POHJOIS-KARJALAN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

Laura Hiltunen

TIETOTURVAKOULUTUS RÄÄKKYLÄN OPETUSHENKILÖKUNNALLE

Opinnäytetyö
Kevät 2012

POHJOIS-KARJALAN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Toukokuu 2012
Tietojenkäsittelyn koulutusohjelma

Länsikatu 15
80200 JOENSUU
p. 050 311 6310

Tekijä
Laura Hiltunen

Nimeke
Tietoturvakoulutus Rääkkylän opetushenkilökunnalle

Tiivistelmä

Opinnäytetyön aiheena oli järjestää tietoturvakoulutus opetushenkilökunnalle. Tietoturvakoulutuksen tarkoituksena oli tuoda esille tietoturvan tärkeyttä niin työelämässä kuin työelämän ulkopuolella tapahtuvissa tilanteissa sekä kertoa koulutettaville myös tietoturvan laajuudesta syvällisemmin.

Opinnäytetyön tarkoituksena oli tarkastella koulutettavien yleistä tietoutta ja osaamista tietoturvallisuuteen liittyvissä tilanteissa ja asioissa keskustelujen, omien kokemusten sekä harjoitustehtävien avulla. Opinnäytetyössä tutustutaan tarkemmin tietoturvaan, sen eri osa-alueisiin, koulutuksen suunnitteluun ja toteutukseen, sekä lopussa opinnäytetyön yhteenvetoon. Opinnäytetyön materiaali sisältää tämän kirjallisen materiaalin lisäksi myös liitteitä, joita tietoturvakoulutuksessa käytettiin.

Havainnot osoittavat, että koulutettavat olivat riittävän hyvällä tasolla oma tietämyksensä kanssa tietoturvallisuuteen liittyvissä asioissa ja tilanteissa, joita he kohtaavat heidän omalla työpaikallansa sekä työpaikan ulkopuolella. Koulutettavat halusivat tuoda omia näkemyksiään esille keskustelemalla. Keskusteluista voitiin päätellä, että koulutettavat olivat kiinnostuneita tietoturvallisuudesta. Koulutuksen lopussa pidettyjen tietoturvaharjoitusten perusteella koulutettavien perustietämys tietoturvallisuudesta oli tavoitteiden mukaista.

Kieli
suomi

Sivuja 44
Liitteet 4

Asiasanat
tietoturva, koulutus, Rääkkylä

NORTH KARELIA
UNIVERSITY OF APPLIED SCIENCES

THESIS
May 2012
Degree Programme in Business Information Technology

Länsikatu 15
80200 JOENSUU
FINLAND
Tel. +358-50 311 6310

Author
Laura Hiltunen

Title
Information Security Training to the Teachers of Rääkkylä Municipality

Abstract

The subject of this thesis was to arrange data security training to teachers. The purpose of security training was to highlight the importance of information security at work and outside of work in many different situations. Also to provide the teachers with some deeper understanding about the large scope of the information security issues.

The aim of this thesis was to examine teachers' general knowledge and expertise in security-related situations and issues through discussions based on personal experiences and through exercises. This thesis deals with different aspects of information security and the planning and implementation of the information security training.

The study revealed that the teachers' knowledge about security issues and situations inside and outside their work was good enough. The teachers also wanted to bring out their own views through discussions. It also can be concluded that the teachers were quite interested in security. Also exercises showed that their basic knowledge of security was adequate.

Language	Pages 44
Finnish	Appendices 4

Keywords

data security, training, Rääkkylä

Sisältö

1 Johdanto 5
2 Tietoturvan aihealueet 6
2.1 Hallinnollinen tietoturva 8
2.2 Tietoaineiston tietoturva 11
2.3 Henkilöstöturvallisuus 16
2.4 Käyttöturvallisuus 18
2.5 Tietoliikenneturvallisuus 20
2.6 Fyysinen turvallisuus 22
2.7 Laitteistoturvallisuus 24
2.8 Ohjelmistoturvallisuus 26
2.9 Lainsäädökset 28
2.10 Haittaohjelmat ja niiden torjunta 29
3 Koulutuksen suunnittelu 31
3.1 Osaamisen kehittäminen 32
3.2 Koulutuksen sisältö 33
3.3 Pedagogiikka 35
4 Koulutuksen toteuttaminen 35
5 Yhteenveto 38
Lähteet 41

Liitteet
Liite 1 Tietoturvaohje
Liite 2 Tietoturvan ABC
Liite 3 Tietoturvaharjoitusten vastaukset
Liite 4 Tietoturvakoulutuksen PPT-esitys

1 Johdanto

Tietoturva on yhä tärkeämmässä roolissa etenkin tässä nykytietoyhteiskunnassa, ja se on muodostunut yhdeksi tärkeäksi liiketoimeksi yrityksissä. Tietoturva on käsitteenäkin jo hyvin laaja ja sen takia useassa yrityksessä myös vaikeasti sisällytettävä ja kohdennettava asia. Lisäksi tietoturvan tärkeyttä usein myös laiminlyödään. On pohdittava, miten voitaisiin kehittää yrityksen tietoturvaa niin, että se kattaisi lainsäädännön asettamat vaatimukset ja yrityksen tietoturvaan liittyvät tarpeet. On laadittava erilaisia suunnitelmia, joiden avulla voidaan seurata tietoturvallisuutta ja siihen liittyviä toimenpiteitä, kartoitetaan tilannetta, luodaan analyysejä ja luokitellaan yritysten sisäisiä tietoja.

Opinnäytetyöni aihe sai alkunsa keväällä 2010. Opinnäytetyöni aiheena on järjestää tietoturvakoulutus. Ensin tarkoituksenani oli pitää tietoturvakoulutukseni jollekin yritykselle, mutta päästyäni Rääkkylän kunnan sivistystoimeen työharjoitteluun IT-harjoittelijaksi syksyllä 2011, pidin tietoturvakoulutukseni peruskoulun opetushenkilökunnalle. Tämän opinnäytetyön toimeksiantajana toimi siis Rääkkylän kunta.

Tavoitteenani oli kouluttaa lyhyessä aikataulussa tärkeimpiä kohtia eri tietoturvan aihealueista. Koulutuksessani käytin esimerkkejä käytännön tilanteista tietoturvallisuutta ajatellen, laadin tehtäväharjoituksia koulutettaville sekä keskustelimme tietoturvasta yhdessä koulutettavien kanssa koko koulutuksen ajan.

Halusin pitää koulutukseni sopivan yksinkertaisena, eli en käytä vaikeita, erikoisia tietoteknillisiä tai muutoin ehkä vaikeasti ymmärrettävää IT-sanastoa. Tarkoituksenani oli puhua itse aiheesta niin, että se on jokaisen ymmärrettävissä ja sisäistettävissä, mistä missäkin kohtaa koulutuksen edetessä on kysymys. Tällainen käytäntö edesauttaa myös aiheen oppimista.

Toisessa luvussa tutustutaan tarkemmin tietoturvan eri aihealueisiin. Näitä aihealueita ovat hallinnollinen tietoturvallisuus, tietoaineistoturvallisuus, henkilöstöturvallisuus, käyttöturvallisuus, tietoliikenneturvallisuus, fyysinen turvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, lainsäädökset, haittaohjelmat sekä

niiden torjuminen. Kolmannessa luvussa tarkastellaan osaamista, suunnitellaan pedagogisia, kasvatuksellisia sekä sisällöllisiä tavoitteita. Neljännessä luvussa arvioidaan koulutuksen toteutus ja miten tavoitteisiin päästiin. Viidennessä luvussa arvioidaan kokonaisuudessaan opinnäytetyön vaiheita.

2 Tietoturvan aihealueet

Tietoturvassa on kyse tietojen, palveluiden, järjestelmien ja tietoliikenteen suojaamisesta eli tietoturvan avulla suojataan tärkeiden tietojen pääsyä vääriin käsiin. Tietoturva on myös tietojen luottamuksellisuutta, eheyttä, kiistämättömyyttä, pääsynvalvontaa, saatavuutta ja tarkastettavuutta. Luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat vain niihin oikeuttavien käytettävissä. Eheydessä kyse on tiedon muuttumattomuudesta tiedon luomisen, käsittelyn ja siirron aikana. Kiistämättömyyden avulla pyritään valvomaan tiedon siirtoa ja sen käsittelyvaiheessa osallistuneiden käyttäjien tunnistamista. Pääsynvalvonta rajoittaa ja valvoo käyttäjien pääsyä käyttää saatavilla olevaa tietoa. Saatavuus on tiedon helppoa ja viiveetöntä käyttöä oikeutetuille henkilöille. Tarkastettavuudessa puolestaan on kysymys tietojenkäsittelyn tuloksena saadusta tiedosta, jota pyritään tarkastamaan ja osoittamaan saadun tiedon oikeellisuutta. (Suomen Internetopas 2012.)

Tietoturva nykytietoyhteiskunnassa on yhä tärkeämmässä roolissa Internetmaailmassa. Www-sivujen tietoja voidaan muokata luvatta, manipuloida Internet-hakuja, sähköpostiviestien -ja osoitteiden väärinkäyttö on lisääntynyt, ja käyttäjien käyttäjätunnukset salasanoineen ovat jatkuvan tietoturvauhan alaisena. Myös verkkopankkiasioinnin yleistyessä, tapahtuu useita väärinkäyttöjä ja tietoturvauhkia, esimerkiksi sähköposteihin lähetettyjen, joidenkin pankkien nimellä tilinumero ja luottokorttiuteluita. Jos tietoturva ei ole hyvällä tasolla, voi tästä seurata haittaohjelmien pääsy tietojärjestelmään ja pahemmassa tapauksessa se aiheuttaa mittavia vahinkoja, kuten ajaa laitteisto siihen tilaan, että se on käyttökelvoton. Myös tietojen väärinkäyttöä ilmenee. Siksi onkin erittäin tärkeää käyttää erilaisia suojausmenetelmiä tällaisia tietoturvauhkia vastaan. (Suomen Internetopas 2012.)

Suojausmenetelmiä ovat tekninen, fyysinen ja hallinnollinen suojausmenetelmä. Teknisellä tietoturvalla tarkoitetaan sitä, että käytetyissä laitteissa ja ohjelmissa ei ole tietoturvallisia puutteita. On siis mietittävä tietoturvaa jo laitteiden ja ohjelmien hankintavaiheessa. Salasanojen ja käyttäjätunnusten avulla valvotaan tietojärjestelmiin pääsyä ja niissä olevien tietojen säilymistä luottamuksellisena. Käyttäjätunnukset määrittelevät, mihin tietoihin kullakin käyttäjällä on oikeus päästä käsiksi. Kuitenkaan käyttäjätunnukset ja salasanat eivät ole niitä varmimpia tietoturvaratkaisuja, koska salasanojen päättely tai haltuunotto tiedonsiirron aikana on aika helppoa. (Suomen Internetopas 2012.)

On varmistettava laajemmissa tietoverkoissa, jotka ovat yhteydessä lähiverkkoihin se, etteivät ulkopuoliset käyttäjät pääse käsiksi sen sisältöön. Näitä varten on olemassa erilaisia palomuuriratkaisuja, tietoturvaohjelmia sekä käsiteltävissä olevan tiedon koodaaminen lukukelvottomaksi, ja ainoastaan koodiavaimen eli purkunumerosarjan omaava henkilö pystyy muuttamaan tietoa. Fyysinen tietoturva suojaa laitteistoa lukituissa tiloissa, ja tällä tavoin varmistetaan se, ettei kukaan ulkopuolinen pääse käsiksi laitteistoon. Hallinnollisessa tietoturvassa on kyse yrityksen ja henkilökunnan riittävästä tietoturvaosaamisesta. Henkilöstön on syytä ymmärtää, miten tunnuksia käsitellään ja missä niitä säilytetään. (Suomen Internetopas 2012.)

Kun salasanoja käytetään huolellisesti ulkopuolisten silmiltä suojattuina, hankaloitetaan myös ulkopuolisten mahdollisuutta päästä käsiksi yrityksen tietoturvajärjestelmään ja vähentää myös tietoturvauhkia. Teknisellä tietoturvalla tarkoitetaan tietojärjestelmän palomuuria ja suojaustekniikoita kuten VPN (*Virtual Private Network*), SSL (*Secure Sockets Layer*), SSH (*Secure Shell*) ja PGP (*Pretty Good Privacy*.) (Suomen Internetopas 2012.)

Palomuuri suodattaa julkisen ja yksityisen verkon välillä tapahtuvaa liikennöintiä sekä estää esimerkiksi tietokonevirusten pääsyn tietojärjestelmään. Yleensä palomuuri sisältää erillisiä laitteita ja sovelluksia, jonka avulla liikennöinnin suodattaminen tapahtuu, kuten reititin ja sovellus tietokoneella. Palomuureja on monenlaisia, ilmaisversioina tai maksullisina versioina, mutta yleensä riittää

esimerkiksi Windows – käyttöjärjestelmän oma palomuuri yhdessä virustorjuntaohjelman kanssa suojaamaan tietokonetta. (Suomen Internetopas 2012.)

VPN:n avulla luodaan salattu yhteys esimerkiksi kahden verkon välille käyttäjän huomaamatta. SSL:ssa salataan käyttäjän ja palvelimen välinen tunnistaminen, SSL:ää käytetään pankkipääteyhteyksissä. SSH on Unix-palvelimille ja - koneille tarkoitettu salausprotokolla. PGP:tä käytetään sähköpostien salauksessa, jonka avulla käyttäjä voi itse suojata PGP:n menetelmän avulla vastaanottamiaan ja lähettämiään tiedostoja sähköpostiviestien kautta (Ruohonen 2002, 64; Suomen Internetopas 2012).

2.1 Hallinnollinen tietoturva

Hallinnollisella tietoturvalla tarkoitetaan niin yrityksen henkilöstön riittävää yleistä tietämystä tietoturvallisuudesta. Esimerkiksi tärkeitä asiakirjoja, tunnuksia tai tietokoneen käyttöä on myös tietoturvallisesti ajatellen huomioitava erittäin huolellisesti ja tarkoin. On katsottava, miten asiakirjat jätetään työpisteelle tai kirjoitetaanko tunnuksia lapuille ja missä niitä säilytetään. Kun tiedostetaan riittävän hyvin tietoturvan tarkoitus ja panostetaan kukin omalta kohdaltamme sen huolellisesta hoitamisesta, vähennämme tietoturvavuotoja.

Henkilöstön organisoinnissa jaetaan vastuut ja tehtävät:

- ylin johto
- tietoturvallisuuden johto
- tietoturvapäällikkö
- ATK – yksikkö
- tekniset asiantuntijat
- osastojen johto ja muut esimiehet
- tietojärjestelmien omistajat ja pääkäyttäjät

Tärkeitä dokumentoitavia aihealueita ovat:

- kartoitetaan nykytilaa (millä tasolla tällä hetkellä tietoturva on)
- riskienhallinta (on olemassa sisäisiä ja ulkoisia riskejä, joita kartoitetaan ja tehdään analyysia)

- tietoturvapolitiikkaa (vastuualueiden tarkastaminen, organisointi ja viestintä, valikoidaan tietoturvasta vastaavat henkilöt ja sovitaan viestinnästä ja raportointikäytännöistä)
- laaditaan tietoturvaohjelma (ohjeistuksen ja koulutuksen tarjonta työntekijöille, tällä tavoin lisätään tietoturvatietoa)
- luodaan suunnitelmia (jatkuvuus-, toipumis- ja tietoturvan kehittämissuunnitelmien laatiminen ja ylläpito)
  (Tietojesiturvaksi 2011b.)

Työpaikan hallinnon on määriteltävä tietoturvallisuuden pääperiaatteet ja tehtävä siihen liittyvät toimenpiteet. Esimiesten vastuulle kuuluvat tiedotus, seuraaminen ja mahdollisista laiminlyönneistä huomauttaminen. Yrityksellä tulisi olla tietoturvavastaava, joka järjestää tietoturvakoulutuksen ja ohjeistuksen. Tietoturvasta vastaava tietoturva-asiantuntija voidaan myös hankkia yrityksen ulkopuolelta. On panostettava siis perusturvallisuuteen välttäen laiminlyöntejä kuten epätavallisia tietoturvaratkaisuja. (Tietojesiturvaksi 2011b.)

Niin muut tietoturvaosa-alueet kuin hallinnollinenkin tietoturvallisuus sisältää erilaisia tietoturvariskejä. Tietoriskeiltä suojautuminen on tietoturvariskien hallinnoimista. Päätehtäväksi luetaan käytännön toteuttaminen ja suojaustason seuranta suojaustoimenpiteinä. Yrityksen on tunnettava tietoturvariskit, jotta tietoturvariskejä voitaisiin ennaltaehkäistä riskien hallinnoimisella, riskien arvioimisella ja analysoimalla. (Paavilainen 1998, 52 – 56.)

Riskianalyysi selvittää erilaisiin kohteisiin liittyviä tietoturvariskejä. Riskienhallinta sisältää erilaisia toimenpiteitä kuten miten tietoturvariskit vältetään, estetään, havaitaan, kuinka niistä toivutaan ja miten sellainen tilanne pyritään korjaamaan, johon on jollain tapaa iskenyt jo tietoturvariski. On olemassa ennakoivaa toimintaa, seurantatoimenpiteitä ja jo vahingon sattuessa olevia toimenpiteitä. (Paavilainen 1998, 52 – 56.)

Vaikkei tietoturvallisuutta pitäisi ajatella rahallisesti, on se kuitenkin tietyissä kohtaa aika arvokastakin. Toisaalta, kun ajatellaan tilannetta, jossa ei panosteta tietoturvallisuuteen, käy tietoturvauhat monta kertaa kalliimmaksi kuin se, että

tietoturvallisuuteen panostettaisiin. Tietoriskejä arvioidaan mm. tietoverkkojen, tietojärjestelmien ja tietoon liittyvien ja kohdistuvien tietoturvauhkien ja riskien kautta. Arviointi ei kuitenkaan ole ihan niin helppoa, kuin sen kuvitellaan olevan. Tietoverkot – ja järjestelmät ovat monimutkaisia, ja täten myös riskien arvioinnit monimutkaistuvat. (Paavilainen 1998, 52 – 56.)

Millaisista toimenpiteistä tietoturvauhkien vähentäminen sitten koostuu? Tällaisia toimenpiteitä ovat mm. uhkien määrittely, uhkien aiheuttamien riskitekijöiden tunnistaminen, uhan toteutumisen seurausvaikutuksen arvioiminen, suojaustavoitteiden määrittely, luodaan erilaisia toimenpiteitä, joiden avulla toteutetaan suojaustavoitteissa annetut vaatimukset sekä käytetään mittareita, jotka varmistavat toteutuksien onnistumiset. (Paavilainen 1998, 52 – 56.)

Riskianalyysin avulla selvitetään erilaisia tietoturvauhkia, niiden todennäköisyyksiä ja vahinkojen suuruuksia. Riskianalyysi käsittää yhteensä seitsemän erilaista mutta tärkeää sekä ennakoivaa toimenpidettä tietoturvauhkia ajatellen, ja ne ovat:

- tietoarvojen tunnistaminen
- arvojen määrittely
- uhkien tunnistaminen
- haavoittuvuus
- riskien todennäköisyys
- turvallisuustoimenpiteet
- tietoturvaohjelman seuraaminen ja mahdolliset korjaukset
  (Paavilainen 1998, 60 – 73.)

Riskianalyysin valmistuessa, tehdään päätöksiä riskien hallinnoimisesta. Kyseessä on tietoturvaohje. Yritys varautuu tietoturvauhkiin riskienhallinnan avulla. Tähän alueeseen halutaan panostaa mm. liiketaloudellisista syistä, tietojärjestelmien käytöstä, henkilöstön luotettavuuteen liittyvien seikkojen takia, lakisäädösten puitteissa, teknologisista syistä, erilaisten tietoturvastandardien perusteilla ja tietoverkkojen vuoksi. (Paavilainen 1998, 60 – 73.)

