoja, ei niitä tarvitse ladata enää uudelleen seuraavan käyttökerran yhteydessä, jolloin käyttö on nopeampaa. Tällöin koneelle jää paljon tietoja, joista osa voi olla tarpeetonta tai vastakohtaisesti sisältää tärkeitäkin yksityiskohtia käyttöhistoriasta tai muista tiedoista, joita mahdolliset haittaohjelmat tai muut tahot voivat hyödyntää eri tavoilla. Jos kone on yleisessä käytössä, käyttöhistoria ja muut tiedot on hyvä poistaa jo pelkästään käyttäjän yksityisyyden kannalta, mutta välillä koneelle jää vain tilaa tai käyttötehoja vieviä turhia ohjelmia ja tiedostoja, jotka voivat luoda riskejä. Onkin hyvä huolehtia, että eri ohjelmat eivät kerää turhaan tietoja tai kerätyt tiedot ja väliaikaistiedostot tulisi

poistaa tietyin väliajoin. Moni ohjelma tarjoaakin usein erilaisia vaihtoehtoisia asetuksia tiedostojen keräämiseen, säilytykseen tai poistamiseen. Taustalla pyörii monesti myös ohjelmia, joita tavallinen käyttäjä ei edes huomaa, joten kokonaiskuvan hahmottaminen kaikista tietoja keräävistä ohjelmista voi olla haastavaa. On olemassa erilaisia työkaluja, jotka mahdollistavat esimerkiksi useiden eri ohjelmien käyttöhistorioiden, turhien väliaikaistiedostojen ja rekisterimerkintöjen poistamisen.

Tietoja myös usein poistetaan tai hävitetään vahingossa. Välillä kadonnut tiedosto voi löytyä väliaikaistiedostona, roskakorista tai vain väärästä kansiosta etsi-toiminnon avulla. Toisaalta tiedosto voi olla oikeasti poistettu tai laite on voinut vaikkapa vaurioitua. Tällöin on hyvä turvautua erilaisiin ohjelmiin, jotka on kehitetty poistettujen tietojen palauttamiseen, ja on olemassa myös yrityksiä, jotka tarjoavat tietojen palautuspalveluita.

3.9 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan tietojenkäsittelyyn käytettävien laitteiden päivittäiseen toimivuuteen vaikuttavia toimenpiteitä, kuten laitteiden ylläpitoa, käyttöä, huoltoa ja valvontaa (Järvinen 2002, 112). Käyttöturvallisuus koskettaa lähes kaikkia tietojenkäsittelyyn käytettäviä laitteita, verkkoja, ohjelmistoja ja järjestelmiä. Tämä ei tarkoita, että käyttöturvallisuus olisi ainoastaan teknisen tuen tai ATK-vastaavien huolehdittavana, koska organisaatioiden tavalliset työntekijät ovat myös vastuussa monista eri käyttöturvallisuutta koskettavista osa-alueista. Organisaation on kyettävä valvomaan ja havainnoimaan mahdollisia tietoturvaa uhkaavia tekijöitä ja tapahtumia, mutta itse käyttäjienkin on tunnettava omat vastuualueensa ja velvollisuutensa.

Eri organisaatioissa on huolehdittava, että käyttäjät ovat tietoisia, miten toimintaa valvotaan ja miten tulee toimia ongelmatilanteissa, esimerkiksi kenelle ja miten raportoidaan mahdollisesta tietoturvauhasta. Käyttäjien on tiedettävä omia tehtäviään koskettavista tietoturva-asioista, kuten omien käyttäjätunnuksien, PIN-koodien ja salasanojen oikeanlaisesta käsittelystä. Käyttäjien tietämyksen tukemiseksi eri organisaatioiden onkin hyvä laatia käyttöohjeita, hyvät tiedotuskanavat ja -menetelmät sekä selkeät tehtävänkuvaukset, jotka pitävät sisällään vastuualueet. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003, 52.)

Salasanojen hallinnointi on hyvin tärkeä osa-alue, koska työntekijät, kuten myös tavalliset kotikäyttäjätkin, joutuvat käsittelemään, laatimaan ja hallinnoimaan useiden eri ohjelmien ja palveluiden salasanoja. Käyttäjät joutuvat myös muistamaan useita eri salasanoja, usein myös palveluihin, joita ei käytetä kuin harvoin. Tämän lisäksi salasanat voivat olla hankalia muistaa ja vaihtua usein. Moni kokenutkin käyttäjä saattaa tämän vuoksi tehdä helposti vältettävissä olevia virheitä. Yleistä on käyttää samoja salasanoja monissa eri palveluissa, ja salasana voi olla liian yksinkertainen ja helposti arvattavissa. Pahimmissa tapauksissa käyttäjän salasana voi olla hänen itsensä tai läheisensä nimi tai käytettävän ohjelman, palvelun tai laitteen alkuperäistä oletussalasanaa ei ole välttämättä edes vaihdettu.

Hyvän salasanan on oltava ainakin kahdeksan merkkiä pitkä sekä sisältää erikokoisia kirjaimia, numeroita ja symboleita. Salasanan ei myöskään pidä muistuttaa oikeita tai yleisesti tunnettuja sanoja, joita on helppo arvata tai etsiä esimerkiksi sanakirjoista. (Hyvät salasanat: luominen ja käyttäminen 2006.) Hyvästä salasanasta ei ole hyötyä, jos käyttäjä ei itsekään kykene muistamaan sitä, jonka vuoksi moni joutuu kirjaamaan ylös omia salasanojaan. Ylöskirjoitetut tunnukset, salasanat ja muut vastaavat on säilytettävä turvallisissa paikoissa.

Työntekijöitä on hyvä ohjeistaa valitsemaan mahdollisimman vahvoja salasanoja, välttämään niiden luovuttamista ja ylöskirjaamista sekä vaihtamaan ne tietyin väliajoin. Salasanojen paljastuminen ja vuotaminen ja siitä aiheutuvat ongelmat, kuten tunkeutujan pääsy järjestelmään, ovat kuitenkin niin suuri riski, että on tapauskohtaista, voidaanko luottaa työntekijöiden tunnollisuuteen salasanojen hallinnassa. Jos mahdollista, on kannattavaa pakottaa käyttäjät teknisillä keinoilla laatimaan vahva salasana. Tämä onnistuu esimerkiksi käyttämällä ohjelmia, jotka vaativat uuden, tietyt vaatimukset täyttävän salasanan, tietyin väliajoin.

4 TIETOTURVAKOULUTUS

4.1 Koulutuksen ja ohjeistusten tarve

Henkilöstön tietoturvakoulutuksen tarve voi olla hyvin tapauskohtaista. Koulutus on hyvä pitää esimerkiksi, jotta henkilöstö olisi ajan tasalla yleisistä asioista tai jos organisaatiossa on tapahtunut suuri muutos, kuten uuden järjestelmän hankinta tai eri prosessien muuttaminen sähköiseen muotoon. Koulutuksen tulisi kattaa perustason asiat,

kuten turvallinen Internet-selaus, sähköpostin tietoturvallisuus ja muut vastaavat arkipäiväisessä työskentelyssä vaikuttavat osa-alueet. Koulutuksen järjestämisessä on hyvä huomioida, mikä on koulutettavien osaamistaso ja vastuualueet. Tietoturvakurssi voidaan järjestää koko henkilökunnalle, yksittäisille kouluttajille tai tiettyjen osastojen henkilöstölle. Kurssien sisällön täytyy olla ymmärrettävää, selkeää ja ohjeistavaa, koska tietotekniikan tuntemus voi usein olla todella vaihtelevaa. Ihanteellista olisi saada tietoturvasta jonkinlainen yleinen käsite ja toimitapa, eikä vain kieltoja sisältävä säännöstö. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003,55.) Jokainen organisaatio, joka harjoittaa liiketoimintaa sähköisessä muodossa, tarvitsee tietoturvaosaamista. Tietoturvan hallinta ja sen parantaminen organisaatiossa ei ole kannattavaa ainoastaan riskienhallinnan vuoksi, vaan se on myös kilpailuetu, koska asiakkaat tai muut sidosryhmät voivat kokea ja saada suurta lisäarvoa yhteistyöstä ja palveluiden tuottamisesta, jos tietoturva on hoidettu hyvin. Eri organisaatioille on olemassa erilaisia tietoturvasertifikaatteja, jotka kertovat tietoturvan tason ja miten se on hoidettu yrityksissä, ja viestivät siitä ulkopuolisille. Kilpailuedun tai turvallisuuden parantamisen lisäksi laki velvoittaa useilla eri tasoilla huolehtimaan tietoturvasta.

4.2 Koulutuksen järjestäminen

Koulutusta järjestettäessä on huomioita ajan tarve, koska tiettyjen aihepiirien läpikäyminen voi viedä useita tunteja. Toisaalta pidettäessä perustason koulutusta, voi osallistujien oppiminen kärsiä, jos koulutuksen kesto on liian pitkä. Esitysmateriaaliksi on hyvä tehdä erilaisia esityksiä hyödyntäen esimerkiksi PowerPointia sekä laatia muuta jaettavaa lisämateriaalia. Koulutettavien taso tulee huomioida jo koulutuksen suunnitteluvaiheessa tarkasti. Materiaalin pitää olla oikein suunnattua ja helppolukuista. Jos kyseessä on toimistotyöntekijöiden perustietoturvakoulutus, ei kannata sisällyttää kovin teknisiä tai vaikeasti ymmärrettäviä käsitteitä koulutukseen, vaan pysytään perusasioissa, kuten turvallisessa nettiselaamisessa tai sähköpostin tietoturvassa. Toisaalta, jos koulutettavat edustavat jonkinlaista tietotekniikan asiantuntijaryhmää, voi materiaali olla hyvinkin syvällistä ja sisältää paljon tarkempia ja monimutkaisempia asioita, joita voidaan tukea erilaisilla asiantuntijaluennoilla. Voidaan myös miettiä, onko mahdollista järjestää koulutus vain organisaation tietoturvavastuuhenkilöille, jotka voivat siirtää oppimansa tiedot muille työntekijöille töiden lomassa.

Kirjoja tai muuten pitkiä koulutusmateriaalien käyttöä kannattaa välttää ja yrittää saada koulutettavat ymmärtämään asiat käytännön esimerkkien avulla niin, ettei ole tarvetta laatia laajasisältöisiä opaskirjoja tai ohjeistuksia työpisteisiin myöhemmin. Tietoturvaohjeet on hyvä laatia lyhyehköön ja nopealukuiseen paperimuotoon, jolloin ohjeistukset voidaan kiinnittää esimerkiksi työpisteen seinälle.

Olisi ihanteellista, jos koulutuksesta saadaan viihtyisä ja hauska tapahtuma, jolloin ihmiset saadaan osallistumaan ja oppimaan paremmin. Yritetään siis saada tietoturvasta automaattinen toiminta- ja ajattelutapa ilman, että se olisi vain ulkomuistista tulevaa pakosti noudatettavaa säännöstöä.

