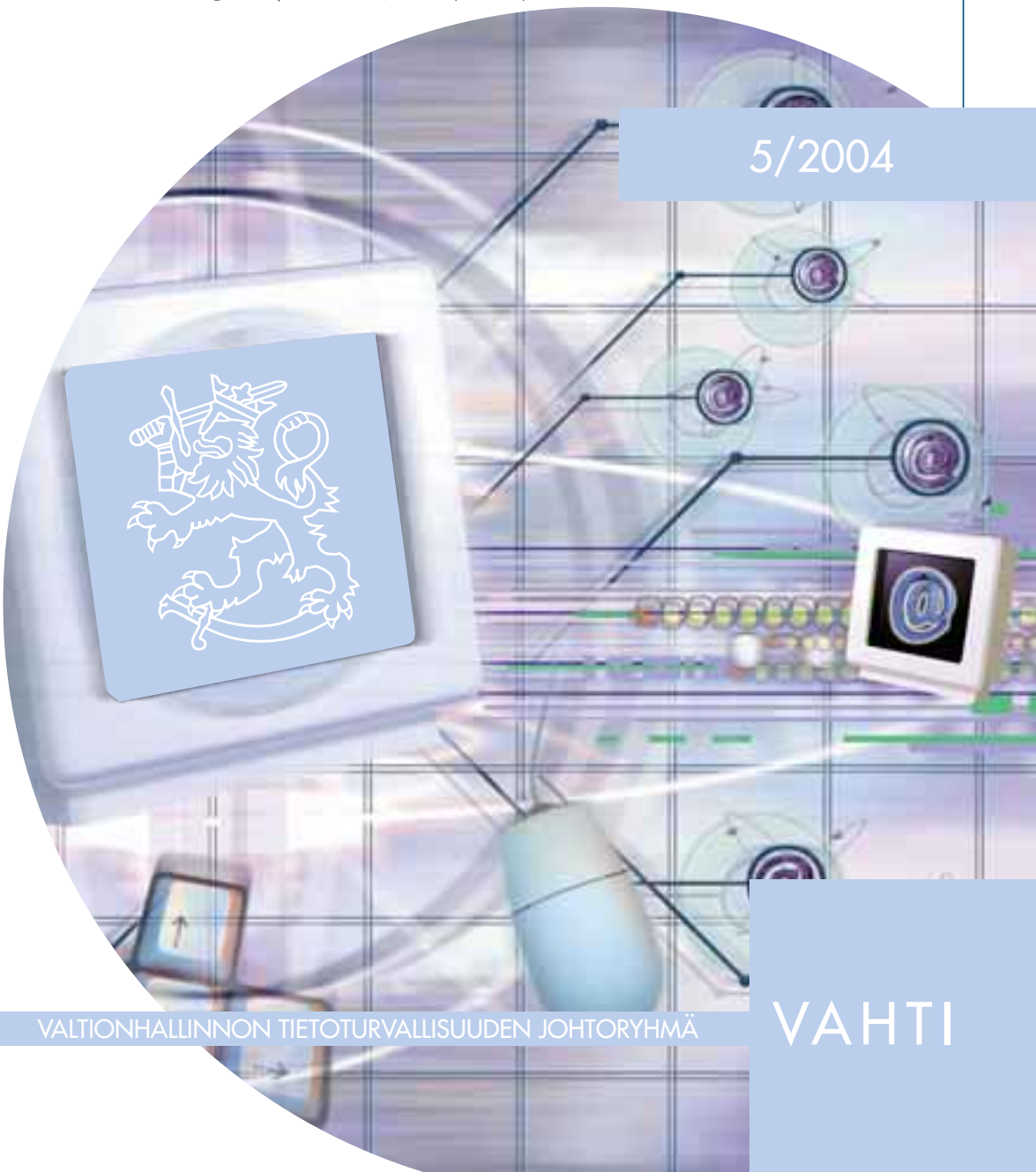
VALTIOVARAINMINISTERIÖ

VALTIONHALLINNON KESKEISTEN TIETOJÄRJESTELMIEN TURVAAMINEN

5/2004



VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

VALTIONHALLINNON KESKEISTEN TIETOJÄRJESTELMIEN TURVAAMINEN

5/2004

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

VALTIOVARAINMINISTERIÖ
Snelmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
vahtijulkaisut@vm.fi

ISSN 1455-2566
ISBN 951-804-467-8 (nid.)
ISBN 951-804-468-6 (PDF)

Edita Prima Oy
HELSINKI 2004

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

OHJE
1.12.2004

Ministeriöille, virastoille ja laitoksille

VALTIONHALLINNON KESKEISTEN TIETOJÄRJESTELMIEN TURVAAMINEN

Valtiovarainministeriö antaa oheisen tietoturvaohjeen (jäljempänä ohje), joka on laadittu ministeriön asettaman ja johtaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimesta. Ohje täydentää laajaa valtiovarainministeriön antamaa tietoturvaohjeistoa. Ohje on osa VM:n käynnistämän valtion tietoturvallisuuden kehitysohjelman (VAHTI-julkaisu 1/2004) toimeenpanoa ja se liittyy mm. perusinfrastruktuuriin suojaamiseen.

Ohjeen tavoitteena on helpottaa valtion keskeisten tietojärjestelmien tietoturvallisuuden parantamista ja näiden järjestelmien turvaamisen erityiskysymysten tunnistamista. Ohjeen pääasiallisina kohderyhminä ovat johto, keskeisten järjestelmien omistajat sekä niiden turvallisuudesta ja toimivuudesta vastaavat henkilöt. Ohje sisältää hyödyllistä tietoa myös teknisille asiantuntijoille ja tietotekniikkatoimittajille. Ohjetta voi käyttää tarkistuslistatyyppisesti apuna myös muiden kuin keskeisten tietojärjestelmien suojaamisessa.

Keskeiset tietojärjestelmät vaativat tietoturvallisuuden osalta merkittäviä ponnistuksia. Ohjeessa kuvataan näitä tietoturvallisuuden vaativia tehtäviä ja osa-alueita. Ohje tukee riippuvuuksien hallintaa ja yhteiskunnan haavoittuvuuksiin liittyvää riskienhallintaa. Ohjeen mukainen toiminta vahvistaa luottamusta eri sidosryhmien turvallisuustasoon.

Valtion organisaatioissa keskeisten tietojärjestelmien turvaamista tulee hoitaa suunnitelmallisesti siten, että tietoturvallisuuden eri osa-alueet mukaan lukien varautuminen häiriötilanteisiin ja poikkeusoloihin tulevat katetuiksi. Erityistä huomiota tulee kiinnittää turvallisuusjohtamiseen ja riskianalyysiin.

Keskeisiin tietojärjestelmiin lasketaan mukaan erityisesti valtion tiedonkäsittelyn tärkeysluokituksen ensimmäisen tärkeysluokan mukaisten virastojen tietojärjestelmiä. Lisäksi keskeisiä tietojärjestelmiä on tyypillisesti myös toisen tärkeysluokan organisaatioissa. Viraston on tietojärjestelmiin tukeutuvan toiminnan riskianalyysiin pohjautuen itse tarkemmin määriteltävä eri tietojärjestelmiensä keskeisyys valtion toiminnan kannalta.

Ohje tulee VAHTIn Internet-sivuille *(www.vm.fi/vahti)* ja sitä kehitetään tarvittaessa mm. VM:n hallinnon kehittämisosastolle (hko@vm.fi) toimitettavan palautteen pohjalta.

Lisätietoja antavat neuvotteleva virkamies, VAHTIn puheenjohtaja Mikael Kiviniemi sekä neuvotteleva virkamies Arja Terho (etunimi.sukunimi@vm.fi).

Toinen valtiovarainministeri Ulla-Maj Wideroos

Ylijohtaja Jorma Karjalainen

Liite Valtionhallinnon keskeisten tietojärjestelmien turvaaminen (VAHTI 5/2004)

1 JOHDON YHTEENVETO

Yhteiskunnan elintärkeät toiminnot toteutetaan keskeisillä tietojärjestelmillä, jotka verkottuneena kokonaisuutena muodostavat valtiotasoisen keskeisen tietojärjestelmän, joka on osa valtionhallinnon perusinfrastruktuuria.

Tietoturvallisuutta ja siihen liittyviä toimenpiteitä valtionhallinnossa ohjaa valtiovarainministeriön hallinnon kehittämisosaston yleisohjaus. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi.

Valtiovarainministeriö ohjaa pitkäjänteisesti valtionhallinnon tietoturvatyötä mm. tietoturvan kehitysohjelmalla. Tämä valtionhallinnon keskeisten tietojärjestelmien turvaamisohje on osa valtion tietoturvallisuuden kehitysohjelman toimeenpanoa.

Jokaisen viraston on itse määriteltävä ne tietojärjestelmät, jotka ovat keskeisiä valtion toiminnan kannalta. Tämän määrittelyn on pohjauduttava toiminnalliseen riskianalyysiin; riskianalyysiin on sisällytettävä virastojen väliset riippuvuudet.

Virastot muodostavat verkottuneen kokonaisuuden, jonka tietoturvallisuuden hallinnointi on haasteellinen tehtävä. Keskeinen tehtävä tällaisen laajan kokonaisuuden tietoturvallisuuden hallinnoinnissa on kattava tietoturvallisuuden organisointi ja vastuutus.

Viraston ylimmän johdon tulee johtaa tietoturvallisuutta ja sen kehittämistä. Tässä ohjeessa korostetaan suunnitelmallisuuden, riskien analysoinnin ja turvallisuusjohtamisen merkitystä.

Tietoturvallisuutta ohjataan säädöksillä, määräyksillä ja ohjeilla. Tässä ohjeessa on tuotu esille tietoturvallisuuden kehittämisessä huomioitavia säädöksiä, määräyksiä sekä ohjeita. Johdon keskeinen tehtävä on vastata siitä, että niitä noudatetaan läpi koko viraston ja sen toiminnan. Tässä tulee käyttää tukena sekä itsearviointeja ja ulkoisia arviointeja että sisäisiä ja ulkoisia auditointeja.

Vertaiskehittäminen on eräs tärkeä menettelytapa laajan verkottuneen kokonaisuuden tietoturvallisuuden parantamisessa. Tällä tuetaan tasalaatuisen ja korketasoisen tietoturvallisuuden saavuttamista. Tässä dokumentissa kuvataan keskeisten tietojärjestelmien edellyttämien tietoturvavaatimusten lisäksi myös ns. tietoturvallisuuden perustaso, joka jokaisen viraston tulee vähintään saavuttaa.

Keskeisten tietojärjestelmien toiminnan jatkuvuus on oleellista. Järjestelmät tulee toteuttaa siten, että niiden ydintoiminnot ovat käytettävissä kaikissa tilanteissa. Järjestelmien vähemmän tärkeistä toiminnoista tulee pystyä luopumaan hallitusti lohkomalla järjestelmät osakokonaisuuksiin.