Yritykseen kohdistuvassa tietoturvarikoksessa kyse on yleensä tietotekniikkaan kohdistuvasta rikoksesta. Usein tietoturvarikoksen tekijä on yrityksen henkilökuntaa, joka tietää millaista tietojärjestelmää yritys ylläpitää ja miten ne ovat suojattu. Tietoturvarikoksen onnistuessa, tekijä on yleensä itse hyvin perillä tietoteknillisistä asioista ja on kykenevä tietoturvauhkien ja rikosten tekoon. Jos vastaavasti henkilö varastaisi yritykselle kuuluvia laitteistoja tai ohjelmistoja, kyseessä olisi varastaminen eikä niinkään tietoturvarikos. Jos yrityksen arkaluontoista tietoa vuodetaan ulkopuolisten tietoon, on kyseessä yrityssalaisuuden paljastamiseen liittyvä rikos. (RL 30:11§) Tietojärjestelmään voidaan myös tunkeutua ja varastaa sieltä tietoa. (Paavilainen 1998, 76 – 79.)

Tietotekniikkaan liittyviä rikoksia on erilaisia. Osa näistä kohdistuu laitteisiin kun taas osa tietoihin. Onnettomuudet, laitteistoon tai ohjelmistoihin liittyvät virheet, inhimilliset erehdykset, tahallinen tuhoaminen, väärinkäytökset ja rikollisuus, yritysvakoilut ja tietovuodot ovat yleisimpiä vahinkoja tai väärinkäyttöjä erilaisissa tietoturvarikoksissa. Tietorikoksen sattuessa on varmistettava tapahtumien yksityiskohtainen kirjaaminen ja tekijän etsiminen. Mikäli kyseessä olisi tietotekniikkarikos, on tärkeää toimia harkinnanvaraisesti niin, ettei tekijä huomaa hänen rikollisia tekemisiään (Paavilainen 1998, 76 – 79.)

2.2 Tietoaineiston tietoturva

Tietoaineistoturvallisuudessa on kysymys erilaisten materiaalien asianmukaisesta suojaamisesta. Myös tietoaineistoturvallisuudelle voidaan asettaa erilaisia luokituksia. Tietoaineistoturvallisuudella hallinnoidaan ja säilytetään tietovälineitä jokaisessa vaiheessa, mitä tietojenkäsittely vaatii sen olevan. Tietoaineiston tärkein päämäärä on suojata, varmistaa, säilyttää ja hävittää tietoa. (Paavilainen 1998, 26.)

Tärkeitä ja olennaisia tietoaineiston tietoturvaan liittyviä toimenpiteitä ovat mm. käyttöoikeuksien määrittäminen, tiedostojen varmuuskopiointi ja palautus sekä tiedon turvallinen säilytys ja tuhoaminen.

Tietoaineiston turvallisuudessa tärkeitä dokumentoitavia asioita ovat

- inventaario
- luokittelu
- tiedon salaus
- ohjeistus

(Tietojesiturvaksi 2011g.)

Käyttäjä voi tahtomattaan tai tietämättään vahingoittaa tai tuhota tietoa. Syitä voi olla esimerkiksi ohjelmisto – tai laitteistoviat, yllättäviä vahinkoja, joita voi sattua käsittely-ympäristössä tai tietovälineiden vääränlaisesta käytöstä. On siis muistettava varmuuskopioida tietoa tarpeeksi usein, jolla voidaan ennaltaehkäistä tiedon vahingoittumista tai tuhoutumista. Varmuuskopiointi, arkistointi ja kopioiden säilyttäminen on osa tietoaineistoturvallisuutta. (Paavilainen 1998, 27.)

Tieto on ”hyvin perusteltu” tosi. Kun väitetään tiedon olemassa oloa, on tiedon oltava ennen kaikkea perustellusti tosi. Tiedon on pysyttävä muuttumattomana eikä se saa hävitä vaikka tallennetta, johon tieto on tallennettu, tai sijaintipaikkaa muutetaan jollain tapaa. Jos tietoa muutetaan, kyseessä ei ole enää sama tieto kuin alun perin ollut muuttumaton tieto. Tietoa voidaan tallentaa usealle sijainnille tai tallenteelle pysyen kuitenkin muuttumattomana. Kun tietoa muutetaan jollain tapaa, syntyy uutta tietoa, jolloin olemassa oleva tieto jakautuu kahteen tieto-osaan. Toinen osa on alkuperäinen ja toinen uutta tietoa. (Paavilainen 1998, 27 – 29.)

Tallenteelle tallennetaan tietoa ja näin ollen myös tallenteen on pystyttävä säilyttämään tallennettu tieto alkuperäisenä ja muuttumattomana eli sellaisenaan kuin tieto on tallenteelle tallennettuna. Myös tallenteiden määrä muuttuu, jos tiedot tallennetaan eri tallenteille tai vastaavasti tallenne pysyy samana, jos tietoa tallennetaan samalle tallenteelle. Tallenteita on monenlaisia. Paperitallenteiden sijaan nykytietoyhteiskunnassa käytetään yhä enemmän ja enemmän elektronisia tallennusvälineitä kuten tietokantoja, palvelimia, sähköpostia jne. (Paavilainen 1998, 27 – 29.) Nykyisin myös muunlaiset tallennusvälineet kuten CD/DVD-levyt, muistitikut, ulkoiset kovalevyt ovat suosiossa.

Kun käsitellään tietoa, on pyrittävä varmistamaan tiedon koko elinkaaren mittainen turvallinen käsittely aina alkuhetkistä loppuun saakka. Tiedon turvaluokitukset eivät myöskään saa muuttua missään vaiheessa eikä tietoa saa käsitellä ulkopuoliset henkilöt. Jokaisella tiedonkäsittelyn vaiheessa on siis tietoaineistoturvallisuus mukana. (Paavilainen 1998, 27 – 29.)

Tallenteiden hävittäminen on suoritettava huolellisesti ja niin, ettei tietoa jää minnekään. Jos tietoa ei hävitetä huolellisesti, jäljelle jäänyt tieto voi joutua vääriin käsiin, ja kyseessä on tietoturvariski. Erilaiset tietoturvaluokitukset määrittelevät, miten ja millaista tietoa hävitetään. Paperiasiakirjat kannattaa silpoa pieniksi silpuiksi, että se on mahdotonta koota yhdeksi kappaleeksi.

Laitteistoa hävittäessä on ensisijaisen tärkeää, ettei kovalevylle jää tärkeää tietoa, vaan poistetaan koko sisältö, jotta vältettäisiin tiedon väärinkäyttö. Sähköisen materiaalin tuhoaminen on yhtä helppoa ja tehokasta kuin fyysisenkin, kun toimintaohjeita noudatetaan. Se, että poistetaan ainoastaan tieto muistitikulta, kovalevyltä tai muulta tallennusmedialta, ei ole riittävää. Onkin olemassa erilaisia keinoja hävittää sähköinen tiedosto, kuten tuhota tallennusmedia fyysisesti niin, ettei sitä voida käyttää uudelleen. Kun tiedoista halutaan eroon täydellisesti, on tuhottava myös varmuuskopioinnit. Paperisia asiakirjoja hävittäessä silvotaan asiakirjat niin pieniksi paloiksi, että niiden uudelleen kasaaminen on hyvin hankalaa. (Paavilainen 1998, 27 – 29; Tietojesiturvaksi 2011g.)

Lisäksi on suotavaa dokumentoida poistetut ja hävitetyt arkaluontoiset tiedot ja laitteistot, jotta voidaan myöhemmässä vaiheessa tarkastella, mitä tietoa tai laitteita on hävitetty. Laitteistotietokanta sisältäisi käytössä olevat laitteet, mutta myös poistetut laitteet.

Tiedolle voidaan asettaa omat turvaluokituksensa tiedon arkaluonteisuuden ja käyttötarpeen mukaan ja turvaluokitukset määrittelevät myös tiedon julkistamismahdollisuudet. Tunnistetaan tietoa ja luokitellaan tietoa sitä mukaan, mitä tunnistaminen tapahtuu. Seuraavaksi suoritetaan työntekijöiden henkilötietoja ja muita asioita, jotka vaikuttavat osaltaan yrityksen liiketoimintaan liittyviä tietoturvallisia suojaustoimenpiteitä. Kun Tallennettaessa henkilötietoja, on muistettava

sille lain asettamat puitteet, tässä voidaan soveltaa esimerkiksi henkilötietolakia ja tietosuojalakia. Minkälaista tietoa siis tallennetaan, ja millaiseen tietoon on annettu lupa. Tieto jaetaan usein salaisiin ja julkisiin luokkiin.

Turvaluokitus auttaa työntekijöiden sisäistämistä tietojenkäsittelyyn liittyvissä periaatteissa. On suotavaa laatia ohjeistus, miten tietoturvallisesti ajatellen kannattaa säilyttää tietoa, materiaalia, välineitä jne., yrityksessä. Myös varmuuskopiointi on tässäkin tietoturvallisuuden osa-alueessa tärkeää, joten se on myös hyvä muistaa. Tietoa voidaan myös tallentaa eri tallenteille, joita ovat mm. ulkoinen kovalevy, USB-tikku, erilaiset levyt (CD, DVD, jopa ”disketit”), ja paperimuotoon, jotka on myös suojattava ulkopuolisilta henkilöiltä. On myös tarkasteltava, missä näitä säilytetään. (Paavilainen 1998, 33; Tietojesiturvaksi 2011g.)

Tänä päivänä sähköposti on vakiinnuttanut suosionsa viestimisvälineenä. Sitä käytetään niin työasioissa kuin henkilökohtaisemmissa kontakteissa. Sähköpostin välityksellä sähköpostiviestin lisäksi voidaan lähettää erityyppisiä tiedostoja, joita voivat olla erilaiset kuvat, tekstitiedostoliitteet, video/musiikkiliitteet jne. Työssä käytettävä sähköposti on työasioihin käytettävä sähköpostiviestin, eikä sitä sovi käyttää muuhun tarkoitukseen.

Kun puhutaan työelämässä käytettävästä sähköpostiviestinnästä, viestien arkistointi ei ole täysin ongelmatonta. On olemassa oma sähköpostipalvelimensa, jota varmistetaan usein ja näin myös työntekijöiden viestit säilyvät jopa vuosia. Arkistoinnilla pyritään säilyttämään saapuneet ja lähetetyt viestit. Mikäli sähköpostiviestit olisivat ainoastaan tekstisisältöisiä, arkistointi tapahtuisi helpommin ja nopeammin. Mutta yleensä viestit voivat sisältää myös erilaisia liitteitä, jotka tekevät arkistoinnista hankalampaa, kuten tekstiliitteitä, kuvaliitteitä jne. (Järvinen 2009, 107 – 109.)

Sähköpostejakin varmuuskopioidaan siinä missä muunlaista tietoa. Työelämässä sähköpostipalvelin hoitaa varmuuskopioinnit, kun taas työelämän ulkopuolella sähköpostin käyttäjä joutuu itse manuaalisesti tallentamaan haluamansa sähköpostiviestit. Tärkeät liitteet olisi suotavaa ottaa talteen esimerkiksi myöhempää käyttöä ajatellen, ja mieluiten liitetiedoston saatua, ettei tarvitsisi myö-

hemmässä vaiheessa etsiä satojen sähköpostiviestien joukosta etsimiänsä tiedostoja. (Järvinen 2009, 107 – 109.)

Ajatellen lankapuhelin aikaa, sitä käytettiin ainoastaan puhumista varten eikä lankapuhelimissa ollut oikeastaan muita lisäominaisuuksia kuin puhelinvastaaja, kun taas matkapuhelimia käytetään normaalin puheviestinnän lisäksi tekstiviestien ja mahdollisten multimediaviestien lähettämiseen, Internetin käyttöön, valokuvien tallentamiseen, soittoäänien ja videomateriaalien käyttöön, pelien pelaamiseen, kalenterimerkintöihin, asiakirjojen luontiin ja useisiin muihin käyttötarkoituksiin riippuen matkapuhelimen ominaisuuksista ja sovelluksista. Tänä päivänä myös erilaiset älypuhelimet ovat hyvin suosittuja, mutta myös tietoturvariskit kasvavat kokoajan mitä pisimmälle puhelimet kehittyvät. Myös matkapuhelimissa on tavattu haittaohjelmia. Siksi onkin suotavaa pitää huolta myös matkapuhelimen tietoturvasta. Matkapuhelimen käyttöohjeessa on usein annettu tietoturvallisia vinkkejä matkapuhelimen tietoturvasuojaamisesta. (Järvinen 2009, 129.)

Matkapuhelin on tänä päivänä yksi suosituimmista viestintävälineistä. Ensimmäinen kädessä pidettävä matkapuhelin oli kaikkien saatavilla vuodesta 1973, ja ensimmäinen matkapuhelinverkko otettiin käyttöön jo vuonna 1979 Japanissa. Matkapuhelimiin tallennetaan myös yhä enemmän tietoa, joten käyttäjän on varmistuttava, ettei arkaluontoisiin tietoihin pääse käsiksi ulkopuolinen henkilö. Tällaisia arkaluontoisia asioita voivat olla työasioihin liittyvät, mutta myös henkilökohtaisiin asioihin liittyvät tiedot. Myös kommunikoivat puhelimitse julkisilla paikoilla kovaäänisesti, jolloin tärkeimpiäkin asioita ikään kuin huomaamatta pääsee muiden korville. Matkapuhelinta vaihtaessa, tallentuu yleensä vanhaan puhelimeen tietoa SIM -kortin ja muistikortin lisäksi. Onkin syytä varmistua, ettei esimerkiksi yhteystietoja jää puhelimeen. (Järvinen 2009, 129; Wikipedia 2012a.)

Myös CD/DVD-levyille tallennetaan tietoa. Se voi olla esimerkiksi musiikkia, videomateriaalia tai muunlaista dataa. CD/DVD-levyjä on eri kapasiteettisia, toisiin mahtuu enemmän tai vähemmän sisältöä ja on muutenkin erilaisia levyjä eri tarkoituksiin. Kuinka kauan tällaiset levyt sitten säilyvät? Sehän riippuu miten

levyjä säilytetään. Levyt säilyvät sitä paremmin miten huolellisesti niitä säilytetään. Ei päästetä levyjä naarmuuntumaan, katsotaan millaiseen levyn lukulaitteisiin levy asetetaan (esimerkiksi vääränlainen cd-asema voi vahingoittaa levyä) tai missä/miten levyjä säilytetään. CD-levyt voivat säilyä vuosiakin huolellisesti säilytettynä. Myös yritykset tallentavat tietoa CD-levyille. On siis tärkeää tietoturvan osalta tarkastella, missä CD-levyjä säilytetään, ja millaista tietoa levyille tallennetaan. Kun levyt halutaan hävittää, on suotavaa katkoa levyt, jonka jälkeen levy laitetaan sekajätteisiin (Järvinen 2009, 295, 307).

2.3 Henkilöstöturvallisuus

Henkilöstöturvallisuudessa on kyse siitä, että henkilöstöön liittyvien tietoturvariskien hallinta henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta. Suurin osa tietorikoksista tapahtuu yrityksen sisäpuolelta tai entisen työntekijän toimesta. On siis varauduttava tällaiseenkin siitä huolimatta, vaikka kyse olisi henkilökunnasta. (Tampereen Teknillinen Yliopisto 2011.)

Henkilöstöturvallisuuden tärkeyttä saatetaan aliarvioida, ja tällöin syntyy myös riski, johon ei aina osata täysin varautua. Ei pidä pois sulkea sitä vaihtoehtoa, ettei yrityksen henkilöstö aiheuttaisi vaaraa ja tietoturvauhkaa yritykselle. On selvitettävä tietoturvallisuuteen liittyviä tavoitteita sekä mahdollisten laiminlyöntien seuraamuksia yritykselle. Kun työntekijä irtisanotaan tai hän irtisanoutuu itse työtehtävästään, työntekijän mukana kulkeutuu aina tietoa, ja onkin varmistettava, ettei näitä tietoja pääsisi vuotamaan, esimerkiksi jos entinen työntekijä siirtyy kilpailevaan yritykseen työskentelemään. Myös kulkuluvat, tunnukset ja muut riskitekijät on hävitettävä välittömästi, ettei niitä pystytä väärinkäyttämään.

Erotettu työntekijä voi myös kostoksi ajatella levittävänsä yrityksen tietoa eteenpäin, tuottaa vahinkoa yritykselle fyysisesti esimerkiksi tuhoamalla laitteistoa tai hävittää tai muuttaa yritykselle tärkeää tietoa. Riskejä voi olla esimerkiksi suuri tietotekniikan asiantuntemus tai kiinnostus tekemäänsä työtä kohtaan on vähäinen eikä työnteko muutenkaan tunnu kiinnostavan. Silloin tehdään usein erilaisia laiminlyöntejä. Myös asenne yleistä tietoturvaa kohtaan saattaa olla vähin-

täänkin ala-arvoista, jolloin jälleen kerran syntyy uusia riskitekijöitä. Ei välitetä, miten tunnuksia säilytetään, mihin tärkeät asiakirjat sijoitetaan, tilojen lukitseminen unohtuu jne. Riskitekijöitä voi olla useanlaisia. Pääpainona onkin välttää riskit ennakkoon ja estää riskin synty – myös pienillä teoilla on yllättävän suuri vaikutus. (PKAMK 2003b; Tietojesiturvaksi 2011c.)

Henkilöstöä kouluttamalla parannetaan heidän tietoturvatietoutta ja osaamistaan, ja näin myös saadaan ennaltaehkäistyä lukuisia tietoturvauhkia. Henkilöstön on tiedostettava oma roolinsa myös tietoturvaa ajatellen yrityksen sisällä ja työpaikalta poistuessaan. Työntekijä voi tahtomattaan tai tietämättään loukata yrityksen tietoturvaa, ja tähän auttaa yleensä henkilökunnalle järjestettävät tietoturvakoulutukset. Kun henkilökunta saa tarvittavan määrän tietoturvakoulutusta, tietoturvauhan iskiessä tiedetään miten tilanteessa toimitaan eikä synny paniikkia tai tehdä hätäisiä ratkaisuja, joista voi koitua enemmän vahinkoa yritykselle. (Paavilainen 1998, 91 – 93.)

Kun uusi työntekijä saapuu yritykseen, on hyvä mitata työntekijän luotettavuutta yritystä ja muita työntekijöitä kohtaan. Tähän liittyy erilaisia tapoja, kuinka selvitetään ja tarkkaillaan työntekijän luotettavuutta, ja näitä tapoja ovat esimerkiksi poliisilta saatu luotettavuuslausunto, mutta tähän vaaditaan hakijan hyväksyntä. Kieltäytyminen luotettavuuslausunnosta saattaa antaa tulevasta työntekijästä kuvan, ettei hän olisi luotettava tai muuten palkkaamisen arvoinen henkilö, eli kärsitään jonkunlaista luottamuspulaa, ja yleensä tämän jälkeen yritys ei välttämättä halua palkata työntekijää minimoimalla luotettavuusriskiä. (Paavilainen 1998, 91 – 93.)

Luotettavuuslausuntoa käytetään useassa yrityksessä ja se onkin hyvä keino selvittää uuden työntekijän taustaa, mutta kuten kolikolla, on myös tässä asiassa toinen puolensa, sillä mikäli työntekijä on aiemmin tehnyt virheen, on se ikään kuin häneen leimattuna myös tulevia työpaikkoja ajatellen, ja se saattaa vaikeuttaa työhön pääsyä tai vastaavasti vaikkei olisikaan mitään rikosmerkintöjä tai muuta vastaavaa, voi tällainen työntekijä tulevaisuudessa aiheuttaa yritykselle jonkinlaista vahinkoa. (Paavilainen 1998, 91 – 93.)

Millaisia voivat olla sitten jo palkatun työntekijän riskit yrityksessä? Myös jo palkattu työntekijä voi jossakin vaiheessa tehdä toiminnoillaan tai ratkaisuillaan hallaa yritykselle. Tähän vaikuttaa yleensä motivaation pula työntekoa kohtaan, työuupumus, mahdollinen henkilökohtainen kosto kokemastaan vääryydestä yritystä kohtaan tai hän saattaa myös osaamattomuutensa ja kokemattomuutensa takia aiheuttaa vahinkoa yritykselle. Kun taas työntekijä irtisanotaan tai irtisanoutuu, vie hän aina jonkin verran tietoa mukanaan. Pystytäänkö luottamaan siihen, ettei tietoa vuodeta ulkopuoliselle työntekijän lopetettua työnsä yrityksessä. On myös poistettava tunnukset, kulkuluvat ja muut työpaikalle liittyvät asiat pois käytöstä, ettei niitä voida uudelleen käyttää. (Paavilainen 1998, 91 – 93.)

