Tampereen ammatillinen
opettajakorkeakoulu

Opettajankoulutuksen kehittämishanke

Työpaikan tietoturvakoulutuksen suunnittelu, järjestäminen ja koulutusmateriaalin luonti

Pekka Poutanen

2009

Pekka Poutanen

Työpaikan tietoturvakoulutuksen suunnittelu, järjestäminen ja koulutusmateriaalin luonti
35 sivua + 4 liitesivua
Opettajankoulutuksen kehittämishanke
Tampereen ammatillinen opettajakorkeakoulu

Ryhmän opettaja Kaarina Ranne
Maaliskuu 2009
Asiasanat Oppiminen, koulutus, koulutussuunnitelma, tietoturva

Tiivistelmä

Kehittämishankkeeni aiheena on työpaikan tietoturvakoulutuksen suunnittelu, järjestäminen ja koulutusmateriaalin luonti. Kehittämishankkeen tavoitteena on suunnitella ja toteuttaa sopiva tietoturvakoulutuskokonaisuus organisaation tarpeisiin ja tarjota työntekijöille lisäksi myös itseopiskelumahdollisuus ja luoda omaa tietoturvakulttuuria.

Sisällysluettelo

Johdanto

Aloitin työskentelyn puolustusvoimissa jo vuonna 1995 ja olen siitä lähtien työskennellyt samalla alalla yhtä poikkeusta lukuun ottamatta. Vuonna 2005 toimin noin vuoden kouluttaja paikallisessa aikuiskoulutuskeskuksessa. Tuolloin sain kipinän opetukseen ja nykyisessäkin työssäni haluan kehittyä ja kouluttaa työntekijöitämme.

Kehittämishanke jakaantuu kahteen osaan eli tietoturvaopetuksen suunnitteluun ja koulutusmateriaalin luontiin. Aluksi käydään läpi opetukseen, koulutukseen ja ohjaukseen liittyviä asioita. Kehittämishankkeeni loppuosassa on tietoturvallisuus koulutusmateriaalin opetusrunko. Kehittämishankkeessa käsitellään organisaation sisäistä tietoturvakoulutusta ja hankkeessa käytetään myös apuna jo puolustusvoimien olemassa olevia ohjeita ja määräyksiä.

Kehittämishankkeessa pohditaan myös asiaa opetuksellisista lähtökohdista. Tarkoitukseni on toteuttaa koulutuksesta mahdollisimman interaktiivinen jolloin kuulija pääsee mahdollisimman paljon osallistumaan opetukseen ja myös oppia omaa tiedonhankintaa.

1 TIETOTURVA

Nykypäivänä tietotekniikan merkitys työelämässä lisääntyy jatkuvasti ja ihminen ei elää enää ilman tietotekniikkaa.

Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien ja palveluiden asianmukaista turvaamista sekä normaali- että poikkeusoloissa lainsäädännön ja muiden toimenpiteiden avulla. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä suojataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai tahallisten, tuottamuksellisten ja tapaturmaisten inhimillisten tekojen aiheuttamilta uhilta ja vahingoilta.

Tietoturvan merkitystä nyt ja erityisesti tulevaisuudessa ei kukaan voi kiistää. Tietoturvan asettamat säännöt ja rajoitukset tulee työntekijöiden huomioida kaikissa toiminnoissaan. Tietoturva on varmaankin yksi nopeimmin kehittyvistä aloista maailmassa geeniteknologian jälkeen. Tietoturva on verraten nuori ala, jossa kulttuuri on

vasta kehitysvaiheessa. Ratkaisut, jotka nyt teemme, heijastuvat pitkälle tulevaisuuteen ja mallit, jotka nyt luomme, ovat pohjana tulevaisuuden ratkaisuille.

Tietoturvallisuus on osa yrityksen kokonaisturvallisuutta ja siksi onkin tärkeää että työntekijät ymmärtävät tietoturvallisuuden merkityksen. On myös tärkeää muokata ihmisten asenteita niin että kaikki työntekijät ymmärtävät tietoturvallisuuden merkityksen koko yrityksen toiminnassa.

Tietoturvallisuutta vaarantavat erilaiset uhkatekijät. Uhasta muodostuu organisaatiolle riski, jos sen todennäköisyys on suurempi kuin nolla (uhan toteutuminen on mahdollinen), ja jos siitä aiheutuu toteutuessaan huomattavaa välitöntä tai välillistä vahinkoa (vahinkokustannus on merkittävä).

Tietoturvavahingoissa on toistuvasti ollut kyse siitä, ettei uhkaa ole käytännön työtilanteessa tiedostettu, oikeita menettelyjä ei ole tiedetty tai ohjeita ei ole noudatettu. Ihminen on tärkein tekijä, tekniset ratkaisut eivät sitä muuta. Jokainen on omalta osaltaan vastuussa tieto- turvallisuudesta ja jokainen vaikuttaa sen toteutumiseen. Turvallisuustietoisuuden lisäämiselle on selvä tarve ja tässä henkilöstön koulutus on avainasemassa.

Tietoturvassa ei ole kyse vain tekniikasta, vaan ihmisten työskentelytavoista. Kaikkien tulee tietää, kuinka tietoturvasta voidaan huolehtia. On myös tietoja, joiden turvaamiseen yrityksellä on lainsäädännön velvoite.

Tietoturvallisuuden uhkina pidetään esimerkiksi erilaisia huijausyrityksiä, henkilökohtaisen yksityisyyden loukkauksia, roskapostia, teollisuusvakoilua, piratismia, tietokoneviruksia, verkkoterrorismia ja elektronista sodankäyntiä.

1.1 Tietoturvan merkitys

Julkishallinnon toiminta on erittäin riippuvaista tiedoista ja tietotekniikasta. Tietoyhteis- kuntakehitys, kansainvälistyminen, verkottuminen sekä toimintojen ja palveluiden siirtyminen tietoverkkoihin lisäävät niiden merkitystä edelleen. Tietoturvallisuuden avulla varmistetaan tärkeiden tietojen hallinta ja toiminnan jatkuvuus.

Tietoturvallisuus on myös tärkeää, koska julkishallinnossa käsitellään paljon tärkeää tietoa, kuten esimerkiksi henkilötietoja, taloustietoja ja eri organisaatioiden asiakirjoja. Osa tiedoista on salassa pidettävää, arkaluonteista tai muuta luottamuksellista tietoa. Salassa pidettävällä tiedolla tarkoitetaan lailla salassa pidettäväksi säädettyjä asiakirjoja tai tietoja. Eräät viranomaisten salassa pidettävistä asiakirjoista on määritelty turvaluokittelun piiriin. Ne kuuluvat mm. julkisuus-, tietosuoja-, henkilötieto- tai yrityssalaisuuslainsäädännön piiriin, jonka vuoksi on tärkeää, että tiedot eivät päädy tahallisesti tai tahattomastikaan asiattomien haltuun. Lisäksi julkishallinnossa on paljon tietoa, joka ei ole salassa pidettävää, vaan luonteeltaan julkista, mutta tällaisenkin tiedon oikeellisuudesta, muuttumattomuudesta ja saatavuudesta on huolehdittava. (http://www.yliopistojentt.fi/VAHTI-CD/Sivusto/kayttajan_ohje/012_merkitys.htm luettu 28.3.09)

1.2 Tietoturvan määritelmä

Tietoturvallisuudella tarkoitetaan 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, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.

Tietoturvallisuuden keskeisillä käsitteillä tarkoitetaan seuraavaa:
Käytettävyys: järjestelmien tiedot ja palvelut ovat niihin oikeutettujen käytettävissä etukäteen määritellyssä vasteajassa. Tiedot eivät ole tuhoutuneet tai tuhottavissa vikojen, tapahtumien tai muun toiminnan seurauksena.
Eheys: tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia, eivätkä ne ole hallitsemattomasti muuttuneet tai muutettavissa laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai inhimillisen toiminnan seurauksena.
Luottamuksellisuus: tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen-käytettävissä. Sivullisille ei anneta mahdollisuutta muuttaa tai tuhota tietoja eikä muutoin käsitellä tietoja.
Muita yleisiä tietoturvallisuuteen kuuluvia vaatimuksia ovat osapuolten todentaminen ja tapahtuman kiistämättömyys, jotka ovat erityisen tärkeitä silloin, kun järjestelmän

käyttäjät tulee pystyä tunnistamaan esimerkiksi käytettäessä vuorovaikutteisia sähköisiä asiointipalveluita tai etätyötä tehtäessä.
Todentaminen (autentikointi) tarkoittaa osapuolten (henkilö tai järjestelmä) luotettavaa tunnistamista.
Kiistämättömyys tarkoittaa tapahtuneen todistamista jälkeenpäin, jolloin tavoitteena on juridinen sitovuus. Kiistämättömyys varmistaa sen, ettei toinen osapuoli voi kieltää toimintaansa jälkeenpäin. (http://www.yliopistojentt.fi/VAHTI-CD/Sivusto/kayttajan_ohje/011_johdanto1.htm. luettu 23.3.09)

Valtionhallinnossa on luotu VAHTI-tietoturvaohjeet, joita hyödynnetään valtionhallinnon lisäksi kunnallishallinnossa, elinkeinoelämässä ja kansainvälisessä tietoturvayhteistyössä. VAHTI:n mukaan tietoturvariskin suuruusluokka määräytyy sen mukaan, miten vakava riski on ja kuinka todennäköisenä sen toteutumista pidetään. Tämän luokituksen mukaan esimerkiksi suljetun lähdekoodin ohjelmat aiheuttavat ohjelmavirheineen sietämättömän riskin. Network Associatesin teettämän selvityksen mukaan yritykset menettävät ohjelmavirheiden mahdollistamien virusten takia yhteensä noin 22 miljardia euroa vuosittain. Valtionhallinnon ohjeet edellyttäisivät tällöin seuraavaa: 1) näin riskialtista toimintaa ei pitäisi aloittaa, 2) riski on poistettava ja toimenpiteet aloitettava välittömästi, ja 3) riskialtis toiminta pitää keskeyttää, kunnes riski on poistettu.

Tietoturvallisuuden kehittämistoimet on jaettu VAHTI:ssa seuraavaan kahdeksaan osa-alueeseen.

Neljä ulointa kerrosta ovat:

- Hallinnollinen tietoturva
- Henkilöstöturvallisuus
- Fyysinen turvallisuus
- Tietoliikenneturvallisuus

Näiden neljän kerroksen suojaamana ovat sisimpänä:

- Ohjelmistoturvallisuus
- Tietoaineistoturvallisuus
- Käyttöturvallisuus
- Laitteistoturvallisuus

Suomen valtionhallinto on määritellyt tietoturvan tärkeäksi keinoksi, jonka avulla kansalaiset ja yritykset saadaan luottamaan tietoyhteiskuntaan.
Tarkemmin osa-alueista kerrotaan luvussa 7.