Ohjeessa ei anneta yksityiskohtaisia toimintamalleja ja -sääntöjä, vaan virastojen edellytetään tukeutuvan laajaan, olemassa olevaan viitemateriaaliin. Virastolla tarkoitetaan tässä ohjeessa kaikkia valtionhallinnon organisaatiotyyppejä. Työntekijällä tarkoitetaan tässä ohjeessa kaikkia henkilöitä, jotka ovat viraston palveluksessa kuten virka- ja työsopimussuhteisia.

Sisällys

1 JOHDON YHTEENVETO 5
2 JOHDANTO 11
2.1 Kohdejärjestelmät 11
2.2 Kohderyhmä 13
2.3 Sisältö 13
2.4 Käyttötapa 14
2.5 Ohjeen laatiminen 15
3 LÄHTÖTILANNE JA TAVOITTEET 17
3.1 Lähtötilanne 17
3.2 Tavoitteet 18
3.2.1 Lyhyen aikavälin tavoitteet 19
3.2.2 Pitkän aikavälin tavoitteet 19
4 KESKEISTEN TIETOJÄRJESTELMIEN ERITYISHAASTEITA 21
4.1 Tietoturvakulttuurin rakentaminen 21
4.2 Haasteita 22
4.2.1 Johdon sitoutuminen ja vastuu 22
4.2.2 Eheys 22
4.2.3 Käytettävyys 22
4.2.4 Luottamuksellisuus 22
4.2.5 IT-arkkitehtuuri 23
4.2.6 Tietojärjestelmäkehitys 23
4.2.7 Dokumentaatio 23
4.2.8 Ylläpito 24
4.2.9 Testaus 24
4.2.10 Henkilöresurssit 24
4.2.11 Ulkoistaminen 24
4.2.12 Sidosryhmäyhteistyö 25
4.2.13 Poikkeusolot 25
4.3 Keskeisten järjestelmien luokittelu 25
4.3.1 Eheys, käytettävyys ja luottamuksellisuus tärkeitä 26
4.3.2 Eheys ja käytettävyys tärkeitä 26
4.3.3 Eheys ja luottamuksellisuus tärkeitä 26
5 HALLINNOLLINEN TURVALLISUUS 27
5.1 Tietoturvallisuuden johtaminen 30
5.2 Suhteet sidosryhmiin ja asiakkaisiin 32
5.3 Hankinnat 33
5.3.1 Laitehankinnat ja huolto 33
5.3.2 Käyttö-, hallinta- ja tietojenkäsittelypalvelut 34
5.3.3 Valmisohjelmistohankinnat 34
5.3.4 Sovelluskehitys 35
5.3.5 Konsultointi- ja asiantuntijapalvelut: 35
5.4 Dokumentointi 35
5.5 Muutoksen hallinta 36

5.6 Varautuminen poikkeusoloihin 37
5.7 Järjestelmäluokkien erityispiirteet 37
5.7.1 Eheys, käytettävyys ja luottamuksellisuus tärkeitä 37
5.7.2 Eheys ja käytettävyys tärkeitä 37
5.7.3 Eheys ja luottamuksellisuus tärkeitä 38
6 HENKILÖSTÖTURVALLISUUS 39
6.1 Henkilöstön toimenkuvat 41
6.2 Henkilöstön soveltuvuus 42
6.3 Henkilöstön osaamisen varmistaminen 43
6.4 Avainhenkilöstö 43
6.5 Työhöntuloprosessi 44
6.6 Prosessi työsuhteen päättyessä (tai keskeytyessä pitkäksi ajaksi) 44
6.7 Sijais- ja väliaikaisjärjestelyt 45
6.8 Työnkierto ja lomat 45
6.9 Ulkopuolinen työvoima 45
6.10 Varautuminen poikkeusoloihin 46
6.11 Järjestelmäluokkien erityispiirteet 46
6.11.1 Eheys ja käytettävyys tärkeitä 46
6.11.2 Eheys ja luottamuksellisuus tärkeitä 46
7 FYYSINEN TURVALLISUUS 47
7.1 Yleistä 48
7.2 Tilat 49
7.3 Olosuhdehallinta 49
7.4 Toiminta tiloissa 50
7.5 Henkilö- ja tavaraliikenne 50
7.6 Poistumistiet ja pelastustoimen reitit 50
7.7 Turvavalaistus 51
7.8 Palontorjunta 51
7.9 ATK- ja teletilojen pakko-ohjaukset 51
7.10 Rikosilmoitinjärjestelmät 51
7.11 TV- ja videovalvonta 52
7.12 Tekniset henkilöturvajärjestelmät 52
7.13 Väestönsuojat 52
7.14 Sähkönsyötön turvaaminen 52
7.15 Teletilat ja -reitit 52
7.16 Viestijärjestelmät 52
7.17 Asennuslattia 53
7.18 Varautuminen poikkeusoloihin 53
7.19 Järjestelmäluokkien erityispiirteet 53
7.19.1 Eheys, käytettävyys ja luottamuksellisuus tärkeitä 53
7.19.2 Eheys ja käytettävyys tärkeitä 53
8 TIETOLIIKENNETURVALLISUUS 54
8.1 Suunnittelu 55
8.2 Dokumentaatio 56
8.3 Palomuurit 56
8.4 Verkon varmistukset ja varajärjestelyt 57

8.5 Operointi ja valvonta....57
8.6 Langattomat tietoliikenneyhteydet....58
8.7 Ulkopuoliset yhteydet ja palvelut....58
8.8 Varautuminen poikkeusoloihin....59
8.9 Järjestelmäluokkien erityispiirteet....59
8.9.1 Eheys, käytettävyys ja luottamuksellisuus tärkeitä....59
8.9.2 Eheys ja käytettävyys tärkeitä....59
8.9.3 Eheys ja luottamuksellisuus tärkeitä....59
9 LAITTEISTOTURVALLISUUS....61
9.1 Käytettävyys....62
9.2 Toiminta, seuranta ja laajennettavuus....63
9.3 Käyttöönotto....63
9.4 Kunnossapito....63
9.5 Käytöstä poisto....63
9.6 Laadunvarmistus....64
9.7 Laitetyyppien erityisvaatimuksia....64
9.7.1 Palvelimet....64
9.7.2 Päätelaitteet....64
9.7.3 Verkkolaitteet....65
9.7.4 Levyjärjestelmät....65
9.8 Varautuminen poikkeusoloihin....66
9.9 Järjestelmäluokkien erityispiirteet....66
9.9.1 Eheys ja käytettävyys tärkeitä....66
9.9.2 Eheys ja luottamuksellisuus tärkeitä....66
10 OHJELMISTOTURVALLISUUS....67
10.1 Ohjelmistot....69
10.1.1 Käyttöjärjestelmät....69
10.1.2 Tietoliikenneohjelmistot....70
10.1.3 Tietoturvaohjelmistot....70
10.1.4 Valmissovellukset....70
10.1.5 Räätälöidyt valmissovellukset....70
10.1.6 Teetetyt sovellukset....71
10.1.7 Itse tehdyt sovellukset....73
10.1.8 Välitason sovellukset....73
10.1.9 Sovelluskehitystyökalut....73
10.1.10 Tietoturvallinen ohjelmointi....73
10.2 Ohjelmistoasennukset....74
10.3 Turvallisuustoimet....74
10.4 Tarkkailu- ja paljastustoimet....77
10.5 Varautuminen poikkeusoloihin....77
10.6 Järjestelmäluokkien erityispiirteet....77
10.6.1 Eheys ja käytettävyys tärkeitä....77
10.6.2 Eheys ja luottamuksellisuus tärkeitä....78
11 TIETOAINEISTOTURVALLISUUS....79
11.1 Tietojen luokitus ja tietojärjestelmien luokittelu käytettävien tietojen perusteella....81

11.2 Omistajuus ja käyttöoikeudet 81
11.3 Salassapitosopimukset 82
11.4 Dokumenttien hallinta 82
11.5 Tietoaineiston eheyden varmistaminen 82
11.6 Tietovälineiden käsittely 82
11.7 Tietoaineiston säilytys ja arkistointi 83
11.8 Tietoaineiston varmuuskopiointi 83
11.9 Tietoaineiston jakelu, luovutus, tulostus 83
11.10 Tietoaineiston hävittäminen 84
11.11 Yksityisyyden suoja 84
11.12 Varautuminen poikkeusoloihin 84
11.13 Järjestelmäluokkien erityispiirteet 85
11.13.1 Eheys ja luottamuksellisuus tärkeitä 85
12 KÄYTTÖTURVALLISUUS 86
12.1 Ulkoistaminen ja sopimukset 89
12.2 Etäkäyttö, etätyö ja etähallinta 90
12.3 Prosessien hallinta 91
12.4 Muutosten hallinta 92
12.4.1 Päivitykset 92
12.4.2 Korjauspäivitykset 93
12.4.3 Tietoturvakorjaukset 93
12.4.4 Järjestelmäintegroinnit 93
12.4.5 Toimittajavaihdokset 93
12.5 Varautuminen poikkeusoloihin 93
12.6 Järjestelmäluokkien erityispiirteet 94
12.6.1 Eheys ja käytettävyys tärkeitä 94
12.6.2 Eheys ja luottamuksellisuus tärkeitä 94
13 TIETOTURVALLISUUDEN ARVIOINTI 95
13.1 Itsearviointi 95
13.2 Ulkoinen arviointi 95
13.3 Sisäinen tarkastus 95
13.4 Ulkoinen auditointi 96
13.5 Mittaaminen 96
13.6 Valvonta 97
13.7 Yhteistyökumppaneiden arviointi 97
14 LIITTEET 98
Liite 1: Lainsäädäntö 99
Liite 2: Ohjeet ja määräykset 102
Liite 3: Standardit, parhaat käytännöt 104
Liite 4: Sanasto 106
Liite 5: Kotimaiset viitteet 107
Liite 6: Ulkomaiset viitteet 108
Liite 7: Valtion ja virastojen yhteiset tietoturvaorganisaatiot 109
Liite 8: Liitteet 110

2 JOHDANTO

2.1 Kohdejärjestelmät

Määritelmä: Keskeiset tietojärjestelmät ovat tietojärjestelmiä, jotka toteuttavat tai tukevat toimintoja, joiden puuttuminen, tietojen virheellisyys tai paljastuminen tuottavat yhteiskunnalle suuria taloudellisia tai muita vahinkoja. Toiminnot voivat olla myös sellaisia, että niiden puuttuminen tai häiriintynyt toiminta vaikuttaa yhteiskuntaa tai organisaation toimintaa lamauttavasti tai henkilöiden turvallisuutta heikentävästi.

Keskeinen tietojärjestelmä voi muodostua useasta, keskenään kommunikoivasta tietojärjestelmästä.

Normaalioloissa käytettävien keskeisten tietojärjestelmien lisäksi on olemassa myös keskeisiä tietojärjestelmiä, joita käytetään vain poikkeusoloissa.

Tässä ohjeessa keskitytään kuvaamaan valtionhallinnon keskeisten tietojärjestelmien tietoturvallisuudessa huomioitavia asioita ja toimenpiteitä. Keskeiset tietojärjestelmät vaativat tietoturvallisuuden osalta merkittäviä ponnistuksia, ja tässä ohjeessa kuvataan erityisesti tietoturvallisuuden vaativimpia tehtäviä ja osa-alueita.

