RAPORTEJA

TERO TAMMISALO

Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi

Periaatteet ja menetelmät

STAKES

Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus

postimyynti: Stakes / Asiakaspalvelut PL 220, 00531 Helsinki
puhelin: (09) 3967 2190, (09) 3967 2308 (automaatti)
faksi: (09) 3967 2450 • Internet: www.stakes.fi

Taitto: Christine Strid

ISBN 978-951-33-1936-6 (nid.)
ISSN 1236-0740 (nid.)
ISBN 978-951-33-1937-3 (PDF)
ISSN 1795-8210 (PDF)

Stakes, Helsinki 2007

Valopaino Oy
Helsinki 2007

Esipuhe

Stakes on kehittänyt koko 2000-luvun aktiivisesti yhteistyössä sosiaali- ja terveysministeriön kanssa ohjeistusta sosiaali- ja terveydenhuollon asiakastietojen tietoturvalliselle tietojenkäsittelylle. Osana kansallista terveysprojektia Stakes on julkaissut mm. suositukset sähköisestä suostumuksesta, potilastietojen luovutuksesta sekä ohjeen tietoturvallisista toimintaperiaatteista. Lisäksi Stakes on osallistunut sekä kansalliseen lainsäädäntötyöhön että kansainväliseen terveydenhuollon tietojenkäsittelyn standardisointityöhön.

Tämän hankkeen tavoitteena on ollut tuottaa ohje sosiaali- ja terveydenhuollon toimintayksiköille ja organisaatioille tietoturvallisuuden hallinnointiin. Hanke käynnistyi vuoden 2006 alussa ja se on ollut yhteisrahoitteinen projekti sosiaali- ja terveysministeriön kanssa. Hankkeessa on tuotettu tietoturvakoulutusta ja -hallinnointia tukevaa materiaalia terveydenhuollon käytännön toimijoille sekä koulutettu kouluttajia. Tämä hallinnointiopas on osa hankkeessa tuotettua materiaalia.

Hankkeen projektiryhmän jäseniä ovat olleet:
- Tero Tammisalo/Stakes
- Emmi Tenhunen/Stakes
- Ville Komula/Varsinais-Suomen sairaanhoitopiiri
- Maritta Korhonen/Pohjois-Savon sairaanhoitopiiri
- Pentti Körkkö/Pohjois-Pohjanmaan sairaanhoitopiiri
- Pekka Nevalainen/Pohjois-Karjalan sairaanhoito- ja sosiaalipalvelujen kuntayhtymä.

Asiantuntijoina ryhmän toimintaan ovat osallistuneet:
- Esa Kemppainen/Pohjois-Savon sairaanhoitopiiri
- Juha Malinen/Pohjois-Karjalan sairaanhoito- ja sosiaalipalvelujen kuntayhtymä.

Sekä ryhmän vakiojäsenet että mainitut asiantuntijat ovat antaneet asiantuntija-apua tätä opasta kirjoitettaessa.

Projektin ohjauksesta Stakesissa on vastannut tutkimusprofessori Pekka Ruotsalainen.

Oppaasta on pyydetty lausuntoja usealta taholta. Osa vastaajista on myös kommentoinut oppaan asiasisältöä ansiokkaasti jo kirjoitustyön aikana.

Tietoturvan hallinnointi noudattaa pääsääntöisesti samoja lainalaisuuksia toimialasta riippumatta. Siksi tämä opas voi toimia apuvälineenä myös sosiaali- ja terveydenhuollon ulkopuolella. Suurimmat erot muihin toimialoihin verrattuna liittyvät sosiaali- ja terveydenhuollon tietojen arkaluonteisuuteen ja salassapitoon sekä toiminnan organisointiin, jossa on huomioitava sekä lainsäädännölliset että eettiset vastuut.

Tietoturvallisuuden toteutumisesta vastaa viime kädessä kukin henkilö omalta osaltaan. Standardinomaiset hallinnointimenettelyt mahdollistavat organisaation tietoturvan kehittämisen, ylläpidon ja mittaamisen nimeämällä näihin tehtäviin vastuulliset henkilöt ja sopimalla tarvittavista toimenpiteistä. Tällöin tietoturva voi toteutua osana organisaation normaalia toimintaa.

Sosiaali- ja terveydenhuollon yksikköjen koot vaihtelevat suuresta yliopistollisesta sairaanhoitopiiristä yksittäiseen ammatinharjoittajaan. Suuren yksikön toiminnat ja siten myös tietoturvallisuuden hallinnointi edellyttävät monimutkaisempaa organisaatiota kuin mitä tarvitaan pienessä yksikössä. Jotta tämä opas soveltuisi käytettäväksi erikokoisissa organisaatioissa, on oppaassa esitetty kokonaismallin ohella myös pienelle yksikölle soveltuvat minimivaatimukset.

Stakesin tavoitteena on ylläpitää tätä opasta ja päivittää sitä käytännössä saatujen kokemusten pohjalta. Mahdolliset kommentit pyydetään ystävällisesti toimittamaan Stakesin tietoyhteiskuntayksikköön osoitteella ursula.corner@stakes.fi.

Stakesin tietoyhteiskuntayksikkö kiittää lämpimästi projektiryhmän jäseniä, asiantuntijoita ja kaikkia tämän oppaan laatimiseen osallistuneita heidän arvokkaasta panoksestaan.

Helsingissä 5.3.2007

Päivi Hämäläinen
Sosiaali- ja terveysalan
tietoyhteiskuntayksikön päällikkö

Pekka Ruotsalainen
Tutkimusprofessori

Tiivistelmä

Tero Tammisalo. Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi. Periaatteet ja menetelmät. Stakes, Raportteja 5/2007. Helsinki 2007. 74 sivua, hinta 17 €.
ISBN 978-951-33-1936-6

Tietoturvallisuuden kehittäminen ja ylläpito muodostuu oleelliseksi osaksi jokaisen sosiaali- ja terveydenhuollon organisaation (tieto)hallintoa varsinkin, kun asiakas- ja potilastietoja on alettu säilyttää, käsitellä ja siirtää kokonaan sähköisessä muodossa. Tämä asettaa tietoturvan hoidolle entistä suurempia haasteita ja vaatimuksia; on oletettavaa, että tietoriskien hallinta tulee lähitulevaisuudessa näyttelemään ratkaisevaa osaa jokaisen organisaation toiminnassa.

Tämä opas esittelee mallin, jonka avulla organisaatio voi kehittää ja ylläpitää tietoturvatoimintaansa standardilla tavalla. Mallissa on esitetty:

- tietoturvan kehittämisprojekti, jolla tietoturvatoiminta perustetaan, sekä
- tietoturvan hallinnointiprosessi, jonka mukaisesti organisaation tietoturvaa hallitaan jatkuvana toimintana.

Lisäksi liitteinä on hyödyllistä tietoturvatietoa ja erilaisia asiakirjoja esimerkin antamiseksi.

Opas soveltuu käytettäväksi sosiaali- ja terveydenhuollon organisaatioissa, mutta sitä voidaan soveltaa myös toimialan ulkopuolella. Opas sopii käytettäväksi sekä suurille että pienille organisaatioille, kuten myös tietoturvatoimintansa vasta aloittaville ja sitä jo toteuttaville organisaatioille. Opasta voidaan myös hyödyntää vain osittain: organisaatiossa voidaan valikoida käyttöön kulloiseenkin tietoturvan kehittämistilanteeseen sopivat osat.

Avainsanat: tietoturva, tietojenkäsittely, terveydenhuolto

Sisällys

1 JOHDANTO

Tässä luvussa kuvataan lyhyesti hallinnointiopas kokonaisuutena ja esitetään katsaus sen sisältöön.

Opasta kirjoitettaessa lähestymistavaksi on otettu luettelomainen ote, jotta oppaan hyödyntäminen eri organisaatioissa olisi mahdollisimman helppoa ja vaivatonta, ja jotta eri osioita voitaisiin hyödyntää toisistaan riippumattomasti. Erilaisia osakokonaisuuksia on lisäksi pyritty jäsentämään tarkastuslistatyyppisiksi kokonaisuuksiksi.

Tässä oppaassa esitetään malli, jonka mukaan organisaation tietoturvatoiminta voidaan perustaa ja jolla voidaan organisoida päivittäinen toiminta. Myös muunlaisilla toimintamalleilla on mahdollista saada aikaan laadukas tietojen turvaamistoiminta ja hyvä tietoturvan taso. On tärkeää tiedostaa, että ei ole ainoastaan yhtä oikeaa tapaa toimia, vaan on olemassa useita hyviä ja kelpaavia toimintamalleja. Tämä opas ei pohjaudu yhteenkään nimenomaiseen tietoturvallisuuteen, riskienhallintaan tai niiden johtamisen standardiin, mutta eri standardeja on otettu tarvittaessa huomioon oppaan laatimisen yhteydessä, ja oppaassa mahdollisista vaihtoehdoista esitetään yksi toimivaksi havaittu.

Oma organisaatio, vaikkakin virtuaalinen, on välttämätön tietoturvan hoidossa. Virtuaalisuus tarkoittaa sitä, että tietoturvavastuut ja -tehtävät on määriteltävä nimetyille henkilöille, jotka hoitavat nämä vastuut oman toimensa ohella ja raportoivat niistä sovitulla tavalla. Tyypillisesti terveydenhuollon organisaation tietoturvavastuut jakautuvat esimerkiksi johtavalle ylilääkärille (terveydenhuollosta vastaava johtaja), käyttöpäällikölle, ATK- tai IT-päällikölle, henkilöstöpäällikölle, tekniselle päällikölle ja mahdolliselle valmiuspäällikölle, eikä kokonaisuus siten aina ole kenenkään hallinnassa. Tästä syystä oppaassa esitetään, että hallinta ja valvonta määrätään yhdelle henkilölle, tietoturvapäällikölle, joka koordinoi kaikkien edellä mainittujen henkilöiden kanssa tietoturvallisuuden johdon. Lisäksi useat sertifioinnit edellyttävät, että organisaatiossa on erillinen tietoturvasta vastaavan henkilön toimenkuva ja siihen nimetty henkilö.

Oppaassa esitettyä mallia voidaan käyttää erikokoisissa organisaatioissa. Opasta voivat hyödyntää myös sellaiset organisaatiot, joilla on jo käytössään erilaisia olemassa olevia tietoturvan hallinnointimalleja ja -käytäntöjä. Näin lienee valtaosassa organisaatioita. Tämän oppaan esittämistä tehtävistä voidaan ottaa joustavasti käyttöön vain osa, ja tarvittaessa mainittuja tehtäviä voi muokata oman organisaation vaatimusten mukaisiksi vastaamaan täsmällisemmin niihin yksityiskohtaisiin olosuhteisiin, joita kussakin organisaatiossa on. On nähtävissä, että sosiaali- ja terveydenhuollon organisaatioilta tullaan edellyttämään niiden tietoturvan sertifiointia, luultavimmin jonkun viranomaistahon tai siihen tehtävään erikseen valtuutetun sertifiointiyhteisön toimesta. Nämä vaatimukset täsmentävät jatkossa sen minimitason, joka organisaatioiden on täytettävä tietoturvan hoidossa.

Sosiaali- ja terveydenhuollossa tietosuojan toteutumisesta ja henkilö-, potilas- ja asiakastietojen suojaamisesta on tarkoin säädetty lainsäädännöllä. Tietojen suojaaminen on välttämätöntä lakien vaatimusten lisäksi myös tietojen tärkeyden ja arkaluonteisuuden vuoksi – vaikka täsmällisiä vaatimuksia ei olisikaan lailla säädetty, on organisaation silti huomioitava tärkeiden ja organisaation toiminnan kannalta oleellisten tietojen suojaaminen taatakseen toimintakykynsä. Henkilö-, potilas ja asiakastietojen lisäksi tällaisia tietoja ovat esimerkiksi organisaation henkilöstön, yhteistyökumppaneiden ja omaan toimintaansa liittyvät tiedot ja asiakirjat. Se, että monet näistä tiedoista on talletettu sähköisessä muodossa erilaisiin tietojärjestelmiin ja tietoverkkoihin, asettaa niiden suojauksen erityisen tärkeään asemaan – väärinkäyttömahdollisuuden lisääntyvät

ja riskit rahallisestikin arvokkaan tiedon väärinkäytölle kasvavat. Tämä teknologinen muutos on otettu huomioon myös lainsäädännössä, joka ottaa tietojen suojaamisvaatimuksissa huomioon enenevässä määrin myös tietojen käyttötavat, toimintaympäristön ja -kulttuurin.

Käytännössä tämän oppaan avulla voidaan siis perustaa tietoturvallisuuden hallintajärjestelmä, ISMS (*Information Security Management System*), joka on systemaattinen lähestymistapa – menetelmä ja prosessi – jolla hallitaan organisaation tietoturvaa ja suojataan niitä tietoja, joiden on katsottu tarvitsevan suojaamista. Oppaan tarkoitus on motivoida ja auttaa organisaatioita tietoturvallisuuden hallinnointimenettelyiden laadinnassa ja käyttöönotossa. Valitettava totuus on, että useassa organisaatiossa tietoturvan hoito on puutteellista ja tietoturvan taso liian matala – olipa syy tähän kustannusten leikkaukset, liiketoiminnallisen voiton tehostaminen tai osaamisen, ymmärryksen tai tarvittavien resurssien puute.

Aiemmin mainituista tietoturvallisista toimintaperiaatteista (Stakes Raportteja 5/2005) löytyy termistö, luettelo laeista ja joistakin tietoturvaan ja sen hallinnointiin liittyvistä standardeista, kattava lista tietoturvaperiaatteista/kontrolleista ja joitakin mallidokumentteja. Tietohallintoon, riskinhallintaan, jatkuvuussuunnitteluun ja kriisinhallintaan liittyviin standardeihin ja ohjeistuksiin kannattaa vielä tutustua erikseen tarpeen mukaan. Näitä ei tässä oppaassa kuitenkaan mainita kirjallisuutena tai lähteinä; ainakin osittain käyttökelpoisia ja tutustumisen arvoisia ohjeistuksia on tarjolla runsaasti, ja valtaosa niistä on kaupallisia.

Tässä oppaassa on esitetty tietoturvapäällikön tai tietoturvavastaavan toimenkuva täysipäiväiseksi. Näin ei kuitenkaan välttämättä ole, eikä vaatimus suinkaan ole ehdoton. Tietoturvasta vastaavan henkilön tietojen suojaamiseen käyttämä aika on luonnollisesti riippuvainen organisaation koosta ja tilanteesta – vaativatko tarvittavat toimenpiteet ylipäätään yhden henkilön täysipäiväisen työn, ja onko organisaatiossa mahdollisuuksia varata tämän tehtävän hoitoon tällainen henkilö ja lisäksi muut tarvittavat resurssit. Huolimatta siitä, että tietoturvapäällikön toimenkuva ei olisikaan täysipäiväinen, on vastuu organisaatiossa kuitenkin nimettävä yhdelle henkilölle, joka vastaa kaikkien välttämättömiksi katsottujen tehtävien hoitamisesta ja organisoi tietoturvallisuuden toteutumista kokonaisuutena. Lainsäädännössä on mainittu tietosuojavastaavan tehtäväkuva. Hänen vastuulleen määrätyt tehtävät eivät kuitenkaan sisällä kaikkia tietoturvan hoidossa tarvittavia tehtäviä. Organisaatiossa on myös ymmärrettävä jokaisen esimiehen rooli tietoturvallisuuden toteuttamisessa: esimerkin näyttämisessä, omien alaistensa toiminnan seuraamisessa ja palautteen antamisessa.

Rajauksena mainittakoon, että oppaassa ei tarjota mallia tietoturvan hallinnoinnin tason tai laadun mittaamiseen. Liitteenä oleva projektisuunnitelma voi toimia kehitysvaiheen tarkastuslistana, mutta tässä tarkoituksessa mittaamisen suureina voivat pääasiallisesti olla vain tehtävien tila (”valmis”, ”kesken”) ja valmistumisen ajankohta. Sertifioitaessa tietoturvatoiminta (esimerkiksi BS:n tai ISO:n mukaisesti) on tarkoitus sertifioida nimenomaan jatkuva tietoturvan hallinta. Sertifioivalta taholta saadaan tarkat toimintaohjeet ja tiedot, millaisia mittareita organisaation tarkastuksen yhteydessä käytetään ja miten standardien noudattaminen todennetaan. Uusimmat standardit ottavat aiempaa paremmin huomioon sekä johdon sitoutumisen että organisaation osaamisen. Tietoturvan hallintaprosessin ja sen toimivuuden mittaaminen on yksi avaintekijä sertifioinnin yhteydessä.

Mittaamisen suureista voi kuitenkin yleisohjeena todeta, että hyvä tapa on käyttää eräänlaista kypsyysmallia (*CMM, capability maturity model*). Kypsyysmallissa mitataan, missä määrin organisaatio on saavuttanut sen tietoturvatoiminnalle asetetut tavoitteet: käytännössä sillä voidaan osoittaa, kuinka hyvin käytössä oleva hallinnointimalli toteuttaa standardoidulle tietoturvan hallintajärjestelmälle asetetut vaatimukset. Kypsyysmalli vaihtelee tyypillisesti nollatasosta (tavoitteita ja toimintaperiaatteita ei ole tunnistettu, niitä ei ole olemassa eikä niitä siten myöskään mitata) huipputasoon (toimintaperiaatteet ja prosessit on optimoitu vastaamaan organisaation toimintaa, ne on dokumentoitu ja koko organisaation tiedossa; toimintaa mitataan tehokkaasti

ja kehitetään vastaamaan tulevaisuuden muutostarpeisiin). On myös todettava, että mittaamista ei kannata aloittaa liian aikaisin: on oltava selkeästi mitattavat kohteet, ettei vääriä tulkintoja tietoturvan toteutumisesta ja laadusta pääse syntymään.

Yksi suurimmista yksittäisistä riskeistä tietoturvan ja tietosuojan loukkauksiin on henkilöstön asenne ja osaaminen: miten tietojen käsittelyn turvallisuuteen ja ohjeiden noudattamiseen suhtaudutaan sekä kuinka hyvin oikeanlaiset toimintatavat osataan. Henkilöstön koulutus, osaamisen ylläpito ja motivointi riittävine seurantatoimineen muodostaa pohjan koko organisaation toiminnan turvallisuudelle. Koulutuksen tärkeyttä on tähdennettävä, sillä se on luultavasti helpoin ja varmin keino nostaa tietoturvan tasoa. Koska tässä oppaassa eri tehtäviä ei ole asetettu tärkeysjärjestykseen eikä koulutusta (luvussa 5.2.11 Koulutuksen suunnittelu ja toteutus) ole siten nostettu esiin muiden tehtävien joukosta, on koulutuksen tärkeys otettu esiin tässä yhteydessä.

Oppaasta on rajattu tietoturvapäällikön täsmällisten työtehtävien ja niiden aikataulujen kuvaaminen, ”tietoturvapäällikön viikko-ohjelma”. Tällainen ohjelma on laadittavissa kullekin organisaatiolle, kun on tiedossa hallinnoinnin, valvonnan ja päivittäisten tarkastusten täsmälliset tehtävät, toimenpiteet ja niihin kuluva aika. Ohjeellista viikko-ohjelmaa ei ole nähty tarkoituksenmukaiseksi laatia.

Myös erilaiset lomakepohjat, kuten raportointilomakkeet, kokouspöytäkirjat, esityslistat ja muut vastaavat hallinnoinnissa käytettävät asiakirjat on rajattu tämän oppaan ulkopuolelle.

2 TÄMÄN DOKUMENTIN KÄYTTÖ

Tässä luvussa annetaan ohjeistusta siitä, miten tätä opasta voi ja kannattaa hyödyntää.

Opas jakautuu kolmeen osioon, joista kukin kuvaa yhden tehtäväkokonaisuuden tietoturvatoiminnan organisoinnissa ja kehittämisessä. Kukin osio sisältää joukon toimenpide-ehdotuksia, joita kyseisessä vaiheessa on hyödyllistä toteuttaa.

Koska seuraavassa esitettyjen ensimmäisen ja toisen osion kuvaama määritystyö on kertaluonteinen työ, se voidaan siten toteuttaa projektina. Projekti voidaan nimetä esimerkiksi tietoturvahallinnoinnin kehittämisprojektiksi. Liitteessä on yleistasoinen esimerkki projektisuunnitelmasta sekä projektin tehtävistä. Yleisesti voi todeta, että vaiheiden 1 ja 2 tehtävät (oppaan osio 1) ovat käytännössä projektin valmistelutyötä ja vastuiden määrittelyä, kun taas vaiheet 3 ja 4 (oppaan osio 2) varsinaisen tietoturvatoiminnan ja tehtävien suunnittelua.

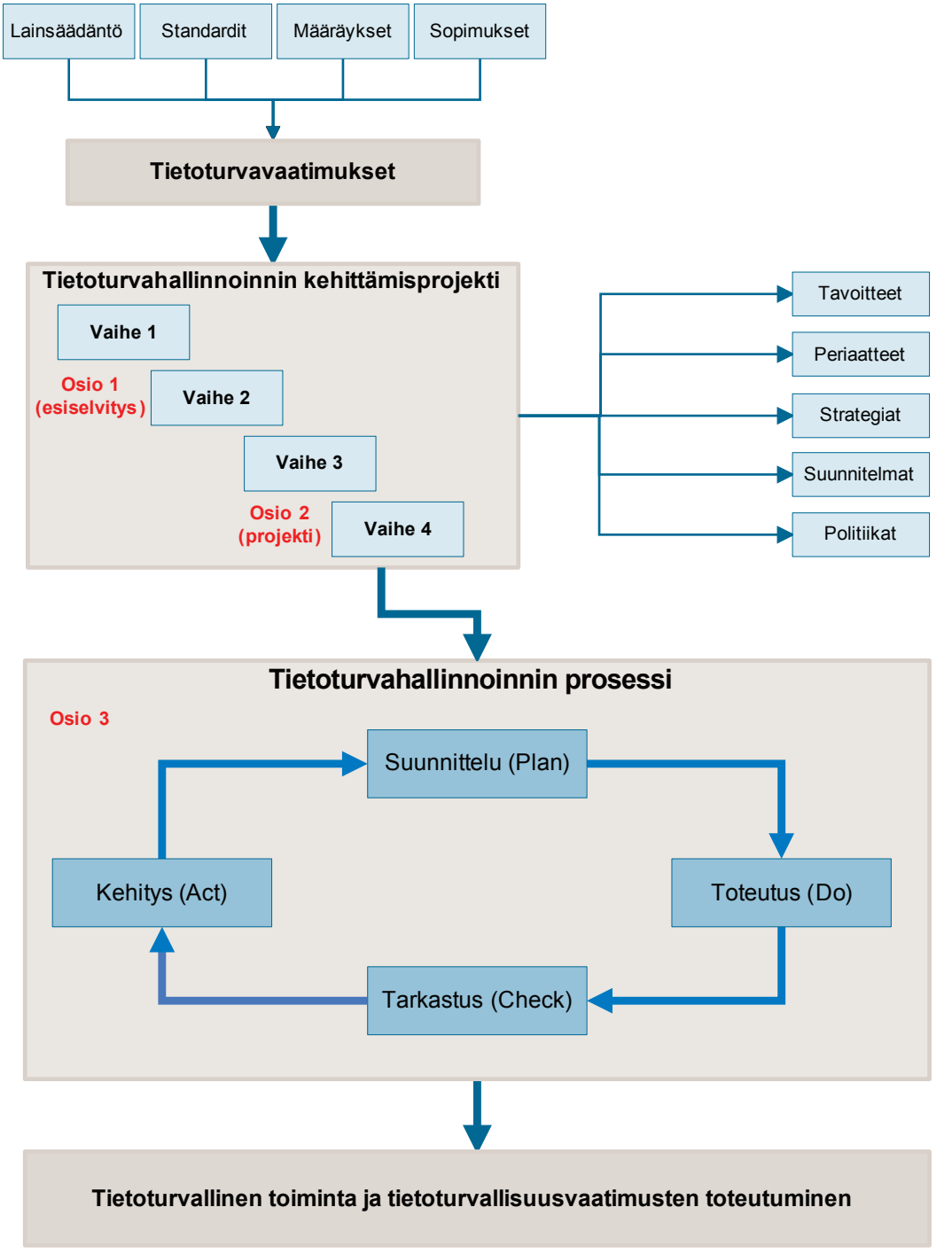
Ensimmäinen osio koostuu kehittämistoiminnan vaiheista 1 ja 2: tällöin määritellään raamit tietoturvaorganisaatiolle ja sen toiminnalle (vaihe 1) ja nimetään tietoturvaorganisaatio (vaihe 2) tai vähintäänkin sen johto, toisin sanoen tietoturvapäällikkö. Voi siis sanoa, että näiden vaiheiden tavoite on määritellä tietoturvapäällikön ja tietoturvaorganisaation roolit ja vastuut sekä nimittää tietoturvapäällikkö, joka toimii projektipäällikkönä seuraavissa vaiheissa. Ensimmäisessä osiossa tehdään siten projektin esiselvitystyö.

Toinen osio koostuu vaiheista 3 ja 4. Tällöin oletetaan, että tietoturvapäällikkö on jo nimetty ja osallistuu täysipainoisesti tietoturvan kehittämistyöhön molemmissa vaiheissa 3 ja 4. Vaiheessa 3 laaditaan organisaatiolle tietoturvasuunnitelma ja -strategia sekä niihin oleellisesti liittyvät muut asiakirjat. Vaiheessa 4 sovitaan kehitysprojektin yksityiskohtaisista aikatauluista ja tehtävistä tietoturvapäällikön kanssa, kuten myös määritellään prosessi, jonka mukaan tietoturvaa hallinnoidaan. Näiden vaiheiden tavoitteeksi voisikin määritellä organisaation, hallinnointimallin sekä yksityiskohtaisten olosuhteiden ja ympäristön luomisen siten, että tietoturvahallinnointi voidaan käynnistää standardinomaiseksi jatkuvaksi toiminnaksi.

Kolmas osio on kertaluontoisen käynnistämisen jälkeen jatkuvaa toimintaa syklisenä prosessina: tietoturvan ylläpito toteutetaan jatkuvana prosessina. Organisaation tietoturvatoimintaan liittyviä dokumentteja on luonnollisesti arvioitava aika ajoin osana tietoturvan hallinnointia, ylläpidettävä dokumentteja vastaamaan muuttuviin ja kehittyviin olosuhteisiin, ja siten tehtävä dokumentteihin ajan mittaan tarvittavia muutoksia. Tämä koskee sekä suunnitelmia, strategioita että politiikkoja.

Tämän oppaan liitteinä on erilaisia esimerkkejä ja malleja, esimerkiksi tehtävälistoja, tarkastuslistoja ja muita asiapapereita, joita organisaatio voi käyttää hyväkseen tietoturvan kehittämistyössään.

Kuva 1 osoittaa tietoturvahallinnoinnin kehittämisprojektin ja sen tuloksena syntyvän jatkuvan prosessin välisen yhteyden.



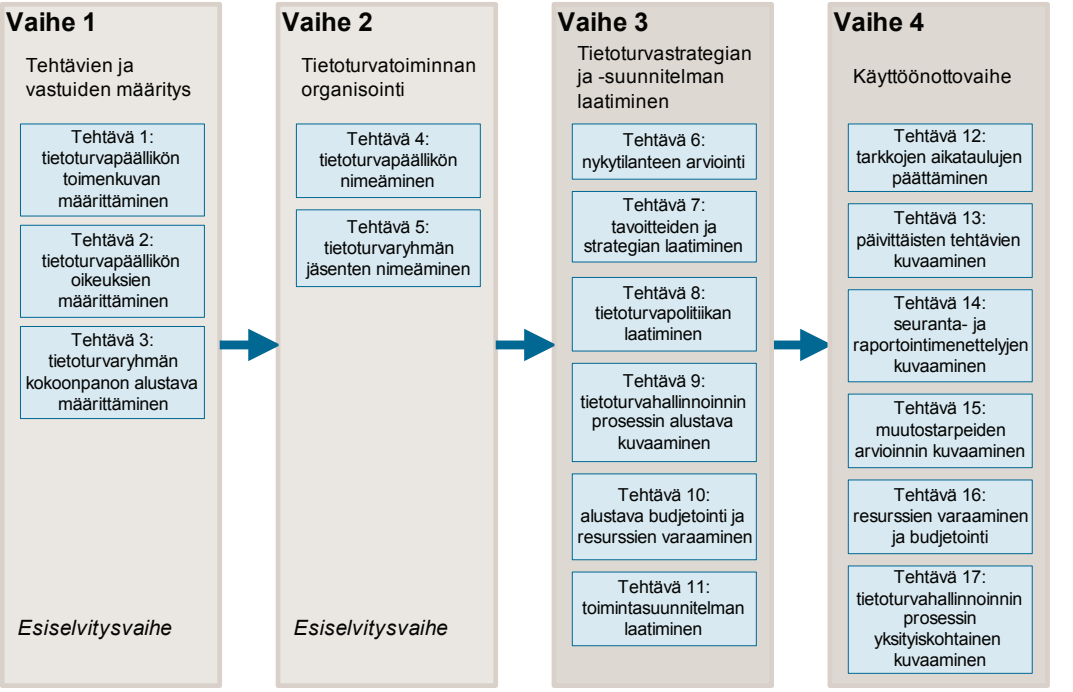
KUVA 1. Tietoturvahallinnoinnin kehittäminen

3 OSIO 1: ESISELVITYS

Organisaation tietoturvatoiminnan omistaa organisaation johto. Esiselvitysvaiheessa selvitetään, millaisella organisaatiolla ja menettelyillä organisaation tietoturvatoiminta voidaan perustaa ja miten sitä voidaan kehittää. Varsinainen toiminta on jatkuva prosessi, jonka omistaa ja jota valvoo organisaation johto.

Kuva 2 esittää yksinkertaisessa muodossa seuraavilla sivuilla esitetyn tietoturvahallinnoinnin kehittämisprojektin kulun tehtävineen. Kuvassa on esitetty, kuinka tietoturvahallinnoinnin kehittämisprojekti ja siinä aikaansaatavat dokumentit luovat pohjan tälle jatkuvalle prosessille, jolla organisaation tietoturvaa hallinnoidaan ja vaadittu (tai valittu) tietoturvan taso voidaan toteuttaa.

Esimerkinomainen projektisuunnitelma on löydettävissä tämän dokumentin liitteenä.



KUVA 2. Kehittämisprojektin vaiheet ja tehtävät

3.1 Vaihe 1: Tietoturvatoiminnan tehtävien ja vastuiden määritys

Tehtävä 1. Määritellään toimenkuva ja vastuut sekä tietoturvapäällikölle että tietoturvan hallinnoinnin organisaatiolle.