2.4 Käyttöturvallisuus

Käyttöturvallisuudessa on kyse käyttöoikeuksien ja erilaisista tunnistus- ja todennusmenetelmistä. Käyttöturvallisuudella pyritään järjestelmien ja palveluiden tehokkaaseen, tarkoituksenmukaiseen ja turvalliseen käyttöön. Tietoturvan loukkaukset johtuvat usein inhimillistä tietojärjestelmän käyttöön liittyvistä asioista. Tiedon häviäminen ja muuttuminen johtuvat usein käyttäjän tahattomista teoista, vahingoista, tietämättömyydestä tai osaamattomuudesta. Tätä käyttöturvallisuutta voidaankin edistää koulutusta lisäämällä. (Teeriaho 2010.)

Käyttöturvallisuus sisältää kaiken manuaalisen ja automaattisen tietojenkäsittelyn suojaustoimenpiteet kuten salasanojen hallinnoinnin ja järjestelmien valvonnan. Huolehditaan toimivuuden valvonnasta, käyttöoikeuksien hallinnasta, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpitoon, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuuskopioinnista sekä häiriöraportoinnista. (Tietojesiturvaksi 2011d; Kunnat 2012.)

Suojataan tietojärjestelmät haittaohjelmilta palomuurein ja tietoturvaohjelmistoin. On kiinnitettävä myös huomio ulkoistettaessa tietojenkäsittelytoimintoja, otettaessa käyttöön uusia toimintamalleja ja tehtäessä hankintoja. Kun vastuut on ohjeistettu selkeästi, on helpompi syventyä sekä seurata yksittäisten tietoturvatoimenpiteiden toimivuutta. (Kunnat 2012.)

Käyttöturvallisuudessa on seuraavanlaisia menettelytapoja:

- Käyttöoikeudet ja niiden hallinta
  - määritetään käyttöoikeudet tehtävien ja roolien mukaisesti
  - roolit ja roolien saamat tiedon luku-, kirjoitus – ja muutosoikeudet
  - käyttöoikeuksien ja lisäoikeuksien jakaminen käyttäjäryhmien mukaan
  - käyttöoikeudet tulee suojata hyvin
- Käyttötoiminnan varmistaminen laitteistojen ja henkilöstön osalta
  - kyseessä on laitteiden ja henkilöstön kahdentaminen ja tarpeellisten varamateriaalien saatavuus
  - huoltosopimukset
  - varamateriaalit
  - varahenkilöstö ja sen kouluttaminen tiettyihin tehtäviin, kuten tietojärjestelmien ylläpitoon liittyvät työtehtävät ja siihen vaadittava tietotaito
  - ohjeiden teko ajatellen varahenkilöstöä että muuta henkilökuntaa, tämä kohta mahdollistaa henkilöiden riittävän osaamisen toimia tilanteissa, joissa tarvitaan ratkaisukykyä, esimerkiksi erilaiset ongelmanratkaisutilanteet
- Varmuuskopiointi
  - varmuuskopioinnilla tarkoitetaan tiedon tallentamista eri lähteisiin
  - varmuuskopiointi varmistaa tietojen pysymisen jatkuvuuden, eli jos tietokone, johon on tallennettu tietoa, hajoaa, on varmuuskopioitu tärkeää tietoa muihin tallennusvälineisiin, josta se on edelleen saatavissa
  - tämä on siis erittäin tärkeää muistaa tiedon säilymisessä
- Erilaiset suunnitelmat kuten toipumissuunnitelma ja valmiussuunnitelma
  - toipumissuunnitelmalla tarkoitetaan ennakointia erilaisia poikkeavia tilanteita ajatellen ja varmistaa toimintojen jatkuvuutta
  - toipumissuunnitelmia on esimerkiksi erilaiset hätätoimenpiteet, varmistusmenettelyt, palautustoimenpiteet ja testausohjelmat
  - valmiussuunnitelmassa kyse on valtiolle tärkeistä järjestelmistä, joita ei oikeastaan käytetä tyypillisissä tavallisissa yrityksissä
- Tehtävien kahdentaminen
  - tehtävien kahdentamisessa on kyse tilanteista, jossa vältetään yritystä joutumassa sellaiseen tilanteeseen, jossa jokin toiminta olisi vain yhden henkilön ohjaksissa

  - kahdentamista hoidetaan esimerkiksi erilaisin sijais- ja varahenkilöstöin
- Tehtävien eriyttäminen
  - tehtävien eriyttämisellä tarkoitetaan toimintoja, jotka estävät vaarallisten työryhmien syntyä
  - riskit; roolit jaetaan väärin, jolloin työryhmät sekoittavat yrityksen sisäistä toimintaa, on siis tärkeää katsoa ja määrittää työnjako tiettyjen puitteiden mukaisesti eikä niin, että siitä olisi haittaa yrityksen toiminnalle
- Toimintojen kohdistaminen (lokien pitäminen)
  - lokien avulla seurataan tietojärjestelmässä tapahtuvia toimenpiteitä

(Paavilainen 1998, 214 – 226.)

2.5 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudessa suojataan verkossa liikkuvan tiedon eheyttä, luottamuksellisuutta ja saatavuutta. Tärkeimpiä tietoliikenneturvallisuudessa huomioitavia asioita ovat mm. roolit ja vastuut, verkon rakenne, datan, ohjeistusten laadinta tietoturvauhkien varalle, ja erilaisten huolto- ja ylläpitosopimusten luominen. Varmistetaan tiedon koskemattomuus, alkuperäisyys, lähettäjän ja vastaanottajan keskeinen kommunikaatio, varmistetaan tietoliikennöinnissä käytettävien laitteistojen ja ohjelmistojen tietoturva sekä estetään väärinkäyttöä. (Tietojesiturvaksi 2011h; Paavilainen 1998, 108.)

Tietoliikenneturvallisuuteen kuuluvat mm. salaus, verkon palveluvarmuuden turvaaminen, turvallisen reitityksen järjestäminen, vain sallittujen palveluiden salliminen, vaihtoehtoisten tiedonsiirtotapojen suunnittelu ja yksityisyyden suoja. Tietoliikenneturvallisuuden ollessa hyvällä tasolla, on pysyttävä mukana tekniikoiden, sovellusten ja laitteistojen kehityksessä eli tehdä esimerkiksi laitteistohankintoja, kouluttauduttava ja pidettävä tietämys tietoliikenneturvallisuutta kohtaan riittävän hyvällä tasolla. Näin myös varmistetaan suojausta ulkopuolisia uhkia vastaan. Tietoturvaohjelmistojen järjestelmissä on oltava ajan tasalla ja muutenkin hyvät, eli virustorjuntaohjelman ja palomuurin ylläpidon tärkeyttä korostetaan myös tässä tietoturvallisuuden osa-alueessa. (PKAMK 2003a.)

Jotta tietoliikennejärjestelmiä voitaisiin hallita ja luoda, on olemassa erilaisia standardeja, joiden avulla pyritään yhtenäistämään tietoliikenteen erilaisia rakenteita, ja yksi näistä standardeista on esimerkiksi ISO-standardi. Millaisia lähiverkkoja on sitten käytössä? Erilaisia lähiverkkoratkaisuja ovat mm. LAN, MAN, WAN ja VAN. Lisäksi on olemassa FDDI, ATM, Apple LocalTalk verkkoratkaisuja. Jo 90-luvulta alkaen tietoliikenneverkkojen yleistyminen ja tietoliikennekapasiteettitarpeiden kasvaminen on ollut vauhdikasta ja sitä se on edelleenkin, tekniikka kehittyy koko ajan, ja on oltava kehityksessä mukana. Nämä seikat ovatkin aiheuttaneet ongelmia järjestelmien käytettävyyttä ajatellen. (Paavilainen 1998, 109, 116 – 119, 137 – 139.)

Sisäisiä uhkia ovat mm.

- yrityksen henkilökunta
- ulkopuoliset henkilöt
- ohjelmisto – ja laitteistoviat
- ilkivalta
- luonnonkatastrofit ja onnettomuudet
- kapasiteetin määrä

Kuten henkilöstöturvallisuudessa myös tietoliikenneturvallisuudessa henkilöstö voi tietämättään aiheuttaa vahinkoa yritykselle. Henkilökunta onkin yksi suurimmista uhkatekijöistä yritykselle. Tällaisia henkilöstön toimenpiteistä johtuneita uhkia voivat olla esimerkiksi tietotaidon vähäisyys, tiedon luottamuksellisuuden, eheyden ja käytettävyyden horjuminen, kapasiteetin kuormitukset ja tietojärjestelmän luvaton käyttö sekä henkilökunnan välinpitämättömyys ja motivaation puute. (Paavilainen 1998, 109, 116 – 119, 137 – 139.)

Ulkoisia uhkia ovat mm.

- hakkerointi tietojärjestelmään tai verkkoon
- työpaikan sisäisten asioiden, henkilöiden tmv. vakoilu tai salakuuntelu
- siirtohäiriöt
- kapasiteetin määrä
- verkkoon liittyvien aktiivilaitteiden manipulointi (aktiivilaitteet kuten keskitin, kytkin, reititin)

Edellisessä luetelmassa mainitaan sana hakkerointi. Hakkeroinnilla tarkoitetaan tahallista tunkeutumista järjestelmään aiheuttaen vahinkoa ja ylimääräisiä kuluja yritykselle. Pahemmillaan hakkeri voi tuhota tietojärjestelmiä käyttökelvottomiksi käyttäjilleen, ja varastaa arvokasta tietoa, mutta myös sotkea tietoliikennettä (Paavilainen 1998, 109, 116 – 119, 137 – 139).

2.6 Fyysinen turvallisuus

Fyysisen turvallisuuden tärkein tehtävä on suojata järjestelmiä erilaisilta fyysisiltä uhkilta ja vahingoilta, jotka voivat olla ihmisten tai luonnonilmiöiden aiheuttamia. Fyysiseen turvallisuuteen kuuluvat mm. rakenteen suojaus, lukitus, kulunvalvonta, tekninen valvonta, vartiointi, murtosuojaus sekä palo-, vesi-, sähkö- ja ilmastointivahinkojen torjunta. Suojataan siis yrityksen toimitiloja ja niissä sijaitsevia laitteistoja. On varmistettava, ettei jokin onnettomuus kuten tulipalo, vesivahinko tai maanjäristys pääse tuhoamaan tietoa tai laitteistoa. Pyritään välttämään riskit kulunvalvonnan, vartioinnin, hälytysjärjestelmien ja lukitusten avulla, muistetaan tietojen varmuuskopiointi. (Teknillinen korkeakoulu 2012.)

Yrityksen ominaisuudet vaikuttavat siihen, millaiset suojauskeinot kannattaa asettaa. Jokainen yritys, ominaisuuksista huolimatta, tietenkin turvataan mahdollisimman hyvin tietoturvallisuutta ajatellen. Asetetaan tietyt tietoturvatavoitteet, joita pyritään noudattamaan parhaimmalla mahdollisella tavalla. Miten tilat, ohjelmistot ja laitteistot esimerkiksi turvataan ulkopuolisilta. Keskitetään kuitenkin tietoturvallisuutta sitä mukaan, millaisesta yrityksestä on kyse. Esimerkiksi jos kyse on ohjelmistoyrityksestä, jossa on useita palvelimia ja erilaisia sovelluksia käytössä, jotka vaikuttavat olennaisesti yrityksen toimintaan, keskitetään fyysistä turvaa eritoten näille ominaisuuksille. Vastaavasti jos kyse olisi vähemmän tietoteknisestä yrityksestä, otetaan tietoturvallisuus enemmän huomioon muissa ominaisuuksissa. (Tietojesiturvaksi 2011a.)

Myös fyysisessä tietoturvassa on suotavaa luoda kirjallista materiaalia ja dokumentaatiota tietyntyyppisistä asioista, ja näitä ovat mm.:

- turva-alueiden määrittely
- suojaus

- koulutus
- riskitekijät

Kuten tietoaineistoturvallisuudessa, myös fyysisessä tietoturvassa voidaan asettaa turvaluokituksia. Kun kyseessä on fyysinen tietoturvallisuus, luokitellaan yrityksen toimitiloja sitä mukaan, miten niitä käytetään ja millaisessa roolissa ne ovat yrityksessä. Yleensä alemmalle tasolla turvaluokituksessa luokitellaan aulatilat tai muut vastaavat julkiset tilat. Toisaalta asiakaspalvelupisteissäkin voidaan säilyttää tärkeitä tietoja ja dokumentteja, joten tätä ei sovi unohtaa eikä laiminlyödä tästäkään huolimatta. Ulkopuolisilta tulee evätä pääsy myös muihin työhuoneisiin ja suojata ne riittävän hyvin. (Tietojesiturvaksi 2011a.)

Lisäksi tulee varautua myös erilaisiin vahinkoihin, joita voivat olla erilaiset luonnonmullistukset, sähkökatkokset, vaarallisiin kemikaaleihin liittyvät tilanteet sekä vahingonteot. Tiloja suojatessa on otettava huomioon erilaisia suojausluokkia, joita ovat mm. fyysisen turvallisuuden suojaaminen, jotka kattavat mm. asianmukaiset säilytystilat ja lukittavat kalusteet, tässä on perussuojaamisesta. Tehostetuksi perussuojaamiseksi kutsutaan taas sellaista tilaa, jossa perussuojausta täydennetään kulunvalvonnalla ja rikokseen liittyvillä ilmoituslaitteilla. Erityissuojauksessa suojataan tilat perussuojauksen lisäksi palo- ja murtohälytinjärjestelmillä. Fyysinen tietoturva on siis yhtä tärkeää tietoturvallisuudelle siinä missä muutkin tietoturva-aihealueet. Jos tämä tietoturvan aihealue ei olisi kunnossa, ei myöskään muutkaan aihealueet olisi toimivia, eikä tällöin voida luottaa yleiseen tietoturvallisuuteen. (Paavilainen 1998, 96 – 106.)

Kulunvalvonta vaikuttaa yrityksen tietoturvaan sitä mukaan mitä arkaluonteisimpia tietoja käsitellään. Kulunvalvonnan tärkeänä tehtävänä on mahdollistaa niille henkilöille, joilla on oikeudet päästä liikkumaan työtiloissa, pääsevät liikkumaan työtiloissa, kun taas sellaiset, joilla ei ole lupaa liikkua työtiloissa, eivät myöskään sinne pääse. Kulunvalvonta valvoo myös tiloissa liikkuvia henkilöitä ja rakennuksessa olevien ihmisten lukumäärää. Tulipalon tai muun katastrofin sattuessa, nämä tiedot ovat ratkaisevassa roolissa mm. pelastautumisen vuoksi. Lisäksi myös voidaan valvoa mahdollisesti niitä henkilöitä, jotka ovat päässeet käsiksi yrityksen laitteistoihin.

Kulunvalvonta tietoturvallisuutta ajatellen, luodaan tietoturvatasot, joita voivat olla esimerkiksi yrityksen tiloihin perustuvat tietoturvatasot: Julkinen tila (aula, asiakaspalvelu jne.), varsinaiset työtilat (eristetty alue julkisesta alueesta), tilat, joissa säilytetään salaisia tietoja, kuten asiakirjoja, palvelintilat, laitteistotilat jne. Niiden mukaan rakennetaan fyysinen, portaittainen turvaluokitus tai vastaavasti luodaan tietoturvatasot asiakirjoille, laitteistoille, ohjelmistoille jne. (Paavilainen 1998, 97 – 98; 100 – 101).

2.7 Laitteistoturvallisuus

Laitteistoturvallisuudessa on kyse teknisten laitteiden suojaamisesta. Tietoturvallisesti ajatellen tärkeitä kohteita voivat olla esimerkiksi kannettavat, palvelimet, tulostimet ja matkapuhelimet. On suotavaa kirjata jokainen laite erilliseen asiakirjaan. Tietokoneiden ja muiden laitteistojen ylläpitoa myös helpottaa kunnollinen laitteistodokumentti. Asiakirjaan on suotavaa sisällyttää laitteiden ominaisuudet, komponentit, asennetut ohjelmistot, mahdolliset huoltosopimukset ja muut tarvittavat asiat kuten missä tiloissa laitteita pidetään, sarjanumerot jne. Henkilöstön tutustuttaminen laitteistoihin ja muihin yleisiin ohjeisiin on tärkeää, sillä moni ei tiedä, että myös hajonneen tietokoneen kovalevyn sisältö voi olla luettavissa huolimatta siitä, vaikkei kone olisi toiminnassa. (Tietojesiturvaksi 2011e.)

Miten sitten turvataan laitteistoa? Laitteiston turvallisuuden suunnittelu ja toteutus voidaan esimerkiksi aloittaa inventaariolla. Organisaation kannattaa selvittää, millaisia laitteita on käytössä ja minkälaisia suojauksia laitteet tarvitsevat. Yrityksen johto määrittää omien laitteiden käyttöpolitiikkaa. (Tietojesiturvaksi 2011e.)

Myös laitteiden sijainti vaikuttaa tietoturvallisuuteen. Miten toimitilat on suojattu varkauksien ja muiden fyysisten uhkien riskitekijöiltä. Laitteita ei kannata sijoittaa ulospääsyteiden läheisyyteen, sillä näin ne ovat helposti vietävissä pois yrityksen toimitiloista. On suotavaa pitää hälytysjärjestelmä kytkettynä aina, sillä jos ne eivät olisi kytkettyinä kuin ainoastaan öisin tai silloin kuin talossa ei ole muuta väkeä, voidaan tilaisuutta käyttää hyväkseen, ja varkaus on helpompaa

suorittaa. Lisäksi on varmistettava tietoturvaa lukituksilla ja pääsynvalvonnalla. Pääsynvalvonnalla varmistetaan se, etteivät ulkopuoliset henkilöt pysty käyttämään laitteita luvattomasti. Esimerkiksi tila, jossa säilytetään palvelinta, tulee tietokoneiden luvaton käyttö estää fyysisesti ja mahdollisten etäyhteyksien kautta. (Tietojesiturvaksi 2011e.)

Laitteistoa kannattaa myös huoltaa tietyin aika välein. Pitämällä laitteisto toimintakunnossa, voidaan välttyä odottamattomilta yllätyksiltä, kuten jos palvelin hajoaa, tuottaa se ylimääräistä työtä ja kustannuksia. Rikkoutumista voidaan minimoida varmistamalla jatkuva sähkönsyöttö ja suojaamalla laitteisto ulkoisilta uhkatekijöiltä, joita voivat olla esimerkiksi vedestä ja lämpötilojen vaihteluista johtuvat ongelmat. Tavoitteena on siis se, että ongelmatilanteissa tietojen luottamuksellisuus, eheys ja saatavuus säilyvät. Jos ylläpitoa laiminlyödään, voi rikkoutuneen laitteen mukana hävitä yritykselle tärkeitä tietoja. (Tietojesiturvaksi 2011e.)

Laitteistoturvallisuus käsittää siis laitteistoon liittyvää turvallisuutta ja niihin liittyviä varusohjelmistoja. Tällaisia turvallisuusosa-alueita ovat mm. laitteiston tunnistamiset, eristämiset, pääsynvalvonta, tarkkailuun ja paljastumiseen liittyvät toimenpiteet ja laadunvarmistaminen. Laitteistoja ovat erilaiset palvelimet, kämmentietokoneet, tulostimet ja erilaiset verkkokomponentit kuten mm. reitittimet ja kytkimet. Palvelimia ovat mm. tietokantapalvelimet, tulostuspalvelimet ja tiedostopalvelimet. Kun käytössä on useita eri palvelimia, myös ylläpidolliset työt lisääntyvät. (Tietojesiturvaksi 2011e.)

Laitteistoon liittyvien tietoturvavaatimusten on käytävä yksi yhteen tiedon ominaisuuksien kanssa. Tiedot tulisi luokitella niin, että luottamuksellisuus säilyisi muuttumattomana, luotava säännöt tietojen käyttämiseen → kenellä on oikeus käyttää tietoa, luoda menettelytapoja, jotka estävät korkeammalla turvaluokituksessa olevan tiedon viemisen alempaan turvaluokkaan ja vastaavasti korkeimpiin turvaluokkiin kuuluvien tietojen käytön kirjaaminen ylös. Laitteistoon voi tulla erilaisia vikoja, jotka vaikuttavat työskentelyyn ja pahemmassa tilanteessa hajoavat käyttökelvottomiksi vieden mukanaan tärkeää tietoa, joita ei välttämättä ole edes vielä varmuuskopioitu.

Vikoja voivat olla mm.