Keskeisiin tietojärjestelmiin lasketaan mukaan erityisesti valtionhallinnon tiedonkäsittelyn tärkeysluokituksen ensimmäisen tärkeysluokan mukaisten virastojen tietojärjestelmiä, mutta yllä olevan määrittelyn mukaisesti löytyy myös muita keskeisiä tietojärjestelmiä tyypillisesti toisen tärkeysluokan organisaatiosta. Viraston on tietojärjestelmään tukeutuvan toiminnan riskianalyysiin pohjautuen itse määriteltävä, onko tietojärjestelmä valtionhallinnon toiminnan kannalta keskeinen vai ei.

Valtiovarainministeriö on laatinut ministeriöiden, virastojen ja laitosten tiedonkäsittelyn tärkeysluokituksen. Viraston sijainti tärkeysluokituksessa on myös hyvä indikaatio siitä ovatko viraston tietojärjestelmät keskeisiä.

Keskeisille tietojärjestelmille tyypillistä on:

- Keskeinen liityntä yhteiskunnan elintärkeisiin toimintoihin
  - Valtion johtaminen
    - Valtionjohdon päätöksenteko
    - Valtakunnan johtamisjärjestelmä
  - Ulkoinen toimintakyky
    - Ulkoministeriön ja ulkomaanedustuksen toimintavalmius
    - Ulkomaankauppa
    - Hallinnonalojen kansainvälinen yhteydenpito
    - Suomen kansalaisten avustaminen ulkomailla
    - EU:n sisärajat ylittävä yhteistoiminta
- Valtakunnan sotilaallinen puolustus
  - Puolustusjärjestelmä
- Sisäinen turvallisuus
  - Laillinen oikeus ja yhteiskuntajärjestys
  - Yleinen järjestys ja turvallisuus
  - Yhteiskunnan suojaaminen
  - Pelastustoiminta
  - Rajavalvonta
- Talouden ja yhteiskunnan toimivuus
  - Talouspolitiikka
  - Viestintäjärjestelmät ja liikenne
  - Yhteiskunnan perustoimintojen ylläpitäminen
- Väestön toimeentuloturva ja toimintakyky
  - Sosiaaliturva
  - Sosiaali- ja terveydenhuollon palvelujärjestelmä
  - Terveysuhkien havainnointi-, seuranta- ja torjuntajärjestelmät
- Henkinen kriisinsietokyky
  - Tiedotustoiminta
  - Opetustoiminta
  - Hengellinen toiminta
  - Kulttuuritoiminta
- Aikakriittisyys – tietojärjestelmän jatkuva toiminta on välttämätöntä
- Toiminnan ohjaus – esim. sulautetut järjestelmät, energiajakeluverkkojen ohjaus, liikenteenohjaus, yms.
- Korvaamattomuus – toimintaa ei voida korvata toisen organisaation järjestelmällä tai manuaalitoiminnoilla

2.2 Kohderyhmä

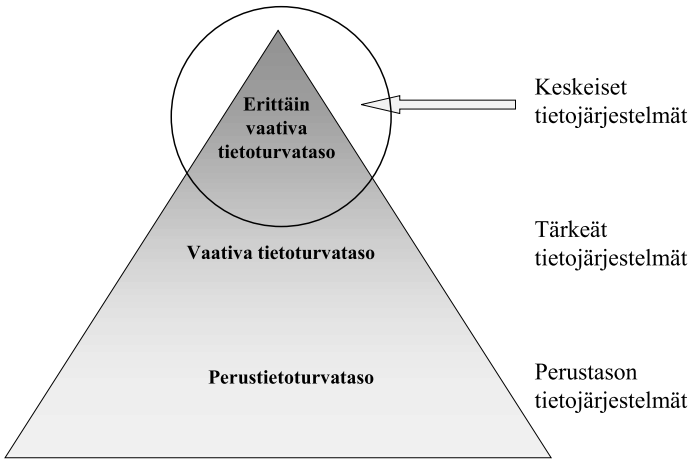
Ohjeen kohderyhmänä ovat pääasiassa valtion virastojen johto, keskeisten järjestelmien omistajat sekä niiden turvallisuudesta ja toimivuudesta vastaavat henkilöt. Ohje sisältää hyödyllistä taustatietoa myös teknisille asiantuntijoille sekä tuote- ja palvelutoimittajille. Ohjetta voidaan soveltuvin osin käyttää myös valtionhallinnon ulkopuolella.

Ohjeen lukijoilta edellytetään hyvää yleiskäsitystä tietoturvallisuudesta ja peruskeinoista tietoturvallisuuden parantamiseksi.

2.3 Sisältö

Ohje on keskeisten tietojärjestelmien turvallisuuden erityisvaatimuksiin keskittyvä. Ohjeessa oletetaan perustavaa laatua olevien ja tärkeimpien tietoturvatarpeiden ja -tehtävien olevan tiedossa ja niiden osalta viitataan olemassa olevaan ohjeistukseen. Muusta ohjeistuksista löytyviä tärkeimpiä asioita on paikoitellen korostettu tässäkin ohjeessa.

Ohje ei sisällä teknisiä ratkaisuja ja yksityiskohtia. Keskeisen tietojärjestelmän tietoturvallisuuden lähtötason vaatimukset on esitetty taulukkoina osa-alueittain lukujen alussa. Lähtötasolla kuvataan keskeisen tietojärjestelmän perustietoturvatehtävät, jotka oletetaan olevan kunnossa ja jotka on kuvattu hyvin viitemateriaaleissa. Tärkeimmät viitteet ja standardit tietoturvallisuuden kehittämiseksi ja toteuttamiseksi ovat samoin taulukkoina osa-alueittain. Kuva 1 esittää tämän ohjeen fokuksen.



Kuva 1: Ohjeen fokus

Ohjeen rakenne perustuu valtionhallinnon käyttämään tietoturvallisuuden VAHTI-jaotteluun, mutta sisältöä on laajennettu:

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

Ohjeen sisältöön vaikuttivat erityisesti:

- Hallituksen tietoyhteiskuntastrategia
- Kansallinen tietoturvastrategia 4.9.2003
- Valtion tietoturvallisuuden kehittämisohjelma
- Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia 27.11.2003
- Valmiuslaki
- Laki valtion talousarviosta annetun lain muuttamisesta (217/2000) ja muutokset (1216/2003)
- Talousarvioasetus 15.4.2004
- VAHTI-ohjeistus

Ohjeessa on esitetty myös laajempia tavoitteita valtionhallinnon tietojärjestelmien tietoturvallisuuden kannalta sekä kannanottoja tietoturvallisuuden tason mittaamiseksi.

2.4 Käyttötapa

Tätä ohjetta ei tule käyttää yksinään tietoturvallisuuden kehittämiseen ja toteuttamiseen. Ohjeen käyttäjältä oletetaan hyvää tietämystä tietoturvallisuudesta. Ohje auttaa keskeisten järjestelmien tietoturvallisuuden erityiskysymysten huomioimisessa, mutta varsinaiset toimenpiteet löytyvät pääasiassa esitetyistä viitteistä. Ohjeessa oletetaan perusturvallisuuden olevan jo hallinnassa.

Ohjeessa korostetaan riskianalyysin ja lähtötilanteen tuntemuksen vaatimusta. Viraston on selvitettävä oma tietoturvallisuuden lähtötilanteensa kattaen valtionhallinnon tietoturvallisuusjaottelun kaikki osa-alueet. Viraston on myös kuvattava keskeiset tietojärjestelmänsä kokonaisuudessa, mukaan lukien arkkitehtuurit, tietoliikenneratkaisut, sidosryhmäriippuvuudet ja toimintaprosessit. Toiminnasta ja siihen liittyvästä tietojärjestelmästä on tehtävä riskianalyysi, joka toimii jatkossa tietoturvaratkaisujen ja päätösten perustana.

Tämä ohje on tehty valtionhallinnon näkökulmasta keskeisistä tietojärjestelmistä vastaaville, mutta ohjetta voi soveltaa tietoturvakriittisiin järjestelmiin myös valtionhallinnon ulkopuolella. Ohje toimii myös tarjouspyyntöjen valmistelussa ja tarjousten arvioinnissa sekä tietojärjestelmäauditointien apuvälineenä tarjoten näiden järjestelmien tietoturvan vähimmäistason.

Ohjeeseen ei ole sisällytetty viitteitä aihepiiriin liittyviin salassapidettäviin dokumentteihin.

2.5 Ohjeen laatiminen

Ohje laadittiin valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) alaisuudessa ja ohjauksessa. Tehtävään nimetyn työryhmän kokoonpano oli seuraava:

Puheenjohtaja:
Hellevi Huhanantti, Tietoturvapäällikkö,Väestörekisterikeskus

Jäsenet:
Lars Gröndahl, Erityisasiantuntija, Verohallitus
Kimmo Helaskoski, Järjestelmäpäällikkö, Pääesikunta
Kalervo Jakonen, Tietoturvapäällikkö, Tullihallitus
Riku Kalinen, Järjestelmäasiantuntija, Suojelupoliisi
Kari Kekki, Tietohallintojohtaja, Valtiovarainministeriö
Pirkko Kilpeläinen, Tietoturvallisuuspäällikkö, Ilmatieteen laitos
Pentti Kurjenluoma, Projektijohtaja, TE-keskukset, Kauppa- ja teollisuusministeriö
Erkki Liutu, Tietohallintopäällikkö, Keskusrikospoliisi
Perttu Luhtakanta, Osastoesiupseeri, Pääesikunta
Seppo Sauvala, Kehityspäällikkö, Huoltovarmuuskeskus
Juhani Sillanpää, Tietoturvallisuusasiantuntija, Valtioneuvoston tietohallintoyksikkö
Pekka Sinkkilä, Tietohallintopäällikkö, Liikenne- ja viestintäministeriö
Seppo Sundberg, Tietoturvapäällikkö, Valtiokonttori
Arja Terho, Neuvotteleva virkamies, Valtiovarainministeriö

Työryhmän konsultit ja sihteerit:
Jari Pirhonen, Tietoturvallisuuskonsultti, Netsol Oy
Pekka Viitasalo, Tietoturvallisuuskonsultti, Netsol Oy

VAHTIn perustama työryhmä aloitti työskentelynsä 12.11.2003 ja kokoontui 15 kertaa ajanjaksolla 12.11.2003 – 4.11.2004.

VAHTI ohjasi ryhmän työtä mm. kokouksissaan elokuussa ja marraskuussa 2004. VAHTI päätti ohjeen viimeistelystä ja julkaisemisesta marraskuussa 2004. Ohje viimeisteltiin VM/HKOn, VRK:n ja verohallinnon edustajien toimesta.

Tämän ohjeen lisäksi työryhmä on laatimassa esitystä tärkeimmiksi toimenpiteiksi valtion keskeisten tietojärjestelmien tietoturvallisuuden edelleen kehittämiseksi.