2 TIETOTURVAKOULUTUS

2.1 Tietoturvakoulutuksen nykytila ja kehittämishankkeen tavoite

Lähes kuukausittain kuulemme uutisista että jokin uusi virus leviää internetissä ja tämä tilanne tekee meidät peruskäyttäjät hyvin levottomiksi.
Kuitenkin meidän kaikkien täytyy muistaa että tietoturvakoulutus sisältää muutakin kuin ” internetin käytön ohjeistusta tai virustorjuntaa.

Tietoturvakoulutuksen ja tietoturvaosaamisen nykytilaan vaikuttavat:

- organisaation johdon asenne tietoturvallisuuteen
- organisaation tietoturvakulttuuri ja asenne
- järjestetyt tietoturvakoulutukset
- tietoturvallisuutta koskeva säännöllinen tiedottaminen
- käytössä oleva tietoturvakoulutusmateriaali
- käytettävissä olevat resurssit koulutuksen ja tietoturvahenkilöstön osalta
- osallistuminen tietoturvallisuutta kehittäneisiin hankkeisiin.

(http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Tietot/vahti6_taitto_NETTI_%2B_KANNET.pdf luettu 20.3.2009)

Tällä hetkellä työpaikassani ei ole järjestetty tietoturvakoulutusta ainakaan neljään vuoteen. Työntekijöillä on epävarmuutta ja tietämättömyyttä siitä mikä on oikea toimintatapamalli. Puolustusvoimien hallinnollisesta tietojärjestelmästä on myös luotu yhteys ulkomaailmaan eli internettiin.
Koulutuksen tavoitteena että jokainen työntekijä osallistuu tietoturvakoulutuksen mahdollisimman pian työn vastaanotettuaan. Koulutuksesta saa työntekijä todistuksen jolla hänelle anotaan tietojärjestelmien käyttöoikeuksia. Lisäksi on tarkoitus tehdä

koulutusmateriaali ja lisätä siihen puolustusvoimien omien järjestelmien tietoturvallisuus.

Tietojärjestelmät ovat muuttuneet varsin radikaalisti puolustusvoimilla 2000-luvulla ja lisäksi osa palveluista on myös ulkoistettu. Tällä hetkellä tietotekniikka henkilöstökin on ulkoistettu ja joukko-osastoissa on vain paikalla enää tietohallintopäälliköt. Atk-tukihenkilöt ja muuta tietotekniikka osaajat ovat omissa yksiköissään kaukana asiakkaista. Siksi usein työpaikallani tuleekin tietokoneen käyttäjiltä päivittäin kyselyjä onko joku asia sallittua vai ei.

2.2 Miksi tietoturvallisuus on niin tärkeää jokaisen kohdalla?

Puolustusvoimien toiminta on erittäin riippuvaista tiedoista ja tietotekniikasta. Tietoyhteiskuntakehitys, kansainvälistyminen, verkottuminen sekä toimintojen ja palveluiden siirtyminen tietoverkkoihin lisäävät niiden merkitystä edelleen. Tietoturvallisuuden avulla varmistetaan tärkeiden tietojen hallinta ja toiminnan jatkuvuus.

Tietoturvallisuus on myös tärkeää, koska puolustusvoimissa käsitellään paljon mm.

- maanpuolustuksen kannalta tärkeää ja salassa pidettävää tietoa,
- arkaluonteista henkilötietoja,
- taloustietoja ja
- eri organisaatioiden luottamuksellista tietoa.

Salassa pidettävällä tiedolla tarkoitetaan lailla salassa pidettäväksi säädettyjä asiakirjoja tai tietoja. Salassa pidosta säädetään mm. julkisuus- ja henkilötietolaissa sekä muissa erityislaeissa.

Näistä tärkeimpiä ovat rikoslaki (34:1,2 ja 38), henkilötietolaki, arkistolaki ja perustuslaki (2 luku 10 § ja 12 §). Puolustusvoimien ja joukko-osastojen sisäiset määräykset perustuvat lisäksi lailla voimaan saatettuihin kansainvälisiin sopimuksiin ja puolustusvoimien erityisasemaan kriisin ajan keskeisimpänä turvallisuusorganisaationa.

Salassa pidettävät asiakirjat on määritelty turvaluokittelun piiriin. Tämän vuoksi on

tärkeää, että tiedot eivät päädy tahallisesti tai tahattomastikaan asiattomien haltuun. Lisäksi julkishallinnossa on paljon tietoa, joka ei ole salassa pidettävää, vaan luonteeltaan julkista, mutta tällaisenkin tiedon oikeellisuudesta, muuttumattomuudesta ja saatavuudesta sekä lain mukaisesta käsittelystä on huolehdittava.

Tietoturvallisuuden päämääränä on mahdollistaa osaltaan puolustusvoimien toimintakyky kaikissa olosuhteissa turvaamalla sen toiminnalle merkittävän tiedon käytettävyys, eheys ja luottamuksellisuus hyvää tiedonhallintatapaa noudattaen. Tietojärjestelmät ja tietojen käsittelymenetelmät on rakennettava siten, että nämä vaatimukset täyttyvät puolustusvoimien sekä sidosryhmien osalta. Koko puolustusvoimien henkilöstön edellytetään noudattavan korkeaa tietoturvallisuuskulttuuria.

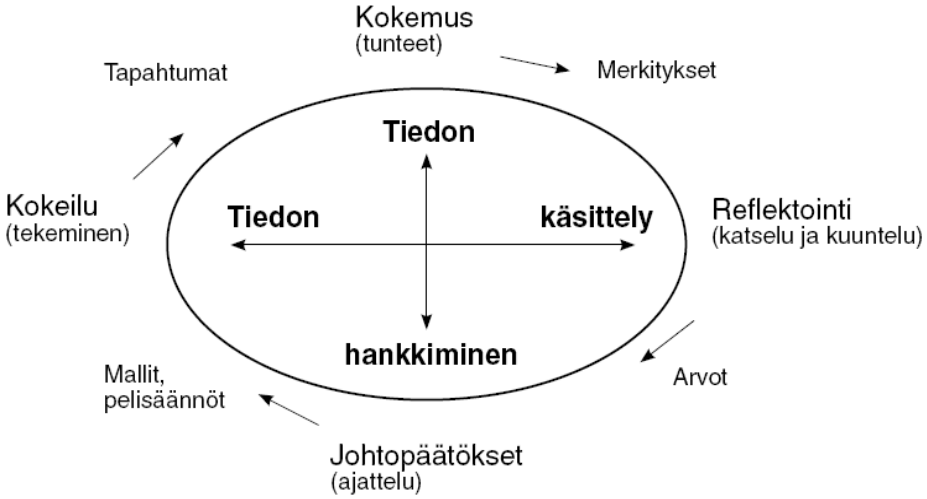
3 KOULUTUS JA OPPIMINEN

Tietoturvakoulutukseen pätevät yleiset koulutuksen lähtökohdat, joihin kouluttajan kannattaa tutustua. Julkishallinnon organisaatioissa sisäinen tietoturvakouluttaja on usein asiantuntija tietoturvallisuudessa, mutta ei kouluttamisessa.

3.1 Hyvä oppiminen

Nykytutkimuksen mukaisen oppimiskäsityksen perusajatus on, että ihminen oppii uutta liittämällä sen olemassa oleviin tietoihin ja taitoihin.
Aikuisen oppiminen on kokemuksellista, sellainen tieto tai taito, jolla on kokemuksemme mukaan merkitystä, opitaan.

Kuviossa 1 on David Kolbin (1984) kokemuksellisen oppimisen kehän pohjalta muokattu malli siitä, miten aikuinen ihminen kuljettaa mielessään ja käytännössään uutta asiaa. Kokemuksellisen oppimisen malli havainnollistaa hyvin sen, että oppiminen on muutakin kuin ajattelua. Uuden asian omaksumiseen sitoutuu paljon tunteita ja kokemuksia. Mitä enemmän on kyse asenteiden uudelleen oppimisesta, sitä enemmän kosketaan myös tunteiden ja arvojen maailmaan.
Tietoturva-asioiden omaksuminen on suuressa määrin paitsi tiedollista oppimista myös oikein toimintatapojen ja asenteiden oppimista.



KUVIO 1. Kolbin kehää mukaillen

Oppiminen mahdollistaa selviytymisen uusista ja oudoista tilanteista. Virheistään (ja myös muiden tekemistä virheistä) voi ottaa opiksi, jolloin kerran ratkaistuihin ongelmiin ei tarvitse palata uudelleen ja uudelleen. Oppiminen heijastuu muutoksena yksilön toiminnassa. Oppiminen voidaan määritellä prosessiksi, jossa tietyn kokemuksen merkitys tulkitaan uudelleen tai sen tulkintaa tarkistetaan siten, että syntynyt uusi tulkinta ohjaa myöhempää ymmärtämistä, arvottamista ja toimintaa (Mezirow 1996). Uutta oppiessaan ihminen aina valikoi informaatiota ja tekee siitä omat tulkintansa käsitystensä, odotustensa ja tavoitteittensa pohjalta. Uutta informaatiota pyritään omaksumaan jo olemassa olevan tiedon perusteella. Tieto ei siirry oppijaan, vaan oppija tulkitsee sen itse. (von Wright 1996.)

3.2 Osaamisen tasot ja oppimisen muodot

On todettu että ihminen säilyttää oppimiskykynsä työuransa läpi. Kuitenkin täytyy muistaa että aiemmin opittu on uuden oppimisen perusta.
On kuitenkin tärkeää ja ei ole tarkoituksenmukaista pyrkiä opettamaan kaikkia asioita kaikille vaan että työntekijä havaitsee työn kannalta merkityksellisiä asioita.

Erilaisia osaamisen tasoja voivat olla esimerkiksi (Peltonen 1985):
1. *Tunnistaminen*: pystyy valitsemaan vaihtoehdoista
2. *Palauttaminen*: pystyy vastaamaan avoimeen kysymykseen

3. *Rutiini*: pystyy nopeaan, tarkkaan ja varmaan palauttamiseen myös häirityssä tilanteessa
4. *Automaatio*: pystyy rutiinisuoritukseen ponnisteluitta ja tarvittaessa myös muun toiminnan yhteydessä

Aikaisemman tiedon aktivoimiseksi pitäisi pyrkiä herättää oppijat ajattelemaan, mitä he tietävät asiasta ennestään, mitkä he eivät ymmärrä ja miten asia liittyy muuhun tietoon. Tavoitteena on tiedollisen ristiriidan synnyttäminen.