Koulutuksessa voidaan jakaa myös esimerkiksi julisteita, mukeja, hiirimattoja tai muita sellaisia, jotka jäävät käyttöön ja muistuttamaan opitusta myöhemmin. Kannattaa myös laatia erilaisia harjoitustehtäviä, jotta koulutettavat kertaavat oppimaansa ja saavat palautetta osaamisestaan välittömästi. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003, 56.)

Koulutustilaisuuteen kannattaa varata luennointiin sopivat tilat, joissa on mahdollisuus käyttää projektoria. Luennon alkuun on hyvä sisällyttää teoriaosuus, jossa kurssinvetäjä käy läpi koulutuksen tavoitteet ja yleistä teoriaa tietoturva-aiheesta. Osallistujat tulisi saada mukaan mahdollisimman nopeasti, joten ajan ja resurssien puitteissa kannattaa pitää jonkinlainen keskustelutuokio, jossa osallistuja kertoo osaamisestaan ja ongelmistaan tai täyttää kyselylomakkeen. Koulutuksen aikana kannattaa järjestää erilaisia yksilö- ja ryhmätehtäviä. Kurssista ei pidä tehdä liian virallista tai arvostella osaamista, vaan rohkaista ja motivoida ihmisiä omaksumaan tietoturva-ajattelu toimitapana ja käytäntönä, eikä vain johdon laatimana tiukkana säännöstönä. Kurssin lopussa voidaan jakaa erilaiset oheismateriaalit, mutta tärkeää on myös jakaa palautelomakkeet, jolloin koulutusta voidaan kehittää myöhemmin. Ennen kurssin järjestämistä olisi ihanteellista resurssien puitteissa kerätä kyselylomakkeilla tietoa henkilöstön osaamisasteesta tietoturva-asioissa, jolloin kurssin sisältöä voidaan muokata ja kohdistaa paremmin aihepiireihin, joissa koulutusta tarvitaan. Johdon osallistuminen koulutuksen suunnitteluun on ensiarvoista, jotta koulutus voidaan kohdistaa tarvittaviin osa-alueisiin.

Jos kyseessä on tilanne, jossa otetaan käyttöön esimerkiksi uusia järjestelmiä tai tapahtuu muita muutoksia, jotka vaikuttavat tietoturvaosaamisen tarpeeseen, on kurssin

pitämisen ajoitus tärkeää. Koulutus menettää arvonsa, jos se pidetään liian etuajassa, jolloin ihmiset unohtavat oppimiaan asioita. Välillä taas koulutusta järjestetään tilanteessa, jossa järjestelmät on jo otettu käyttöön tai muutokset ovat jo tapahtuneet. Tämä voi luoda huonoa ilmapiiriä, koska työntekijät eivät osaa käyttää järjestelmiä ja tuntevat tarvetta saada koulutusta aiheesta. Riskit lisääntyvät myös, koska työntekijät tekevät virheitä tai omaksuvat vääriä toimitapoja, ja voivat näin aiheuttaa erilaisia uhkatilanteita. Vääristäkin toimitavoista voi olla vaikea päästä eroon koulutuksella, jos henkilöstö on kerinnyt jo omaksua ne arkipäiväiseen rutiiniinsa.

5 TIETOTURVAKOULUTUS KOUVOLAN LÄÄKÄRIASEMALLE

5.1 Koulutuksen tavoitteet ja toteuttamistavat

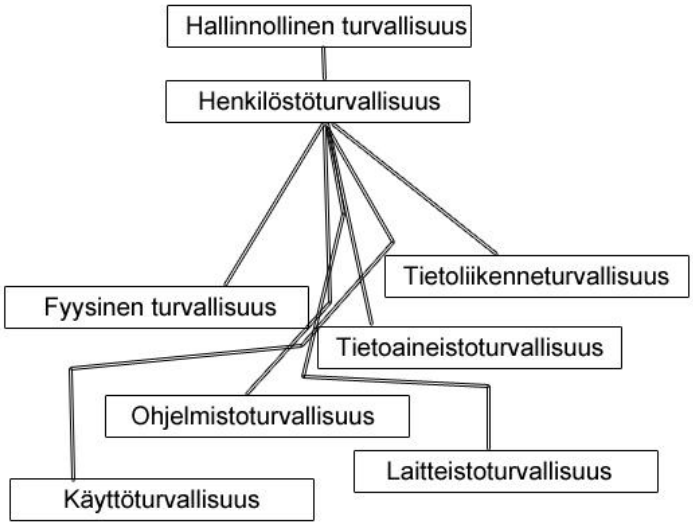
Tavoitteena on luoda koulutus, jossa käydään läpi tietoturvan perusasiat kertomalla erilaisista uhista, käsitteistä ja turvallisemmista toimitavoista. Kohderyhmänä ovat perustason käyttäjät, joten ei ole mielekästä käsitellä aihepiiriä liian yksityiskohtaisesti tai tarkastella sitä teknisestä näkökulmasta. Koulutusta ei ole myöskään erikseen suunnattu Lääkäriaseman henkilökunnalle, vaan aihepiiri käsittelee yleisesti tietoturvaa. Koulutuksen kestoksi on arvioitu noin kolme tuntia harjoituksineen ja keskusteluineen.

Koulutuksessa käsitellään tietoturvaa lähinnä peruskäyttäjän näkökulmasta, mutta jonkin verran myös hallinnon puolelta. Koulutustapana on luennointi, jota tuetaan koulutusmateriaalilla (Liite1). Koulutusta varten on myös kerätty Internetistä useita eri uutisartikkeleita, jotka kertovat käytännön esimerkkitapauksista. Monia aihepiirejä käsitellään hyvin vapaasta näkökulmasta ja mahdollisimman helposti ymmärrettävin tavoin. Koulutuksen vapaamuotoisuuden vuoksi ei ole järkevää kirjata kaikkea käsiteltävää tietoa materiaaliin, koska pitää myös huomioida mahdolliset esiin tulevat keskustelut sekä kysymykset, jotka vaativat usein aihepiiristä poikkeamista tai tietyn odottamattoman asian läpikäymistä. Koulutusmateriaali jaetaan koulutettaville, mutta tarkoituksena ei ole ollut laatia ohjekirjaa tai tarkkoja ohjeistuksia työpaikalle, vaan antaa yleisaiheinen tiivistelmä, joka sopii monelle käyttäjälle tai erilaisille organisaatioille. Lisäksi koulutettaville jaetaan täytettäviksi palaute- ja tehtävälomakkeet (Liite 2, liite 3).

5.2 Koulutuksen sisältö ja lisämateriaalit

Koulutusta varten laadittiin 24 sivua käsittävä koulutusmateriaali (Liite 1). Materiaalin sisältö on poimittu suurimmaksi osaksi opinnäytetyöstä tai sen tekoon käytetyistä lähteistä sekä osittain kirjoittajan omista tiedoista. Materiaalin laatiminen oli aikaa vievää, koska oli haastavaa päättää, mitä aiheita kannattaa sisällyttää perustason koulutukseen ja kuinka tarkasti. Suurin osa materiaalista jouduttiin kirjoittamaan tai muotoilemaan uudelleen, joten suorat lainaukset opinnäytetyöstä eivät olleet useinkaan mahdollisia. Koulutus alkaa pienellä kyselytuokiolla, jossa tiedustellaan koulutettavien kokemuksia tietoturva-asioista ja pyritään etsimään niistä keskustelunaiheita. Aloituksen jälkeen koulutus on jaettu kahteen eri pääosioon. Ensimmäinen osio käsittelee tietoturvaa käsitteenä eli käydään läpi yleisiä termejä ja asioita: mitä tarkoitetaan viruksilla, mitä ovat madot tai miten tietoturva määritellään ja miten se on yleisesti jaoteltu eri osa-alueisiin. Osa-aluemäärittelyt on laadittu opinnäytetyön käyttämien määritelmien mukaisesti, jotka pohjautuvat valtionhallinnon eri ohjeisiin. Osa-alueista kertomalla saadaan koulutettaville selkeä kuva, mistä tietoturva koostuu. Eri käsitteitä ei ole vain selitetty, vaan niistä on pyritty myös tekemään erilaisia esimerkkejä. Eri kohdissa esitetään Internetistä etsittyjä tietoturva-aiheisia uutisia, joiden tarkoituksena on antaa esimerkkejä oikeista tapauksista ja tehdä koulutuksesta mielenkiintoisempaa.

Koulutuksen toinen osio käsittelee erilaisia toimitapoja ja keinoja, joilla yleisiä tietoturvauhkia voidaan ehkäistä. Toisessa osiossa käydään läpi sähköpostia, salasanoja, varmuuskopiointia, tietojen tuhoamista, fyysisiä uhkia, etätyöhön liittyviä asioita ja lopuksi on listattu yleisiä ohjeita eri aihepiireistä. Koulutuksessa tehdään myös harjoitustehtäviä, mutta niitä ei kerätä takaisin, vaan ne käydään suullisesti läpi (Liite 3). Kurssin lopuksi jaetaan palautelomakkeet, joihin osallistujat vastaavat nimettöminä (Liite 2).



Kuva 2. Tietoturvan eri osa-alueita esittävä kuva, joka on laadittu valtionhallinnon tietoturvaohjeita mukaillen. Kuvaa käytettiin koulutusmateriaalissa (Liite 1).

Koulutusmateriaalin loppuun on myös etsitty erilaisia tietoturva-aiheisia linkkejä tietolähteeksi, josta saa päivitettyä ja yksityiskohtaisempaa lisätietoa tarvittaessa. Koulutuksessa käytettävät harjoitukset muodostuvat kaksi sivua käsittävistä monivalintakysymyksistä, jotka laadittiin kyseistä tietoturvakurssia varten (Liite 3). Kysymyksissä kerrataan joitakin läpikäytyjä aihepiirejä, mutta myös testataan, osaavatko vastaajat soveltaa oppimiaan asioita. Monivalintakysymyksiin päädyttiin, koska vapaasti vastattavat kysymykset tai itsenäiset tiedonhakutehtävät saattavat olla liian aikavieviä tai vaikeita koulutettaville. Kurssia varten tehtiin palautelomake, jolla pyritään saamaan tietoa muun muassa koulutuksen onnistumisesta, kouluttajan toiminnasta sekä mahdollisista kehittämisideoista (Liite 2).

5.3 Koulutuksen arviointi ja palaute

Koulutus pidettiin 16.4.2010 Kymenlaakson ammattikorkeakoulun liiketalouden toimipisteen tiloissa, ja siihen osallistui viisi Kouvolan Lääkäriaseman työntekijää, jotka työskentelevät hoitajina tai toimistopuolella. Koulutus kesti taukoineen noin kolme ja puoli tuntia, ja kaikki suunnitellut osa-alueet käytiin onnistuneesti läpi. Koulutuksessa ei ilmennyt ongelmia ja koulutettavat olivat aktiivisesti mukana kuunnellen ja esittäen kysymyksiä tai kertoen omia kokemuksiaan. Koulutusmateriaali käytiin läpi kohta kohdalta luennoiden ja välissä esitettiin kuhunkin aiheeseen sopivia uutisartikkeleita. Koulutuksen lopuksi käytiin läpi oppimistehtäviä (Liite 3) ja täytettiin palautelomak-

keet (Liite 2). Palaute oli lähes kokonaan positiivista. Lähes kaikki osallistujat kokivat koulutuksen opettavaisena ja sisällön tarpeellisena sekä koulutukseen käytetyt menetelmät ja toteutustavat koettiin onnistuneiksi. Negatiivista palautetta ei tullut kuin yhdeltä osallistujalta, jonka palautteessa koulutuksen sisältö, materiaalit ja kouluttajan toiminta arvioitiin keskinkertaiseksi. Koulutus onnistui kuitenkin kaiken kaikkiaan hyvin, varsinkin kun huomioidaan kouluttajan vähäinen kokemus koulutustilaisuuksien pitämisestä. Sen lisäksi tietoturva on aihealueena monimutkainen ja laaja, jolloin eri ihmisillä on mahdollisesti hyvinkin erilaisia käsityksiä tai odotuksia, mitä vastaavanlaisessa koulutuksessa pitäisi käsitellä ja oppia. Jos koulutus pidettäisiin uudelleen, ei siihen tehtäisi enää muutoksia.