3 LÄHTÖTILANNE JA TAVOITTEET

3.1 Lähtötilanne

Kattavaa nykytilan analyysiä ei voitu aikataulun ja resurssien puitteissa tehdä. Arvio perustuu työryhmän jäsenten tietämykseen sekä käytettyyn taustamateriaaliin.

Yhteiskunnan ydintoiminnot rakentuvat yhä enenevässä määrin tieto- ja viestintätekniikan (ICT) varaan. Tietoverkoista on tullut yksi yhteiskunnan perusinfrastruktuuri, jonka toimivuudesta koko yhteiskunta on tullut riippuvaiseksi.

Tietoverkoissa korostuu Internetin ja tulevan langattoman internetin asema ja merkitys. Toisaalta tietojärjestelmien toimivuus riippuu yhteiskunnan muusta perusinfrastruktuurista, kuten sähköverkosta ja logistiikkajärjestelmistä. Suomen sähköverkko on kytketty naapurivaltioiden sähköverkkoihin, jolloin niissä mahdollisesti ilmenevät häiriöt voivat levitä Suomen sähköverkkoon ja sitä kautta tietojärjestelmiin aiheuttaen toiminnan pysähtymisen kokonaan tai osittain.

Valtioneuvosto on tehnyt 27.11.2003 päätöksen, jonka tarkoituksena on strategiatasolla turvata yhteiskunnan elintärkeät toiminnot (Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, Valtioneuvoston periaatepäätös 27.11.2003). Strategia sisältämät tavoitteet tulee saada myös osaksi jokapäiväistä operatiivista toimintaa, siten että niitä seurataan ja valvotaan reaaliaikaisesti.

Suomi on sitoutunut ja tulee myös vastaisuudessa sitoutumaan erilaisiin EU:n tietotekniikkastrategioihin ja -toimintaohjelmiin. Tämä aiheuttaa Suomelle velvoitteita.

Myös kansainväliset sopimukset sekä kansainvälinen lainsäädäntö antavat pakottavia reunaehtoja niille yrityksille, jotka käyvät kansainvälistä kauppaa. Esimerkiksi USA:n Sarbanes-Oxley-laki vuodelta 2002 velvoittaa yritykset tallentamaan kaiken liiketoimintaan liittyvän aineiston. EU-lainsäädäntö tullee seuraamaan USA:n esimerkkiä omien kokemustensa pohjalta.

OECD antoi vuonna 2002 suosituksen tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteiksi. Periaatteet esittävät tarpeen lisätä turvallisuustietoisuutta ja -ymmärrystä, johon liittyy turvallisuuskulttuurin kehittämistarve.

Sähköisen kaupankäynnin ja asiakirjahallinnon kautta valtionhallinto on jo nyt vahvasti kytkeytynyt tietoverkkojen ja -järjestelmien välityksellä yksityiseen sektoriin. Tästä ovat hyviä esimerkkejä TYVI-palvelut (Tietovirrat Yritysten ja Viranomaisten välillä) ja EU-tasolla valtionhallintojen tiedonvaihtoyhteistyö. Kehitys tulee jatkumaan voimakkaasti ja myös kansainvälinen viranomaisten ja yksityisen sektorin yhteistyö tulee voimistumaan. Tämä tuo tietoturvallisuuden kannalta yhä vaativampia asioita ratkaistavaksi.

Nykyisin palveluita pyritään kokoamaan yhteen www-pohjaisilla portaaleilla, johon on linkitetty lukuisa joukko erilaisia palveluita. Palvelujen huonosti kontrolloitu yhdistäminen saattaa aiheuttaa tietoturvallisuuden tai tietosuojan kannalta ei toivottuja tietojen yhdistelmiä.

Monet nykyiset tietoturvaongelmat ratkeavat uusilla tekniikoilla, mutta toisaalta samaan aikaan tulee uusia tietoturvauhkia, jotka vaativat yhä laajempaa osaamista toiminnasta ja sen riskeistä sekä samanaikaisesti yhä laajempaa osaamista tietotekniikan tietoturvariskeistä. Ongelmat ja riskit on pystyttävä ratkomaan yhä geneerisemmällä tasolla ja mallintamalla asiat riittävästi. Yhteistoiminta toimivien osapuolien välillä on tässäkin oleellisen tärkeää.

Toimintojen yhä lisääntyvä ulkoistaminen tuo uusia tietoturvariskejä ja jotkut tietoturvariskit saattavat kasvaa. Myös ulkoistettavien toimintojen koko kasvaa. Tämäkin tuo uusia tietoturvariskejä.

Valtioneuvosto hyväksyi kansallisen tietoturvastrategian 2003 ja sen tavoitteiden saavuttamiseksi on käynnistetty useita hankkeita.

Kukin virasto omalla toiminnallaan edistää sekä omaa että koko valtionhallinnon tietoturvallisuutta.

3.2 Tavoitteet

VM on käynnistänyt valtion tietoturvallisuuden kehitysohjelman (VAHTI 1/2004), jolla kehitetään laaja-alaisesti hallinnon tietoturvallisuutta. Kehitysohjelmaan sisältyy myös perusinfrastruktuurin turvaaminen. Kehitysohjelmaan sisältyy kaikkiaan 28 kehittämiskohdetta.

Seuraaviin kirjattuihin tavoitteisiin sisältyy myöskin sellaisia tavoitteita, jotka on jo saavutettu.

3.2.1 Lyhyen aikavälin tavoitteet

Organisaatioiden on kattavasti dokumentoitava tietojärjestelmänsä ja toimintaprosessinsa. Oman toiminnan ja tietojärjestelmäkokonaisuuden ymmärtäminen on perusta kattavan riskianalyysin muodostamiselle. Riskianalyysi puolestaan toimii tietoturvaratkaisujen perustana.

Organisaatioiden on riskianalyysiin pohjautuen muodostettava tietoturva-arkkitehtuuri, jonka pohjalta tietoturvaratkaisuja voidaan jatkossa toteuttaa. Tavoitteena tulee olla ympäristö, jossa tietoturvallisuutta voidaan rakentaa hallitusti ja yhteen toimivasti.

Organisaatioiden kehittämisen ja tietotekniikan hyödyntämisen tulee perustua prosessikehittämiseen Prosessikehittäminen tulee tehdä siten, että toimintaprosessit linkitetään riittävän selkeästi toimintojen hyödyntämiin tietojenkäsittelyprosesseihin.

Riittävän kattava prosessien kuvaaminen ja prosessimainen toiminta takaavat häiriötilanteissa nopean toipumisen, mikä on yksi hyvän tietoturvallisuuden hallinnan merkki.

Valtionhallinnon tietojärjestelmät on liitetty yleiseen tietoverkkoon, Internetiin. Tätä kautta myös valtionhallinnon tietojärjestelmät ovat haittaohjelmien aiheuttamien häiriöiden kohteena. Haittaohjelmilta tulee suojautua lohkomalla verkot tarvittaviin osaverkkoihin koko valtionhallinnon tasolla sekä organisaatioittain. Verkkojen ja niiden lohkojen välillä tulee olla riittävät suojaus- ja valvontamekanismit, jotta häiriöiltä voidaan suojautua. Suojausmekanismien tulee kattaa myös verkkojen ja järjestelmien sisäisen toiminnan suojaaminen ja valvonta. Valvontamekanismien tulee olla lainsäädännön asettamien vaatimusten mukaiset. Niiden keräämiä tietoja tulee käsitellä huolellisesti mm siksi, että tiedot pätisivät oikeudessa.

Riippuvuutta yleisestä tietoverkosta tulee vähentää tarvittavilla erillisverkoilla ja mahdollisella vain valtionhallinnon omaan käyttöön tarkoitetulla, suljetulla verkolla sekä siihen liitetyillä palvelukeskuksilla, joihin valtionhallinnon keskeisten tietojärjestelmien järjestelmät on sijoitettu riittävästi hajasijoitettuna.

3.2.2 Pitkän aikavälin tavoitteet

Tietoturvatyön tulee integroitua viraston normaaliin toimintaan siten, että tehdyt ratkaisut ovat harkittuja, perusteltuja ja normaaliin työhön sisältyviä. Tavoitteena tulee olla suojattu, testattu, dokumentoitu, mitattu ja jatkuvassa seurannassa, valvonnassa ja kehitysprosessissa oleva järjestelmä.

Uuden kehittäminen vaatii myös ylimääräisiä määrärahoja ja muita resursseja. Laadukkaat, tietoturvalliset ja asiakasohjautuneet tietotekniset palvelut mahdollistavat toiminnan tehostamisen ja sen laadun ja varmuuden parantamisen, jonka kautta taas saadaan tarvittavat säästöt kehittämisen perusteluiksi. Tulosohjaukseen ja hankesuunnitelmiin tulee kuulua kustannus–hyöty-analyysit sisältäen riittävän kattavan tietoturvatarkastelun.

Yhteistyön pitää olla toimivaa valtionhallinnon sekä kunnallisen ja yksityisen sektorin välillä. Yhteistoiminnan tulee kattaa myös tutkimus- ja koulutusorganisaatiot sekä standardointiorganisaatiot.

Yksi toiminnan kehittämismenetelmä on matriisimainen toiminta kattaen organisaatioiden ja tarvittavien elimien sisäisen ja niiden välisen toiminnan soveltuvissa kohteissa, kattaen myös kansainvälisen näkökulman. Tähän tulee yhdistää tarvittava laatutoiminta.

Valtionhallinnon organisaatioiden ja työntekijöiden tietoturvaosaamisen ja -tietoisuuden taso tulee olla korkealla tasolla. Tätä tulee tukea tarvittavilla uusilla tietoturvatehtävillä ja -orgaaneilla sekä tarvittavalla lainsäädännöllä organisaatio-, kansallisella ja kasainvälisellä tasolla sekä riittävällä yhteistyöllä koulutus ja tutkimuslaitosten kanssa.

Valtionhallinnolle on tarpeen kehittää tietotekniikan hallintaan oma rakenteellinen, teknisistä ratkaisuista riippumaton ja riittävän stabiili malli, joka tukee organisaatioiden tietotekniikkapalvelujen hankintaa ja muodostamista, kustannusten hallintaa ja arkkitehtuurien muodostamista.