- palvelinviat
- päätelaiteviat
- fyysisen verkon viat
- verkkokomponenttiviat

(Paavilainen 1998, 175–176.)

2.8 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudessa kyse on ohjelmistojen ja erilaisten sovellusta käyttämästä tietoturvallisuudesta. Ohjelmistoturvallisuudessa tärkeää on huolehtia ohjelmiston ajantasaisesta päivittämisestä ja lisenssien ajantasaisuudesta. Mikäli ohjelmistolisenssien ajantasaisuudesta ei huolehdita riittävän tarkasti, kyseessä voi olla eri sovellusten käyttökelvottomuuteen asettuminen. Ohjelmaturvallisuudessa valvotaan ulkopuolisten pääsyä käsiksi ohjelmiin ja järjestelmiin. Kun ohjelmistojen tietoturvallisuus on ajan tasalla, myös tietoturvauhat - ja riskit ovat minimaaliset siihen nähden mitä ne voisivat olla, mikäli ohjelmiston tietoturvallisuutta laiminlyötäisiin. (Tietojesiturvaksi 2011f.)

Varmuuskopiointi olisi hyvä muistaa myös tiedon jatkuvuutta ajatellen. Kun tärkeät ja tarpeelliset tiedot on varmuuskopioitu ja arkistoitu, voidaan niitä hyödyntää tulevaisuudessa tai mikäli järjestelmä kaatuu, jonka mukana menevät sitten tärkeätkin tiedostot, mahdollistaa varmuuskopiointi tietojen löytymisen jatkossa muualta, tallennetusta paikasta. Varmuuskopiointi on tärkeä operaatio, niin työelämässä kuin työelämän ulkopuolella. Hyviä suojauskeinoja ovat mm. ohjelmistojen pääsynvalvonta, ohjelmistojen tapahtumatietojen seuranta, varmuuskopiointi, asianmukainen ohjelmistodokumentaatio, asianmukaisesti laaditut ylläpito- ja huoltosopimukset sekä rekisteröityjen ohjelmistojen käyttö. On muistettava myös luoda käyttäjäkohtaiset tunnukset, joiden avulla suojataan järjestelmää ja ohjelmistoa ulkopuolisilta henkilöiltä. (Tietojesiturvaksi 2011f.)

On lisäksi mietittävä, millaisia ohjelmia yrityksessä on käytössä, ja myös työntekijöiden on kysyttävä lupa, mikäli työasemiin haluttaisiin asentaa uusia ohjelmistoja. Tällaisten ohjelmistojen on liityttävä työhön, eikä tietokoneille saa asentaa ylimääräisiä, kuulumattomia sovelluksia. Vääränlaiset ohjelmat yrityskäytössä ovat riski tietoturvallisesti ajatellen. On tarkastettava ohjelmien laatua, mistä ne hankitaan ja mitä ne sisältävät. Palvelevatko ohjelmat siis yritykselle asetettuja ohjelmallisia ominaisuuksia? Ovatko ohjelmat luotettavia, entä millainen suoja ohjelmille on luotu tietoturvauhkia vastaan? Näitä kysymyksiä on hyvä pohtia ohjelmistoa hankkiessa yrityskäyttöön. (Tietojesiturvaksi 2011f.)

Ohjelmien käyttöä on myös hyvä jollain tapaa valvoa. Valvonnan mahdollistaa esimerkiksi ohjelmistoon integroitu loki, joka kirjaa ylös kuka ohjelmaa on viimeksi käyttänyt, milloin ja minkä järjestelmän kautta. Yrityksen palvelimet olisi myös suotavaa konfiguroida, eli valvotaan järjestelmässä tapahtuvaa toimintaa. Tällä käytännöllä seurataan siis sitä, ettei järjestelmässä tapahdu mitään eisallittua, ja mikäli tällaista ilmenee, palvelin lähettää tiedot palvelimen ylläpitäjälle. Tällaisen käytännön avulla hallitaan myös ongelmatilanteita, joihin pyritään saamaan heti ratkaisu. (Tietojesiturvaksi 2011f.)

Tietotekniikka ja laitteistot ovat kehittyneet hurjaa vauhtia, mutta myös ohjelmistot kehittyvät siinä samalla. Tämä hankaloittaa osaltaan myös ohjelmistoturvallisuuden tärkeyden arvioimista.

Ohjelmistoturvallisuudessa kyse on siis lyhyesti seuraavista asioista:

- ohjelmistot ja tietokonearkkitehtuuri
- tietokonevirukset
- ohjelmistojen salaportit

Ohjelmistoturvallisuuteen liittyviä osatekijöitä:

- käyttöjärjestelmien turvallisuus
- kääntäjien turvallisuus
- sovellusten turvallisuus
- tietokonevirukset ja torjunta

(Paavilainen 1998, 185.)

2.9 Lainsäädökset

Kuten monessa muussakin asiassa, myös tietoturvallisuuteen liittyy useita erilaisia lainsäädäntöjä. Tietoturvalle itsessään ei niinkään ole laadittu omaa tietoturvalakia, vaan tietoturvaa on pääasiassa käsitelty useiden muiden määräysten ja lakien yhteydessä. Seuraavassa on listattuna näitä säädäntöjä, joita tietoturvallisuudesta puhuttaessa voidaan käyttää: (Yliopistojen tietoturva 2007b.)

Esimerkkejä tietoturvaan liittyvistä lakiasetuksista:

- Perustuslaki 2 luvun 10 § ja 12 §
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki sähköisestä asioinnista viranomaistoiminnassa (12/2003)
- Henkilötietolaki (523/1999)
- Arkistolaki (831/1994)
- Rikoslaki (39A/1889, RL 38:3, 38:5-7, 38:8, 34:1a ja 35:1 sekä 28:7)
- Valmiuslaki (1080/1991, muutos 198/2000)
- Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)
- Valtion virkamieslaki (750/1994)
- Laki kunnallisesta viranhaltijasta 11.4.2003/304
- Työsopimuslaki (26.1.2001/55)
- Asetus yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (723/1999)
- Laki huoltovarmuuden turvaamisesta (1390/1992)
- Laki sähköisistä allekirjoituksista (14/2003)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Henkilökorttilaki (829/1999)
- Laki turvallisuusselvityksistä (177/2002)
- Vahingonkorvauslaki (31.5.1974/41)
- Laki yksityisyyden suojasta työelämässä 8.6.2001/477
- Laki puolustustaloudellisesta suunnittelukunnasta (238/1960, muutokset 1241/1987 ja 623/1999)

- Väestötietolaki (507/1993, muutokset 202/1994 ja 527/1999)
- Asetus puolustustaloudellisesta suunnittelukunnasta (239/1960, muutokset 42/1981, 1391/1992 ja 444/1997)
- Viestintämarkkinalaki (369/1997)
- Laki sähköisestä viestinnän ja automaattisen tietojenkäsittelyn käyttämisestä yleisissä tuomioistuimissa (594/1993)
- Asetus valtion talousarviosta (1243/1992)
- Valtioneuvoston ohjesääntö (262/2003)
- Henkilörekisteriasetus (476/1987; 479/1988; 59/1993; 431/1994)
- Työelämän tietosuojalaki (516/2004; 759/2004)

(Uimonen 2010; Yliopistojen tietoturva 2007a.)

2.10 Haittaohjelmat ja niiden torjunta

Tietokoneviruksessa on kyse ohjelmasta, joka kopioi itseään ja pyrkii levittymään tietokoneesta toiseen aiheuttaen monia erilaisia ongelmia käyttäjille. Tietokonevirus sotketaan usein muunlaisiin haitta- ja vakoiluohjelmiin, josta ei kuitenkaan ole kyse.

Kun tietokonevirus havaitaan isäntäkoneessa, leviää virus myös helposti toiseen tietokoneeseen esimerkiksi tiedostojen, sähköpostiviestien tai tietoturva-aukkojen avulla. Tietokonevirus voi kulkeutua koneesta toiseen myös USB-tikun, CD tai DVD-levykkeen välityksellä. Virus aiheuttaa tietokoneessa erilaisia ongelmia, kuten vahingoittaa järjestelmää hidastamalla tämän käyttämistä, lukita järjestelmiä, hävittää tiedostoja, ja pahimmassa tapauksessa tuhota tietokoneen BIOS – järjestelmän, jolloin tietokone ei enää käynnisty. (Helenius 2004; Wikipedia 2012c.)

Nykyisin viruksia esiintyy myös matkapuhelimissa, pääosin älypuhelimissa. Esimerkiksi verkkosurffauksen kautta matkapuhelimeen voi päästä viruksia. Matkapuhelimiin voi myös liittää erilaisia laitteistoja, kuten oma USB-laite tai muistikortti, jonka välityksellä voi myös esiintyä erilaisia tietoturvariskejä.

Myös viruksilla on luokituksensa. Näitä luokituksia voivat olla esimerkiksi tiedostoissa ilmeneviä viruksia, komentojonoviruksia jne. Virukset luokitellaan tartunnan saaneiden kohteiden perusteella. Virukset leviävät pääasiassa verkkotyöskentelyn välityksellä, joten Internet onkin yksi virusten päälähteistä. Kyseessä on usein sähköpostitse leviävät virukset tai jos tavataan erilaisia tietoturva-aukkoja, kuten virustorjuntaohjelmiston ja palomuurin uupuminen tietojärjestelmästä. Pääasiassa virustiedostot ovat .com - ja .exe-päätteisiä, jotka voivat tunkeutua mihin tahansa suoritus - ja ajokelpoiseen tiedostoon tietokoneesta toiseen. (Helenius 2004.)

Sähköpostien avulla leviävät virukset ovat tänä päivänä ehkä yleisin tapa saada virus tietokoneelle. Yleensä myöskään jotkut sähköpostiohjelmat eivät sisällä minkäänlaisia virusten torjuntaan vaikuttavia ominaisuuksia, joka taas mahdollistaa omalta osaltaan tietokonevirusten levinneisyyden eteenpäin. Kyse voi olla sellaisista viruksista, jotka joko monistavat itseään lukuisille eri sähköpostiosoitteille tai sitten pelkästään yhteen sähköpostiosoitteeseen kerralla. Käyttäjän onkin kohdattava kriittisesti tällaiset liitetiedostot, joita hän saa sähköpostiviestien mukana. Kaikkeen ei pidä ja kannata luottaa, ei edes tuttavien lähettämiin sähköpostiviesteihin, joissa on jokin liite. On suhtauduttava siis kriittisesti sähköpostiviestintään ja käytettävä maalaisjärkeä. (Helenius 2004.)

Usein myös tunne oudosta liitteestä ja sähköpostin muusta sisällöstä estää avaamasta itse viestiä. Näin myös estetään mahdollisten virustiedostojen lähettäminen eteenpäin ja tietenkin estetään viruksen pääsyä käyttäjän koneelle. Myös päivittämällä ohjelmat ajantasaisiksi ja pidettävä ohjelmistolisensseiden voimassaolosta huoli, parannetaan tietoturvaominaisuuksia entisestään. Ajantasainen päivittäminen esimerkiksi virustorjuntaohjelmistolle, on erittäin suotavaa. Usein tosin eri virustorjuntaohjelmat päivittävät itse itsensä automaattisesti. Käyttäjän vastuulle jää yleensä ajantasainen tarkastaminen järjestelmälle virustorjuntaohjelman avulla. Järjestelmässä on oltava myös palomuuri päällä, joka valvoo verkkoliikennöintiä ja turvaa näin myös omalta osaltaan järjestelmää. Windows -käyttöjärjestelmällä on usein valmiiksi oma palomuurinsa, eikä erillisiä palomuureja tarvitse asentaa. (Helenius 2004.)

Jos tietokoneella on tai ei ole laisinkaan minkäänlaista suojausta tietoturvauhkia vastaan, peli on käytännössä jo menetetty, joten pidetään huoli järjestelmän tietoturvasta. On saatavilla paljon erilaisia virustorjuntaohjelmistoja, niin ilmaisversioina kuin maksullisina, joten valinnan varaa löytyy. On myös päivitettävä itse käyttöjärjestelmää. Usein käyttöjärjestelmä tarjoaa itse päivittämistään, ja heti tässä kohtaa onkin välittömästi suotavaa suorittaa päivitysoperaatio. Käyttöjärjestelmän päivittämisen tärkein ominaisuus on täyttää mahdolliset tietoturva-aukot. (Helenius 2004.)

Komentoriviviruksissa on taas kysymys sellaisista viruksista, jotka hyödyntävät järjestelmässä tehtäviä komentojonoja, joita tällaiset virukset käyttävät leviämiseensä. Haittaohjelmia, viruksia, matoja ja hakkereita torjutaan päivittämällä käyttöjärjestelmää, tietokoneella olevalla virustorjuntaohjelmistolla ja palomuurilla, ja lisäksi myös roskapostien torjunnalla. Käyttäjän on itse käytettävä myös maalaisjärkeään, millaisia liitteitä avaa mm. sähköpostien mukana kulkeutuvista tiedostoista, jotka voivat sisältää haittaohjelman. Virustorjuntaohjelman tärkeimpänä tehtävänä on suojata ja blokata viruksia, kun palomuurin tehtävänä on suojella tietokonetta rajoittamalla ja estämällä ei-toivottua tietoliikennettä verkosta tietokoneelle ja tietokoneelta verkkoon (Helenius 2004).

3 Koulutuksen suunnittelu

Tässä kappaleessa on perehdytty tarkemmin tietoturvakoulutuksen suunnittelu- ja toteutusvaiheisiin osaamisen sekä pedagogisten- ja sisällöllisten tavoitteiden avulla, joita koulutukselle asetetaan. Lisäksi on lueteltuina, millaista materiaalia koulutuksessa on käytetty ja millainen tarkoitus materiaalilla on koulutuksen aikana ollut.

3.1 Osaamisen kehittäminen

Ihminen kerää ja oppii uutta tietoa jatkuvasti, huomaamatta tai tarkoituksenmukaisesti. Oppimistapoja on myös erilaisia. Aiemmin kyseessä oli behavioristista oppimista, jossa tarkasteltiin lähinnä oppimista ulkoisena tiedon siirtona opettajalta oppilaalle, kun taas nykyään on kyse konstruktiivisesta oppimisesta, jolloin opitaan itsenäisesti ja aktiivisesti rakennetaan omaa tietämystä käyttäen uutta tietoa, mutta myös aiemmin hankittua tietoa ja kokemusta. (Tampereen yliopisto 2002.)

Oppimisen tunnusmerkkeinä voitaneen pitää oppimisprosessiin ja oppimiseen liittyviä tuloksia, yksilön arvoihin ja asenteisiin, tietoihin, taitoihin ja strategioihin liittyvissä muutoksissa, vuorovaikutuksesta ja muutoksista, jotka joko on tai ei ole tietoisesti tarkoituksellista. Jokainen myös oppii eri tavalla, sillä jokainen on yksilö. Ei siis ole niin sanottua yhtenäistä oikeaa tapaa oppia, vaan jokin toinen oppija voi oppia eri tavalla erilaisissa oppimistilanteissa kuin toinen oppija. On siis kehitetty erilaisia oppimistapoja ja -strategioita, joilla oppimisesta tehdään joustavaa, jossa oppija myös itse valitsee itselleen sopivan strategian. Kun ihminen tiedostaa oman tapansa oppia, pystyy hän paremmin toimimaan myös muuttuvissa tilanteissa, ja tässä kohtaa kyse on metakognitiivisista taidoista ja/tai reflektiosta. (Tampereen yliopisto 2002.)

Oppiminen on myös henkilökohtaista. Kukaan ei opi toisen puolesta ja kullekin muodostuu oma tapansa oppia. Mitä enemmän tulee ikää, sitä enemmän myös elämänkokemus karttuu, ja sen mukana asiat saavat uusia, erilaisia näkemyksiä ja tulkintoja. Oppimiseen liittyy myös erilaisia ongelmia, joita voivat olla psykologiset, asenteisiin liittyvät oppimisesteet tai muunlaiset oppimisvaikeudet. Tällaisiin ongelmiin on saatavissa myös ulkopuolista apua esimerkiksi erityisopetuksena tai neuropsykologiset avut. (Tampereen yliopisto 2002.)

Työelämässäkin vaaditaan tietynlaista osaamista, tietotaitoa riippuen siitä, missä työskennellään, ja mitä vaaditaan. Etenkin nykyään työnteon kohdistuessa yhä enemmän kiinteämpään vuorovaikutukseen, useamman ihmisen tekemän työn ja työympäristöjen laitteistojen yhteen sitominen on muodostunut uudeksi haasteeksi työelämässä. (Koskilammi 2010.)

Organisaatioon liittyvät osaamistarpeet ja yleinen kehitystarve muodostaa yksilön osaamiselle liittyviä kehittämistarpeita, organisaatiossa oleva osaamistarpeessa kyse on ammatillisesta osaamisesta sekä työntekoon edellyttämistä taidoista. Yksilöiden on huolehdittava siitä, että heidän tietotaito ja sen kehittäminen on rakennettu varmalle pohjalle. Organisaation henkilöstöä pyritään myös kehittämään esimerkiksi erilaisilla koulutusmenetelmillä. Kullakin on oltava myös asennetta ja halua kehittää itseään (Koskilammi 2010).

Alla olevassa luetelmassa kerrotaan osaamiseen liittyvät tavoitteet:

- omaksutaan ja pohditaan kutakin tietoturvan aihealuetta
- tehtävien (liite 3) avulla pyritään tarkkailemaan koulutettavien perustietoutta tietoturvasta
- laadittujen tietoturvaohjeiden (liite 1) ja tietoturvan ABC:n (liite 2) kautta kukin omalla tahollaan seuraa ja tarkastelee, miten työpaikalla pystytään itse vaikuttamaan yleiseen tietoturvaan, miten toimia mahdollisten tietoturvauhkien yllättäessä jne.
- koulutettavat seuraavat koulutusta lisäksi PowerPoint-diojen (liite 4) kautta
- koulutuksen loputtua, koulutettavat poistuvat takataskussaan uutta tietoa tietoturvasta

3.2 Koulutuksen sisältö

Tässä luvussa käydään läpi koulutuksessa hyödynnettyjä, suunnitteluun liittyviä asioita sekä koulutukseen asetettuja tavoitteita. Aluksi esittelen tietoturvakoulutuksen järjestelyyn liittyvät seikat.

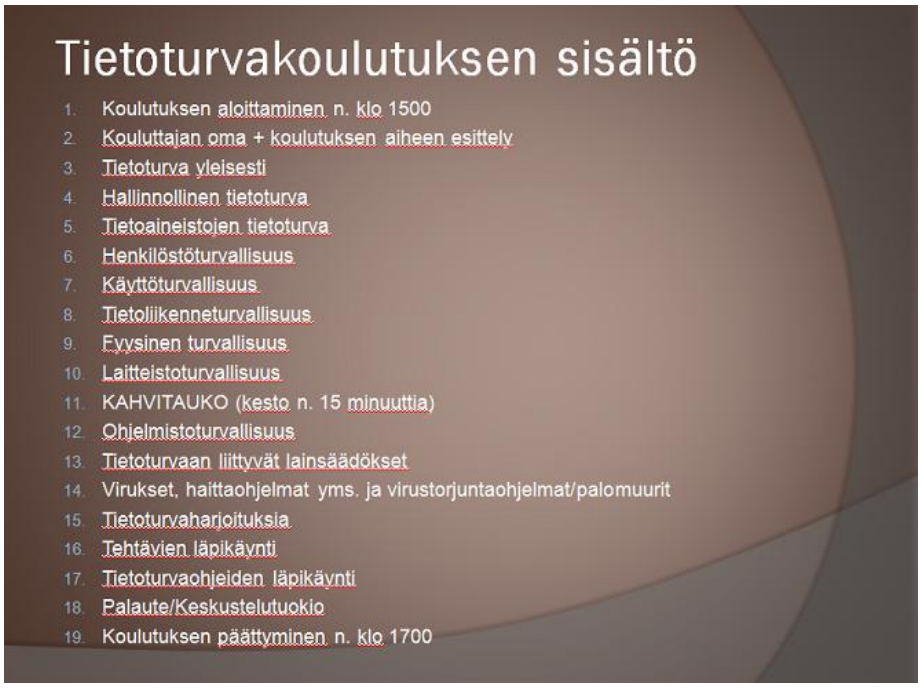
Koulutukseni kohderyhmänä ovat Rääkkylän peruskoulun opetushenkilöstö. Koulutustilana on Rääkkylän peruskoulun yläkoulun teorialuokkatila. Koulutuksessani käytetään omaa kannettavaa tietokonetta, johon on asennettu Windows 7 -käyttöjärjestelmä ja mm. Microsoft Office 2007 -työvälineohjelmisto, jota käytetään koulutusmateriaalia työstäessä ja koulutuksen aikana. Microsoft Office 2007 -työvälineohjelmistosta käytetään PowerPoint- ja Word-ohjelmistoja. Lisäksi käytössä on videotykki koulun puolelta, jonka avulla PowerPoint-diat ja

muu materiaali heijastetaan taululle. Koulutuksessa käytetään myös peruskoulun Internet-yhteyttä tutkiessamme CERT.fi -sivustoa.

