VALTIOVARAINMINISTERIÖ

Tieto-turvallisuus on asenne!

Selvitys julkishallinnon tietoturva-koulutus-tarpeista

6/2008 VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

Tietoturvallisuus on asenne!

Selvitys julkishallinnon tietoturvakoulutustarpeista

Valtionhallinnon tietoturvallisuuden johtoryhmä

6/2008

VAHTI

Painotuote

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 09 16001 (vaihde)
Internet: www.vm.fi
Taitto: Taina Ståhl ja Pirkko Ala-Marttila

ISSN 1455- 2566
ISBN 978-951-804-892-6 (nid)
ISBN 978-951-804-893-3 (pdf)

Edita Prima Oy
Helsinki 2008

Esipuhe

Valtiovarainministeriö (VM) vastaa julkishallinnon tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTIssa käsitellään kaikki merkittävät valtionhallinnon tietoturvalinjaukset ja tietoturvatoimenpiteiden ohjausasiat. VAHTI käsittelee valtion-hallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTIn käsittelyn kohteina ovat kaikki tietoturvallisuuden osa-alueet.

VAHTIn toiminnalla on parannettu valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainväli-sesti. Tuloksena on aikaansaatu erittäin kattava yleinen tietoturvaohjeisto (www.vm.fi/VAHTI). Valtiovarainministeriön ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita.

VAHTI on valmistellut, ohjannut ja toteuttanut valtion tietoturvallisuuden kehitysohjelman, jossa on aikaansaatu merkittävää kehitystyötä yhteensä 26 kehityskohteessa yli 300 hankkeisiin nimetyn henkilön toimesta. VAHTI edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä. Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynne-tään laajasti myös kunnallishallinnossa, yksityisellä sektorilla, kansalaistoiminnassa ja kansainvälisessä yhteistyössä. VAHTI on saanut kolmena perättäisenä vuotena tunnustuspalkinnon esimerkillisestä toiminnasta Suomen tietoturvallisuuden parantamisessa.

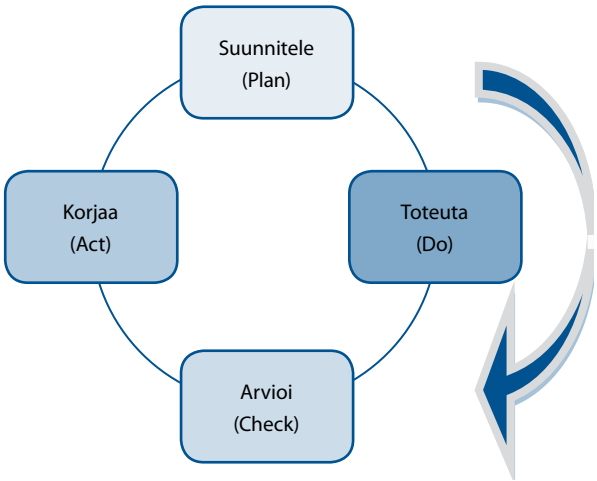
Tämän selvityksen on laatinut VAHTIn alainen julkishallinnon tietoturvakoulutustarpeet-työryhmä. Selvitys on käsitelty VAHTI-johtoryhmän kokouksessa lokakuussa 2008

Tiivistelmä

Julkishallinnossa otetaan käyttöön jatkuvasti uusia tietojärjestelmiä ja sähköisiä palveluita. Niiden käyttöönotto edellyttää työtehtävien ja toimintaprosessien uudistamista. Uudet teknologiat mahdollistavat myös entistä tehokkaampia ajasta ja paikasta riippumattomia etätyöskentelymahdollisuuksia. Organisaation tietoturvallisuus joutuu uusien haasteiden eteen.

Eräs organisaation johdon tärkeimpiä tietoturva-asennetta ja –ilmapiiriä muovaavia toimenpiteitä on kattavan tietoturvakoulutuksen ja -ohjeistuksen järjestäminen. Säännöllinen, muutostarpeet huomioiva organisaation henkilöstön kattava tietoturvakoulutus on tarvittavan tietoturvaosaamisen rakentamisen ja ylläpitämisen perusedellytyksiä.

Kuva 1. Tietoturvakoulutuksen, kuten muunkin tietoturvatyön kehittämisen tulee olla jatkuva prosessi PDCA-syklin mukaisesti.



Tietoturvaohjeistuksen ja -koulutuksen sisältöä tulee päivittää säännöllisesti vastaamaan käyttöönotettavia uusia mahdollisuuksia, haasteita ja uhkakuvia sekä palveluita.

Organisaatiosta löytyy useita työtehtäviä tai -rooleja, jotka edellyttävät syventävää tietoturvakoulutusta. Tällaisia kohderyhmiä ovat organisaation johto, esimiehet sekä ICT- ja turvallisuus-henkilöstö. Myös muu organisaation henkilöstö, joka joutuu käsittelemään työtehtävissään erityissuojattavia, ts. salassa pidettäviä tietoaineistoja, tarvitsee lisäkoulutusta. Organisaation omien työntekijöiden ohella toimintaverkoston henkilöstö, joka toimii esimerkiksi organisaation yhteistyökumppaneina tai palveluntuottajina, pitää sisällyttää tietoturvakoulutuksen kohderyhmäksi.

Tietoturvakoulutukseen liittyviä haasteita ovat:

- miten tietoturvaohjeistus ja -koulutus voidaan toteuttaa sellaisella tavalla, että käyttäjien mielenkiinto päivittyviin materiaaleihin säilyy?
- ohjeiden helppo saatavuus ja luettavuus
- miten käyttäjät saadaan motivoitua osallistumaan tietoturvakoulutuksiin, jotka toistuvat säännöllisesti?
- miten tietoturva-asennetta ja -kulttuuria voidaan kehittää?

Uudet sähköiset oppimisympäristöt ja multimedia-muotoiset oppimateriaalit mahdollistavat vuorovaikutteisemman koulutuskokemuksen.

Koulutusten tasoa, asioiden omaksumista ja koulutuksiin osallistumista tulee arvioida säännöllisesti ja ryhtyä tarvittaviin korjaustoimenpiteisiin.

Tietoturvakoulutuksen toteuttaminen itse tai ulkopuolelta ostaminen edellyttää riittäviä resursseja. Syventävän tietoturvakoulutuksen järjestämiseksi kannattaa selvittää yhteistyömahdollisuudet muiden organisaatioiden kanssa.

Kuva 2. Tietoturvakoulutus koostuu perus- ja syventävän koulutuksen ohella myös sovellus- ja työtehtäväkohtaisesta koulutuksesta. Koulutuksen tehokkuuteen ja omaksumiseen vaikuttaa organisaatiossa vallitseva asenne ja ilmapiiri tietoturvallisuutta kohtaan.

Tietoturvatasojen on suunniteltu astuvan voimaan vuoden 2011 alusta. Tietoturvatasoissa määritetään tietoturvakoulutusta koskevat vaatimukset ”Osaamisen ja tietoisuuden kehittäminen ja sanktiot” osa-alueella. Tässä selvityksessä ja jatkotoimenpide-ehdotuksissa on huomioitu tietoturvatasojen valmistelussa esille nostetut asiat.

Organisaation ylin johto ja esimiehet toimivat omalla esimerkillään esikuvana tietoturvallisuuden kehittämisessä. Tietoturvakulttuuri, asenne ja motivointi tietoturvallisuuteen alkavat johdosta. Johdon sitoutuminen tietoturvallisuuden kehittämiseen ja tietoturvakoulutukseen toimii hyvänä mallina muulle organisaatiolle.

Tietoturvallisuuden johtamista ei voi ulkoistaa. Jokaisen organisaation tulee itse huolehtia tarkoituksenmukaisten hallinnollisten ja teknisten tietoturvaratkaisujen käyttöönotosta ja ylläpidosta.

Selvityksessä korostetaan seuraavia tietoturvakoulutuksessa huomioitavia seikkoja:

- Kehitä tietoturvakulttuuria – tee tietoturvallisuudesta asenne!
- Yhdistä tietoturvallisuus prosesseihin.
- Varaudu tietoturvatasoihin.
- Mitoita tietoturvallisuus oikein - yhdistä tietoturvallisuus helppokäyttöisyyteen.
- Hyödynnä uutta teknologiaa tietoturvakulttuurin kehittämisessä.
- Motivoi oppilaat ja konkretisoi tietoturvauhat.
- Sitouta johto ja esimiehet osallistumaan koulutuksiin.
- Tee tietoturvaohjeet helposti omaksuttaviksi.
- Järjestä koulutusta toistuvasti ja seuraa sen vaikuttavuutta.
- Hyödynnä VAHTI-ohjeistoa koulutuksessa.

Tämän selvityksen ehdotukset painottuvat tietoturvakulttuurin edistämiseen ja sähköisten palveluiden kehittämiseen.

Tietoturvakulttuuria edistävät toimenpiteet

- Kehitetään johdon, esimiesten ja prosessinomistajien tietoturvatietoisuutta.
- Resursoidaan tietoturvakoulutukseen riittävästi.
- Selvitetään tietoturvakoulutuksen vaikuttavuus.
- ”Kilpaillaan” tietoturvasta.

Sähköiset palvelut

- Kehitetään julkishallinnon yhteinen tietoturvallisuuden oppimisalusta.
- Tuotetaan kaikille yhteinen, säännöllisesti päivittyvä VAHTI- perusohje.

- Tuotetaan ”Hauskat tietoturvavideot” -video-ohjeet / opasteanimaatiot .
- Tuotetaan ”Päivän tietoturvamietelause”-palvelu.
- Rakennetaan tietoturvamateriaalipankki.

Muut kehittämisideat

- Kehitetään julkishallinnon tietoturva-ajokortti.
- Laaditaan tietoturvallisuuden koulutusohjelma turvallisuus-henkilöstölle.
- Lisätään tietoturvallisuus osaksi kehityskeskusteluita ja osaamisvaatimuksia.
- Tuotetaan Tietoturvallisuus on asenne –julistesarja.
- Toteutetaan julkishallinnon yhteinen ICT-koulutuskalenteri.