6 YHTEENVETO

Tietoturva pitää sisällään kokonaisuuden, johon esimerkiksi lukeutuvat useat eri käsitteet, erilaiset tietoturvauhat, järjestelmät ja laitteistot, tietojenkäsittely, ylläpito ja hallinnointi. Tietoturvan aihepiirin laajuuden vuoksi ei enää voida olettaa, että organisaation johto tai muu perustason henkilökunta olisi kykenevä huolehtimaan näin laajasta, tärkeästä ja jatkuvasti muuttuvasta alasta. Organisaatiot tarvitsevat asiantuntijoita tai asiantuntevia yhteistyökumppaneita, jotka ovat ajan tasalla ja tuntevat järjestelmät, uhat ja ratkaisut. Tämäkään ei vielä riitä, koska opitut tiedot ja toimitavat pitää saada toteutettua käytännössä. Tiedot on siirrettävä työntekijöille ja mahdollisesti muillekin sidosryhmille, kuten tavarantoimittajille tai muille vastaaville, joilla on yhteys organisaation järjestelmiin ja tietoihin. Työntekijöiden ei ole tarpeellista tietää kaikkea mahdollista, vaan pienetkin opasteet ja paremmat toimintatavat voivat nostaa tietoturvan tasoa.

Opinnäytetyön laatimisen aikana selkenivät erilaiset yleiset käsitteet sekä tavat, joilla tietoturva jaetaan osa-alueisiin. Ongelmia aiheutti työn rajaus, koska työ alkoi seminaarikurssin harjoituksena, yleisenä katsauksena tietoturvaan, ilman koulutusosuutta. Työn rakenteessa oli tämän vuoksi suuria ongelmia, ja useita osioita piti moneen kertaan siirtää, muokata tai poistaa kokonaan, jotta saatiin kerättyä oleelliset tiedot ja muodostettua selkeä rakenne. Kaikkea koulutuksessa käytävää asiaa ei myöskään voitu kirjoittaa ylös varsinaiseen opinnäytetyöhön. Aihepiiriä käytiin läpi hyvin vapaamuotoisesti, ja syntyneet kysymykset ja keskustelut koskettivat monia eri asioita, joiden yksityiskohtainen läpikäyminen työssä ei ollut järkevää.

Lopputuloksena syntyi opinnäytetyö, jossa käsitellään yleisesti tietoturvan eri osa-alueita, käsitteitä, uhkia sekä tapoja, joilla voidaan parantaa tietoturvatasoa. Näiden tietojen pohjalta laadittiin ja toteutettiin tietoturvakoulutus lisämateriaaleineen Kouvolan Lääkäriaseman toimistotyöntekijöille.

LÄHTEET

Botit ja bottiverkot – kasvava uhka. Symantec. Saatavissa: http://www.symantec.com/fi/fi/norton/theme.jsp?themeid=botnet [viitattu 15.3.2010].

F-Secure: Mobiilitietoturva kasvussa. HighTech Forum / Oulu. Saatavissa: http://www.hightechforum.fi/index.cfm?j=837269 [viitattu 20.2.2010].

Haittaohjelma. Saatavissa: http://fi.wikipedia.org/wiki/Haittaohjelma [viitattu 15.1.2010]

Hakala, M., Vainio M. & Vuorinen, O. J. 2006. Tietoturvallisuuden käsikirja. Porvoo: WS Bookwell.

Henkilötietolaki 22.4.1999/523. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523 [viitattu 21.3.2010].

Hyvät salasanat: luominen ja käyttäminen. Microsoft. Saatavissa: http://www.microsoft.com/finland/protect/yourself/password/create.mspx [viitattu 22.3.2010].

Järvinen, P. 2002. Tietoturva & yksityisyys. Porvoo: WS Bookwell.

Kouvolan Lääkäriasema. Saatavissa: http://www.kouvolanlaakariasema.fi [viitattu 27.3.2010].

Laaksonen, M., Nevasalo & T., Tomula, K. J. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

Lainsäädäntö ja internet. Viestintävirasto. Saatavissa: http://www.tietoturvaopas.fi/perusohjeet/lainsaadantojainternet.html [viitattu 23.3.2010].

Langattoman verkon tietoturva kuntoon. Lumo. Saatavissa: http://www.lumonetti.fi/portaali/tietoturva/artikkelit/langattoman.html [viitattu 13.3.2010]

Muista sähköpostin käytössä. Viestintävirasto. Saatavissa: http://www.tietoturvaopas.fi/uhatjaniidentorjunta/muistasahkopostinkaytossa.html [viitattu 17.3.2010].

Salausmenetelmät. Viestintävirasto. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat.html [viitattu 23.3.2010].

Sampo Pankin asiakkaat äänestävät jaloillaan. Tekniikka & Talous. Saatavissa: http://www.tekniikkatalous.fi/ict/article76842.ece [viitattu 17.11.2009].

Securely Removing Data. Information Security Office, Indiana University. Saatavissa: http://informationsecurity.iu.edu/articles/Securely_Removing_Data [viitattu 15.2.2010].

Suojausmenetelmät. Suomen Internet-opas. Saatavissa: http://www.internetopas.com/yleistietoa/tietoturva/suojausmenetelmat [viitattu 5.10.2009].

Sähköisen viestinnän tietoturva ja –suoja. Viestintävirasto. Saatavissa: http://www.ficora.fi/index/saadokset/lait/svt.html [viitattu 23.3.2010].

Tietosuojavaltuutetun toimisto 2009. Yhteisötilaajan oikeus käsitellä tunnistamistieto- ja väärinkäytöstapauksissa. Saatavissa: http://www.tietosuoja.fi/uploads/lf9uwtx86.pdf [viitattu 19.10.2009].

Tietoturvallisuus. Valtionvarainministeri. Saatavissa: http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/index.jsp [viitattu: 2.10.2009].

Tietoturvaopas – Haittaohjelmat. Viestintävirasto. Saatavissa: http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haittaohjelmat.html [viitattu 15.1.2010].

Valtionvarainministeriö 2003. Opas julkishallinnon tietoturvakoulutuksen järjestämisestä. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53763/53760_fi.pdf. PDF-versio [viitattu 26.11.2009].

Valtionvarainministeriö 2003. Valtionhallinnon tietoturvakäsitteistö. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf. PDF-versio [viitattu 4.2.2010].

Varmuuskopioi tiedostosi. F-Secure. Saatavissa: http://www.f-secure.com/fi_FI/about-us/pressroom/news/2009/fs_news_20091105_01_fi.html [viitattu 17.11.2009]

Väärät virustorjuntaohjelmat huijaavat ihmisiä netissä. Iltalehti. Saatavissa: http://www.iltalehti.fi/digi/2009101910448321_du.shtml, [viitattu 19.10.2009].

Kari Niemi KYAMK

Tietoturvakoulutus 16.4.2010
Tietoturvan perusteet

Koulutusmateriaali

Sisältö

1. Yleistä tietoturvasta

Mitä tarkoitetaan tietoturvalla ja mitä osa-alueita se pitää sisällään

- Tietoturva tarkoittaa tietojen, järjestelmien, laitteiden sekä tietoliikenteen suojaamista erilaisia uhkia vastaan.
- Tietoturva ja tietosuoja ovat eri käsitteitä. Tietosuojalla pyritään takaamaan mm. henkilöiden oikeus yksityisyyteen, henkilötietojen luottamuksellisuus, tietojen oikeanlainen käsittelytapa jne. Tietosuoja perustuu lainsäädäntöön (perustuslaki).

- **Tietoturva muodostetaan yleensä seuraavista käsitteistä:**
  CIA (Confidentiality, integrity, availability) = Luottamuksellisuus, eheys, käytettävyys
  Luottamuksellisuus: Tietoja pääsevät käsittelemään ja näkemään ainoastaan henkilöt, joilla on siihen oikeus. Esim. potilastietoja saavat avata ainoastaan tiettyjä tehtäviä hoitavat henkilöt.
  Eheys: Tietojen pitää olla paikkansapitäviä ja niitä ei pitäisi pystyä muuttamaan vahingossa tai tahallisesti. Jos tiedot ovat virheellisiä tai niitä voi muokata kuka tahansa, niihin ei voi enää luottaa. Esim. Wikipedia on yleisesti lainattu lähde, joka näyttää luotettavalta tietosanakirjalta, mutta todellisuudessa kuka tahansa voi muokata tietoja.
  Käytettävyys: tiedot ovat saatavilla ja käytettävissä halutuilla tavoilla niiden käsittelyyn oikeutetuilla henkilöillä.

  Tietoturvaan liitetään usein myös seuraavat käsitteet:
  Todennus: Todentamisella tarkoitetaan käyttäjän, palvelun, osoitteen tai muun vastaavan aitouden varmistamista. Kun esim. asiakas kirjautuu verkkopankkiin tunnuksillaan, on niiden lisäksi syötettävä vielä avainlukuja, joilla pyritään varmentamaan käyttäjän aitous.
  Pääsynvalvonta: Pääsynvalvonnalla tarkoitetaan eri keinoja, joilla estetään asiattomien pääsy palveluun ja sallitaan käyttö todennetuille käyttäjille. Käytöstä pitää myös tallentua tietoja lokeihin, jotta esimerkiksi ongelmatilanteessa voidaan nähdä, mitä tietty käyttäjä on oikeasti palvelussa tehnyt.

Kiistämättömyys: Kiistämättömyydellä tarkoitetaan, että tietty tapahtuma voidaan jälkikäteen todistaa sitovasti. Kiistämättömyys-käsite on erityisen tärkeä esimerkiksi verkon kautta tapahtuvassa kaupankäynnissä, jolloin ostotapahtumaan liittyvien eri vaiheiden kiistämättömyys on lähes välttämätöntä.