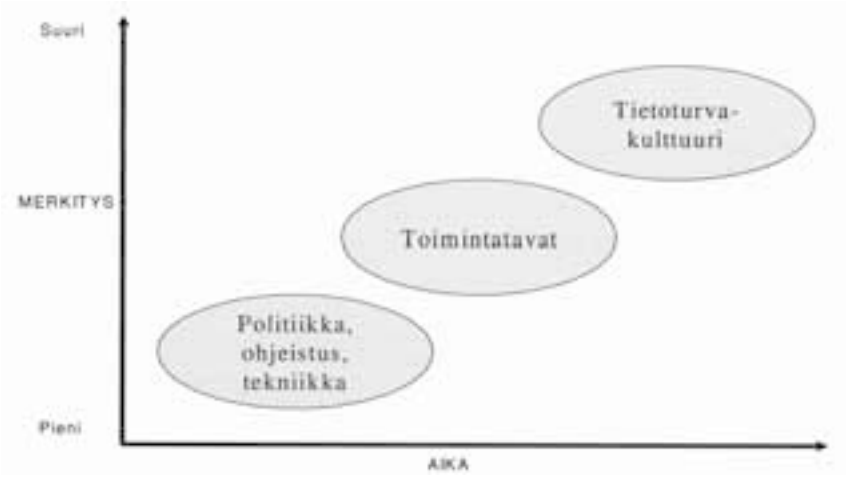
Ulkoistuksessa tietoturvariskejä voidaan pienentää laadukkaalla ja kattavalla vaatimusten hallinnalla ja määrittelyllä. Tähän olisi hyvä luoda pakottava ohjeistus sekä soveltuvat tuki ja valvontamenettelyt valtionhallintotasolla ja virastoissa. Ulkoistettujen osien ohjaus, kehittäminen ja valvonta on pystyttävä jäljitettävästi pitämään ulkoistavan organisaation käsissä. Tarvittaessa tätä on tuettava uusilla säädöksillä.

Valtionhallinnon keskeisten tietojärjestelmien tietoturvallisuuden varmistaminen vaatii todennäköisesti myös huoltovarmuuden uudelleen arviointia. Tähän vaikuttaa mm. uudet teknologiat ja toimintamallit valtionhallinnossa sekä hajautetut palvelinhotellit ja mahdollinen teknisen infrastruktuurin yhdenmukaistaminen valtio-konsernin tasolla.

4 KESKEISTEN TIETOJÄRJESTELMIEN ERITYISHAASTEITA

4.1 Tietoturvakulttuurin rakentaminen

Kuva 2 esittää, kuinka tietoturvakulttuurin kehittäminen on pitkäjänteistä työtä ja muutokset näkyvät hitaammin kuin toimintamallien tai teknisten ratkaisujen aiheuttamat muutokset. Toisaalta tietoturvakulttuurin kehittämisen kautta saadaan pysyvämpiä tuloksia.



Kuva 2: Tietoturvakulttuurin luominen

4.2 Haasteita

4.2.1 Johdon sitoutuminen ja vastuu

Johdon sitoutuminen tietoturvallisuuden kehittämiseen on tyypillinen haaste organisaatioille. Johdon tulee tiedostaa viraston toiminnan tietoturvavaatimukset ja tehdä riittäviä, taloudellisesti järkeviä, riskianalyysiin pohjautuvia panostuksia. Johdon tahtotilan selkeä kommunikointi vaatii jatkuvaa tiedottamista ja henkilökunnan kouluttamista.

4.2.2 Eheys

Tietojärjestelmä toimii luotettavasti vain, jos sen käsittelemät tiedot ovat eheitä. Lähtötietojen oikeellisuuden tarkistaminen vaatii sekä manuaalisia toimenpiteitä että automatisoituja ratkaisuja. Järjestelmän tiedoille tulee olla käsittelysäännöt. Haasteena on arvioida järjestelmän tietojen vaadittava eheystaso ja optimoida sekä lähtötietojen tarkastus että käsittelysäännöt riittäviksi mutta ei liikaa kuormittaviksi.

4.2.3 Käytettävyys

Kriittisen tietojärjestelmän on toimittava keskeytyksettä lähes kaikissa olosuhteissa. Tämä asettaa haasteita valittavien laitteiden, ohjelmistojen, palveluiden ja kumppaneiden luotettavuudelle. Keskeinen tietojärjestelmä on usein laaja järjestelmä, johon on useita sidosryhmäliittymiä. Koko tietojärjestelmän riittävän käytettävyyden takaaminen myös häiriö- ja poikkeustilanteissa vaatii huolellista suunnittelua ja testausta.

Monentaminen on suunniteltava sellaiseksi, ettei yksittäisen komponentin rikkoutuminen vaaranna toimintaa. Rikkoutunut komponentti on kyettävä vaihtamaan järjestelmän ollessa käytössä. Samoin huolto- ja ylläpitotoimenpiteet on kyettävä suorittamaan käyttöä häiritsemättä.

Tietojärjestelmän tilaa on jatkuvasti seurattava ja analysoitava sekä pyrittävä ennakoimaan häiriötilanteet.

4.2.4 Luottamuksellisuus

Keskeisissä tietojärjestelmissä käsitellään usein salassapidettäviä ja turvaluokiteltuja tietoja. Tietojen turvaluokittelu määrää tietoturvatoimet tietojen suojaamiseksi. Tietojen suojaamisen lisäksi ajantasainen käyttäjätietojen hallinta on tärkeää. Käyttö- ja pääsyoikeudet on pystyttävä myöntämään ja poistamaan nopeasti. Sekä tietylle henkilölle myönnetyt oikeudet että tiettyyn tietoon oikeutetut henkilöt on kyettävä raportoimaan nopeasti. Samoin tietojärjestelmän on pidettävä kattavaa lokia tietojen käytöstä ja muutoksista. Käyttäjätietoja ja niiden hallintaa keskittämällä saavutetaan monia etuja, kuten käyttäjäkokemuksen parantuminen, ylläpidon helpottuminen, käyttäjätietojen oikeellisuuden ja ajantasaisuuden varmistaminen ja tietoturvallisuuden parantuminen.

4.2.5 IT-arkkitehtuuri

Toimivan IT-arkkitehtuurin luominen ja eri osa-alueiden yhteensovittaminen vaatii huolellista suunnittelua, dokumentointia ja ohjeistamista. Verkko-, laite-, sovellus- ja tietoturva-arkkitehtuureja ei saa kehittää erillisinä vaan niiden on toimittava saumattomasti yhteen.

Valittu kokonaisarkkitehtuuri määrittää projekteille, toimittajille ja palveluntarjoajille ratkaisujen reunaehdot. Lisähaasteita tuo muiden virastojen ja yhteistyökumppaneiden arkkitehtuurien ja ratkaisujen yhteensovittaminen viraston suunnitteleman arkkitehtuurin kanssa.

4.2.6 Tietojärjestelmäkehitys

Sovellusten tietoturvallisuus on usein vaarallinen heikko lenkki tietojärjestelmässä. Sovelluksen virheellistä logiikkaa tai toteutusvirheitä hyödynnettäessä sovelluksen ulkopuolisista tietoturvajärjestelyistä on usein vain minimaalinen hyöty. Huonosti toteutettu sovellus voi avata oikeudettoman pääsyn suoraan tietojärjestelmän ytimeen.

Sovelluskehittäjiltä ja –kumppaneilta tulee vaatia näyttöä tietoturvaosaamisesta ja tietoturvallisuuden integroinnista sovelluskehitysprosessiin. Tietoturvallisuus tulee huomioida sovelluskehitysprosessin kaikissa vaiheissa.

Tietojärjestelmäkehityksen eri vaiheissa tarvitaan erityyppistä tietoturvaosaamista, esim.:

- riskianalyysi- ja määrittelyvaiheessa tarvitaan hyvää yleisnäkemystä tietoturvakentästä ja tietojärjestelmän käyttötarkoituksesta ja –tavasta
- suunnitteluvaiheessa tarvitaan kokemusta tietoturvaratkaisujen suunnittelusta ja valinnasta
- ohjelmoijien tulee tuntea turvallisen ohjelmoinnin periaatteet, yleisimmät sudenkuopat ja tietysti käyttämiensä työkalujen tietoturvapiirteet
- testausvaiheessa tarvitaan työkaluja ja henkilöitä hakemaan sovelluksen tietoturvaongelmia eli toiminnallisuutta, jota sovellukseen ei oltu tarkoitettu
- asennusvaiheessa turvallisen ympäristön toteuttaminen vaatii monipuolista osaamistasekä tietoturvallisuudesta että asennettavasta järjestelmästä

4.2.7 Dokumentaatio

Koko tietojärjestelmän ja siihen liittyvien toimintojen dokumentointi on oleellista. Tietojärjestelmän koko historia pitää olla taltioituna aina suunnittelukriteereistä, henkilöstön koulutuksesta, käyttöönotosta ja ylläpidosta aina käytöstä poistoon asti. Toimintaprosessit on dokumentoitava yhtenäisten toimintatapojen varmistamiseksi ja auditointien tueksi. Dokumentointia ja arkistointia varten tarvitaan omat standardit, prosessit ja työvälineet.

Dokumentointi on usein tietojärjestelmä- ja tietoturvaprojektien heikko kohta eikä siihen varata riittävästi aikaa. Siksi siihen tulee kiinnittää erityishuomiota ja vaatia hyvää dokumentointia myös yhteistyökumppaneilta.

4.2.8 Ylläpito

Vähemmän kriittisiin tietojärjestelmiin tottuneille kumppaneille ja palveluntarjoajille keskeisten tietojärjestelmien tietoturvahaasteet voivat tulla yllätyksenä. Tavanomaisia toimintaprosesseja ei useinkaan ole mietitty riittäviksi keskeisiä tietojärjestelmiä ajatellen. Tämä voi vaikuttaa laitehuoltoon, sovellusten ylläpitoon, palvelutarjontaan, jne. Keskeisten tietojärjestelmien ylläpito tulee eriyttää muista järjestelmistä ja etähallintaa tulee rajoittaa.

4.2.9 Testaus

Testaus on oleellista käytettävyyden ja tietoturvaratkaisujen varmistamiseksi. Laajan järjestelmän testaus on työlästä ja tietoturvaratkaisujen testaukseen vaaditaan erityisosaamista. Perustestaus tulee tehdä erillisessä, tuotantoympäristöä jäljittelevässä testiympäristössä. Tuotantoympäristön kanssa identtisen testiympäristön järjestäminen on haaste, kun halutaan varmistaa toiminnallisuus kaikkine tietoturvaratkaisuineen ja verkkokomponentteineen. Erillinen testiympäristö on kuitenkin välttämättömyys tuotannon häiriöttömyyden takaamiseksi ja toisaalta testeissä on usein mukana sellaisia kumppaneiden edustajia, joille ei voida antaa pääsyä tuotantojärjestelmään.

Testaaminen vaatii erityistyökaluja ja –osaamista. Tietoturvaongelmien löytäminen vaatii testaajalta erilaista näkökulmaa ja osaamista kuin toiminnallisuutta testaavalta.

4.2.10 Henkilöresurssit

Osaavien henkilöiden riittävyys kaikissa tilanteissa tulee varmistaa. Oma osaamistaso on pidettävä korkealla ja yhteistyökumppaneiden resurssien saatavuus on varmistettava. Häiriö- ja poikkeustilanteessa osaavia henkilöitä on saatava paikalle nopeasti sekä organisoitava näitä tilanteita varten tarvittavat yhteistyöverkostot.

4.2.11 Ulkoistaminen

Toimintoja ulkoistettaessa nousee haasteeksi palveluntarjoajan toimintojen ja henkilöiden linkittäminen kokonaisuuteen ja toimittajien yritysturvallisuusselvitykset. Linkittämistä tulee tukea tarpeellisilla prosessikuvauksilla. Erityisesti resurssien saaminen häiriö- ja poikkeustilanteissa on varmistettava.