Monimutkaisten sisältöjen hallitsemiseksi tulisi harjoitella autenttisia tilanteita ja ongelmia, ilmiön monimutkaisuus ja haasteellisuus tulisi tuoda esiin, sekä yhteydet muuhun tietoon. Monipuolisella lähestymistavalla saadaan elävyyttä opiskeluun; käytetään erilaisia medioita, yhdistetään teoriaa ja käytäntöä, tiedon eri rakenteita ja tarkastelutasoja, sekä käytetään runsaasti esimerkkejä. Yhdessäoppiminen on yksi oppimisen muodoista. Opetuksessa tulisi käyttää yhteisöllisiä työkaluja, yhdessä suoritettavia tehtäviä, sekä tallentaa ja jakaa tuotettua tietoa. Ajattelun visualisointi helpottaa myös oppimista. Erilaisia visualisoimisen tapoja opetuksessa ovat oppijan työskentelyprosessin tallentaminen ja esittäminen, sekä töiden julkistaminen ja kommentointi. Analoginen päättely auttaa oppimista. Tätä voidaan harjoittaa useiden tilanteiden ja esimerkkien tarkastelun avulla, tietoisella vertailulla, yhtäläisyyksien ja erojen etsimisellä ja selittämisellä. Taitojen harjaannuttamisessa tulisi keskittyä perustaitoon. Nopea palaute pitäisi saada suoritukseen perustuen. Oppimista nopeuttaa myös selkeä oppimisprosessin tavoitteiden määrittely, jolloin huomio kiinnitetään suoritustapaan, omien tietojen arviointiin, työskentelyn suunnitteluun, sekä oman toiminnan tarkasteluun ja arviointiin. (http://www.kookas.fi/articles/read/6697 luettu 20.3.2009)

Kouluttajan siis kannattaa tarkastella oppimisen muotoja ja miettiä mihin haluaa vaikuttaa tietoihin, taitoihin vai asenteisiin.

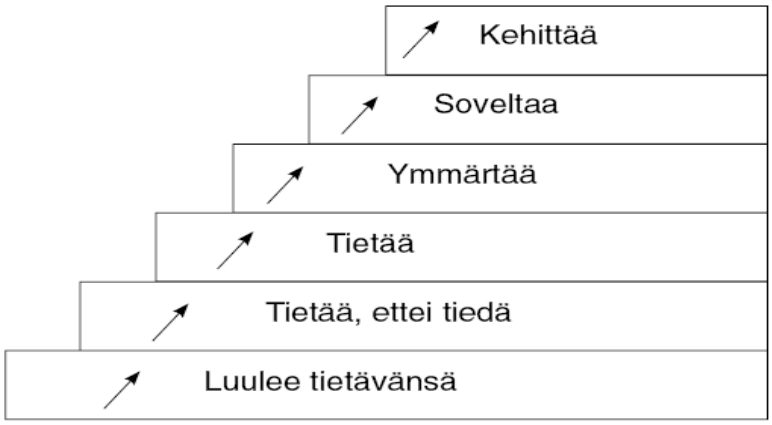
3.3 Oppiminen ja vuorovaikutus

Yksilön oppimisen määritelmänä voidaan käyttää esimerkiksi seuraavaa Sydänmaanlakan esittämää määritelmää (2001): Oppiminen on prosessi jossa yksilö

hankkii uusia tietoja, taitoja ja asenteita, kokemuksia ja kontakteja jotka johtavat muutoksiin hänen toiminnassaan.

Tietoja oppii aistien kautta erilaisissa tilanteissa, lukemalla ja luentoja kuuntelemalla.
Taitoja oppii taas harjoittelun avulla ja tekemällä itse.
Asenteita oppii parhaiten kokemusten avulla, keskustelemalla ryhmätöillä.

Laajemmin käsiteltynä todellinen oppiminen on pitkävaiheittainen prosessi.



Kuvio 2. Oppimisen portaat (Sydänmaanlakka 2000)

Oppia voi, kun tiedostaa, ettei tiedä. Kuviossa 2 on kuvattu oppimisen portaat. Mitä vähemmän tiedät, sen enemmän luulet tietäväsi. Todellinen oppiminen voi alkaa kun ymmärtää ettei tiedäkään. Tällöin voi herätä motivaatio saada tietää enemmän tai alkaa tutkia, miten uusi tieto poikkeaa siitä, jonka on luullut tietävänsä.

Valtaosa ihmisen oppimisesta tapahtuu sosiaalisessa vuorovaikutuksessa muiden kanssa (Rauste von Wright & von Wright, 1995).

Piaget'n mukaan yksilö kokee sosiaalisessa vuorovaikutuksessa ristiriidan oman käsityksensä ja muiden esittämien ajatusten välillä. Tämä pakottaa hänet tarkentamaan omia tiedollisia rakenteitaan ja jäsentämään niitä uudelleen.(*von Wright 1994*) Vuorovaikutuksessa yksilön ajatteluprosessit tulevat "näkyviin" niin hänelle itselleen kuin muillekin; näin hän voi reflektoida niitä sekä itsekseen että vastavuoroisesti muiden kanssa. Kun ryhmän jäsenet perustelevat käsityksiään ja ratkaisujaan

toisilleen, luodaan edellytykset sekä muilta oppimiselle että myös omien ajatusprosessien itsestään selvien asioiden kyseenalaistamiselle. (*Rauste-von Wright & von Wright 1995* .)

Opettamisessa etusijalla ei ole aihe - vaan oppija! Oppijan pitää tuntea sekä, ongelma, että ratkaisu omikseen. Työnläheinen peruskysymys on: Mitä käytännön pulmia työtilanteessa esiintyy?

Jokaisen kouluttajan tulee hallita motivointi-, kommunikointi- ym. perustaidot. Ne eivät kuitenkaan yksin takaa hyviä oppimistuloksia, koska oppijan omat lähtökohdat ja tarpeet luonnollisesti vaikuttavat myös. Jokaiseen oppilaaseen eivät kaikki keinot vaikuta yhtä tehokkaasti ja samalla tavalla. (Uusikylä ym. 2000.)

Aikuisten oppimista määrittävät vahvasti työelämä ja sen asettamat vaatimukset. Yleisiin työelämävalmiuksiin kuuluvat mm. oppimisen taito, ongelmanratkaisutaito, vuorovaikutustaito, kuuntelutaito, suullinen ja kirjallinen viestintätaito, koordinointikyky, päätöksentekotaito, suunnittelu- ja organisointitaito, johtamistaito, hahmottamiskyky ja innovatiivisuus (Pohjonen 2005).

Yksi aikuisten ihmisten oppimisen este on muistaminen sillä iän myötä lyhytkestoisen muistin kapasiteetti heikkenee mutta täytyy muistaa että aikuisella ihmisellä on ns. loogista järkeilyä ja kokemusvarastoa.

3.4 Hyvä Kouluttaja

Hyvä kouluttaja tuntee oppimisen lainalaisuudet. Hän pystyy valitsemaan monista kouluttamisen keinoista sellaiset, jotka parhaiten lisäävät organisaation toiminnassa syntyvää ja kehittyvää asiantuntijuutta.

Kun kouluttajana haluat rakentaa vuorovaikutusta ryhmässä, roolisi muuttuu tiedon jakajasta organisaattoriksi. Tällöin tärkein tehtäväsi on saada oppijat kommunikoimaan keskenään.

Tietoturvallisuus on asiantuntijuusalue, jossa vaaditaan jatkuvaa osaamisen ja ammattitaidon kehittämistä. Asiantuntijan odotetaan osaavan aikaisemmin

harvinaisina pidettyjä tietoja ja taitoja. Asiantuntija tänään ei ole enää asiantuntija huomenna, jos yksityiskohtaisestikin hallittu tieto vanhenee ja muuttuu tarpeettomaksi.

Hyvän kouluttajan tunnusmerkistöön kuuluvat sisällöllisen osaamisen ohella (Rogers 2004):

- Organisointikyky
- Sosiaaliset taidot
- Innostuneisuus
- Läsnä olevuus
- Aktivoiva opetustyyli
- Taito havaita ja ratkaista oppijoiden ongelmia
- Rohkeus puolustaa asiaansa
- Taito esittää monimutkaiset asiat selvästi

4 KOULUTUSSUUNNITELMA

Koulutussuunnittelun tarkoituksena on laatia lyhyen ja pitkän aikavälin koulutussuunnitelmat. Niihin otetaan mukaan niin yleiset kuin kohdennetutkin koulutukset. Suunnitelmat pohjautuvat organisaation strategioihin ja koulutus-tarpeiden selvittämiseen. Laaditun suunnitelman on tarkoitus ohjata koulutus-toimintaa. Lähestymistapoja koulutussuunnitteluun on useita.
Eräs perusidea on ensin määritellä toiminnan tavoitteet ja hakea sitten vaihtoehtoisista tavoista ne, joilla tavoitteisiin päästään parhaiten (esim. määrä, nopeus, taloudellisuus). (Leino ym. 1995.)

4.1 Sisällön suunnittelu

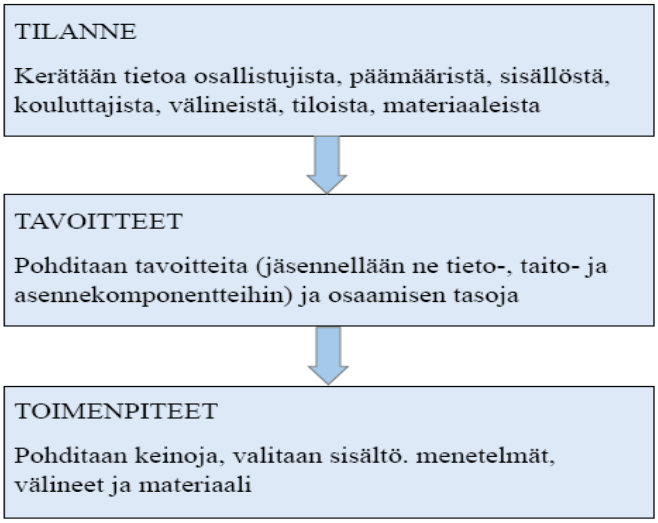
Kouluttajan peruskysymyksiä on, mitä asioita eri kohderyhmien kanssa tulisi käydä läpi. Yleistä ja yksiselitteistä vastaus ei ole. Koulutuksen sisältöä mietittäessä pitää miettiä mitä asioita kohderyhmän kanssa tulisi käydä läpi.
Kouluttajan on itse suunniteltava, käykö kerralla useampia asioita ehkä karkeammalla tasolla läpi vai paneutuuko tietyssä koulutuksessa vain johonkin tai joihinkin kysy-myksiin syvällisemmin. (Koulutuksessa käytävät asiat 4.3)

Olen kuitenkin omassa hankkeessani keskittynyt organisaation koko henkilöstön koulutuksen suunnitteluun ja koulututusta olisi tarkoitus järjestää vuosittain.

4.2 Koulutustilaisuuden suunnittelu ja toteutus

Koulutustilaisuuden suunnittelussa on otettava huomioon opetettavan asian tavoitteet ja oppisisältö, opiskelijoiden aiemmat tiedot ja taidot asiasta, käytettävissä oleva aika ja paikka sekä koulutusmenetelmät. Oppisisällöllisesti avain on tietoturvavastuiden ja -tehtävien organisoinnissa, koska jokaiselle tulee tarjota riittävät edellytykset huolehtia vastuistaan ja tehtävistään. Koulutuksen tavoitemäärittelyä ja oppimisympäristön suunnittelua voikin lähestyä esim. seuraavilla kysymyksillä:

Keitä osallistujat ovat?
Mihin he tähtäävät tällä koulutuksella?
Mitä heidän pitää oppia?
Mitä he tietävät aiheesta entuudestaan?
(Peltonen 1985, Rogers 2004, Puhakainen 2006.)