Koulutusmateriaalina käytetään Word-dokumentteja ja PowerPoint-dioja. Muuna materiaalina käytetään konseptipaperia, johon koulutettavat kirjoittavat tehtävävastaukset. Lisää koulutuksessa käytössä olevista materiaaleista löytyy liitteinä olevista asiakirjoista. Koulutuksessa käytetään tarjolla olevaa laitteistoa ja ohjelmistoa. Tarkoitus on, että koulutettavat seuraavat omilta paikoiltaan koulutusta diojen ja muun materiaalin avulla, joita esittelen kohta kohdalta. Samalla selostetaan eri aihealueita, ja käytetään erilaisia esimerkkejä, jotta koulutettavat myös sisäistäisivät opetettavat asiat paremmin. Samalla koulutuksen edetessä käymme keskustelua tietoturvallisuudesta.

Tietoturvakoulutukseen liittyvät tehtävät laaditaan koulutettaville. Tehtävälomake avataan esille koulutuksen loppuvaiheessa, josta koulutettavat kirjoittavat vastauksiaan konseptipapereille. Tehtäviä on tarkemmin kuvattu liitteessä 3. Koulutuksen on tarkoitus kestää kolme tuntia, ja se pidetään iltapäivän aikana.

Alla oleva kuva 1 esittää, millainen sisältö tietoturvakoulutuksella on. Tarkempi sisällön kuvaus esitellään liitteessä 4.



Kuva 1. Koulutuksen sisältö.

3.3 Pedagogiikka

Pedagogiikassa on kyse opetuksen tavasta, sekä siihen liittyvistä näkemyksellisistä kasvatuksellisista periaatteista. Pedagogiikkaa jaetaan mm. varhaiskasvatus, aikuiskasvatus ja erityispedagogiikan alueisiin. (Wikipedia 2012b; Pedakurssi 2012.)

Pedagogiikka sisältää useita eri merkityksiä, kuten kasvatus- ja opetusoppiin/taitoon, ajatus- ja toimintasuuntaiseen ja kasvatustieteeseen liittyvää opetusta tai tutkimusta. Pedagogiikka voi olla esimerkiksi andragogiikkaa, jota sovelletaan pääasiassa aikuisten oppimisessa, tai didaktiikkaa, joka tarkoittaa kasvatustieteen osa-aluetta, jonka tutkimuskohteena on opettaminen ja oppiminen (Itä-Suomen yliopisto 2012).

Pedagogisina tavoitteina koulutuksen toteutuksen aikana olivat seuraavat kohdat:

- mielenkiinnon herättäminen ja itsenäiseen oppimiseen ohjaaminen
- käytössä oleva materiaali, joka osaltaan ohjaa pohtimaan ja päättelemään
- omien mietteiden pohdintaa, määritellään mietteitä sekä mietitään niiden perusteluja
- herätetään keskustelua aihealueiden sisällöistä, esitetään kysymyksiä ja saadaan kysymyksiin vastauksia
- opitaan uutta ja kehitytään
- pohditaan kuinka jokainen voi omilla toiminnoillaan ja valinnoillaan vaikuttamaan tietoturvaan niin työpaikalla kuin työpaikan ulkopuolella
- vuorovaikutus kouluttajan ja koulutettavan välillä

4 Koulutuksen toteuttaminen

Koulutus pidettiin siis Rääkkylän peruskoulussa, yläkoulun teorialuokassa. Koulutusvälineinä oli oma kannettavani, josta löytyivät tarvittavat dokumentit. PowerPoint-esitys, Word-asiakirjat ja muut materiaalit heijastin taululle videotykillä, joka oli luonnollisesti peruskoulun puolelta, kuten konseptipaperit ja kirjoitusvälineet, jotka oli varattu tehtäväharjoitusten tekemistä varten. Lisäksi tarvittiin

verkkoyhteys, jonka tarjosi niin ikään peruskoulu. Kohderyhmänä oli peruskoulun opetushenkilökunta.

Tietoturvan eri aihealueiden käsittely kesti n. 10 – 15 minuuttia. Tehtäviä ratkottiin yhteensä n. 35 minuuttia sisältäen tehtävien teon ja tehtävien tarkastusajan. Tietoturvaohjeiden läpikäynnissä käytettiin n. 10 minuuttia. Koulutuksen kesto hieman lyheni suunnitellusta aikataulusta, eli koulutus kesti noin kaksi tuntia. Sisällön tavoitteena oli luoda aikatauluun sopiva, mutta kuitenkin käsitellä jokaista aihealuetta ja herättää keskustelua kustakin aihealueesta. Hyvin lyhyestä aikataulusta oli kyse, ja tähän haluaisin kiinnittää tulevaisuudessa enemmän huomiota, jotta saataisiin aikaiseksi kattava ja perusteellisempi koulutuspaketti.

Arviointini koulutettavien ja koulutukseen liittyvistä arviointitoimenpiteistä perustuu vuorovaikutustilanteisiin kouluttajan ja koulutettavien välillä, sekä tehtäväharjoitusten tulosten tarkasteluihin. Kysyin alussa koulutettavilta, millainen pohjatieto heillä on tietoturvasta. Koulutuksen aikana kävimme keskustelua tietoturvan eri osa-alueista, joita koulutuksessa käsiteltiin, sekä annoimme kukin käytännön esimerkkejä omista kokemuksistamme tietoturvallisuuden saralta.

Tehtäväharjoitusten tarkastuksen aikana tein yleisiä havaintoja siitä, miten koulutettavat olivat seuranneet koulutusta ja keränneet siitä tietoa. Tämän perusteella pystyin siis arvioimaan tarkemmin koulutettavien tietoturvaosaamista. Pääasiassa käytin arviointimenetelmänä avointa haastattelutilannetta ja tarkemmin ryhmähaastattelua, jossa jokainen koulutettava sai tuoda esille asioita koko koulutuksen keston aikana.

Omien tekemieni arviointien eli tehtäväharjoitusten tuloksia vertaillessa ja avointa ryhmäkeskustelua käydessämme koulutuksen aikana, mielestäni tietoturvaan liittyvät tulivat hyvin opituksi. Arviointini mukaan uusia asioita tietoturvasta opittiin. Moni ei osannut aavistaa, kuinka laaja tietoturva aihealueena on. Oli havaittavissa kehitystä, joka näkyi tehtävien vastauksissa, ja vuorovaikutuksessa kouluttajan ja koulutettavien välillä.

Tavoitteiksi asetinkin saada hyvää pohjatietoa tietoturvallisuudesta ja pohtimaan, miten itse siihen voidaan vaikuttaa työpaikalla ja työpaikan ulkopuolella, ja että itseään voi aina lisää kehittää myös tällä saralla. Lisäksi halusin herättää keskustelua ja vuorovaikutusta esimerkiksi omien kokemusten kautta, ja vastailla esille nousseisiin kysymyksiin, sekä esittää kysymyksiä koulutettaville.

Mitä jatkossa lisäisin ja kehittäisin osaamisen osalta tällaisissa koulutustilanteissa? Ainakin tehtäväharjoitusten lisäksi voisi järjestää pienimuotoisen tentin, suullisesti tai kirjallisesti. Tämä vaatisi tietenkin enemmän myös aikataulullisesti ja suunnitelmallisesti, mutta tämä olisi mielestäni asiallinen vaihe ko. koulutuksessa, ja silloin pystyisi vielä tarkemmin seuraamaan koulutettavien kehitystä ja osaamista, ja sitä miten hyvin he seuraisivat opetusta. Lisäksi keskustelua ja kysymyksiä olisi hyvä lisätä jatkossa enemmän.

Tekemieni havaintoni perusteella, koulutettavien mielenkiinto koulutukseen oli asiallinen. Olisin toki toivonut, että jokainen olisi osallistunut keskusteluun hieman aktiivisemmin, ja usein olikin vain tietyt henkilöt aktiivisemmin keskustelua herättämässä, mm. tuoden esille pohtimiaan asioita, kysymyksiä ja kokemuksiaan, kun vastaavasti toiset olivat vähän vaisummin mukana. Tähän olisin itse voinut vaikuttaa niin, että olisin esittänyt kysymyksiäni suoraan vähemmän aktiivisemmille koulutettaville, ja näin ottanut jokaisen paremmin myös huomioon. Muuten kyllä oli hienoa seurata, miten moni halusi tuoda omia näkemyksiään esille, ja pitää yllä hyvää ja rakentavaa keskustelua.

Kehitettävää myös jäi. Olisin voinut enemmän ottaa huomioon sellaiset koulutettavat, jotka eivät olleet joko laisinkaan tai hyvin vähän keskusteluissa mukana, esimerkiksi kohdistamalla kysymyksiä suoraan heille ja ottaa mukaan keskusteluihin. Eli vuorovaikutukseen liittyviä seikkoja olisi hyvä jatkossa kehittää ja ottaa entistä paremmin huomioon.
Tavoitteenani oli edistää sekä kehittää koulutettavien omaa tietoturvallisuuden osaamista ja perustietoutta tuomalla tietoturvallisuuteen liittyviä asioita esille tavalla, jolla ne olisivat helpommin ymmärrettävissä ja sisäistettävissä. Lisäksi halusin herättää keskustelua mm. koulutettavien omista kokemuksista, joita he ovat jollain tapaa kokeneet työelämässä ja työelämän ulkopuolisissakin tilan-

teissa. Myös erilaiset koulutuksen aikana esitetyt esimerkit mahdollistivat havainnollistamista sekä asioiden ymmärrettävyyttä.

Asettamani tavoitteet toteutuivat pääasiallisesti tarkasteltuna asiallisesti ja suunnitelmien mukaisesti, mutta varmasti kehitettävääkin jäi, jotka tulee huomioida jatkossa entistä paremmin. Näitä ovat mm. jokaisen koulutettavan huomioonottaminen paremmin, koulutuksen ja opetuksen yleisen selkeyden ja sisällön kehittäminen sekä aikatauluun liittyvät kehittämiset. Kouluttajan sekä koulutettavien keskinäinen kommunikaatio ja viestintä ovat oppimisen ja itsensä kehittämisen kannalta hyvin tärkeässä roolissa, joten tätäkään kohtaa ei voi tarpeeksi peräänkuuluttaa. Myös etukäteen tehtävää suunnittelua voisi kehittää ja opetettavan/opetettavien asioiden sisältöä.

Koulutuksen sisältö oli laaja, vaikka aikataulu oli vastaavasti hyvin suppea. Sovitettavaa siis oli näiden osalta, että kustakin aihealueesta saatiin koottua sopivan kattava paketti koulutettavia ajatellen. Näistä seikoista johtuen oli selvitettävä, mitä halutaan jättää koulutuksen ulkopuolelle, mistä tietoa hankitaan ja mitä tietoa annetaan. Omien havaintojeni perusteella onnistuin tilanteeseen nähden hyvin saavuttamaan asetettuja tavoitteita koulutuksen sisältöä ajatellen.

Mitä sitten kehittäisin tällä osuudella? Jatkossa koulutustilaisuuksia ajatellen olisi varattava aikatauluun enemmän aikaa. Koulutuksen kesto voisi olla minimissään yhden päivän mittainen, jotta jokainen tärkeä aihealue tulisi käytyä tarkoin läpi. Toisaalta näin saataisiin koulutukseen myös enemmän aihealueita mukaan.

5 Yhteenveto

Ensimmäinen vaihe koko opinnäytetyössä oli päättää se, mistä sitä alkaisi työstää. Olin jo hieman aiemmin ajatellut opinnäytetyön aiheeksi jotakin tietoturvaan liittyvää aihetta. Vuonna 2010 opiskeluihin liittyvässä kehityskeskustelussa, keskustelimme opinto-ohjaajani kanssa muiden aiheiden lisäksi myös opinnäytetyöstä, ja tuolloin opinnäytetyön aihe tarkentui tietoturvakoulutukseksi.

Perehdyin tarkemmin opinnäytetyöhöni keväällä 2011, kun otin yhteyttä sähköpostitse opettajaan, joka vastasi oman koulutusohjelmani opinnäytetöistä, ja kerroin, millaisesta opinnäytetyöstä omalla kohdallani oli kyse. Samalla esitin erilaisia kysymyksiä saadakseni selvyyden, miten aloittaa opinnäytetyön tekeminen, ja millaisia vaiheita siihen kuuluu. Keskustelussamme nousi esille asioita, joita tietoturvakoulutukseen voisi sisällyttää, kuten esimerkiksi tietoturvaan liittyvät aihealueet. Itse en vielä tuossa vaiheessa ollut täysin tietoinen tietoturvan laajuudesta, sillä sehän on todella laaja-alainen aihe, joten opin myös uusia asioita kokoajan mitä pisimmälle opinnäytetyöni eteni.

Myös materiaalin työstäminen vei näin ollen oman aikansa aiheen laajuuden vuoksi. Etsin tietoa niin Internet, kuin kirjallisuuslähteistä. Itse materiaalia aloin työstämään kesällä sekä hieman syksymmällä vuonna 2011. Lopulliset korjaukset ja muokkaukset tein opinnäytetyöhöni vielä ennen koulutuksen ajankohtaa, kuten esimerkiksi tietoturvatehtävien valmistelua.

Tietoturvakoulutuksen kohderyhmä täsmentyi alkusyksyllä 2011, kun kysyin työharjoittelupaikkani esimieheltä, olisiko mahdollista pitää kyseinen koulutus heille, jolloin saimme sovittua koulutuksen järjestettäväksi 1.11.2011. Aluksi tarkoituksenani oli pitää koulutus opetushenkilökunnan lisäksi muille kunnan työntekijöille, kuten päiväkodin-, kunnantalon- ja kirjaston työntekijöille, mutta lopuksi kohderyhmä oli pelkästään opetushenkilökunta. Ratkaisuna tällainen muutos oli hyvä asia, sillä aikaa itse koulutukselle oli suunniteltu hyvin vähän, tietoturvakoulutus kesti yhteensä siis noin kaksi (2) tuntia.

Tietoturvallisuuteen liittyvän sisällön halusin tuoda kokonaisuudessaan koulutuksessa esille, sillä jokainen aihealue on hyvin tärkeä käsiteltäväksi, ja etenkin sen takia, jotta koulutettavat saisivat jonkinlaisen käsityksen tietoturvan laajuudesta ja siitä, miten kuhunkin kohtaan voi itse omalla kohdalla vaikuttaa. Edelleen palaten aikatauluun, oli se hyvin suppea, joten poimin jokaisesta aihealueesta tärkeimmät kohdat esille, ja kävimme keskustelua myös koulutuksen aikana koulutettavien kanssa. Pyrin kertomaan koulutettaville jokaisesta aihealueesta tiivistettyä tietoa esimerkein ja keskustelujen kautta.

Koulutuksen päättyessä oli mahdollisuus keskustella tietoturvallisuudesta sekä koulutuksesta, mutta aikaa tähän keskusteluun oli varattu vain vähän, sillä koulutukseni jälkeen tila oli varattu heti toiseen tarkoitukseen. Tietoturva on tärkeä ja laaja aihealue, joten mielestäni siihen tulisi varata aikaa huomattavasti enemmän. Minimissään noin yhden (1) päivän mittainen koulutus olisi sopivampi. Järjestämäni tietoturvakoulutus oli ensimmäinen tietoturvaan liittyvä koulutus Rääkkylän kunnassa. Uskonkin, että pitämäni koulutus avasi erilaisia näkemyksiä tietoturvallisuudesta sekä siitä, miten kukin itse pystyy vaikuttamaan arkielämässä työn sekä vapaa-ajan tietoturvallisiin tilanteisiin, ja myös lisäämään omaa perustietämystään tietoturvallisuuteen liittyen.

Miksi valitsin sitten tietoturvakoulutuksen opinnäytetyöaiheekseni? Olen itse ollut kiinnostunut tietoturvasta sekä halunnut jollain tapaa vaikuttaa siihen omalta osaltani mm. järjestämällä tietoturvakoulutuksia tai muita vastaavia tietoturvaan liittyviä opastustilanteita. Opinnäytetyöni edetessä aina alkuvaiheesta loppuvaiheisiin, opin myös itse lisää tietoturvallisuudesta ja itse koulutustilanteesta. Haluan kehittää itseäni jatkossa enemmän myös kouluttajana.

Tämä opinnäytetyön kirjallinen osuus vaati paljon aikaa ja syventymistä, jotta tästä dokumentista saatiin koulutusprojektiin sopiva kokonaisuus. Kävin läpi eri lähteitä, joista kokosin tärkeimmät kohdat opinnäytetyöhöni. Koulutusprojektin aikana PowerPoint-esitykseeni listasin muistilauseet, joita käytin koulutuksen aikana esityksessä. Tällöin koulutettavat saivat silmäillä omassa rauhassa, mitä eri aihealueet käsittelivät. Laitteistona minulla oli oma kannettava tietokone, josta tärkeimmät koulutukseen vaadittavat asiakirjat löytyivät. Käytössäni oli myös videotykki, jonka avulla heijastin esitykseni taululle. Esityksen ohjelmistona käytin PowerPoint 2007- ja Word 2007-ohjelmaa. Edellä mainittujen valintojen osalta, olin tyytyväinen lopputulokseen.

Tietoturvaohjeistus ja tietoturvan ABC:n (liite 1 ja liite 2) välitin sähköpostitse työharjoittelupaikkani esimiehelle. Tietoturvaharjoitusten (liite 3) avulla katsoin, millä tasolla koulutettavien tietoturvatietämys on. Koulutettavat tekivät tietoturvaharjoitukset asiallisesti ja niihin perehtyen. Näytin lopuksi harjoitusten vastaukset, joista koulutettavat tarkistivat omia vastauksiaan. Keräsin koulutettavilta

tehtävälomakkeet nimettöminä, ja niitä tarkastellessani huomasin, että tietoturvatason perustietämys on riittävä koulutettavilla.

Tietoturvakoulutus kireästä aikataulusta huolimatta onnistui hyvin. Haluan kuitenkin kehittää itseäni lisää ja tehdä tietoturvakoulutuksista aikataulullisesti ja materiaalisesti tarkempia ja laajempia. Tietoturva on aihe, jota pitäisi tutkia, ja siihen pitäisi perehtyä syvällisemmin. Moni yritys tai organisaatio ei sen tärkeyttä vielä ymmärrä, ja siksi tietoturvakoulutuksia olisi järjestettävä säännöllisesti.

Lähteet

Helenius, M. 2004. Tietokoneviruksista. http://www.cs.uta.fi/titu/tietokoneviruksista_v3.1.html. 12.3.2012.

Järvinen, P. 2009. Digiarkistointi – Säilytä muistot ja tiedostot. Helsinki: Sanoma Pro.

Koskilammi T. 2010. Ilkka-Yhtymän henkilöstön atk-koulutus, Asenteet ja oman osaamisen kehittäminen https://publications.theseus.fi/bitstream/handle/10024/24049/ONT.pdf?sequence=1. 5.2.2012

Kunnat. 2012. Käyttöturvallisuus. http://www.kunnat.net/fi/asiantuntijapalvelut/tyk/tietohallinto/tietoturva/Sivut/default.aspx. 12.3.2012.

Metropolia. 2010. Lyhyt tietoturvaohje. https://wiki.metropolia.fi/display/tietohallinto/Lyhyt+tietoturvaohje. 30.1.2012.

Paavilainen, J. 1998. Tietoturva. Espoo: Suomen Atk-kustannus Oy.

Pedakurssi. 2012. Pedagogiikka. http://pedakurssi.wikispaces.com/Pedagogiikka. 7.2.2012.

Pohjois-Karjalan ammattikorkeakoulu. 2003a. Tietoliikenneturvallisuus. http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva3.html. 12.3.2012.

Pohjois-Karjalan ammattikorkeakoulu. 2003b. Tietoturvan osa-alueet. http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html. 12.3.2012.