Organisaation oma osaaminen tulee pitää riittävällä tasolla, jotta palvelun laatua ja vaatimusten mukaisuutta voidaan luotettavasti seurata ja kehittää. Tässä korostuu virastojen välinen yhteistyö etenkin, jos käytetään saman toimittajan palveluja ja resursseja.

4.2.12 Sidosryhmäyhteistyö

Keskeiseen tietojärjestelmään liittyy tyypillisesti useita yhteistyökumppaneita. Haasteena on varmistaa, että kumppanit ymmärtävät tietojärjestelmän erityisvaatimukset ja varautuvat yhteistyöhön riittävin resurssein.

4.2.13 Poikkeusolot

Poikkeusoloissa toimintaympäristö saattaa muuttua totaalisesti. Resursseja puuttuu, palveluita ei ole saatavilla, huolto ei toimi, yhteydet katkeavat, jne. Mikäli keskeinen tietojärjestelmä on määritelty poikkeusoloissa tarvittavaksi, on erittäin huolellisesti määriteltävä tarvittavat toiminnot sekä suunniteltava ja harjoiteltava poikkeusoloissa toimiminen.

Poikkeusoloihin vaadittavien valmiussuunnitelmien laatiminen on vaativa prosessi. Lisäksi valmiussuunnitelmien koordinointi on oma haasteensa.

Useisiin VAHTI-ohjeisiin sisältyy myös poikkeusoloihin varautumisen näkökulma ja linjauksia.

4.3 Keskeisten järjestelmien luokittelu

Keskeiset tietojärjestelmätkin ovat keskenään hyvinkin erilaisia ja tietoturvavaatimuksissa on eroja. Valtionhallinnon tärkeysluokitusta voidaan pitää yhtenä kriteerinä, mutta sen lisäksi tietoturvavaatimuksiin vaikuttavat erityisesti käsiteltävän tiedon turvaluokitus ja tietojärjestelmän käytettävyysvaatimukset.

Tietojärjestelmät koostuvat usein monista osajärjestelmistä ja sidosryhmäliittymistä. Tietojärjestelmän toimintaprosesseihin osallistuu paitsi viraston omaa henkilökuntaa, myös muiden virastojen henkilökuntaa, tuotetoimittajia, palveluntarjoajia, sekä ulkopuolisia asiantuntijoita ja konsultteja.

Viraston on selvitettävä, kuvattava toimintansa ja siihen liittyvät keskeiset tietojärjestelmät kokonaisuudessaan, mukaan lukien tiedot ja toiminnot. Toiminnan kriittisyyden lisäksi lait, säädökset,määräykset ja ohjeet velvoittavat virastoja varautumaan häiriö- ja poikkeustilanteisiin sekä poikkeusoloihin eri tavoin. Vaativimpien järjestelmien tulee olla käytettävissä mahdollisimman pitkään kaikissa olosuhteissa.

Keskeisten järjestelmien yhtenäinen luokittelu on vaikeaa, joten tässä ohjeessa on käytetty tietoturvavaatimuksiin eheys, käytettävyys ja luottamuksellisuus perustuvaa luokittelua:

1. Eheys, käytettävyys ja luottamuksellisuus tärkeitä
2. Eheys ja käytettävyys tärkeitä
3. Eheys ja luottamuksellisuus tärkeitä

Tietojen eheydestä ei voida tinkiä, mutta käytettävyyden ja luottamuksellisuuden kesken voidaan mahdollisesti tehdä priorisointia. Järjestelmien ominaisuudet saattavat vaihdella ajankohdasta ja ulkoisista tekijöistä riippuen.

Niillä tietoturvallisuuden osa-alueilla, joissa löydettiin selkeitä painotuksia tai mahdollisuuksia tietoturvavaatimusten mukaan, on tässä ohjeessa otettu kantaa luokittelun mukaisesti.

4.3.1 Eheys, käytettävyys ja luottamuksellisuus tärkeitä

Tämän luokan järjestelmät eivät salli kompromisseja ja ovat siten vaativimpia toteutettavia.

Tähän luokkaan kuuluvat esim. johtamisen reaaliaikajärjestelmät sekä useat hallinta- ja valvontajärjestelmät.

4.3.2 Eheys ja käytettävyys tärkeitä

Tämän luokan järjestelmissä painotetaan tietojen käytettävyyttä. Häiriö- ja poikkeustilanteissa halutaan erityisesti varmistaa nopea toipuminen.

Tähän luokkaan kuuluvat esim. sääpalvelut ja julkiset rekisterit.

4.3.3 Eheys ja luottamuksellisuus tärkeitä

Tämän luokan järjestelmissä painotetaan tietojen luottamuksellisuutta. Häiriö- ja poikkeustilanteissa toipumista ei voi nopeuttaa tietojen luottamuksellisuutta vaarantaen.

Tähän luokkaan kuuluvat esim. rahoitusjärjestelmät ja sähköisten varmenteiden tuotantojärjestelmät.

5 HALLINNOLLINEN TURVALLISUUS

Tietoturvallisuuteen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta. (VAHTI 4/2004: Valtionhallinnon tietoturvakäsitteistö)

Lähtötaso	
Vaatimus	Kuvaus
Tietoturvastrategia	Johto on linjannut tietoturvallisuuden tavoitteet.
Tietoturvapolitiikka	Johto on dokumentoinut ja tiedottanut näkemyksensä tietoturvallisuuden merkityksestä, periaatteista ja toteutuksesta.
Toimintaan liittyvät säädökset, määräykset, ohjeet ja muut velvoitteet	Toimintaa ohjaavat säädökset ja velvoitteet on tunnistettu ja niitä noudatetaan.
Tietojärjestelmä- ja tietoturvakuvaukset	Suojattavat tietojärjestelmät on dokumentoitu kokonaisuudessaan mukaan lukien tietoverkot, integraatiot ja sidosryhmäliittymät. Samoin on dokumentoitu käytettävät tietoturvaratkaisut ja liitynnät kokonaistietoturvaan.

Lähtötaso	
Vaatimus	Kuvaus
Toimintaprosessit	Toimintaprosessit ja niiden kytkennät tietojärjestelmiin on dokumentoitu.
Tietojen omistajuus	Tiedoille on nimetty vastuuhenkilö, joka vastaa tietojen eheydestä, käytettävyydestä ja luottamuksellisuudesta.
Riskianalyysi	Tietojärjestelmälle on tehty riskianalyysi, jossa yksilöidään suojattavat kohteet ja niihin kohdistuvat uhat. Riskianalyysissä on huomioitu myös kohteiden väliset suhteet ja toimintaprosessit. Uhkiin varautuminen ja valmiussuunnitelmat perustuvat riskianalyysiin. Riskianalyysi on viraston/laitoksen ydintoiminta-/liiketoimintalähtöistä.
Tietoturvavastuiden ja –tehtävien organisointi ja resursointi	Tietoturvallisuuden kehittämiseen ja toteuttamiseen liittyvät vastuut ja tehtävät on määritelty selkeästi henkilötasolle asti. Tietoturvatyöhön on varattu riittävät resurssit.
Tulosohjaus	Toiminnan tehokkuus ja kustannukset on huomioitu myös tietoturvatyössä. Tietoturvatyön tulosohjaus on kytketty muuhun tulosohjaukseen.
Koulutus- ja viestintäsuunnitelma	Johdon hyväksymien tietoturvatavoitteiden ja -periaatteiden tehokas viestintä organisaatiossa on suunniteltu. Samoin viestintä asiakkaille ja kumppaneille sekä normaali- että häiriötilanteiden varalle. Henkilökunnan jatkuva koulutus ja tietoturvavallisen käyttäytymisen kehittäminen on suunniteltu.
Kehittämis- ja toimintasuunnitelma ja budjetointi	Organisaatiolla on tietoturvastrategiaan ja -politiikkaan pohjautuva tietoturvallisuuden kehittämis- ja toimintasuunnitelma, jonka perusteella tietoturvatyö budjetoidaan. Tietoturvan tulee olla keskeisenä osana toimintastrategiaa.
Dokumentointi	Järjestelmät, prosessit, tietoturvaratkaisut ja niiden perustelut, toimintaperiaatteet, suunnitelmat ja käytännöt on dokumentoitu.

Lähtötaso	
Vaatimus	Kuvaus
Mittarit	Tietoturvatyön oikeellisuuden ja tehokkuuden varmistamiseksi organisaatiossa on valittu sopivat mittarit ja päätetty niiden soveltamisesta.
Poikkeamien ja rikkomusten hallinta	Poikkeamien, ongelmien ja rikkomusten hallintaan on luotu prosessi, jotta ne voidaan havaita, korjata ja raportoida ja jotta tapahtumista voidaan oppia. Hallintamenetelmien tulee olla lainsäädännön asettamien vaatimusten mukaisia, ja niiden tuottamia tietoja tulee käsitellä huolellisesti mm. siksi, että tiedot pätisivät oikeudessa.
Tietoturvakulttuurin kehittäminen	Henkilöstö motivoidaan huomioimaan tietoturvanäkökohdat ja huomaamaan ja raportoimaan poikkeamat automaattisesti osana jokapäiväisiä työtehtäviä.
Kustannukset	Kontrollien kokonaiskustannukset ovat verrannolliset suojattavien kohteiden tai toiminnan arvoon. Kontrolleja valittaessa on huomioitu myös mahdolliset aineettomat vahingot.

Perusohjeistus
Valtioneuvoston periaatepäätös valtion tietoturvallisuudesta 11.11.1999
Kansallinen tietoturvastrategia 25.11.2002
Hallituksen strategia-asiakirja 2003: Tietoyhteiskuntaohjelma
VM Hallinnon Kehittämisosaston työryhmämuistio 9/2003: Tulosohjauksen terävöittäminen
VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi
VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 6/2001: Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista
VAHTI 1/2001: Valtion viranomaisen tietoturvallisuustyön yleisohje

VAHTI 2/2004: Tietoturvallisuus ja tulosohjaus
PTS Tietojärjestelmäjaoston ohje 1/2002: Tietotekniikan turvallisuus ja toiminnan varmistaminen
Valtiokonttorin määräys 20/03/2001: Taloussääntöjen uudistaminen

Standardit
BS7799
ISF
ITIL

5.1 Tietoturvallisuuden johtaminen

Tietoturvatyön onnistumisen perusta on johdon sitoutuminen tietoturvallisuuden kehittämiseen ja turvallisuuden perusvaatimusten ymmärtäminen ja toteuttaminen johdon taholta. Johdolla tulee olla tieto järjestelmäkokonaisuuksista niihin liittyvine prosessikuvauksineen ja riskeineen. Viraston ydintoimintalähtöiseen riskianalyysiin perustuen johdon tulee suunnitella, valtuuttaa ja resursoida organisaation tietoturvatyö. Turvallisuus- ja tietoturvajohto raportoivat suoraan organisaation ylimmälle johdolle. Turvallisuus- ja tietoturvajohdon tukena tulee olla tietoturvaryhmä, jonka jäsenet edustavat laajasti organisaation eri osia ja näkökantoja. Tietoturvaryhmä voi antaa tietoturvajohdolle laajan näkemyksen organisaation tarpeista, haasteista ja prioriteeteista. Toisaalta tietoturvaryhmä voi välittää eteenpäin tietoturvajohdon näkemyksiä ja päätösten perusteluita.