1.1 Lainsäädäntö

- Suomessa ei ole tällä hetkellä tarkkaa ja yhtenäistä tietoturvaa koskevaa lainsäädäntöä, vaan eri säännökset tulevat useista eri laeista ja asetuksista. Tällaisia ovat esim. perustuslaki, sähköisen viestinnän tietosuojalaki, henkilötietolaki, arkistolaki, rikoslaki jne.
- Kunnianloukkaus ja yksityiselämää koskettavien tietojen levittäminen on kiellettyä. Moni käyttäjä ei välttämättä kykene tiedostamaan, että keskustelupalstalla toisen nimittely, uhkailu tai rasismi otetaan vakavasti.
- Älä levitä, kerää tai säilytä henkilötietoja ilman syytä.
- Käyttäessäsi erilaisia palveluita, kuten chatteja, keskustelupalstoja, yhteisöpalveluita (esim. Facebook, IRC-galleria, MySpace), on huomioitava useita seikkoja. Lähetettyjä kirjoituksia tai kuvia voi olla todella vaikea saada pois Internetistä. Henkilökohtaiset tiedot päätyvät myös monille eri tahoille ja voivat olla kaikkien saatavilla. Älä levitä arkaluonteisia tai muuten liian henkilökohtaisia tietoja.
- Viestintäsalaisuus suojelee viestintää, kuten mm. sähköpostia, puheluita ja kirjeitä.
- Erikseen kiellettyjä ovat: virusten tekeminen ja levitys, tietoverkkojen häirintä, järjestelmiin tunkeutuminen tai sen yrittäminen sekä niiden luvaton käyttö ja roskapostitus
- Tekijänoikeuslaki on huomioitava erityisesti. Älä tue piratismia. Huom. toisten tekemät kuvat, tekstit yms. ovat lain suojaamia. Älä käytä toisten tekemää materiaalia ilman lupaa.
- Kun rekisteröidyt uuteen palveluun, ota huomioon palvelun käyttöehdot, joihin yleensä sitoudutaan rekisteröinnin yhteydessä.

2. Tietoturvakäsitteitä

Yleisiä käsitteitä ja tietoturvauhkia

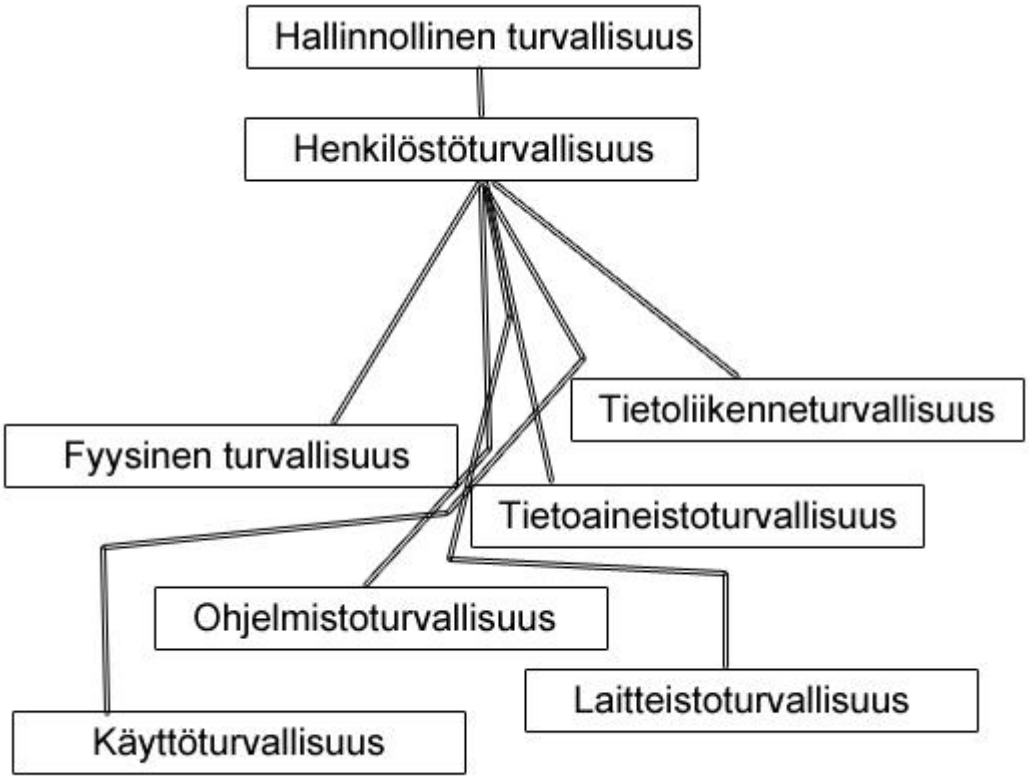
- **Virustorjuntaohjelma** – Ohjelma joka pyrkii tunnistamaan, etsimään ja tuhoamaan eri tavoin järjestelmiä uhkaavia tiedostoja ja ohjelmia. Haittaohjelmia voidaan esim. yrittää tuhota tai asettaa karanteeniin.
- **Palomuuri** – Palomuuri on ohjelma, joka hallinnoi koneiden välistä tietoliikennettä estäen esimerkiksi ei-haluttuja yhteydenottoja ja tunkeutumisyrityksiä.
- **Ohjelmointivirheet / haavoittuvuudet / tietoturva-aukot** – Lähes kaikki ohjelmat ja järjestelmät sisältävät virheitä ja puutteita, joita esim. järjestelmiin tunkeutuva taho voi hyödyntää. Tietoturva-aukot ja erilaiset takaovet tarkoittavat järjestelmien virheitä, joiden kautta mahdollinen tunkeutuja voi esim. saada pääsyn järjestelmään luvattomasti.
- **Virus** – Virukset ovat ohjelmia, jotka pyrkivät tarttumaan eri tiedostoihin ja ohjelmiin ja sitä kautta leviämään muihin järjestelmiin. Virukset leviävät usein muiden tiedostojen mukana, kuten sähköpostiviesteissä tai Internetistä ladattavien ohjelmien kautta.
- **Mato** – Virusten tapaan haittaohjelmia, jotka ovat kuitenkin itsenäisiä, eli ne kykenevät leviämään verkoissa itsenäisinä ohjelmina.
- **Troijalainen** – Haittaohjelma, joka on pyritty naamioimaan niin, että käyttäjä ei tunnista sitä haitalliseksi. Tavoitteena on saada käyttäjä uskomaan, että troijalainen tai ohjelma, johon se on liitetty, on turvallinen.
- **Vakoiluohjelma (Spyware)** – Ohjelma, joka kerää luvatta tietoja järjestelmästä tai käyttäjästä. Vakoiluohjelma saattaa esim. kerätä tietoja käyttäjän Internet-selailusta hyödyntäen tietoja roskapostituksessa tai mainonnassa. Pahimmassa tapauksessa vakoiluohjelma saattaa kyetä tallentamaan jopa näppäinpainalluksetkin.
- **Mainosohjelma (Adware)** – Ohjelma, joka pyrkii näyttämään käyttäjälle mainoksia. Esim. haittaohjelma, jonka vuoksi Internet-selaimessa alkaa avautua ylimääräisiä mainosikkunoita käytön yhteydessä.
- **Sosiaalinen manipulointi (Social Engineering) –** Käyttäjiltä huijataan tietoja psykologisin menetelmin, eli periaatteessa kierretään tekniset suojaukset (esim. esiinnytään teknisenä tukena ja tiedustellaan käyttäjätunnuksia).

- **Kalastelu (Phising)** – ”Kalastellaan” käyttäjiltä luottamuksellisia tietoja, kuten luottokortti- ja käyttäjätunnuksia sekä salasanoja (esim. lähetetään sähköposti, jossa esiinnytään pankkina ja pyydetään tunnuksia).
- **Palvelunestohyökkäys** – Lamautetaan tietyn palvelun toiminta eri keinoilla. Esim. valjastetaan joukko koneita lähettämään valtavia määriä sähköpostia tietyn yrityksen sähköpostipalvelimelle, jolloin koko palvelin saattaa kaatua.
- **Bottiverkko** – Suuri määrä koneita kaapataan ”bottien” avulla ja niistä muodostetaan ”bottiverkkoja”. Koneet tottelevat kaappaajaa ja niillä voidaan esim. toteuttaa palvelunestohyökkäyksiä. Käyttäjä ei yleensä tiedä edes koneen saastuneen ja bottiverkkoon voi kuulua tuhansia koneita.
- **Roskaposti (Spam)** – Roskapostiksi luokitellaan esimerkiksi erilaiset mainosviestit, joita lähetetään suuria määriä ilman vastaanottajalta saatua hyväksyntää.

Muita esimerkkejä tietoturvaa uhkaavista tekijöistä:

- Käyttäjän omat virheet (huonot salasanat, tietovuodot, tietämättömyys, huolimattomuus jne.)
- Erilaiset huijaukset ja tiedon kalasteluyritykset
- Virukset
- Vakoiluohjelmat
- Tietovarkaudet, vakoilu
- Roskaposti
- Tietoliikenteen häirintä
- Ohjelmointivirheet ja muut järjestelmien ja ohjelmien haavoittuvaisuudet
- Motiiveja: tietovarkaudet, puhdas tuhon aiheuttaminen (esim. tietojen muuttaminen tai poistaminen), vakoilu, taloudellinen hyöty…

Tietoturva on laaja osa-alue, joka kannattaa jaotella eri osa-alueisiin. Valtionhallinnon VAHTI-tietoturvaohjeiden mukainen jaottelu:



2.1 Hallinnollinen turvallisuus

Mitä on hallinnollinen turvallisuus

- Hallinnollisella turvallisuudella tarkoitetaan organisaation johdon tai muun hallinnollisen elimen laatimia yleisiä suunnitelmia, säännöksiä, ohjeistuksia ja ajatuksia tietoturvasta ja eri tavoista, joilla sitä tullaan ylläpitämään.
- Käytännössä hallinnollinen turvallisuus luo perustan ja lähtöasetelmat tietoturvalle sekä tietoturvapolitiikan.
- Hallinnolliseen turvallisuuteen sisältyvät vastuualueiden ja resurssien jako sekä riskien arviointi.
- On tärkeää, että organisaation hallinnosta vastaavat ovat asiantuntevia tai saavat asiantuntija-apua laatiessaan tietoturvajärjestelyjä ja -ohjeistuksia. Hallinnolla on myös oltava kokonaiskuva organisaation eri tietoturvatarpeista ja niiden ajantasaisuudesta.

- Organisaation on huolehdittava asianmukaisesta tiedottamisesta, perehdyttämisestä, koulutuksesta ja vastuualueiden jaosta työntekijöiden tehtävänkuvauksissa.
- Jos organisaatiossasi ei ole tietoturvalinjauksia tai ohjeistuksia, pyri välttämään yleisiä riskejä (epäilyttävät sähköpostiviestit, surffailu epäluotettavilla sivustoilla jne.). On pyrittävä varmistamaan, että työntekijät tutustuvat ohjeistuksiin. Tietoturvaohjeistuksen ei pidä sisältää ainoastaan sääntöjä ja kieltoja, vaan myös toimintaohjeita, mitä tulee tehdä ja keneen tulee ottaa yhteyttä ongelmatilanteen syntyessä.