KUVIO 3. Opetuksen suunnitteluprosessi (Peltonen 1985)

Toteutussuunnitelmassa on tarkoitus järjestää aluksi 4-5 henkilölle ns. pilottikoulutus ja tehdä siitä arvioita koulutuksen soveltuvuudesta ja tehdä myös heille erillinen kysely. Lopuksi on tarkoitus toteuttaa noin 4 tunnin tietoturvakoulutus kaikille työntekijöille.

Usein opetettavan ryhmän koolla on suuri merkitys ja kuinka aktiivisia ryhmän jäsenet ovat ja he osallistuvat keskusteluun. Organisaatiossamme koulutukseen osallistujat ovat lähes poikkeuksetta aikuisia.

Kouluttajan kannattaa joka tapauksessa käyttää vaihtelevia opetusmenetelmiä, esim. luento, vuoropuheinen opetus, demonstraatio, ryhmätyö, case-menetelmä, harjoitus, itseopiskelu. Osallistava ja neuvotteleva malli voi hyvin toimia myös tietoturvakoulutuksessa. Samoin on pohdittava vaihtelevia materiaaleja ja opetusvälineitä. Niiden valinta on keskeisiä suunnittelun kohteita. (Uusikylä ym. 2000.) Kouluttajalla on menetelmien vapaus koulutussuunnitelman rajoissa.

4.3 Tietoturvakoulutuksessa käsiteltävät asiat

Koulutus mahdollistaa jo opittujen asioiden osaamisen säilymisen sekä uusien asioiden oppimisen. Koulutuksessa olisi hyvä käydä läpi seuraavia asioita:

- Tietoturvatoiminnan tavoitteet
- Tietoturvatoiminnan organisointi, vastuut ja tehtäväjako
- Noudatettava ohjeisto ja sen sijainti
- Peruskäsitteet
- Viranomaisen toiminnan julkisuus ja salassapitovelvoitteet
- Asianhallinnan turvallisuus
- Asiakirjojen luokittelu ja käsittely
- Henkilötietojen käsittely
- Tietokoneen käyttö
- Internetin ja sähköpostin käyttö
- Toimitilaturvallisuuden perusteet
- Vierailijakäytäntö
- Etätyö ja etäkäyttö
- Matkatyö ja mobiililaitteiden käyttö
- Aloitetoiminta
- Toiminta ongelmatilanteissa ja ilmoitusvelvollisuus
- Seuraamukset

- tietoturvallisuuden yhteyshenkilöt yrityksessä ja lisätietojen hankinta.(http://www.webtoimisto.fi/iPortfolio/Pdftiedostot/Tietoturvaohje.pdf luettu 22.3.2009)

Tietoturvakoulutusta järjestettäisiin muutaman vuoden välein tai aina uuden työntekijän perehdyttämisen yhteydessä.

5 KOULUTUSMATERIAALI JA SEN SISÄLTÖ

Kun organisaatiossa laaditaan omia koulutus- ja ohjeaineistoja, on suositeltavaa noudattaa seuraavia kriteerejä ja laadullisia ominaisuuksia:
Ohje- ja koulutusaineiston on oltava helppolukuista

- Ohje on ymmärrettävä kaikille työntekijöille organisaatiosta tai työtehtävästä riippumatta.
- Kirjoitustyylin on oltava lukijalle läheinen. Tätä tavoitellaan mm. sinuttelulla ja opastamisella
- Ohjeen on herätettävä käyttäjät ajattelemaan tietoturva-asioita omassa työssään

5.1 Esitysmateriaali

Kouluttajan esitysmateriaalipaketti on tarkoitettu organisaatioiden tietoturvakouluttajille.

Se sisältää valmiin materiaalin, jota kouluttaja voi käyttää koulutuksissa joko sellaisenaan tai vielä mieluummin muokaten sitä omia tarpeitaan ja koulutustilanteitaan vastaaviksi. Materiaali on tehty niin, että se muodostaa luentokokonaisuuden, mutta tarvittaessa materiaalista voidaan poimia käsiteltäväksi vain haluttu osa. Aineisto on tuotettu aluksi word-dokumenttina ja sen jälkeen siitä on tehty Microsoft PowerPoint -muoto jossa lisävinkkejä muistiinpano-osiosta.

5.2 Tietoturvallisuuden osa-alueet

Hallinnollinen turvallisuus on useimmiten organisaatiossa tietoturvan perusalusta. Organisaation hallinnon on määriteltävä tietoturvallisuuden pääperiaatteet ja tehtävä toimenpiteet. Pelkästään yksilötasolla tietoturvan ylläpitoon mahdollisuudet ovat rajalliset. Esimiesten vastuulla on tiedottaminen, seuraaminen ja laiminlyönneistä huomauttaminen. Tiedotus tapahtuu vain niille, joita kyseinen tietoturva-asia koskee. Hallinnollinen tietoturva koostuu siis johdon hyväksymistä periaatteista, vastuunjaosta, tarkoitukseen varatuista resursseista sekä riskien arvioinnista. Tietoturvallisuuden avainhenkilöille annetaan järeän tason turvallisuus- ja valmiuskoulutusta sekä koko henkilöstölle perustason koulutusta turvallisuuden ylläpitämiseksi sekä poikkeustilanteiden varalle. Yleensä yritysten lähiverkoissa on osallisina kahdenlaisia ihmisiä; toiset vastaavat yritysten ja organisaatioiden tietojärjestelmien ja verkkojen toiminnasta, toiset vain käyttävä niitä. Tältä pohjalta näkemyseroja tietoturvallisuudessa voi syntyä. Lähtökohtana on, että yritykseen määritellään riskianalyysi, jonka avulla olemassa olevat uhat saadaan paikallistettua, vaiheen perusteella luodaan ohjeistus ja toiminta-ohjeet. Hallinnollisessa tietoturvassa päämääränä on luoda organisaatioon toimintatapa, jolla pystytään välttämään tietoturvariskit. (http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html luettu 23.3.2009)

Useimmat vahingot syntyvät perusturvallisuuden laiminlyönnistä. Perusturvallisuuteen liittyvät asiat on suunniteltava, määriteltävä, toteutettava ja testattava. Ongelmiksi voivat muodostua mm. ylimitoitetut ja epäkäytännölliset turvaratkaisut, jotka johtavat turvatason alenemiseen – niin yllättävältä kuin se saattaa tuntuakin. Ihmiset eivät jaksa käydä läpi turvamenetelmiä, tai eivät jopa halua käyttää turvaratkaisuja, koska se on liian vaikeaa. Toipumissuunnitelmat on hyvä laatia. Niissä määritellään vahingon jälkeiset toimenpiteet ja se, kuinka tilanteesta toivutaan ja jatketaan eteenpäin.

Henkilöstöturvallisuus on usein liian vähälle huomiolle jätetty alue. Henkilöstö on organisaatiota ylläpitävä voima ja toisaalta myös riski. Yleensä henkilöstö aiheuttaa vahinkoa tietämättään. Inhimillisiin vahinkoihin auttaa usein koulutus. Tietoturvan päämäärät sekä huolimattomuuden ja vahingon seuraukset on hyvä selvittää. Henkilön persoonan ominaisuudet vaikuttavat myös reagointiin yllättävissä tilanteissa.

Tahallisia vahingontekoja myös esiintyy, ne liittyvät usein erottamiseen. Pitkään palveluksessa ollut henkilö vie väkisinkin tietoa mukanaan. Kulkuluvat, salasanat ja muut tulisi mitätöidä mahdollisimman pian erottamistapauksissa. Vierailijoiden valvonta kuuluu myös henkilöstöturvallisuuteen. (http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html luettu 23.3.2009)

Henkilöstöturvallisuuden tavoite on, ettei työntekijä tietämättömyyden, huonon motivaation tai pahantahtoisuuden vuoksi pääse muuttamaan tai tuhoamaan tietoa, tai mahdollista jonkun ulkopuolisen käyttämään sitä. Henkilöstöturvallisuuden pääpaino on riskien välttäminen ennakkoon ja synnyn estäminen. Salasanoja ei kirjoiteta muistilapuille, eikä säilytetä asiaankuulumattomien ihmisten ulottuvilla. Uutta henkilöä palkattaessa voidaan mitata hänen luotettavuuttaan psykologisilla testeillä tai pyytää lausunto poliisilta. Henkilöstöturvallisuuden riskeiksi voivat muodostua liian laajat käyttöoikeudet, liika asiantuntemus, välinpitämätön asenne tietoturvallisuutta kohtaan sekä motivaation puute ja tyytymättömyys työhön.

Fyysiseen turvallisuuteen liittyy kulunvalvonta, työasemien murtosuojaus ja turvamerkintä, palvelintilojen lukitseminen ja paloturvallisuus, varmuuskopioiden ja lisenssien turvallinen säilytys, hälytysjärjestelmät ja vartiointi sekä verkkokaapeloinnin ja laitekaappien suojaus ulkopuolisilta. Fyysinen turvallisuus on laaja-alaistaja näin ollen myös vaikeasti hallittavaa. Fyysinen turvallisuus koostuu monesta eri osatekijästä, turvallisuuden perusta kuitenkin luodaan jo rakennusvaiheessa. Laitteistoturvallisuudesta puhuttaessa, sillä tarkoitetaan järjestelmässä olevia turvallisuusominaisuuksia, jotka on toteutettu tietokonelaitteistoa hyväksikäyttäen. Näin pyritään varmistamaan tietokonelaitteiden luotettava ja häiriötön toiminta. Ongelmia voivat aiheuttaa väärät käyttöolosuhteet, laitteistovirheet tai laitteiden virheellinen käyttö. Laitteistoturvallisuutta varmistaa säännöllinen huolto, huollon nopea saatavuus vika- ja ongelmatilanteissa sekä varaosien ja tarvikkeiden nopea saatavuus. Edellä mainittujen uhkatekijöiden lisäksi tulee ottaa huomioon tärinän aiheuttamat vahingot, energiakatkokset ja jännitevaihtelut, pöly- ja kaasuvahingot ja erilaiset vahingonteot. (http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html luettu 23.3.2009)

Tietoliikenneturvallisuudella pyritään varmistamaan tietoturvan perustavoitteet eli verkossa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys. Keskeisenä

tavoitteena on varmistaa viestien alkuperäisyys, koskemattomuus ja luottamuksellisuus. Tietoliikenneturvallisuudessa on kyse on kaikista niistä toimenpiteistä joilla varmistetaan tietojen turvallisuus tiedon liikkuessa järjestelmän sisällä tai organisaatioiden välillä. Usein mielletään, että tietoliikenneturvallisuudessa on kyse ainoastaan tietokoneisiin kytkettyjen verkkojen turvallisuudesta. Tietoliikenneturvallisuuteen kuuluvat kuitenkin kaikki ne asiat, jotka koskevat teleliikennöintiä, verkkojen rakentamista ja niiden suunnittelua. Jotta tietoturva pystyttäisiin pitämään riittävän korkealla tasolla, on jatkuvasti seurattava alan kehitystä, hankittava laitteistoja tai ohjelmistoja, joilla suojaudutaan uusia uhkia vastaan. (http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html luettu 23.3.2009)