- Tietoturvaa hallinnoiva organisaatio on tyypillisesti virtuaaliorganisaatio, jota kutsutaan tässä dokumentissa vastedes nimellä tietoturvaryhmä. Tietoturvaryhmä ohjaa ja valvoo tietoturvan toteutumista organisaatiossa ja toimii myös sisäisenä tarkastajana sertifioitaessa tietoturvatoiminta. Käytännössä tietoturvaryhmä toimii siis eräänlaisena ohjausryhmänä tai tietoturvan johtoryhmänä. Tästä huolimatta kokonaisvastuu tietoturvasta säilyy kuitenkin organisaation johdolla.
- Tietoturvaryhmän toiminta täytyy tarkastaa aika ajoin myös erillisen sisäisen tarkastajan toimesta esimerkiksi pistokokein. Tämä on erityisen tärkeää silloin, kun organisaation tietoturvatoiminta sertifioidaan. Tällöinhän tietoturvan hallinnointiprosessi arvioidaan organisaation ulkoisen osapuolen toimesta valittua standardia noudattaen, ja sertifiointi tyypillisesti edellyttää myös säännöllisiä sisäisiä tarkastuksia.
- Kun tietoturvapäällikkö on nimetty (nimeäminen projektin vaiheessa 2), hän osallistuu jatkotyöhön toteutusvastuullisena, ohjaa tietoturvan toteutumista, toimii tarvittaessa tietoturvaprojektien projektipäällikkönä ja vastaa tietoturvaryhmän säännöllisestä kokoon kutsumisesta.
- Vaikka tietoturvatehtävät sisältävät runsaasti myös teknisiä toimenpiteitä, tietoturvapäällikön rooli on ennen kaikkea hallinnollinen eikä niinkään tekninen. Tietoturvan hoidon teknisiä tehtäviä suorittavat ne henkilöt, jotka ovat asiantuntijoita kukin omalla alallaan.

Esimerkki tietoturvapäällikön vastuista ja tehtävistä on esitetty liitteessä 5.

Tehtävä 2. Määritellään tietoturvapäällikön oikeudet. Näitä voivat olla esimerkiksi

- tehtävien jako tietoturvaryhmän jäsenille etukäteen tiedossa olevien raamien mukaisesti,
- (järjestelmien ja toiminnan) tarkastukset, testit ja harjoitusten järjestäminen,
- tietoturvakoulutusten järjestäminen ja henkilöiden määrääminen koulutuksiin (esimiesten välityksellä),
- tietoturvaloukkauksissa ja -poikkeamissa korjaavien toimenpiteiden järjestäminen ja ohjaus,
- muutosvaatimusten esittäminen esimerkiksi teknisten syiden takia, jossa tapauksessa toimenpiteiden hyväksyntä tehdään tarvittavalla tasolla organisaatiossa,
- mahdollisesti (pienimuotoisten) sanktioiden järjestäminen,
  - pääsääntöisesti esimiesten välityksellä
  - kollektiivirangaistuksia on vältettävä
- tiedottaminen,
  - yleispreventio; tiedotus havaituista loukkauksista ja rangaistuksista esimerkin antamiseksi (ei kerrota tapahtumien yksityiskohtia, ei paljasteta henkilöitä)
- sekä tietoturvamittausten tulosten julkistaminen sovitusti.

Tehtävä 3. Määritetään tietoturvaryhmän kokoonpano (tehtäväkuvat) ainakin alustavasti.

- Määritellään tarpeellinen määrä sopivia tehtäviä, toiminteita ja funktioita. Määritellään jokaisen henkilön rooli, tehtävä ja vastuut tietoturvan hoidossa. Varsinaisia henkilöitä ei tässä vaiheessa tarvitse nimetä.
- Yleensä tietoturvaryhmän jäseninä toimivat tarvittavien organisaatioyksiköiden (riittävän päätöksentekovaltaiset) edustajat.
- Tietoturvaryhmän tehtäviä ovat tyypillisesti muun muassa:
  - ohjata ja valvoa organisaation tietoturvatoimintaa,
  - huolehtia tietoturvaperiaatteiden toteutumisesta,
  - vastata tietoturvallisuuden kehittämishankkeiden valmistelutyöstä tai osallistua hankkeiden valmistelutyöhön,
  - koordinoida tietoturvatoimenpiteitä kukin jäsen omalta osaltaan,
  - tarjota tietoturvan erityisosaamista ja tietoturvapalveluita eri yksiköille aina tarvittaessa ja myös turvata tällaisen osaamisen saanti,
  - seurata ja valvoa tietoturvatilannetta sekä tarvittaessa reagoida ja puuttua havaittuihin ongelmiin ja uhkiin,
  - huolehtia, että yksiköt ja tietohallinto ovat tehneet jatkuvuussuunnitelmat poikkeustilanteita varten sekä infrastruktuurin että kaikkien keskeisten tietojärjestelmien osalta,
  - huolehtia, että tiedot ja tietojärjestelmät on turvaluokiteltu,
  - huolehtia uhkien ja riskien säännöllisestä analysoinnista sekä jäännösriskien (suojaustoimenpiteiden jälkeen jäljelle jäävät riskit) kirjaamisesta ja hyväksyttämisestä),
  - ohjeistaa tietoturva-asiat ja huolehtia, että ohjeista tiedotetaan ja koulutetaan,
  - huolehtia auditointien järjestämisestä,
  - toimia sisäisenä tiedottajana poikkeustilanteissa (tietoturvaan liittyen) sekä
  - luonnollisesti huolehtia myös muista, tässä mainitsemattomista tietoturvaan liittyvistä toimenpiteistä aina tarpeen mukaan.

3.2 Vaihe 2: Tietoturvatoiminnan organisointi

Tehtävä 4. Nimetään tietoturvapäällikkö (nimike voi poiketa, mikäli siihen on tarve). Tämä voi edellyttää haku-, valinta- ja palkkausprosessin, jos organisaatiossa ei ole tehtävään soveltuvaa henkilöä. Tässä tapauksessa on kiinnitettävä erityinen huomio valittavan henkilön taustan ja soveltuvuuden tarkastamiseen. Tietoturvapäällikön tehtäväkuvaan liittyvistä ominaisuuksista on hyvä huomioida ainakin seuraavat:

- Tehtävä on käytännössä kokopäivätoiminen. Tämä riippuu luonnollisesti organisaation koosta ja tietoturvaan kohdistuvista vaatimuksista (ja toimialasta: sosiaali- ja terveydenhuollossa vaatimukset ovat moneen muuhun toimialaan verrattuna poikkeuksellisen yksityiskohtaiset ja tiukat).
- Tietoturvapäällikkö vastaa käytännön toteutuksesta ja toiminnasta ja voi toimia projektipäällikkönä tietoturvan kehitysprojekteissa.
- Tietoturvapäällikkö on suoraan ylimmän johdon alaisuudessa ja raportoi tietoturvatoiminnan omistajalle (organisaation johto).
  - Johto ohjaa tietoturvapäällikön tehtäviä ja valtuuttaa tietoturvapäällikön toiminnan.
  - Tietoturvapäällikkö raportointi suoraan johdolle.

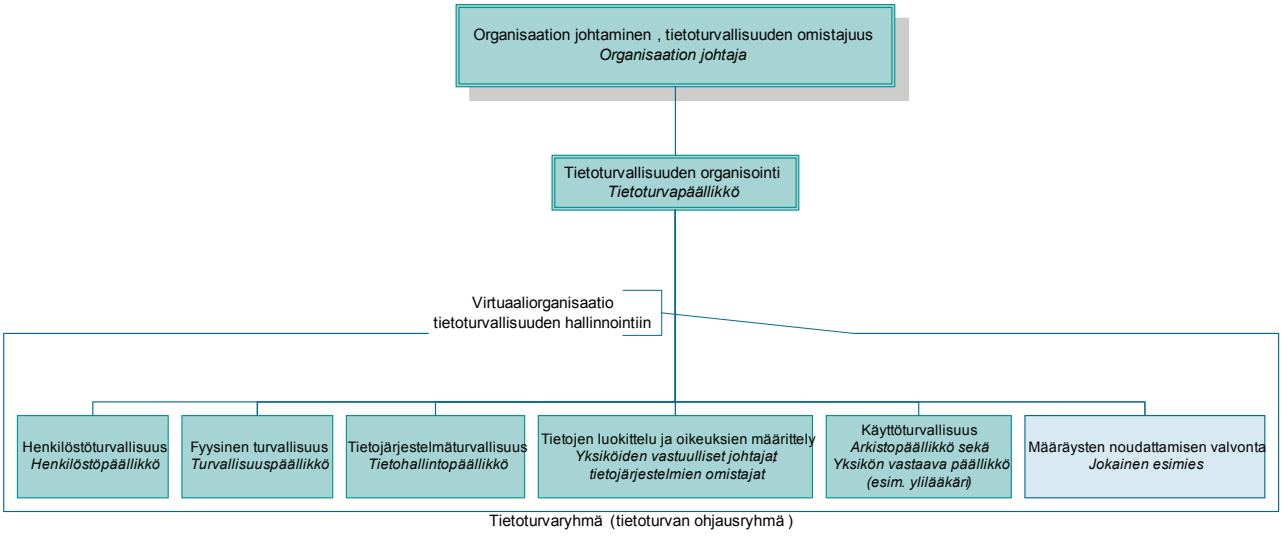
- Johtajan tai johtoryhmän lisäksi yksikään organisaation henkilö ei voi vaikuttaa tietoturvapäällikön toimintaan tai sen laatuun.
- Tämä antaa mahdollisuuden saada täysimääräiset resurssit tietoturvatoiminnan organisointiin.
- Tämä takaa raportoinnin riippumattomuuden ja puolueettomuuden.
- Tämä mahdollistaa oikea-aikaisen ja riittävän tasoisen puuttumisen tietoturvarikkeisiin ja reagoinnin havaittuihin uhkiin.
- Tehtäväkuvana tietoturvapäällikön raportointi- ja valvontatehtäviä voi verrata esimerkiksi tilintarkastustoimintaan tai organisaation ”sisäiseen tarkastukseen”. Imagomielessä jälkimmäistä rinnastusta on syytä välttää, jotta koko organisaation yhteistyö ja asennoituminen on vapaaehtoista eikä vastentahtoista.
- Auditointien järjestämisen vuoksi toiminta ei voi sijaita esimerkiksi tietohallinnossa.
- Tietoturvapäällikön ja tietoturvaryhmän toimien valvonta ja tarkastus on nimenomaan ”organisaation tietoturvatoiminnan sisäistä tarkastusta”.

Tehtävä 5. Määritetään ja nimetään muut henkilöresurssit ja vastuut tietoturvaryhmään (toisin sanoen yhteistyötahot organisaation sisältä), joka vastaa käytännössä tietoturvan toteuttamistyön ohjauksesta. Tietoturvaryhmää nimettäessä on hyvä huomioida ainakin seuraavat asiat, joita henkilöiltä, ryhmän vastuilta ja toiminnalta voidaan olettaa. Tarvittaessa tehtävässä 16 voidaan täydentää tämän tehtävän aikaansaannoksia.

- Aina tarpeen mukaan tietoturvaryhmän toimintaan osallistuu kustakin organisaation osasta vastuullinen henkilö siten, että kaikki tietoturvan osa-alueet on katettu ja kunkin organisaation osan tietoturvan toteutuksesta vastaava henkilö on nimetty.
- On erityisen tärkeää, että nämä organisaation sisäiset tiedotus- ja yhteistyökanavat luodaan valmiiksi etukäteen, ennen kuin toiminta varsinaisesti käynnistyy. Kun yhteistyökanavat ovat olemassa, yhteistyötahojen "nimet ja naamat" ovat entuudestaan tuttuja, ja riski tiedonvälityksen katkoille tai yhteistyön epäonnistumiselle pienenee oleellisesti.
- On erityisesti kiinnitettävä huomiota tietohallintoon, henkilöstöhallintoon ja fyysiseen turvallisuuteen. Organisaation jokaisen henkilön vastuulla on toteuttaa tietoturvaa ja noudattaa määräyksiä; tämän valvonta kuuluu esimiehille ja siksi käytönvalvonta (yksiköiden päälliköt) on yksi oleellinen kokonaisuus. Jokaisen päällikön ei silti tarvitse olla tietoturvaryhmässä jäsenenä.
- Vaikka nämä henkilöt osallistuvat tietoturvahallinnointiin tietoturvaryhmän jäseninä, ei heidän tarvitse olla nimellisesti tietoturvapäällikön alaisuudessa. Paras tulos saavutetaankin, kun tietoturvaryhmän jäsenet kuuluvat organisatorisesti omiin yksiköihinsä ja toivat oman yksikkönsä edustajina tietoturvaryhmässä. Tietoturvapäällikön alaisuuteen sopii organisaatiomielessä esimerkiksi tietoliikenteen ja palomuurien teknisiä asiantuntijoita, mutta yleinen käytäntö on, että nämä puolestaan kuuluvat hallinnollisesti organisaation tietohallinnon alaisuuteen.
- Huomaa myös kriisinhallintaorganisaation tai valmiusorganisaation läsnäolo tietoturvatoiminnassa. Kriisitilanteissa ja mahdollisissa poikkeusolosuhteissa kriisinhallintaorganisaatio saattaa vastata koko organisaation toiminnasta ja mahdollisesta pelastustoiminnasta, jolloin myös tietoturvan johtamisessa saatetaan noudattaa poikkeuksellisia järjestelyjä.

Kuva 3 osoittaa esimerkinomaisesti tietoturvan hallinnointia varten perustettavan virtuaaliorganisaation rakenteen. Raportointi tällaisessa organisaatiossa tapahtuu suoraan ”ylöspäin” ja käskytys ”alaspäin”. Jokainen kyseisen organisaation jäsen on menettelytavoista ja vastuista tietoinen.

- Kustakin toiminnasta vastaava taho raportoi tietoturvapäällikölle, joka raportoi suoraan johdolle.
- Tietoturvaan liittyvien toimeksiantojen luonteesta ja laajuudesta, ja tietoturvapäällikölle tähän tarkoitukseen myönnetystä toimivallasta on erikseen ja etukäteen sovittu.
- Kaikki tietoturvatehtävät suoritetaan ennalta sovitun mukaisesti.
- Kuvassa oleva virtuaaliorganisaatio muodostaa yhteysverkoston koko organisaatiolle molemminpuolista ja -suuntaista yhteydenpitoa varten.
- Virtuaaliorganisaatiosta valitaan sopivat tahot, jotka toimivat yhteyshenkilöinä ulkopuolisiin tahoihin (esimerkiksi CERT), ja mobilisoivat omassa organisaatiossa yhteistyötoiminnan ja sopivat käytännön menettelytavoista yhteydenpidossa.



KUVA 3. Virtuaaliorganisaatio tietoturvan hallinnoinnissa

4 OSIO 2: PROJEKTI

4.1 Vaihe 3: Tietoturvastrategian ja -suunnitelman laatiminen

Vaihe 3 voidaan käynnistää, kun tietoturvapäällikkö on nimetty ja aloittanut tehtävässään. Hän osallistuu työhön ja avustaa dokumenttien ja toimintasuunnitelmien laatimisessa. Seuraavassa on mainittu tehtäväkokonaisuudet vaiheessa 3.

Tehtävä 6. Arvioidaan nykytila sekä kartoitetaan ja analysoidaan ongelmakohdat.

- Tämä voidaan tehdä myös ilman tietoturvapäällikön osallistumista, jolloin tarvittava osaaminen hankitaan esimerkiksi ulkoiselta konsultilta. Tämä ei kuitenkaan missään tapauksessa ole suositeltavaa: tietoturvapäällikön motivaatio on paras ja ammattitaito saadaan parhaiten hyödynnettyä, kun hän saa olla mukana määrittelytyössä alusta alkaen. Lisäksi konsulttia käytettäessä on vaarana, että kartoitustyössä syntynyt arvokas tieto ei jääkään kokonaisuudessaan organisaation käyttöön, vaan osa siitä jää ainoastaan konsultin henkiseksi pääomaksi. Jos näyttää, että konsulttityötä tarvitaan, ulkoisten konsulttien työn on järkevintä olla tietoturvapäällikön määrittelemää ja valvomaa. Muutenkin, jos työtä tekemään tarvitaan organisaation ulkopuolisia henkilöitä, teetettävän työn on syytä olla mahdollisimman käytännönläheistä, jotta osaaminen ja kokemukset ei valu oman organisaation ulkopuolelle.
- Kun hallinnointiprosessi saadaan käyntiin, vastaavanlainen työ sisältyy vaiheeseen suunnittelu (plan).
- Tässä tehtävässä voidaan myös hahmottaa tietoturvan kehittämisen pilotti, eräänlainen kokeilu (proof of concept), jossa tietoturvan kehittämistoimia suunnitellaan ja kokeillaan rajoitetulla osajoukolla ja kevennetyllä mallilla (hyödyntämällä osion 3 prosessia kevennetysti). Tällöin voidaan kokeilla esimerkiksi joukko menetelmiä, metodeja ja teknologioita, ja saadaan valittua omaan organisaatioon parhaiten soveltuvat, ja sovitettua ne helpommin oman organisaation päivittäiseen toimintaan.

Tehtävä 7. Kirjataan organisaation tietoturvatoiminnan tavoitteet ja strategia niiden toteuttamiseksi viralliseksi dokumentiksi.

- Määritellään tietoturvatoiminnan kattavuus (applicability). Tämä on tärkeää, jos esimerkiksi joitakin osakokonaisuuksia halutaan sulkea määritellyn tietoturvatoiminnan ulkopuolelle. Tällaisia voivat olla esimerkiksi poikkeuksellinen maantieteellinen voimassaolo (jos eri organisaatiot vastaavat toiminnasta eri maantieteellisillä alueilla) tai tiettyjen toiminteiden tai toimialojen siirtäminen kokonaan oman tietoturvatoimintansa vastuulle (kuten palkkahallinto tai pysyväisarkisto). Ulkopuolelle voidaan rajata myös sellaiset kokonaisuudet, joihin omalla organisaatiolla ei ole vaikutusvaltaa. Tällaisia voivat olla esimerkiksi valtakunnanlaajuisessa käytössä olevat tai sellaisiksi valitut arkkitehtuurit tai teknologiat, kuten kansallinen tietojärjestelmäarkkitehtuuri tai sähköisen reseptin teknologiat.
- Tavoitteet organisaation tietoturvatoiminnalle määräytyvät tyypillisesti sekä ulkoisten vaatimusten että toisaalta sisäisen tarpeen perusteella. Vaatimuksia asettavat esimerkiksi suojattavien kohteiden (asset) kriittisyys, riskianalyysin

tulokset ja erilaiset mittaus- ja raportointitulokset (skannaukset, loukkausraportit, reklamaatiot ym.). Jotkin tavoitteet voidaan katsoa niin tärkeiksi ja strategisiksi, että ne kirjataan myös organisaation tietoturvastrategiaan. Edellisessä tehtävässä tehty nykytilanteen kartoitus ja tavoitteet muodostavat yhdessä GAP-analyysin, jolloin analysoidaan ero ("kuilu") nykyhetken ja tavoitetilan välillä. Tavoitteet voivat sisältää erilaisia mittareita toteutuneen tietoturvan tasolle. Näitä mittareita voivat olla esimerkiksi

- tilasuureet, kuten
  - "organisaation tietoturvatoiminta täyttää lakien vaatimukset",
  - "tietoturvan hallintaprosessi on kiinteä osa koko organisaation hallintoa ja noudattaa standardoituja menettelytapoja",
  - "käytössä olevat potilastietojärjestelmät noudattavat standardinmukaisia tietoturvaominaisuuksia",
  - "tietoturvan toteutumista seurataan säännöllisesti",
  - "raportointimenettelyt ovat tehokkaita ja raportointi tapahtuu ajallaan",
  - "sekä johto että henkilöstö on sitoutunut tietoturvan toteuttamiseen" tai
  - "tietoturvapolitiikka on julkaistu",
- erilaiset numeeriset suureet, kuten määrää tai prosentuaalista osuutta osoittavat
  - "ei yhtään asiakkaan tai potilaan tekemää epäilystä tietojen väärinkäytöstä",
  - "jokaiselle organisaation työntekijälle on jaettu tietoturvakäsikirja",
  - "kaikkien alihankkijoiden ja kolmansien osapuolten kanssa on solmittu salassapitosopimus",
  - "ei yhtään onnistunutta virushyökkäystä",
  - "90 prosenttia roskapostista pystytään suodattamaan ennen loppukäyttäjää" tai
  - "75 prosenttia henkilöstöstä on osallistunut tietoturvakoulutukseen ja tietoiskuihin".

- Strategia on joukko tärkeimpiä toimintaperiaatteita, jotka ovat parhaita tai optimaalisia tavoitellun tietoturvatason saavuttamiseksi. Joissakin tapauksissa tietty osa tietoturvastrategiaa voi olla organisaation toiminnan kannalta niin tärkeä, että se voidaan ottaa osaksi koko organisaation toiminnallista strategiaa. Tietoturvaa ohjaavat strategiset päätökset ovat ajallisesti riittävän kauaskantoisia. Kun tietyt tavoitteet on saavutettu, ne voidaan liittää osaksi strategiaa, kuten seuraavassa kaksi ensimmäistä esimerkkiä. Strategiassa voidaan mainita esimerkiksi:
  - ”organisaation tietoturvatoiminta täyttää lakien vaatimukset”,
  - ”tietoturvan hallintaprosessi on kiinteä osa koko organisaation hallintoa ja noudattaa standardoituja menettelytapoja”,
  - ”henkilöstölle annetaan säännöllisesti tietoturvakoulutusta”,
  - ”kaikki uusimmat tietojärjestelmien tietoturvapäivitykset arvioidaan ja testataan ja otetaan tarvittaessa käyttöön mahdollisimman nopeasti” tai
  - ”kaikkiin tietoturvarikkeisiin puututaan”.
- On myös hyvä kirjata organisaation tietoturvatoimintaa koskevat periaatteet yksityiskohtaisesti. Periaatteiksi voidaan valita sopivimmat esimerkiksi aiemmin mainitusta Stakesin raportista1 Sosiaali- ja terveydenhuollon tietojärjes-

telmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt. Jos tietoturvatoiminta halutaan sertifioida, toimintaa kuvaava dokumentaatio on helpompi laatia ja kouluttaa organisaatiolle silloin, kun periaatteista määräytyvät reunaehdot ovat selvillä.

- Tässä yhteydessä on myös tärkeää linjata tietoturvan hallinnointijärjestelmän (ISMS) dokumentoinnin periaatteet. Varsinainen dokumentointityö kuuluu oleellisena osana jatkuvaan prosessiin, joka on kuvattu osiossa 3. Tietoturvatoiminnan jatkuvuuden ja laadun takaamiseksi dokumentoinnin periaatteet on oltava tiedossa jo alkuvaiheessa.

Tehtävä 8. Laaditaan ja julkaistaan organisaation tietoturvapolitiikka.

- Jos organisaatiossa on jo olemassa oleva tietoturvapolitiikka, se arvioidaan ja tarvittavat muutokset tehdään, jotta politiikka vastaa määriteltyjä tavoitteita ja strategiaa.
- Tietoturvapolitiikka on johdon hyväksymä näkemys ja julkaistu kannanotto organisaation tietoturvan tärkeimmistä päämääristä, periaatteista ja toteutuksesta. Sillä voidaan osoittaa tietoturvaan sitoutuminen sekä omalle organisaatiolle että kolmansille osapuolille.

Tehtävä 9. Kuvataan tietoturvan johtamisen ja hallinnoinnin prosessi.

- Yksityiskohtainen kuvaus on esitetty tämän oppaan osiossa 3. Prosessin kulun yksityiskohtainen määrittely voidaan tehdä myös vaiheessa 4; tässä yhteydessä on tärkeä sopia prosessin kulusta ja tärkeimmistä tehtävistä kussakin vaiheessa (suunnittelu, toteutus, tarkastus, kehitys).
- Kuvattu tietoturvan johtamisen prosessi pohjautuu nimenomaan riskien hallintaan.
- Prosessia operoi ja hallinnoi tietoturvapäällikkö yhdessä tietoturvaryhmän kanssa. Tietoturvaryhmä johtaa ja valvoo tietoturvatavoitteiden toteutumista. Tietoturvaryhmän toiminta voidaan aika ajoin tarkastaa erillisessä sisäisessä tarkastuksessa. Tämä on hyvä tehdä säännöllisesti.
- Tässä yhteydessä on myös hyvä selvittää, onko organisaation tietoturvaa tarpeen sertifioida. Jos näin on, sertifiointiin liittyvät yksityiskohdat voidaan suunnitella käyttöönoton valmistelussa tai vasta myöhemmin osana päivittäistä hallinnointityötä.

Tehtävä 10. Varataan alustavat resurssit ja tehdään alustava budjetti tai luodaan raamit seuraavaan budjettiin.

- Tämä koskee erityisesti johdon ja tietoturvaryhmän omia resursseja (esimerkiksi riittävän ajan varaaminen).
- Tarvittavat muutokset ja täsmennykset tehdään projektin seuraavassa vaiheessa 4.

Tehtävä 11. Laaditaan vaiheen lopuksi sovittujen tavoitteiden ja riskianalyysin perusteella lähivuosien toimintasuunnitelma, tietoturvasuunnitelma.

- Lyhyen ajan toimintasuunnitelma, "tietoturvan kehitysprojekti", tehdään vaiheessa 4.
- Tässä yhteydessä on myös hyvä rakentaa yhteys muihin pidemmän ajan suunnitelmiin, joita voivat olla esimerkiksi valmiussuunnitelma, jatkuvuussuunnitelma, kriisienhallintasuunnitelma, toipumissuunnitelmat, henkilöstön

kehitys- ja koulutussuunnitelmat sekä erilaiset toiminta- tai liiketoimintasuunnitelmat.

- Tässä vaiheessa kirjataan myös jäännösriskit ja hyväksytetään ne, mikäli tilannekartoitus on jo tuottanut riittävän riskianalyysin. Luonnollisesti osana päivittäisen tietoturvahallinnoinnin prosessia tehdään riskianalyysi, jonka jälkeen havaitut jäännösriskit hyväksytetään. Riskianalyysin teko ja jäännösriskien arviointi on kuvattu osiossa 3.

4.2 Vaihe 4: Käyttöönoton valmistelu

Tässä vaiheessa 4 sovitaan yhteistyössä tietoturvapäällikön kanssa seuraavassa mainituissa asioista ja niiden hoitamisen vastuista. Vaiheen tehtäväkokonaisuuksia on mainittu seuraavassa.

Tehtävä 12. Sovitaan kehitysprojektin tarkennetuista aikatauluista tietoturvapäällikön kanssa. Muun muassa seuraavista asioista sovitaan:

- heti toteutettavat toimenpiteet,
- myöhemmin toteutettavat toimenpiteet,
- jatkotyö
  - ei-toteutettavat kohteet,
  - myöhempi kehitystyö,
  - tarpeiden uudelleenarviointi,
  - mahdollinen organisaation tietoturvan sertifiointi ja siihen liittyvät seikat (noudatettava sertifiointiohjelma, sertifioitavat kohteet, tavoitteet, aikataulu ym.)
    - sertifioinnin ja sen ylläpidon määrittelyt osana organisaation säännöllistä tietoturvatoimintaa
- sekä kaikki ne välttämättömät tehtävät, jotka täytyy tehdä, että tietoturvan kehitystyö voi ylipäätään alkaa
  - välineiden hankinta,
  - olemassa olevien käytäntöjen ja järjestelmien kirjaus,
  - dokumentointi tarvittavalla tarkkuustasolla.

Tehtävä 13. Luetellaan päivittäisen tietoturvatoiminnan johtamisessa ja organisoinnissa suoritettavat tehtävät. Huomaa, että tietoturvapäällikön tehtäviä, vastuita ja oikeuksia on lueteltu aiemmin tässä dokumentissa, vaiheen 1 kuvauksessa. Organisoinnin tehtäviä voivat olla esimerkiksi

- kontrollien määrittelystä ja seurannasta sopiminen,
- sopiminen turvaamistoiminnasta yleensä, esimerkiksi teknisten ja ei-teknisten ratkaisuiden toteutuksesta (ohjelmistot, laitteistot, kulunvalvonta ym.),
- materiaalien (manuaalit ym.) ja ohjeistusten laatimisesta sopiminen,
- tietoturvakoulutuksen järjestämisestä sopiminen,
- poikkeustilanteiden ja hälytysten yhteydessä vikojen tai poikkeamien korjauksista ja osallistumisesta korjaustehtäviin (incident response team), mahdollisista tilapäisratkaisuista ja niiden tiedottamisesta sopiminen tarpeen mukaan,
- säännöllisestä testaamisesta ja standardinomaisten testimenettelyiden ylläpidosta sopiminen ja
- CERT-toiminnasta sopiminen.

Tehtävä 14. Luetellaan tietoturvapäällikön vastuulla olevat päivittäisen tietoturvatoiminnan johtamis-, raportointi- ja seurantamenettelyt. Näitä ovat esimerkiksi
- raportointimenettelyt, määräajat ja raporttien laatu ja
- kokouskäytännöt, kuten
  - tietoturvaryhmän koolle kutsumisen menettelyt ja
  - arvioidut kokoontumisaikataulut tai -välit.

Tehtävä 15. Luetellaan tietoturvapäällikön vastuulla olevat teknologisen kehityksen seuraamisen, uusien uhkien arvioinnin ja organisaation käytössä oleviin (tietoteknologisiin) ympäristöihin kohdistuvien muutospaineiden arvioinnin tehtävät ja vastuut. Nämä voivat sisältää esimerkiksi seuraavia:
- Tietoturvapäällikkö ylläpitää omaa osaamistaan ja asiantuntemustaan ajan tasalla.
- Tietoturvapäällikkö laatii muutosehdotuksia tarpeen mukaan.
- Tietoturvapäällikkö vastaa, että tietoturvatoiminta on tiiviissä yhteistyössä tietoteknologiasta vastuullisen organisaation kanssa.