Sisältö

1 Tausta ja tavoite

1.1 Selvityksen virallinen tausta

Selvitys on osa valtiovarainministeriön Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) vuodelle 2008 asetettuja tavoitteita. Selvityksen pohjalta VM ja VAHTI voivat tehdä tarkempia esityksiä ja hankkeita julkishallinnon tietoturvakoulutuksen kehittämiseksi tulevina vuosina 2009-2010.

Työryhmän jäsenet

Björklund, Eeva	Ilmailulaitos Finavia, puheenjohtaja
Ahjokannas, Tuomo	valtiovarainministeriö
Aro, Jyri-Petteri	Maanpuolustuskorkeakoulu
Hatakka, Heidi	ulkoasiainministeriö
Joki, Jyri	Verohallinto
Jokinen, Olli	Maanmittauslaitos
Karlqvist, Harry	Teknologian kehittämiskeskus
Kivilompolo, Mika	Helsingin yliopisto
Korhonen, Seija	valtiovarainministeriö
Mäkinen, Riitta	Helsingin kaupunki
Palmunoksa, Jaana	Ilmatieteen laitos
Kimmo Rousku	konsultti, Norbu Oy

1.2 Selvityksen tavoitteet

Selvityksen tarkoituksena on kartoittaa julkishallinnon tietoturvakoulutustarpeita ja valmistella ehdotuksia ja kuvauksia tietoturvakoulutuksen toimenpiteiksi ja kehityskohteiksi.

Selvityksessä on otettava huomioon koulutuksen kohdentaminen eri henkilöryhmille sekä valtionhallinnon, hallinnonalojen ja organisaatiotasojen tarpeet ja yhteistyömahdollisuudet.

2 Johdanto

Tietoturvallisuuden merkitys julkishallinnossa on kasvanut voimakkaasti, tietoaineistojen ja palveluiden sähköistyessä. Muutos edellyttää ajantasaista ohjeistusta ja koulutusta. Uusien ICT-teknologioiden tarjoamat käyttömahdollisuudet ja uudet tietoturvauhat korostavat ohjeistuksen ja koulutuksen säännöllisyyden merkitystä.

Organisaation ylimmän johdon tehtävä on huolehtia siitä, että tietoturvakoulutuksessa huomioidaan seuraavat seikat:

- riittävä resursointi
- toiminnan tarpeiden vastaavuus
- säännöllisyys
- koko henkilöstön kattavuus
- perillemenon seuranta ja varmistaminen.

Organisaation johto ja esimiehet toimivat suunnan näyttäjinä ja esimerkkinä tietoturvakulttuurin kehittämisessä. Tällä on vaikutusta myös esimiesten mahdollisuuksiin motivoida ja innostaa työntekijöitä kehittämään omaa tietoturvaosaamista. Tietoturvallisuus tulee olla osa hyvin toteutettua organisaation johtamiskulttuuria.

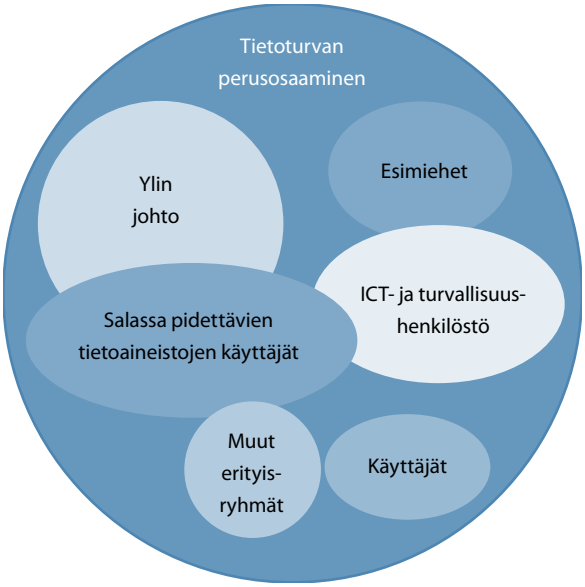
Tehtävissä, joissa edellytetään tietoturvallisuuden huomioimista, tietoturvallisuuden ei pidä olla erillinen osa-alue, vaan sen pitää sisältyä työvaiheisiin ja -prosesseihin oletuksena. Tämän johdosta tietoturvallisuuden kouluttaminen on haastavaa; kaikkien tulee tietää tietoturvallisuuden perusteet, mutta syvemmän osaamisen tarve vaihtelee työtehtävittäin. Nykymuotoisessa tietoturvakoulutuksessa tähän ei ole kiinnitetty riittävästi huomiota, ja koulutus on tällöin painottunut tietoturvallisuuden perusteisiin. Koulutusta voidaan kehittää tuomalla tietoturva-asiat konkreettisten esimerkkien avulla jokapäiväisiin työtehtäviin ja sisällyttämällä tietoturva työtehtäviin, -prosesseihin ja työnkuviin.

Tietoturvakoulutuksessa ja -ohjeistuksissa yleisenä ongelmana voidaan pitää sitä, ettei koulutus tavoita kaikkia työntekijöitä (kattavuus). Koulutusta ei tarjota kaikille tai kaikkien työntekijöiden ei edellytetä osallistuvan koulutukseen. Ongelmallista on myös, jos organisaation tietoturvaohjeistusta ei lueta ja/tai ohjeistusta ei noudateta. Toteutetun tietoturvakoulutuksen mittaaminen ja vaikuttavuuden arvioiminen on myös koettu vaikeaksi.

Selvitykseen on koottu esimerkkejä ja ehdotuksia siitä, millä edellytyksillä ja toimenpiteillä tietoturvakoulutuksen onnistuminen voidaan varmistaa.

Selvityksessä nostetaan esille ne kohderyhmät, joita varten tarvitaan räätälöityä koulutusta ja tietoturvaohjeistusta. Tämän ohella ehdotetaan uusia vaihtoehtoisia tapoja tuottaa koulutusta ja koulutusmateriaalia.

Kuva 3. Kaikkien käyttäjien tarvitseman peruskoulutuksen lisäksi tarvitaan syventävää tietoturvakoulutusta erityisryhmille.

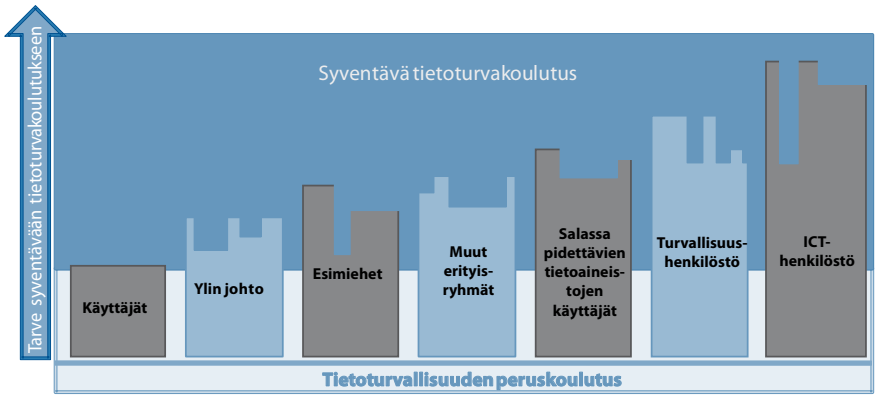


Kaikki käyttäjät tarvitsevat **tietoturvan perusosaamista**. Lisäksi on useita erityisryhmiä, joille tulee järjestää **syventävää** tietoturvakoulutusta (Kuva 4). Julkishallinnon työntekijöistä suurin osa käsittelee myös erilaatuisia salassa pidettäviä tietoaineistoja. Tietoturvakoulutustarpeet on otettava huomioon myös rekrytoinnissa ja vuosittaisissa kehityskeskusteluissa (Kuva 5).

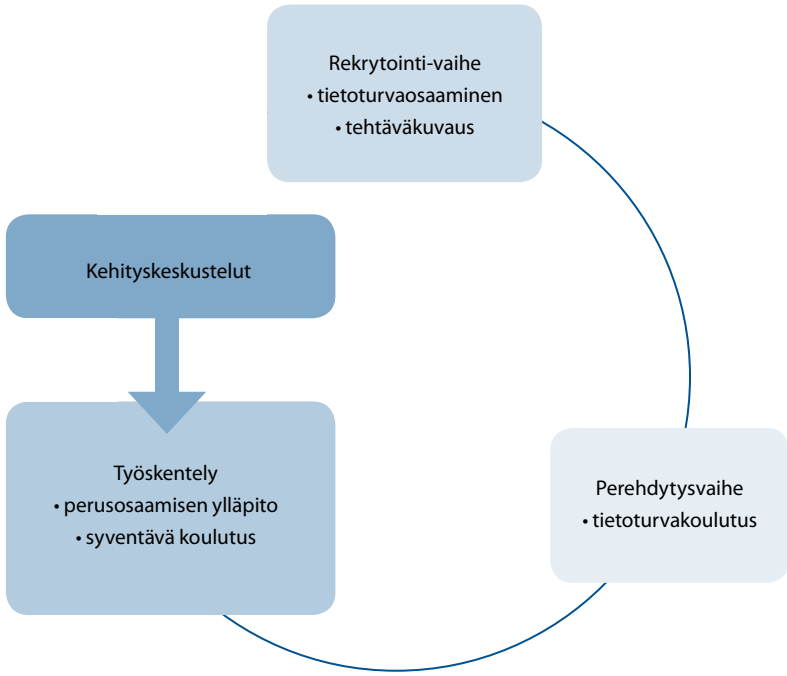
Henkilöllä voi olla useita rooleja ICT- ja tietoturvatehtävistä riippuen. Esimerkiksi organisaation **tietoturvajohtaja ja tietohallintojohtaja** voivat olla johtoryhmän jäseniä ja osa ylintä johtoa, toimia esimiehinä ja ICT- ja turvallisuushenkilöinä ja käsittelevät siksi työssään salassa pidettäviä tietoaineistoja.