Laitteistoturvallisuus käsittää yrityksen tietojenkäsittelylaitteiden tieto-turvallisuuteen liittyvät näkökohdat. Laitteistoturvallisuuden tavoitteena on varmistaa se, että tietojenkäsittelylaitteisto täyttää yrityksen tietoturvallisuus-vaatimukset: laitteiston toimintavarmuus ja tietoturva-ominaisuudet eivät saa vaarantaa riskikartoituksen pohjalta määriteltyä tietoturvatasoa.
Laitteiden hankintaan, asennukseen, käyttöön, huoltoon ja ylläpitoon sekä käytöstä poistoon liittyy runsaasti tietoturvan kannalta kriittisiä seikkoja. Niiden asianmukainen hoitaminen edellyttää ammattitaitoa. Mikäli yrityksestä ei löydy näihin asioihin perehtynyttä henkilöä, tulee kääntyä ulkopuolisen asiantuntijan puoleen.
Laitteistoturvallisuuden tavoitteena on varmistaa se, että tietojenkäsittelylaitteisto täyttää yrityksen tietoturvallisuusvaatimukset: laitteiston toimintavarmuus ja tietoturvaominaisuudet eivät saa vaarantaa riskikartoituksen pohjalta määriteltyä tietoturvatasoa. Laitteiden hankintaan, asennukseen, käyttöön ja käytöstä poistoon liittyy runsaasti tietoturvan kannalta kriittisiä seikkoja. Niiden asianmukainen hoitaminen edellyttää ammattitaitoa. Mikäli yrityksestä ei löydy näihin asioihin perehtynyttä henkilöä, tulee kääntyä ulkopuolisen asiantuntijan puoleen.
(http://www.webtoimisto.fi/iPortfolio/Pdftiedostot/Tietoturvaohje.pdf luettu 22.3.2009)

Ohjelmistoturvallisuuden tavoitteena on varmistaa se, että tietojenkäsittelyohjelmisto täyttää yrityksen tietoturvallisuusvaatimukset: ohjelmiston toimintavarmuus ja tietoturvaominaisuudet eivät saa vaarantaa riskikartoituksen pohjalta määriteltyä tietotur-

vatasoa. Ohjelmistojen hankintaan, asennukseen, käyttöön ja käytöstä poistoon liittyy runsaasti tietoturvan kannalta kriittisiä seikkoja. Niiden asianmukainen hoitaminen edellyttää ammattitaitoa. Mikäli yrityksestä ei löydy näihin asioihin perehtynyttä henkilöä, tulee kääntyä ulkopuolisen asiantuntijan puoleen.
(http://www.webtoimisto.fi/iPortfolio/Pdftiedostot/Tietoturvaohje.pdf luettu 22.3.2009)

Tietoaineistoturvallisuudessa tavoitteena on mm. välttää eri muodoissa (paperi, tiedostot jne.) olevan, yrityksen toiminnan kannalta merkittävän tiedon

- tuhoutuminen
- asiaton muuttaminen (väärentäminen) sekä
- vääriin käsiin joutuminen

Tietoaineisto luokitellaan niiden sisällön perusteella.
Tietoaineiston luokittelulla tarkoitetaan yrityksen toiminnassa tarvittavan tiedon järjestämistä sen mukaisesti, mikä merkitys kullakin tiedolla on yritystoiminnalle. Yksinkertaisimmillaan se tarkoittaa yrityssalaisten tai muulla perusteella salassa pidettävien tietojen luokittelemista eli erottamista yrityksen muista tiedoista. Tärkeä lähtökohta tietoaineiston luokitukselle on nykyinen ja tulevakin lainsäädäntö, joka useissa yhteyksissä edellyttää toiminnanharjoittajan ilmoittavan esimerkiksi tietoja saavalle viranomaiselle tai muulle taholle, mitkä tiedot ovat luottamuksellisia tai muulla tavoin yrityssalaisia.
Edelleen erityissäännöksillä järjestetään se, miten tällaisia tietoja on käsiteltävä: tietosisällön ilmaisukielto, säilyttäminen, kopiointi, hävittäminen jne. Tietoaineiston luokituksella ilmaistaan samalla salassapitotahto ja tehdään konkreettisia tietoturvallisuustoimenpiteitä. Tietoaineiston luokittelu on resurssien kannalta tietoturvallisuusmenettelyn raskain vaihe sen vuoksi, että kaikki tärkeät tietoryhmät on käytävä läpi ja päätettävä toiminnallistaloudellisin perustein, mitkä tiedot luokitellaan yrityssalaisiksi, mitkä jäävät luokittelun ulkopuolelle. Kun tämä on tehty, on menettelyn ylläpitäminen varsin vaivatonta. Tietoaineisto tarkoittaa kaikkea kirjallista tai kuvallista esitystä sekä tallennetta, mikä voidaan lukea, kuunnella tai saada muulla tavoin ymmärretyksi teknisin apuvälinein.
(http://www.webtoimisto.fi/iPortfolio/Pdftiedostot/Tietoturvaohje.pdf luettu 22.3.2009)

Julkishallinnossa käsitellään paljon tärkeää tietoa, kuten esimerkiksi henkilötietoja, taloustietoja ja eri organisaatioiden asiakirjoja. Osa tiedoista on salassa pidettävää, arkaluonteista tai muuta luottamuksellista tietoa. Salassa pidettävällä tiedolla tarkoitetaan lailla salassa pidettäväksi säädettyjä asiakirjoja tai tietoja. Salassa pidosta säädetään mm. julkisuus- ja henkilötietolaissa sekä muissa erityislaeissa. Eräät viranomaisten salassa pidettävistä asiakirjoista on määritelty turvaluokittelun piiriin. Tämän vuoksi on tärkeää, että tiedot eivät päädy tahallisesti tai tahattomastikaan asiattomien haltuun. Lisäksi julkishallinnossa on paljon tietoa, joka ei ole salassa pidettävää, vaan luonteeltaan julkista, mutta tällaisenkin tiedon oikeellisuudesta, muuttumattomuudesta ja saatavuudesta sekä lain mukaisesta käsittelystä on huolehdittava. Lisäksi on otettava huomioon osassa julkishallintoa käytetty viranomaiskäyttöluokka. Tätä käytetään mm. puolustusvoimissa.

Turvaluokiteltavat asiakirjat jaetaan JulkA 2 §:n mukaisesti kolmeen turvaluokkaan, jotka eroavat toisistaan lähinnä asiakirjan ja sen tietojen suojaamiseksi tarvittavan suojaustason osalta:
I turvaluokan asiakirjat varustetaan leimalla tai merkinnällä ”Erittäin salainen” (engl. top secret),
II turvaluokan asiakirjat varustetaan merkinnällä ”Salainen” (engl. secret) ja
III turvaluokan asiakirjat merkinnällä ”Luottamuksellinen” (engl. confidential).
Käyttöturvallisuuden tavoitteena on luoda sellaiset menettelytavat, joilla tieto-turvallisuuden taso säilytetään päivittäisessä toiminnassa, laitteiden ja ohjelmien käyttämisessä. Käyttöturvallisuuteen liittyy mm. Työntekijöiden työtehtävissään tarvitsemien laitteiden ja ohjelmien käytön hallinnan varmistaminen, esim. koulutuksen järjestäminen. Laitteiden ja ohjelmien toimintavarmuus taataan luomalla asianmukaiset hankinta-, asennus-, huolto- ja ylläpitorutiinit. Laitteiden ja ohjelmien käytönvalvonta, tietojärjestelmien käytönvalvonta, salaaminen, tietokoneviruksilta suojautuminen sekä järjestelmien ja tietojen varmennus

Etätyöllä tarkoitetaan sitä, että yrityksen tietojärjestelmiin ollaan yhteydessä muualta, kuin yrityksen hallinnoimista verkoista. Etäkäytöllä ei kuitenkaan tarkoiteta asiakkaille tarkoitettujen palvelujärjestelmien käyttöä. Etäkäyttäjinä voivat olla yrityksen

omat toimihenkilöt ja yhteistyökumppaneiden sekä ohjelmisto-, järjestelmä- tai laitetoimittajien työntekijät.

Etätyöhön liittyvät samat tietoturvariskit kuin toimipistetyöskentelyynkin. Lisäksi tulee ottaa huomioon etä- ja matkatyöhön liittyvät erityisriskit. (http://www.webtoimisto.fi/iPortfolio/Pdftiedostot/Tietoturvaohje.pdf luettu 23.3.2009)

5.3 Henkilöstön tietoturvaohje

Valtionhallinnossa on tehty henkilöstölle suunnattu tietoturvaohje, jonka tavoitteena on yhtenäistää julkishallinnon ohjeistusta ja käytäntöjä. Tämän lisäksi on tarkoitus, että organisaatiokohtaisesti annetaan tarkempia ohjeita, jotka voivat perustellusti myös poiketa yleisistä ohjeista. Ohjeisto on pysyväisluonteinen kuvaus organisaatiossa noudatettavista menettelyistä, ja se on jatkuvasti henkilöstön saatavilla ja tarkistettavissa.

Seuraavaan luetteloon on koottu keskeisimmät tietoturvan ohjeet:
1. Seuraa tietoturvallisuuteen liittyviä tiedotteita, tutustu ohjeisiin ja osallistu sinulle tarjottuun koulutukseen. Toimi saamiesi ohjeiden mukaisesti.
2. Tue osaltasi organisaation kulunvalvontaa ja käytä organisaation toimitiloissa kuvallista henkilökorttiasi.
3. Älä jätä vierasta yksin tai valvomatta työhuoneeseesi tai muihin organisaation tiloihin.
4. Älä anna ulkopuolisen käyttää tietokonettasi.
5. Noudata ns. puhtaan pöydän periaatetta. Älä säilytä työpöydällä salassa pidettävää aineistoa.
6. Käsittele tietoja huolellisesti välineestä riippumatta. olipa tiedon välittäjänä sitten henkilö, tietokone, paperi, puhelin tai telekopio.
7. Älä luovuta henkilökohtaisia käyttäjätunnuksia ja salasanojasi toisen henkilön käyttöön. älä edes tietohallintohenkilöstölle, koska he eivät niitä tarvitse.
8. Älä anna kenenkään nähdä tietokoneesi näyttöä tai näppäimistöä, kun käsittelet arkaluontoista tietoa tai kun syötät käyttäjätunnuksia ja salasanoja.
9. Vaihda salasanat riittävän usein ja heti, kun epäilet niiden paljastuneen.
10. Käytä tietoaineistoja ja työvälineitä vain työtehtäviesi hoitamiseen.