Tehtävä 16. Varataan tietoturvatoiminnan resurssit tarpeen mukaan. On luonnollista, että resurssien ja budjetin suunnittelu ei voi olla alkuvaiheessa tarkkaa.
- Määritellään henkilöresurssit. Tämä tehtävä lisää yksityiskohtia tehtävien 5 ja 10 tuloksiin. Resursseja varattaessa on huomioitava
  - tietoturvaryhmän ohjaustehtävissä tarvitsema aika,
  - teknisiltä asiantuntijoilta tarvittava aika suuntaa antavana arviona sekä
  - varautuminen selvittämään mahdollinen palkkaus- tai koulutustarve myöhemmässä vaiheessa, jos jo tässä vaiheessa havaitaan, että henkilöstöä tai osaamista ei ole riittävästi.
- Organisaatioyksiköiden vetäjien kanssa on sovittava tietoturvaryhmään kuuluvista henkilöistä ja heidän ajankäytöstään mahdollisessa tietoturvatoiminnassa.
- Määritellään budjetti ja rahalliset resurssit.
  - On varattava riittävästi rahaa ja muita tarvittavia aineellisia resursseja tietoturvatoiminnan kehittämiseen ja päivittäiseen organisointiin.
- Varataan johtajan käyttämät resurssit ja tarvittaessa johtoryhmältä vaadittavat resurssit (henkilöt, aika).
  - Johdon täytyy varata riittävästi aikaa johtamiseen, raportteihin tutustumiseen ja tietoturvan seurantakokouksiin. Johtamistoimintaan oikein delegoimalla ja vastuita jakamalla riittänee yksi tai kaksi henkilötyöpäivää kalenterivuodessa; alkuvaiheessa aikaa saatetaan tarvita enemmän.
- Muita tarvittavia resursseja ovat esimerkiksi:
  - fyysiset tilat (konesalit, ”laboratorio” testausta ja harjoittelua varten, koulutusluokka ym.),
  - järjestelmät (esimerkiksi varmistuslaitteistot, kulunvalvonnan laitteet ja ohjelmistot, tarvittavat turvajärjestelmät verkkohyökkäyksiltä suojautumiseen),
  - proaktiiviset tietoturvan valvonta-, hälytys- ja raportointivälineet ja -palvelut,
  - riskienhallintaprosessia tukevat välineet,
  - tietoturvaportaalin tarjoamisessa tarvittavat välineet ja palvelut, sekä
  - CERT-toiminnassa tarvittavat työkalut.

Tehtävä 17. Määritellään prosessi, jota noudatetaan tietoturvan hallinnoinnissa. Tässä tehtävässä prosessin vaiheet määritellään yksityiskohtaisesti. Prosessin kulku on määritelty jo aiemmin tehtävässä 9.

- Prosessin yksityiskohtainen kuvaus on esitetty tämän dokumentin osiossa 3. Kukin prosessin vaihe voi toimia itsenäisesti muista riippumatta.
  - Esimerkiksi vaiheen toteutus työtehtäviä suoritetaan usein päivittäisenä toimintana ilman erillistä käynnistintä.
  - Vaihetarkastus suoritetaan myös säännöllisesti, vaikka mitään muutoksia ei olisikaan prosessissa (suunnittelu, toteutus). Tässä vaiheessa seurataan ja mitataan tietoturvan toteutumista.
  - Vaihekehitys puolestaan käynnistyy ainoastaan vaiheen tarkastus käynnistämänä.

5 OSIO 3: HALLINNOINTIPROSESSI

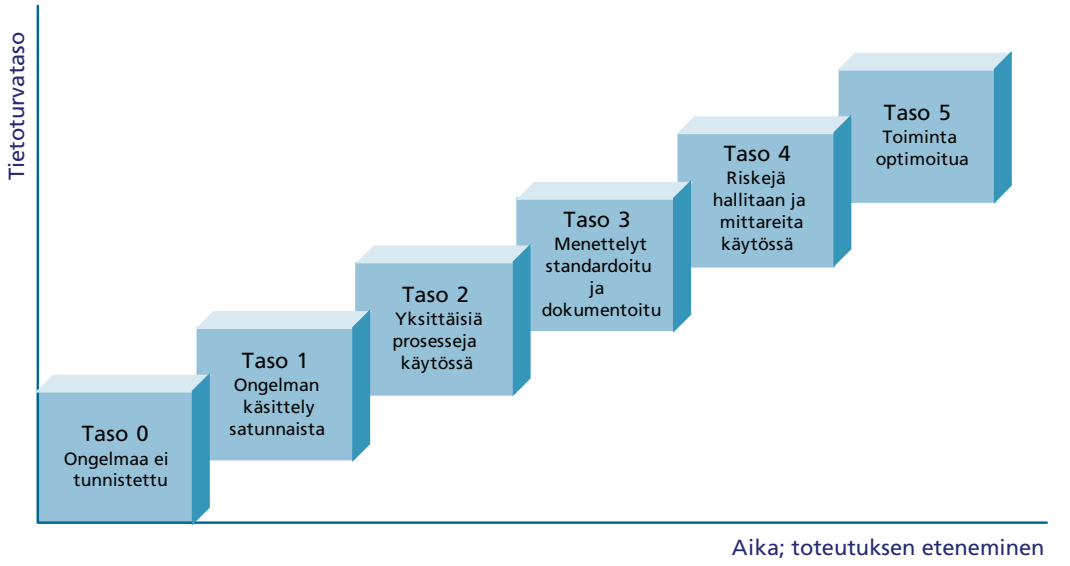
5.1 Tietoturvan hallinnointiprosessi

Tietoturvan hallinnointiprosessi on pyritty kuvaamaan sellaiselle tarkkuustasolle, että malli on otettavissa sopivilla muutoksilla ja lisäyksillä käyttöön valtaosassa erilaisia ja erikokoisia organisaatioita.

Prosessin vaiheet käyvät ilmi jäljempänä esitetystä kuvasta 5 luvussa 5.2. Vaiheet sisältävät muun muassa seuraavat tietoturvan kehittämisessä ja ylläpidossa tarvittavat osa-alueet:

- Tietojen turvaluokittelu.
- Uhka- ja riskianalyysin teko.
- Politiikkojen, ohjeiden ja sääntöjen kirjaus/laatiminen.
- Koulutuksen ja tietoturvatietoisuuskampanjoiden suunnittelu ja toteutus.
- Suojausmenettelyiden ja turvamekanismien, kontrollien, valinta ja toteutus.
- Säännöllinen seuranta ja raportointi.
- Tietoturvan toteutumisen arviointi ja tarvittavien muutosten toteutus.

Tietoturvan hallinnoinnin kypsyysmalli ja sen eri tasot käy ilmi kuvasta 4. Kuva ilmentää tietoturvatason paranemisen, joka saavutetaan tietoturvaongelmien hallinnoinnin ja käsittelyn menettelytapojen suunnittelulla ja kehittämisellä.



KUVA 4. Tietoturvahallinnoinnin kypsyysmalli

Tässä oppaassa ei ole esitetty menetelmiä tai työkaluja tietoturvahallinnoinnissa käytettävän prosessin mittaamisen tueksi. Yleisohjeena voidaan kuitenkin todeta, että yksi esimerkki hyvästä tavasta mitata hallinnointiprosessia on käyttää eräänlaista kypsyysmallia (*CMM, capability maturity model*). Kypsyysmallissa mitataan, missä määrin organisaatio on saavuttanut sen tietoturvatoiminnalle asetetut tavoitteet, toisin sanoen kuinka hallinnointiprosessi vastaa tietoturvatoimintaan

kohdistuviin vaatimuksiin. Kypsyysmallin tasoja organisaation tietoturvaongelmien ratkaisussa – eli käytännössä organisaation tietoturvahallinnoinnin prosessissa – voivat olla esimerkiksi:

- Taso 0: Organisaatio ei ole tunnistanut ongelman (tai kehitettävän kohteen) olemassaoloa, joten mitään toimintaperiaatteita, prosesseja tai mittareita ei ole luotu tai käytössä.
- Taso 1: Ongelma on alustavasti tunnistettu, mutta käsittely on satunnaista tai epäjohdonmukaista, toimintaperiaatteet ovat summittaisia ja ratkaisuja tuotetaan yksittäisiin tarpeisiin tapauskohtaisesti. Seurantaa harjoitetaan vain reaktiivisesti.
- Taso 2: Ongelma on tiedostettu koko organisaatiossa, ja toimintaperiaate on luotu. Ongelman käsittelyä varten on luotu prosessit, mutta ne eivät ole koko organisaation laajuisessa käytössä, vaan pikemminkin yksittäisten henkilöiden vastuulla. Mittaamisen tarve on periaatetasolla tunnistettu, mutta mittaaminen on satunnaista ja kehitysasteella.
- Taso 3: Ongelman ratkaisun tarve on ymmärretty ja hyväksytty, ja periaatteet on linjattu yhteensopiviksi organisaation muiden toimintaperiaatteiden kanssa. Menettelyt ja toimintatavat on standardoitu, dokumentoitu ja toteutettu koko organisaatiossa. Tällöin myös tarvittavaa koulutusta järjestetään organisaation henkilöstölle. Toiminnan mittareita on kehitetty ja seurataan, mutta seurannassa ei analysoida tapahtumien syitä eikä seurantatietoja oteta huomioon prosessien kehityksessä.
- Taso 4: Kuten tasolla 3, ongelman ratkaisun tarve on ymmärretty ja hyväksytty, ja periaatteet ja toteutus on organisaation laajuisesti käytössä. Riskien hallinta on otettu huomioon hallinnoinnissa, ongelmien käsittelyssä ja prosessin kehittämisessä. Prosessiin osallistuvat henkilöt on koulutettu ja he ovat tietoisia uhkista, riskeistä ja vaihtoehdoista. Prosesseja parannetaan mittareiden tuottamiin tuloksiin pohjautuen, poikkeamat ja tulosten raja-arvot on määritelty.
- Taso 5: Edellisen tason 4 toteuman pohjalta organisaation tietoturvahallinnoinnin kehitystyö suuntautuu tulevaan. Periaatteiden, toimintatapojen ja prosessien kehityksen apuna käytetään vertailua myös ulkopuolisiin tahoihin (eri standardien kehitys ja vertailuryhmät, benchmarking), jonka mukaan optimoidaan omaa toimintaa. Ulkoisia asiantuntijoita käytetään vertailukohtien saamiseksi.

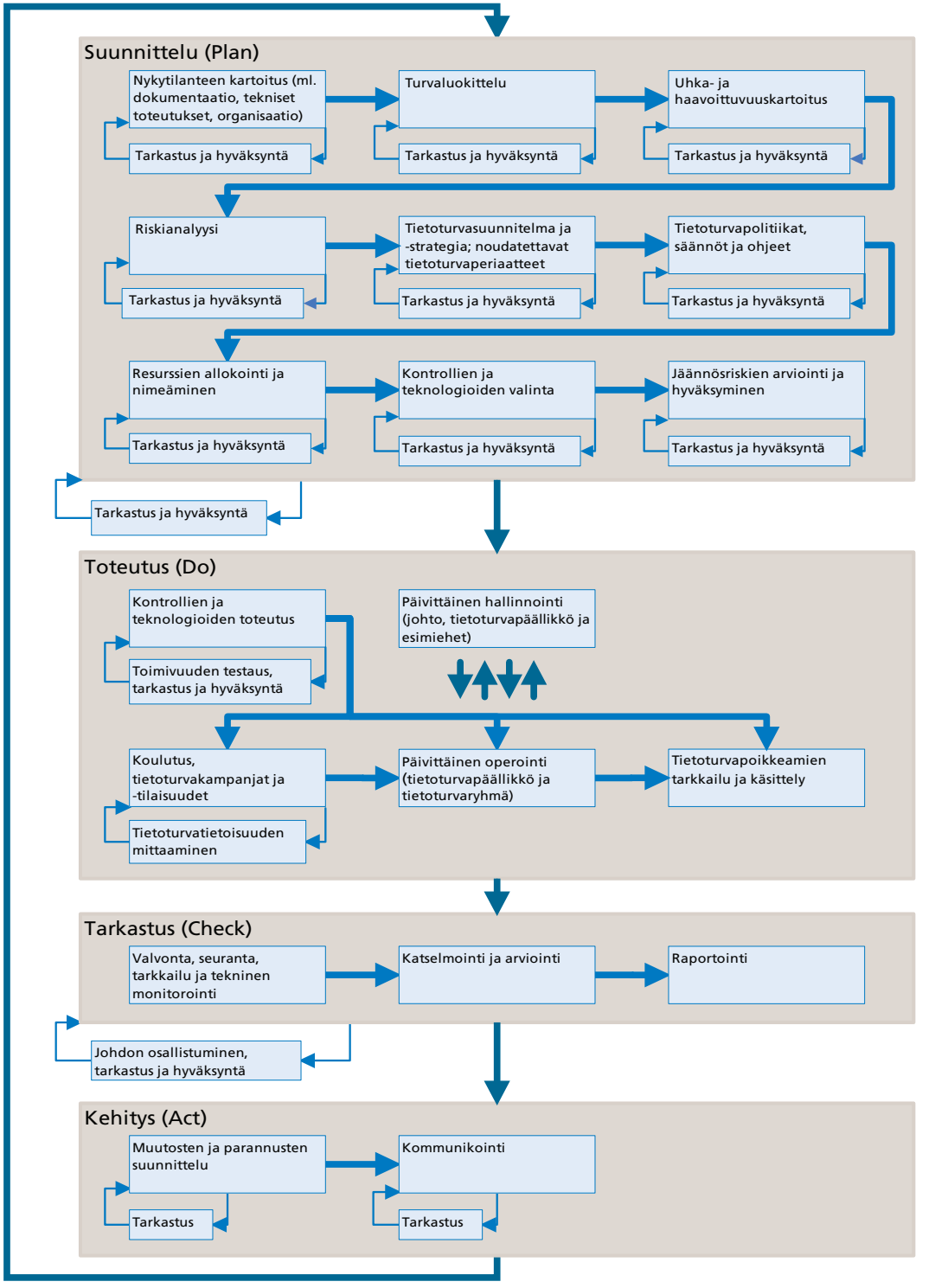
5.2 Tietoturvan hallinnointiprosessin vaiheet

Kussakin seuraavassa kappaleessa on kiteytys prosessin eri vaiheissa suoritettavista tehtävistä. Prosessi on kuvattu kuvassa 5. Kuva selventää hallinnointiprosessin eri vaiheita ja niiden välisiä suhteita. Prosesseja ei ole kuvattu yksityiskohtaisesti; kukin organisaatio voi suunnitella kunkin prosessin yksityiskohdat oman organisaationsa toimintamahdollisuuksien mukaisesti.

Vaiheen *Suunnittelu* prosesseissa luodaan raamit ja säännöt organisaation tietoturvallisuuden hoidolle. Valittuja periaatteita toteutetaan vaiheessa *Toteutus*, seurataan ja tarkastetaan vaiheessa *Tarkastus* ja muutostarpeet arvioidaan ja suunnitellaan vaiheessa *Kehitys*. Vaiheessa *Toteutus* suoritetaan organisaation päivittäiset ja säännölliset tietoturvatoimet vaiheessa *Suunnittelu* luotujen kehysten perusteella.

Vaiheessa *Tarkastus* valvotaan ja arvioidaan organisaation tietoturvallisuuden tilaa kokonaisuudessaan, raportoidaan tietoturvasta tarvittavassa laajuudessa ja hankitaan tietoturvatoiminnalle valittu sertifiointi. Arvioinnin lopputuloksena tiedetään organisaation tietoturvahallinnoinnin (ISMS) kelpaavuus ja toimintakyky asetettuihin vaatimuksiin nähden, ja sen perusteella voidaan suunnitella ja toteuttaa tarvittavat muutokset hallinnointiprosesseihin.

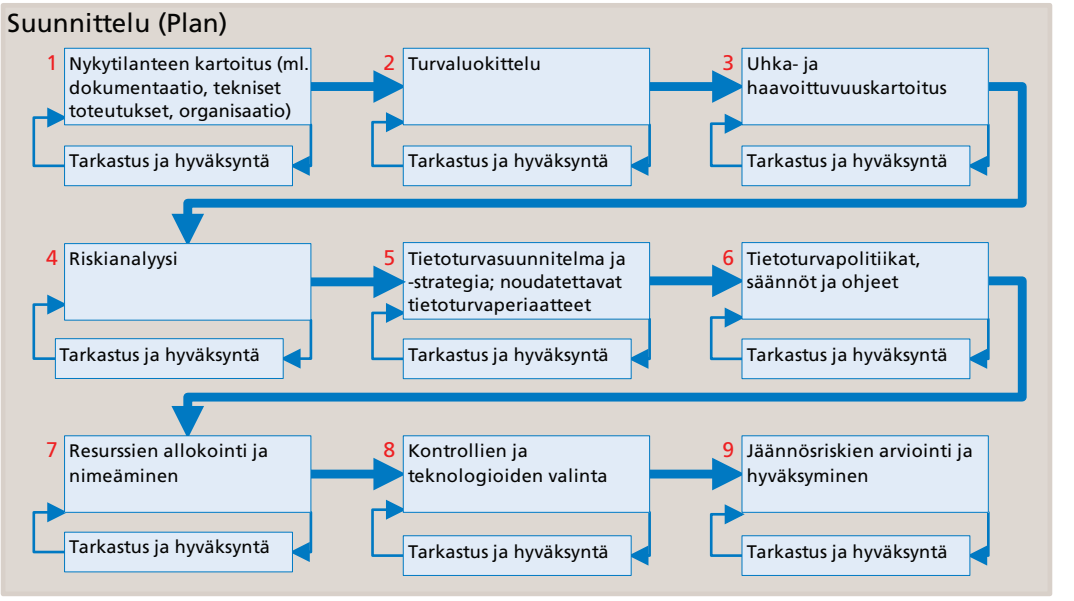
Vaihe *Kehitys* täydentää syklisen prosessin kehän: siinä arvioidaan tarvittavat muutokset, jotka aloittavat ja joita käsitellään uudessa syklissä prosessista *Suunnittelu* alkaen.



KUVA 5. Hallinnointiprosessi ja eri vaiheiden tehtävät

Suunnittelu

Vaiheen *Suunnittelu* prosesseissa luodaan raamit ja säännöt organisaation tietoturvallisuuden hoidolle. Valittuja periaatteita toteutetaan vaiheessa *Toteutus*, seurataan ja tarkastetaan vaiheessa *Tarkastus* ja muutostarpeet arvioidaan ja suunnitellaan vaiheessa *Kehitys*.



KUVA 6. Hallinnointiprosessi: tehtävät vaiheessa Suunnittelu

5.2.1 Nykytilanteen kartoitus

Prosessissa selvitetään organisaation tietoturvan nykytila ja tavoitteet. Kuva nykytilasta luodaan katsastamalla toiminta esimerkiksi olemassa olevien dokumenttien, lokien ja erikseen tehtävien haastattelujen perusteella. Organisaation tietoturvatavoitteet selviävät dokumentista, joka on laadittu kehittämisprojektin vaiheessa 3.

Prosessissa hyödynnetään olemassa olevia dokumentteja, joita ovat esimerkiksi:

- toimintaa (tai liiketoimintaa) kuvaavat dokumentit,
- organisaatiota ja sen rakennetta kuvaavat dokumentit,
- organisaation osien tai tilojen sijaintia kuvaavat dokumentit,
- teknologia- ja tietojärjestelmäkuvaukset,
- organisaation prosessikuvaukset,
- tietoturvatavoitteet, -strategia, -periaatteet ja -politiikat,
- yhteistyösuhteisiin ja -kumppaneihin liittyvät dokumentit,
- voimassa olevat sopimukset sekä
- lait, säädökset ja standardit, joita organisaation on noudatettava.

Prosessissa syntyy organisaation tietoturvan nykytilanteen kuvaava dokumentti, joka palvelee jatkossa erityisesti tietoturvatoimenpiteiden suunnittelua. Lisäksi voi syntyä mahdollisia tarpeita edellä mainittujen asiakirjojen päivittämiseen ajan tasalle.

Prosessi tarkastetaan ja hyväksytään sisäisessä menettelyssä, jossa tarkastetaan nykytilannekuvaus ja mahdollisesti pöytäkirjoja. Tarkastustyö on osa sisäistä laadunvalvontaa ja edellytys, jos organisaation tietoturvatoiminnalle hankitaan ulkoinen sertifiointi.

5.2.2 Turvaluokittelu

Tässä vaiheessa turvaluokitellaan tiedot ja tietojärjestelmät sekä määritellään niiden tärkeys, jotta myöhemmin voidaan suunnitella tietojen suojaus. Tarvittavia toimenpiteitä ovat esimerkiksi:

- Tunnistetaan suojattavat tiedot ja tietojärjestelmät.
- Kuvataan lyhyesti kunkin suojattavan kohteen ominaisuudet, esimerkiksi
  - tyyppi (tietojärjestelmä, palvelu, tietokanta, ohjelmistoresurssi, paperidokumentti ym.),
  - säilytystapa (tiedostojärjestelmä tai tietokanta, cd-levy tai nauha, muu media ym.),
  - säilytyksen kesto ja tuhoamiselle asetetut vaatimukset,
  - käyttötarkoitus,
  - muoto tai formaatti (tiedon rakenteen kuvaus tai standardi tai mahdollisesti ohjelmisto, jolla tietoja voidaan käsitellä) sekä
  - sijainti.
- Tunnistetaan ja nimetään jokaiselle suojattavalle kohteelle omistaja. Omistaja määrittelee tiedoille haltijan (tekninen vastuu; custodian).
- Määritetään jokaisen suojattavan kohteen tärkeys ja arvo (sikäli, kun se pystytään määrittämään). Tärkeys voidaan jakaa esimerkiksi luokkiin
  - erittäin tärkeä,
  - tärkeä ja
  - ei-tärkeä.

Sosiaali- ja terveydenhuollossa luokittelu on kohtuullisen yksinkertaista – kaikki henkilötiedot ovat pääsääntöisesti joko erittäin tärkeitä tai tärkeitä. Muiden käytettävien tietojen (esimerkiksi yhteistyökumppaneiden tiedot ja organisaation omat asiakirjat) luokittelu vaatii enemmän työtä ja on luultavasti tehtävä organisaatiokohtaisesti.

- Määritetään jokaisen suojattavan kohteen kriittisyys ja riskitaso (tiedon tärkeys suhteessa tietoturvaloukkausten seurauksiin).
- Määritetään tietojen luottamuksellisuus. Tietojen salaisuuden aste voi terveydenhuollossa olla tyypillisesti joko julkinen tai salassa pidettävä. Salassa pidettävän tiedon luottamuksellisuuden taso esimerkiksi potilastietojen osalta on luottamuksellinen, jolloin vain oikeutetuilla tahoilla tulee olla pääsy tietoihin (siinä laajuudessa ja käyttötarkoituksessa kuin on säädetty). On huomattava, että terveydenhuollossa on käsiteltävä salassa pidettävinä myös muita tietoja kuin potilastietoja: näitä ovat esimerkiksi henkilöstöön liittyvät tiedot. Organisaatiossa on oltava selkeät käsittelysäännöt kaikille tiedoille ja asiakirjoille erilaisilla luottamuksellisuuden tasoilla, ja sääntöjen on koskettava kaikkia tietojen ja asiakirjojen elinvaiheita.
- Määritetään ne tahot, jotka tarvitsevat pääsyn tietoihin (sikäli, kun se tässä vaiheessa voidaan määrittää), missä laajuudessa ja millaisilla valtuuksilla pääsy myönnetään.
- Tunnistetaan prosessit, joissa tietoja käsitellään tai tarvitsee käsitellä (sikäli, kun se tässä vaiheessa voidaan määrittää). Tämä liittyy jo ylempänä mainittuihin ominaisuuksien kuvaamiseen.

Yllä mainitut ominaisuudet voidaan kirjata turvaluokitukseksi esimerkiksi erilliseen taulukkoon. Prosessin lopputuloksena onkin organisaation tiedot kattava turvaluokitus, josta ilmenee suojattavat tiedot, niiden tärkeys ja muut edellä mainitut seikat. Turvaluokitus sisältää mahdollisuuksien

mukaan pääsynhallintaluettelon. Prosessin tuloksena voi mahdollisesti syntyä myös päivitetty omaisuusluettelo.

Prosessissa hyödynnettäviä olemassa olevia dokumentteja ovat esimerkiksi:
- luettelo tiedoista (tai omaisuusluettelo, list of assets; inventory of assets), sekä
- aiemmin laadittu tietojen turvaluokitus.

Yksi oleellinen kysymys on, miten tietojen arvo arvioidaan. Koska monilla tiedoilla ei käytännössä ole rahallista arvoa, on käytettävä ”maalaisjärkeä”. Etenkin julkishallinnossa monet vaatimukset ovat juridisia, laeilla säädettyjä, eivätkä niinkään taloudellisia, joten arvon määrittämisessä on käytettävä ensisijaisena mittarina tärkeyttä. Esimerkiksi henkilö- ja potilastiedot ovat tärkeitä ja suojattavia tietoja, vaikka niille ei taloudellista arvoa myöhempää riskianalyysiä ajatellen voidakaan määrittää.

Prosessi tarkastetaan ja hyväksytään sisäisessä menettelyssä, jossa tarkastetaan esimerkiksi tietty otos prosessin tehtävistä tutustumalla laadittuihin asiakirjoihin, lokitietoihin ja pöytäkirjoihin. Tarkastustyö kuuluu osaksi sisäistä laadunvalvontaa, mutta se voi palvella myös ulkoista tietoturvasertifiointia.

5.2.3 Uhkien ja haavoittuvuuksien kartoitus

Tässä vaiheessa tunnistetaan ja arvioidaan haavoittuvuudet ja uhkat. Uhkia voidaan selvittää esimerkiksi vastuuhenkilöille ja käyttäjille tehtävillä kyselyillä, tutustumalla tiedossa oleviin uhkiin (esimerkiksi CERT:n raportit teknologioihin liittyen), tutustumalla organisaation toiminta-, prosessi- ja järjestelmäkuvauksiin sekä suunnitelmallisella testauksella. Apuna käytettäviä tietoja ja dokumentteja ovat esimerkiksi:
- valvontatiedot ja raportit,
- käyttäjiltä tulleet tiedot, kuten palautteet ja reklamaatiot,
- julkiset haavoittuvuustiedot (valmistajien, muiden tahojen tai CERT:n julkaisemat),
- valmiit kysymyslistat esimerkiksi johdolle, vastuuhenkilöille ja käyttäjille,
- vastuuhenkilöille esitettyjen kysymysten vastaukset,
- olemassa olevat prosessikuvaukset sekä
- olemassa olevat määrittelyt, ohjeet ja arkkitehtuurikuvaukset.

Testausmenettelyinä voidaan käyttää esimerkiksi:
- skannauksia,
- järjestelmä-, verkko- tai palvelukohtaisia tunkeutumistestejä,
- haavoittuvuustestausta sekä
- rasitus- ja kuormitustestejä.

On myös otettava huomioon sellaiset toistuvat tai jatkuvasti voimassa olevat (mutta muuttuvat) uhkat, jotka eivät sinänsä liity organisaation toimintaan. Näitä ovat esimerkiksi verkkohyökkäykset ja virukset, jotka uhkaavat jokaista organisaatiota: uhkien tekniikka muuttuu, mutta uhkan luonne ei. Myös kertaluonteiset uhkat esimerkiksi projekteissa on huomioitava.

Prosessissa syntyy kartoitus ja analyysi haavoittuvuuksista ja uhkista, jotka kohdistuvat organisaatioon tai sen omistamiin tai hallussa pitämiin suojattaviksi luokiteltuihin tietoihin.

Prosessi tarkastetaan ja hyväksytään sisäisessä menettelyssä, jossa tarkastetaan esimerkiksi tietty otos prosessin tehtävistä tutustumalla uhkakartoituksen menetelmiin ja dokumentteihin, esimerkiksi laadittuihin pöytäkirjoihin, raportteihin ja uhkakartoitukseen.

5.2.4 Riskien analysointi

Tässä vaiheessa analysoidaan riskit. Ne tunnistetaan kullekin kohteelle (suojattavat tiedot) ja arvioidaan vertaamalla riskejä – uhkien ja haavoittuvuuksien toteutumisen todennäköisyyttä ja vaikutusten seurauksia – kohteen tärkeyteen ja kriittisyyteen. Oleellista on, että tunnistetaan mahdollisten tietoturvaloukkausten (haavoittuvuudet ja uhkat) vaikutus. Tarkan arvion tekeminen voi olla vaikeaa tai mahdotonta, joten yleensä summittainen arvio riittää oikeiden tai riittävien suojaustoimenpiteiden määrittämiseksi. Prosessissa käytettäviä dokumentteja ovat ensisijaisesti turvaluokittelu ja kartoitus uhkista ja haavoittuvuuksista.

Riskien hallintaan liittyen on olemassa erilaisia matemaattisia malleja. Koska ensinnäkin sosiaali- ja terveydenhuollossa tietojen arvon rahallinen määrittäminen tai vertailukohtien löytäminen voi olla vaikeaa tai mahdotonta, ja toiseksi hajautettuihin tietojärjestelmiin ja tietoverkkoihin liittyvien riskien (jolloin identtisiä tietoja saatetaan käsitellä ja säilyttää useissa eri organisaatioissa) todennäköisyyden arviointi voi olla yhtä vaikeaa, tässä dokumentissa ei ole esitetty laskennallista mallia riskianalyysin tekoon ja prioriteetin valintaan. Päinvastoin, ”talonpoikaisjärjen” käyttöä suositellaan ensisijaisena vaihtoehtona.

Prosessissa syntyy riskianalyysi, joka sisältää tarvittavan yksityiskohtaisen tiedon kaikista sellaisista organisaation tiedoista, joihin kohdistuu sellaisia uhkia, joihin on syytä varautua tai joilta pitää suojautua. Riskien seurauksista – tietoturvaloukkausten seurauksista – laaditaan vaikutuskartoitus (*impact analysis*), joka kertoo toteutuneiden riskien vaikutuksen organisaation toimintaan ja tietoturvaan. Erillisiä vaikutuskartoituksia tietoturvan eri osa-alueisiin, kuten luottamuksellisuuteen, eheyteen tai saatavuuteen, voidaan tehdä tarvittaessa. Yleensä uhka tai haavoittuvuus kuitenkin kohdistuu luonteensa vuoksi johonkin tiettyyn näistä (sähkökatkos vaikuttaa lähinnä saatavuuteen, tulosteiden jättäminen työpöydälle lähinnä luottamuksellisuuteen), joten vaikutuksen erikseen analysointi on usein turhaa. Lisäksi sosiaali- ja terveydenhuollossa tietojen luottamuksellisuuden säilymistä on suojattava jo lakien vaatimuksista johtuen samalla tärkeysasteella kuin tietojen saatavuutta ja eheyttäkin (esimerkiksi säilyminen, käytettävyys ja muuttumattomuus). Seuraavassa on muutama esimerkki riskianalysoinnin toimenpiteistä.

1) Arvioidaan riskin todennäköisyys, joka voidaan jakaa karkeasti arvioiden esimerkiksi neljään luokkaan:
   - korkea,
   - keskimääräinen,
   - alhainen ja
   - ei merkitystä.

   Näistä kaksi ensimmäistä sisältävät runsaasti tyypillisiä uhkia ja haavoittuvuuksia, kuten verkkohyökkäykset ja virukset, henkilöiden tekemät väärinkäytökset ja inhimilliset virheet, sähkökatkokset ja tietojärjestelmien vikaantumiset. Esimerkki alhaisesta todennäköisyydestä on tulipalo. Koska tulipalon seurausten vakavuus on kuitenkin suuri, siihen täytyy organisaatiossa varautua. Suomen oloissa luokkaan ”ei merkitystä” kuuluu suurin osa erilaisista luonnonkatastrofeista, jolloin kyseisiltä riskeiltä ei suojauduta lainkaan. On kuitenkin tärkeää huomata, että tietyt erittäin epätodennäköiset tapahtumat, kuten sairauksiin liittyvät epidemiat tai maanlaajuiseen tai alueelliseen sähkönjakeluun liittyvät häiriöt, voivat aiheuttaa niin vakavia seuraamuksia, että niihin on tarpeen varautua muihin uhkiin varautumisen yhteydessä – esimerkiksi normaalien varamiehityksen ja varasähkön järjestämisen yhteydessä.