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

Suomen Internetopas. 2012a. Tietoturva. http://www.internetopas.com/yleistietoa/tietoturva/. 17.1.2012.

Suomen Internetopas. 2012b. Suojausmenetelmät. http://www.internetopas.com/yleistietoa/tietoturva/suojausmenetelmat/. 17.1.2012.

Tampereen teknillinen yliopisto. 2011. Henkilöstöturvallisuus. http://sec.cs.tut.fi/maso/materiaali.php?id=100. 12.4.2012.

Tampereen yliopisto. 2002. Oppia ikä kaikki. http://www.uta.fi/tyt/verkkotutor/oppimin.htm. 31.1.2012.

Teeriaho J. 2010. Käyttöturvallisuus. http://docs.google.com/viewer?a=v&q=cache:KU8sdgU1XgMJ:ta.ramk.fi/~jouko.teeriaho/tt8.doc+K%C3%A4ytt%C3%B6turvallisuus&hl=fi&gl=fi&pid=bl&srcid=ADGEEShuAHLpJ3R-n-bcYP0m06UWwLeIUjAKYIu59kC_8xanxbfJqNrOKxl6jIiUESlDhaWSnfqV8YEjPAq8jyb8L2-b8H_0rgavLwfkNLkldBK3Lb-K6m_Yr-8S2C0qFTos3bNLYqzB&sig=AHIEtbSZwptaazGAEEzoZQNpMaFxYbkwhQ. 31.1.2012

Teknillinen korkeakoulu. 2012. Tietoturvan peruskivet. http://users.tkk.fi/mkangasl/tsp/4.perus.html. 13.1.2012.

Tietojesiturvaksi.fi. 2011a. Fyysinen tietoturva. http://www.tietojesiturvaksi.fi/content/fyysinen-tietoturva. 31.3.2012.

Tietojesiturvaksi.fi. 2011b. Hallinnollinen tietoturva. http://www.tietojesiturvaksi.fi/content/hallinnollinen-tietoturva. 5.3.2012.

Tietojesiturvaksi.fi. 2011c. Henkilöstöturvallisuus. http://www.tietojesiturvaksi.fi/content/henkil%C3%B6st%C3%B6turvallisuus. 5.3.2012.

Tietojesiturvaksi.fi. 2011d. Käyttöturvallisuus. http://www.tietojesiturvaksi.fi/content/k%C3%A4ytt%C3%B6turvallisuus. 4.1.2012.

Tietojesiturvaksi.fi. 2011e. Laitteistoturvallisuus. http://www.tietojesiturvaksi.fi/content/laitteistoturvallisuus. 4.1.2012.

Tietojesiturvaksi.fi. 2011f. Ohjelmistoturvallisuus http://www.tietojesiturvaksi.fi/content/ohjelmistoturvallisuus. 4.1.2012.

Tietojesiturvaksi.fi. 2011g. Tietoaineistoturvallisuus. http://www.tietojesiturvaksi.fi/content/tietoaineiston-turvallisuus. 31.1.2012.

Tietojesiturvaksi.fi. 2011h. Tietoliikenneturvallisuus. http://www.tietojesiturvaksi.fi/content/tietoliikenneturvallisuus. 13.1.2012.

Tietojesiturvaksi.fi. 2011i. Tietoturvallisuuden peruskäsitteitä. http://www.tietojesiturvaksi.fi/content/tietoturvallisuuden-perusk%C3%A4sitteit%C3%A4. 25.3.2012.

Tietoturvaopas. 2012. Tietoturvaohjeet-1.pdf.
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvaohjeet.pdf. 20.1.2012.

Turun yliopisto. 2012. Tietoverkon käyttösäännöt.
https://wiki.utu.fi/pages/viewpage.action?pageId=3147883.
20.1.2012.

Wikipedia. 2012a. Matkapuhelin.
http://fi.wikipedia.org/wiki/Matkapuhelin. 26.1.2012.

Wikipedia. 2012b. Pedagogiikka.
http://fi.wikipedia.org/wiki/Pedagogiikka. 14.3.2012.

Wikipedia. 2012c. Tietokonevirus.
http://fi.wikipedia.org/wiki/Komentoliittym%C3%A4. 13.3.2012.

Yliopistojen tietoturva. 2007a. Tietoturvaan liittyviä lakeja ja asetuksia.
http://www.yliopistojentt.fi/VAHTI-CD/Sivusto/lait/index.htm.
25.4.2012

Yliopistojen tietoturva. 2007b. Tietoturvallisuus Suomen lainsäädännössä.
http://www.yliopistojentt.fi/VAHTI-CD/Sivusto/lait/suomessa.htm.
20.3.2012.

Muut lähteet

Uimonen, J. 2010. Pohjois-Karjalan ammattikorkeakoulu.
Tietoturva-opintojakso. 5.2.2012

Tietoturvaohje

- Tietoliikenneyhteydet on tarkoitettu vain työnteon käyttöön
- Käyttäjä on vastuussa käyttäjätunnuksesta ja tunnussanasta
- Käyttäjän on muistettava vaitiolovelvollisuus
- Laitteita, tietoliikenneyhteyttä sekä ohjelmistoja ei saa käyttää luvattomasti tai muuhun käyttöön mihin ne on tarkoitettu
- Jos käyttäjä huomaa laitteistossa, järjestelmästä tai muusta tietoturva-aukon, on siitä ilmoitettava välittömästi ylläpitoon eikä hyödyntää sitä itse
- Tietoliikennettä rajoitetaan jos yhteys on kuormittunut tai aiheuttaa jonkinlaisia turvallisuusriskejä
- Mikäli väärinkäyttöä huomataan, tulee niihin puuttua välittömästi

Turun yliopisto. 2012. Tietoverkon käyttösäännöt.
https://wiki.utu.fi/pages/viewpage.action?pageId=3147883. 20.1.2012.

Työtilat

- Poistuessa tiloista, on pidettävä ovet ja ikkunat lukittuina, menetpä sitten käymään WC:ssä tai kahvilla.
- Selvitä, missä tilanteessa työpisteesi on esimerkiksi tulipalon taholta, missä pidät laitteistot ja tärkeät asiakirjat työpisteessäsi, eli varmista asiaa myös paloturvallisuuden kantilta.
- Lukitse työasemasi estäessäsi luvattoman käytön työasemalla ulkopuolisilta poistuessasi hetkeksi tietokoneeltasi (Windows – käyttöjärjestelmissä lukitaan kone menemällä Käynnistä -valikon kautta, tai yksinkertaisesti klikkaamalla Windows -näppäintä ja L -kirjainta.)
- Säilytä laitteet ja asiakirjat lukituissa tiloissa ja paikoissa.
- Kun tulostat verkkotulostimella, hae tulostetut dokumentit mahdollisimman pian.
- Mikäli työpaikalla työskentelee esimerkiksi työharjoittelija, olisi jokaisen henkilökunnassa olevan henkilön tiedettävä ko. asiasta.
- Henkilökunta vastaa ulkopuolisista vierailijoista tiloissa aina siihen asti, kun he poistuvat työtiloista.

Työasemat ja laitteistot

- Hyvä salasana on sopivan pitkä ja sisältää mieluiten erikokoisia kirjaimia ja numeroita, eikä tunnuksia pidä jättää missään nimessä muistilapuille työpisteelle tmv. näkyville vaan pidettävä omana tietonaan täysin, salasanaa kannattaa myös vaihtaa tietyin aikavälein.
- Varmista, ettei ulkopuoliset pääse käyttämään työasemia tai muuta laitteistoa.
- Sijoita tietokoneen näyttö niin, ettei ulkopuoliset pääse näkemään tietoja.
- Sijoita oheislaitteet kuten tulostin niin, ettei ulkopuoliset pääse näkemään tulostettuja asiakirjoja.
- Tietohallinto vastaa kiintolevyllä olevien tietojen poistamisesta, mutta käyttäjän on suotavaa poistaa myös itse omia turhia tiedostoja koneelta koneen poistuessa käytöstä, tai otettava (vaikkei olisikaan poistumassa käytöstä) tärkeät tiedostot ulkoiselle tallennuslaitteelle.
- Kun työsuhde lakkaa, käyttöoikeudet lakkaavat myös.
- Omien ohjelmien asennus ja niiden käyttäminen ei ole sallittua työasemassa, tietohallinto voi poistaa tällaiset ohjelmat jos niistä on haittaa järjestelmän toiminnalle ilman, että informoisi siitä käyttäjää.
- Pidä huoli, että käyttöjärjestelmässä on ajantasainen virustorjuntaohjelma tietoturvariskien kuten haittaohjelmien varalta.
- Tallenna työsi säännöllisesti tai hyödynnä automaattitallennusta.
- Sulje avoinna olevat ohjelmat, mikäli poistut työpisteeltäsi pidemmäksi aikaa.
- Työasemat ja laitteistot ovat ainoastaan työkäyttöön tarkoitettu eikä niitä saa antaa ulkopuolisten käyttöön.
- Aja virustorjuntaohjelma säännöllisesti tietokoneellasi.
- Tietoturvauhan iskiessä: Älä hätäänny! Pysy rauhallisena, ota yhteys esimieheen ja tietoturvasta vastaavaan henkilöön.

Internet

- Internet – yhteyttä käytetään työtehtävien hoitamista varten, samoin työpaikan omaa sähköpostia.
- Verkkoyhteyttä valvotaan palomuuriohjelmalla.
- Ohjelmien ja työhön kuulumattomien materiaalinen lataaminen työkoneelle ei ole soveliasta.
- Mikäli havaitset tietoturvariskin, muussakin tapauksessa kuin Internetin välityksellä tapahtuva, ota välittömästi yhteys tietohallintoon.
- Tyhjennä säännöllisesti selaimen välimuistit.
- Ajan tasalla oleva virustorjuntaohjelma suojaa Internetin välityksellä tulevat tietoturvauhkat palomuurin lisäksi, joten varmista, että virustorjuntaohjelmaan on asennettu viimeisimmät päivitykset ja virustunnisteet.

Metropolia. 2010. Lyhyt tietoturvaohje.
https://wiki.metropolia.fi/display/tietohallinto/Lyhyt+tietoturvaohje. 30.1.2012.

Tietoturvan ABC

Johdanto

Tämän tietoturvallisuusohjeen tarkoituksena on opastaa Rääkkylän kunnan henkilökuntaa tietoturvasta tietojärjestelmässä. Yksi tärkein osa toimivassa tietojärjestelmässä on tietoturva.

Tietoturva

Tietoturvalla pyritään ennaltaehkäisemään vahinkoa. Tietoturvalla suojataan tietoja, palveluita, järjestelmiä ja tietoliikennettä.
Tietoturva käsittää seuraavat vaiheet:

- Hallinnollinen tietoturva
- Henkilöstöturvallisuus
- Fyysinen turvallisuus
- Tietoliikenneturvallisuus
- Ohjelmistoturvallisuus
- Tietoaineistoturvallisuus
- Käyttöturvallisuus ja
- Laitteistoturvallisuus

Laitteiston käyttäjät voivat antaa tunnuksensa toisen henkilön käyttöön, ja salasanoja voi olla kirjoitettu lapuille, jotka sijaitsevat aivan tietokoneen lähellä. Sähköposteissa taas liitetiedostoja availlaan sen ihmeemmin miettimättä tietoturvaa. Annetaan huoletta myös henkilökohtaisia tietoja Internetin kautta miettimättä kuka on kysyjä, ja mihin/miten hän tietoja käyttää. Tietoturvan osat ovat saatavuus, luottamuksellisuus sekä eheys.

Tietoturva: Riskit ja uhat

Ennakointiin ja suunnitteluun kuuluvat mahdollisten riskien tiedostaminen ja niiden löytäminen. Ne kohteet, joissa tietoa voi joutua vääriin käsiin tai ne hukataan, ovat tietoturvariskejä.

Yleisimmät riskit:

- Laitteisto

  Tietokoneen sisältö on vaarassa joutuessaan vääriin käsiin mm. varkauden tai huollon yhteydessä. On tärkeää tyhjentää sekä ottaa talteen tiedostot, joita tietokoneeseen on aiemmin tallennettu.
- Internet

  Käyttäjät voivat syöttää arkaluotoista tai muuten vain henkilökohtaista tietoa Internetissä, joita voidaan väärinkäyttää. On mietittävä, millaista tietoa annetaan, mitä vähemmän tietoa annetaan, sitä vähemmän on väärinkäytettävää.
- www-tiedostot

  www-tiedostot ja laajennukset voivat sisältää useita tietoturva-aukkoja, joihin käyttäjän on kiinnitettävä huomionsa.
- Tiedostonjako

  Kun verkossa jaetaan tarkoituksellisesti tai tahattomasti tiedostoja, se voi usein olla riskialtista tietoturvallisesti ajatellen.
- USB yms. tallennusvälineet

  On hyvin tärkeää katsoa, miten ja missä kuljettaa tallennusvälinettä. Hukattaessa tallennusväline saattaa joutua vääriin käsiin. Kun tietoja ei enää tarvita, on suositeltavaa poistaa tällaiset tiedot.
- Sähköposti

  Jos on havaittavissa epäilyttävä sähköpostiviesti, ei sitä myöskään kannata avata. Kannattaa suhtautua kriittisesti myös sähköpostiviesteissä oleviin liitteisiin, jotka voivat sisältää viruksia tai haittaohjelmia. Roskapostisuodatus ei aina tuhoa suoraan roskapostiviestiä, vaan se poistetaan manuaalisesti itse. Ei suositella avattavan linkkejä, joita roskapostiviesteissä on yleensä mukana.

Tietoturvallisuus: Kuka on vastuussa?

Koko organisaatio on vastuussa tietoturvasta. Jokaisella käyttäjällä on vastuu järjestelmän kokonaisturvallisuudesta. Tunnukset, ja siihen liittyvät salasanat ovat henkilökohtaisia, eikä niitä saa luovuttaa muiden käyttöön.

Teknisessä tietoturvassa varmistutaan siitä, ettei käytössä olevissa laitteistoissa ja ohjelmistoissa ole tietoturvapuutteita. Tietojärjestelmiin pääsyä valvotaan salasanojen ja käyttäjätunnuksien avulla. On tärkeää varmistaa tietoverkot palomuurein.

Tietoturvaopas.2012.
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvaohjeet.pdf. 20.1.2012.

Yleisiä ohjeita

1. Toimitilat ja niihin pääsy
    - määritellään normaalit ja poikkeusreitit
    - hätäuloskäynnit
    - kulkuluvista huolehtiminen
2. Miten yrityksen tiloissa toimitaan
    - yhteiset tilat ja niissä keskusteleminen
    - salassapitovelvollisuus
3. Järjestelmän tunnukset
    - tunnusten/salasanojen voimassaoloaika, salasanan vanheneminen
    - tunnusten/salasanojen sisältö ja sen ohjeistus
    - mikäli salasana on unohtunut, miten toimitaan tällaisissa tilanteissa
4. Virustorjunta
    - millainen virustorjunta on yrityksen käytössä, miten sitä ylläpidetään ja hoidetaan
    - sähköposti -> miten salaus ja liitteiden avaus on ohjeistettu
    - verkosta ladattujen tiedostojen asentaminen -> millaisia ohjelmia saa Internetistä asentaa työasemalle
5. Varmuuskopiointi
    - kuka huolehtii, miten siitä on huolehdittu palvelimissa
    - tehdään tiedostojen arkistointi varmuuskopioista huolimatta
6. Oheislaitteet
    - millaiset oheislaitteet ovat käytössä, missä niitä säilytetään/mitä niissä säilytetään
    - tulostaminen ja ohjeistus

7. Luottamuksellinen materiaali
    - missä materiaali säilytetään, miten se tuhotaan tai hävitetään
8. Työaseman ja kannettavan käyttäminen
    - poistuttaessa hetkeksi työpisteestä, lukitaan tietokone painamalla kerran CTRL-ALT-DEL -näppäinyhdistelmää
    - mikäli työasema tms. jaetaan, tarkastetaan kellä/keillä on pääsy tiedostoihin, on myös hyvä muistaa, ettei levyasemaa tule jakaa juuresta alkaen, sillä tässä tapauksessa kaikki levyllä olevat tiedostot ovat jaossa
    - kun ollaan poissa toimistotiloista, kannettavan jättö näkyville ei ole suotava
    - jos työhön liittyviä tiedostoja käsitellään kotikoneella, on huolehdittava siitä, että koneessa on palomuuri ja virustorjunta ajan tasalla
9. Esitystilaisuudet
    - esityksessä käytettävät tiedostot tulee tallentaa koneelle, tai varmistaa, ettei verkon yli päästä käsiksi niihin ennen esitystilaisuuden alkamista
    - jos tiedostoja haetaan intranetistä palaverin aikana, tämän on tapahduttava tietokoneen oman näytön kautta, ei esim. videotykin
    - palaverin jälkeen tilasta pöydiltä, fläppitauluilta tms. olevat muistinpanot
10. Internetin käyttäminen
    - Internetin käytön ohjeistaminen, käyttäminen sekä kiellettyjen www-sivujen määrittäminen
11. Alihankkijat ja freelancerit
    - yritysprojekteissa käytettävien alihankkijoiden ja freelancereiden kanssa on tehtävä tarvittavat salassapitosopimukset ennen työn aloittamista

Tietoturvaopas. 2012.
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvaohjeet.pdf. 20.1.2012.

Tietoturvaharjoitusten vastaukset

1. Mitä on tietoturva?
   - on tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä.
   - tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnonilmiöiden sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.

2. Mitä on tiedon luottamuksellisuus, eheys ja käytettävyys?
   - Luottamuksellisuus
     → Tiedot ja järjestelmät ovat käytettävissä niille käyttäjille, joilla on niihin käyttöoikeudet, tieto salataan – salattu viesti on ulkopuoliselle, käyttäjät pyritään todentamaan.
   - Eheys
     → tietojen ja järjestelmien luotettavuutta, oikeellisuutta ja ajantasaisuutta, eivätkä ne ole hallitsemattomasti muuttuneet tai muutettavissa laitteisto- tai ohjelmisto-vikojen, luonnonilmiöiden tai inhimillisen toiminnan seurauksena.
   - Käytettävyys
     → järjestelmien palvelut ja tiedot ovat niihin oikeutettujen käytettävissä etukäteen määritellyssä vasteajassa, tiedot eivät ole tuhoutuneet tai tuhottavissa vikojen, tapahtumien tai muun toiminnan seurauksena.

3. Miksi tietoturva on tärkeää?
   - On tärkeää, etteivät tiedot päädy tahallisesti tai tahattomasti asiattomien haltuun.
   - Julkishallinnoissa säilytetään ja käsitellään paljon tärkeää ja arkaa tietoa (henkilötiedot, taloustiedot, tietokantoja yms.), ja osa näistä tiedoista on salassa pidettävää, arkaluonteista tai muuten luottamuksellista tietoa, joita halutaan suojella ulkopuolisten silmiltä.

4. Onko tietoturva ja tietosuoja sama asia?
   - Ei ole, sillä tietosuojalla tarkoitetaan tietosuojalainsäädäntöön kirjoitetussa merkityksessä sitä, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava ulkopuolisten käsittelyltä.
   - Tietosuoja sisältää tietoturvan keskeisimmät ulottuvuudet, mutta lisäksi tietosuojaan kuuluu monia muita elementtejä, joihin tietoturva ei ota kantaa.
   - Tietoturva sisältää taas lukuisia osatekijöitä, jotka vain välillisesti vaikuttavat tietosuojaan.

5. Mikä on palomuurin tehtävä? Entä virustorjuntaohjelman?
   - Palomuurin tehtävänä on suojella ja tarkkailla tietokonetta rajoittamalla ja estämällä ei-toivottua tietoliikennettä verkosta tietokoneelle ja tietokoneelta verkkoon.
   - Virustorjuntaohjelman avulla suojaudutaan virus- ja matotartunnoilta, virustorjuntaohjelma etsii tietokoneelta haittaohjelmia ja estävät niiden aiheuttamia vahinkoja tai poistavat havaitut haittaohjelmat koneelta kokonaan.