11. Älä asenna ohjelmistoja tai tee niiden asetusmuutoksia, ellei tämä kuulu työtehtäviisi.
12. Tallenna tekemäsi työ verkkopalvelimen levylle, mistä tiedot varmistetaan keskitetysti.
13. Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen.
14. Muista, että organisaation laitetta, verkkoa tai sähköpostia käyttäessäsi näyt ja esiinnyt tietoverkossa aina. tahtomattasikin. organisaation edustajana.
15. Käytä aina asianmukaista salausta, mikäli sinun on siirrettävä Internetin kautta salassa pidettävää tietoa.
16. Mikäli siirrät aineistoa muistitikun tai muun muistivälineen avulla, valvo siirtoa aina henkilökohtaisesti.
17. Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi aina kun poistut työpisteestäsi.
18. Työpäivän päättyessä kirjaudu tietojärjestelmästä ulos ja sammuta työasemasi organisaatiokohtaisen ohjeen mukaisesti.
19. Ilmoita aina tietoturvallisuuteen liittyvistä ongelmatilanteista ja havaitsemistasi uhkista ja suojauspuutteista välittömästi tietoturvavastaavalle, tietohallinto-organisaatioon tai omalle esimiehellesi. Heidän velvollisuutenaan on ryhtyä tarvittaviin toimenpiteisiin.
20. Pyydä tarvittaessa neuvoa organisaatiosi asiantuntijoilta.
(http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061127Henkil/Vahti_10_06.pdf luettu 20.3.2009)

5.4 Työpaikalla

5.4.1 Tietokoneen käyttö

Tietokoneen käyttö sisältää sekä oman työaseman että verkon kautta käytettävien palveluiden käytön. Puolustusvoimien työskentely tapahtuu puolustusvoimien tuotteistamilla ja hyväksytyillä työvälineillä. Siksi henkilökunta ei voi käyttää työpaikallaan itse hankittuja välineitä tai lisävarusteita, joten esimerkiksi:
Ohje:

- Vastaat käyttäjänä omasta koneestasi. Ole siis huolellinen.
- Vain tietohallinto-organisaatio saa asentaa tietokonelaitteita verkkoon ja asentaa tai päivittää koneisiin ohjelmia.

- Kirjaudu koneelle aina omilla käyttöoikeuksillasi.
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi (Windows-työasemalla
- paina Ctrl+Alt+Del ja valitse Lukitse tietokone) aina kun poistut työpisteestäsi.
- Lisävarmistuksena voit myös käyttää salasanasuojattua näytönsäästäjää. Toimi organisaatiokohtaisen ohjeistuksen mukaisesti.
- Tallenna työsi käyttäen välitallennuksia. Älä jätä työtä tallentamatta, kun poistut työpisteestäsi.
- Tallenna kaikki tärkeä tieto sellaisen verkkopalvelimen levylle, josta tietohallinto-organisaatio ottaa säännöllisesti varmuuskopiot.
- Jos työaseman kiintolevy tai muu tallennusväline, kuten esimerkiksi muistitikku tai CD-/DVD-levy rikkoutuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin.
- Huolehdi hävittämisestä organisaation ohjeistuksen mukaisesti tai toimita tallennusväline tietohallinto-organisaatioon hävitettäväksi.
- Kirjaudu ulos sekä ohjelmistoista että koneeltasi ja sammuta tietokoneesi työpäivän päättyessä organisaation ohjeistuksen mukaisesti.
- ulkoisia USB-kiintolevyjä ei saa käyttää (ei ole tuotteistettu)
- omien laitteiden kuten matkapuhelimien, kameroiden tai CD-Rom –levyjen liittäminen tietoverkkoon on kielletty

(http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061127Henkil/Vahti_10_06.pdf luettu 23.3.2009)

5.4.2 Käyttöoikeudet ja salasanat

Puolustusvoimien tietojärjestelmiin tarvitaan käyttöoikeus. Käyttöoikeus on henkilökohtainen ja se on yhdistetty juuri sinun henkilöllisyyteesi ja työtehtävääsi. Käsittele käyttäjätunnusta ja salasanaa samalla tavalla kuin pankkikorttiasi ja tunnuslukuasi.

- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanojasi, toimikorttiasi tai PIN-koodejasi toisen henkilön käyttöön. älä edes tietohallinnolle. Suhtaudu epäilevästi kaikkiin tiedusteluihin, jotka liittyvät salasanoihisi tai järjestelmien käyttöoikeuksiisi.
- Vaihda salasanat riittävän usein ja heti, jos epäilet niiden paljastuneen.

- Huolehdi, että salasanat ovat riittävän monimutkaisia ja vältä tuttujen jokapäiväisten sanojen käyttöä salasanana. Hyvässä salasanassa voi olla pieniä ja isoja kirjaimia, numeroita ja jopa erikoismerkkejä. Kaikkiin järjestelmiin ei kuitenkaan käy erikoismerkit. Hyvä salasana on sinun helppo muistaa, mutta vaikea ulkopuolisen arvata.
- Älä kirjoita salasanoja muistiin, ainakaan sellaiseen paikkaan, mistä ne ovat helposti löydettävissä.
- Älä käytä organisaation antamaa käyttäjätunnusta ja salasanaa Internetin palveluihin rekisteröityessäsi.
- Mikäli joissain tilanteissa tai järjestelmissä on pakko käyttää yhteistunnuksia, siitä päättää järjestelmän tai tietojen omistaja. Yhteistunnusten käyttö on sallittu vain omistajan luvalla. Yhteistunnuksen salasana täytyy vaihtaa aina, kun jonkun käyttäjän käyttöoikeus siihen lakkaa tai epäillään jonkun ryhmään kuulumattoman saaneen sen tietoonsa. Salasana tulee muutoinkin vaihtaa riittävän usein.

(http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061127Henkil/Vahti_10_06.pdf luettu 23.3.2009)

5.4.3 Internet ja sähköposti

Internet ja sähköposti ovat hyviä työvälineitä sekä tiedon hakuun että yhteydenpitoon. On kuitenkin muistettava, että sähköpostissa tai Internetissä ei itsessään ole mitään suojausta, vaan tiedot liikkuvat salaamattomana julkisessa verkossa. Sähköpostin ja Internetin käyttö vaativatkin käyttäjältä huolellisuutta.

- Internet ja sähköposti on työpaikalla tarkoitettu työkäyttöön. Käytä henkilökohtaiseen viestintääsi yksityistä sähköpostiosoitettasi.
- Käytä vain sellaisia palveluita, jotka tiedät asiallisiksi.
- Internetin kautta ei ole luvallista välittää salassa pidettävää tietoa ilman asianmukaista vahvaa salausta. Tällaiset viestit ja liitetiedostot on salattava tietohallinto-organisaation hyväksymillä tuotteilla.
- Opettele salaustuotteiden oikea käyttö, jotta tieto ei vahingossa lähde salaamattomana.
- Ohjelmien lataus Internetin kautta on puolustusvoimilla kokonaan kiellettyä. Tällöin tietohallinto-organisaatio asentaa kaikki tarvittavat ohjelmat.

- Jos käytät julkisia päätteitä tai tilapäisesti toisen henkilön hallussa olevaa tietokonetta, muista tyhjentää Internet-selaimen välimuisti ja evästeet (cookies). Pyydä tarvittaessa tietohallinnolta apua.
- Muista, että viranomaisella on velvollisuus käsitellä virkasähköposti.
- Virkasähköpostia saa käsitellä vain oman organisaation tai mahdollisesti muun julkishallinnon organisaation omistamilla laitteilla.
- Työhön liittyvä sähköposti vastaanotetaan ja ohjataan oman organisaation sähköpostijärjestelmään. Sitä ei saa ohjata tai jatkolähettää organisaation sähköposti-järjestelmän ulkopuolelle.
- Ohjaa sähköisesti asioivat asiakkaat lähettämään käsittelyyn tulevat, vireille saatetut asiat organisaation määrittelemään sähköpostiin.
- Muista, että vastaat henkilökohtaiseen sähköpostiin tulevasta työpostista virkavelvollisuuksien mukaisesti.
- Muiden kuin virkasähköpostin (esimerkiksi Internetin ilmaissähköpostiohjelmat tai kotisähköposti) käyttö töissä on sallittua vain oman organisaation luvalla.
- Varmista, että sähköpostisi käsittelyyn liittyvät velvollisuudet tulevat hoidettua myös poissaolosi aikana virkavelvollisuuksien mukaisesti.
- Sähköpostin liitetiedostot voivat sisältää haittaohjelmia (viruksia, matoja tai troijalaisia). Varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja. Älä avaa epäilyttäviä viestejä, vaan toimi ohjeistuksen mukaisesti. Tarvittaessa voit ilmoittaa asiasta tietohallintoon.
- Roskapostia voivat olla esim. sähköpostiin tilaamatta tulleet mainokset. Roskapostiin ei kannata vastata, vaan se kannattaa tuhota heti. Jos viestiin vastaa, tietää roskapostittaja sähköpostiosoitteesi toimivaksi ja jatkaa roskapostien lähettämistä ja lisäksi välittää osoitteesi myös muille roskapostittajille.
- Älä anna työsähköpostiosoitettasi ulkopuolisille muissa kuin työhön liittyvissä yhteyksissä.
- Ole terveen epäluuloinen sähköpostiviestin luotettavuuteen. Sähköpostiviesti voi tulla myös muualta kuin viestin lähettäjäkentässä näkyvältä taholta. Myös virukset voivat lähettää sähköpostia ilman käyttäjän toimenpiteitä. Varo ns. kalasteluviestejä., joissa sinua pyydetään syöttämään tunnuksia ja salasanoja aidontuntuisiin palveluihin.
- Älä välitä ketjukirjeitä eteenpäin.

- Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite. Mikäli oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
- Jakelulista on henkilöluettelo, jonka jokainen vastaanottaja saa tietoonsa ja se voi olla henkilörekisteritieto tai salassa pidettävä tieto, jonka luovuttamisesta on erikseen säädetty. Voit käyttää sähköpostin piilokopiotoimintoa, jos haluat estää jakelulistalla olevien osoitteiden näkymisen vastaanottajille.
- Huolehdi, että lähettämäsi sähköpostiviesti on kohdistettu oikeille henkilöille ja oikeisiin osoitteisiin, myös valmiita jakelulistoja käyttäessäsi. Vältä turhien sähköpostien lähettämistä. Esimerkiksi joulutervehdysten lähettäminen kuormittaa sekä sähköposti-järjestelmää että vastaanottajan sähköpostilaatikkoa.
- Työsuhteen päättyessä sähköpostiosoite ja -laatikko poistetaan. Siirrä virkapostisi työnantajan käyttöön ja poista mahdolliset henkilökohtaiset viestit.

(http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061127Henkil/Vahti_10_06.pdf luettu 23.3.2009)

5.4.4 Toimitilojen turvallisuus

Toimitilojen turvallisuudella varmistetaan, että tietoja, asiakirjoja ja tietokonelaitteita säilytetään ja käsitellään asianmukaisesti turvallisissa tiloissa. Toimitilojen turvallisuus sisältää mm. kulunvalvonnan, teknisen valvonnan ja vartioinnin, palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunnan sekä lähettipalvelujen ja tietoaineistoja sisältävien lähetysten turvallisuuden.