Organisaation **IT-tukihenkilö** kuuluu ICT- ja turvallisuushenkilöstöön, joka käsittelee työssään salassa pidettäviä tietoaineistoja. **Henkilölle**, joka käsittelee - edes satunnaisesti – salassa pidettäviä tietoaineistoja, tulee järjestää syventävää tietoaineistojen käsittelyä koskevaa tietoturvakoulutusta.

Kuva 4. Syventävän tietoturvallisuuden koulutuksen tarve ja määrä riippuu käyttäjän rooleista.



Kuva 5. Tietoturvakoulutuksen määrän ja tarpeen arviointi sekä seuranta tulee sisällyttää osaksi henkilön työuraa.



3 Tietoturvakoulutuksen kohderyhmät

Tietoturvakoulutuksella on useita kohderyhmiä. Peruskohderyhmä on organisaation koko henkilöstö. Muiden tässä selvityksessä tunnistettujen kohderyhmien koulutuksen laajuuden tulee perustua sen tehtävistä johdettuihin koulutustarpeisiin.

3.1 Organisaation koko henkilöstö - peruskoulutus

Tietoturvakoulutuksen peruskohderyhmä on organisaation koko henkilöstö. Sitä varten tarvitaan kattava, organisaation toimintatarpeista liikkeelle lähtevä peruskoulutus tarvittavine ohjeistuksineen.

Peruskoulutus tulee toteuttaa moduuleina. Työntekijöiden ei tarvitse silloin yrittää kerralla sisäistää kaikkea tarvittavaa tietoa. Peruskoulutus tulee sovittaa yhteen syventävää osaamista vaativan koulutuksen kanssa siten, että osaamista voi syventää myös peruskoulutuksen aikana.

Peruskoulutusta tulee järjestää myös määräaikaiselle ja muulle tilapäiselle henkilöstölle, kuten esimerkiksi harjoittelijoille ja siviilipalvelusmiehille.

Uusien työntekijöiden perehdyttämiseen liittyvä tietoturvakoulutus on erittäin tärkeää. On huolehdittava siitä, että uudet henkilöt osallistuvat ensimmäiseen mahdolliseen tietoturvakoulutukseen. Perehdyttämiskoulutuksen yhteydessä heille voidaan järjestää tiivistetty tietoisku tarvittavasta tietoturvaosaamisesta.

Organisaation yleisen tietoturvaohjeiston tulee kuulua automaattisesti jokaisen uuden henkilön perehdyttämismateriaaliin.

3.2 Erityisryhmät – syventävä koulutus

Kattavan peruskoulutuksen ohella syventävää tietoturvakoulutusta (”tietoturvan jatkokoulutus”) tarvitsevat seuraavat seitsemän kohderyhmää:

- Ylin johto
- Esimiehet
- Muut erityisryhmät
- Salassa pidettävien tietoaineistojen käyttäjät
- Turvallisuus-henkilöstö
- ICT-henkilöstö
- Toimintaverkosto

Organisaation omien työntekijöiden ohella toimintaverkoston henkilöstö, joka toimii esimerkiksi organisaation yhteistyökumppaneina tai palveluntuottajina, pitää sisällyttää tietoturvakoulutuksen kohderyhmäksi. Toimintaverkoston tietoturvakoulutustason tulee vastata vähintään heidän tarjoamiensa palveluiden edellyttämää tietoturvatasoa.

4 Tietoturvakoulutuksen nykytila

4.1 Osaamisen nykytila

Tietoturvakoulutuksen toteutustavoissa ja laajuudessa sekä tietoturva-asenteissa ja -kulttuurissa on merkittäviä eroja organisaatioiden välillä. On oletettavaa, että tulevat julkishallintoon rekrytoitavat uudet henkilöt omaavat entistä paremmat valmiudet ja tietoturvallisuuden perusosaamisen. Tämän mahdollistaa osittain opiskeluihin kuuluva tietoturvakoulutus sekä yleinen ICT-käyttötaitojen kehittyminen. Todennäköisesti tulevien sukupolvien tietoturvakoulutuksessa tulevat korostumaan teknisen osaamisen sijaan tietoturva-asenteeseen ja yksityisyydensuojan huomioimiseen liittyvät asiat.

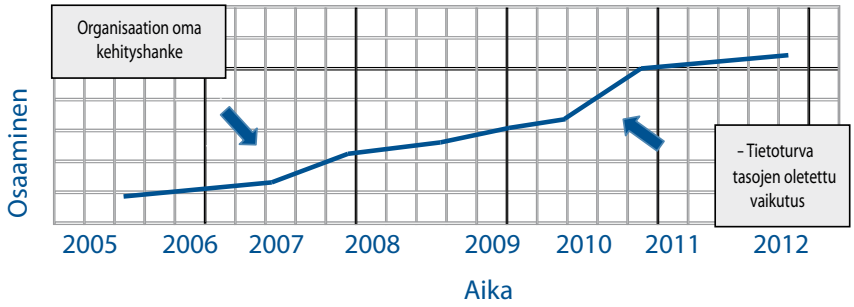
Tietoturvakoulutuksen ja tietoturvaosaamisen nykytilaan vaikuttavat:

- 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.

Edellä lueteltujen seikkojen takia esiintyy sekä hallinnonala että aluekohtaisia eroja.

Valtiovariaiministeriön tietoturvahankkeet edistävät osaltaan tietoturvaosaamista. Kehitystä tapahtunee erityisesti niissä organisaatioissa, joissa tietoturvallisuuden kehittämiseen suunnatut resurssit ovat olleet rajalliset tai tietoturvakulttuurin kehittämiseen ei ole huomattu panostaa riittävästi. Tietoturvallisuuden kehittämisen tulee olla jatkuvaa ja pohjautua organisaation ylimmän johdon hyväksymään toimintasuunnitelmaan.

Kuva 6. Organisaation tietoturvaosaamiseen vaikuttavia seikkoja ovat olleet esimerkiksi toteutetut kehityshankkeet. Tulevaisuudessa tietoturvatasojen voidaan olettaa tuovan piristysruiskeen tietoturvakoulutukseen ja osaamiseen.



4.2 Peruskoulutuksen nykytila

Julkishallinnossa järjestettyjen tietoturvakyselyiden perustella voidaan todeta, että valtaosa käyttäjistä saa mielestään riittävästi tietoturvakoulutusta ja -ohjeistusta. Siitä huolimatta osa käyttäjistä ei noudata tietoturvaohjeita (Liite 1).

Yleinen ongelma organisaatioissa on ohjeiden päivittämättömyys. Ohjeistuksia on syytä päivittää, koska uusia mahdollisuuksia, haasteita ja uhkakuvia sekä teknologioita tulee käyttöön tihenevään tahtiin. Joissain organisaatioissa ongelmia on tuottanut muun kuin suomenkielisen tietoturvamateriaalin ja -koulutuksen tuottaminen.

Perinteisten koulutusten ja ohjeiden rinnalle ovat nousseet multimedia- ja oppimisympäristöissä toteutetut koulutukset ja oppimateriaalit. Näiden käyttöönottoa toivotaan laajennettavan, koska ne tarjoavat mahdollisuuden peruskoulutuksen ohella syventävän koulutuksen järjestämiseen.

4.3 Syventävän koulutuksen nykytila

Syventävän koulutuksen (ns. ”jatkokoulutus”) osalta ongelmana on, että edellisessä luvussa kuvatuille erityisryhmille on saatavilla niukasti sopivaa koulutusta tai koulutusmateriaalia.

Syventävän koulutuksen osalta paras tilanne on tietoturva- ja ICT-henkilöstöllä. Sille on saatavilla niin teknistä toimittajariippuvaista kuin myös yleisempää tietoturvasertifiointeihin johtavaa koulutusta.

5 Työryhmän ehdotukset

5.1 Tietoturvakoulutuksen kehittäminen

Tässä osassa esitellään seikkoja, joiden avulla voidaan varmistaa tietoturvakoulutusten onnistuminen sekä tuodaan esille hyviä käytäntöjä, joilla koulutuksen vaikuttavuutta voidaan lisätä.

Tietoturvakoulutuksessa huomioitavia seikkoja:

- Kehitä tietoturvakulttuuria – tee tietoturvallisuudesta asenne!
- Yhdistä tietoturvallisuus prosesseihin.
- Varaudu tietoturvatasoihin.
- Mitoita tietoturvallisuus oikein - yhdistä tietoturvallisuus helppokäyttöisyyteen.
- Hyödynnä uutta teknologiaa tietoturvakulttuurin kehittämisessä.
- Motivoi oppilaat ja konkretisoi tietoturvauhat.
- Sitouta johto ja esimiehet osallistumaan koulutuksiin.
- Tee tietoturvaohjeet helposti omaksuttaviksi.
- Järjestä koulutusta toistuvasti ja seuraa sen vaikuttavuutta.
- Hyödynnä VAHTI-ohjeistoa koulutuksessa.

5.1.1 Kehitä tietoturvakulttuuria – tee tietoturvallisuudesta asenne!	
Kohderyhmä	Organisaation johto ja esimiehet, prosessien omistajat Turvallisuushenkilöstö
Vaikuttavuus	Koko henkilöstö

Tietoturvakulttuurista vastaa koko henkilöstö. Esimiesten tehtävä tietoturvallisuuden edistämisessä helpottuu, kun johto osallistuu aktiivisesti tietoturvallisuuden kehittämiseen ja tietoturvakoulutuksiin.

5.1.2 Yhdistä tietoturvallisuus prosesseihin	
Kohderyhmä	Organisaation johto ja esimiehet, prosessien omistajat Turvallisuushenkilöstö
Vaikuttavuus	Koko henkilöstö Toimintaverkosto

Tietoturvallisuuden tulee olla osa organisaation prosessimallia/prosessikarttaa, ja se tulee sisällyttää osaksi työntekijöiden tehtäväkuvauksia ja kehityskeskusteluja. Tällöin tietoturvallisuus ei ole työtehtävistä irrallinen tai erikseen muistettava seikka, vaan siitä tulee luontainen prosessin osa. Kun prosessia kehitetään ja arvioidaan, tietoturvallisuus tulee samalla automaattisesti huomioitua. Prosessien taustalla toimivalla teknisellä valvonnalla voidaan yrittää pienentää tietoturvallisuudesta piittaamattomien käyttäjien aiheuttamaa riskiä.