2.2 Henkilöstöturvallisuus

Mitä on henkilöstöturvallisuus

- ”Henkilöstöön liittyvien tietoturvariskien hallinta henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta.” (Valtionhallinnon tietoturvakäsitteistö 2003)
- Heikoin lenkki on yleensä työntekijä itse. Johtoporras voi antaa sääntöjä, kieltoja, kannusteita ja ohjeita, mutta työntekijästä itsestään riippuu, kuinka hyvin ohjeet sisäistetään ja noudatetaanko niitä.
- Henkilöstöturvallisuus koskettaa monia eri osa-alueita, kuten työhönottoa, vastuualueita ja työrooleja, henkilötietojen käsittelyä, yhteistyökumppaneita jne.

Henkilöstöturvallisuusriskejä

- Henkilöstö on yleensä itse suurin riskitekijä (esim. työntekijöiden tekemät virheet ja heidän toiminnastaan aiheutuvat riskit).
- Käsiteltäviä tietoja voi vuotaa tai niitä käsitellään huolimattomasti tai muuten asiattomasti. Tiedot voivat sisältää arkaluonteista materiaalia henkilökunnasta, asiakkaista tai muuten salassapidettäviä tietoja, kuten liikesalaisuuksia.
- Huonosti koulutettu tai tehtävään muuten ei-soveltuva työntekijä.
- Hallinnollisen tietoturvan puutteet, organisaatiosta puuttuu suunniteltu tietoturva.
- Huonosti jaetut käyttöoikeudet, työroolit, vastuualueet (esim. vastuuhenkilöt puuttuvat tai eivät voi hoitaa tehtäviään halutulla tavalla).

- Vaaralliset työyhdistelmät, esim. yksi ja sama henkilö ei saisi olla asemassa, joka antaa mahdollisuuden oikeuksien väärinkäyttöön itsensä tai läheisten tahojen hyväksi.
- Työntekijän sairastuminen tai muu poissaolo voi vaikuttaa toimintaan. Esim. mitä tapahtuu, jos yrityksen ainoa ATK-asiantuntija sairastuu ja tulee tietotekninen ongelmatilanne?

Miten henkilöstöturvallisuutta voidaan parantaa

- Selvä roolien ja vastuualueiden jako (selvät vastuuhenkilöt ja ei ristiriitaisia tai riskitilanteita aiheuttavia oikeuksia ja rooleja). Huolehdittava myös sijaisuuksista sekä varahenkilöistä, jolloin tiedot ja palvelut ovat todennäköisemmin saatavilla ja käytettävissä myös ongelmatilanteiden aikana.
- Tietoa, kulkulupia, käyttöoikeuksia yms. jaetaan ainoastaan henkilöille, jotka oikeasti niitä tarvitsevat.
- Työsuhteiden loppuessa on huolehdittava oikeanlaisesta henkilötietojen käsittelystä ja poistettava työntekijän käyttöoikeudet ja kulkuluvat (esim. tilanne, jossa irtisanotulla työntekijällä on vielä käyttöoikeudet yrityksen järjestelmiin, antaa mahdollisuuden vilppiin).
- Erilaisten sopimusten ja sopimusehtojen laatiminen (esim. salassapitosopimus, kilpailukiellot, lisenssit jne.).
- Henkilökunnan koulutus ja ohjeistus (esim. tietoturvakoulutus ja selkeät ohjeet)
- Oikeanlaiset palkkaus- ja työhönottomenettelyt (taustaselvitykset, haastattelut, työnhakijan soveltuvuus tehtävään).
- Henkilöstöturvallisuuden eri osa-alueiden kartoitus ja jatkuva valvonta. Näin hahmotetaan eri työtehtävät ja niihin liittyvät alueet, joiden kautta voi tulla esille esim. erilaisia riskitekijöitä.
- Yhteistyökumppaneihin liittyvien seikkojen huomiointi (esim. vaikuttaako asiakkaiden, siivoojien ja huoltomiesten läsnäolo toimitiloissa tietoturvallisuuteen? Onko yhteistyökumppani luotettava ja asiantunteva?).

2.3 Tietoliikenneturvallisuus

- Tietoliikenneturvallisuudella tarkoitetaan verkoissa tapahtuvan tietoliikenteen suojaamista eri keinoilla.
- Eri organisaatioiden verkoissa liikkuu suuria määriä tietoja monilla eri tavoilla ja muodoissa (esim. yrityksen sisäisessä verkossa olevat koneet lähettävät tietoja omassa ja ulkopuolisessa verkossa oleviin koneisiin). Tämän liikenteen suojaaminen on ensiarvoisen tärkeää.
- Tietoliikennettä voidaan suojata esim. palomuureilla, virustorjunnalla tai erilaisilla salausmenetelmillä, jotka estävät tai vaikeuttavat ulkopuolisen tahon pääsyä tietoihin.
- Tietoliikenneturvallisuutta koskettaa erityisesti Internetin, sähköpostin ja etäyhteyksien käytön turvallisuus. Tämän lisäksi on huolehdittava monista muista osa-alueista, jotka voivat vaikuttaa tietoliikenteen toimivuuteen, luotettavuuteen ja ylläpitoon (esim. verkkoyhteyksien toimivuus, tietojen luottamuksellisuus, eheys ja käytettävyys eri tilanteissa, kuten tiedostojen siirrossa tai vikatilanteissa).
- Työntekijöitä on hyvä ohjeistaa esim. Internetin ja sähköpostin turvallisesta ja oikeanlaisesta käytöstä, mahdollisista salausmenetelmistä ja muista yleisistä turvallisista toimintatavoista.

2.4 Fyysinen turvallisuus

- ”Fyysinen turvallisuus tarkoittaa niitä toimenpiteitä, joilla tietojenkäsittelyyn liittyviä kohteita suojellaan fyysisiltä tapaturmilta tai vahingoittamisyrityksiltä. Laitteet ja tietovarastot suojataan asiaankuulumattomilta henkilöiltä ja erilaisilta palo-, vesi- ja kiinteistövahingoilta.” (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä, s. 43)
- Fyysisestä turvallisuudesta huolehdittaessa on huomioitava esim. kulunvalvonta, toimitilojen yleinen turvallisuus (varashälyttimet, tilojen lukitseminen, tulipalot…), laitteiden oikeanlainen käsittely ja säilytys, tiloissa liikkuvat ulkopuoliset…

2.5 Laitteistoturvallisuus

- Laitteistoturvallisuus tarkoittaa mm. tietojenkäsittelyyn käytettävien laitteiden, kuten tietokoneiden hankintaan, kunnossapitoon, käytettävyyteen ja toimivuuteen liittyviä asioita.
- Hallinnollisesta näkökulmasta on tärkeää huomioida mistä laitteet hankitaan, miten ne asennetaan, millä aikataululla, kuka huoltaa laitteet, laitteiden takuuajat jne. On huomioitava myös tulevaisuuden tarpeet ja mahdolliset muutokset (esim. toimiiko nyt ostettava tietokone lähitulevaisuudessa ilman työläitä tai kalliita päivityksiä).
- Eri laitteiden asianmukainen käyttö (vältetään käyttöä, joka tuhlaa energiaa tai altistaa laitteita turhalle rasitukselle tai erilaisille vioille).
- On tärkeää huomioida myös työpaikalla olevat muut laitteet, kuten puhelimet, muistitikut, MP3-soittimet yms.
- Työntekijöiden ei pidä liittää omia laitteitaan organisaation laitteisiin (vaarana esim. tietovarkaudet, haittaohjelmat, yhteensopivuusongelmat, vialliset laitteet jne.).

2.6 Ohjelmistoturvallisuus

- Ohjelmistoturvallisuudella tarkoitetaan tietojenkäsittelyyn käytettävien laitteiden ohjelmistojen suojaamista. Tähän liitetään myös ohjelmistojen käytettävyyteen liittyviä seikkoja, kuten ohjelmistojen yhteensopivuus, päivitys tai mahdolliset käyttölisenssit.
- Koneet on suojattava (esim. virustorjunta ja palomuurit) ja huolehdittava, että käytettävät ohjelmat ovat turvallisia, luvallisia ja laadukkaita.
- Varsinkin organisaatioissa on huomioitava, minkälaisia eri ohjelmia tarvitaan. Monet eri toiminnot voivat vaatia suuren määrän ohjelmistoratkaisuja, jotta järjestelmät pysyvät pystyssä ja niiden käyttöä voidaan seurata ja ylläpitää.
- Eri ohjelmien käyttöoikeuksiin saattaa vaikuttaa olennaisesti, käytetäänkö ohjelmia yksityiskäytössä vai yrityksissä tai muissa organisaatioissa. Mahdolliset käyttölisenssit ja muut erityisehdot on huomioitava (esim. ohjelman kokeiluversion

käyttö liiketoiminnassa voi olla laitonta tai ohjelma ei saata enää toimia tai päivittyä, jos käyttölisenssejä ei uusita).

- Eri ohjelmistot ja niiden eri versiot tai niillä tuotettu aineisto eivät ole välttämättä yhteensopivia eri laitteiden ja ohjelmien kanssa (esim. uudella Wordilla tehdyt asiakirjat eivät saata avautua vanhoissa Wordeissa).
- Ohjelmistojen pitäisi olla aitoja ja rekisteröityjä ja niiden päivittämisestä on huolehdittava. Hankintojen yhteydessä on myös huomioitava eri ohjelmistoratkaisujen kestävyys (esim. toimivatko nyt hankittavat ohjelmat vielä parin vuoden päästä, kun organisaation tietokoneisiin asennettaan uudet käyttöjärjestelmät, kuten uusi Windows).
- Organisaation tietokoneille ei saisi ladata ohjelmia ilman lupaa. Ohjelmat voivat aiheuttaa käyttöongelmia, sekoittaa koneita ja sisältää haittaohjelmia. Työntekijöiltä on rajoitettava ohjelmien haku ja asennus joko kielloilla tai teknisillä keinoilla.

2.7 Käyttöturvallisuus

- Käyttöturvallisuus koostuu turvallisen tietotekniikan käytön periaatteista, valvonnasta, ylläpidosta ja ohjeistuksista, joiden avulla pyritään minimoimaan tietoturvaa uhkaavia riskitekijöitä. Näin pyritään varmistamaan laitteiden ja eri järjestelmien oikeanlainen käyttö ja turvallisuustaso.
- Työntekijöillä on oltava selkeä kuva, miten ohjelmia käytetään oikeaoppisesti. On tiedettävä omia tehtäviään koskettavista tietoturva-asioista, kuten omien käyttäjätunnuksien, PIN-koodien ja salasanojen oikeanlaisesta käsittelystä.
- Organisaation on kyettävä myös valvomaan ja havainnoimaan mahdollisia tietoturvaa uhkaavia tekijöitä ja tapahtumia, jotta käyttöturvallisuus pysyy eheänä. Työntekijöiden on myös tiedettävä, miten toimia ongelmatilanteissa.