   Riskin todennäköisyyden arvioinnin yhteydessä on hyvä arvioida myös riskin toteutumisaika: kuinka kauan kestää, että uhka konkretisoituu. Esimerkiksi teknisten laitteiden vioittumisen tai toimintakyvyn loppumisen todennäköisyys on pitkällä aikavälillä 1. On

tyypillistä, että samoin kuin teknisten laitteiden hidasta vioittumista, myöskään organisaation toimintakulttuureihin liittyvän rappeutumisen vaikutuksia ei heti huomata.

2) Määritetään riskiluokat. Riskianalyysissä verrataan tietojen suojaamisen kriittisyyttä (tietojen turvaluokittelu ja tietojen tärkeys) riskin toteutumisen todennäköisyyteen (edellä) ja seurausten vakavuuteen (vaikutuskartoituksen tulokset). Lopputuloksena saadaan esimerkiksi riskiluokat
   - sietämätön riski,
   - merkittävä riski,
   - kohtalainen riski,
   - vähäinen riski ja
   - merkityksetön riski.

3) Tietojen suojaamisen menettelyiden helpottamiseksi organisaatioon on syytä määrittää suojaustasot sopivaksi katsotulla tarkkuudella, esimerkiksi jakamalla suojaustaso numeroituihin luokkiin yhdestä neljään. Tällöin kukin suojaustaso käsittää tietyt menettelyt ja tekniset toteutukset. Kun kukin suojattava tieto nimetään tiettyyn suojaustasoon, tiedetään myös, miten kunkin tiedon suojaaminen on toteutettu. Suojaustasoista voidaan luonnollisesti poiketa. Niiden valinta etukäteen helpottaa kuitenkin tietoturvallisuusjärjestelyiden toteuttamista.

   Eri suojaustasoissa noudatettavat menettelyt ja tekniset toimet voidaan määritellä myöhemmin (esimerkiksi kohdassa 5.2.8, kontrollien ja teknologioiden valinta). Edellä mainitun riskianalyysin perusteella kullekin tiedolle valitaan suojaustaso esimerkiksi seuraavalla tavalla:
   - sietämätön riski: suojaustaso 1
   - merkittävä riski: suojaustaso 2
   - kohtalainen riski: suojaustaso 3
   - vähäinen riski: suojaustaso 4.

   Suojaustaso 4 sisältää esimerkiksi kulunvalvontaan, fyysisiin tiloihin ja tietoverkkoihin liittyviä toimenpiteitä, joita noudatetaan kaikissa organisaation tiloissa ja kaikissa organisaation tietoverkkoihin kytketyissä tietojärjestelmissä. Suojaustaso 3 voi sisältää kovennettuja menettelyitä esimerkiksi sähkövirran saatavuuteen ja varavoimaan, tietojärjestelmiin sisään kirjautumiseen, varmuuskopiointiin tai tiedon salaukseen (erityisesti kannettavat tietokoneet) liittyen. Suojaustaso 2 sisältää esimerkiksi normaaleihin konesalitiloihin liittyviä määräyksiä, toimenpiteitä sekä niissä noudatettavia menettelyitä ja suojaustaso 1 korkean turvallisuuden konesaleihin, varalaitteisiin sekä varatiloihin liittyviä menettelyitä.

   Riskianalyysin ja vaikutuskartoituksen perusteella valitaan siis ne toimenpiteet ja menetelmät, joilla riskit voidaan välttää, joilla niiltä voidaan suojautua kokonaan tai osittain, tai joilla riskiä voidaan siirtää muille tahoille esimerkiksi sopimuksellisesti. Osa riskeistä jätetään tarkoituksellisesti huomioimatta ja hyväksytään sellaisenaan ilman suojaustoimenpiteitä; tämä koskee erityisesti erittäin epätodennäköisiä riskejä todennäköisyydellä "ei merkitystä".

4) Riskeiltä suojauduttaessa jäljelle jäävät jäännösriskit arvioidaan ja hyväksytään myöhemmin erikseen määritellyillä toimilla.

   Prosessi tarkastetaan ja hyväksytään sisäisessä menettelyssä, jossa tarkastetaan esimerkiksi tietty otos riskianalyysistä ja laadituista pöytäkirjoista. Tarkastuksessa on hyvä käyttää myös aiempia riskianalyysejä ja tietoa toteutuneista riskeistä: tämä kertoo, onko riskit tunnistettu ja analysoitu käyttämällä oikeita perusteluita, ja onko riskeiltä onnistuttu suojautumaan

suunnitellun mukaisesti. Sellaisten riskien ei pitäisi toteutua, jotka on analysoitu ja joilta organisaatiossa on suunniteltu suojauduttavan.

5.2.5 Tietoturvasuunnitelman laatiminen

Tässä vaiheessa laaditaan tietoturvasuunnitelma organisaatioon kohdistuvien vaatimusten, suojattavien tietojen ja tiedossa olevien riskien perusteella. Tietoturvasuunnitelman laadinnassa käytetään apuna riskianalyysin ja vaikuttavuuskartoituksen lisäksi kehittämisprojektin vaiheessa 3 laadittuja dokumentteja (esimerkiksi tietoturvatavoitteet, -strategia, -periaatteet ja -politiikat).

Prosessissa laadittava tietoturvasuunnitelma linjaa sopivan yksityiskohtaisesti ne toimenpiteet, joita suoritetaan päivittäisessä ja säännöllisessä tietoturvatoiminnassa. Toimenpiteillä suojaudutaan niiltä riskeiltä, jotka riskianalyysissä on todettu niin vakaviksi, että niiltä pitää organisaatiossa suojautua.

Tietoturvasuunnitelmassa määritellään esimerkiksi:

- osallistuvat henkilöt tai organisaatioyksiköt sekä heidän vastuunsa,
- riittävän yksityiskohtaiset toimenpiteiden ja tehtävien töiden kuvaukset (työsuunnitelmat),
- tehtäville asetetut prioriteetit,
- aikataulut sekä
- töiden tarkastuksen ja hyväksynnän menettelyt.

Jos tietoturvan hallinnoinnin prosessia (ISMS) tarvitsee kehittää, muutokset tehdään käytännössä tässä prosessissa. Muutostarpeet, jotka on todettu vaiheessa *Kehitys*, ja niiden toteutus suunnitellaan ISMS:iin. Myös organisaation tietoturvatavoitteita ja noudatettavia periaatteita voidaan tarvittaessa päivittää.

Tässä prosessissa syntyy tai päivitetään organisaation dokumentit ”tietoturvasuunnitelma” ja ”tietoturvastrategia”.

Prosessi tarkastetaan ja hyväksytään sisäisessä menettelyssä, jossa tarkastetaan esimerkiksi tietty osa tietoturvasuunnitelmasta ja varmistetaan vastaavuus organisaatiolle asetettuihin tavoitteisiin ja organisaatioon kohdistuviin ulkopuolisiin vaatimuksiin. Tarkastus on tärkeää: mahdollisten virheiden ja puutteiden löytäminen tietoturvasuunnitelmassa vähentää mahdollisuutta riskien toteutumiselle joko vääränlaisesta tai puutteellisesta suojauksesta johtuen.

5.2.6 Politiikkojen, sääntöjen ja ohjeiden laatiminen

Tässä vaiheessa laaditaan politiikat, säännöt ja ohjeistus (kaikki sellainen ohjeistus, mikä voidaan tässä vaiheessa laatia). Seuraavat toimenpiteet sisältyvät tähän vaiheeseen:

- Arvioidaan voimassa olevien politiikkojen ja sääntöjen kelpaavuus.
- Päivitetään asiakirjat tarvittaessa ajan tasalle tai muuttuneiden vaatimusten mukaisiksi.
- Tutustutaan alihankkijoiden (esimerkiksi järjestelmä- ja sovellustoimittajat) ohjeisiin ja manuaaleihin.
- Laaditaan kaikki sellaiset politiikat, säännöt ja ohjeet, joita tarvitaan tietoturvan hoitamisessa suunnitellussa laajuudessa ja sovitulla tasolla.
- Laaditaan suunnitelmat, proseduurit ja tarvittavat muut dokumentit (esimerkiksi tarkastuslistat), millä hallinnointiprosessia ja sen eri osat tarkastetaan ja arvioidaan.
- Laaditaan tietoturvakäsikirja ja varmistetaan, että se on jaettu kaikille organisaatiossa työskenteleville.
- Tiedotetaan ja koulutetaan kaikki politiikat, säännöt, ohjeet ja muutokset koko henkilöstölle.

Prosessissa käytettäviä dokumentteja ovat esimerkiksi edellisissä vaiheissa syntyneet riskianalyysi, vaikutuskartoitus ja tietoturvasuunnitelma. Myös kehittämisprojektissa syntyneet asiakirjat on huomioitava, ja niitä on käytettävä apuna politiikkojen ja sääntöjen laatimisessa. Organisaatiossa käytettävien tietojen erilaiset suojaustasot (kuten on mainittu kohdassa 5.2.4, riskien analysointi) ja menettelyt kussakin suojaustasossa voidaan alustavasti sopia tässä vaiheessa, vaikka varsinaisesti suojaustasot määritetään vaiheessa 5.2.8, kontrollien ja teknologioiden valinta.

Prosessi tarkastetaan ja hyväksytään sisäisessä menettelyssä, jossa tarkastetaan esimerkiksi tietty osa laadituista politiikoista ja ohjeista, ja varmistetaan niiden vastaavuus asetettuihin tavoitteisiin nähden.

5.2.7 Resurssien varaus ja nimeäminen

Johdon toimia aliprosesseissa ovat (jotka pitää jyvittää oikeisiin aliprosesseihin):
- Vastuiden määrittäminen.
- Resurssien varaus ja nimeäminen.

Budjetoinnissa ja sen suunnittelussa on otettava huomioon, että tarvittavia resursseja ovat esimerkiksi
- henkilöresurssit ja työntekijöiden tietoturvan hoitoon käyttämä aika (henkilöstöbudjetti),
- tietoturvan hoidossa tarvittavat työkalut, kuten ohjelmistot, laitteistot, tilat ja muut tarvikkeet (rahan varaaminen budjetissa),
- aineettomat resurssit, kuten koulutus ja osaamisen ylläpitäminen (henkilöstöbudjetti ja ajankäytön suunnittelu).

Tässä oppaassa ei puututa yllä mainittua enempää resurssien varaamisen toimenpiteisiin.

Resurssien varaamista ja budjetointia sekä niiden onnistumista voidaan arvioida esimerkiksi seuraamalla sekä henkilöstön, erityisesti asiantuntijoiden, ajankäyttöä että taloudellisten mittareiden toteutumista.

5.2.8 Kontrollien ja teknologioiden valinta

Tässä vaiheessa valitaan käytettävät kontrollit, turvamekanismit (esimerkiksi valvonta- ja seurantamenettelyiden sekä hälytysten menettelyt). Valittujen kontrollien ja teknologioiden avulla suojaudutaan tietoturvauhkilta. Niillä seurataan, valvotaan ja raportoidaan tietoturvauhkista ja toteutuneista loukkauksista, ja niitä käytetään korjaus- ja toipumistilanteissa. Tässä dokumentissa ei ole kuvattu niitä erilaisia menettelyitä, joissa organisaatio voi valita omaan toimintaansa nähden parhaat kontrollit ja teknologiat, tai joissa niitä voidaan arvioida, eikä myöskään tietoa erilaisista tarjolla olevista vaihtoehdoista. Vaihtoehtoja ja yksityiskohtia on olemassa liikaa ja ne ovat liian teknisiä, jotta niitä voitaisiin tässä oppaassa käsitellä.

Oma huomionsa on kiinnitettävä ulkoisista toimijoista ja alihankkijoista aiheutuvien riskien torjuntaan ja kontrollien valintaan, kuten myös omaan ohjelmistokehitystoimintaan, mikäli sellaista organisaatiossa harjoitetaan.

Esimerkkejä kontrolleista on löydettävissä runsaasti: lukuisia erilaisia standardeja, ohjeita, suosituksia hyviksi käytännöiksi ja muita julkaisuja on saatavissa markkinoilta. Lähteenä voidaan käyttää esimerkiksi jo aiemmin mainittua Stakesin raportteja -sarjan julkaisua 5/2005 (Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt).

Kontrollien ja teknologioiden valinnan yhteydessä kirjataan tietoturvasuunnitelman ja riskianalyysin perusteella sopivat menettelyt erilaisille suojaustasoille. Organisaatiossa käytettävät tiedot voidaan siten suojata sopivalla tasolla niiden tärkeyden ja kriittisyyden perusteella. On luonnollista, että kaikkia tietoja ei voida luokitella yhteismitallisiin suojaustasoihin, mutta näiden käyttö voi helpottaa huomattavasti hallinnointia.

Tämän vaiheen tarkastus voidaan tehdä pistokoeluonteisesti esimerkiksi arvioimalla tiettyjen organisaation toimintojen suojaaminen valituilla kontrolleilla. Tarkastaminen voidaan toteuttaa esimerkiksi kuvitteellisilla uhkilla (”paperilla”) tai vaikkapa testaamalla joku valittu teknologia ja sen kyky suoriutua valitun kohteen suojaamisessa hyökkäyksiä vastaan.

5.2.9 Jäännösriskien hyväksyminen

Tässä prosessin vaiheessa arvioidaan, kirjataan ja hyväksytään ne riskit, joihin valitut kontrollit eivät vaikuta, ja joita vastaan valituilla kontrolleilla ei voida suojautua. Jäännösriskien tunnistaminen ja hyväksyminen on oleellinen osa riskien hallintaa: siinä

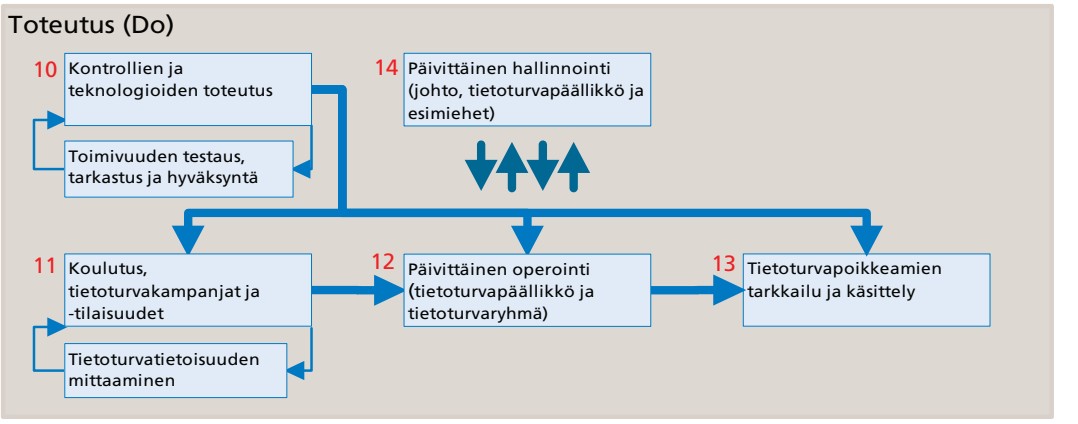
- tunnistetaan ne riskit, joiden suuruuden ei katsota yltävän sellaiselle riskitasolle, että niitä vastaan kannattaa suojautua, ja valitaan suojautumattomuus tietoisesti, sekä
- tunnistetaan ne valittujen suojaustoimien jälkeen jäljelle jäävät riskit, joihin suojautumistoimilla ei voida vaikuttaa ja joihin niillä ei tarvitse vaikuttaa, koska riskitaso katsotaan liian pieneksi. Suojautumattomuus myös näitä riskejä vastaan on tietoinen päätös.

Jäännösriskien hyväksyminen voidaan tarkastaa organisaatiossa sisäisesti samalla menettelytavalla kuin riskianalyysi: arvioimalla prosessin eteneminen esimerkiksi pöytäkirjoista, valitsemalla muutama riski uudelleen analysoitavaksi sekä arvioimalla aiempia riskianalyysejä ja vertaamalla niiden onnistumista toteutuneisiin riskeihin. Tarkastuksessa tulee havaita myös sellaiset riskit, joiden suuruus on arvioitu väärin ja asetettu tästä syystä jäännösriskeiksi. Lopputuloksena näiden riskien osalta saattaa olla uudelleen tehty riskianalyysi ja suojautumistoimenpiteiden suunnittelu.

Toteutus

Seuraavissa prosesseissa suoritetaan organisaation päivittäiset ja säännölliset tietoturvatoimet. Kehykset toiminnalle on määritelty jo aiemmin – tämä vaihe on olemassa olevien raamien mukaista toimintaa. Siksi vaihe Toteutus on itseohjautuva: esimerkiksi poikkeamien käsittelyssä havaitut seikat voivat aikaansaada muutoksia teknologioiden toteutukseen, jos nämä muutokset ovat sellaisia, että ne noudattavat voimassa olevaa toimintasuunnitelmaa eikä niitä siten tarvitse hyväksyttää erikseen tietoturvaryhmässä. Tällaisia asioita voivat olla esimerkiksi muutokset roskapostien käsittelyyn, virustorjunnan ja palomuurien asetuksiin, järjestelmien sisäänkirjauksen menettelyihin (kuten salasanojen pituudet tai vaihtoväli), etä- ja kotikäytön menettelyihin tai kulunvalvonnassa käytettävät toimintatavat. (Kuva 7.)

On tyypillistä – ja ISMS:n luonteeseen hyvin sopivaa – että toteutusvaiheen aliprosessit toimivat itsenäisesti niiden vaatimusten ja määrittelyiden mukaisesti, mitkä kullekin aliprosessille on luotu suunnitteluvaiheessa.



KUVA 7. Hallinnointiprosessi: tehtävät vaiheessa Toteutus

5.2.10 Kontrollien ja teknologioiden toteutus

Aiemmin on valittu kontrollit ja teknologiat organisaation suojaamiseksi. Tässä vaiheessa toteutetaan nämä valitut teknologiat ja kontrollit. Tässä dokumentissa ei ole kuvattu, miten näitä voidaan parhaiten toteuttaa. Erilaisia tähän yhteyteen sopivia standardeja ja ohjeita esimerkiksi tietojärjestelmien toteutukseen ja laadun varmistukseen liittyen on löydettävissä helposti Internetistä. Monet tällaiset standardit ja ohjeet ovat maksullisia.

Tässä vaiheessa laaditaan runsaasti erilaisia kontrolleihin ja teknologioihin liittyviä asiakirjoja ja dokumentteja. Osa dokumenteissa voidaan tuottaa myös vaiheessa 5.2.12 (päivittäinen operointi). Tuotettavia dokumentteja ovat esimerkiksi

- käyttöohjeet ja manuaalit,
- arkkitehtuuri- ja järjestelmäkuvaukset,
- työnkuvaukset ja proseduurit sekä
- lomakkeiden ja raporttien malliluonnokset (template).

Tämä vaihe on oleellinen myös muutosten hallinnassa. Vaiheessa tehdään myös tarvittavat muutokset ohjeisiin ja hallitaan muutoksia:

- Ohjeiden, proseduurien ja prosessien laadinta (ja päivitys), jotta ne vastaavat politiikkojen vaatimuksia (ja muutosvaatimuksia).
- Tarvittavat muutokset prosesseissa.
- Tarvittavat muutokset teknologioissa ja menetelmissä.

Tarkastus voidaan tehdä pistokoeluonteisesti vertaamalla toteutettavan järjestelmän kykyä sille asetettuihin vaatimuksiin. On erityisen tärkeää, että kohtuullisen suurten tietoturvainvestointien (esimerkiksi virustorjunta-, palomuuri-, tunkeutumisenesto- ja roskapostin suodatusohjelmistot) toimivuus ja tehokkuus testataan, jotta ohjelmistot saadaan tehokkaaseen käyttöön ja investointien hyödyllisyys voidaan turvata.

5.2.11 Koulutuksen suunnittelu ja toteutus

Suunnitellaan ja toimeenpannaan koulutus- ja tietoisuusohjelma. On oleellista, että ohjelma sisältää vähintäänkin

- koulutusmateriaalien laadinnan ja ajantasaisuuden varmistamisen,
- säännöllisten koulutustilaisuuksien ja tietoiskujen järjestämisen,
- tietoturvakampanjat aina tarvittaessa (esimerkiksi julisteet, näytönsäästäjät, muistutukset ja kyselyt) sekä
- teemapäivät ja teemaluennot aina tarpeen mukaan (esimerkiksi Internetin käyttö, sähköpostin käyttö, roskapostin suodatus, virustorjunta, etäkäyttö ja kannettavat tietokoneet, salasanakäytännöt).

Henkilöstön asenteet tietoturvaa kohtaan, ymmärrys sen tärkeydestä ja osaaminen – tiedot ja taidot – muodostavat suuren riskin tietoturvan toteutumiselle. Tästä syystä henkilöstön jatkuva kouluttaminen on yksi tärkeimmistä toimenpiteistä, joita tietoturvallisuuden hoitoon ja kehittämiseen kuuluu.

Osana koulutusta voidaan pitää myös materiaalin julkaisemista ilman erillisiä koulutustilaisuuksia. Tähän liittyy esimerkiksi verkkosivuston ylläpito (”tietoturva-intranet”), joka sisältää tarvittavaa tietoturvatietoa ja -sääntöjä, tietoturvakäsikirjan sekä mahdollisia verkko-opiskeluun ja itsetestaukseen käytettäviä työkaluja.

Myös johto ja tietoturvaryhmä tarvitsevat koulutusta. Johdon velvollisuuksiin kuuluu ylläpitää omaa tietoa ja osaamista johtamisen menettelyistä. Tietoturvaryhmän velvollisuuksia on ylläpitää oma osaamisensa ajan tasalla – koskipa se teknisiä tietoturva-asioita, menetelmiä tai valitun sertifioinnin vaatimia osa-alueita. Sertifioinnin ylläpito on oma osaamisalueensa, jota tietoturvapäällikön on ylläpidettävä. Tietoturvallisuuden hallintaan on olemassa useita erilaisia ammatillisia tutkintoja ja sertifiointeja, joista valtaosa on maksullisia. On tyypillistä, että sertifioinnin ylläpito edellyttää jatkuvaa itsensä kouluttamista sekä tietojen ja taitojen ajan tasalla pitämistä.

Koulutustoiminta voidaan tarkastaa pistokokein sekä otteilla julkaistuista materiaaleista että osallistumalla koulutustapahtumiin. Myös koulutuksen vaikuttavuutta voidaan arvioida toteuttamalla erilaisia kyselyitä. Näillä voidaan selvittää esimerkiksi organisaatioon kuuluvien henkilöiden tietoturvatietoisuutta tai yksittäisten koulutusten vaikuttavuutta.

5.2.12 Päivittäinen operointi

Toimeenpanovaihe sisältää kaikki päivittäisessä operoinnissa tehtävät asiat. Tässä dokumentissa ei kuvata päivittäisiä toimia, joihin kuuluu suuri määrä erilaisia hallinnollisia toimia (käyttäjätunnusten hallinnoinnista ja kulunvalvonnasta aina virussuojaukseen, palomuurisäännöstöjen ylläpitoon ja tietojärjestelmäkohtaisiin ylläpitotoimiin ja varmuuskopiointiin).

Testaus (esimerkiksi satunnaiset ja säännölliset skannaukset, tunkeutumis-, haavoittuvuus-, rasitus- ja kuormitustestit, varmuuskopioiden toimintakunnon tarkastaminen, toiminnan testaaminen poikkeus- ja hälytystilanteissa sekä kaikkien uusien ja käyttöön otettavien järjestelmien testaaminen) ja erilaisten harjoitusten järjestäminen on oleellinen osa tietoturvan hoidon säännöllisiä velvollisuuksia, vaikkei testausta harjoitettaisikaan päivittäin. Testaus- ja harjoitusaikataulut voidaan myös sitoa tietoturvaryhmän kokousaikatauluihin, jolloin kokouksissa voidaan tehokkaimmin käsitellä testeistä saatuja tuloksia, tehdä mahdollisia tulosten edellyttämiä päätöksiä ja ryhtyä tarvittaviin toimenpiteisiin.

Päivittäinen operointi kuvataan erilaisiin oppaisiin, ohjeisiin ja proseduurien kuvauksiin ja muihin tarvittaviin dokumentteihin. Teknologiset ratkaisut kuvataan arkkitehtuuri- ja järjestelmäkuvauksiin mahdollisimman yksityiskohtaiselle tasolle.

Päivittäinen prosessi tuottaa lokitietoina erilaisia raportteja, pöytäkirjoja ja lokeja, joita käytetään myös tarkastettaessa päivittäisen operoinnin laadukkuus ja varmistettaessa sen kyvykkyys säilyttää organisaation tietoturvan taso ja toimintakyky omalta osaltaan. Operointia valvotaan ja tarkastetaan osana prosessia 5.2.14 (päivittäinen hallinnointi).

5.2.13 Poikkeamien käsittely

Tässä prosessin vaiheessa käsitellään tietoturvapoikkeamat, joista on saatu tietoa esimerkiksi valvonnasta ja seurannasta, yhteistyötoiminnasta (kuten CERT) sekä muista eri lähteistä (esimerkiksi palautteista ja reklamaatioista).

On oleellista, että tietoturvapoikkeamat havaitaan, että havaitsemisen jälkeen jokainen poikkeama käsitellään sille kuuluvalla tärkeydellä, ja että kaikkiin oikeisiin, tarvittaviin ja riittäviin toimenpiteisiin ryhdytään. Tällöin poikkeamista toipuminen saadaan tehokkaaksi ja aiheutuneet haitat voidaan minimoida.

Poikkeamien käsittely sisältää

- tarvittavien pohjatietojen hankinnan
  - lokitiedot
  - kulunvalvontatiedot
  - järjestelmien käyttötiedot
  - hälytystiedot (sekä manuaaliset että automaattiset hälytykset)
  - muut tiedot (kuormitustilanteet, statistiikka, tilastot ym.)
- palautumisen normaalitilaan
  - ongelmien ratkaisu
  - vikojen ja virheiden korjaus
  - toimenpiteiden kirjaaminen
  - raportointi
  - tilastointi
- poikkeamaan johtaneiden syiden ja seurausten analysoinnin
  - virheistä oppiminen ja samojen tai vastaavien tilanteiden toistumisen estäminen
  - uusien kontrollien suunnittelu tai olemassa olevien kontrollien muuttaminen
  - ohjeiden, manuaalien ja työkuvausten päivittäminen tarvittavalla tasolla
- palautteen antamisen
  - sanktioiden valinta syiden perusteella ja ”syyllisen” rankaiseminen
  - esimerkin antaminen organisaatiolle opetus- ja varoitustarkoituksessa
  - koulutuksen suunnittelun (poikkeamasta saadun tiedon lisääminen koulutuksiin ja materiaaleihin) tarvittaessa
- tiedotuksen
  - asianosaiset
  - oma organisaatio
  - muut tahot, esimerkiksi
    - potilaat,
    - asiakkaat ja alihankkijat.

Prosessissa tuotetaan erilaisia pöytäkirjoja, lokitietoja ja raportteja, joissa kuvataan yksityiskohtaisesti prosessin aikana havaitut seikat sekä kaikki toimenpiteet ja olosuhteet.

On huomattava, että poikkeamien käsittely voi organisaatiosta riippuen kuulua oleellisena osana organisaation jatkuvuuden suunnitteluun, valmiussuunnitteluun ja toipumissuunnitteluun. Joka tapauksessa jatkuvuus-, valmius- ja toipumissuunnitelmissa täytyy huomioida tämän prosessin 5.2.13 olemassaolo: se voi tuottaa oleellista tietoa kyseisille prosesseille esimerkiksi hälytyksinä (esimerkiksi sähkökatkokset), vikailmoituksina (esimerkiksi yhteys- ja käyttökatkokset) tai yleisenä tietojärjestelmien kuormitustietona.

Poikkeamien käsittely on syytä tarkastaa esimerkiksi tarkastamalla tiedot toteutuneiden poikkeamien käsittelystä esimerkiksi lokikirjoista ja arvioimalla tehtyjen toimenpiteiden oikeellisuus ja riittävyys. On myös tarkastettava, että jokainen poikkeama on ylipäätään käsitelty: yhtään tietoturvapoikkeamaa ei pidä hyväksyä ilman käsittelyä. Poikkeamien käsittelyn laatu tarkastetaan osana prosessia 5.2.14 (päivittäinen hallinnointi).

5.2.14 Päivittäinen hallinnointi

Päivittäinen hallinnointi on käytännössä prosessin vaiheen *Toteutus* ydin. Siinä tuotetaan tarvittava tieto, jonka avulla osaprosessien onnistumista, laatua ja tehokkuutta voidaan valvoa ja arvioida prosesseissa 5.2.15 (valvonta ja seuranta) ja 5.2.16 (katselmointi) ja jonka avulla tietoturvatoiminnasta raportoidaan prosessissa 5.2.17 (raportointi).

Päivittäisen tietoturvan hallinnoinnin tehtävät sisältävät esimerkiksi:

- Tutustuminen raportteihin, kuten:
  - lokitiedot (esimerkiksi tapahtuma-, kuormitus- ja virhelokit),
  - käyttötiedot (tietojärjestelmät, verkot),
  - potilastietojen käyttö (potilastietojärjestelmien lokit, käyttötiedot ja pääsynhallinnan tiedot),
  - toimintaraportit,
  - tilastot ja trendit,
  - testien ja harjoitusten tulokset,
  - vikailmoitukset ja tiedot tietoturvapoikkeamista,
  - palautteet ja erilaiset muut esimerkiksi potilailta, käyttäjiltä, yhteistyökumppaneilta ja asiakkailta saadut tiedot,
  - kyselyt ja niiden vastaukset sekä
  - ulkopuolisista lähteistä saatu tietoturvatieto (esimerkiksi CERT).
- Edellä mainittujen dokumenttien ja niistä saatujen tietojen perusteella tehdyt päätökset ja päivittäisen toiminnan ohjaaminen – esimerkiksi prosessin vaiheissa
  - 5.2.10 (kontrollien ja teknologioiden toteutus),
  - 5.2.11 (koulutuksen suunnittelu ja toteutus),
  - 5.2.12 (päivittäinen operointi) ja
  - 5.2.13 (poikkeamien käsittely).
- Säännöllisten kokousten koollekutsuminen: tietoturvaryhmä kutsutaan säännöllisesti kokoon ohjaamaan tietoturvatoimintaa. Kokouksissa käsitellään esimerkiksi
  - kaikkea oleellista seurantatietoa tietoturvan toteutumisesta organisaatiossa,
  - tietoturvan toteutumisen tiedottamista organisaatiossa ja mahdollista ulkoista julkaisemista,
    - viranomaiset
    - CERT
    - julkinen media
  - kaikki edellisen kokouksen jälkeen tapahtuneet vakavat tietoturvaloukkaukset (kaikissa poikkeamissa tietoturvaryhmän käsittelyä ei suinkaan tarvita) sekä
  - mahdollisuuksien mukaan säännöllisten harjoitusten ohjaamista ja tuloksia.