Prosessinomaisesti toteutettua riskienhallintaa käytetään keskeisenä tietoturvan seuranta- ja kehittämisvälineenä.

5.1.3 Varaudu tietoturvatasoihin	
Kohderyhmä	Organisaation johto Turvallisuushenkilöstö
Vaikuttavuus	Koko henkilöstö Toimintaverkosto

Tietoturvatasot tulee huomioida tulevina vuosina tietoturvakoulutuksen kehittämisessä. Etenkin syventävä tietoturvakoulutus tulee suunnitella siten, että siinä huomioidaan organisaation toiminnoilleen asettamat tietoturvatasot. Jos esimerkiksi salassa pidettävien tietoaineistojen käsittelylle on asetettu erityistasovaatimus, tietoturvakoulutuksessa ja koulutusmateriaaleissa on vastaavasti huomioitava ko. korkein taso.

Kaikkien organisaatioiden tulee saavuttaa vähintään perustaso, joten sen tulee olla siksi myös tietoturvakoulutuksen peruskoulutuksen lähtötaso. Niillä osa-alueilla, joilla tarvitaan korkeampaa tasoa, voidaan peruskoulutustasoa vastaavasti nostaa tai järjestää tarvittava koulutus syventävän tietoturvakoulutuksen yhteydessä.

5.1.4 Mitoita tietoturva oikein – yhdistä tietoturvallisuus helppokäyttöisyyteen	
Kohderyhmä	Organisaation johto Turvallisuushenkilöstö Tietojärjestelmien omistajat ICT-henkilöstö
Vaikuttavuus	Koko henkilöstö Toimintaverkosto Ulkoiset asiakkaat

Tietoturvallisuus koetaan usein tietojärjestelmien ja ICT-tekniikan helppokäyttöisyyttä heikentävänä tekijänä.

ICT-toimintaan liittyvät riskit tulee mallintaa riskienhallinta-prosessin avulla. Riskien pienentämiseen liittyvät niin hallinnolliset kuin tekniset toimenpiteet tulee sovittaa sellaiselle tasolle, jolla tietoturvallisuus on riittävä helppokäyttöisyyttä unohtamatta.

Liikemaailmasta tuttua ilmausta ”Raha on hyvä konsultti” voidaan soveltaa myös tietoturva-asioissa. Muuttamalla se muotoon ”Tietoturva on hyvä konsultti” voidaan paremmin ymmärtää se tosiasia, että tietoturvatason heikennys voi tulla kalliiksi.

5.1.5 Hyödynnä uutta teknologiaa tietoturvakulttuurin kehittämisessä	
Kohderyhmä	Turvallisuushenkilöstö ICT-henkilöstö
Vaikuttavuus	Koko henkilöstö

Uuden ICT-teknologian käyttöönotto vaikuttaa kaksitahoisesti tietoturvakoulutukseen. Uusi teknologia aiheuttaa lisää työtä ja edellyttää uudenlaista koulutusta ja ohjeistusta. Toisaalta tällaisessa tilanteessa organisaation on mahdollista uudistaa ja järkevöittää toimintaprosessejaan.

Esimerkkejä:

- Nykyaikana ei tarvitse erikseen skannata virusten varalta levykeasemaan asetettavaa ”korppua”, koska niitä ei käytetä ja taustalla toimivat haittaohjelmien torjuntajärjestelmät tekevät tämän tarkastuksen automaattisesti.

- Korppujen tilalle on tullut uutena tallennusmediana usb- ja muut ulkoiset, siirrettävät apumuistit. Miten nämä on huomioitu ICT- ja tietoturvakoulutuksissa? Onko käyttäjiä ohjeistettu käyttämään apumuisteja tietoturvallisesti?

5.1.6 Motivoi oppilaat ja konkretisoi tietoturvauhat	
Kohderyhmä	Tietoturvakouluttajat Koulutusmateriaalia laativat henkilöt Turvallisuushenkilöstö
Vaikuttavuus	Koko henkilöstö

Motivoitunut opiskelija on paras oppija. Pyri esittämään koulutuksissa ja ohjeistuksissa sekä noudatettaviksi määrätyt että kielletyt asiat esimerkkien ja perusteluiden avulla. Tällöin opiskelija ymmärtää ne syyt, miksi jokin asia pitää toteuttaa koulutuksessa ja ohjeistuksessa määrätyllä tavalla.

Tietoturvaohjeistuksen ei tarvitse olla laaja, kerralla opittavaksi tarkoitettu kokonaisuus, vaan se voidaan pilkkoa pienemmiksi kokonaisuuksiksi vastaamaan henkilön työtehtäviä ja prosessikohtaisia ohjeita.

Esimerkkejä:

- Miten koulutuksissa ja ohjeistuksissa on henkilöstöä opastettu käyttämään internetiä? Sen sijaan että kirjallisessa, tiivistetyssä ohjeessa lukee pelkästään ”Henkilö saa käyttää internet-selainta vain omien työtehtävien hoitamisen lisäksi pankkiasiointiin”, henkilöstölle tulee asian omaksumisen vuoksi osoittaa koulutuksissa millainen selaimen käyttö on vaarallista ja miksi.

- Esimerkiksi ”Henkilö päätyy holtittoman nettiselaimen käytön perusteella sellaiselle www-sivulle, jolta hänen tietokoneeseen yritetään upottaa vaarallinen vakoiluohjelma. Varomattomalla toiminnallaan hän altistaa oman yksityisyydensuojan ohella organisaation tietoaineistot ulkopuoliselle tietomurtautujalle. Vältä turhaa selaimen käyttöä! Ole erityisen varovainen avatessasi sähköpostiviesteissä olevia linkkejä, sillä niiden avulla tietomurtautuja yrittää houkutella käyttäjiä huijaus-www-sivuille. Tietomurtautuja lupaa sinulle vaikka kuun taivaalta saadakseen sinut sivuilleen.”

5.1.7 Sitouta johto ja esimiehet osallistumaan koulutuksiin	
Kohderyhmä	Organisaation johto ja esimiehet Turvallisuushenkilöstö
Vaikuttavuus	Koko henkilöstö

Tietoturvakulttuuriin vaikuttaa merkittävästi organisaation ylimmän johdon sitoutuminen tietoturvan kehittämiseen. Johto vaikuttaa omalla esimerkillään työntekijöiden asenteeseen tietoturvallisuutta kohtaan. Tietoturvan kehittämiseen sitoutunut johto helpottaa esimiesten työtä tietoturvallisuuden ylläpitämisessä ja kehittämisessä.

Esimerkkejä:

- Ovatko johtoryhmän jäsenet osallistuneet tietoturvakoulutukseen? Kantavatko organisaation johtoryhmän jäsenet henkilökorttia samalla tavalla kuin muu henkilöstö? Miten esimiehet varmistuvat omasta ja alaisten riittävästä tietoturvaosaamisesta? Kuinka he ovat selvillä siitä, millaisia tietojärjestelmiä ja –aineistoja alaiset käsittelevät?

- Onko johdon ja esimiesten sitoutumiseen tietoturvallisuuteen laadittu mittareita?

5.1.8 Tee tietoturvaohjeet helposti omaksuttaviksi	
Kohderyhmä	Tietoturvakouluttajat Turvallisuushenkilöstö
Vaikuttavuus	Koko henkilöstö

Tietoturvakoulutus edellyttää huolella suunniteltua koulutustilannetta, jotta se koetaan onnistuneeksi. Kouluttajan tulee huolehtia opetettavan asian ja käytettävän terminologian selkeästä esitystavasta ja tutustuttaa koulutettavat ko. materiaaliin ja terminologiaan. ICT- ja tietoturvahenkilöstö voi keskenään puhua erikoistermeillä ja lyhenteillä. Koulutus- ja asiakaspalvelutilanteissa heidän pitää osata sovittaa esitystapa asiakkaan ymmärtämään muotoon.

Esimerkkejä:

- Onko tietoturvakoulutusmateriaaleissa käytetyt lyhenteet ja ammattitermit selostettu ymmärrettävästi? Onko kouluttaja opastanut koulutettavia oppimateriaalin käyttöön ja terminologiaan koulutuksen alusta pitäen?

- Onko ohjeissa huomioitu:
  - helppolukuisuus
  - ohjeiden saatavuus ja löydettävyys
  - ajantasaisuus
  - luettavuus – ”lyhyestä virsi kaunis”

5.1.9 Järjestä koulutusta toistuvasti ja seuraa sen vaikuttavuutta	
Kohderyhmä	Turvallisuushenkilöstö Tietoturvakouluttajat
Vaikuttavuus	Johto ja esimiehet Koko henkilöstö

Tietoturvakoulutusta tulee järjestää säännöllisesti eikä esimerkiksi pelkästään ohjeiden päivittyessä. Mikäli kouluttajia on useampia, koulutuskokonaisuus tulee toteuttaa siten, että koulutukset ovat samansisältöisiä. Ohjeita tulee tarkistaa säännöllisesti ja päivittää aina kun uudet teknologiaratkaisut tai mahdolliset uhat sitä edellyttävät.

Organisaation ja alihankkijoiden henkilöstön tulee osallistua tietoturvakoulutukseen säännöllisesti. Joissakin organisaatioissa tähän koulutukseen osallistuminen on sidottu osaksi kehityskeskusteluita tai tietojärjestelmien käyttöoikeuksien myöntämismenettelyä. Koulutuksen vaikuttavuutta tulee seurata ja esim. palautekyselyijen ja itsearvioinnin avulla.

Esimerkkejä:

- Miten organisaatiossa voidaan tarkistaa, milloin henkilö on viimeksi osallistunut tietoturvakoulutukseen? Miten organisaatiossa voidaan varmistua siitä, että annettu koulutus on saavuttanut sille asetetut tavoitteet?