2.8 Tietoaineistoturvallisuus

- ”Tietoaineistoturvallisuudella tarkoitetaan tietoja ja niitä sisältävien järjestelmien tunnistusta, luokittelua ja valvontaa käsittelyn eri vaiheissa.” (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä, 49)

- Tietoa on olemassa useissa eri olomuodoissa ja niiden käsittelyyn liittyy valtava määrä erityisvaatimuksia. Jotta kokonaisuutta voidaan hallita, on kyettävä tunnistamaan ja lajittelemaan erilaiset tiedot omiksi luokikseen.
- Kun tiedot on luokiteltu (esim. salaiset ja ei salaiset tiedot), voidaan organisaatiossa sopia tietyt toimitavat, joita noudatetaan tietojenkäsittelyssä (Esim. minne salaisia tietoja tallennetaan ja miten niitä siirretään? Miten huolehditaan niiden säilytyksestä tai tuhoamisesta jne.)
- Ilman minkäänlaista luokittelua suurten tietomäärien hallinta muuttuu erittäin vaikeaksi ja epäluotettavaksi. Luokittelun avulla tiedot voidaan tunnistaa ja niiden käsittelyyn voidaan laatia selkeät toimintaohjeet.

3. Yleisiä käytäntöjä ja toimintatapoja uhkien ehkäisemiseksi

3.1 Sähköposti

Sähköpostin yleisiä ongelmia

- Sähköpostiliikenteen mukana kulkee suuri määrä arkaluonteista ja salassapidettävää tietoa, joka voi monilla eri tavoilla vuotaa väärille tahoille.
- Sähköpostiliikenne kulkee suojaamattomana, joka mahdollistaa vakoilun, jollei viestejä ole erikseen suojattu.
- Vastaanottajan osoite on kirjoitettava täydellisesti oikein, tai viestit voivat päätyä väärälle taholle. Lähettäjä ei saa varmistusta, onko viesti päätynyt oikealle vastaanottajalle.
- Väärät tahot voivat lähettää ja lukea viestejä toisten omistamista sähköposteista.
- Viestit saattavat sisältää liitetiedostoja tai käyttää muita keinoja, jotka mahdollistavat vastaanottajan koneen tai jopa verkon saastumisen.
- Väärennetyt viestit, esim. haittaohjelmia sisältävät mainokset tai erilaiset huijausviestit.
- Työsähköposteja käytetään henkilökohtaiseen viestintään.

- Sähköpostiosoitteen rekisteröiminen vääriin palveluihin (esim. käytetään työpaikan sähköpostitiliä ulkopuolisissa palveluissa, jolloin osoitteita voi vuotaa roskapostituslistoille tai muille vastaaville).
- Huonosti laaditut salasanat, jotka on helppo murtaa.
- Sähköpostiohjelmat saattavat muistaa kirjautumistunnukset tai palveluista ei kirjauduta ulos, jolloin kuka tahansa pääsee käsiksi viesteihin.
- Roskaposteja voidaan suodattaa ja poistaa automaattisesti, mutta joukossa häviää välillä myös oikeita viestejä.

Roskaposti (spam)

- Roskapostiksi luokitellaan esimerkiksi erilaiset mainosviestit, joita lähetetään suuria määriä ilman vastaanottajalta saatua hyväksyntää.
- Suuri osa sähköpostiliikenteestä koostuu ainoastaan roskapostista.
- Viestit sisältävät yleensä mainoksia tai haittaohjelmia sekä kuormittavat palvelimia ja haittaavat järjestelmien toimintoja.
- Roskapostituksen estoon kulutetaan valtavia määriä resursseja vuosittain eri organisaatioissa.

Sähköpostin turvallinen käyttö

- Vahva salasana ja sen vaihtaminen riittävän usein.
- Yleinen tietoturvasta huolehtiminen ja ajan tasalla olevan sähköpostiohjelman käyttö.
- Epämääräisten tai muuten epäilyttävien viestien välttäminen, varsinkin jos viestit sisältävät liitetiedostoja. Älä koskaan välitä epämääräisiä viestejä eteenpäin.
- Tarkista aina vastaanottajan osoite lähettäessäsi viestejä. Pienikin virhe voi johtaa viestin päätymiseen väärälle henkilölle tai henkilöille.
- Välittäessä viestiä eteenpäin huolehdi, ettei mukana kulkeudu arkaluonteisia tai turhia tietoja.
- Jos mahdollista, avaa viestit esikatselutilassa, joka estää esim. kuvien, uusien ikkunoiden tai linkkien avautumisen (esim. viesti voi yrittää automaattisesti avata linkkiä tai tiedostoa, joka sisältää haittaohjelman).
- Käyttäjän oma tietämys (opi tunnistamaan roskaposti!).
- Älä rekisteröi työpaikkasi osoitetta ulkopuolisiin palveluihin (esim. keskustelupalstat).

- Pyri välttämään arkaluonteisten tietojen käyttämistä viesteissä.
- Älä säilytä postilaatikossa arkaluonteisia tietoja tai salasanoja. Sähköpostin muistissa ei myöskään ole kannattavaa pitää suuria määriä vanhentuneita tai muuten turhia viestejä.
- Vältä esim. turhia ketjukirjeitä organisaation sisällä (monesti lähetetään hauskoja ketjukirjeitä, jotka kulkevat tuttavapiirissä ja työpaikalla).
- Kirjaudu aina ulos sähköpostista, äläkä pidä tunnuksiasi näkyvillä. Huolehdi, ettei kone muista tunnuksiasi varsinkaan, jos kyseistä tietokonetta käyttää useampi henkilö.

Sähköposti hallinnon näkökulmasta

- Järjestelmien ajantasalla pitäminen ja yleinen huolehtiminen tietoturvallisuudesta, kuten huolehtimalla sähköpostin virustorjunnasta.
- Työntekijöiden ohjeistaminen turvallisesta sähköpostin käytöstä ja säännöt postin käyttöön (esim. henkilökohtaisten viestien kieltäminen).
- Työntekijöiden posteja ei saa avata (lainsäädäntö rajoittaa, lukeminen mahdollista poikkeustilanteissa).
- Organisaation sähköpostiosoitteita ei pidä käyttää ulkopuolisissa palveluissa.
- Viestiliikenteen suojaaminen, jos mahdollista. (Viestien suojaamiseen voidaan käyttää erilaisia ohjelmia tai esim. digitaalisia allekirjoituksia)
- Sähköpostiosoitteet tulisi pitää piilossa. Esim. organisaation kotisivuilla ei kannata listata muuta kuin välttämättömät yhteystiedot.
- Roskapostin ja muiden haitallisten viestien suodatus (esim. olemassa erilaisia listoja, joiden perusteella voidaan suoraan estää tiettyjen lähettäjien viestit).
- On hyvä välttää suurten liitetiedostojen lähettämistä varsinkin suurissa organisaatioissa (verkon toiminta voi heikentyä huomattavasti esim. tilanteessa, jossa lähetetään suuria liitetiedostoja samanaikaisesti useille työntekijöille).
- Huolehditaan, ettei organisaatiossa ole vanhentuneita tai turhia sähköpostitilejä (esim. entiset työntekijät eivät pysty käyttämään organisaation sähköpostipalveluja).

3.2 Salasanat

Heikot salasanat

- Helposti arvattavat esim. käyttäjän oma nimi, läheisen nimi, lemmikin nimet, syntymävuodet jne.
- Liian yksinkertaiset salasanat, esim. auto, talo, 123auto jne. Salasana ei saisi tarkoittaa mitään yleistä helposti arvattavissa olevaa käsitettä.
- Pelkät kirjain- ja numeroyhdistelmät tai muita selkeitä kaavoja käyttävät salasanat ovat heikkoja, esim. 123456789, abcdefg.
- Useat erilaiset ohjelmat osaavat testata lukuisia salasanayhdistelmiä, jolloin heikot salasanat ovat helposti murrettavissa. Kaikki sanat, jotka ovat sanakirjoissa millä tahansa kielellä, ovat ohjelmille helposti arvattavissa.
- Saman salasanan käyttö useammassa palvelussa (salasanan paljastuessa tunkeutuja voi samanaikaisesti murtautua useisiin kohteisiin).
- Uusi salasana, joka muistuttaa vanhaa salasanaa rakenteellisesti tai muilla tavoilla, muodostaa riskin.

Vahvat salasanat

- Hyvä salasana on mahdollisimman pitkä, vähintään kahdeksan merkkiä.
- Salasanan on hyvä sisältää erilaisia ja erikokoisia merkkejä, numeroita sekä symboleita, (esim. 9jannu<545Xs).
- Salasana on vaihdettava usein. Organisaatioissa on hyvä vaatia työntekijöitä vaihtamaan salasanat mahdollisimman usein tai jos mahdollista, toteuttaa tämä vaade teknisin keinoin.
- Jos mahdollista, pakotetaan käyttäjä teknisillä keinoilla tekemään tarpeeksi monimutkainen salasana (esim. ohjelma ei hyväksy uutta salasanaa, jollei se ole tarpeeksi pitkä ja sisällä erikokoisia kirjaimia ja numeroita).
- Salasanoja ei pidä kirjoittaa ylös tai jättää näkyville paikoille. Mahdolliset ylöskirjoitetut salasanat on säilytettävä turvallisessa paikassa.
- Palveluiden ylläpitäjät eivät kysele salasanojen perään. Älä luovuta salasanoja muille tahoille (esim. monissa huijausyrityksissä voi tietyn palvelun ylläpitäjänä esiintyvä taho pyrkiä kalastelemaan (*phishing)* käyttäjien salasanoja tai muita tunnuksia vaikkapa sähköpostitiedusteluin).

- Monet palvelut antavat mahdollisuuden testata salasanojen vahvuutta (esim: http://www.microsoft.com/finland/protect/yourself/password/checker.mspx).
- Internet-selaimien ja muiden ohjelmien asetukset on hyvä säätää niin, etteivät ne muista käyttäjätunnuksia tai salasanoja (esim. sähköpostiin kirjautuminen on nopeaa, jos kone muistaa jo valmiiksi tunnuksesi, mutta tunkeutujalle tämä on suuri etu).

3.3 Varmuuskopiointi

Miksi varmuuskopioida?

- Varmuuskopiointi on helppoa ja nopeaa verrattuna kadonneiden tietojen uudelleen luontiin ja se on tärkeää jokaiselle tietokonetta käyttävälle.
- Kadonnutta tietoa voi olla vaikea tai jopa mahdoton noutaa tai luoda uudelleen. Kadonneet tiedot voivat olla korvaamattomia (esim. tuhoutuneet asiakastiedot voivat vaarantaa ja pysäyttää koko yrityksen toiminnan aiheuttaen näin valtavia tappioita).
- Varmuuskopiointi vähentää kuluja ja vaivaa, jos tietoturvauhkatilanne toteutuu ja järjestelmät menettävät toimintakykynsä ja tietoja katoaa. Järjestelmät saadaan palautettua toimintaan ja tärkeimmät tiedot noudettua (esim. hallinnollisesta näkökulmasta järjestelmien toimivuus ja tietokantojen palautus on tärkeintä, mutta tavalliselle työntekijälle monet asiakirjat, kuten lomakepohjat tms. joita käytetään jokapäiväisessä työnteossa, ovat monesti yhtä tärkeitä).