Kokonaisturvallisuuden takaamiseksi turvallisuus- ja tietoturvatyö tulee synkronoida ja integroida toisiinsa. Tietoturvallisuutta tulee hallita kokonaisuutena varmistaen, että tavoitteet ja tehtävät ymmärretään samoin koko organisaatiossa ja että vuorovaikutus toimii organisaatioyksiköiden välillä yhteisten tietoturvatavoitteiden toteutumiseksi. Tietoturvatyön tulee olla avointa, koko organisaatiota matriisimaisesti lähestyen. Avoimuus varmistaa myös sen, että tarpeet ja mahdollisuudet tulevat huomioitua riittävän laajasti eikä organisaatioon jää tietoturvallisuudenn kannalta heikkouksia.

Tietoturvatrategia- ja -politiikkadokumenteilla johto esittää tahtotilansa ja näkemyksensä tietoturvallisuuden tärkeydestä organisaatiossa sekä asettaa tavoitetilan tietoturvatyötä tekeville. Nämä ylimmän tason dokumentit ohjaavat koko henkilökuntaa päivittäisessä toiminnassa. Johdon asettamat tavoitteet on tehokkaasti tiedotettava henkilökunnalle ja niiden toteutumista on ohjattava ja seurattava sekä varmistettava resurssien riittävyys. Johdon oma esimerkki on luonnollisesti tärkeä henkilökunnan kannustamisessa tietoturvalliseen käyttäytymiseen ja perustan luomiseksi organisaation turvallisuuskulttuurille.

Tietoturvallisuuden johtaminen vaatii perustellun päätöksen tavoitellusta, täsmällisesti määritellystä tietoturvatasosta. Virastolla tulee olla dokumentoitu, koko toiminnan kattava tietoturva-arkkitehtuuri, joka ohjaa paitsi tietoturva- myös tietojärjestelmäratkaisuja.

Tietoturvatason toteutumista on pystyttävä mittaamaan ja analysoimaan säännöllisesti. Ratkaisuja valittaessa on huomioitava mitattavuus ja mittarit on valittava siten, että saatavien tietojen perusteella voidaan tehdä johtopäätöksiä tietoturvallisuudenn tasosta ja tarvittaessa ryhtyä tietoturvallisuutta parantaviin toimenpiteisiin. Mittareiden on ohjattava tietoturvallisuuden kehittämiseen kokonaisuuden kannalta – ei pistemäisiin ratkaisuihin. Tarvittaessa tehdyt konkreettiset ratkaisut on pystyttävä jäljittämään niihin johtaneisiin päätöksiin ja perusteluihin. Tietoturvallisuuttakin täytyy kehittää iteratiivisesti käytössä olevien resurssien ja ympäristön muutosten ohjaamana – mittarit ovat siis oleellisia myös pidemmän aikavälin kehityksen seurantaan.

Tietoturvallisuuden tulee sisältyä myös organisaation laatukriteereihin. Laadukas toiminta edellyttää tietoturvallisuutta ja toisaalta tietoturvallisuuden edistäminen parantaa toiminnan laatua.

Valtionhallinnon tietoturvallisuutta tulee tarkastella kokonaisuutena. Tämä tarkoittaa ensi vaiheessa sitä, että virastojen kannattaa kehittää yhteistoimintaansa hakemalla yhteisiä ratkaisuja, jakamalla tietoa ja kokemuksia, vertailemalla tehtyjä ratkaisuja ja yleensäkin aktiivisesti hakemalla synergioita virastojen tietoturvallisuuden kehittämiseen. Parhaimmillaan virastojen välinen yhteistyö on automaattista, toimintaan sisäänrakennettua

Tietojärjestelmiä suunniteltaessa ja rakennettaessa helposti keskitytään teknisiin järjestelyihin ja tuotekohtaisiin ratkaisuihin unohtaen ihmisen ja tekniikan kohtaaminen. Tietoturvaratkaisut on suunniteltava käyttäjiä varten ja käyttäjien on saatava riittävä koulutus ymmärtääkseen, mitä ratkaisuja on tehty ja miksi ne on valittu.

Henkilökunnan tulee olla tietoturvallisuuden vahvin lenkki – siksi tiedotus ja koulutus ovat oleellisia tehtäviä. Henkilökunnan tulee ymmärtää annetut tietoturvatavoitteet ja tietoturvallisuuden olevan oleellinen osa päivittäistä työskentelyä. Motivoitunut ja tietoturvatietoinen henkilökunta pystyy parhaiten jatkuvaan riskien analysointiin ja parannusehdotusten tekemiseen omien tehtäviensä osalta. Viestinnän ja koulutuksen tehokkuutta on jatkuvasti seurattava henkilökunnan osaamistason ja tietoturvatietoisuuden varmistamiseksi.

Henkilökunnalle tulee avoimesti kertoa tietoturvallisuuden mittaamisesta ja seuraamisesta sekä rikkomusten seuraamuksista. Havaittuihin rikkomuksiin on syytä reagoida välittömästi ja tarvittaessa parantaa ohjeistusta tai koulutusta.

5.2 Suhteet sidosryhmiin ja asiakkaisiin

Keskeiset tietojärjestelmät eivät ole itsenäisiä saarekkeita, vaan niihin sisältyy erilaisia asiakas- ja sidosryhmärajapintoja. Toiminnan turvallisuutta ja jatkuvuutta suunniteltaessa on huomioitava myös nämä liittymät. Oman haasteensa tietojärjestelmän turvaamiseen tuovat palveluntarjoajat, alihankkijat ja tuotetoimittajat. Toiminnan riskikartoitus täytyy ulottaa yhteistyökumppaneihin.

Kaikkien tietojärjestelmän toimivuuteen vaikuttavien osapuolien kanssa on luotava toimivat suhteet ja käytännöt huomioiden myös toiminta häiriö- ja poikkeustilanteissa ja poikkeusoloissa. Suhteiden hallinta on syytä suunnitella ja yhteistyön toimivuutta tulee seurata säännöllisesti. Seurantamekanismeja ovat mm. jatkuva raportointi, seurantapalaverit ja ulkopuolinen auditointi. Yhteistyökumppaneiden toimintaraportit on kyettävä huomioimaan viraston tietoturvallisuuden kokonaissuunnittelussa. Yhteistyötä ja häiriö- ja poikkeustilanteiden hallintaa on harjoiteltava säännöllisesti sekä organisaatio- että henkilötasolla. Yhteistyön sujuvuutta helpottavat säännölliset, yhteistyön kehittämiseen tähtäävät organisaatioiden väliset vierailut.

Yhteistyökumppaneiden tietoturvaosaamisen taso tulee varmistaa esim. heidän toimintaansa ja tietoturvaohjeistukseensa ja käytäntöihinsä tutustumalla. Laatu- ja tietoturvasertifikaatit antavat viitteen siitä, että organisaatiossa on panostettu tietoturvallisuuteen. Tietoturvaosaamisen lisäksi myös muut potentiaalisten yhteistyökumppaneiden taustat tulee selvittää, kuten taloudellinen tilanne, yhteiskunnallisten velvollisuuksine hoitaminen, jne. Virastojen välinen vertaiskehittäminen kannattaa huomioida myös yhteistyökumppaneiden valinnassa. Avoin kommunikointi, kokemusten ja parhaiden käytäntöjen jakaminen ja toiminnan vertailu virastojen välillä edistää koko valtionhallinnon tietoturvallisuutta.

Viraston kannattaa myös minimoida viraston ulkopuolisten liittymien kriittisyys. Poikkeustilanteessa on hyvä selvitä mahdollisimman pitkään omin resurssein. Viraston tulee varoa liiallista riippuvuutta tietystä yksittäisestä palveluntarjoajasta tai toimittajasta.

Yhteistyökumppaneita valittaessa tulee varmistaa, että kaikilla osapuolilla on riittävä tieto viraston tietoturvavaatimuksista ja -tarpeista. Sopimuksissa on selkeästi huomioitava tietoturvavaatimukset mittareineen. Tietoturvavaatimusten toteutumatta jääminen on oltava selkeästi sanktioitu. Sopimuksissa on syytä huomioida myös optiot tietoturvatason nostoon tarpeen vaatiessa.

Tiedottamiskäytännöt on suunniteltava etukäteen myös häiriö- ja poikkeustilanteiden sekä poikkeusolojen varalle. Yhteistyökumppaneille tarvitaan tietoa jo ennen julkista tiedottamista. Asiakkaille tulee tiedottaa toiminnan häiriöistä, niiden syistä ja mahdollisista poikkeuksellisista toimintatavoista. Myös kansalaiset, henkilökunta, viranomaiset ja muut virastot tarvitsevat tietoa tilanteesta. Tietosisältöä ja julkaisuajankohtaa on porrastettava tilanteen ja kohteen mukaan. Oikean tiedon perille menemisen varmistamiseksi rutiinit, hyväksymismenettelyt ja yhteyshenkilöt on oltava suunniteltuina ja tiedossa.

5.3 Hankinnat

Tietojärjestelmiä, tuotteita ja palveluja hankittaessa on ostajan huolehdittava tietoturvavaatimustensa määrittelystä, varmistettava, että toimittaja ymmärtää vaatimukset ja että toimitus on vaatimusten mukainen. Ostajan on tiedettävä tarpeensa ja vaadittava niihin vastaamista. Ostajan on huolehdittava siitä, ettei joudu tekemään päätöksiä pakon edessä, esim. aikataulu- tai resurssisyistä.

Toimittajalle on korostettava keskeisten järjestelmien tärkeyttä ja korkeita tietoturvavaatimuksia. Tietoturvaominaisuudet tai -taso on määriteltävä selkeästi niin, ettei tulkinnanvaraa jää. Tämä ohje määrittää vähimmäistason. Ostaja voi määritellä ongelman ja halutut tietoturvapiirteet yksityiskohtaisesti, jolloin toimittajan tehtäväksi jää vastata tarpeeseen parhaan kykynsä mukaan. Toinen vaihtoehto on, että ostaja suunnittelee ja määrittelee ratkaisun itsenäisesti tai konsultointiapua käyttäen, jolloin toimittaja tarjoaa esitetyn ratkaisumallin mukaisesti. Tarjouspyynnöissä ja sopimuksissa on huomioitava salassapitovaatimukset.

Hankinnoissa on syytä selvittää muiden virastojen mahdollisia kokemuksia vastaavista hankinnoista ja mahdollisuutta yhteishankintaan. Hankinnoissa on varmistettava yhteensopivuus viraston tietoturva- ja muihin arkkitehtuureihin sekä tietoturvastrategiaan ja -suunnitelmiin. Yhteensopivuusvaatimus ei rajoitu pelkästään viraston omiin toimintoihin ja järjestelmiin, vaan yhteensopivuus on varmistettava myös kumppaneiden ja asiakkaiden järjestelmiin. Hankintaa tehtäessä on jo varauduttava mahdolliseen tietoturvatason tai kapasiteetin nostoon tulevaisuudessa.