- Onko koulutuksissa huomioitu:
  - riittävän konkreettiset ja helposti ymmärrettävät esimerkit
  - esimerkkien sijoittaminen koulutettavien työtehtäviin

5.1.10 Hyödynnä VAHTI-ohjeistoa koulutuksessa	
Kohderyhmä	Turvallisuushenkilöstö Tietoturvakouluttajat
Vaikuttavuus	Johto ja esimiehet Koko henkilöstö

VAHTI on tuottanut kattavan, kansainvälisesti arvostetun materiaalikokonaisuuden tietoturvallisuuden eri osa-alueille. Organisaatioiden tulee noudattaa näitä asiakirjoja omien hallinnollisten asiakirjojen ja teknisten tietoturvaratkaisujen toteuttamisessa. Tietoturvakoulutusta voidaan kehittää Tietoturvakouluttajan opas, VAHTI 11/2006 –julkaisussa esitetyillä tavoilla.

5.2 Ehdotuksia tietoturvakoulutusta edistäviksi toimenpiteiksi

Työryhmä on jakanut toimenpide-ehdotukset kolmeen eri aihepiiriin:

Tietoturvakulttuuria edistävät toimenpiteet

- Kehitetään johdon, esimiesten ja prosessinomistajien tietoturvatietoisuutta.
- Resursoidaan tietoturvakoulutukseen riittävästi.
- Selvitetään tietoturvakoulutuksen vaikuttavuus.
- ”Kilpaillaan” tietoturvasta.

Sähköiset palvelut

- Kehitetään julkishallinnon yhteinen tietoturvallisuuden oppimisalusta.
- Tuotetaan kaikille yhteinen, säännöllisesti päivittyvä perusohje.
- Tuotetaan ”Hauskat tietoturvavideot” –video-ohjeet / opasteanimaatiot.
- Tuotetaan ”Päivän tietoturvamietelause”-palvelu.
- Rakennetaan tietoturvamateriaalipankki.

Muut kehittämisideat

- Kehitetään julkishallinnon tietoturva-ajokortti.
- Laaditaan tietoturvallisuuden koulutusohjelma turvallisuushenkilöstölle.
- Lisätään tietoturvallisuus osaksi kehityskeskusteluita ja osaamisvaatimuksia.
- Tuotetaan Tietoturvallisuus on asenne –julistesarja.
- Toteutetaan julkishallinnon yhteinen ICT-koulutuskalenteri.

5.2.1 Tietoturvakulttuuria edistävät toimenpiteet

Kehitetään johdon, esimiesten ja prosessinomistajien tietoturvatietoisuutta	
Kohderyhmä	Johto Esimiehet Prosessinomistajat
Vaikuttavuus	Koko henkilöstö
Toteutuksen ohjaus	VAHTI
Toteuttaja	Kunkin organisaation johto ja tietoturvahenkilöstö

Organisaation tietoturvallisuuden kehittämiseen vaikuttaa organisaation johdon ja esimiesten tietoturvatuntemus ja sitoutuminen tietoturvan kehittämiseen. Tämän takia heille tulee rakentaa tiivis, erityisesti heidän tarpeisiin räätälöity koulutuskokonaisuus, jossa nostetaan esille:

- riskienhallinnan ja prosessikartan tärkeys
- konkretisoituneet tietoturva-uhat
- selkeä kokonaiskuva tietoturvallisuuden osa-alueista johdon ja esimiesten näkökulmasta tarkasteltuna
- ne edellytykset, joita nykyaikainen tietoturvallisuuden hallintajärjestelmä edellyttää voidakseen olla toimiva.

Samaa koulutuskokonaisuutta voidaan hyödyntää sopivasti räätälöitynä myös prosessinomistajien tietoturvatietoisuuden kasvattamisessa niiltä osin, joissa omistaja ei muuten kuulu tähän ryhmään. Samaa sähköistä koulutusjärjestelmää voidaan hyödyntää myös muiden koulutusten tuotantojärjestelmänä

Resursoidaan tietoturvakoulutukseen riittävästi	
Kohderyhmä	Johto Esimiehet Tietoturvahenkilöstö
Vaikuttavuus	Koko henkilöstö
Toteutuksen ohjaus	Valtioneuvosto ja VM
Toteuttaja	Kukin organisaatio ja sen ylin johto

Tietoturvallisuuden kehittäminen vaatii henkilöresurssien ohella taloudellisia resursseja. Pienemmissä organisaatioissa tietoturvallisuuden ylläpitämiseen ja kehittämiseen varatut resurssit ovat yleensä rajalliset, jolloin priorisoitaessa työtehtäviä saattaa tietoturvakoulutuksen asema kärsiä.

Tämän johdosta kaikki ne keinot, joilla voidaan kehittää itseopiskelumahdollisuuksia sekä hyödyntää multimedia-pohjaisia oppimateriaaleja, hyödyttävät varsinkin pienempien organisaatioiden tietoturvallisuuden kehittämistä.

Selvitetään tietoturvakoulutuksen vaikuttavuus	
Kohderyhmä	Kaikki tietoturvakoulutukseen osallistuvat (koko organisaatio)
Vaikuttavuus	Koko henkilöstö
Toteutuksen ohjaus	VAHTI
Toteuttaja	VM ja organisaatiot

Eri hallinnonaloilla järjestetyistä tietoturvakyselystä ja itsearvioinneista saadut kokemukset ovat olleet positiivisia. Työryhmä suosittelee yhteisen kyselyn tuotteistamista ja toteuttamista hallinnonaloittain säännöllisesti. Kaikille yhteisten kysymysten lisäksi kyselyssä voisi olla organisaation omia kysymyksiä. Tehdyt kyselyt tallentuvat tietokantaan, jolloin tuloksia voidaan käyttää anonyymeihin benchmark-vertailuihin. Järjestelmä voidaan liittää osaksi myöhemmin kuvattua sähköistä oppimisalustaa.

Eräs keino kerätä tietoja on lisätä muutama keskeinen kysymys vuosittaiseen ”Tietoja valtion tietohallinnosta ja tietotekniikasta” -kyselyyn.

”Kilpaillaan” tietoturvasta	
Kohderyhmä	Koko henkilöstö
Vaikuttavuus	Koko henkilöstö
Toteutuksen ohjaus	VM, LVM ja VAHTI
Toteuttaja	Organisaatiot

Eräs yksittäinen keino nostaa tietoturvallisuutta esille on organisaatio- tai hallinnonalakohtainen ”tietoturvakilpailu”. Kilpailun voisi liittää osaksi kan-

sallista tietoturvapäivää. Kilpailun voittaja olisi se organisaation ryhmä tai yksikkö/toimiala, joka on esimerkiksi osallistunut aktiivisimmin tietoturvakoulutuksiin tai muuten edistänyt organisaation tietoturvaa kuluneen vuoden aikana poikkeuksellisen aktiivisesti.

Kilpailua voitaisiin myös laajentaa valtakunnalliseksi esimerkiksi siten, että VAHTI valitsee organisaatioiden voittajista vuoden tietoturvakilpailun voittajan. Näin voitaisiin osaltaan levittää hyviä tietoturvakäytäntöjä laajemmin julkishallinnossa sekä samalla palkita niitä, jotka kiitoksen ansaitsevat.

5.2.2 Sähköiset palvelut

Kehitetään julkishallinnon yhteinen tietoturvallisuuden oppimisalusta	
Kohderyhmä	Koko henkilöstö
Vaikuttavuus	Koko henkilöstö
Toteutuksen ohjaus	VAHTI
Toteuttaja	Päätetään erikseen (VIP?)

Tietoturvakoulutusta tulee kehittää hyödyntämään nykyaikaisia sähköisiä oppimisvälineitä. Eräs tällainen ratkaisu on palvelu, joka toimii julkishallinnon yhteisenä tietoturvan sähköisenä oppimisalustana. Mikäli järjestelmälle halutaan laajempia käyttömahdollisuuksia, voi se tarjota palveluita myös muille kuin tietoturvayhteisölle. Palvelu sisältäisi esimerkiksi seuraavia toiminnallisuuksia:

- ajantasainen, sähköinen VAHTI-peruskäyttäjän tietoturvaohje
- tähän liittyvät multimediamateriaalit, videoluennot ja -esitykset
- ohjeeseen liittyvä testi
- valmius vastaavanlaisten syventävien oppimateriaalien tuottamiseen muille tässä selvityksessä kuvatuille kohderyhmille
- materiaaleja voi räätälöidä vaivattomasti organisaation omiin tarpeisiin
- tietoturvamateriaalipankki-toiminnallisuus
- tuotettua materiaalia voidaan hyödyntää tarvittaessa hyvin laajasti; materiaalin levittämistä voidaan määritellä käyttöoikeuksien avulla esimerkiksi julkiseksi tai rajoittaa hallinnonala- tai organisaatiokohtaisesti.

Tuotetaan julkishallinnolle yhteinen, säännöllisesti päivittyvä VAHTI perusohje	
Kohderyhmä	Koko henkilöstö
Vaikuttavuus	Koko henkilöstö
Toteutuksen ohjaus	VAHTI
Toteuttaja	Perustetaan ryhmä

Tämä ehdotus liittyy edelliseen kohtaan Kehitetään julkishallinnon yhteinen tietoturvallisuuden oppimisalusta.

Julkishallinnon tietoturvallisuuden peruskoulutuksen kehittymisen kannalta pidetään tärkeänä sitä, että henkilöstön tietoturvaohjetta päivitetään säännöllisesti, ja että siitä laaditaan erityyppisiä esitysmateriaaleja. Tällaisia olisivat esimerkiksi tietoturvaluennot (6 kpl 10 minuutin luentoja keskeisistä aiheista) ja videomuodossa olevat tietoturvatietoiskut.

Tässä yhteydessä tulisi selvittää, olisiko mahdollista velvoittaa työntekijöitä noudattamaan automaattisesti tällaista perusohjetta työssään. Organisaatio voisi tiukentaa / soveltaa perusohjetta omien toimintatapojen mukaisesti.