Varmuuskopiointikeinot ja niihin liittyviä ongelmia

- Muistitikut voivat olla hyvä keino lyhytaikaiseen säilytykseen ei-tärkeille ja ei-arkaluonteisille tiedostoille. Muistitikut häviävät helposti ja ovat hyvin alttiita varkauksille ja hajoamiselle.
- CD- ja DVD-levyt ovat kestäviä ja niille mahtuu paljon materiaalia. Levyt pitää kuitenkin aina polttaa ja tyhjentää, joka vie aikaa, eikä näin ole järkevä keino jokapäiväiseen käyttöön. Levyt ovat myös samalla tavoin alttiita riskeille, kuten muistitikutkin.
- Toiset tietokoneet, verkkoasemat ja ulkoiset kovalevyt ovat hyvä keino varmuuskopiointiin, ja niiden tallennuskapasiteetti on suuri.

- Varmuuskopiot on hyvä säilyttää turvallisessa paikassa, esim. kassakaapissa tai lukituissa tiloissa.
- Varmuuskopioinnin jälkeen on tarkistettava, että kopiointi on onnistunut ja tiedostot ovat varmasti käyttökelpoisia!
- Varmuuskopiointi pitää toteuttaa tietyin väliajoin, vanhentuneista kopioista ei ole hyötyä.
- Varmuuskopiointiin on erikoistunut useita yrityksiä, joiden tietokantoihin voidaan esimerkiksi lähettää eri keinoilla varmuuskopioitavia tietoja. Suurten tietomäärien varmuuskopiointi kannattaakin hoitaa erilaisilla ohjelmistoilla automaattisesti. Organisaatioiden kannattaakin turvautua asiantuntijatahoihin tai muihin yrityksiin varmuuskopioinnissa.
- Tietoja tai laitteita hajoaa tai ne saattavat muuttua sellaisiksi, ettei varmuuskopioiden noutaminen ole enää mahdollista. Tietyt yritykset tarjoavat palveluita, joiden avulla pystytään välillä noutamaan tietoja hyvinkin vaurioituneilta laitteilta.

3.4 Tietojen tuhoaminen

- Tietokoneen kiintolevyt, muistitikut, levykkeet, CD- ja DVD-levyt yms. voivat sisältää paljon tietoa, joita ei pitäisi joutua ulkopuolisten tahojen haltuun. Tämä pitää huomioida, kun laitteita myydään, hävitetään tai käytetään uudelleen.
- Vaikka laite olisi näennäisesti hajonnut, se ei tarkoita, etteikö joku muu kykenisi noutamaan tietoja esim. hajonneelta kovalevyltä. Tämän vuoksi laitteet on aina hävitettävä aina oikeaoppisesti.
- Kiintolevyt, DVD-levyt, disketit, muistitikut yms. on varminta tuhota henkilökohtaisesti (esim. leikkaa DVD-levy kahtia tai tuhoa muistitikun sisältö fyysisesti).
- Tiedostojen siirtäminen roskakoriin ja sen tyhjentäminen eivät oikeasti poista tietoja. Ne ovat edelleen palautettavissa. Edes koneen uudelleenasennuskaan ei riitä tietojen perinpohjaiseen poistamiseen.
- Kun poistat eri ohjelmia, etsi aina ohjelman poistotiedosto (esim. uninstall.exe) tai käytä ohjauspaneelin ”Lisää tai poista sovellus”-ominaisuutta. Pelkän ohjelman pikakuvakkeen tai kansion poistaminen ei pyyhi ohjelmaa koneelta.

- On olemassa useita ilmaisia sekä maksullisia ohjelmia, joilla kykenee tyhjentämään koneen, niin etteivät tiedostot ole enää palautettavissa.
- Yritysten ja muiden organisaatioiden on hyvä turvautua ulkopuoliseen apuun. On olemassa useita yrityksiä, jotka hoitavat tietojen hävitystä (tietojen poispyyhintä tai koneiden ja muiden laitteiden oikeaoppinen tuhoaminen).

3.5 Fyysiset uhat

Fyysiset uhat

- Tietoturvauhat eivät rajoitu ainoastaan verkosta tai muualta tuleviin ”sähköisiin” uhkiin, kuten haittaohjelmiin ja hakkerointeihin.
- Tietokoneet ja muut laitteistot ovat alttiita lukuiselle ympäristöstä tuleville uhille, kuten tulipaloille, sähköhäiriöille, pölylle, kosteudelle, laitteistovioille, varkauksille jne.
- Organisaation toimitiloissa saattaa liikkua ulkopuolisia tai asiattomia henkilöitä, jotka aiheuttavat tietoturvauhkia (esim. tietokone- ja puhelinvarkaudet, muistitikku- ja muut tallennusvälinevarkaudet, tietokoneiden luvaton käyttö jne.)
- Ulkopuoliset voivat nähdä arkaluonteisia tietoja esim. väärin suunnatulta näytöltä, mutta myös yleisillä paikoilla (esim. kannettavan tietokoneen käyttö junassa, jolloin kuka tahansa vieressä oleva henkilö voi nähdä tietokoneen näytön).

Fyysisten uhkien ehkäiseminen

- Tietokoneet, kännykät ja muut laitteet tulee aina suojata salasanoin ja käyttäjätunnuksin, joita ei saa pitää nähtävillä. Arkaluonteisia tietoja, sähköpostiosoitteita tai muita vastaavia ei myöskään pidä jättää näkyville paikoille.
- Asettele tietokoneen näyttö niin, ettei ulkopuolinen näe sitä helposti. On olemassa myös erilaisia heijastesuojia, jolloin näyttö näkyy pimeänä sivustakatsojalle.
- Kun et ole työpisteessäsi, lukitse tilat ja kone.
- Työympäristö ja muut tilat, joissa koneet sijaitsevat, tulee turvata asianmukaisin keinoin (palovaroitin, varkaudenestojärjestelmät ja kulunvalvonta, asianmukainen lämpötila ja kunnossapito, laitteiden sijoittelu ja säilytys jne.)
- Työympäristön on hyvä olla siisti ja hyvin hoidettu. Eri laitteet ja tallennusvälineet säilytetään mahdollisimman turvallisissa paikoissa (esim. muistitikkuja, asiakirjoja,

CD-levyjä tai muita vastaavia ei pidä jättää pöydille, jossa ne voivat vahingoittua tai hävitä).

- Kaikista tärkeistä tiedoista kannattaa tehdä varmuuskopiot tai palautuslevyt tietyin väliajoin ja ne tulee säilyttää asianmukaisessa paikassa.
- Älä käytä laitteita väärin. Esim. mitään laitteita ei kannatta jättää auringonpaisteeseen tai muihin sopimattomiin tiloihin. Monien laitteiden ei myöskään tarvitse olla päällä kaiken aikaa. Jos laitteet reistailevat, on siitä ilmoitettava huollolle.
- Huolehdi, ettei toimitiloissa liiku asiattomia henkilöitä tai ettet itse tuo sellaisia toimitiloihin. Kiinnitä myös huomiota ylimääräisiin laitteisiin.

3.6 Etätyö

Etätyön tietoturvaongelmia

- Etätöiden määrä on kasvanut huomattavasti tekniikan kehittyessä. Työntekijöillä on suuremmat mahdollisuudet tehdä töitä kotoa tai muualta käsin.
- Organisaation palveluita on monenlaisessa käytössä, esim. työsähköposteja käytetään kotoa käsin tai työntekijöillä on mahdollisuus käyttää organisaation sisäisiä palveluita yrityksen ulkopuolellakin.
- Organisaation tietoturva voi olla uhattuna, jos etätyöntekijä käyttää omaa tietokonettaan, joka ei ole asianmukaisesti suojattu.
- Monen työntekijän henkilökohtainen tietokone voi olla saastunut ja huonosti suojattu työntekijän sitä tietämättä. Saastuneilla koneilla saatetaan lukea esim. yrityksen sähköpostia, käsitellä arkaluonteista materiaalia ja siirtää haitat työpaikan verkkoon.
- Kannettavat tietokoneet ovat yleisiä etätyössä. Niitä käytetään monenlaisissa olosuhteissa, jolloin niihin kohdistuu monia uhkia. Kannettava on helppo unohtaa, hukata tai sitä voidaan säilyttää helposti varastettavissa paikoissa. Koska kannettavia käytetään työpaikan ulkopuolella, ovat ne alttiita myös monille muille riskeille (esim. kylmä ilma, kosteus, henkilökohtaisen käytön aiheuttamat tietoturvauhat jne.).

- Työtietokoneita käytetään kotona, mutta myös yleisillä paikoilla, joka luo riskin tietovuodoista (esim. junassa takana istuva saattaa nähdä tärkeitä tietoja, tai kotona muu perhe käyttää samaa tietokonetta).
- Tietokoneiden lisäksi yhä tärkeämmässä osassa ovat matkapuhelimet, joilla voidaan toteuttaa samoja toimintoja verkossa kuin tietokoneillakin. Matkapuhelimet ovat myös alttiita viruksille ja muille tietoturvauhille, ja niiden tietoturva usein sivutetaan.
- Laitteiden säilytyksessä on oltava erityisen tarkkoja. Esim. kannettavia ei pitäisi koskaan jättää näkyville paikoille.
- On huomioita mahdolliset seuraukset, jos esim. kannettava varastetaan. Koneet on hyvä suojata esim. salausmenetelmillä, käyttäjätunnuksilla, omistajamerkinnöillä (tehdään koneelle tiedosto tai jokin muu merkintä, jonka kautta kone voidaan tunnistaa omaksi).
- Jos käytetään langattomia yhteyksiä, on yhteyksien salauksesta huolehdittava. Esim. kaupunkialueilla voi olla huomattava määrä langattomia tukiasemia, joita ei ole suojattu. Niitä käyttäessä on mahdollista, että toinen taho voi vakoilla toimintaa.
- Huolehdi aina, että kone yhdistää oikeaan langattomaan verkkoon ja yhteys on suojattu.
- Turvallisuutta lisää käyttäjän oma tietämys ja oikein suojattu tietokone. Ihanteellista olisi, että työnantaja kustantaisi etätyötä tekeville ajantasaiset tietoturvaohjelmistot ja antaisi koulutusta aiheesta tai estäisi muilla keinoilla etäyhteydet huonosti suojatuista työntekijöiden koneista. Yrityksen omat tietoturvaponnistelut voivat helposti valua hukkaan, jos tietoturva-aukko syntyy työntekijän kotikoneelta.

3.7 Turvallinen käyttö

Yleisiä turvaohjeita kotiin sekä työpaikalle

- Huolehdi tietokoneen järjestelmien päivittämisestä. Tähän sisältyvät Internet-selaimet, virusohjelmat, palomuurit ja varsinkin Windows-käyttöjärjestelmä.