- Suuntaa asiakaspalvelupisteessä ja -tilanteessa tietokoneesi näyttö harkitusti, onko tarkoitus, että tiedot näkyvät asioijalle vai ei? Käytä näytön suojaa.
- Noudata kulunvalvonnasta annettuja ohjeita. Käytä organisaation toimitiloissa kuvallista henkilökorttiasi (mikäli sellainen on annettu).
- Tarkista työpisteeseesi tullessasi, ettei mitään asiatonta ole tapahtunut poissaolosi aikana.
- Jokaisella vieraalla tulee olla isäntä. Isäntä vastaa vieraidensa oleskelusta ja kulkemisesta toimitiloissa.
- Säilytä tieto ja laitteet turvassa, mahdollisuuksien mukaan lukitussa kaapissa ja huoneessa.

- Älä jätä kannettavaa tietokonetta tai matkapuhelinta ilman valvontaa. Säilytä laitteita lukitussa tilassa. Huolehdi myös muistitikkujen, CD-/DVD-levyjen, paperitulosteiden ym. asianmukaisesta säilyttämisestä.
- Noudata .puhtaan pöydän. periaatetta. Työpöydällä ei saa säilyttää salassa pidettävää tietoa.
- Älä jätä vierasta yksin tai ilman valvontaa työhuoneeseesi tai muihin toimitiloihin.
- Kuvaaminen organisaation tiloissa on kiellettyä. Noudata organisaatiokohtaista ohjeistusta. Valvo myös vieraidesi toimintaa ja esim. kamerakännyköiden käyttöä.
- Lukitse työhuoneesi ovi työpäivän päättyessä tai poistuessasi pidemmäksi aikaa työpisteestäsi.
- Ohjaa vieraat tai eksyneet. henkilöt oikeisiin paikkoihin. Älä päästä asiattomia henkilöitä toimitiloihin esim. töistä lähtiessäsi.
- Älä jätä kulunvalvonnassa olevia tai muuten suljettuina pidettäväksi tarkoitettuja ovia auki.

(http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061127Henkil/Vahti_10_06.pdf luettu 23.3.2009)

5.4.5 Etätyö ja mobiililaitteet

Monet liikkuvan työn välineet voivat vastata ominaisuuksiltaan ja sisällöltään työpaikan työasemia. Laitteet eivät enää ole esim. pelkkiä puhelimia. Liikkuvan työn välineisiin ja niiden käyttöön liittyy vastaavia uhkia kuin kiinteämmin asennettuihin, joten kyseeseen tulevat soveltuvin osin samat turvallisuusohjeet. Kun välineitä lisäksi kuljetetaan ja käytetään työpaikan toimitilojen tarjoamien turvatoimien ulkopuolella, tarvitaan erityistä huolellisuutta.

- Huolehdi työnteossa käyttämiesi kannettavien tietokoneiden, matkapuhelinten, kommunikaattoreiden ja kämmentietokoneiden turvallisuudesta. Älä säilytä niissä ylimääräistä tietoa.
- Tutustu laitteen ja siinä olevien ohjelmien käyttöohjeisiin ja turvallisuusominaisuuksiin (mm. PIN-kyselyt, Bluetooth-asetukset, sovellusten lataaminen).
- Huolehdi, että matkapuhelimessasi on päällä PIN-kysely. Vaihda laitevalmistajan tai palveluntarjoajan antamat PIN-koodit.

- Älä lataa ja asenna laitteisiin mitään työhön kuulumatonta.
- Käytä tietojen salausta mahdollisuuksien mukaan.
- Huolehdi tietojen varmuuskopioinnista ja/tai tarvittaessa synkronoinnista muuhun tietojärjestelmään organisaatiokohtaisen ohjeen mukaisesti.

Etätyöllä tarkoitetaan muualla kuin organisaation vakituisessa toimipisteessä suoritettavaa työtä. Tyypillinen etätyö on kotoa tehtävää toimistotyötä. Etätyötä voidaan tehdä myös muusta vakituisesta paikasta (esim. organisaation järjestämä etätyöpiste) tai matkoilla (esim. hotelli tai toisen organisaation tilat), jolloin käyttöympäristöt vaihtelevat eikä ympäristön turvallisuuteen voida juurikaan vaikuttaa. Etätyöntekijän omilla toimenpiteillä ja menettelytavoilla on tällöin suuri merkitys. Etäyhteisön tietoliikenneyhteys organisaation sisäverkon ulkopuolelta ja etäkäyttö tietoteknistenpalvelujen käyttöä etäyhteyden avulla. Langattomien verkkoyhteyksien yleistyessä etätyöntekijän on entistä useammin kyettävä tekemään itsenäiset arviot etätyöympäristön turvallisuudesta. (http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061127Henkil/Vahti_10_06.pdf luettu 23.3.2009)

5.4.6 Kotikone

Mikäli sinulla on oma tietokone ja Internet-liittymä, on tärkeää huolehtia myös niiden tietoturvallisuudesta.

- Tee jokaiselle käyttäjälle omat henkilökohtaiset tunnukset, joilla on vain ns. normaalikäyttäjän oikeudet ja käytä ylläpitäjän tunnusta (esim. Järjestelmänvalvoja, Administrator) vain ylläpitotehtäviin.
- Asenna vain virallisia, ajan tasalla olevia ohjelmistoja.
- Huolehdi käyttöjärjestelmän ja muun varusohjelmiston jatkuvasta automaattisesta päivittymisestä.
- Käytä tunnettua ja hyvämaineista tietoturvaohjelmapakettia (sis. mm. virustorjunta, palomuuri, vakoiluohjelmatorjunta, roskapostisuodatus) ja huolehdi sen jatkuvasta automaattisesta päivittymisestä.
- Älä avaa epäilyttäviä sähköpostiviestejä ja -liitteitä.
- Tee säännöllisesti varmuuskopiot ja harjoittele niiden käyttöönottoa.

- Kun kirjaudut Internetin palveluihin ja teet esim. ostoksia, käytä vain luotettavia palveluita ja toimittajia. Älä anna enempää henkilökohtaista tietoa kuin on tarpeen
- Älä anna työnantajaan liittyvää tietoa lainkaan.
- Sammuta tietokone ja katkaise Internet-yhteys, kun et käytä niitä.

(http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061127Henkil/Vahti_10_06.pdf luettu 23.3.2009)

5.5 Ongelmatilanteet, ilmoitusvelvollisuus ja seuraamukset

Mikäli hallussasi oleva laite, kulkukortti, tunniste tms. katoaa tai varastetaan, ilmoita siitä välittömästi ao. vastuuhenkilölle oman vastuusi rajaamiseksi.
Ilmoita aina haittaohjelmista (esim. virukset, madot tai troijalaiset) ja muista tietoturvallisuuteen liittyvistä ongelmista välittömästi tietoturvavastaavalle, tietohallinto-organisaatioon tai omalle esimiehellesi. Ilmoita aina myös muista turvallisuuteen liittyvistä epäilyistä, suojauspuutteista tai ongelmista turvallisuusvastaaville tai omalle esimiehellesi.

Jos epäilet tietoturvaloukkausta tai haittaohjelmatartuntaa

- Älä hätiköi.
- Tietokonetta ei tarvitse sulkea, mutta irrota lähiverkkokaapeli työasemastasi.
- Kirjoita ylös, mitä mahdollisessa ilmoituksessa tai varoituksessa luki. Kirjoita muistiin tekemisesi ja kirjaa menetetty työaika mahdollista korvausvaatimusta varten.
- Ota yhteyttä tietohallinto-organisaatioon ja/tai tietoturvavastaavaan.
- Auta tutkinnassa. Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti.
- Toimi saamiesi ohjeiden mukaisesti.
- Kirjoita muistiin tekemisesi ja kirjaa menetetty työaika mahdollista korvausvaadetta varten.

Työntekijöiden seuraamukset tietoturvarikkomuksista voivat olla seuraavat.
Lakien, määräysten ja ohjeiden rikkomisesta käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Rikkomuksista tiedotetaan aina esimiehelle. Mikäli rikkomuksesta aiheutuu taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin. Tietojen vää-

rinkäyttö tai tahallinen tai huolimaton lakien, määräysten ja ohjeiden vastainen toiminta voi johtaa kurinpidollisiin seuraamuksiin, kuten irtisanomiseen ja/tai rikosoikeudellisiin seuraamuksiin.
(http://www.webtoimisto.fi/iPortfolio/Pdftiedostot/Tietoturvaohje.pdf luettu 24.3.2009)

5.6 Yleisimmät tietoturvauhat

Tutkimusten mukaan suurimman tietoturvauhan on muodostanut perinteisesti yrityksen oma henkilökunta, vaikkakin nykyisin avoimien tietoverkkojen käytön lisääntyminen on kasvattanut myös ulkoista uhkaa. Osa uhista on tarkoituksella aiheutettuja, mutta suurin osa ongelmista aiheutuu osaamattomuudesta, käyttäjän virheestä tai inhimillisestä erehdyksestä. Myös teollisuusvakoilu, palo- ja vesivahingot sekä tekniset viat saattavat aiheuttaa yrityksille todellisia tietoturvauhkia.
Yleisimmät tietoturvavahingot ja -väärinkäytökset

- Osaamattomuus, vahingot, inhimilliset erehdykset.
- Luvallisten käyttäjien tekemät kielletyt toimenpiteet
- Luvattomien käyttäjien tekemät kielletyt toimenpiteet
- Tallennetun tiedon muuttaminen ja kopiointi
- Tietokonevirukset
- Laitteisto- ja ohjelmistovirheet
- Varkaus, kavallus, petos
- Tietojärjestelmään tunkeutuminen
- Tietojen paljastuminen: salakuuntelu, tiedon sieppaaminen, pengonta
- Ohjelman muuttaminen
- Tietojen tai tiedonkäsittelyresurssien vioittuminen tai tuhoutuminen
- Tahallinen tuhoaminen ja haitanteko: sabotaasi, vandalismi, ddos-hyökkäys (distributed denial of service)

(http://www.webtoimisto.fi/iPortfolio/Pdftiedostot/Tietoturvaohje.pdf luettu 24.3.2009)

6 POHDINTA JA JOHTOPÄÄTÖKSET

Kehittämishankkeen alussa huomasin että minulla oli vaikeuksia löytää sopivaa hanketta ja siksi hankkeen aihe vaihtuikin alkuperäisestä. Omien pohdintojeni jälkeen

halusin kuitenkin tehdä sellaisen hankkeen josta olisi hyötyä niin minun omassa työssäni kuin minun työnantajalleni. Sitten löysin tämän itseäni kiinnostavan aiheen eli tietoturvan ja siihen liittyvän koulutuksellisen näkökulman. Täten kehittämishankkeeni liikkeelle lähtö viivästyi ja sen toteutuksen kanssa tuli hieman kiire. Hakiessani opettajakoulutukseen en ajatellut asioita niin kauaskantoisesti että työssäni kouluttaisin oman työpaikan henkilöstöä. Mutta koulutuksen myötä olen saanut kipinän kouluttamiseen ja kiinnostus opetusasioihin on herännyt.