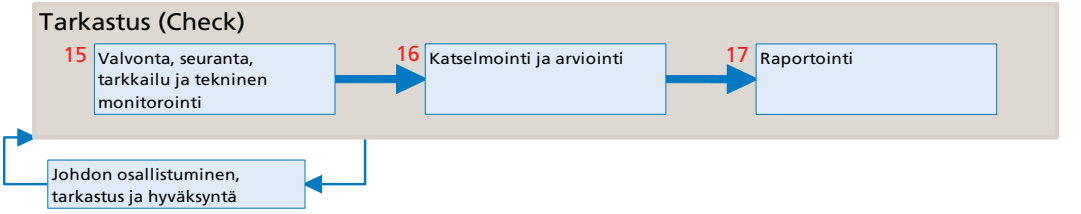
- Palautteen antaminen, johon kuuluu mm.
  - poikkeamien käsittely,
  - organisaation tietoturvatoiminnan laadun ja määrän käsittely, esimerkiksi trendien ja tilastojen esittely sekä
  - laadukkaan ja esimerkillisen toiminnan palkitseminen.

Prosessissa tuotetaan erilaisia päivittäiseen hallinnointiin liittyviä pöytäkirjoja, lokitietoja ja raportteja.

Prosessi välittää tarkastusta varten tiedot prosesseille 5.2.15 (valvonta ja seuranta), 5.2.16 (katselmointi) ja 5.2.17 (raportointi), joiden perusteella johto voi arvioida tietoturvallisuuden toteutumista, tehdä tarvittavia päätöksiä ja ohjata organisaation tietoturvatoimintaa.

Tarkastus

Prosesseissa valvotaan ja arvioidaan organisaation tietoturvallisuuden tilaa kokonaisuudessaan, raportoidaan tietoturvasta tarvittavassa laajuudessa ja hankitaan tietoturvatoiminnalle valittu sertifiointi. Arvioinnin lopputuloksena tiedetään organisaation tietoturvahallinnoinnin (ISMS) kelpaavuus ja toimintakyky asetettuihin vaatimuksiin nähden, ja sen perusteella voidaan suunnitella ja toteuttaa tarvittavat muutokset hallinnointiprosesseihin. (Kuva 8.)



KUVA 8. Hallinnointiprosessi: tehtävät vaiheessa "Tarkastus"

5.2.15 Valvonta ja seuranta

Prosessi saa tarvitsemansa tiedot prosessista 5.2.14 (päivittäinen hallinnointi). Valvonnassa ja seurannassa tarvittavia tietoja ovat:

- sekä automaattiset että manuaaliset seurantatiedot,
- raportit poikkeustilanteista ja niiden käsittelystä,
- tapahtumakirjauksen ja kuormituksen statistiikka ja
- muu tilastointi.

Tässä prosessissa seurataan tietoturvallisuuden toteutumista ja tuotetaan tarpeellinen tieto organisaation tietoturvan hallinnoinnista myöhempää arviointia varten. Tässä prosessissa ei varsinaisesti käsitellä poikkeustilanteita eikä suunnitella toipumista vikatilanteista. Tämä toiminta kuuluu prosessiin 5.2.13 (poikkeamien käsittely).

Prosessi jalostaa seurantatiedot sellaiseen muotoon, että niiden perusteella voidaan arvioida organisaation tietoturvan toteutuminen, sen laatu ja tehokkuus ja mahdolliset kehitystarpeet prosessissa 5.2.16 (katselmointi) ja että organisaation tietoturvallisuudesta voidaan raportoida tarvittavassa laajuudessa ja tarvittavalla tarkkuudella prosessissa 5.2.17 (raportointi).

5.2.16 Katselmointi

Säännöllinen katselmointi on oleellinen osa tietoturvatyötä. Prosessissa katselmoidaan, vastaako toteutunut tietoturva sille asetettuja vaatimuksia, onko riskit arvioitu oikein ja onko niihin varauduttu riittävästi ja onko resurssien käyttö suunnitellun mukaista. Toisin sanoen prosessissa arvioidaan ISMS:n kyky vastata sille asetettuihin vaatimuksiin. Myös uudet järjestelmät, vaatimukset ja muutokset olosuhteissa (lakien muutokset, kehittyvät standardit sekä uudet ja muuttuvat teknologiat ym.) otetaan huomioon katselmoinnissa.

Yhteistyökumppanit, alihankkijat ja muut organisaatiolle välttämättömät ulkoiset toimijat on myös syytä katselmoida aika ajoin. Tällä varmistetaan kolmansien osapuolten toiminnan laatu ja sen yhteensopivuus oman organisaation vaatimuksiin. On oletettavaa, että sosiaali- ja terveydenhuollolle palveluita ja tuotteita tekevien tahojen katselmointiin tehdään malli, jota sosiaali- ja terveydenhuollon organisaatiot voivat käyttää katselmointinsa tukena.

Katselmoinnin lopputuloksena voi syntyä hyväksynnän ja toiminnan parannusvaatimusten lisäksi erilaisia muutos- ja kehitystarpeita organisaation toimintaan tai sen käyttämiin teknologioihin. Nämä muutos- ja kehitystarpeet uudelleen suunnittelua varten käsitellään ja dokumentoidaan vaiheessa *”Kehitys”*.

Organisaation tietoturvan sertifiointi kuuluu osaksi katselmointityötä. Tällöin ulkopuolinen taho arvioi tietoturvan toteutumisen standardeja vasten. Toteutumisen tasoa voidaan verrata myös muihin mahdollisiin organisaatioihin tai oman organisaation yksiköihin, jolloin organisaatioon saadaan tietämys tietoturvatoiminnan laadukkuudesta verrattuna muihin (benchmarking).

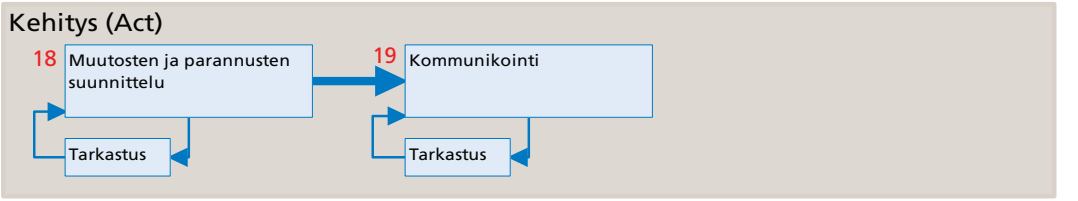
5.2.17 Raportointi

Raportointiin kuuluvat esimerkiksi tietoturvatilanteen (status), tilastojen ja trendien sekä tapahtumatietojen laatiminen ja julkaiseminen. Myös katsaukset ja tieto lainsäädännöstä ja sen muutoksista, standardien kehityksestä ja yleisestä markkinatilanteesta (esimerkiksi teknologioiden kehittyminen, uudet tuotteet, piirteet ja menetelmät, uudet uhkat ja haavoittuvuudet) ovat oleellinen osa raportointia.

Raportteja seurataan erityisesti johdossa – niillä voidaan esittää sekä tilannekatsauksia organisaation tietoturvatoimintaan että perustella mahdollisia tulevaisuuden tarpeita. Kun 5.2.16 (katselmointi) esittää tarpeet ja vaatimukset prosessin nopeillekin muutoksille ja pikaiselle kehittämiselle, raportteja voidaan hyödyntää pidemmän aikavälin suunnittelussa ja hankintaesitysten tukena.

Kehitys

Vaihe ”Kehitys” täydentää tietoturvahallinnoinnin syklisen prosessin kehän: siinä arvioidaan muutos- ja kehitystarpeet organisaation hallinnointiprosessiin ja -menettelyihin (ISMS). Muutostarpeiden käsittely ja muutosten toteuttaminen aloittaa uuden hallinnointisyklin prosessista ”Suunnittelu” alkaen. (Kuva 9.)



KUVA 9. Hallinnointiprosessi: tehtävät vaiheessa ”Kehitys”

5.2.18 Muutosten ja parannusten suunnittelu

Tässä prosessissa arvioidaan muutostarpeet ja tehdään niiden perusteella toimeksianto (input) vaiheelle Suunnittelu. Esitietoina käytetään vaiheen 5.2.16 (katselmointi) tuloksia. Prosessin tuloksena tietoturvahallinnoinnin syklinen prosessi käynnistyy alusta, ja prosessissa havaittuja muutostarpeita ja vaatimuksia päästään suunnittelemaan ja toteuttamaan – alkaen jälleen prosessin ”Suunnittelu” ensimmäisestä vaiheesta. Kaikki havaitut muutos- ja kehitystarpeet välitetään suunnitteluun riittävine yksityiskohtineen.

Tyypillisimmin muutostarpeet kohdistuvat toimintaan ja menettelyihin yksittäisissä osaprosesseissa ja niiden vaiheissa. Joissakin tapauksissa muutostarve voi kohdistua myös hallinnointiprosessiin (ISMS) ja sen kulkuun eikä ainoastaan yksittäisiin prosesseihin. Jos ISMS:iin tarvitsee toteuttaa muutoksia, myös kaikki asiakirjat ja mallidokumentit täytyy muuttaa vastaamaan muutoksia prosessissa.

Hallinnointiprosessiin tehtävät muutokset kohdistuvat tyypillisimmin nykytilanteen kartoitukseen, tietojen turvaluokitukseen (omaisuusluettelon ylläpitoon), resurssien varaukseen ja budjetointimenettelyihin sekä vaiheisiin ”Tarkastus” ja ”Kehitys”. Näihin tehdyt muutokset vaikuttavat eniten organisaatiossa käytettävän hallinnointimallin kypsyyteen. Erityisesti vaiheiden ”Tarkastus” ja ”Kehitys” toimilla voidaan vaikuttaa hallinnointiprosessissa oleviin riskeihin, prosessin mitattavuuteen ja tietoturvatoiminnan ja sen hallinnoinnin tehokkuuteen ja optimointiin.

5.2.19 Kommunikointi ja tiedotus

Prosessissa huolehditaan, että kaikki asianosaiset tahot saavat riittävät ja tarvitsemansa tiedot tulevista muutostöistä ja tulevasta kehityksestä. Tässä vaiheessa kaikkia yksityiskohtia ei välttämättä ole tiedossa, joten myös suunnittelun aikana huolehditaan niiden tahojen tiedotuksesta, joihin muutokset vaikuttavat.

Prosessissa voidaan käyttää hyväksi esimerkiksi organisaation tiedotuspolitiikkaa ja -suunnitelmaa, jos sellaiset on organisaatiossa laadittu.

5.3 Asiakirjat tietoturvan hallinnoinnissa

Tietoturvan hallinnoinnin on oltava suunnitelmallista ja hyvin dokumentoitua toimintaa. Siinä tarvitaan, syntyy ja käytetään suurta määrää erilaisia asiakirjoja. Seuraavassa luettelossa on esitetty esimerkinomainen lista niistä dokumenteista, joita tietoturvan hallinnoinnissa ja päivittäisessä hoidossa tarvitaan ja tuotetaan. Erillisessä liitteessä on mainittu, mitä dokumentteja voidaan käyttää missäkin projektin vaiheessa, ja mihin käyttötarkoituksiin (kirjoitus, muokkaus, luku). Kullekin asiakirjalle on nimettävä omistaja, joka vastaa siitä, että asiakirjat ovat oikein suojattu, että niitä ylläpidetään ajan tasalla ja että niillä on olemassa haltija (joka voi vastata esimerkiksi asiakirjojen teknisestä säilytyksestä, saatavuudesta ja ylläpidosta). Kunkin asiakirjan omistaja hyväksyy asiakirjaan tehtävät muutokset. Asiakirjoja päivitettäessä ylläpidetään muutoshistoria riittävän tarkalla tasolla.

- Lait ja säännökset
- Noudatettavat standardit
- Voimassa olevat sopimukset ja kolmansien osapuolten kanssa käytetyt asiakirjat
- Henkilöstöosastolla käytettävät dokumentit – esimerkiksi työsopimuksiin, palkkaukseen, salassapitoon liittyvät dokumentit
- Budjetit
- Tietoturvatavoitteet

- Strategiat ja suunnitelmat, mukaan lukien jatkuvuussuunnitelma, valmiussuunnitelma, erilaiset varautumis- ja toipumissuunnitelmat vikatilanteiden varalle sekä tiedotussuunnitelma
- Tietoturvapolitiikka
- Toimintaperiaatteet ja hyväksytyt menetelmät
- Muut politiikat ja säännöt
- Tietoturvakäsikirja
- Prosessikuvaukset ja muut organisaation rakennetta ja toimintaa kuvaavat dokumentit
- Organisaatiokaaviot, jotka sisältävät tiedot tietoturvavastuista
- Fyysisten tilojen kuvaukset
- Suojattavien tietojen luettelo (omaisuusluettelo), tietojen turvaluokitus ja pääsynhallintalistat
- Tietojen ja asiakirjojen käsittelysäännöt luottamuksellisuuden eri tasoilla (mahdollisesti osana tietoturvakäsikirjaa)
- Riskianalyysi
- Kuvaukset tietojen suojaamisen menettelytavoista eri suojaustasoilla
- Tietojärjestelmien, tietoverkkojen, tietoliikenneyhteyksien ja arkkitehtuurien kuvaukset
- Tietojärjestelmien ja ohjelmistojen konfiguraatio-, rakenne- ja asennustiedot
- Kuvaukset varmuuskopiointimenettelyistä, testaussuunnitelmat ja lokitiedot
- Toimintaohjeet, työnkuvaukset ja proseduurit
- Käyttöohjeet ja manuaalit
- Tarkastuslistat
- Kyselyt ja kyselyiden vastaukset
- Testaustulokset ja harjoitusten tulokset
- Päivittäiset pöytäkirjat, raportit ja erilaiset lokitiedot
- Suunnitelma ulkoiseksi sertifioinniksi
- Tietoturvahallinnoinnin prosessia kuvaavat dokumentit:
  - nykytilanteen kartoituksen prosessikuvaus ja mallit pöytäkirjoiksi, raporteiksi, tarkastuslistoiksi ja muiksi lomakkeiksi
  - turvaluokittelun prosessikuvaus sekä mallit tietojen turvaluokitukseksi ja pääsynhallintalistaksi
  - uhka- ja haavoittuvuuskartoituksen prosessikuvaus, malli uhkakartoitukseksi ja kysymys- ja vastauslomakkeiksi
  - riskien analysoinnin prosessikuvaus, malli riskianalyysiksi, vaikuttavuuskartoitukseksi ja suojaustasoiksi
  - tietoturvasuunnittelun prosessikuvaus, mallit tietoturvasuunnitelmaksi, -strategiaksi ja -periaatteiksi
  - politiikkojen ja sääntöjen laatimisen prosessikuvaus, malliohjeet
  - resurssien varauksen prosessikuvaus ja mallit budjetiksi ja vastuiden kuvaukseksi
  - kontrollien ja teknologioiden valinnan prosessikuvaus ja malli arviointilomakkeeksi
  - jäännösriskien arvioinnin prosessikuvaus ja malli riskitaulukoksi
  - kontrollien ja teknologioiden toteutuksen toteutusprosessin kuvaus ja malli tarkastuslomakkeeksi
  - koulutuksen suunnittelun prosessikuvaus, mallit koulutusmateriaalien vaatimuksiksi ja kyselylomakkeiksi
  - päivittäisen operoinnin prosessien kuvaus ja prosesseissa tarvittavat mallidokumentit
  - poikkeamien käsittelyn prosessikuvaus, mallit sanktioista ja tiedotteista sekä mallit hälytys-, vikailmoitus-, käyttö-, kuormitus- ja kulunvalvontailmoituksiksi, ja erilaisiksi kirjauslomakkeiksi ja raporteiksi

- päivittäisen hallinnoinnin prosessikuvaus ja malli palautelomakkeeksi
- valvonnan ja seurannan prosessikuvaus
- katselmoinnin prosessikuvaus, sisäisen auditoinnin tarkastuslistan malli sekä malli ulkoiseksi sertifioinniksi
- raportoinnin prosessikuvaus ja malliraportit
- kehityksen prosessikuvaus ja malli muutosehdotukseksi
- kommunikoinnin ja tiedotuksen prosessi.

Liite 1

Käytetyt termit

Tässä on listattu dokumentissa käsiteltäviä termejä selityksineen. Lähdesanastona on käytetty pääasiassa Valtiovarainministeriön julkaisua *Valtionhallinnon tietoturvakäsitteistö 2/2003*. Termien selitykset saattavat sisältää lisäyksiä alkuperäisiin selityksiin.
(en = englanninkielinen termi)

aikaleima
en time stamp
tapahtumatietoon tai viestiin liitetty tieto luomis-, lähetys-, saapumis- tai käsittelyajankohdasta ja mahdollisesti tapahtuman osapuolista

Aikaleimalla saadaan aikaan tapahtuman ajankohdan kiistämättömyys.

allekirjoitus
en signature
asiakirjaan, viestiin tai muuhun tekstiin liitetty henkilön omakätinen nimikirjoitus tai muu tieto, jonka vain kyseinen henkilö on voinut tuottaa, osoituksena siitä, että teksti vastaa hänen tahtoaan tai aikomustaan

Koska sähköisen asiakirjan allekirjoittaminen omakätisesti ei ole mahdollista, on luotu menetelmä, jota käyttämällä henkilö voi tehdä allekirjoituksen sähköisesti siten, että se vastaa sekä teknisesti että juridisesti käsin tehtyä allekirjoitusta. Sähköinen allekirjoitus on tietoturvallisempi kuin käsin tehty, sillä siihen liittyvä väärinkäyttö, esimerkiksi väärentäminen, on käytännössä mahdotonta.

biometriset tunnisteet
en biometric identification, biometric authentication
ihmisen tunnistaminen tai todentaminen fyysisten tuntomerkkien perusteella

Biometrisia tunnisteita ovat esimerkiksi henkilön sormenjäljet ja kasvokuva. Tietojärjestelmissä biometrisia tunnisteita käytetään todentamiseen: järjestelmään kirjautunut tai kirjautumassa oleva, toisin sanoen jo tunnistettu henkilö, todistaa identiteettinsä biometriatietoon perustuen. Biometrisia tunnisteita ei käytetä ihmisen tunnistamiseen. Jos näin tehtäisiin, järjestelmän pitäisi saada biometriatiedon perusteella henkilön identiteettitieto suoraan tietojärjestelmästä, joka edellyttäisi rekisterin olemassaoloa henkilöiden biometrisista tunnisteista.

CA
en certificate authority
katso varmentaja ja TTP

Myös termiä CSP (*cryptographic service provider*) käytetään joissakin yhteyksissä.

CERT
en CERT (Computer Emergency Response Team)
tietoturvainformaatiota jakava puolueeton taho, joka kerää tietoturvallisuuteen liittyvää tietoa, havainnoi tietoturvaloukkauksia ja ennaltaehkäisee tietoturvauhkia julkistamalla ja jakamalla tietoturvallisuuteen liittyvää informaatiota

Keskenään yhteistyötä tekeviä CERT-organisaatioita on useita ympäri maailmaa. Suomessa CERT-organisaationa toimii Viestintäviraston alainen CERT-FI.

digitaalinen allekirjoitus
en digital signature
sähköinen allekirjoitus, jonka tuottamiseen on käytetty henkilön salaista avainta ja joka voidaan tarkastaa käyttämällä henkilölle myönnetyssä varmenteessa sijaitsevaa henkilön julkista avainta

Viestiin tai asiakirjaan liitetty digitaalinen allekirjoitus yksilöi lähettäjän ja on todiste asiakirjan ja lähettäjän aitoudesta sekä asiakirjan eheydestä. Käytännössä digitaalinen allekirjoitus saadaan aikaan epäsymmetrisellä salauksella, jossa allekirjoitettavan viestin tiiviste salataan käyttäjän salaisella avaimella. Salauksen purku onnistuu vain käyttäjän julkisella avaimella, jolloin myös allekirjoittajan henkilöllisyys todentuu. Tiiviste muodostetaan allekirjoitettavasta asiakirjasta siten, että alkuperäisen asiakirjan muuttaminen on mahdotonta muuttamatta myös tiivistettä. Täten allekirjoitus on matemaattisesti kiistämätön: tiivistefunktio ei salli asiakirjaan tehtäviä muutoksia ja allekirjoituksessa käytettävä salausalgoritmi yhdistää allekirjoittajan vedenpitävästi alkuperäiseen asiakirjaan.

eheys
en integrity
tietojen tai tietojärjestelmän aitous, sisäinen ristiriidattomuus ja väärentämättömyys: ominaisuus, että tietoa, viestiä tai asiakirjaa ei ole oikeudettomasti muutettu eikä se ole muuttunut

Tiedon eheyttä kuvatessa käytetään usein myös termejä alkuperäisyys, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus. Tieto voi kuitenkin täyttää eheysvaatimuksen, vaikkei olekaan kattava tai ajantasainen. Tässä mainitut termit kuvaavat pikemminkin tiedon käytettävyyttä ja kelpoisuutta eli tietosisällön laatua.

epäsymmetrinen salaus
en asymmetric encryption
salaus, jossa viestin avaaminen tapahtuu eri avaimella kuin sen salakirjoitus

Käyttäjän hallussa olevaa avainta kutsutaan salaiseksi tai yksityiseksi avaimeksi. Varmenteessa oleva avain on julkinen avain, jota käytetään salaisen avaimen haltijan identiteetin todentamisessa tai salaisen avaimen haltijalle lähetettävän viestin salaamisessa.

Vastaavasti symmetrinen salaus tarkoittaa salausta, jossa viestin salakirjoitus ja avaaminen ja tehdään käyttämällä samaa avainta.

fyysisen ympäristön turvallisuus
en physical and environmental security
henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen, varastojen ja vastaavien suojaaminen tuhoja ja vahinkoja vastaan turvaamalla muun muassa kulun- ja tilojen valvonnan, vartioinnin sekä torjumalla palo-, vesi-, sähkö-, ilmastointi- ja murtovahingot

Fyysinen turvallisuus sisältää myös esimerkiksi työntekijöiden hyvinvoinnin sekä käytössä olevien työ- ja toimitilojen turvaamisen. Tähän voidaan lukea mukaan työhuoneissa näkyvillä oleva turvattava materiaali. Myös kuriirit ja tietoaineistoja sisältävät lähetykset on turvattu.

haavoittuvuus
en vulnerability
alttius tietoturvallisuutta uhkaaville tekijöille

Haavoittuvuus on joku tietty (esimerkiksi) tietojärjestelmän ominaisuus, joka aiheuttaa tai johon voi kohdistua uhka tietojärjestelmälle tai sen toiminnalle. Esimerkiksi käyttöjärjestelmissä on usein ohjelmointi- ja suunnitteluvirheiden johdosta erilaisia haavoittuvuuksia, joita löydettäessä ohjelmistotoimittaja julkaisee korjauspaketin, jonka asentaminen poistaa tai korjaa haavoittuvuuden.

Uhkia kartoitettaessa ja riskejä analysoitaessa on hyvä, mitä enemmän haavoittuvuuksia on tiedossa, jotta ainakin tunnettujen haavoittuvuuksien osalta voidaan varautua niistä mahdollisesti aiheutuviin riskeihin.

hakemistopalvelu
en directory service
julkisen avaimen infrastruktuurin palvelu, joka hallitsee varmenteita ja sulkulistoja sisältäviä hakemistoja

Hakemistopalvelun ominaisuuksista on luotu standardit X.500 ja LDAP (kevytversio, *lightweight directory access protocol*), joissa määritellään esimerkiksi hakemistojen ja niissä sijaitsevien objektien ja tietojen rakenteet ja ominaisuudet, tietojen hakumenetelmät ja hakuprotokollat.

hallinnollinen tietoturvallisuus
en administrative information security, organizational information security
tietoturvallisuuteen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta

Hallinnollisen tietoturvallisuuden toteuttamisessa ovat avainasemassa koulutus, seuranta, valvonta, palautteen antaminen ja poikkeustilanteiden hallinta.

henkilöstöturvallisuus
en personnel security
henkilöstöön liittyvien tietoturvariskien hallinta esimerkiksi henkilöiden soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta

henkilövarmenne
en personal certificate, identity certificate
varmenne, jota käytetään henkilön tunnistamiseen tai todentamiseen sähköisessä asioinnissa ja sähköisten allekirjoitusten tarkastamisessa

Jos varmenteen kohteena ei ole henkilön identiteetti vaan esimerkiksi rooli, puhutaan roolivarmenteesta. Tällöin on huomattava, että varmenteesta ei käy ilmi henkilön identiteetti. Tällaista varmennetta voidaan käyttää esimerkiksi sovellukseen kirjautumisen yhteydessä, kun käyttäjän identiteetillä ei ole merkitystä vaan ainoastaan sillä, onko käyttäjällä tehtävään tai rooliin perustuva käyttövaltuus järjestelmään. Sähköisen allekirjoituksen yhteydessä varmennetta ei ole syytä käyttää, sillä varmenteesta ei käy ilmi allekirjoittaja.

Kansalaisvarmenne on Väestörekisterikeskuksen myöntämä ja ylläpitämä varmenne. Laatuvarmenne on sähköisestä allekirjoituksesta säädettyyn lakiin perustuvat ominaisuudet omaava varmenne, jota käytetään sähköiseen allekirjoitukseen. Laki koskee nimenomaan julkisesti myönnettäviä varmenteita, joten esimerkiksi organisaation työntekijöilleen myöntämät varmenteet eivät ole laatuvarmenteita. Organisaation myöntämien varmenteiden oletetaan yleensä noudattavan vähintään niitä laadullisia ominaisuuksia kuin mitä laatuvarmenteista on säädetty. Laatuvarmenteet sellaisenaan eivät usein kelpaa organisaatiokäyttöön tiettyjen ominaisuuksien takia, esimerkiksi laissa mainittu allekirjoittajan nimi on mahdollista olla myös salanimi.

ISMS
en information security management system
katso tietoturvallisuuden hallintajärjestelmä

ISO
en International Organization for Standardization
kansainvälinen standardointiorganisaatio, joka tuottaa standardeja esimerkiksi tietoturvallisuuteen

ISO 17799 on tietoturvallisuusstandardi, joka pohjautuu Britannian standardointi-instituutin julkaisemaan suositukseen (BS7799) yrityksen tietoturvallisista toimintaperiaatteista ja turvallisuustodistusten myöntämisperusteista. ISO 27001 on edellä mainituista ISO 17799:stä ja BS 7799-2:sta kehitetty standardi organisaation tietoturvallisuuden hallinnointiin.

julkisen avaimen infrastruktuuri
en public key infrastructure, PKI
julkisen avaimen menetelmään perustuvaa infrastruktuuri, jossa nimetyt varmentajat tuottavat käyttäjille avainparit, varmentavat ne digitaalisella allekirjoituksellaan ja jakavat ne käyttäjille, ylläpitävät tarvittaessa julkisten avainten hakemistoja ja sulkulistoja sekä mahdollisia muita infrastruktuuriin kuuluvia palveluita, kuten aikaleimapalvelu

Infrastruktuuri on kokonaisuus ja koostuu kaikista sitä hyödyntävistä laitteista, ohjelmistoista, sovelluksista ja palveluista mukaan lukien käyttäjien toimikortit ja palveluiden käyttöliittymät. Infrastruktuuri perustuu epäsymmetriseen salausmenetelmään, jossa kaksi matemaattisesti toisiinsa liitettyä avainta muodostavat perustan käyttäjien tunnistukseen ja todentamiseen, tiedon salaukseen ja eheyteen, sähköiseen allekirjoitukseen ja tapahtumien kiistämättömyyteen.

kiistämättömyys
en non-repudiation
tietoverkoissa eri menetelmin saatava varmuus siitä, että tietty henkilö on allekirjoittanut tai lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys) tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi

Tapahtumaan, viestiin tai allekirjoitukseen voidaan liittää myös aikaleima, jolloin myös tapahtuman ajankohta on kiistämätön.

kontrolli
en control, myös safeguard
(tässä yhteydessä) riskien hallinnan tavoite, keino tai menetelmä: suunnitelmallinen jatkuva toiminta, kertaluonteinen tai toistuva toimenpide, jolla varaudutaan tai suojaudutaan tietoturvaloukkauksia vastaan

Kontrollin asemesta käytetään usein myös termiä turvamekanismi.

kryptografia, kryptaus
en cryptography
salakirjoitus tai salaustekniikka; menetelmät ja välineet tiedon salaamiseen ja kätkemiseen

Salakirjoittamisessa alkuperäinen tieto muutetaan eli salataan (*encryption*) siten, että salauksen purku (*decryption*) ja siten tiedon alkuperäinen sisältö on mahdollista selvittää vain tietämällä salauksen purkuun tarvittava menetelmä (*encryption algorithm*) ja mahdollinen salauksen purkuun käytettävä avain.

käytettävyys
en usability, usein myös availability
tieto on tallennettu siten ja sellaisessa muodossa, että se on luettavissa, ymmärrettävissä ja tulkittavissa oikein

Käytettävyyteen liittyy myös, että saatavilla olevat tiedot ovat kattavia, ajantasaisia, oikeellisia ja muuten käyttökelpoisia vaadittavalla tavalla ja helppokäyttöisesti ilman tulkinta- ja väärinkäyttömahdollisuutta. Usein käytettävyydellä tarkoitetaan myös sitä, että tiedot ovat saatavilla, siis saavutettavissa ja käytettävissä. Tätä vaatimusta kuvaa kuitenkin paremmin termi saatavuus.

käyttöoikeus
en access right
käyttäjälle annettava tiettyyn tietoon, ohjelmistoon tai järjestelmään annettava oikeus

Käyttöoikeuksia ovat esimerkiksi lukuoikeus, kirjoitusoikeus, muutosoikeus, tuhoamisoikeus ja hallintaoikeus eli muiden käyttäjien oikeuksien määrittely.

käyttöturvallisuus
en operations security
tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvät keinot tietoturvallisuuden parantamiseksi

käyttövaltuus
en user right, authorization, privilege
tietojärjestelmän käyttäjälle myönnetyt yksilöidyt oikeudet nimettyjen tietojen, järjestelmien, ohjelmistojen tai niiden osien käyttöön

laitteistoturvallisuus
en computer security
tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen toimivuuteen ja tietoturvallisuuteen liittyvät toimet

loki
en log
tiedosto, johon tehdään aikajärjestyksessä merkinnät tapahtumista ja niiden aiheuttajista

Loki kerätään yleensä automaattisesti (*automatic logging, audit trail*) ja samaan järjestelmään liittyviä lokeja voi olla useita, esimerkiksi vikaloki ja laskutusloki. Lokitiedosto voi olla järjestelmän sähköisesti allekirjoittama ja lokitapahtumat sovelluksen sähköisesti allekirjoittamia, jolloin lokitiedoston eheys ja kiistämättömyys voidaan taata. Lokitietoja käytetään tyypillisesti tapahtumien ja käyttäjien toimien seurannassa ja raportoinnissa (*auditing, reporting*), valvonnassa (*monitoring*), tarkastuksissa ja laskutuksessa (*accounting*).