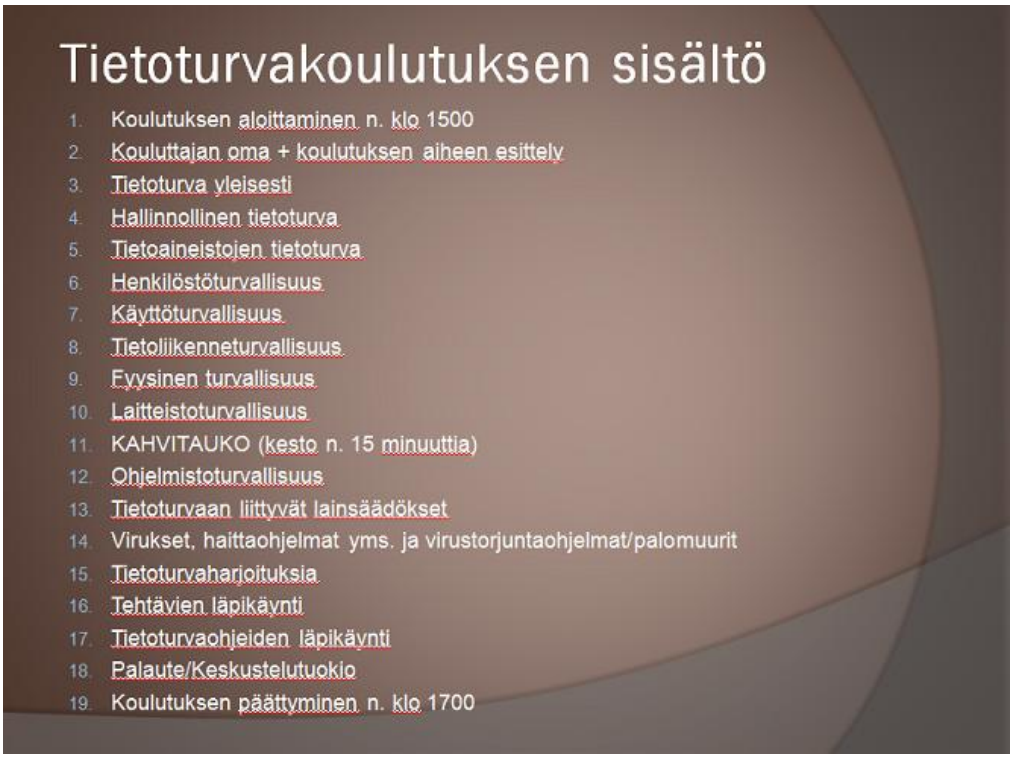
6. Millaista vahinkoa haittaohjelmat voivat tietokoneellesi aiheuttaa?
   - Virus voi käyttää tietokoneen käytettävissä olevaa muistia ja hidastaa koneen toimintaa tai estää sen toiminnan täysin.
   - Virus voi myös vahingoittaa käyttäjän tietoja, tuhota tiedot täysin tai tehdä kovalevystä käyttökelvottoman.

EXTRAKYSYMYKSET

1. Miten voit vaikuttaa omalta osaltasi työpaikkasi hyvään tietoturvatasoon?
2. Kommentoi työpaikkasi tietoturvan tasoa:
   Millä tasolla tietoturva on työpaikallasi? Kehitettävää, huomioitavaa?

HUOM!
Tehtävät palautetaan nimettöminä. Tehtävät kerätään lopuksi, josta teen yleiskatsauksen, eli koonnin, millä saralla tietoturvatietoisuus on koulutettavilla. Yleiskatsaus on pieni osa opinnäytetyötäni.

Tietoturvakoulutuksen PPT-esitys

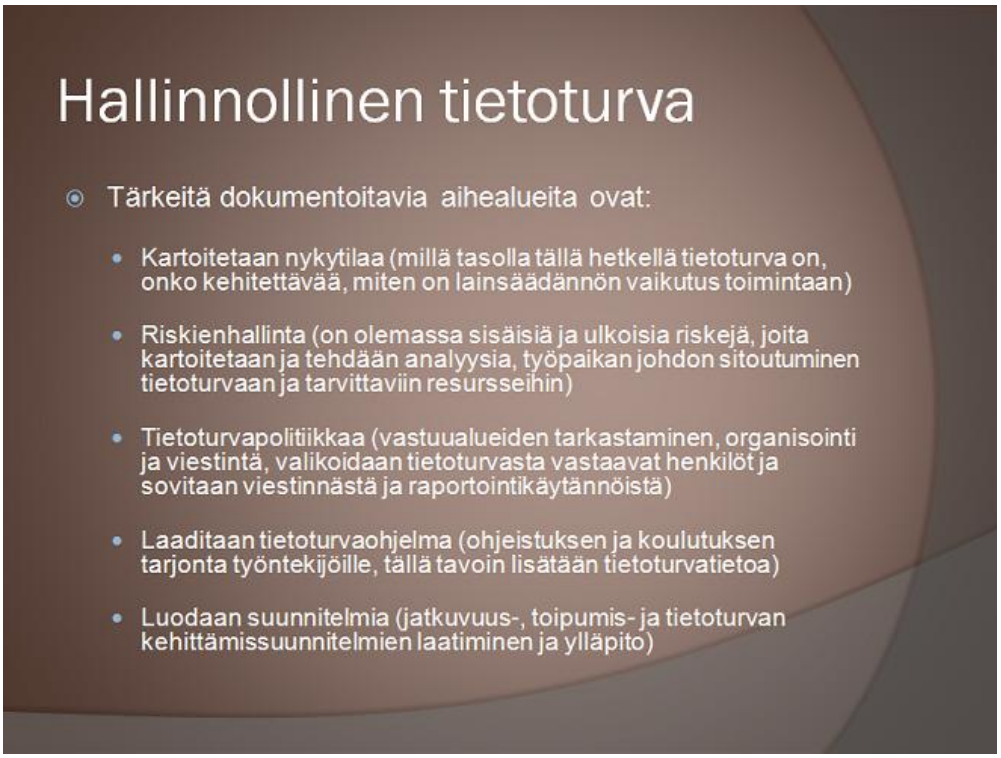


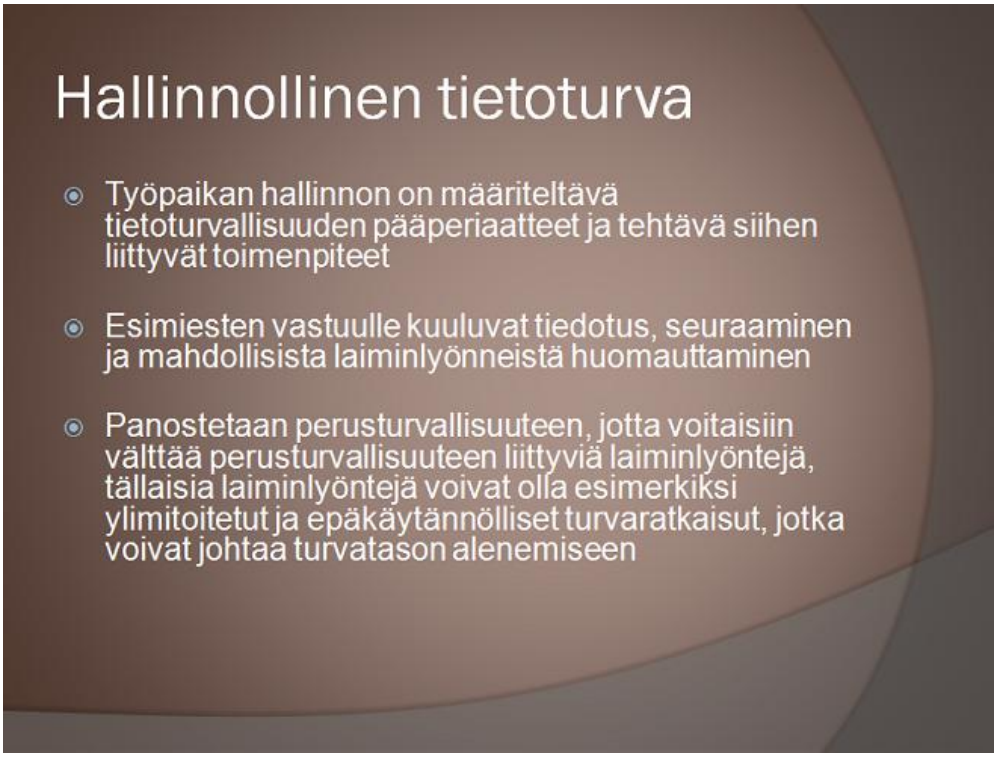
Tietoturva yleisesti

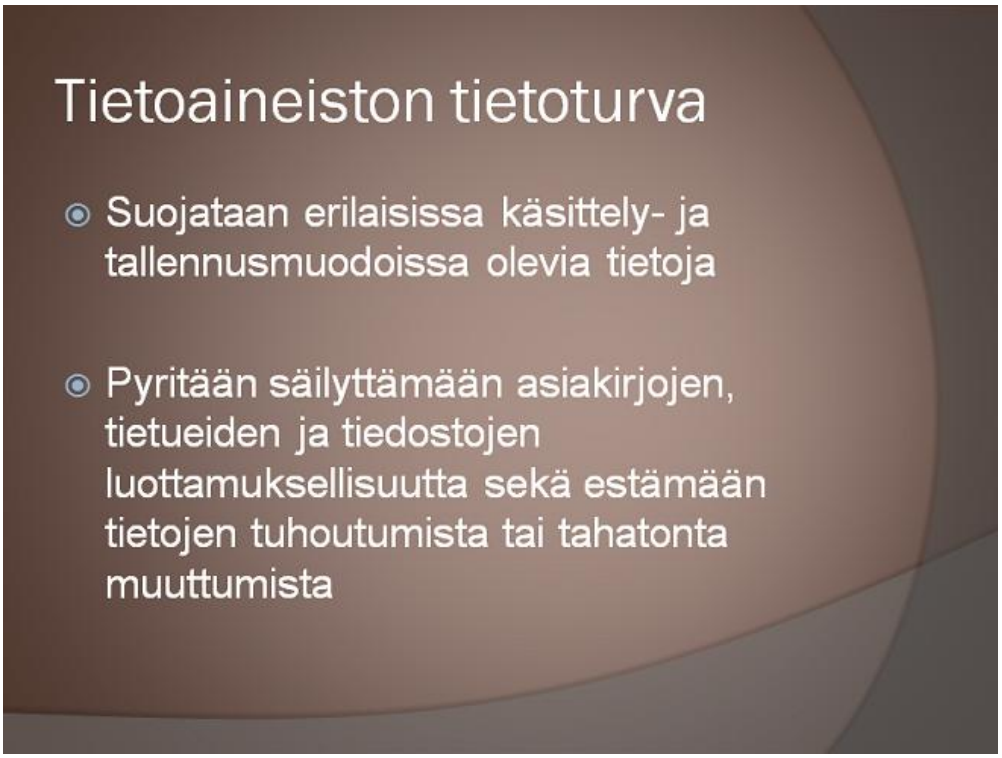
- Tiedoille ja dokumenteille on laadittu turvaluokitus, joka määrittelee kenellä on oikeus tietojen käyttöön, säilytykseen ja tuhoamiseen
- Tietoturvan tavoitteita →
  - Eheys tarkoittaa tiedon muuttumattomuutta luodessa, käsitellessä ja siirrettäessä tietoa
  - Kiistämättömyyden avulla valvotaan tiedon siirtoon tai käsittelyyn osallistuneiden käyttäjien tunnistamista varmistaen sen, ettei kukaan voi käsitellä tietoa huomaamatta
  - Pääsynvalvonnalla valvotaan ja rajoitetaan käyttäjien tietoon pääsyä
  - Saatavuudella tarkoitetaan tiedon helppoa ja viivetöntä käyttöä käyttäjille, joilla on siihen oikeus
  - Tietojenkäsittelyn tuloksena saatu tieto on kyettävä tarkastamaan ja sen oikeellisuus kyettävä osoittamaan – tässä on kyse tarkastettavuudesta
- Tietoturvalla tarkoitetaan tietotekniikan tietoturvaa ja ulkoisia tietoturvauhkia, näitä ovat esimerkiksi virukset ja haittaohjelmat

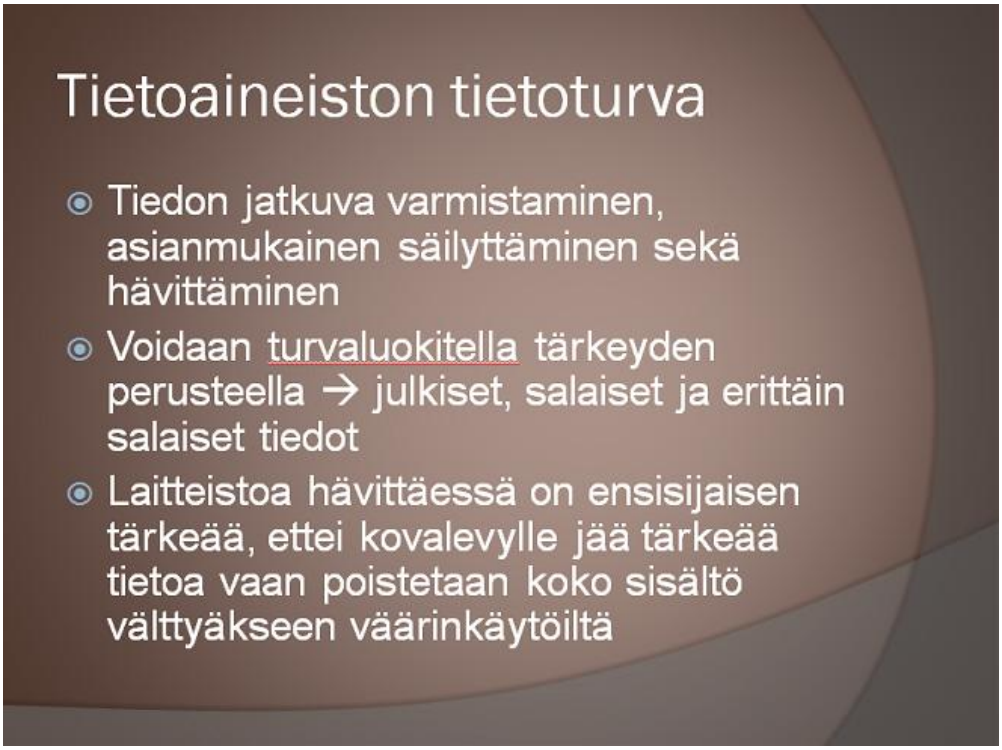
Hallinnollinen tietoturva

- On järjestettävä tietyin aikavälein tietoturvakoulutuksia pitääkseen henkilökunta ajan tasalla tietoturvasta
- Näkyvämpiä tuotoksia ovat yleiset linjaukset, erilaiset tietoturvadokumentit ja henkilöstön organisointi
- Tietoturvasuunnitelmien ja dokumenttien laatiminen auttaa selviämään erilaisista riskitilanteista


Hallinnollinen tietoturva
Tärkeitä dokumentoitavia aihealueita ovat:
Kartoitetaan nykytilaa (millä tasolla tällä hetkellä tietoturva on, onko kehitettävää, miten on lainsäädännön vaikutus toimintaan)
Riskienhallinta (on olemassa sisäisiä ja ulkoisia riskejä, joita kartoitetaan ja tehdään analyysia, työpaikan johdon sitoutuminen tietoturvaan ja tarvittaviin resursseihin)
Tietoturvapolitiikkaa (vastuualueiden tarkastaminen, organisointi ja viestintä, valikoidaan tietoturvasta vastaavat henkilöt ja sovitaan viestinnästä ja raportointikäytännöistä)
Laaditaan tietoturvaohjelma (ohjeistuksen ja koulutuksen tarjonta työntekijöille, tällä tavoin lisätään tietoturvatietoa)
Luodaan suunnitelmia (jatkuvuus-, toipumis- ja tietoturvan kehittämissuunnitelmien laatiminen ja ylläpito)


Hallinnollinen tietoturva
Työpaikan hallinnon on määriteltävä tietoturvallisuuden pääperiaatteet ja tehtävä siihen liittyvät toimenpiteet
Esimiesten vastuulle kuuluvat tiedotus, seuraaminen ja mahdollisista laiminlyönneistä huomauttaminen
Panostetaan perusturvallisuuteen, jotta voitaisiin välttää perusturvallisuuteen liittyviä laiminlyöntejä, tällaisia laiminlyöntejä voivat olla esimerkiksi ylimitoitetut ja epäkäytännölliset turvaratkaisut, jotka voivat johtaa turvatason alenemiseen


Tietoaineiston tietoturva
Suojataan erilaisissa käsittely- ja tallennusmuodoissa olevia tietoja
Pyritään säilyttämään asiakirjojen, tietueiden ja tiedostojen luottamuksellisuutta sekä estämään tietojen tuhoutumista tai tahatonta muuttumista

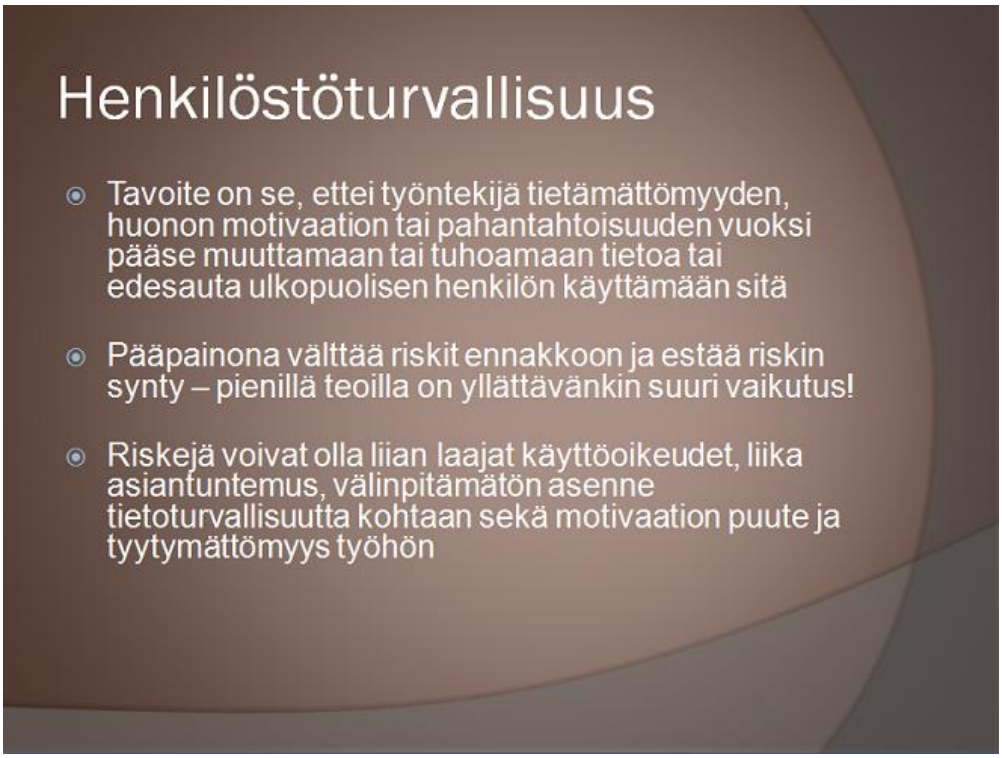

Tietoaineiston tietoturva
Tiedon jatkuva varmistaminen, asianmukainen säilyttäminen sekä hävittäminen
Voidaan turvaluokitella tärkeyden perusteella → julkiset, salaiset ja erittäin salaiset tiedot
Laitteistoa hävittäessä on ensisijaisen tärkeää, ettei kovalevylle jää tärkeää tietoa vaan poistetaan koko sisältö välttyäkseen väärinkäytöiltä

Henkilöstöturvallisuus

- Pyritään estämään työntekijöistä ja sidosryhmistä johtuvat tietoturvariskit
- Henkilöstöturvallisuuden tärkeyttä aliarvioidaan turhan usein, etenkin kun henkilöstö on organisaatiota ylläpitävä voima ja täten myös riski → yleensä henkilöstö aiheuttaa vahinkoa tietämättään, jolloin inhimillisiin vahinkoihin auttaa usein kouluttaminen

Henkilöstöturvallisuus

- On selvitettävä tietoturvan päämäärät sekä huolimattomuuden ja vahingon seuraukset
- Kun työntekijä irtisanoutuu/irtisanotaan työtehtävästään, on varmistettava, että kulkuluvat, salasanat ja muut riskitekijät mitätöitäisiin mahdollisimman pian
- Myös vierailijoiden valvonta on osa henkilöstöturvallisuutta


Henkilöstöturvallisuus
Tavoite on se, ettei työntekijä tietämättömyyden, huonon motivaation tai pahantahtoisuuden vuoksi pääse muuttamaan tai tuhoamaan tietoa tai edesauta ulkopuolisen henkilön käyttämään sitä
Pääpainona välttää riskit ennakkoon ja estää riskin synty – pienillä teoilla on yllättävänkin suuri vaikutus!
Riskejä voivat olla liian laajat käyttöoikeudet, liika asiantuntemus, välinpitämätön asenne tietoturvallisuutta kohtaan sekä motivaation puute ja tyytymättömyys työhön


Käyttöturvallisuus
Yrityksen päivittäisten toimintojen ja rutiinien turvaamista kutsutaan yleisesti käyttöturvallisuudeksi
Käyttöturvallisuus sisältää kaiken manuaalisen ja automaattisen tietojenkäsittelyn suojaustoimenpiteet kuten salasanojen hallinnoinnin ja järjestelmien valvonnan
Huolehditaan toimivuuden valvonnasta, käyttöoikeuksien hallinnasta, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpitoon, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuuskopioinnista sekä häiriö raportoinnista

Käyttöturvallisuus

- Suojataan tietojärjestelmät haittaohjelmilta
- Kun vastuut on ohjeistettu selkeästi, on helpompi syventyä sekä seurata yksittäisten tietoturvatoimenpiteiden toimivuutta

Tietoliikenneturvallisuus

- Tarkoitetaan siirrettävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaamista tietojen siirron aikana
- Tietoliikenneturvallisuuteen kuuluvat mm. salaus, verkon palveluvarmuuden turvaaminen, turvallisen reitityksen järjestäminen, vain sallittujen palveluiden salliminen, vaihtoehtoisten tiedonsiirtotapojen suunnittelu, yksityisyyden suoja jne.