- Suurin osa ohjelmista osaa hakea itsenäisesti päivityksiä, mutta ohjelmat saattavat tarjota käyttäjälle mahdollisuuden estää päivitysten haun. Anna ohjelmien aina päivittyä.
- Huolehdi, että virusturva ja palomuuri ovat aktivoituina. Tee viikoittain tai ainakin kuukausittain virustesti.
- Asentaessasi ohjelmia pyri varmistumaan niiden luotettavuudesta ja käyttöehdoista. Huom. työpaikoilla itsenäinen ohjelmien haku ja asentaminen usein kielletty.
- Selaimet ja muut ohjelmat tallentavat tietoja, kun käytät Internetiä. Esim. Internet-selain tallentaa tietoja, tunnuksia, kuvia, osoitteita ja kerää lokia eri käyttösessioiden aikana. Samaan aikaan koneelle voidaan tallentaa haittaohjelmia, jotka voivat vakoilla ja käyttää selaustietojasi esim. markkinointiin.
- Älä tallenna salasanoja tai käyttäjätunnuksia. Tyhjennä selaimien ja muiden ohjelmien välimuisti käytön jälkeen (esim. Internet Explorerin sivuhistoria). Selaimen asetuksista on mahdollista säätää niin, ettei se tallenna tietoja.
- Vältä epäilyttäviä sivustoja ja linkkejä.
- Älä käytä muiden tunnuksia tai luovuta omiasi.
- Kirjaudu aina ulos palveluista ja koneelta ja tarvittaessa muista lukita kone.
- Jos laitteistot eivät toimi oikein, pyri ilmoittamaan asiasta (esim. koneiden hidastelu tai reistailu usein voi olla viatonta, mutta taustalla voi olla muitakin syitä).
- Vältä piratismia (suuri määrä haittaohjelmia leviää piratismin kautta).
- Opettele tunnistamaan tiedostopäätteitä (esim. .zip, .rar, .jpg, .exe).
- Ole erityisen varovainen tuodessasi omia laitteita työpaikalle ja vältä niiden yhdistämistä työlaitteisiin (esim. henkilökohtaiset muistitikut, MP3-soittimet, kannettavat tietokoneet)
- Yhteydet, laitteet sekä tietoliikenne ja viestintä kannattaa suojata esim. käyttämällä salausmenetelmiä. Tavallisen käyttäjän ei tarvitse huolehtia niin paljoa salauksesta.
- Käyttäessäsi etäyhteyksiä huolehdi, että yhteys on suojattu. Huom. tärkeää niin kotikäyttäjälle kuin organisaatiollekin.
- Älä paljasta arkaluonteisia tietoja keskustelupalstoilla tai Internet-yhteisöissä (esim. Facebook).
- Älä avaa epäilyttäviä sähköpostiviestejä, varsinkaan jos et tunne lähettäjää ja ne sisältävät liitetiedostoja. Älä lähetä arkaluonteisia tietoja sähköpostilla.

- Jos epäilet tietokoneesi saastuneen etkä tiedä mitä tehdä, etsi apua (esim. tuttavat, atk-liike). Älä jatka käyttöä saastuneella koneella.
- Käytä järkeäsi. Erilaiset haittaohjelmat ja huijaukset leviävät ja tapahtuvat useilla eri kekseliäillä tavoilla, jotka voivat vedota käyttäjän hyväuskoisuuteen tai huolimattomuuteen.

Ilmaisia tietoturvaohjelmia kotikäyttöön

- Kaupoista löytyy suuri määrä erilaisia tietoturvaohjelmia erilaisiin tarpeisiin, mutta moni ei halua maksaa vuosittain ohjelmien käyttömaksuja. Vähintään kannattaa turvautua ilmaisiin ohjelmiin, vaikka ne eivät tuokaan samanlaista tietoturvatasoa.

- Virusohjelmia ja palomuureja: Avira Antivir, Symantec, Comodo, ZoneAlarm
- Ad-Aware ja Spybot Search & Destroy etsivät haittaohjelmia kuten vakoilu- ja mainontaohjelmia.
- CCleaner-ohjelmalla on helppo ja nopea poistaa sivuhistoriat, väliaikaistiedostot, salasanat ja käyttäjätiedot yms.
- Hyviä Internet-selaimia: Firefox, Chrome, Opera.

3.8 Tietoturvalinkkejä

http://www.tietoturvaopas.fi

http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/

http://www.cert.fi/

http://fi.wikibooks.org/wiki/Tietoturva

http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html

Lähteet

Haittaohjelmat. Saatavissa: http://fi.wikipedia.org/wiki/Haittaohjelma

Hakala, M., Vainio M. & Vuorinen, O. J. 2006. Tietoturvallisuuden käsikirja. Porvoo: WS Bookwell.

Hyvät salasanat: luominen ja käyttäminen. Microsoft. Saatavissa: http://www.microsoft.com/finland/protect/yourself/password/create.mspx

Järvinen, P. 2002. Tietoturva & yksityisyys. Porvoo: WS Bookwell.

Laaksonen, M., Nevasalo & T., Tomula, K. J. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

Langattoman verkon tietoturva kuntoon. Lumo. Saatavissa: http://www.lumonetti.fi/portaali/tietoturva/artikkelit/langattoman.html

Securely Removing Data. Information Security Office, Indiana University. Saatavissa: http://informationsecurity.iu.edu/articles/Securely_Removing_Data

Sähköisen viestinnän tietoturva ja –suoja. Viestintävirasto. Saatavissa: http://www.ficora.fi/index/saadokset/lait/svt.html

Tietoturvallisuus. Valtionvarainministeri. Saatavissa: http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/index.jsp

Tietoturvalliseen yhteiskuntaan. Viestintävirasto. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html

Tietoturvaopas – Viestintävirasto. Saatavissa: http://www.tietoturvaopas.fi/.

Valtionvarainministeriö 2003. Opas julkishallinnon tietoturvakoulutuksen järjestämisestä. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53763/53760_fi.pdf. PDF-versio

Valtionvarainministeriö 2003. Valtionhallinnon tietoturvakäsitteistö. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf. PDF-versio

Palautelomake

Tietoturvakoulutus 16.4.2010

Ympyröi vaihtoehto. Arvosteluasteikko (5=erittäin hyvä, 4, 3, 2, 1=erittäin huono)

Koin koulutuksen opettavaisena ja sisällön tarpeellisena	**5 4 3 2 1**
Koulutus vastasi odotuksiani	**5 4 3 2 1**
Kouluttajan toiminta	**5 4 3 2 1**
Opetustapa ja -materiaali	**5 4 3 2 1**

Vastaa lyhyesti

Miten koulutusta olisi voinut parantaa tai muuttaa?

_____

_____

_____

Muuta

_____

_____

_____

Kiitos osallistumisestasi ja palautteestasi!

Tietoturvakoulutustehtävät

1. Olet ladannut tietokoneellesi uuden virustorjuntaohjelman. Et ole varma sen luotettavuudesta. Ystäväsi kehottaa sinua asentamaan toisen virustorjuntaohjelman lisäksi, jotta saat vähintään tuplasuojan. Onko neuvossa perää?
A) On
B) Ei ole

2. Yrität keksiä uutta salasanaa. Mikä vaihtoehdoista on paras?
A) Naapurin koiran nimi yhdistettynä serkkusi syntymävuoteen
B) Sattumanvarainen numerosarja yhdistettynä vieraskieliseen sanaan
C) Suosikkilaulajasi nimi yhdistettynä sattumanvaraiseen numerosarjaan, jonka jälkeen lisäät vielä vieraskielisen sanan
D) Numeroita, merkkejä ja erikokoisia kirjaimia sisältävä hankalasti muistiin painuva merkkiyhdistelmä

3. Tietokoneen palomuuri ilmoittaa, että sinulle tuntematon ohjelma yrittää muodostaa yhteyttä Internetiin. Palomuuri tiedustelee, estetäänkö yhteydenotto vai sallitaanko se. Soitat ystävällesi, joka epäilee, että kyseessä on tunkeutumisyritys. Hän myös neuvoo sinua yleensäkin estämään kaikki yhteydenotot. Onko neuvossa perää?
A) On
B) Ei ole

4. Etsit tietoa Internetistä ja löydät mielenkiintoisen sivuston. Yhtäkkiä huomaat, että näytölle avautuu ikkuna, jossa ilmoitetaan tietokoneesi saastuneen useista erilaisista viruksista ja on suositeltavaa ladata virustorjuntaohjelma klikkaamalla avautunutta ikkunaa, jotta haittaohjelmat voidaan poistaa.
A) Paina ikkunaa ja yritä poistaa tietokonettasi vaivaavat virukset
B) Älä tee mitään

5. Mikä seuraavista osa-alueista on tärkein vaikuttaja tietoturvan kannalta erilaisissa organisaatioissa?
A) Henkilöstöturvallisuus
B) Hallinnollinen turvallisuus
C) Tietoaineistoturvallisuus

6. Löydät työpaikkasi käytävältä muistitikun. Tiedustelet ystävältäsi, onko hän hävittänyt muistitikun, mutta hänkään ei tunnista sitä omakseen. Hän ehdottaa tikun kytkemistä tietokoneeseen sen varalta, jos tikun sisällön perusteella voisi päätellä sen omistajan. Onko neuvossa perää?
A) On
B) Ei ole

7. Tietokoneesi hidastelee jatkuvasti ja koneesta kuuluu omituisia ääniä. Avaat koneen ja huomaat, että koneen tuuletin ei toimi kunnolla. Onko kyseessä tietoturvaa uhkaava tekijä?
A)On
B) Ei ole

8. Kokoushuoneessa on videotykki, jota käytetään kannettavalla tietokoneella. Kannettava ilmoittaa usein, että saatavilla on Windows-päivityksiä, mutta ilmoitus aina jostakin syystä saa koneen kaatumaan, jolloin kestää kauan aikaa saada videotykki takaisin päälle. Pomosi on raivoissaan jatkuvista keskeytyksistä ja käskee sinua korjaamaan asian.
A) Laitat päivitysten haun pois päältä
B) Käynnistät koneen uudelleen, joka vie aikaa, mutta yrität päivittää koneen myöhemmin, vaikka epäilet sen onnistumista
C) Kytke koneen Internet-yhteys irti, jolloin päivityksiä ei enää haeta tai tarkisteta, mutta toisaalta kone ei ole enää alttiina verkon tietoturvauhilla

9. Asiantunteva ystäväsi asentaa koneellesi lukuisia eri tietoturvaohjelmistoja ja kertoo, että koneen tietoturva on kunnossa. Kone on nyt suojattu asianmukaisesti, mutta ainoana haittapuolena on, että asennetut ohjelmat vievät paljon tehoja koneelta, ja välillä eri tiedostojen avaaminen voi kestää useitakin minuutteja. Onko tietoturva kuitenkin kunnossa?
A) On
B) Ei

10. Eri ohjelmien ja järjestelmien päivittäminen on aina hyvä vaihtoehto paremman tietoturvan ja käytettävyyden kannalta.
A) Kyllä
B) Ei

11. Työtiloissa tapahtuu vesivahinko. Onko tämä ongelmallista:
A) Luottamuksellisuuden kannalta
B) Eheyden kannalta
C) Käytettävyyden kannalta
D) Kaikkien yllämainittujen kannalta
E) Vesivahingot eivät ole olennaisia tietoturvan kannalta

12. Tavallisten käyttäjien koneilla ei ole yleensä mitään arvokasta nettirikollisille. Tämän vuoksi järjestelmiin tunkeutuminen ja muut rikkeet on suunnattu pääosin yrityksiä ja muita organisaatioita kohtaan.
A) Totta
B) Epätosi

13. Valtionhallinnon, pankkien, sanomalehtien ja muiden vastaavien sivustoilla surffailu on aina turvallista.
A) Totta
B) Epätosi