(tietojen) luokitus, luokittelu
en (information) classification
tietojen ryhmittely jollakin tietyllä perusteella

Tietojen luokittelun perusteena voi olla esimerkiksi tärkeys ja kriittisyys, merkitys organisaation toiminnalle, salassa pidettävyys ja luottamuksellisuus, suojaustarve ja haavoittuvuus asiattomalle käsittelylle tai omistajuus. Luokitusta, joka asettaa vaatimuksia tietojen turvaamiselle, kutsutaan yleensä turvaluokitukseksi.

luottamuksellisuus
en confidentiality
vain tietyn tai tiettyjen henkilöiden tietoon tarkoitettujen tietojen säilyminen heidän hallussaan ja tiedossaan sekä näiden tietojen suojaaminen paljastumiselta esimerkiksi tietojen käsittelyn yhteydessä myös tietoliikenteen osalta

notaaripalvelu
en notary service
verkkonotaarin palvelu, esimerkiksi aikaleimojen antaminen

ohjelmistoturvallisuus
en software security
käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvat toimet, kuten ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi

PKI
en public key infrastructure
katso julkisen avaimen infrastruktuuri

politiikka
en policy
(tässä yhteydessä) asiakirja, joka kuvaa pääpiirteissään jonkin tietyn kokonaisuuden: päämäärät, määritellyt ja sovitut toimintaperiaatteet, päätökset, ratkaisut ja niiden käytännön toteutuksen

Ratkaisujen ja käytännön toteutuksen kuvaaminen ei ole yksityiskohtaista, vaan kuvataan vain tarvittaessa ja ainoastaan riittävällä tasolla. Tietoturvallisuuden kehittämisessä ja hallinnassa tarvittavia asiakirjoja ovat esimerkiksi tietoturva-, tietosuoja- ja varmennepolitiikka.

pääsynhallinta
en access control
toiminnot ja menettelyt, joiden avulla tietojärjestelmään pääsy tai tiedon saanti sallitaan vain valtuutetuille henkilöille tai sovelluksille

Pääsynhallinnassa tietojärjestelmien, tietoverkkojen ja tietojen käyttäjät tunnistetaan ja todennetaan sovitulla tavalla. Todennetuille käyttäjille myönnetään valtuudet – käyttäjien tehtävien ja roolien mukaisesti etukäteen sovitut käyttöoikeudet – järjestelmiin ja tietoihin.

riski
en risk
(tässä yhteydessä) tietoturvallisuuden ja sen vaarantumisen uhka: todennäköisyys, että uhka toteutuu ja aiheuttaa tietyn suuruisen menetyksen tai vahingon

Riskin odotusarvo voidaan mitata kertomalla uhkan todennäköisyys mahdollisen vahingon arvolla. Organisaation riskien hallinta perustuu riskianalyysiin. Tällöin uhkat ja riskit arvioidaan systemaattisin menetelmin, ja arvioinnin perusteella organisaatio varautuu valittuihin riskeihin valituilla toimenpiteillä. Riskejä ei voida kokonaan poistaa; suojautumisen menetelmiä ovat mm. vähentäminen, pienentäminen ja rajoittaminen (sopivilla suojautumistoimilla), siirtäminen (esimerkiksi sopimuksellisesti toiselle osapuolelle) ja hyväksyminen (pienet tai epätodennäköiset riskit). Jäännösriski on suojautumistoimien jälkeen jäljelle jäävä riski, joka on riskien hallinnan yhteydessä erikseen kirjattava ja hyväksytettävä.

saatavuus, saavutettavuus
en availability, accessibility
tiedon tai tietojärjestelmän ominaisuus, että siihen on riittävän esteetön, vaivaton ja nopea pääsy

skannaus
en scan, scanning
(tässä yhteydessä) automaattinen tai manuaalisesti tehty tietoliikenteen, tietoliikenneverkon tai yksittäisen tietojärjestelmän tarkastus, jossa pyritään etsimään tietoverkon tai tietojärjestelmän (järjestelmien) tietoturvaheikkoudet ja -haavoittuvuudet

sähköinen allekirjoitus
en electronic signature
katso digitaalinen allekirjoitus

sähköinen identiteetti
en electronic identity
henkilön identiteetti ja henkilöllisyys tietojärjestelmän kannalta

Tyypillisesti tietojärjestelmässä henkilön identiteettiä vastaa käyttäjätunnus. Henkilö valtuutetaan tietojärjestelmän käyttöön ja hänelle myönnetään järjestelmässä olevien tietojen käyttöoikeudet sähköisen identiteettinsä, käyttäjätunnuksensa perusteella. Julkisen avaimen infrastruktuurissa rekisteröijä tunnistaa ja todentaa henkilön ja luo tälle rekisteröitymisen yhteydessä sähköisen identiteetin, varmenteen. Käytännössä tämä varmenne vastaa fyysisen maailman henkilöllisyystodistusta.

tarkastettavuus
en auditability
järjestelmän ominaisuus, että järjestelmän tapahtumat kirjataan ja järjestelmän toiminta ja siinä esiintyvät virheet, epäsäännöllisyydet ja väärinkäytökset tuodaan esiin

tietoliikenneturvallisuus
en telecommunications security
tietoturvallisuuden toteuttaminen tietoliikenteen osien (laitteiden, järjestelmien ja ohjelmistojen) ja niissä kulkevien tietojen osalta

tietosuoja
en privacy protection, data protection
tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen, henkilötietojen suojaaminen valtuudettomalta ja henkilöä vahingoittavalta käytöltä

Tietosuoja tarkoittaa yksilön suojaa – ihmisten yksityiselämän ja yksityisyyden suojaa – ja näitä turvaavia oikeuksia esimerkiksi henkilö- tai potilastietoja käsiteltäessä. Tietosuoja-termi on nimenomaan juridinen, ja sen toteuttamisesta ja vaatimuksista on säädetty useassa eri laissa.

tietosuojapolitiikka
en privacy policy, privacy protection policy, data protection policy
tietosuojasäädökset ja niiden toimeenpanoa koskevat päätökset

Jos organisaatio käsittelee yksityishenkilöiden henkilötietoja, se laatii asiakirjan *tietosuojapolitiikka* tai *henkilötietojen käyttö*, jossa kuvataan henkilöön liittyvien henkilötietojen tai muiden luottamuksellisten tietojen käytön periaatteet ja käytäntö organisaatiossa. Asiakirja voidaan jakaa myös niille, joiden henkilötietoja organisaatio käsittelee, jolloin voidaan edesauttaa luotettavan kuvan syntymistä organisaation toiminnasta.

tietoturva, tietoturvallisuus
en information security
tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu.
asiantila, jossa tietojärjestelmien ja tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhkat eivät aiheuta merkittävää riskiä.

Tietoturvan toteutuminen edellyttää tietojen asianmukaista luokittelua, tietoja uhkaavien uhkien ja riskien kartoittamista sekä sopiviin suojaustoimenpiteisiin ryhtymistä. Täytyy olla tiedossa, mitä tietoja suojataan, miksi näitä tietoja suojataan ja miltä tietoja ollaan suojaamassa. Suojaaminen sisältää erilaisia hallinnollisia ja teknisiä päätöksiä, periaatteita, menettelytapoja ja toimenpiteitä, joilla varaudutaan tietoihin kohdistuviin uhkiin ja estetään riskien toteutuminen tai vähennetään niiden vaikutuksia.

tietoturvallisuuden hallintajärjestelmä
en ISMS, information security management system
dokumentoidut menettelytavat ja prosessi, joilla organisaation tietoturvallisuustoiminta perustetaan, ja joilla sitä ylläpidetään, kehitetään, seurataan ja mitataan

ISMS:llä hallinnoidaan organisaation tietoturvallisuutta: suojataan organisaatiota ja sen tietoja tiedossa olevilta uhkilta suunnitelmallisesti ja systemaattisesti. ISO 27001:n vaatimusten mukaisesti toteutetut tietoturvallisuuden menettelytavat voidaan sertifioida. Tällöin arvioidaan, kuinka organisaation käytössä oleva ISMS ja valitut kontrollit, turvamekanismit, vastaavat organisaation toiminnan asettamia vaatimuksia.

tietoturvapolitiikka
en security policy, information security policy, data security policy
organisaation tasolla johdon hyväksymä näkemys ja julkaistu kannanotto tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta

Tietoturvapolitiikka annetaan tyypillisesti esimerkiksi asiakkaiden, yhteistyökumppaneiden tai toimittajien luettavaksi. Se on osoitus organisaation tahdosta ja kyvystä käsitellä tietoja turvallisesti ja luotettavasti. Tietoturvapolitiikka ei yksilöi periaatteita eikä käytäntöä niin tarkasti, että dokumentin jaolla organisaation ulkopuolelle olisi vaikutusta tietoturvallisuuteen.
Jotta organisaatiossa toimitaan tietoturva- ja tietosuojapolitiikkojen mukaisesti, on noudatettavat käytännöt, ohjeet ja periaatteet hyvä koota yhteen, ”*tietoturvakäsikirja*ksi”.

tiiviste
en hash, digest
(tässä yhteydessä) tiedosta, viestistä tai asiakirjasta jonkin säännön mukaan muodostettu lyhyempi uusi tieto, eräänlainen tarkistussumma, varmisteen luomiseksi alkuperäisestä tiedosta

Tiivisteestä ei ole mahdollista päätellä alkuperäistä tietoa tai jotakin muuta tietoa, joka tuottaisi alkuperäisen tiedon kanssa identtisen tiivisteen. Alkuperäisestä tiedosta laskettu tiiviste on samaa funktiota käyttämällä aina identtinen. Täten tiivistettä voidaan käyttää sähköisen allekirjoituksen yhteydessä todisteena, että allekirjoitus koskee nimenomaisesti alkuperäistä ja muuttumatonta asiakirjaa. Tiivistettä kutsutaan joskus myös sormenjäljeksi (*fingerprint*).

todennus
en authentication, verification
tietojärjestelmän käyttäjän (kuten henkilö, laite tai ohjelmisto) tai viestinnän toisen osapuolen aitouden ja oikeellisuuden varmistaminen

Käyttäjän todennuksen yhteydessä käyttäjä todistaa olevansa se, joka hän väittää olevansa. Esimerkiksi salasanan tietämällä käyttäjä todistaa olevansa henkilö, joka on oikeutettu käyttäjätunnuksen käyttöön, vastaavasti pankkiasioinnissa PIN-koodin tietämällä henkilö todistaa olevansa oikeutettu pankkikortin käyttöön. Vastaavaa toimikorttiin perustuvaa menetelmää käytetään vahvan tunnistamisen omaavassa sähköisessä asioinnissa: henkilö tunnistautuu tietojärjestelmään toimikortilla ja todentautuu PIN-koodin tai sormenjäljen käytöllä.

toimikortti
en smart card
suorittimen ja mikropiirejä sisältävä luottokortin kokoinen muovikortti

Toimikortti toimii erityisen lukulaitteen yhteydessä. Lukulaite voi olla joko kontaktillinen tai langaton toimikortinlukija esimerkiksi kulunvalvontaa tai tietojärjestelmän käyttöä varten. Kortille voi olla tallennettuna tietoja ja erilaisia sovelluksia. Usein toimikortilla käytettävien sähköisten palveluiden ja tietojärjestelmien käyttö on mahdollista myös vastaavat ominaisuudet omaavalla USB-avaimella (*USB token*).

TTP
en trusted third party
luotettu kolmas osapuoli; luotettu taho, joka tuottaa esimerkiksi varmennepalveluita (varmentaja) tai verkkonotaarin palveluita

Katso myös varmentaja.

tunnistus
en identification
menettely, jolla yksilöidään esimerkiksi tietojärjestelmän käyttäjä

Tyypillisesti tunnistus tapahtuu tarkistamalla, onko käyttäjän esittämä käyttäjätunnus hyväksyttävien tunnusten joukossa. Tunnistuksen jälkeen käyttäjä tyypillisesti todennetaan eli hän todistaa olevansa kyseinen henkilö esimerkiksi salasanan avulla.

turvallisuustietoisuus
en security awareness
organisaation henkilöstön tiedot ja asenteet, jotka koskevat turvallisuuden tavoitteita ja keinoja

Turvallisuustietoisuus on organisaation tietoturvallisuuteen mahdollisesti eniten vaikuttava kokonaisuus. Ilman hyvää turvallisuustietouden tasoa tekniset turvaamiskeinot saattavat olla turhia; suurimmat riskit koituvat tyypillisesti aina ihmisten toiminnan tai toimimattomuuden seurauksena.

turvaluokitus
en security classification
tietojen ja asiakirjojen jakaminen luokkiin niiden salassa pidettävyyden perusteella

Turvaluokkia voivat olla esimerkiksi julkinen, luottamuksellinen, salainen ja erittäin salainen. Terveydenhuollon asiakirjojen turvaluokittelussa voidaan noudattaa eri periaatteita kuin valtionhallinnon vastaavassa luokittelussa (katso VAHTI-ohjeistus). Esimerkiksi luottamuksellinen tieto voidaan tarvittaessa jakaa alaluokkiin ”luottamuksellinen, hoitotieto” ja ”luottamuksellinen, muu tieto”.

uhka
en threat
(esimerkiksi) organisaatioon, tietoihin tai tietojärjestelmään tietyltä taholta kohdistuvan vahingon tai häiriön mahdollisuus

vaarantaa
en compromise
asettaa alttiiksi uhkalle tai riskille

Julkisen avaimen infrastruktuurissa salaisen avaimen vaarantuessa (*compromised private key*) esimerkiksi PIN-koodin paljastumisesta tai toimikortin hukkumisesta johtuen henkilölle myönnetty varmenne mitätöidään ja merkitään varmentajan ylläpitämälle sulkulistalle. Tällöin tarkastettuaan sulkulistan mikä tahansa sähköisen asioinnin osapuoli voi estää palvelun, jos joku yrittää käyttää asiointiin kyseistä identiteettiä. Henkilölle myönnetään uusi avainpari ja uusi varmenne mitätöidyn tilalle.

vahva tunnistus
en strong authentication
käyttäjän tunnistus ja todennus, joka käyttää ainakin kahta kolmesta menetelmästä: jotakin, mitä käyttäjä on (sormenjälki); jotakin, mitä käyttäjä tietää (salasana, PIN-koodi) tai jotakin, mikä käyttäjällä on hallussaan (avain, toimikortti)

varmenne
en certificate
aitoustodistus, sähköinen identiteettitodistus, jonka ulkopuolinen luotettu taho (varmentaja) on myöntänyt julkisen avaimen infrastruktuurin mukaisessa palveluverkossa toimivalle taholle

Varmenne voidaan myöntää esimerkiksi henkilölle, laitteelle tai sovellukselle. Varmenteiden ominaisuuksista on määrittelyitä ITU:n standardissa X.509.

Varmenne sisältää tietoja esimerkiksi varmenteen voimassaolosta, myöntäjästä (varmentaja), käyttötarkoituksesta ja varmenteen kohteesta (kuten henkilö tai palvelin) sekä tämän julkisen avaimen. Laajennusosaan voi olla merkittynä muita tarpeelliseksi katsottuja tietoja, kuten henkilön sähköpostiosoite, valokuva tai muu biometrinen tunniste tai linkki julkiseen hakemistoon muita, mahdollisesti muuttuvia tietoja varten. Varmenne on varmentajan sähköisesti allekirjoittama, joten varmenteen aitous on varmistettavissa.

Katso myös henkilövarmenne.

Laitteistolle tai ohjelmistolle myönnettyä varmennetta kutsutaan tapauskohtaisesti laitevarmenteeksi, palvelinvarmenteeksi tai ohjelmistovarmenteeksi. Koska tällainen varmenne identifioi tyypillisesti sen organisaation, jonka palveluita kyseisellä laitteistolla ja ohjelmistolla tuotetaan, käytetään tässä yhteydessä joskus myös termiä organisaatiovarmenne.

varmentaja
en certificate authority
julkisen avaimen infrastruktuurissa luotettu taho, joka tuottaa käyttäjille avainparin, myöntää ja jakelee varmenteet ja ylläpitää varmenteet ja sulkulistat sisältävää hakemistoa

Varmenteen myöntöön ja mitätöintiin liittyviä prosesseja hallinnoi varmentajan valtuuttamana rekisteröijä. Käyttäjän salainen avain annetaan ainoastaan käyttäjälle esimerkiksi toimikortille tallennettuna. Avaimen käyttöön oikeuttava PIN-koodi voidaan toimittaa käyttäjälle avaimen toimituksesta erillisellä menetelmällä, mikä lisää toimitusprosessin turvallisuutta. Varmentajaa kutsutaan usein myös varmenneviranomaiseksi.

Väestörekisterikeskus (VRK) toimii varmentajana, joka myöntää kansalaisille sähköistä asiointia varten sähköisiä henkilöllisyystodistuksia, kansalaisvarmenteita. Tällöin salainen avain talletetaan henkilölle annettavaan toimikorttiin, HST-korttiin. Kortti toimii myös virallisena henkilötodistuksena ja matkustusasiakirjana.

viranomaiskortti
en civil service card
sähköinen henkilökortti, jota henkilö käyttää toimiessaan viranomaisena

X
X.509, katso varmenne.

X.500 on hakemistostandardi, jossa on määrittelyitä muun muassa hakemiston rakenteeseen, talletus- ja hakukäytäntöihin sekä hakemistoon talletettavien tietojen, objektien ja niiden ominaisuuksien (attribuuttien) osalta.

älykortti
katso toimikortti

Liite 2

Lainmukaisuuden tarkastaminen

Sosiaali- ja terveydenhuollon asiakastietojen käsittelyn tulee täyttää EU:n tietosuojadirektiivin ja kansallisen lainsäädännön asettamat vaatimukset tietoturvallisuudelle ja yksityisyyden suojalle. Varmuus siitä täyttävätkö tietojärjestelmät tietoturvallisuuden vaatimukset voidaan saada mm. auditoinnin tai sertifioinnin avulla. Henkilötietolaki samoin kuin laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä korostavat ennakkosuunnittelun merkitystä. Tämä tarkoittaa sitä, että lainmukaisuus tulee tarkistaa jo tietojärjestelmien suunnitteluvaiheessa.

Alla olevassa luettelossa on esitetty keskeisimmät sosiaali- ja terveydenhuollon henkilötietojen käsittelyä säätelevät lait ja asetukset:

- Laki potilaan asemasta ja oikeuksista (785/1992)
- Arkistolaki (831/1994)
- Henkilötietolaki (523/1999)
- Laki viranomaisen toiminnan julkisuudesta (621/1999)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki sähköisistä allekirjoituksista (14/2003)
- Sähköisen viestinnän tietosuojalaki (516/2004)
- Laki sähköisestä lääkemääräyksestä (61/2007),
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä (99/2001)
- Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen, Opas terveydenhuollon henkilökunnalle, STM Oppaita 2001:3

Lainsäädännön vaatimuksia on käsitelty yksityiskohtaisesti myös seuraavissa Stakesin julkaisuissa:

- Marja Pajukoski. Sähköinen asiointi sosiaali- ja terveydenhuollossa, lainsäädäntö ja mahdollisuudet. Stakes, Raportteja 283 (2003).
- Tuire Mikola, Hannu Sorvari ja Pekka Ruotsalainen. Suositukset sähköisen suostumuksen periaatteiksi. Osaavien keskusten verkoston julkaisuja 3/2004.

Sosiaali- ja terveysministeriö on yhteistyössä Stakesin kanssa käynnistänyt hankkeen, jossa laaditaan terveydenhuollon tietojärjestelmille sertifiointivaatimukset, jotka potilas- ja asiakastietoja käsittelevän organisaation on täytettävä. Vaatimukset johdetaan voimassa olevista säädöksiin ja kansallisesti käytettävistä standardeista. Vaatimukset julkaistaan vuoden 2008 ensimmäisen neljänneksen aikana.

Liite 3

Projektisuunnitelman malli

Tämä projektisuunnitelman malli (”tietoturvahallinnoinnin kehittämisprojekti”) ei ole otettavissa käyttöön sellaisenaan, mutta se voi toimia pohjana projektisuunnitelman ja tehtäväluettelon laatimisessa ja aikataulutuksessa. Projektisuunnitelman tulisi sisältää ainakin seuraavassa mainitut kohdat:

1) Projektin taustan ja nykytilanteen kuvauksen, jossa esitetään tarve, yleiset perustelut ja syyt projektin käynnistämiselle.
2) Projektin tehtävän ja tavoitteiden kuvauksen sekä tarvittaessa rajauksen projektin ulkopuolelle jäävistä asioista, joiden kuuluminen projektiin voisi ilman rajausta aiheuttaa epäselvyyksiä tai väärinkäsityksiä. Tehtävä kuvaa sitä lopputulosta, joka projektin avulla halutaan saavuttaa, ja sitä asiain tilaa, joka projektin jälkeen on vallalla. Tavoitteet ovat niitä konkreettisia asioita, jotka toteutuvat osana projektia hyödyntämällä projektissa tehtävää työtä ja projektin lopputulosta.
3) Projektin lopputuloksen kuvauksen.
4) Projektiorganisaation kuvauksen tehtävine ja vastuineen. Ainakin projektin omistaja ja johtoryhmä, vastuullinen projektipäällikkö, hänen ohjauksessaan toimiva projektiryhmä ja erilaiset tukiryhmät ja yhteyshenkilöt on hyvä nimetä.
5) Projektin vaiheistuksen, aikataulujen ja ohjauksen kuvauksen. Vaiheistus on hyvä laatia riittävän karkealla tasolla ja siten, että projektissa syntyvät sellaiset tuotokset, joita voidaan käyttää projektin etenemisen tarkastuspisteinä, ovat selkeästi sidoksissa johonkin tiettyyn vaiheeseen tai vaiheen tehtävään. Projektin etenemisen raportointi, seuranta ja ohjaus kuvataan riittävällä tarkkuustasolla. Projektissa tarvittavan oikea-aikaisen päätöksenteon takaamiseksi on määritettävä riittävät ohjausmenettelyt. Tarvittaessa tähän voidaan myös kirjata tiedot muutostenhallinta- ja laadunvalvontamenettelyistä.
6) Tarvittavien resurssien, työmäärien ja kustannusten kuvauksen.
7) Projektin riskien kuvauksen.
8) Projektin yksityiskohtaisen tehtäväluettelon, josta käy ilmi riittävällä tarkkuustasolla ajankohdat, työmäärät, vastuuhenkilöt, käytettävät resurssit ja kustannukset. Mahdolliset tehtävien riippuvuudet edellä mainituista seikoista tai muista projektissa suoritettavista tehtävistä on hyvä kirjata tehtäväluetteloon. Eräs hyvä malli tehtäväluetteloksi on taulukkomuotoinen aikajana, jossa kunkin tehtävän ominaisuudet on lueteltu ja lisäksi aikajana helpottaa tehtävien suhteuttamisen aikaan ja muihin tehtäviin.

Seuraavassa on esimerkki projektisuunnitelmasta edellä mainittujen kohtien mukaisesti.

On huomattava, että projektiin sisältyvät tehtävät 1–5 tähtäävät varsinaisen tietoturvapäällikön, toisin sanoen projektipäällikön, tehtäväkuvan määrittämiseen ja siten projektipäällikön nimittämiseen. Projektin hallintaan liittyen voidaan siten todeta, että tehtävät 1–5 voidaan suorittaa projektin asettamisen yhteydessä ja ovat käytännössä osa projektin esiselvitystyötä tai valmistelutyötä. Projekti voidaan myös jakaa kahteen osaprojektiin: käytännössä tämä nimittäminen edellyttäisi projektipäällikön vaihtamista kesken projektin.

Koska tehtävien 1–5 toteutus vaatii kuitenkin vain kohtuullisen pienen työmäärän ja nimitettävä tietoturvapäällikkö saattaa jo osallistua keskusteluihin ja määrittelytyöhön, on tässä esimerkissä päädytty ratkaisuun, jossa projektin viisi ensimmäistä tehtävää muodostavat projektin valmistelutyön (käytetään myöhemmin termiä esiselvitys), jonka jälkeen nimitetään projektipäällikkö. Tämä projektipäällikkö (käytännössä valittu ja nimitetty tietoturvapäällikkö)

saa kaiken tarvitsemansa tiedon tehtävän 5 jälkeen laadittavasta raportista, ellei ole ollut mukana esiselvitystyössä riittävän aikaisessa vaiheessa.

Projektisuunnitelma: tietoturvahallinnoinnin kehittäminen

1) Projektin taustan ja nykytilanteen kuvaus

<*Organisaation nimi*> käsittelee toiminnassaan arkaluonteisia henkilötietoja, joiden turvaaminen on lakisääteistä ja ensiarvoisen tärkeää. Tästä syystä tietoturvallisuus on otettu yhdeksi lähitulevaisuuden tärkeimmistä kehityskohteista. Kehitystyötä varten perustetaan projekti "tietoturvahallinnoinnin kehittäminen", joka parantaa organisaation tietoturvatoimintaa ja vastaa sille asetettuihin tietoturvavaatimuksiin. Lisäksi organisaation valmius hallita tietoturvaa paranee, kyky puuttua tietoturvarikkeisiin kasvaa, henkilöstö saadaan sitoutumaan tietoturvaan ja ymmärtämään sen tärkeys. Tietoturvatoiminta saadaan osaksi organisaation jokapäiväistä normaalia toimintaa, jonka laatu on mitattavissa, ja joka voidaan haluttaessa sertifioida.

Nykyisin <*organisaation nimi*> toteuttaa ja sillä on selkeästi määriteltyjä tietoturvatoimia, kuten satunnainen käyttäjien tietoturvakoulutus, palomuurien ja virustorjunnan käyttö, kulunvalvonta sekä salasanamenettelyiden käyttö. Tietoturvan hallintaan ei kuitenkaan ole nimetty erillistä vastuuhenkilöä, eikä toiminta ole täysin organisoitua niin, että tietoturvaa voitaisiin hallita keskitetysti koko organisaatiossa. Tietoriskejä ei myöskään säännöllisesti arvioida eikä kaikkia rikkeitä havaita, kaikkiin niihin ei puututa eikä niitä tilastoida. Tietoturvan hallintaa ei ole toistaiseksi katsottu organisaation tärkeäksi strategiaksi, mutta tämä projekti ja sen myötä syntyvä tietoturvatoiminta nostaa tietoturvaan sitoutumisen yhdeksi organisaation toimintaa oleellisesti kuvaavista ominaisuuksista.

2) Projektin tehtävä, tavoitteet ja rajaukset

Projektin tehtävänä on kehittää <*organisaation nimi*> tietoturvaa vastaamaan sille asetettuja vaatimuksia. Tämä toteutuu nimeämällä tietoturvan hallintaan nimetty organisaatio ja suunnittelemalla sellaiset menettelytavat, joilla <*organisaation nimi*> tietoturvaa voidaan toteuttaa kiinteänä osana sen normaalia toimintaa.

Projektin tavoitteet ovat

- tietoturvatoiminnan organisointi (tietoturvapäällikön tehtäväkuvan ja vastuiden määritys, tietoturvapäällikön nimeäminen tai palkkaaminen, tietoturvaryhmän nimittäminen, muiden resurssien varaus),
- tietoturvatoiminnassa tarvittavien asiakirjojen laatiminen (tavoitteet, strategia, toimintasuunnitelma ja politiikat) ja käyttöönotto,
- tietoturvatoiminnassa suoritettavien toimenpiteiden, tarvittavien teknisten välineiden ja turvamekanismien määrittely,
- aikaansaada koko henkilöstölle tarvittava tietoturvan ymmärrys ja sitoutuminen valittujen toimintatapojen noudattamiseen sekä
- erityisesti sen prosessin ja niiden menettelyiden määrittely, jolla tietoturvaa organisaatiossa hallinnoidaan.

Projektin ulkopuolelle rajataan sellaisten tietoturvatoiminnan laadun ja toteutumisen mittareiden laatiminen, joilla organisaation tietoturva voitaisiin sertifioida; projektin lopputuloksia voi tosin hyväksikäyttää laadittaessa tällaisia mittareita. Sertifiointi ja siihen liittyvät yksityiskohtaiset toimet toteutetaan erillisessä projektissa, mikäli näin myöhemmin halutaan.

3) Projektin lopputulos

Projektin lopputuloksena on tavoitteina mainittujen asioiden toteutuminen. Se, kuinka hyvin ja missä aikataulussa tavoitteisiin on päästy, osoittaa projektin onnistumisen asteen. Lopputuloksista voidaan mainita

- dokumentit on laadittu
  - organisaation tietoturvastrategia
  - tietoturvatavoitteet
  - tietoturvapolitiikka
  - tietoturvasuunnitelma
  - yksityiskohtainen toimenpidesuunnitelma
- henkilöt on nimetty
  - tietoturvapäällikkö palkattu ja toimessaan
  - tietoturvaryhmä nimetty ja toiminnassa
- resurssit on varattu
  - budjetti laadittu
  - tarvittavat hankinnat tehty tai suunniteltu
- päivittäiset tietoturvatehtävät on tunnistettu ja lueteltu
  - seuranta- ja raportointimenettelyineen
- tietoturvahallinnoinnin prosessikuvaus on laadittu
  - prosessi valmis käynnistymään.

Osa projektin lopputuloksista valmistuu projektin eri vaiheiden aikana. Näitä voidaan siksi käyttää haluttaessa välitavoitteina, väliraportointikohtina tai projektin etenemisen tarkastuspisteinä.

4) Projektiorganisaatio

Projektin omistaja on <*omistajan nimi*> ja projektin johtoryhmänä toimii <*johtoryhmän nimi tai luettelo henkilöistä*>.

Projektipäällikkönä ja projektin vastuullisena vetäjänä toimii <*projektipäällikön nimi*> esiselvitystyön aikana (projektin tehtävät 1–5). Tehtävässä 4 nimitetään tietoturvapäällikkö, joka toimii projektipäällikkönä projektin tehtävissä 6–17. Projektipäällikön ohjauksessa toimivan projektiryhmän jäsenet ovat <*luettelo henkilöistä*>, joista kukin toimii oman asiantuntemuksensa mukaisesti projektin tehtäväluettelossa mainittujen vastuiden ja työmäärien mukaisesti.