Tietoliikenneturvallisuus

- Kun pyritään pitämään tietoliikenneturvallisuutta riittävän korkealla tasolla, on pidettävä jatkuvasti silmällä alan kehitystä, hankittava laitteistoja tai ohjelmistoja, joilla suojaudutaan uusia uhkia vastaan
- Palomuuriratkaisuilla voidaan vaikeuttaa ulkopuolisten tunkeutumista organisaation sisäiseen verkkoon

Fyysinen tietoturvallisuus

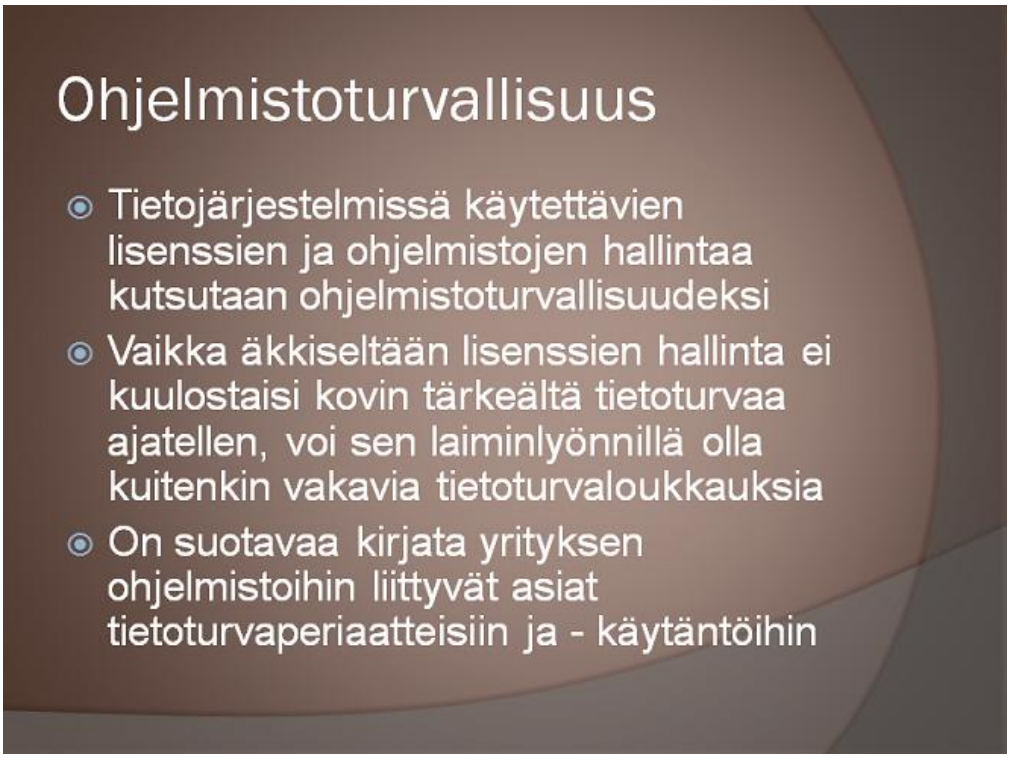
- Tavoite: Varmistaa, ettei kukaan ulkopuolinen pääse kiinni fyysiseen verkkoon tai kopioimaan tietoja tai varastamaan laitteistoja, komponentteja tai muita tiedon tallennusmedioita
- Suojataan yrityksen toimitiloja ja niissä sijaitsevia laitteistoja
- On varmistettava, ettei jokin onnettomuus kuten tulipalo, vesivahinko tai maanjäristys pääse tuhoamaan tietoa tai laitteistoa

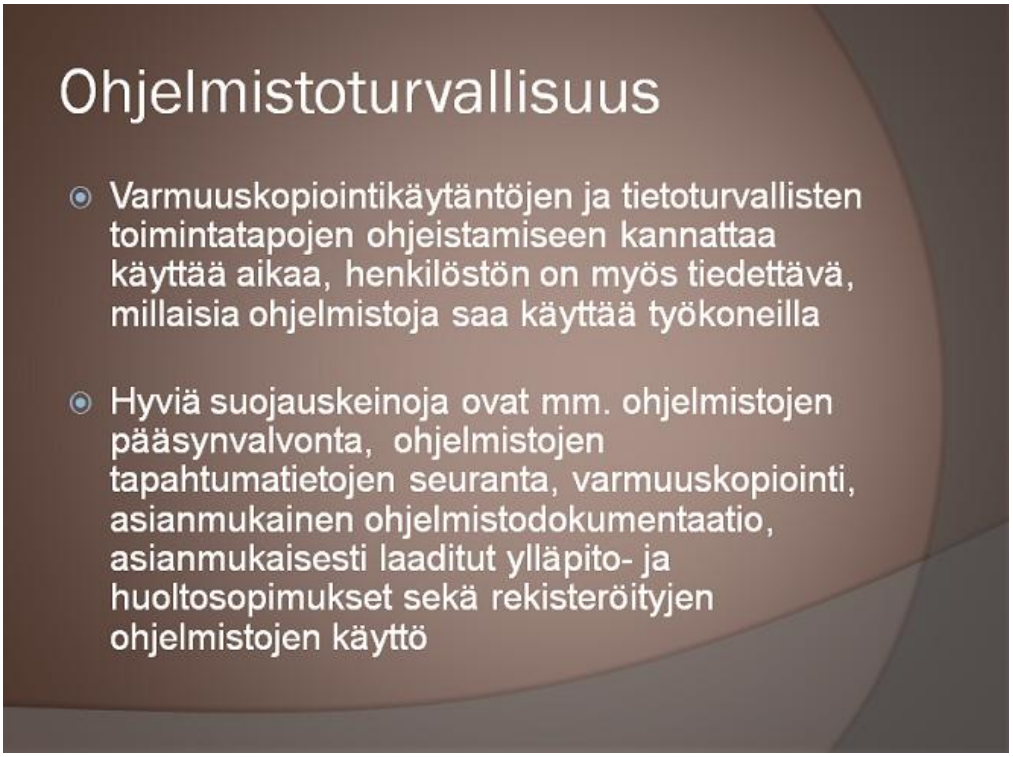
Fyysinen tietoturvallisuus

- Pyritään välttämään riskit kulunvalvonnan, vartioinnin, hälytysjärjestelmien ja lukitusten avulla
- Muistetaan tietojen varmuuskopiointi

Laitteistoturvallisuus

- Teknisten laitteiden suojaamista kutsutaan laitteistoturvallisuudeksi
- Tietoturvallisesti ajatellen tärkeitä kohteita voivat olla esimerkiksi kannettavat, palvelimet, tulostimet ja matkapuhelimet
- On suotavaa kirjata jokainen laite erilliseen asiakirjaan


Ohjelmistoturvallisuus
Tietojärjestelmissä käytettävien lisenssien ja ohjelmistojen hallintaa kutsutaan ohjelmistoturvallisuudeksi
Vaikka äkkiseltään lisenssien hallinta ei kuulostaisi kovin tärkeältä tietoturvaa ajatellen, voi sen laiminlyönnillä olla kuitenkin vakavia tietoturvaloukkauksia
On suotavaa kirjata yrityksen ohjelmistoihin liittyvät asiat tietoturvaperiaatteisiin ja - käytäntöihin


Ohjelmistoturvallisuus
Varmuuskopiointikäytäntöjen ja tietoturvallisten toimintatapojen ohjeistamiseen kannattaa käyttää aikaa, henkilöstön on myös tiedettävä, millaisia ohjelmistoja saa käyttää työkoneilla
Hyviä suojauskeinoja ovat mm. ohjelmistojen pääsynvalvonta, ohjelmistojen tapahtumatietojen seuranta, varmuuskopiointi, asianmukainen ohjelmistodokumentaatio, asianmukaisesti laaditut ylläpito- ja huoltosopimukset sekä rekisteröityjen ohjelmistojen käyttö

Virus/haittaohjelma, virustorjuntaohjelmistot / palomuuri

- Tietokonevirus on ohjelmakoodi, joka monistaa itseään ja näin ollen pystyy leviämään tietokoneesta toiseen
- Virukset leviävät tiedostojen, sähköpostien ja tietoturva-aukkojen välityksellä
- Viruksen saastuttama kone tukkii verkon heikoimpia kohtia tai lukitsee järjestelmiä salasanojen lukuisten avausyritysten takia, pahimmillaan virus voi tuhota PC:n BIOS-muistin, jolloin kone ei enää käynnisty
- Viruksia on myös tavattu matkapuhelimissa
- Viruksia torjutaan virustorjuntaohjelmilla, siksi onkin tärkeää suojata tietokone ajanmukaisilla virustorjuntaohjelmilla ja tehdä ajoittaisia virustarkastuksia

Virus/haittaohjelma, virustorjuntaohjelmistot / palomuuri

- Miten haittaohjelmia, viruksia, matoja ja krakkereita torjutaan:
  - Päivitetään käyttöjärjestelmä
  - Tietokoneella on oltava virustorjuntaohjelmisto ja palomuuri toimintaiskussa ja ajan tasalla
  - Roskapostien torjunta
- Virustorjuntaohjelmia on saatavina ilmaisversioina tai maksullisina
- Palomuurin tehtävänä on suojella tietokonetta rajoittamalla ja estämällä ei-toivottua tietoliikennettä verkosta tietokoneelle ja tietokoneelta verkkoon
- Myös erilaisia palomuuriohjelmistoja on saatavilla, mutta yleensä Windows –käyttöjärjestelmissä on oma palomuurinsa, ja rinnalle riittää hyvä ja toimiva virustorjuntaohjelma

Virus/haittaohjelma, virustorjuntaohjelmistot / palomuuri

- Millaisia virustorjuntaohjelmia on saatavilla
  - avast! Free Antivirus (suomenkielinen täysmittainen antiviruspaketti erityisesti koti- ja ei-kaupalliseen käyttöön)
  - AVG Free Edition (tunnettu helppokäyttöinen ja kevyt virustorjuntaohjelmisto)
  - HijackThis (tehokas, mutta asiantuntemusta vaativa haittaohjelmien etsimis- ja poisto-ohjelma)
  - Avira AntiVir Personal Free antivirus (helppokäyttöinen, kevyt ja kattava virustorjuntaohjelma)
  - F-Secure virustorjuntaohjelma (kotimainen, suosittu, joskin maksullinen virustorjuntaohjelma koti – ja yrityskäyttöön, tarjolla on eri versioita)

Virus/haittaohjelma, virustorjuntaohjelmistot / palomuuri

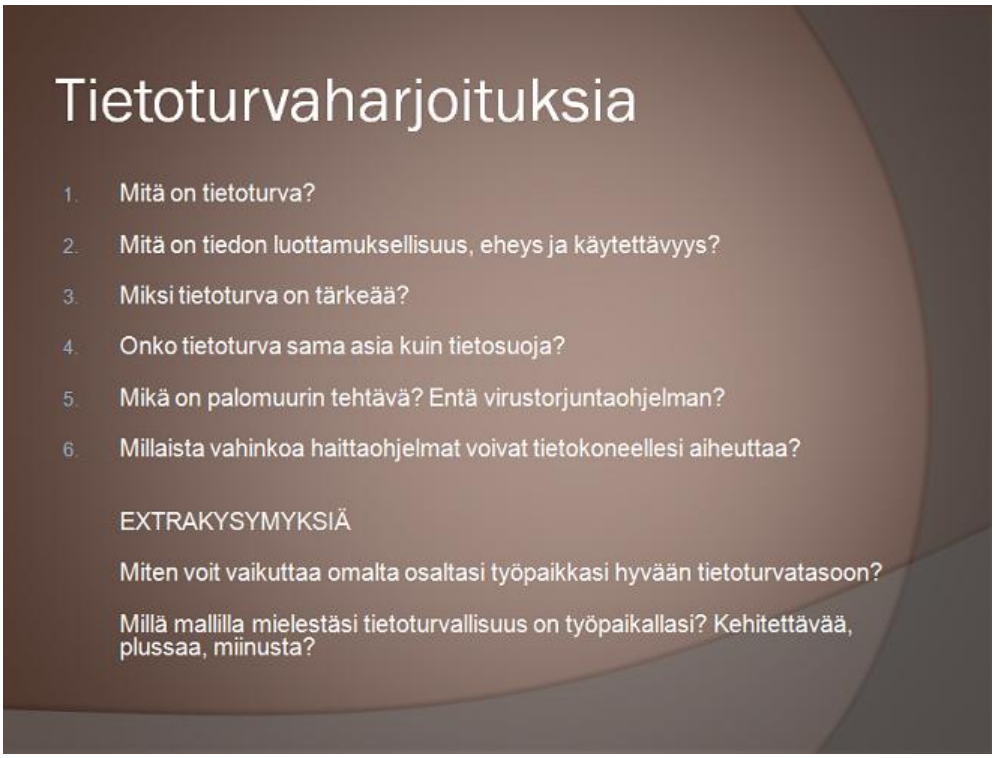
- Hyödyllisiä linkkejä
  - http://www.cert.fi/index.html
  - http://www.internetopas.com/yleistietoa/viruk set/
  - http://www.kuluttajavirasto.fi/fi-FI/huijaukset/haittaohjelmat-ja-tietomurrot/
  - http://www.f-secure.com/fi/web/home_fi/home
  - http://www.download.fi/tietoturva/virustorjunt a/index2.cfm

Tietoturvaan liittyvät lainsäädökset

- Perustuslaki 2 luvun 10 § ja 12 §
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki sähköisestä asioinnista viranomaistoiminnassa (12/2003)
- Henkilötietolaki (523/1999)
- Arkistolaki (831/1994)
- Rikoslaki (39A/1889, RL 38:3, 38:5-7, 38:8, 34:1a ja 35:1 sekä 28:7)
- Valmiuslaki (1080/1991, muutos 198/2000)
- Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)
- Valtion virkamieslaki (750/1994)
- Laki kunnallisesta viranhaltijasta 11.4.2003/304
- Työsopimuslaki (26.1.2001/55)
- Asetus yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (723/1999)
- Laki huoltovarmuuden turvaamisesta (1390/1992)
- Laki sähköisistä allekirjoituksista (14/2003)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)

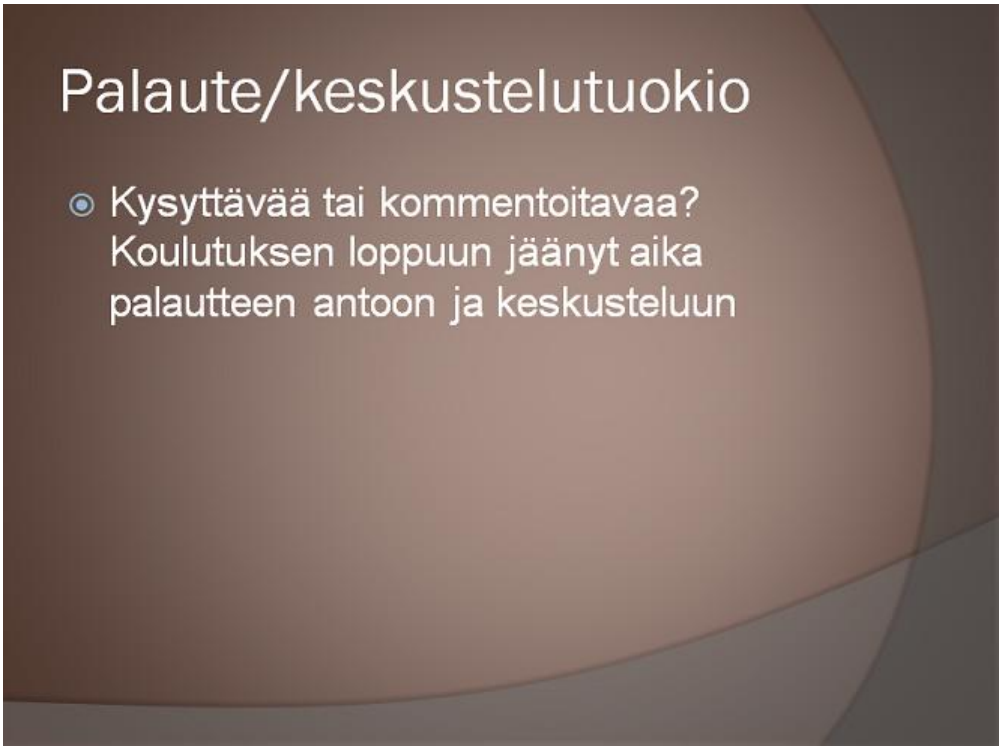
Tietoturvaan liittyvät lainsäädökset

- Henkilökorttilaki (829/1999)
- Laki turvallisuusselvityksistä (177/2002)
- Vahingonkorvauslaki (31.5.1974/41)
- Laki yksityisyyden suojasta työelämässä 8.6.2001/477
- Laki puolustustaloudellisesta suunnittelukunnasta (238/1960, muutokset 1241/1987 ja 623/1999)
- Väestötietolaki (507/1993, muutokset 202/1994 ja 527/1999)
- Asetus puolustustaloudellisesta suunnittelukunnasta (239/1960, muutokset 42/1981, 1391/1992 ja 444/1997)
- Viestintämarkkinalaki (369/1997)
- Laki sähköisestä viestinnän ja automaattisen tietojenkäsittelyn käyttämisestä yleisissä tuomioistuimissa (594/1993)
- Asetus valtion talousarviosta (1243/1992)
- Valtioneuvoston ohjesääntö (262/2003)
- Henkilörekisteriasetus (476/1987; 479/1988; 59/1993; 431/1994)
- Työelämän tietosuojalaki (516/2004; 759/2004)


Tietoturvaharjoituksia
1. Mitä on tietoturva?
2. Mitä on tiedon luottamuksellisuus, eheys ja käytettävyys?
3. Miksi tietoturva on tärkeää?
4. Onko tietoturva sama asia kuin tietosuoja?
5. Mikä on palomuurin tehtävä? Entä virustorjuntaohjelman?
6. Millaista vahinkoa haittaohjelmat voivat tietokoneellesi aiheuttaa?
EXTRAKYSYMYKSIÄ
Miten voit vaikuttaa omalta osaltasi työpaikkasi hyvään tietoturvatasoon?
Millä mallilla mielestäsi tietoturvallisuus on työpaikallasi? Kehitettävää, plussaa, miinusta?


Tehtävien läpikäynti
Tehtävienratkaisut.docx -liite


Tietoturvaohjeiden läpikäynti
Tietoturvaohje.docx -liite
ABC.docx -liite


Palaute/keskustelutuokio
Kysyttävää tai kommentoitavaa? Koulutuksen loppuun jäänyt aika palautteen antoon ja keskusteluun


Tietoturvakoulutus päättyy
Kiitos koulutettaville!