Puolustusvoimissa on viime vuosina eletty suurien muutosten aikaa ja koko tietotekniikan tukipalvelut on ulkoistettu. Esim. meidän organisaatiossa olen ainut henkilö jonka vastuualueeseen tietotekniikka kuuluu. Ulkoistuksen takia on tärkeää että organisaatiossa kiinnitetään enemmän tietoturvallisuuteen.

Puolustusvoimien ohjeistus ja toimintatavat tietoturva-asioissa on pirstoutunutta. Ohjeita ja vaatimuksia on paljon, julkaisumuoto ja sijainti vaihtelevat suuresti, eikä versionhallinnasta ole tietoakaan. Tilannetta kuvaa hyvin se, että lähes kaikesta on olemassa ohje jossakin, mutta harva tietää missä. Pysyväisasiakirjoja noudatetaan hyvin varomääräysten, ajoneuvojen, meriliikenteen ja ammunnan osalta, mutta ei tietoturvan osalta. Merkittävin syy tietoturva-pysyväisasiakirjojen laistamiseen lienee se, että tietoturvaa ei mielletä yhtä tärkeäksi kuin muita määräyksiä ja lisäksi se, että aihealue on eräällä tavalla abstraktimpi. Kehittämispotentiaali on suuri mutta kehittämiseen ei ole kuitenkaan panostettu riittävästi, koska sopivat menetelmät ja kehittämisen tiedollinen perusta ovat puuttuneet.

Uuden työntekijän on opittava tietyt yritystä koskevat perusasiat ennen varsinaisen työn aloittamista. Siksi onkin tärkeää että hänelle annetaan perehdytysvaiheessa riittävä tietoturvakoulutus muiden tietojen lisäksi. On myös tärkeää että työntekijät osaavat ottaa tieturvallisuuden osana normaalia työskentelyä. Lisäksi kaikkien työntekijöiden työskentely tehostuu ja minimoidaan ongelmien virheiden osuus.

Itse sain tästä kehittämishankkeesta varsin paljon tietoa kouluttamisesta, opettamisesta ja opetussisällöntuotannosta joten tätä tietoa voin hyödyntää omassa työssäni tulevaisuudessakin.

LÄHTEET

Helsinki: Helsingin yliopiston Lahden tutkimus- ja koulutuskeskus.
Leino, A.-L. & Leino, J. 1995. Kasvatustieteen perusteet. Helsinki: Kirjayhtymä.
Mezirow, J. (toim.) 1996. Uudistava oppiminen. Kriittinen reflektio aikuiskoulutuksessa.
Peltonen, M. 1985. Koulutusoppi. Helsinki: Otava.
Pohjonen, P. 2005. Työssäoppiminen. Ammatillisen osaamisen perusta. Jyväskylä: PSkustannus.
Rogers, J. 2004. Aikuisoppiminen. Helsinki: Finn Lectura.
Sydänmaanlakka, P. 2000. Älykäs organisaatio. Helsinki: WSOY.
Uusikylä, K. & Atjonen, P. 2000. Didaktiikan perusteet. Helsinki: WSOY.
von Wright, J. 1996. Oppiminen selviytymiskeinona. Psykologia 39/1996
Internet lähteet
VAHTI 11/2006 Tietoturvakouluttajan opas
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/.../Vahti_11_06.pdf - luettu 26.3.09
VAHTI 10/2006 Henkilöstön tietoturvaohje
www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061127Henkil/Vahti_10_06.pdf luettu 23.3.2009
Tietoturvaopas
http://www.yliopistojentt.fi/VAHTI-CD/Sivusto/kayttajan_ohje/011_johdanto1.htm. luettu 23.3.2009
Tietoturvaohje
http://www.webtoimisto.fi/iPortfolio/Pdftiedostot/Tietoturvaohje.pdf luettu 24.3.2009
netti-artikkeli
http://www.kookas.fi/articles/read/6697 luettu 20.3.2009
Tietoturvallisuus on asenne VM 6/2008
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Tietot/vahti6_taitto_NETTI_%2B_KANNET.pdf luettu 20.3.2009
Tietoturva ja lainsäädäntö
(http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html luettu 23.3.2009)

Puolustusvoimien asianhallintajärjestelmä (PVAH)

LIITTEET

Liite 1

Lisää tietoa tietoturvallisuudesta on saatavissa mm. seuraavista lähteistä:

- . Tietoturvavastaava, tietohallintopäällikkö,organisaation omat ohjeet
- . Lainsäädäntö . Valtion säädöstietopankki (www.finlex.fi)
- . Tietoturvallisuutta ohjeistavat ja säätelevät organisaatiot, esimerkiksi
- . Valtiovarainministeriön VAHTI-ohjeet (www.vm.fi /vahti)
- . Tietosuojavaltuutetun toimiston ohjeet (www.tietosuoja.fi)
- . Tietoyhteiskunnan kehittämiskeskuksen ohjeet (www.tieke.fi)
- . Viestintäviraston ohjeet (www.ficora.fi)
- . Julkishallinnon ja elinkeinoelämän yhteiset ohjeet (www.tietoturvaopas.fi)
- . Tietoturva-ammattilaisten yhdistys (www.tietoturva.fi)

Liite 2

Tietoturvallisuutta sääteleviä lakeja

Tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annetun lain (621/1999) ja asetuksen (1030/1999) lisäksi useisiin eri lakeihin. Yksityiselämän suoja ja julkisuusperiaate ovat jo perustuslaissa säädeltyjä perusoikeuksia. Eri lakeihin sisältyvien salassapitosäännösten lisäksi laeista tärkeimpiä ovat:

• Perustuslaki (731/1999) 2.luku 10 § (Yksityiselämän suoja ja luottamuksellisen viestin salaisuus)
• Perustuslaki (731/1999) 2.luku 12 § (Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus)
• Laki viranomaisten toiminnan julkisuudesta (621/1999)
• Henkilötietolaki (523/1999) (Henkilötietojen käsittelyä koskevat yleiset periaatteet)
• Arkistolaki (831/1994) (Asiakirjojen laatiminen, säilyttäminen ja käyttö)
• Valtion virkamieslaki (750/1994) 17§ (Säädös valtion virkasuhteesta)
• Työsopimuslaki (55/2001)
• Rikoslaki (39/1889) 34.luku 9a § (Vaaran aiheuttaminen tietojenkäsittelylle)
• Rikoslaki (39/1889) 38.luku 8 § (Tietomurto)
• Rikoslaki (39/1889) 38.luku 9 § 1. kohta (Henkilötietorikos)
• Henkilötietolaki (523/1999) 48 § (Henkilörekisteririkkomus)
• Vahingonkorvauslaki (41/1974)
• Laki yksityisyyden suojasta työelämässä (477/2001)

Liite 3

Tietoturvallisuuden muistilista

1. Tietoturvallisuus perustuu lainsäädäntöön ja normiohjaukseen.

2. Tietoturvallisuudesta huolehtiminen kuuluu kaikille, myös sinulle.

3. Tunnista organisaatiosi suojattavat kohteet (tiedot, asiakirjat, tilat ja tietojärjestelmät).

4. Tunnista asiakirjojen ja tietojen laatu (salassa pidettävät tiedot, henkilötiedot jne.)

5. Tutustu organisaatiosi tietoturvaohjeisiin ja noudata niitä.

6. Tietojärjestelmien käyttöön tarvitaan aina henkilökohtainen käyttöoikeus.

7. Muista, että esiinnyt tietoverkossa julkishallinnon edustajana.

8. Suojaamattoman sähköpostin turvallisuus on verrattavissa postikortin turvallisuuteen.

9. Haitalliset ohjelmat, kuten virukset, madot ja troijalaiset, voivat levitä pelkästään Internet-sivuja selaamalla.

10. Pyydä tarvittaessa neuvoa organisaatiosi asiantuntijalta.

Liite 4

Organisaation esittely

1. Puolustusvoimat

Puolustusvoimilta edellytetään kaikissa tilanteissa aluevalvontaa ja kykyä koskemattomuuden ja itsenäisyyden puolustamiseen. Puolustuskykymme on estettävä ennalta sotilaallisen voiman käytöllä uhkaaminen ja maamme joutuminen sotilaallisten toimien kohteeksi. Harjoittamalla uskottavaa puolustuspolitiikkaa maahamme hyökkääminen tai alueemme hyväksikäyttö kolmatta osapuolta vastaan tulee kaikin tavoin kannattamattomaksi. Puolustusvoimilla on tällä hetkellä noin 15 000 työntekijää.

2. Koeampumalaitos

Sijaitsee Niinisalossa ja on osa Puolustusvoimien Materiaalilaitosta ja henkilöstöä on noin 70 henkilöä.

Koeampumalaitoksen päätehtävänä on koeammuntojen ampuminen, olosuhdetestausten tekeminen, koeräjäytyksien ja vastaavien kokeiden suorittaminen.

Koeampumalaitos tuottaa puolustusvoimille sekä käytössä oleviin että hankittaviin asejärjestelmiin lisätehokkuutta ja toisaalta aseiden käyttöhenkilöstölle palvelusturvallisuutta.

Koeammuntaa luonnehtii kaksi sanaa: turvallisuus ja rehellisyys.
Koeammunnoilla hyväksytyt tuotteet eivät saa aiheuttaa loppukäyttäjille turvallisuusriskejä. Ammuntaan osallistuvien riskit minimoidaan koulutuksella, ennakkoselvityksillä, vakioiduilla työmenetelmillä ja kiireettömyydellä. Rehellisyys tarkoittaa tulosten luotettavuutta. Pöytäkirjoissa ilmoitettujen tulosten on oltava oikeita, luotettavia mittauslaitteiden antamia arvoja, sekä pitkään kokemukseen perustuvia luotettavia arvioita.

Turvallisuussäännöt eivät kuitenkaan saa kahlita luovuutta. Uusien menetelmien tutkiminen ja kehittäminen on välttämätöntä, kun toimitaan ennen kokeilemattomien aseiden ja ampumatarvikkeiden parissa.

Koeampumalaitoksen tehtävät ja tuotteet

Koeampumalaitoksen toimialaan kuuluu seuraavia aseteknillisen alan sotavarustuksen tutkimukseen, kehittämiseen ja kokeiluun liittyviä asioita:

- kaikkia puolustushaaroja palvelevat kokeet ja koeammunnat sekä teollisuuden sopimuksiin perustuvat ammunnat
- ampumatarvikkeiden olosuhdetestaus

Koeampumalaitoksen tehtävien erityispiirteenä on se, että koeammunta on kovapanosammunta, jossa usein käytetään sotavarusteeksi hyväksymättömiä taisteluvälineitä.