Projektille voidaan erikseen nimetä tukiryhmä tai tukiryhmiä, mikäli sellaisia tarvitaan.

5) Projektin vaiheistus ja ohjaus

Projekti on jaettu neljään päävaiheeseen. Ensimmäisessä vaiheessa määritellään raamit tietoturvaorganisaatiolle, sen vastuille ja toiminnalle. Tämä vaihe sisältää projektin tehtävät 1–3. Toisessa vaiheessa nimetään tietoturvaorganisaatio tai vähintäänkin tietoturvapäällikkö sen johtoon. Tässä vaiheessa suoritetaan projektin tehtävät 4–5. Ensimmäinen ja toinen vaihe yhdessä ovat varsinaisen projektin valmistelutyötä ja esiselvitystä, jossa tietoturvapäällikkö ei ole vielä aloittanut toimessaan. Tästä syystä tietoturvapäällikkö voi aloittaa projektipäällikkönä ja ottaa projektin vastuulleen vasta projektin vaiheen 3 alusta, tehtävästä 6.

Projektin kolmannessa vaiheessa laaditaan organisaatiolle tietoturvasuunnitelma ja -strategia sekä niihin oleellisesti liittyvät muut asiakirjat. Vaihe 3 sisältää projektin tehtävät 6–17. Tällöin tietoturvapäällikkö on jo aloittanut tehtävässään. Projekti alkaa vasta tietoturvapäällikön aloitettua tehtävässään; projektin vetovastuu määrätään tietoturvapäällikölle ennen vaiheen 3 aloitusta. Vaiheen 2 loppu (tehtävän 5 lopussa) toimii myös projektin tarkastuspisteenä, jossa kohdassa kirjoitetaan riittävän yksityiskohtainen dokumentti kaikista tehtävissä 1–5 sovituista asioista.

Vaiheessa 4, siis projektin tehtävissä 12–17, sovitaan päivittäisestä tietoturvatoiminnasta, sen tehtävistä, noudatettavista menettelyistä ja kontrolleista, ja siten myös erillisten kehitysprojektien yksityiskohtaisista aikatauluista ja tehtävistä. Nämä kehitysprojektit alistetaan tarpeen ja mahdollisuuksien mukaan tämän projektin osiksi. Tässä vaiheessa muodostuu myös täsmällinen tietoturvan hallinnointiorganisaatio sekä varataan resurssit ja budjetti toiminnalle. Vaiheen lopussa on saavutettu ja kuvattu riittävälle tarkkuustasolle määritelty prosessi, jonka mukaan organisaation tietoturvaa hallinnoidaan. Tämän vaiheen lopussa laaditaan yksityiskohtainen loppuraportti. Projektin loputtua päivittäinen tietoturvan hallinnointiprosessi on valmis käynnistymään.

Projektin ohjausryhmä seuraa projektin etenemistä, ja jokaisen tehtävän jälkeen pidetään lyhyt ohjausryhmän kuuleminen joko kokouksena, puhelinneuvotteluna tai sähköpostitse. Tällöin projektipäällikkö käy läpi oleelliset tehtävään liittyvät asiat, mahdollisiin ongelmakohtiin puututaan ja tarvittavat ennakoimattomat resurssivaraukset tehdään.

6) Resurssit, työmäärät ja kustannukset

Henkilöresurssit on nimetty kohdassa projektiorganisaatio. Kunkin henkilön työmäärät on merkitty henkilöittäin ja ajankohdittain riittävällä tarkkuustasolla seuraavaan taulukkoon.

Henkilön nimi	Tehtävä	Työmäärä	Ajankohta

Muita tarvittavia resursseja ovat mahdolliset laitteistot ja ohjelmistot, joita joudutaan hankkimaan. Projektisuunnitelmavaiheessa niitä ei ole tiedossa, mutta jos tällaisia ilmenee, ne merkitään tähän kustannusarvioineen. Ylimääräisiä kustannuksia (esimerkiksi tilavuokrat, ulkoinen työ ym.) ei ole näköpiirissä, mutta jos sellaisia ilmenee, ne merkitään tähän.

7) Projektin riskit

Projektin tarkoitus on luoda organisaatiolle tietoturvan hallinnointimenettelyt ja siten ehkäistä organisaatiota kohtaavia tietoturvauhkia, mikä vaatii projektin onnistumiselta lähinnä henkilötyötä. Tästä syystä projektin riskit kohdistuvat lähinnä

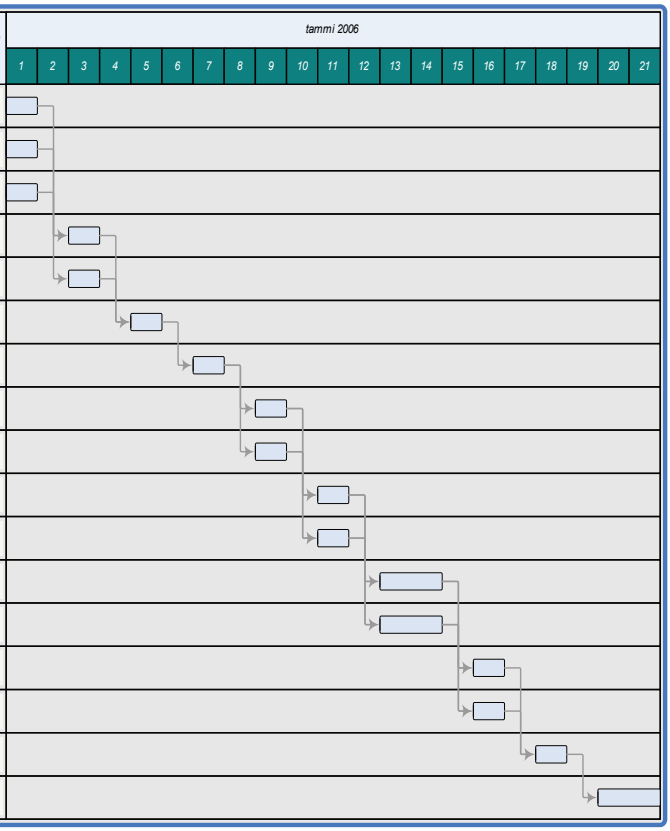
- työaikaan (onko henkilöillä riittävästi resursseja ja projektin vaatima määrä aikaa) ja
- osaamiseen (pystyvätkö henkilöt suoriutumaan tehtävistä siinä ajassa ja sillä laadulla, mitä edellytetään onnistuneelta lopputulokselta).

8) Tehtäväluettelo

Oheisessa kaaviossa on esitetty projektin tehtävät tarvittavine tietoineen. Kuvasta käy ilmi tehtävien riippuvuussuhde toisistaan. Aikataulu ja työmäärät on satunnaisesti valittu mallin laatimisen helpottamiseksi eikä niitä ei voi pitää ohjeellisena. Tämä käynee helposti ilmi esitetyistä luvuista.

Projektin tehtäväluettelo

Tehtävä	Tehtävän nimi	Aloitus-päivämäärä	Valmistumis-päivämäärä	Työmäärä	Vastuuhenkilön nimi
1	Tietoturvapäällikön toimenkuvan määrittäminen	1.1.2006	1.1.2006	1d	
2	Tietoturvapäällikön oikeuksien määrittäminen	1.1.2006	1.1.2006	1d	
3	Tietoturvaryhmän kokoonpanon alustava määrittäminen	1.1.2006	1.1.2006	1d	
4	Tietoturvapäällikön nimeäminen	3.1.2006	3.1.2006	1d	
5	Tietoturvaryhmän jäsenten nimeäminen	3.1.2006	3.1.2006	1d	
6	Nykytilanteen arviointi	5.1.2006	5.1.2006	1d	
7	Tavoitteiden ja strategian laatiminen	7.1.2006	7.1.2006	1d	
8	Tietoturvapolitiikan laatiminen	9.1.2006	9.1.2006	1d	
9	Tietoturvahallinnoinnin prosessin alustava kuvaaminen	9.1.2006	9.1.2006	1d	
10	Alustava budjetointi ja resurssien varaaminen	11.1.2006	11.1.2006	1d	
11	Toimintasuunnitelman laatiminen	11.1.2006	11.1.2006	1d	
12	Tarkkojen aikataulujen päättäminen	13.1.2006	14.1.2006	2d	
13	Päivittäisten tehtävien kuvaaminen	13.1.2006	14.1.2006	2d	
14	Seuranta- ja raportointi-menettelyiden kuvaaminen	16.1.2006	16.1.2006	1d	
15	Muutostarpeiden arvioinnin kuvaaminen	16.1.2006	16.1.2006	1d	
16	Resurssien varaaminen ja budjetointi	18.1.2006	18.1.2006	1d	
17	Tietoturvahallinnoinnin prosessin yksityiskohtainen kuvaaminen	20.1.2006	21.1.2006	2d	



Liite 4

Asiakirjat tietoturvan hallinnoinnissa

Seuraavat taulukot selventävät tietoturvan hallinnoinnissa käytettäviä asiakirjoja ja dokumentteja. Ensimmäinen taulukko kuvaa dokumentit tietoturvan kehittämisprojektissa, toinen taulukko hallinnoinnin prosessissa. Kukin asiakirja on omalla rivillään; projektin ja prosessin eri vaiheet on merkitty kukin omaan sarakkeeseensa.

Taulukoiden rakenteen ja tilankäytön vuoksi sarakkeet on merkitty lyhennetysti pelkillä numeroilla. Ensimmäisessä taulukossa tehtävät on merkitty numeroilla yhdestä seitsemääntoista projektin tehtävänumeron mukaisesti. Jälkimmäisessä esimerkiksi nykytilanteen kartoitus (5.2.1) on merkitty numerolla 1, turvaluokittelu (5.2.2) numerolla 2, ja myös loput vastaavalla menettelyllä.

Taulukoista ilmenee, missä vaiheissa eri asiakirjat luodaan ja missä niitä täydennetään (W; *write*), missä niiden sisältämiä tietoja ja muutostarpeita arvioidaan (M; *modify*) ja missä vaiheissa asiakirjoja käytetään (R; *read*).

Huomaa, että erityisesti ensimmäisessä taulukossa kaikkia asiakirjoja ei vielä välttämättä ole olemassa, vaikka asiakirjan kohdalle olisikin merkitty käyttöä (R). Tässä tapauksessa luonnollisesti todetaan, että kyseistä asiakirjaa ei vielä ole käytettävissä. Se laaditaan projektin aikana asiaankuuluvassa tehtävässä (W).

TAULUKKO 1. Asiakirjat tietoturvan kehittämisprojektissa

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Lait ja säännökset	R					R											
Standardit	R					R											
Voimassa olevat sopimukset	R					R											
Kolmansien osapuolten kanssa käytetyt asiakirjat	R					R											
Henkilöstöhallinnon asiakirjat	W			W	W	R										M	
Budjetti						R				W						M	
Tietoturvatavoitteet	R					R	W										
Tietoturvastrategia						R	W										
Tietoturvasuunnitelma	R					R					W						
Tietoturvapolitiikka	R					R		W									
Toimintaperiaatteet ja hyväksytyt menetelmät	R					R	W										
Tietoturvakäsikirja						R											W
Prosessikuvaukset ja toimintakuvaukset	W	W	W	W	W	R							M	M	M		
Organisaatiokaaviot	R	R	R	W	W	R										M	
Suojattavien tietojen lista (omaisuusluettelo)						R											
Tietojen turvaluokitus						R(W)											
Riskianalyysi						W											
Päivittäisen operoinnin dokumentit, pöytäkirjat, raportit ja suunnitelmat													M	M	M		
Tietoturvahallinnoinnin prosessikuvaukset						R			W					M			M
Suunnitelma; tietoturvan kehitysprojekti											W	M					
Arvio muutostarpeista												W	W	W	W	W	W

TAULUKKO 2. Asiakirjat tietoturvahallinnoinnin prosessissa

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Lait ja säännökset	R																		
Standardit	R																		
Muut ulkopuolelta saatavat dokumentit (CERT ym.)			R									W		R					
Voimassa olevat sopimukset	R		R							W				W				M	
Kolmansien osapuolten kanssa käytetyt asiakirjat	R		R							W				W				M	
Henkilöstöhallinnon asiakirjat	R		R				W							W				M	
Budjetti	R		R				W											M	
Tietoturvatavoitteet	R		R		W													M	
Tietoturvastrategia	R		R		W													M	
Tietoturvasuunnitelma	R		R		W			R										M	
Tietoturvapolitiikka	R		R			W		R										M	
Toimintaperiaatteet ja hyväksytyt menetelmät	R		R		W													M	
Tietoturvakäsikirja	R		R			W		R		W	W	R							
Prosessikuvaukset ja toimintakuvaukset	R		R					R		W	R	R	R					M	
Organisaatiokaaviot	R		R				W			W		R	R	W				M	
Fyysisten tilojen kuvaukset			R					R		W		R	R					M	
Suojattavien tietojen lista (omaisuusluettelo)	R	W	R															M	
Tietojen turvaluokitus	R	W	R	R								R	R					M	
Pääsynhallintalistat		W	R	R						W		R	R						
Uhka- ja haavoittuvuuskartoitus	R		W	R															
Riskianalyysi	R			W				R	W					R					
Suojaustasot ja niiden menettelyt	R			R(W)				W	R(W)			R	R	R				M	
Arkkitehtuurikuvaukset	R		R					R		W		R						M	
Konfiguraatiotiedot										W		R							
Asennustiedot										W		R							
Varmuuskopioinnin kuvaukset										W		R						M	
Testaussuunnitelmat										W		R							
Koulutussuunnitelma			R			W				W	W	R							
Toimintaohjeet, työnkuvaukset ja proseduurit										W	R	W	R						
Käyttöohjeet, manuaalit										W		W	R						
Tarkastuslistat										W		R	R	R	R				
Kyselyt ja kyselyiden vastaukset										W	W	W	R	R	R				
Testaustulokset ja harjoitusten tulokset			R							W		W	R	R	R				
Päivittäiset pöytäkirjat												W	R	R	R				
Raportit												W	W	R	W	W	W		W
Tilastotiedot ja trendit													R	R	W				
Lokitiedot												W	R	R	R				
Tiedotteet											W			W			W		W
Koulutusmateriaali											W								
Mallipohjat pöytäkirjoille, lokeille ja raporteille ym.												W		R	R				
Suunnitelma ulkoiseksi sertifioinniksi														W		W			
Arvio muutostarpeista	R	R	R	R	R	R										W		W	R
Tietoturvahallinnoinnin prosessikuvaukset (kukin tehtävä omalta osaltaan)	R	R	R	R	R	R	R	W	R	R			R	R	R	M	R	W	R

Liite 5

Esimerkki tietoturvapäällikön vastuista ja tehtävistä

Tietoturvapäällikön vastuita ja tehtäviä voivat olla esimerkiksi

- säännöllisten tietoturvatoimenpiteiden määrittäminen ja toteutus (tyypillisesti delegointi teknisille asiantuntijoille tehdään tilanteen mukaan: teknisinä asiantuntijoina voivat toimia kuhunkin tehtäväkuvaan sopivat henkilöt organisaation eri osista),
  - tekniset toimet, esimerkiksi
    - palomuurien ylläpito, hyökkäysten seuranta ja toimenpiteet
    - virustorjunnan ylläpito, statusseuranta ja tarvittavat toimenpiteet
    - roskapostisuodatuksesta huolehtiminen
    - tietojärjestelmien ja -verkkojen tietoturvatapahtumien seuranta ja tarvittavat toimenpiteet tapahtumien perusteella
    - fyysisen kulunvalvonnan, kameravalvonnan ja muiden vastaavien käytössä olevien valvontamenettelyiden seuranta
    - ympäristön teknisten haavoittuvuuksien seuranta ja hallinta
  - hallinnolliset toimet, esimerkiksi
    - tavoitettavissa olo tietoturvapoikkeamien ilmoituksia varten
    - statusseuranta eri organisaatioiden esimiesten raportoinnin perusteella
    - tilastointi ja raportointi
  - tarpeen mukaan tehtävien ja vastuiden jakaminen tietoturvaryhmälle (esimerkiksi teknisten asiantuntijoiden resurssien varaaminen tietoturvatoimintaan)
  - osa tehtävistä on päivittäisiä, osa viikoittaisia tai harvemmin suoritettavia
- tietoturvakontrollien valinta ja toteutuksen ohjaaminen,
  - käytettävät tietoturvamekanismit ovat osa säännöllisiä toimenpiteitä
  - yhteistyössä organisaation eri osien kanssa
- poikkeamien seuranta,
- proaktiivinen seuranta (esimerkiksi tietoturvapäivitysten seuranta ja käyttöönottotarpeen arviointi sekä CERT-ryhmän ja muiden vastaavien tahojen julkaisemien tiedotteiden seuranta)
- projektivastuut tietoturvan kehittämisessä: tietoturvapäällikkö voi toimia projektipäällikkönä tietoturvaprojekteissa ja -hankkeissa,
- koulutus ja organisaation osaamisen ylläpito,
- tietoturvaan liittyvä kommunikointi koko organisaation, sidosryhmien ja erityisesti esimiesten kanssa,
- politiikkojen, säännöstöjen, suunnitelmien ja turvaohjeistuksen kehittäminen ja ylläpito, joista on huomattava myös
  - valmiussuunnitelma
  - viestintäsuunnitelma
  - koulutussuunnitelma
- tietoturvatietoisuuden ja osaamistason seuranta,
- tietoturvatason seuranta (huomaa, että tyypillisesti yleisen turvatason seurannan tuloksena, mikäli turvataso ei täytä asetettuja vaatimuksia, voi olla toiminnan tehostaminen tai vaihtoehtoisesti myös vaatimusten tason laskeminen, jos tietoturvavaatimukset ovat alun perin liian tiukkoja ja toteutettavaksi mahdottomia tai liikaa resursseja kuluttavia)
- toiminta poikkeustilanteissa ja havaittujen uhkien torjunnassa,

- osallistuminen organisaation toiminnan ohjaamiseen aina tarvittaessa, ja osallistuminen myös tietoturvarikkeiden vastatoimiin (incident response team),
- yhteistyö kriisinhallintaorganisaation kanssa kriisitilanteissa,
- yhteistyö tietohallinnon ja muiden organisaatioyksiköiden kanssa aina tarpeen mukaan,
- tapahtumien ja trendien tilastointi,
  - raportoitujen loukkausten (incident reports), reklamaatioiden ja skannaustulosten lisäksi huomioitava myös kaikki ei-tekniset tapahtumat ja toiminta (esimerkiksi roskapostitilastot ja verkkohyökkäystilastot)
- osallistuminen sanktioiden määrittelytyöhön: työoikeudelliset ja muut organisaation sisäiset sanktiot väärinkäytöksissä sekä mahdolliset rikosoikeudelliset sanktiot (jälkimmäisessä tapauksessa lähinnä raportointi, selvitystyö, tiedottaminen ja yhteistyö viranomaisten kanssa),
- raportointi johdolle ja
- muutostarpeiden arviointi (teknologisen ympäristön muuttuessa on varauduttava suojaamismenettelyiden, kontrollien ja testaamisen ajantasaisena pitämiseen ja kehittämiseen, ja toteutettava tarvittavat muutokset suunnitellusti).

Liite 6

Minimitoimet yksityiselle ammatinharjoittajalle ja pienelle organisaatiolle

Erittäin pienelle organisaatiolle – esimerkiksi muutaman lääkärin yksityiselle vastaanotolle – ja itsenäisille ammatinharjoittajille, joille erillisen tehtävän perustaminen tietoturvan hoitoon olisi liian työlästä, minimitaso tietoturvan hoitoon on

- tutustua ja ottaa toiminnassaan huomioon lainsäädäntö ja erilaiset määräykset sähköisten potilastietojen käytöstä sekä käsittelystä (kuten toimikorttien käytön vaatimukset, sähköisen allekirjoituksen käyttö esimerkiksi sähköisen reseptin yhteydessä, ym.),
- tunnistaa käytetyt henkilö- ja potilastiedot ja niiden käsittelytavat,
- tiedostaa käsittelystä aiheutuvat riskit, erityisesti tietojen luottamuksellisuudelle ja oikeille käyttövaltuuksille,
- suojata paperimuotoiset tiedot riittävillä menettelyillä (lukittavat kaapistot ym.),
- suojata käyttämänsä tietojärjestelmät ja tietoliikenneyhteydet (erityisesti virustorjunta- ja palomuurisuojaus),
- velvoittaa sopimuksellisesti käyttämänsä yhteistyökumppanit (laboratoriopalveluiden, ATK-palveluiden, tietoliikennepalveluiden, potilastieto- ja ajanvarausjärjestelmien ym. tuottajat) noudattamaan tietosuojasta säädettyjä lakeja – kaikki eivät välttämättä ole tietoisia tietojen arkaluonteisuudesta ja suojaustarpeesta, ja
- tuottaa asiakkaalle ja potilaalle annettava seloste ja sitoumus tietosuojan ja tietoturvan hoidosta (mahdollisesti osana rekisteriselostetta).

On luonnollista, että eri toimijoiden ja viranomaistoimijoiden tietoturvatoimintaa ohjataan jo nyt erilaisilla laeilla ja määräyksillä (kuten terveydenhuollosta vastaavan johtajan ja tietoturvavastaavan roolit ja vastuut). Nähtävissä on, että standardeja kehitetään, tullaan valvomaan ja tietoturvatoimintaa myös auditoimaan ja sertifioimaan. Tämä koskenee jatkossa myös ulkoisia toimijoita, kuten

- sovellus-, järjestelmä- ja palvelutuottajia,
- tietoliikenneoperaattoreita ja
- muita tahoja (apteekit ym.).

Liite 7

Tietoturvan perusteet

Alla esitetyssä katsauksessa tietoturvan perusteisiin on käytetty lähteenä Stakesin raportti 5/2005, Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt[1].

Tietoturvallisuus ja tietosuoja

Tietoturvallisuudella tarkoitetaan asiantilaa, jossa tietojen, tietojärjestelmien ja tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhkat eivät aiheuta merkittävää riskiä. Suomen lainsäädäntö lähtee siitä, tietoturvallisuus on hoidettava asianmukaisesti (Valtionvarainministeriö). Tietoturvallisuus on kiinteä osa jokaisen sosiaali- ja terveydenhuollon toimijan ja organisaation toimintaa ja se koskee koko henkilöstöä.

Suomessa ei ole yhtenäistä tietoturvallisuuslainsäädäntöä. Tieturvallisuuden järjestämistä koskevia säädöksiä sisältyy useihin lakeihin.

Tietosuojalla tarkoitetaan henkilötietojen suojaamista valtuudettomalta ja henkilöä vahingoittavalta käytöltä ja käsittelemiseltä. Tietosuojatoimien tavoitteena on tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen. Tietosuoja on yksilön suojaa. Henkilötietojen käsittelyyn ja luottamuksellisen viestinnän suojaan liittyviä säännöksiä on lukuisissa eri laissa.

Oikeudesta käsitellä arkaluontoisia ja salassa pidettäviä tietoja on säädetty henkilötietolaissa ja viranomaisten osalta julkisuuslaissa. Henkilötietolain lisäksi sosiaali- ja terveydenhuollon tietojen käsittelyä ohjataan erityislailla ja asetuksilla kuten potilaslailla ja potilasasiakirja-asetuksella (Tuire Mikola, Hannu Sorvari ja Pekka Ruotsalainen, Turvallinen kommunikaatioalusta, Suositukset sähköisen suostumuksen periaatteiksi, OSVE 3/2004, Marja Pajukoski, Sähköinen asiointi sosiaali- ja terveydenhuollossa, lainsäädännön rajat ja mahdollisuudet, Stakes Raportteja 283/2004).

Henkilötietolaki korostaa tietojärjestelmien ja henkilötiedon käsittelyn etukäteissuunnittelua. Toiminnat tulee kartoittaa etukäteen, henkilötietojen käsittely suunnitella ja toteuttaa lainmukaisesti. Henkilötietolain periaatteista voidaan johtaa mm. seuraavat tietojenkäsittelyn vaatimukset (Timo Itälä ja Pekka Ruotsalainen, Tietoturvallinen kommunikaatioalusta, Luovutusten ja luovutuslokin hallinnan suositukset, OSVE 6/2004):

- etukäteissuunnittelun vaatimus
- huolellisuus ja suojaamisvelvoite
- virheettömyys-, eheys- ja luotettavuusvaatimus
- käyttötarkoitussidonnaisuus
- tarpeellisuusvaatimus
- yhteysvaatimus
- informointivelvoite
- tarkastusoikeus
- korjaamisoikeus.

Sosiaali- ja terveydenhuollon organisaation on kehitettävä ja hallinnoitava samanaikaisesti sekä tietoturvallisuutta että tietosuojaa.

Sosiaali- ja terveydenhuollon organisaatioiden toiminta ja päätöksenteko perustuvat nykyään tietoon, jota on yhä enemmän ja joka on entistä yksityiskohtaisempaa. Lisäksi tämä tieto on suurimmaksi osaksi sähköisessä muodossa ja jopa luodaan suoraan sähköisiin järjestelmiin: tietoja

ei välttämättä ole edes olemassa paperimuodossa, vaan kaikki käsittely ja säilytys pitkäaikaisine arkistointeineen hoidetaan sähköisesti. Sähköinen tieto on paperilla olevaa tietoa alttiimpaa erilaisille tietoturvaloukkauksille. Tietoon voi päästä käsiksi ajasta ja paikasta riippumatta pitkienkin matkojen takaa, ja kaikki tieto on saavutettavissa ja kopioitavissa murto-osassa siitä ajasta, mikä kuluisi paperidokumenttien läpikäymiseen. Toisaalta erilaiset vika- ja häiriötilanteet, kuten tietojärjestelmien vioittuminen, voivat estää kaikkien tietojen käytön ja pahimmassa tapauksessa lamauttaa koko organisaation toiminnan.

Tietoturvallisuus ja tietojen suojaaminen onkin muodostumassa yhteiskunnassamme yhä tärkeämmäksi osaksi myös viranomaisten toimintaa. Vaikka viranomaisten toiminta on julkista, ne käsittelevät toimissaan ja päätöksenteossaan usein salaista tai arkaluonteista tietoa, joka on suojattava asianmukaisesti. Toisaalta on välttämätöntä, että tietyt viranomaisen tarvitsemat tiedot ovat aina käytettävissä ja että tiedot ovat oikeellisia. Tietojen käsittelystä ja säilytyksestä, käsittely- ja säilytystapojen turvallisuudesta ja käytettävien tietojen suojaamisesta onkin jo säädetty useassa laissa ja asetuksessa.

Voimassa oleva lainsäädäntö asettaa määräyksiä tietojen turvaamiselle. On huomioitava, että lainsäädännön muuttuessa myös organisaation käytössä oleva tietoturvadokumentaatio ja toimintatavat on päivitettävä ajantasaiseksi.

Tietojen sähkömuotoisuus asettaa mittavat vaatimukset turvallisuudelle. Toisaalta vasta sähkömuotoisuus ja tietojärjestelmien hyödyntäminen tekevät mahdolliseksi monipuolisen ja varman käytön seurannan, valvonnan ja käyttäjien valtuuksien määrittelyn. Valtuudettomalta käyttäjältä estetään pääsy kaikkiin niihin tietoihin, joihin hänelle ei ole nimenomaisesti määritelty pääsyoikeuksia. Seuranta ja poikkeustilanteiden valvonta voidaan toteuttaa reaaliaikaisesti, jolloin ajantasaiset hälytykset esimerkiksi turvaloukkauksista ja virhetilanteista aikaansaavat erittäin nopean korjauksen ja paluun normaalitilanteeseen.

Tietoturvallisuutta ja sen vaarantavia tekijöitä on tutkittu runsaasti. Yleisesti voidaan todeta, että ihmisen toiminta, joko tahallinen tai tahaton, on suurin yksittäinen turvallisuuden vaarantava tekijä. Toisaalta lukuisat eri organisaatioihin tehdyt kyselytutkimukset ovat myös osoittaneet, että suurin osa organisaatioista ei ole varautunut vakaviin riskeihin ja sellaisen kohdatessa vaikutus organisaation toimintaan on lamauttava ja vakavia seurauksia aiheuttava, olipa riski sitten ihmisen toiminnasta tai esimerkiksi teknisestä viasta aiheutuva. Kuitenkin, muokkaamalla henkilöstön asenteita, kouluttamalla työntekijöitä ja parantamalla heidän osaamistaan sekä sitouttamalla kaikki organisaation työntekijät tietoturvalliseen toimintaan saadaan aikaan merkittävä parannus tietoturvallisuuden tasoon. Sitä voidaan täydentää turvaamalla tärkeät prosessit, käyttämällä turvallisia toimintatapoja sekä toteuttamalla tarvittavat tekniset toimet.

Tietoturvan vaarantuminen teknisten ja teknologisten uhkien kautta on usein estettävissä myös teknisiä menetelmiä hyödyntämällä. Esimerkiksi tietojärjestelmärikkoihin voidaan varautua teknisin toimenpitein. Käyttämällä varajärjestelmiä, varayhteyksiä ja vastaavanlaisia toimenpiteitä organisaatio voi tehokkaasti turvata keskeytymättömän toiminnan, vaikka kriittinenkin tietojärjestelmä vikaantuisi. Vastaavasti viruksia ja muita haittaohjelmia vastaan voidaan suojautua teknisin menetelmin: käyttämällä palomuureja, viruksentorjuntaohjelmia, varmistamalla sähköpostin ja liitetiedostojen turvallisuus ja estämällä vaarallisiksi havaittujen tai epäilyttävien verkkosivujen käyttö. Teknisillä toimilla ei kuitenkaan koskaan voida korvata eikä rakentaa vastaavaa tietoturvallisuutta, kuin mikä muodostuu ihmisten riittävästä osaamisesta, oikeanlaisista asenteista ja oikeasta suhtautumisesta turvallisuuteen.

Tietoturvallisuuden osatekijät

Puhuttaessa tietoturvan osista voidaan ensin puhua tietojen saatavuudesta (*availability*) ja käytettävyydestä (*usability*). Ensin mainitulla tarkoitetaan sitä, että tiedot ovat saatavissa silloin, kun niitä tarvitaan ja siellä, missä niitä tarvitaan. Jotta tiedot olisivat saatavilla, on tietojärjestelmien (laitteet, ohjelmistot ja tietoliikenne) toimintakuntoisuus ja saavutettavuus on turvattava. Toimintahäiriöihin voidaan varautua rakentamalla erilaisia tietoturvamekanismeja, jotka estävät tietoturvaloukkauksia. Erilaisista vika- tai ylikuormitustilanteista on kyettävä toipumaan erilaisin varajärjestelyin (*fault management*, *performance management*), kahdennetuin varajärjestelmin, apuohjelmin (kuten virustorjunta ja palomuurit) ja esimerkiksi varmistamalla tiedot nauhakopioille, joista ne ovat palautettavissa käyttöön. Termiä käytettävyys käytetään usein synonyyminä saatavuudelle: tiedot ovat saatavissa eli käytettävissä. Käytettävyydellä tarkoitetaan kuitenkin myös käyttökelpoisuutta: sitä, että tietojen on oltava tallennettuina sellaisessa muodossa, että tiedot ovat yksiselitteisesti sekä luettavissa että ymmärrettävissä. Tällöin ei esimerkiksi muodostu turvariskiä sille, että tietojen tallennusformaatti olisi vanhentunut ja tiedot käyttökelvottomia eikä myöskään sille, että tietojen vaikea muoto voisi aiheuttaa virhetulkinnan.