Näissä ohjeissa tulee erityisesti pyrkiä esimerkkien avulla konkretisoimaan ohjeessa esitettyjä asioita. Niin perus- kuin syventävissä ohjeissa tulee huomioida tietoturvatasojen vaatimukset osaamisessa

Tuotetaan ”Hauskat tietoturvavideot” - video-ohjeet / opasteanimaatiot	
Kohderyhmä	Koko henkilöstö
Vaikuttavuus	Koko henkilöstö
Toteutuksen ohjaus	VAHTI
Toteuttaja	Päätetään erikseen (VIP?)

Tämä ehdotus liittyy edelliseen kohtaan *Kehitetään julkishallinnon yhteinen tietoturvallisuuden oppimisalusta.*

Koska paperimuotoisia ohjeita ei aina jakseta lukea, pitää ohjeistus saattaa myös toisenlaiseen ja mielenkiintoisempaan muotoon, kuten esimerkiksi ”VAHTI-tietoturvavideot - 15 tärkeintä asiaa, joita pitää omassa työskentelyssä noudattaa”. Yksittäisen videon kesto on enintään kaksi minuuttia. Sisältö / käsikirjoitus koostuisi seuraavista osa-alueista:

- ongelman kuvaus eli esimerkki virheellisestä tavasta toimia
- syy-seuraus-suhde eli mitä virheellisestä toimintatavasta voi seurata
- mikä on oikea tapa toimia
- muuta ko. asiasta muistutettavaa.

Tuotetaan ”Päivän tietoturvamietelause”-palvelu	
Kohderyhmä	Koko henkilöstö
Vaikuttavuus	Koko henkilöstö
Toteutuksen ohjaus	VAHTI sihteeristö
Toteuttaja	VM;n tiedotus

Jotta opitut asiat ja tietoturvallisuus eivät unohdu koulutuksen jälkeen, pitää asioita kerrata ja muistuttaa niiden tärkeydestä säännöllisesti. Tähän voidaan käyttää ”päivän tietoturvamietelause” –palvelua. Www-palvelu julkaisee esimerkiksi kolme kertaa viikossa jonkin tietoturvaan liittyvän opetuksellisen muistutuksen. Lisätietoa, tarkempi selvitys ja ohjeita kyseisestä aiheesta löytyy uuteen ikkunaan avautuvasta linkistä. Organisaatio voi linkittää palvelun omaan intranet-verkkoonsa.

Vaihtoehtoisesti voidaan hyödyntää näytönsäästäjää, joka hakee vastaavat mietelauseet www-palvelimelta käyttäjän työaseman näyttöön näytönsäästäjän aktivoituessa.

Rakennetaan tietoturvamateriaalipankki	
Kohderyhmä	ICT-henkilöstö Tietoturvahenkilöstö
Vaikuttavuus	ICT-henkilöstö Tietoturvahenkilöstö ja välillisesti koko henkilöstö
Toteutuksen ohjaus	VAHTI
Toteuttaja	Päätetään erikseen

Julkishallinnossa on tuotettuna todennäköisesti kaikki tarvittava tietoturvaohjeistus mitä tarvitaan niin perus- kuin syventävää tietoturvakoulutusta ajatellen. Syvemmälle tasolle mentäessä materiaalia löytyy kattavasti tunnetuim-

pien sovellus- ja tietojärjestelmien tietoturvallisesta käyttöönotosta aina niiden valmius- ja toipumissuunnittelussa huomioitaviin seikkoihin saakka.

Julkishallinnon yhteisellä materiaalipankilla saadaan tällainen materiaali tehokkaaseen yhteiskäyttöön. Materiaalipankissa oleva aineisto ei sovellu sellaisenaan oman organisaation käyttöön, mutta olemassa olevan materiaalin mukauttamien on tuottavampaa kuin kokonaan uuden keksiminen.

5.2.3 Muut kehittämisideat

Kehitetään julkishallinnon tietoturva-ajokortti	
Kohderyhmä	Tietoturvahenkilöstö
Vaikuttavuus	Koko organisaatio
Toteutuksen ohjaus	VM:n linjaorganisaatio
Toteuttaja	Ulkoinen yhteistyötaho kilpailutuksen pohjalta

Tietoyhteiskunnan kehittämiskeskus TIEKE on ollut kehittämässä tietotekniikan ajokorttitutkintoja, jotka on koettu myönteisinä ja tarpeellisina. Työryhmä esittää julkishallintoon tarkoitetun tietoturva-ajokortin kehittämistä. Kaikki oppimateriaali tuotetaan keskitetysti yhdelle palvelimelle (kuten edellä on esitetty), jossa toimii oppimateriaaliin perehtymisen jälkeen suoritettava sähköinen tentti, jolla varmistetaan asioiden omaksuminen ja osaaminen.

Organisaatio saa palvelun raporttien avulla tietoa suoritetuista tenteistä, joten se voi muistuttaa niitä henkilöitä, jotka eivät sitä ole esimerkiksi edellisen kahden vuoden aikana suorittaneet tenttiä.

Kysymyspankkiin voi lisätä organisaatiokohtaisia kysymyksiä. Palvelua voidaan käyttää myös organisaation ulkoisten palveluyritysten ja konsulttien tietoturvaosaamisen valvomiseen. Palvelulla voidaan tuottaa tarvittava sertifiointi tietoturvallisuuden osalta.

Laaditaan tietoturvallisuuden koulutusohjelma turvallisuus-henkilöstölle	
Kohderyhmä	Tietoturvahenkilöstö
Vaikuttavuus	Koko henkilöstö
Toteutuksen ohjaus	VAHTI
Toteuttaja	Ulkoinen yhteistyötaho kilpailutuksen pohjalta

Organisaatioiden tietoturvasta vastaavien henkilöiden koulutus pohjautuu heidän oman aktiivisuuden, kaupallisen koulutustarjonnan ja laitetoimittajien koulutuksen varaan. Työryhmän mielestä julkishallinnon tietoturvavastaaville tulee tarjota räätälöitynä sekä perus- että syventävä koulutusohjelma.

Nämä koulutukset tulee suunnitella ottaen huomioon lähivuosina tietoturvallisuudessa tapahtuvat merkittävät hankkeet, kuten esimerkiksi tietoturvatasoista aiheutuvat haasteet.

Lisätään tietoturvallisuus osaksi kehityskeskusteluita ja osaamisvaatimuksia	
Kohderyhmä	Johto Esimiehet
Vaikuttavuus	Koko henkilöstö
Toteutuksen ohjaus	VM
Toteuttaja	Organisaatiot ja sen ylin johto

Esimiesten tulee olla selvillä siitä, miten tietoturvallisuus otetaan huomioon työntekijöiden työtehtävissä. Luonnollinen tilaisuus tähän syntyy vuosittaisissa kehityskeskusteluissa, joihin tietoturva ja siihen liittyvä osaaminen pitää saada liitettyä.

Tietoturvaosaaminen ja vaadittavat tietoturvataidot tulee olla myös osana tehtäväkuvauksia sekä mukana alusta alkaen työntekijöiden rekrytointiprosessissa.

Tuotetaan Tietoturvallisuus on asenne -julistesarja	
Kohderyhmä	Koko henkilöstö
Vaikuttavuus	Koko henkilöstö
Toteutuksen ohjaus	VAHTI sihteeristö
Toteuttaja	Organisaation tietoturvahenkilöstö tai ulkopuolinen taho

Yksinkertainen ja tehokas tapa muistuttaa tietoturvallisuuden tärkeydestä on tuottaa ”Tietoturvallisuus on asenne”-julistesarja. Julisteissa muistutetaan hauskasti keskeisistä tietoturvallisuudessa muistettavista asioista.

Julisteet tehdään valmiiksi esimerkiksi PDF- ja taustakuvatiedostoiksi ja sijoitetaan ladattavaksi VAHTI-sivustolle, josta organisaatiot voivat ladata ja tulostaa ne käyttöönsä. Tällainen julistekampanja sopii hyvin osaksi vuosittaista tietoturva-viikkoa.

Toteutetaan julkishallinnon yhteinen ICT-koulutuskalenteri	
Kohderyhmä	ICT-henkilöstö Tietoturvahenkilöstö
Vaikuttavuus	ICT-henkilöstö Tietoturvahenkilöstö
Toteutuksen ohjaus	VM
Toteuttaja	Päätetään erikseen

Useat koulutustilaisuudet mahdollistavat organisaation omien osallistujien lisäksi ulkopuolisten asiakkaiden osallistumisen. Tällaisia tilaisuuksia varten tulee toteuttaa julkishallinnon yhteinen ICT-koulutus -kalenteripalvelu. Koulutuskalenteriin ilmoitetaan ne tilaisuudet, joihin myös ulkopuoliset voivat osallistua. Tällä tavalla parannetaan koulutusten kustannustehokkuutta sekä mahdollistetaan osallistuminen sellaisiin koulutuksiin, joita pienempi organisaatio ei yksin kykene toteuttamaan.

Käyttöönoton jälkeen samaa palvelua voidaan tarjota myös muiden käyttäjäryhmien hyödynnettäväksi.

5.3 Syventävä koulutus

Tässä selvityksessä on pohdittu millaista syventävää tietoturvan jatkokoulutusta tulee järjestää eri kohderyhmille ja miltä tietoturvan eri osa-alueilta.

Syventävän tietoturvakoulutuksen toteuttaminen organisaatiokohtaisesti ei ole kustannustehokasta. Siksi tulee harkita esimerkiksi, että VAHTI tuottaisi ulkopuolisella yrityksellä tässä selvityksessä kuvatuille osa-alueille sähköisen oppimateriaalin vapaasti levitettäväksi julkishallinnon käyttöön.

Valtaosa edellisessä luvussa kuvatuista tietoturvallisuutta edistävistä toimenpiteistä on suoraan hyödynnettävissä myös syventävän koulutuksen osalta.

Kuva 7. Syventävä tietoturvakoulutus tulee suunnitella kohde- ja aiheryhmittäin vastaamaan henkilön työtehtävässään tarvitsemaa osaamista. Tietoturvatasoihin siirtyminen aiheuttaa muutospaineen koulutusten uusimisessa.