Edellä mainitut termit eivät ota kantaa tietojen laatuun ja käyttötarkoitukseen: ovatko sinänsä eheät ja teknisesti käyttökelpoiset tiedot sopivia kussakin asiayhteydessä käytettäviksi, ovatko ne hyödyllisiä tai ylipäätään tarpeellisia. Sosiaali- ja terveydenhuollossa käytettävien tietojen tarkoituksenmukaisuus ja käyttötarkoitus on kuitenkin huomioitu lainsäädännössä.

Yleisiä turvallisuuteen vaikuttavia tekijöitä ovat lisäksi esimerkiksi organisaation kiinteistöjen ja kulunvalvonnan turvallisuus, joka onkin usein kuvattu kohtuullisen tarkasti ja riittävän kattavasti. Kulunvalvonnalla hallitaan sekä pääsy että pääsyn estyminen organisaation tiloihin, joissa on mahdollisuus tietojen käyttöön.

Toiseksi tietojen, joita käytetään, on oltava oikeellisia ja eheitä (*integrity*). Tiedot eivät saa olla vahingossa muuttuneet esimerkiksi ohjelmiston, tietokannan tai järjestelmän vioittumisen tai korruptoitumisen (turmeltumisen) vuoksi. Tiedot eivät saa myöskään olla alttiina väärentämiselle. Tietojen eheyden rikkoutuminen on yleensä erittäin vaikeasti havaittavaa ja aiheuttaa mahdollisesti suuret haittavaikutukset. Tästä syystä tietojen eheyden rikkoutuminen katsotaankin usein yhdeksi vakavimmista tietoturvaloukkauksista. Monesti tietojen olemassaoloon kytketään myös tekijä ja tekoaika, jolloin tietojen aitous ja alkuperäisyys voidaan tunnistaa. On olemassa menetelmiä, joilla asiakirjan tekijä voidaan kiistämättömästi todentaa (*authentication*, *non-repudiation*) ja joilla tietoihin voidaan liittää tekoajan tai muuttumishetken aikaleima. Teknisesti puhuttaessa tällaista menetelmää kuvataan usein termillä sähköinen allekirjoitus. Tietojärjestelmien sisäiseen tietojen käsittelyyn ja järjestelmien väliseen tietojen siirtoon on olemassa menetelmiä, joilla tietojärjestelmät ylläpitävät tietojen eheyttä ja tarkastavat käytettävien tietojen oikeellisuuden automaattisesti. Tekninen termi tällaiselle menetelmälle on järjestelmäallekirjoitus tai organisaatioallekirjoitus. Puhuttaessa sähköisestä allekirjoituksesta on yleensä syytä erottaa, tarkoitetaanko sähköistä allekirjoitusta sen teknisessä vai juridisessa merkityksessä.

Kolmanneksi, tietojen luottamuksellisuus (*confidentiality*) täytyy taata: tietoja käyttävillä henkilöillä on oltava valtuudet (*authorisation*) käyttää tietoja. On myös määriteltävä, millaisin valtuuksin kukin käyttäjä tietoja käsittelee. Tämä edellyttää tietojen luokittelua (*classification*), henkilöiden tunnistamista (*identification*), todennusta (*authentication*) ja valtuuksien määrittelyä (*privilege management*) sekä käsittelytapojen ja -sääntöjen määrittelyä. Esimerkkinä tietojen luokittelusta voidaan käyttää Valtiovarainministeriön tekemää valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohjetta, jossa viranomaisen tieto on luokiteltu julkiseen ja salassa pidettävään tietoon, joista salassa pidettävä on puolestaan jaettu kolmeen alaluokkaan: erittäin salainen, salainen ja luottamuksellinen tieto. Henkilöiden tunnistaminen ja todennus tietojärjestelmien käytön yhteydessä voidaan toteuttaa lukuisilla eri menetelmillä, joista osa noudattaa heikkoja tai erittäin heikkoja tunnistamismenetelmiä (esimerkiksi ryhmäkohtaiset tunnukset

ja salasanat) ja osa vahvaa tunnistamista (toimikorttipohjainen todentaminen). Todennettujen henkilöiden käyttövaltuudet perustuvat esimerkiksi henkilön asemaan, työtehtävään tai rooliin. Valtuudet ja oikeudet on tyypillisesti määritelty tietojärjestelmään. Erilaisia tietojen käsittelytapoja ovat esimerkiksi oikeus luoda, muuttaa tai tuhota asiakirja.

Tietojen käytön yhteydessä puhutaan usein myös jäljitettävyydestä (*logging, audit trail*), tarkastettavuudesta (*auditability*) ja tilivelvollisuudesta (*accountability*). Näillä tarkoitetaan kaikkien tietojärjestelmässä tapahtuvien toimien kirjaamista, järjestelmien ja tietojen käytön seurantaa sekä valvontaa. Kaikista käyttäjien toimista ja järjestelmän automaattisesti suorittamista toimista pitää jäädä sellainen tieto järjestelmään, että tilanteen myöhempi toteaminen (mitä on tehty, milloin on tehty, kuka on tehnyt) on mahdollista. On rakennettava sopivat kontrollit tietojärjestelmien toiminnan turvallisuuden seurantaan sekä ohjelmistojen, laitteistojen että tietoliikenteen osalta (suorituskyky, vikatilanteet). Yhtä lailla, samanlaiset kontrollit on rakennettava käyttäjien toiminnan seurantaan. Kontrollit tukevat organisaation tietoturvasta vastaavien henkilöiden toimintaa ja ylläpitävät organisaatioiden prosesseissa käytettävien tietojen turvallisuutta.

Tietoturvalliset toimintaperiaatteet

Tietoturvallisten toimintaperiaatteiden määrittely on välttämätöntä, jotta organisaation johto saa toteutettua turvalliset tietojenkäsittelytavat koko organisaatioon ja sen kaikkiin prosesseihin. Tietoturvallisuuden vaarantumisen yksi perimmäisistä syistä on inhimillinen toiminta – päivittäisten toimien hoito, ymmärrys, osaaminen, asenteet, johtaminen. Organisaation tietojenkäsittelyn turvallisuuden taso on ainoastaan yhtä vahva kuin sen tietojenkäsittelyprosessien heikoimman osan turvataso. Koska tämän heikoimman lenkin muodostaa yleensä ihmisen – yksilön – toiminta, tietoturvallisten toimintaperiaatteiden määrittelyn tehtävänä ei ole ainoastaan turvattavien ja suojattavien tietojen käsittelyä koskevien periaatteiden, toimintamallien ja ohjeiden luonti. Näiden on myös oltava koko organisaation henkilöstön tiedossa, ymmärtämiä ja käytössä, jotta turvallinen tietojenkäsittelyn taso saavutettaisiin ja sitä voitaisiin ylläpitää. Terveydenhuollon ammattilaisten eettisten ohjeiden on myös vastattava tietojen suojaamisen vaatimuksia.

Tietoturvan kehittäminen ei olekaan projekti vaan prosessi, joka vaatii organisaatiolta ja erityisesti sen johdolta vankkaa sitoutumista. Toimintaperiaatteiden määrittely on ensimmäinen vaihe prosessin kehittämisessä. Tämän jälkeinen tietoturvallisuuden ylläpito vaatii jatkuvaa, järjestelmällistä ja dokumentoitua turvallisuustason kehittämistä, ylläpitoa, seurantaa, valvontaa ja henkilöstön koulutusta sekä osaamisen tason seurantaa. Toiminnan on oltava organisoitua, ja sille on määrättävä nimetyt vastuuhenkilöt ja varattava riittävät resurssit. Tietoturvallisuustoiminnan tulokset ovat myös mitattavissa, ja säännöllisen palautteen antaminen tulosten perusteella ohjaa toimintaa edelleen.

Riskit ja uhkat

Kaikelle tietojen turvaamistoiminnalle on yhteisenä tekijänä ja perusteena tunnistettu riski. Toteutuessaan riski estää tai haittaa tietojen käyttöä siinä tarkoituksessa ja laajuudessa kuin mihin tietoja on tarkoitettu käytettävän. Riskin voi aiheuttaa myös uhka tietojen olemassaololle. Se voi koskea esimerkiksi tietojen katoamista tai tuhoutumista, muuttumista tai väärentämistä, vääränlaista tai valtuudetonta käyttöä, käytettävien tietojen väärää tulkintaa ja inhimillisiä virheitä sekä erilaisten tahallisten tietojärjestelmähyökkäysten tai -murtautumisten vaikutuksia (muun muassa tunkeutumiset, tietomurrot ja palvelunestohyökkäykset). Tästä syystä tietojen turvaamisen yhtenä keskeisenä tarkoituksena onkin erilaisten riskien tunnistaminen ja riskeihin varautuminen. Kaikkiin niihin ei kuitenkaan kannata eikä edes voi varautua: on tunnistettava riskit, jotka ovat

todennäköisiä ja joista toteutuessaan aiheutuu tai voi aiheutua mahdollista haittaa (esimerkiksi sähkökatkokset, tietomurrot ja inhimilliset virheet). Jos haittavaikutusta ei ole, riskiltä ei kannata suojautua, vaikka mahdollisuus olisi kuinka todennäköinen. Toisaalta, vaikka tiettyjen riskien haittavaikutus olisi suuri mutta todennäköisyys erittäin pieni (kuten luonnonkatastrofit ja sodat), ei niihin tietoturvaa määriteltäessä yleensä varauduta.

Yleisesti voidaan sanoa, että on sitä parempi mitä yksityiskohtaisemmin uhkat ja riskit on tunnistettu. Tällöin niiden seuraukset voidaan yksilöidä tarkasti ja varautumistoimet voidaan mitoittaa ja kohdistaa oikein. Suojaamistoimet kohdistuvat näin parhaiten suoraan riskiin eivätkä ole ”yleispäteviä”. Luonnollisesti tietyt toimenpiteet suojaavat monia eri tietoja monilta eri riskeiltä. Esimerkiksi fyysisen kulunvalvonnan kontrolleilla voidaan suojata kaikkia toimitiloissa olevia tietoja. Vastaavasti palomuuri suojaa kaikkia tietoja erityyppisiltä verkkohyökkäyksiltä.

Uhkien tunnistamisessa pitää myös tutustua tietoturvaloukkauksiin, joita muualla on jo tapahtunut. Tietomurtojen yrittäjät käyttävät usein samoja tai samantyyppisiä menetelmiä. Motiivi erilaisiin tietomurtoihin ja siten myös tietomurtoyrityksen todennäköisyys on suoraan verrannollinen tiedon arvoon, joko todelliseen tai kuviteltuun, ja tiedon oletettuun käytettävyyteen murtautujalle. Tiedon arvo voi olla huomattavan erilainen organisaatiolle kuin mitä se on murtautujalle.

Kaikenlaiset haittaohjelmat, muun muassa virukset, troijanhevoset ja madot sekä erilaiset ohjelmistojen takaportit ovat uhka tietoturvalle. Tyypillisesti niiden avulla voidaan joko paljastaa luottamuksellisia tietoja tai vioittaa tietojärjestelmiä, jolloin näiden sisältämät tiedot eivät ole saatavilla. Ne ovat usein uhkia vain tiettyjen käyttöjärjestelmien ja ohjelmistojen käyttäjille, mutta mahdollisuus täytyy silti ottaa huomioon tietoturvariskejä arvioitaessa. Tietojen saatavuuteen voidaan myös yrittää vaikuttaa verkosta tapahtuvilla palvelunestohyökkäyksillä (*DoS, denial of service*), jotka tyypillisesti kohdistetaan tiettyä palveluntarjoajaa kohden tarkoituksena estää verkkokäyttäjien pääsy palveluihin.

Yllä mainitut muodostavat vain pienen osan organisaation tietoturvallisuuskokonaisuudessa. Nämä ovat silti ne uhkat, jotka yleensä ymmärretään parhaiten ja joista julkisestikin puhutaan. Moni mieltääkin tietoturvan ainoastaan virustorjuntana ja palomuureina. Jopa kaupallisilla markkinoilla on yrityksiä, jotka myyvät ”tietoturvan ulkoistamista”, vaikka todellisuudessa yritys tarjoaa ulkoistamispalveluita esimerkiksi ainoastaan virustorjunnan tai verkkosuojauksen hoitoon.

Riskien täydellinen välttäminen on käytännössä mahdotonta – organisaation toimintaan liittyy aina riskejä. Myös yksittäisten riskien ehkäiseminen ja kokonaan poistaminen saattaa aiheuttaa liikaa kustannuksia verrattuna riskeistä aiheutuviin haittoihin. Tästä syystä riskien hallinnan tavoitteena onkin usein pienentää riskiä – pyritään estämään vahinkojen syntyminen sekä vähentämään tai lieventämään niiden seurauksia tunnistamalla riskit yksityiskohtaisesti ja valitsemalla sopivat kontrollit ja suojautumiskeinot. Tiettyjä riskejä voidaan esimerkiksi sopimuksellisesti tai vakuuttamalla siirtää jopa muille, jolloin mahdollisesti aiheutuvat vahingot eivät kohdistu täysimittaisena ainoastaan omaan organisaatioon, vaan mahdolliset korvausvastuut riskin toteutuessa voidaan jakaa useamman organisaation kesken. Toteutumisen seuranta ja monitorointi voi aiheuttaa esimerkiksi toteutuneen riskin korjaamis- ja toipumisprosessin. Riski voidaan jättää myös huomiotta – vaikutus on tiedossa, mutta toistaiseksi riskiltä päätetään olla suojautumatta.

Tietoturvatyön tavoitteet

Tietoturvatyön tavoitteena on parantaa organisaation kykyä turvata käytössään olevat tiedot erilaisilta niihin kohdistuvilta uhkilta. Tietoturvatoiminta pohjautuu sille asetettuihin vaatimuksiin, joissa määritellään sopivat ja sallitut tavat käsitellä ja säilyttää tietoja: tietojenkäsittely

on suunniteltava ja toteutettava siten, että tietojen saatavuus, oikeellisuus, luottamuksellisuus ja käytön seurattavuus eivät vaarannu.

Tietoturvallisuuden kehittämisen yhteydessä on tunnistettavissa seuraavat osa-alueet, joiden toteutuminen on tärkeää, että kehityksessä voitaisiin onnistua:

1. Tunnistetaan ja määritellään suojattavat tiedot ja syyt, miksi tiedot pitää suojata.
2. Tunnistetaan, miltä tiedot pitää suojata (muuttuminen, katoaminen, paljastuminen ym.).
3. Tunnistetaan riskit, jotka johtavat tietoturvaloukkauksiin.
4. Estetään riskien toteutuminen
   - politiikat, käytettävät standardit ja toimintaprosessit
   - tietoturvaorganisaatio ja hallinnointi
   - henkilöstön koulutus ja osaamisen ylläpito
   - turvalliset tietojärjestelmäarkkitehtuurit, menetelmät ja teknologiat,

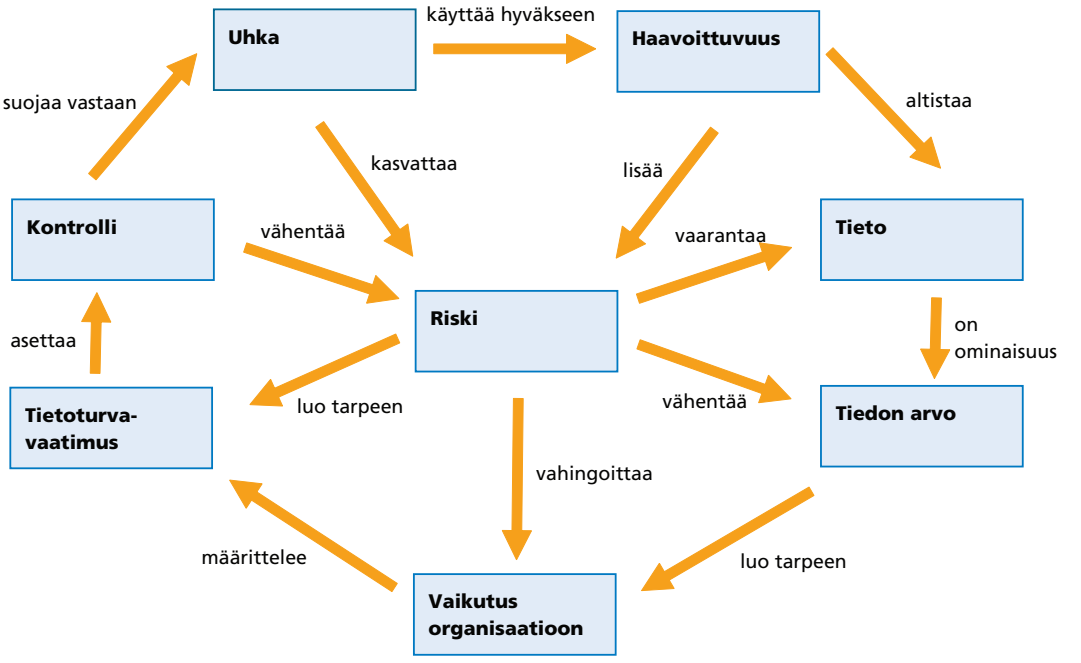
Tietoturvallisuus vaatii ennen kaikkea oikeaa johtamista ja oikeita, kunnollisia menetelmiä. Seuraavassa pikaohjeessa on kuvattuna nimenomaan johdolta vaadittavia toimenpiteitä, jotta turvallisuuspäämäärät voitaisiin parhaiten saavuttaa:

1. Sitoudu, tue ja motivoi.
2. Näytä esimerkkiä.
3. Määritä tavoitteet ja ymmärrä ne.
4. Määritä vastuuhenkilöt ja tietoturvaorganisaatio.
5. Varaa riittävästi resursseja.
6. Huolehdi, että kommunikaatio toimii organisaatiossa ja ettei tietokatkoksia ole.
7. Huolehdi, että koko organisaatio saa riittävästi tietoa ja koulutusta.
8. Valvo, mittaa ja seuraa.
9. Palkitse ja ojenna.

Tietoturvallisuuden toteuttaminen

Tietoturvaa toteutetaan käytännössä erilaisten säätimien ja hallintakeinojen (kontrollien) avulla. Oikein toteutettuna kontrollit voivat olla joko ennalta ehkäiseviä (*proactive*) tai ongelmatilanteissa käynnistyviä tai käynnistettäviä (*reactive*). Yhteisenä näille on se, että ongelmatilanne pyritään korjaamaan ja tietoturvallisuutta vaarantaviin riskeihin varautumaan ennalta suunnitellun mukaisesti. Sopivasti näkyvillä ja näkymättömissä olevat valvontakeinot toimivat myös pelotteena, jolloin on tarkoitus sekä ehkäistä tahallisia väärinkäytösyrityksiä että ohjata oikeutettuja käyttäjiä huolelliseen ja tarkkaan toimintaan.

Tietoturvallisuus toteutetaan suunnitelmallisella työllä: ensin määritellään suojattavat kohteet, siis tiedot ja tietojärjestelmät, niiden arvo ja suojauksen tarve. Tämän jälkeen arvioidaan uhkat ja riskit, jotka uhkaavat suojattavien tietojen turvallisuutta. Kun sekä suojattavat tiedot on määritelty että niitä uhkaavat riskit kartoitettu, voidaan valita sopivat kontrollit – ne toimenpiteet ja säätimet, joilla riskeihin varaudutaan, miten niiden toteutumisesta toivutaan ja ongelmat korjataan sekä miten toimintaa mitataan. Seuraava kuva hahmottaa riskien, haavoittuvuuksien, uhkien ja hallintakeinojen keskinäisiä suhteita.



Riskit, uhkat, haavoittuvuudet ja kontrollit
(lähde: Ross Fraser, ESQ & EHTEL Joint Workshop, Lahti, Finland, 18–19 June 2004)

Tietoturvan ja tietosuojan tekninen toteutus

Teknisiä ratkaisuja ja palveluja, joilla voidaan toteuttaa organisaatiolle asetetut tietosuoja- ja tietoturvavaatimukset, on tarjolla runsaasti. Sähköisen tietojenkäsittelyn alueella uusia tekniikoita ja tietoteknisiä tietoturvajärjestelmiä kehitetään eri yritysten toimesta intensiivisesti. Sen jälkeen kun organisaatio on tunnistanut uhkat ja analysoinut riskit sekä päättänyt niistä kontrolleista, jotka se ottaa käyttöönsä, tulee organisaation valita markkinoilla tarjolla olevista tekniikoista ja palveluista sille teknisesti ja taloudellisesti sopivat ratkaisut.

Valittujen teknisten ratkaisujen tulee toteuttaa samalla kertaa sekä valittu tietoturvan taso että vaadittava tietoturva. Esimerkiksi:

- luottamuksellisuus voidaan saavuttaa tietojen salauksella ja tietojärjestelmien käyttäjien pääsynhallinnalla, käyttöoikeuksien ja suostumusten hallinnalla,
- eheys saavutetaan mm. tarkistussummilla, tarkistuskoodeilla ja digitaalisella allekirjoituksella ja
- käyttäjän todentaminen ja kiistämättömyys voidaan varmistaa mm. käyttämällä PKI:ta soveltavaa järjestelmää ja digitaalista allekirjoitusta.

Tyypillisin käytössä oleva tietojärjestelmien käyttäjien hallinnan, tunnistamisen ja todentamisen menetelmä on käyttäjätunnus-salasanamenetelmä, jossa käyttäjä tunnistetaan käyttäjätunnuksella ja todennetaan oikeaksi ja valtuutetuksi käyttäjäksi salasanalla. Tämä edustaa heikkoa tietoturvaa tyypillisimmillään. Käyttäjällä on yksivaiheinen pääsy tietojärjestelmään – riittää, että hänellä on tiedossaan käyttäjätunnus ja salasana. Vastaavanlainen esimerkki yksivaiheisesta todentamisesta olisi, että pankkiautomaatilla asiointiin riittäisi pelkkä toimikortin käyttö ilman PIN-koodia.

Vahvassa tunnistamisessa tietojärjestelmät tunnistavat ja todentavat käyttäjän kaksivaiheisesti. Kaksivaiheisuudessa yhdistetään kaksi kolmesta ominaisuudesta, jotka voidaan liittää käyttäjään: jotakin, mitä käyttäjä on (käyttäjän henkilökohtainen ts. biometrinen ominaisuus,

kuten kasvokuva, sormenjälki tai DNA), jotakin, mitä käyttäjällä on hallussaan (toimikortti, salasanalista) ja jotakin, mitä käyttäjä tietää (salasana, PIN-koodi). Ensin käyttäjä tunnistetaan jollakin menetelmällä, jonka jälkeen todennus tapahtuu jollakin toisella menetelmällä. Hyvä menetelmä on esimerkiksi sellainen, jossa toimikorttia hyödynnetään käyttäjän tunnistamisessa (jotakin, mikä käyttäjällä on hallussaan) ja vastaavasti PIN-koodia (jotakin, mitä käyttäjä tietää) tai sormenjälkeä (jotakin, mitä käyttäjä on) käyttäjän todentamisessa. Esimerkkinä voidaan käyttää jo edellä mainittua pankkiautomaattiasiointia: saadakseen oikeuden pankkiasiointiin henkilö tarvitsee sekä kortin että PIN-koodin: pankkikortin tunnistamiseen ja kortin käyttöön oikeuttavan PIN-koodin todentamiseen. Vastaava esimerkki vahvasta käyttäjän tunnistamisesta on pankkien verkkoasiointipalveluihin käyttämät menetelmät. Voidakseen asioida verkkopankissa henkilö tarvitsee sekä käyttäjätunnus-salasanayhdistelmän että muuttuvien salasanojen listan. Tässäkin tapauksessa todentaminen on kaksivaiheinen: ensin käyttäjä tietää salaiset tunnuksensa ja salasanansa, jonka jälkeen hänellä on oltava hallussaan muuttuvien salasanojen lista. Jos asiakkaalla ei ole salasanalistaa hallussaan, hänen asiointinsa verkkopankissa estetään.

Jos todentamiseen käytetään esimerkiksi sormenjälkeä, täytyy henkilötietojen ja erityisesti käyttäjän biometristen ominaisuuksien käsittelystä säädettyjä lakeja noudattaa. Vastaavasti, kun kasvokuvan käyttö esimerkiksi passissa on hyväksyttyä, sähköisessä asioinnissa voitaisiin ajatella sormenjäljen käyttöä, koska tietojärjestelmän tekemä luotettava todentaminen kasvokuvasta on erittäin vaikeaa. Joka tapauksessa tämä edellyttäisi, että sormenjälki (ts. kuva tai näyte sormenjäljestä) talletetaan ja säilytetään ainoastaan esimerkiksi henkilön hallussa olevalla toimikortilla vastaavasti, kun kasvokuvakin on ainoastaan passissa. Biometrisistä tunnisteista ei voida ajatella tehtävän rekisteriä, jonka perusteella suoritetaan käyttäjän tunnistaminen. Biometrian käyttö on suotavaa ainoastaan tunnistamis-todentamisprosessin toisessa vaiheessa, kun jo tunnistettu käyttäjä todennetaan biometrista tunnistetta käyttämällä oikeaksi. Joka tapauksessa kaikkien biometristen tunnistusmenetelmien käytöstä on syytä keskustella erikseen tietosuojavaltuutetun kanssa ja hyväksyttää käytettävä menetelmä.

Joissakin keskusteluissa on esiintynyt kysymyksiä, edustavatko esimerkiksi verkkopankkitunnukset aidosti vahvaa tunnistamista – tietäähän myös pankki asiakkaansa käyttäjätunnuksen ja salasanalistat. Pankki ja asiakas ovatkin keskenään sopimussuhteessa ja verkkoasioinnissa osapuolet keskenään, ja tällöin toki vahvan tunnistamisen vaatimukset täyttyvät. Kolmannen osapuolen, esimerkiksi viranomaisen, pitää kuitenkin tarkkaan harkita, voiko se luottaa kyseiseen sopimussuhteeseen ja voidaanko pankkitunnuksia käyttää myös viranomaisasioinnissa, näin tehtäessähän pankilla on tieto asiointitapahtumasta. Tämän lisäksi henkilön tunnukset ovat tosiasiassa myös pankin hallussa, ja halutessaan pankki voisi teoriassa tekeytyä asiakkaakseen. Tämän tietoturvariskin toteutumisen todennäköisyys lienee tosiasiallisesti lähellä nollaa, mutta tärkeää on ainakin ymmärtää riskin olemassaolo. Ymmärtämällä riski voidaan tehdä valintoja, minkä palveluntuottajien (pankit ja vakuutusyhtiöt, kauppojen keskusliikkeet, lentoyhtiöt, hotelliketjut ym.) erilaisiin todentamismenetelmiin luotetaan.

Koulutus ja tietoturvakampanjat

Yksinkertaisin tapa vaikuttaa organisaation tietoturvaan on henkilöstön koulutus ja erilaiset tietoturvakampanjat. Näiden tarkoituksena on pitää tietoturva-asiat ”tuoreena mielessä”, saada ihmiset ymmärtämään tietoturvan merkityksen, motivoitumaan oikeanlaiseen toimintaan ja noudattamaan annettuja ohjeita.

Stakes on laatinut tämän raportin ”Opas sosiaali- ja terveydenhuollon organisaation tietoturvan hallinnointiin” liitteeksi koulutusaineiston, joka on vapaasti kaikkien tietoturvakouluttajien käytössä. Aineisto on saavana Stakesin julkaisuna ja sähköisesti Sosiaali- ja terveysalan tietoyhteiskuntayksikön Internet-sivustolta osoitteesta http://sty.stakes.fi.

STAKES

RAPORTTEJA-sarjassa aiemmin ilmestyneet

2007

Kerttu Perttilä, Minna Uusitalo (toim.): Terveyden edistämisen paikalliset rakenteet ja johtaminen. TEJO-hankkeen väliraportti 2003–2005
Raportteja 4/2007 Tilausnro 4/2007

Maarit Sulavuori: Kehittämistyöllä pallo haltuun. Kehittämisprojektin avulla ideoita lastensuojeluun ja voimavaroja työssä jaksamiseen
Raportteja 3/2007 Tilausnro 3/2007

Päivi Voutilainen (toim.): Laatua laatusuosituksella? Ikäihmisten hoitoa ja palveluja koskevan laatusuosituksen seuranta ja arviointi
Raportteja 2/2007 Tilausnro R2/2007

Päivi Hämäläinen, Jarmo Reponen, Ilkka Winblad: eHealth of Finland. Check point 2006
Report 1/2007 Tilausnro R1/2007

2006

Sinikka Reito: Yhteistyöstä yhteiseen työhön. Ikaalilainen palveluohjaus auttaa työikäistä palvelujärjestelmän labyrintissa
Raportteja 16/2006 Tilausnro R16/2006

Ritva Linnakangas, Asko Suikkanen, Victor Savtschenko, Lauri Virta: Vammaisten osallisuus työmarkkinoilla
Raportteja 15/2006 Tilausnro R15/2006

Päivi Pihlaja, Elina Kontu (toim.): Arjen moninaisuutta. Erityisryhmät päiväkodissa
Raportteja 14/2006 Tilausnro R14/2006

Timo Tuori, Britta Sohlman, Marko Ekqvist, Tytti Solantaus: Alaikäisten psykiatrinen sairaalahoito Suomessa 1995–2004
Raportteja 13/2006 Tilausnro R13/2006

Terhi Hinkka, Juha Koivisto, Riitta Haverinen: Kartoittava kirjallisuuskatsaus sosiaalisen kuntoutuksen työmuodoista ja niiden vaikutuksista
Raportteja 12/2006 Tilausnro R12/2006

Hannele Hyppönen (toim.), Kirsi Hännikäinen, Marja Pajukoski, Pekka Ruotsalainen, Lauri Salmivalli, Emmi Tenhunen: Sähköisen reseptin pilotin arviointi II (2005–2006)
Raportteja 11/2006 Tilausnro R11/2006

Nina Mellin, Jouni Vihmo, Esa Österberg: Alkoholihaittojen yhteiskunnalliset kustannukset Suomessa vuonna 2003
Raportteja 10/2006 Tilausnro R10/2006

Marja Veikkolainen, Päivi Hämäläinen: Sosiaali- ja terveydenhuollon henkilöstön tieto- ja viestintätekniikan koulutus- ja oppimateriaalitarve ja koulutuksen kehittämisen haasteet
Raportteja 9/2006 Tilausnro R9/2006