Kohderyhmä	Peruskoulutus (kaikille yhteinen)	Tuleva tietoturvatasojen edellyttämä osaaminen	Lainsäädäntö	Salassa pidettävien tietoaineistojen käsittely	Rekistereiden ylläpito	Tietosuoja	Sovellus- tai tietojärjestelmä kohtainen osaaminen	Turva-asiat	Valmius- asiat	Jatkuvuus- ja toipuminen	Lokiaineistojen käsittely
Ylin johto	√	√	√				√		√	√	
Esimiehet	√	√	√			√	√				
Erityissuojattavien tietoaineistojen käsittelijät	√	√	√	√	√	√	√				
Muut erityisryhmät	√	√	Riipuu erityisryhmän työtehtävistä								
Turvallisuushenkilöstö	√	√	√	√	√	√	√	√	√	√	√
ICT-henkilöstö	√	√	√	√	√	√	√		√	√	√

Edellyttää koulutuksen päivittämistä

Sanasto

ICT

Information and Communication Technology, suomeksi TVT (Tieto- ja viestintätekniikka), käsittää esimerkiksi sekä tieto- että viestintätekniikkaan liittyvät tuotteet, palvelut ja henkilöt.

Julkinen tietoaineisto

Julkisen tietoaineiston käsittely ei edellytä yhtä tiukkojen tietoturvavaatimusten täyttymistä luottamuksellisuuden osalta kuin salassa pidettävän tietoaineiston käsittely. Tästä huolimatta julkista tietoaineistoa tulee käsitellä siten, että julkisen tietoaineiston huolelliseen käsittelyyn, eheyteen ja käytettävyyteen liittyvät vastuut huomioidaan. Tietoaineiston julkisuus tai suojattavuus voi muuttua aineiston elinkaaren aikana. Osa tietoaineistosta saattaa olla salassa pidettävää ennen sen julkistamista, jonka jälkeen se muuttuu julkiseksi.

Peruskoulutus

Koko henkilöstölle kohdistettua tietoturvallisuuden peruskoulutusta tulee järjestää säännöllisesti. Erityistä huomiota tulee kiinnittää uusiin työntekijöihin.

Salassa pidettävät tietoaineistot

Asiakirja tai tieto, jonka käsittelylle on asetettu erityisiä tietoturvavaatimuksia luottamuksellisuuden (salassapito, tietosuoja), eheyden tai käytettävyyden suhteen. Valtaosa julkishallinnon työntekijöistä käsittelee salassa pidettäviä tietoaineistoja joko omissa työtehtävissään tai omiin henkilötietoihinsa liittyen.

Syventävä tietoturvakoulutus

Syventävä koulutus on tarkoitettu sille henkilöstölle, joka joutuu työtehtävien takia tekemisiin salassa pidettävien tietoaineistojen kanssa.

Tietoturvatasot

Tietoturvatasojen avulla määritetään (valtionhallinnossa) turvattavien kohteiden edellyttämä tietoturvallisuuden minimitaso kypsyystasojen avulla. Kypsyystasoja on viisi ja ne kuvaavat organisaation johtamisen, turvaprosessien ja turvatoimenpiteiden kehittyneisyyttä. Tietoturvatasot ovat luokiteltuja turvatoimenpide- ja menettelyvaatimuksia. Turvattava kohde voi olla esimerkiksi tietojärjestelmä, tietoaineisto tai alihankkijalta hankittava palvelu. Tietoturvatasojen on suunniteltu tulevan velvoittaviksi alkaen 1.1.2011.

Turvallisuushenkilöstö

Turvallisuushenkilöstöllä tarkoitetaan kaikkia niitä työntekijöitä, jotka toimivat joko pää- tai osatoimisina työntekijöinä esimerkiksi pelastus-, suojelu-, turva-, valmius-, tietosuoja- tai tietoturvatehtävissä. Tämä koskee myös ulkoistettuja palveluita kuten esimerkiksi aulapalvelut.

LIITE 1 Case-esimerkki: Sosiaali- ja terveysministeriön hallinnonalan tietoturvakysely

Sosiaali- ja terveysministeriön hallinnonalalla tehtiin syksyllä 2006 tietoturvakysely, jossa kysyttiin myös tietoturvakoulutukseen liittyviä asioita. Kyselyyn saatiin vastauksia 2 341 kpl vastausprosentin ollessa 48,8 prosenttia. Ohessa on kyselyn keskeisiä havaintoja, jotka on poimittu Stakesin järjestelmäasiantuntija Kimmo Janhusen pro gradu -opinnäytetyöstä.

STM:n hallinnonalan henkilöstölle esitettiin useita väittämiä liittyen henkilöstön tietoturvallisuuden eri osa-alueiden kokemiseen. Väittämäjoukon avulla pyrittiin löytämään vastauksia kahteen kysymykseen:

1. Millaisena eri henkilöstöryhmät kokevat tietoturvallisuuden omassa työssään ja vaikuttavatko käytössä olevat tekniset tietoturvaratkaisut työntekoon?

2. Miten tietoturvaohjeistukset ja -koulutukset koetaan ja miten niissä saatuja ohjeita noudatetaan?

Saatujen vastausten pohjalta voidaan todeta, että kaikki henkilöstöryhmät kokevat tietoturvan toteutuvan pääsääntöisesti erittäin hyvin tai hyvin organisaatiossaan (kuva 3). Erityisesti väittämien ”tietoturva toteutuu organisaatiossani hyvin” (keskiarvo 3,958, asteikkona 1 - 5, jossa viisi on erittäin hyvä) ja ”koen tietokoneen käyttämisen turvalliseksi organisaatiossani” (keskiarvo 4,207) vastausten erittäin hyvät keskiarvot lähes kaikissa organisaatioissa puoltavat tätä toteamusta. Huomionarvoista on myös, että vain vajaa 5 prosenttia vastaajista oli jokseenkin eri mieltä tai täysin eri mieltä em. väittämien kanssa.

Kuva 8. STM:n hallinnonalan henkilöstön vastaukset koskien tietoturvaohjeistuksen noudattamista.

STM:n hallinnonalan henkilöstö ilmoittaa luottavansa myös tietosuojan säilymiseen oman organisaation tietotekniikassa ja tietohallinnossa (keskiarvo 3,784). STM:n hallinnonalan henkilöstö uskoo itse käyttävänsä työsähköpostia (keskiarvo 4,255) ja www-selainta (keskiarvo 3,975) tietoturvallisesti.

STM:n hallinnonalan organisaatioissa käytössä olevien teknisten tietoturvaratkaisujen ei koeta häiritsevän (keskiarvo 3,77, ei merkittävää vaihtelua organisaatioiden välillä), mikä on hyvä tulos.

Tietoturvaohjeistuksien ja -koulutuksien osalta kyselyssä oli erilliset väittämät. Vastaukset näihin vaihtelivat organisaatioittain paljon. Tietoturvaohjeistuksien osalta koko STM:n hallinnonalan keskiarvon (3,704) voidaan katsoa olevan hyvä, vaikka tietoturvaohjeistuksien riittävyydestä oli jokseenkin eri mieltä tai täysin eri mieltä yhteensä 12,4 prosenttia henkilöstöstä.

Tiivistetysti tietoturvaohjeistuksista ja –koulutuksista voidaan todeta, että ohjeistuksien riittävyys ei ole ongelma STM:n hallinnonalan organisaatioissa, vaan ohjeiden jalkauttaminen normaaliin työhön. Tätä voidaan edistää muun muassa tietoturvakoulutuksilla, tietoturvatietoiskuilla sekä tiedottamisella.

Selkeitä kehittämisen kohteita STM:n hallinnonalan organisaatioissa on henkilöstöltä saatujen vastausten mukaan seuraavissa asioissa:

- tietoaineiston elinkaaren ja luokittelun ymmärtäminen
- tietoaineiston tietoturvallisen hävittämisen ohjeistukset ja koulutukset
- etäkäytön helppokäyttöisyys
- riittävä tietoturvallisuuskoulutuksen järjestäminen
- tietoturvallisuuteen liittyvistä asioista tiedottaminen
- roskapostin torjunta.

Kyselyn pohjalta jokainen organisaatio on löytänyt asioita oman tietoturvansa kehittämiseksi. Palaute kyselystä on ollut myönteistä niin käyttäjien kuin tietoturvavastaavien osalta.

LIITE 2 Esimerkkejä eri kohderyhmien koulutukseen liittyvistä kehittämistarpeista

Organisaation ylin johto

Tietoturvakoulutukseen liittyvä erityispiirre:
Koska organisaation ylin johto vastaa organisaation kokonaisturvallisuudesta, johdon rooli tietoturvallisuuden kehittämisessä on kriittinen. Johto vastaa myös omalla esimerkillään ja tuellaan tietoturvakulttuurin ja -asenteen kehittymisestä organisaatiossa.

Havaittuja ongelmia:

- tietoturvallisuuden tiedostamatta jättäminen
- ajan puute - tietoturva väistyy muiden tehtävien tieltä
- tietämys tai käsitys olemassa olevista riskeistä ”liian ruusuinen”
- oman vastuun ymmärrys tietoturva-asioissa on puutteellinen

Esimiehet ja prosessinomistajat

Tietoturvakoulutukseen liittyvä erityispiirre:
Esimiesten tehtävänä on huolehtia alaistensa tarvitsemasta tietoturvakoulutuksesta.

Havaittuja ongelmia:

- tietoturvallisuuden tiedostamatta jättäminen
- ajan puute - tietoturva väistyy muiden tehtävien tieltä
- tietoturvan huomioiminen edellyttää selkeää ylimmän johdon tukea
- tietoturva pidetään erillisenä osa-alueena, jota ei osata linkittää omaan esimiestyöhön, prosesseihin ja projekteihin

Asiantuntijat ja projektihenkilöstö

Tietoturvakoulutukseen liittyvä erityispiirre:
Koska työtehtävät saattavat vaihtua erityisesti projektitehtävissä, pitää henkilöstön osata vaihtaa näkökulmaa tietoturvallisuuteen vaihtuvien projektien ja tehtävien mukaisesti.

Havaittuja ongelmia:

- tietoturvallisuuden tiedostamatta jättäminen
- tietoturvallisuuden tasosta tinkiminen mikäli tehtävää tai projektia joudutaan rajaamaan tai resursseja tiukennetaan
- tietoturvallisuutta ei huomioida projektin alusta alkaen
- osaamisvajeet

Hankinnasta vastaavat henkilöt

Tietoturvakoulutukseen liittyvä erityispiirre:
Hankintojen merkitys on muuttunut merkittävästi hankintalakien uudistuessa.

Havaittuja ongelmia:

- tietämys uusista hankintalaeista saattaa olla puutteellinen
- tietoturvallisuutta ei huomioida hankinnoissa

Lakihenkilöstö

Tietoturvakoulutukseen liittyvä erityispiirre:
Lakien merkitys sekä tietohallinnon että ICT-palveluiden tuottamisessa on kasvanut koko ajan. Näiden ohella yksityisyyden suojaa ja tietoaineistojen käsittelyä koskevat kysymykset kasvattavat työmäärää.

Havaittuja ongelmia:

- lakipykälien soveltaminen käytäntöön ja viestintä tietoturvahenkilöstön kanssa usein ongelmallista
- ICT-alan ja tietoturvallisuuden erityiskysymykset vaativat omaa erikoisosaamista (hankinta, sopimukset, tietosuoja)

ICT-johto

Tietoturvakoulutukseen liittyvä erityispiirre:
ICT:stä vastaavan johdon haasteena on yhdistää riskienhallinta, tietoturvallisuus ja käytettävyys positiiviseksi käyttäjäkokemukseksi.

Havaittuja ongelmia:

- tietoturvallisuuteen liittyvien lakien ja asetusten tuntemus saattaa olla puutteellista
- tietoturvallisuuden sitominen toiminnansuunnitteluun on puutteellista
- ajan tasalla pysyminen uusista menetelmistä ja standardeista on puutteellista
- riskienhallinta puutteellista

Tietojärjestelmien ja infrastruktuurin tekniset pääkäyttäjät

Tietoturvakoulutukseen liittyvä erityispiirre:
Teknologian nopea kehittyminen edellyttää jatkuvaa opiskelua. Jatkuva kiire heikentää tietoturvallisuuden huomioimista omassa työssä.

Havaittuja ongelmia:

- käyttöoikeuksien oikeaoppinen käyttäminen ei ole tehokasta
- peruskäyttäjien tarpeita (ml. käytettävyysasiat) ei huomioida riittävästi
- tietoaineistojen luokittelutuntemus saattaa puuttua

Tukihenkilöt

Tietoturvakoulutukseen liittyvä erityispiirre:
Tukihenkilöt toimivat asiakaspalveluhenkilöinä ja muodostavat rajapinnan asiakkaiden ja ICT:n välillä. Heidän tulee näyttää mallia käyttäjille siinä, miten tietoturvallisuus tulee työskentelyssä ottaa huomioon.

Havaittuja ongelmia:

- käyttöoikeuksien oikeaoppinen käyttäminen ei ole riittävän tehokasta
- mikäli tehtävät eivät ole selkeästi ohjeistettuja (prosessinomaisia), jossain tilanteissa saatetaan mennä aidan yli niin matalalta, että tietoturvallisuus vaarantuu
- asiakas vs. esimies - tukihenkilön asema voi olla hankala (asiakaspalvelu)

Sovelluskehitys

Tietoturvakoulutukseen liittyvä erityispiirre:
Sovelluskehittäjät vastaavat tietoturvan toteutumisesta organisaation omassa sovelluskehityksessä.

Havaittuja ongelmia:

- sovelluskehittäjät eivät ole välttämättä ajan tasalla tietoturvariskien osalta tai siitä, miten tietoturvallisuus voidaan paremmin huomioida sovelluskehityksessä
- tietoturvallista koodaamista ei mielletä nopeaksi / tehokkaaksi / tuottavaksi
- ulkopuolinen auditointi on usein puutteellista
- osaamisvajeet

Turvallisuus- ja valmiushenkilöstö

Tietoturvakoulutukseen liittyvä erityispiirre:
Turvallisuus- ja valmiushenkilöstön toiminta ei välttämättä integroidu saumattomasti organisaation muuhun tietoturvatyöhön.

Havaittuja ongelmia:

- yhteistyö muun tietoturvaorganisaation ja tietohallinnon kanssa saattaa olla vajavaista
- tietoteknisen osaamisen puute

Tietosuojasta vastaavat henkilöt

Tietoturvakoulutukseen liittyvä erityispiirre:
Tietosuojan merkitys tietoaineistojen käsittelyssä ja luokituksessa on koko ajan kasvussa, mikä edellyttää säännöllistä koulutuksen ja ohjeistuksen uudistamista.

Havaittuja ongelmia:

- yhteistyö muun tietoturvaorganisaation kanssa saattaa olla vajavaista
- kokonaisuutta tarkastellaan liiaksi tietoaineistojen suunnasta
- yleinen ongelma on, että tietojärjestelmät eivät tue tietoaineistojen luokittelua

Tietoturvasta vastaavat henkilöt

Tietoturvakoulutukseen liittyvä erityispiirre:
Tietoturvasta vastaavien henkilöiden oman koulutuksen tulee tapahtua organisaation ulkopuolisena koulutuksena, jossa on huomioitu julkishallinnon erityispiirteet.

Havaittuja ongelmia:

- tietoturvaongelmia yritetään ratkaista liikaa teknisellä tietoturvalla
- käytettävyyden huomioiminen osana tietoturvallisuutta unohtuu
- tietoisuus voimassa olevista laeista ja asetuksista on puutteellinen

Tietojärjestelmien omistajat ja pääkäyttäjät

Tietoturvakoulutukseen liittyvä erityispiirre:
Tietojärjestelmien omistajien tulee omalta osaltaan huolehtia tietojärjestelmän riskianalyysin sekä muiden tarvittavien hallinnollisten asiakirjojen ajantasaisuudesta teknisen tietoturvan ohella.

Havaittuja ongelmia:

- tietojärjestelmä toimii usein henkilörekisterinä, jolloin ei tiedosteta kaikkia niitä velvoitteita ja vastuita, joita rekisterinpitäjälle kuuluu
- käyttöoikeuksien hallinta puutteellista
- tekninen osaaminen saattaa olla rajoittunutta

Peruskäyttäjät

Tietoturvakoulutukseen liittyvä erityispiirre:
Läheskään kaikki käyttäjät eivät lue tietoturvaohjeistusta tai eivät osallistu järjestettyyn tietoturvakoulutukseen. Tämä aiheuttaa sen, että osa peruskäytttäjistä ei noudata voimassa olevia tietoturvaohjeita.

Havaittuja ongelmia:

- peruskäyttäjät toimivat joko tietoisesti tai tiedostamatta tietoturvaohjeiden vastaisesti
- ongelmana on, että ohjeet ovat sirpaloituneita ja vaikeasti ymmärrettäviä
- ohjeiden vaikea saatavuus

Henkilörekistereiden hoitajat

Tietoturvakoulutukseen liittyvä erityispiirre:
Tähän kategoriaan kuuluvat sellaiset henkilöt, jotka käsittelevät säännöllisesti henkilötietoja töissään.

Havaittuja ongelmia:

- tietoaineistojen luokittelutuntemus puutteellinen
- työtehtävään liittyviä tietoturvariskejä ei riittävästi tiedosteta

Ulkoiset yhteistyötahot & alihankkijat

Tietoturvakoulutukseen liittyvä erityispiirre:
Ulkoisille yhteistyötahoille ja alihankkijoille ei normaalisti järjestetä tietoturvakoulutusta. Kuitenkin esimerkiksi organisaation toimitiloissa työskentelevien alihankkijoiden tulee noudattaa samoja ohjeita. Heidän tulee näin ollen voida osallistua tietoturvakoulutukseen, jotta he voivat noudattaa voimassa olevaa ohjeistusta.

Havaittuja ongelmia:

- sopimuksia laadittaessa tietoturvaa ei muisteta ottaa riittävästi huomioon
- tietoturvaa ei noudateta sopimuksista huolimatta (auditoinnin puute)

LIITE 3 Valtiovarainministeriön voimassaolevat VAHTI-julkaisut

Tietoturvallisuus on asenne! Selvitys julkishallinnon tietoturvakoulutustarpeista, VAHTI 6/2008

Valtion ympärivuorokautisen tietoturvavalvonnan hanke-esitys, VAHTI 5/2008

Valtionhallinnon tietoturva-arviointipoolin toimintaraportti, VAHTI 4/2008

Valtionhallinnon salauskäytäntöjen tietoturvaohje, VAHTI 3/2008

Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008

VAHTIn toimintakertomus vuodelta 2007, VAHTI 1/2008

Tietoturvallisuudella tuloksia – valtionhallinnon tietoturvallisuuden yleisohje, VAHTI 3/2007

Äypuhelimien tietoturvallisuus – hyvät käytännöt, VAHTI 2/2007

Osallistumisesta vaikuttamiseen - valtionhallinnon haasteet kansainvälisessä tietoturvatyössä, VAHTI 1/2007

Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006

Tietoturvakouluttajan opas, VAHTI 11/2006

Henkilöstön tietoturvaohje, VAHTI 10/2006

Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006

Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006

Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006

Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006

Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006

Electronic Mail-handling Instructions for State Government, VAHTI 2/2006

Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005

Valtionhallinnon sähköpostien käsittelyohje, VAHTI 2/2005

Information Security and management by Results, VAHTI 1/2005

Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004

Datasäkerhet och resultatstyrning, VAHTI 4/2004

Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004

Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004

Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006, VAHTI 1/2004

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003

Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003

Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003

Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003

Arkaluonteiset kansainväliset tietoaineistot, VAHTI 4/2002

Valtionhallinnon etätyön tietoturvallisuusohje, VAHTI 3/2002

Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002

Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista, VAHTI 6/2001

Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001

Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001

Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000

Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 Valtioneuvosto
Puhelin (09) 160 01
Telefaksi (09) 160 33123
www.vm.fi

6/2008
VAHTI
joulukuu 2008

ISSN 1455-2566
ISBN 978-951-804-892-6 (nid.)
ISBN 978-951-804-893-3 (pdf)