Organisaatiossa on oltava vastuuhenkilö tai -ryhmä, jolla on kokonaiskäsitys kaikista tehdyistä ja meneillään olevista hankinnoista. Näin saadaan myös paras tietämys yleisestä hintatasosta ja varmistetaan paras hinta/laatu-suhde. Virastossa tulee ylläpitää rekisteriä käytettävistä ja arvioiduista tuotteista ja palvelutoimittajista tai virastojen tulee yhteistyössä luoda yhteinen toimittajarekisteri.

Liiallista riippuvuutta toimittajista tulee välttää. Tämä pätee erityisesti palveluiden hankinnan osalta. Palveluita hankittaessa on selvitettävä palveluntarjoajan omat alihankkijat ja varmistettava koko palveluketjun sitoutuminen viraston palvelu- ja tietoturvatasoon.

5.3.1 Laitehankinnat ja huolto

Laitteiden osalta on varmistettava erityisesti korvaavien laitteiden ja varaosien saatavuus sekä huolto. Laitetoimittajalla on oltava riittävä laite- ja varaosavarasto sekä osaavaa huoltohenkilökuntaa Suomessa. Häiriö- ja poikkeustilanteita varten virastolla on oltava omia varalaitteita ja varaosia kriittisimpien komponenttien osalta, jotka on hyvä hankkia jo varsinaisen laitetilauksen yhteydessä. Virastolla on hyvä olla saatavilla laitetoimittajasta riippumatonta, teknistä henkilökuntaa kriisitilanteiden varalle.

5.3.2 Käyttö-, hallinta- ja tietojenkäsittelypalvelut

Palveluita hankittaessa palvelutasojen täytyy olla selkeästi määriteltyinä mittareineen ja sanktioineen. On varmistettava, ettei tietoturvakriittistä palvelua ajeta samassa ympäristössä vähemmän kriittisten tai peräti muiden asiakkaiden palveluiden kanssa, ellei näidenkin tietoturvatasoa ole nostettu vastaavalle tasolle. Palveluntarjoajan on kyettävä esittämään palvelun tietoturvaratkaisut ja vastaamaan viraston esittämiin vaatimuksiin. Viraston ei tule tyytyä palvelutarjoajan ”pakettiratkaisuun”, jos se ei ole riittävän turvallinen. Vaativien järjestelmien osalta palvelutarjoaja voi joutua tekemään erityisjärjestelyitä taatakseen riittävän palvelutason ja turvallisuuden.

Palveluntarjoajan tarvittavaa henkilökuntaa täytyy olla riittävästi saatavilla lyhyellä varoitusajalla. Viraston on huolehdittava riittävän oman osaamisen säilymisestä siltä varalta, että palvelutarjoajaa halutaan myöhemmin vaihtaa tai ottaa toiminta takaisin omaan haltuun.

Virastoilla on oltava prosessi hankittujen palveluiden hallintaan ja palvelutarjoajan vaihtoon. Viraston on vaadittava riittävää palvelutasoa ja valvottava palvelun laatua. Palveluntarjoajien hallinnassa auttaa ostettavien palveluiden pilkkominen selkeisiin kokonaisuuksiin ja selkeä vastuunjako. Palveluntarjoajia on syytä kilpailuttaa riittävän usein.

5.3.3 Valmisohjelmistohankinnat

Valmisohjelmiston on täytettävä viraston toiminnalliset vaatimukset. Valinnan kriteereinä täytyy lisäksi huomioida yhteensopivuus ja tietoturvallisuus.

Valmisohjelmistot ovat usein ongelmallisia yhteensopivuuden kannalta. Viraston määrittelemät arkkitehtuurit tai käytössä olevat palvelut voivat asettaa selkeitä yhteensopivuusvaatimuksia. Valmisohjelmistoja hankittaessa on määriteltävä, mihin palveluihin ja millä rajapinnoilla ohjelmistojen on liityttävä keskeisessä tietojärjestelmässä. Ohjelmistotuotteen integroituminen olemassa olevaan palveluun on testattava ennen sen hankkimista.

Valmisohjelmistoja hankittaessa on kiinnitettävä erityistä huomiota tietoturvaominaisuuksiin, tietoturvasertifiointeihin, käytettyihin standardeihin, tiedon esitys- ja talletusmuotoihin sekä merkistöihin. Viraston tulee ohjelmistohankinnoissaan välttää sitoutumista yhden toimittajan ratkaisuihin ja pyrkiä aina standardiratkaisuihin, avoimien rajapintojen käyttöön ja mahdollisimman hyvään yhteen toimivuuteen muiden ratkaisujen kanssa. Erityisratkaisut ja suljettujen ratkaisujen käyttö on aina erikseen perusteltava. Jo ohjelmistoa hankittaessa on huomioitava mahdollisuus sen vaihtamisesta toiseen tuotteeseen tulevaisuudessa.

Valmisohjelmistojen osalta on varmistettava riittävä kotimainen tuki ja yhteydet valmistajan parhaimpiin asiantuntijoihin ja tuotekehitykseen. Ohjelmistoa hankittaessa kannattaa selvittää toimittajan halukkuus ottaa vastaan parannusehdotuksia ja reagoida niihin. Ohjelmistotoimittajalta tulee vaatia tuotteen lähitulevaisuuden kehityssuunnitelma.

Viraston tulee seurata lisenssien käyttöä ja varmistaa niiden riittävyys, samoin tulee seurata käytössä olevia ohjelmistoversioita. Lisensoimattomia versioita ei tule sallia ja ohjelmistoversioissa on pyrittävä yhdenmukaisuuteen. Ohjelmistoasennusten seuranta tulee automatisoida mahdollisuuksien mukaan.

5.3.4 Sovelluskehitys

Räätälöityjen sovellusten hankinta vaatii viraston sitoutumista ohjelmistoprojektiin. Oman henkilökunnan resursseja vaaditaan koko projektin ajan. Määrittelyvaihe, työmääräarviot, resurssit ja aikataulu ovat oleellisia projektin onnistumisen kannalta. Toimittajan tekemät arviot on syytä tarkistaa ja varmistaa, että toimittajalla on resursseja vastata yllättäviin lisätarpeisiin ja aikatauluvaatimuksiin. Sovellusprojektia on seurattava huolellisesti ja vaadittava säännöllistä raportointia.

Sovellustoimittajan on kyettävä sopeutumaan viraston valitsemiin arkkitehtuureihin, standardeihin ja palveluihin sekä esittämään vaaditut tietoturvaratkaisut yksityiskohtaisesti.

5.3.5 Konsultointi- ja asiantuntijapalvelut:

Konsultti- ja asiantuntijapalveluita hankittaessa on henkilöiden luotettavuus ja ammattitaito tarkistettava. Virastossa on asetettava kullekin konsultointi- ja asiantuntijatyölle vastaava henkilö, joka seuraa työn etenemistä ja tuloksia. Kaikesta tehdystä työstä on jäätävä virastolle dokumentti, joka helpottaa vastaavan työn hankkimista tai tekemistä jatkossa.

5.4 Dokumentointi

Hyvä ja kattava dokumentaatio on edellytys turvallisuuden hallinnalle. Dokumentaatiolla varmistetaan yhteinen käsitys tietojärjestelmän toiminnasta ja vaatimuksista ja vähennetään henkilöriippuvuutta. Dokumentointi on keskeinen osa tietoturvakulttuurin kehittämistä. Dokumentaatio toimii myös tärkeänä historiatietona uusia järjestelmiä suunniteltaessa ja häiriöihin johtaneita syitä jäljitettäessä.

Kaikki oleellinen tietojärjestelmän toimintaan ja käyttöön liittyvä tulee dokumentoida:

- Määritelmät ja suunnitelmat
- Riskianalyysit
- Tietoturvaratkaisut perusteluineen
- Arkkitehtuuri
- Tietoverkko
- Rajapinnat ja liittymät muihin järjestelmiin
- Sidosryhmäliittymät

- Projektidokumentaatio
- Testaussuunnitelmat ja -tulokset
- Asennussuunnitelmat ja -dokumentaatiot
- Käyttöprosessit
- Auditointisuunnitelmat ja -tulokset
- Poikkeus- ja varautumissuunnitelmat
- Virhe- ja häiriötilanteet korjaustoimenpiteineen
- Järjestelmän muutoshistoria
- jne.

Keskeisen tietojärjestelmän tietoturvaratkaisut ovat aina vähintään luottamuksellisia (turvaluokiteltu III), valmiussuunnitelmat ovat aina salaisia (turvaluokiteltu II); muu dokumentaatio luokitellaan julkisuuslain määräysten mukaisesti. Järjestelmän dokumentaatio tulee ylläpitää keskitetysti ja arkistoida versiohistoriatietoineen. Asiakirjojen kaikkien elinkaaren vaiheiden käsittely, mukaanlukien jakelu ja hävittäminen, pitää tapahtua turvaluokituksen mukaisesti.

Valtiokonttori on antanut erikseen määräyksiä taloushallinnon tietojärjestelmien dokumentoinnista. Määräykset saattavat käytännössä myös vaikuttaa muiden järjestelmien dokumentointivaatimuksiin.

5.5 Muutoksen hallinta

Toimintaympäristö, sidosryhmät, tietoturvariskit ja –vaatimukset muuttuvat jatkuvasti. Nopeaankin tahtiin tapahtuvat muutokset eri osa-alueilla ovat nykymaailmassa itsestäänselvyys, joten niihin varautuminen on tehtävä rutiininomaisesti. Viraston on jatkuvasti evaluoitava tilannetta, päivitettävä riskianalyysejä ja toteutettava tarvittaessa uusia suojausmenetelmiä.

Hyvä apuväline evaluoinnissa on skenaarioajattelu – mietitään jo etukäteen vaihtoehtoisia tulevaisuus- ja uhkamalleja ja niistä selviytymistä. On syytä miettiä myös pahimpia mahdollisia tilanteita, esim. palvelutarjoajan poistuminen markkinoilta, toimitilojen tuhoutuminen, avainhenkilöstön eliminoituminen tai ongelmat suurimman osan toiminnoista ollessa ulkoistettu. Virastojen yhteistyöllä tai resurssien yhteiskäytöllä voidaan varautua joihinkin muutoksiin ja uhkiin.

Tietojärjestelmää ja sen käyttöä suunniteltaessa ja toteutettaessa on varauduttava muutoksiin. Tarpeen vaatiessa on siirryttävä vaihtoehtoiseen toimintaan tai varajärjestelmien käyttöön.

Uudet teknologiat tuovat paitsi uusia toimintamahdollisuuksia, myös uusia tietoturvariskejä. Uusia teknologioita on jatkuvasti evaluoitava myös tietoturvan kannalta ja käyttöönotossa huomioitava vaikutukset koko järjestelmän turvallisuuteen.

5.6 Varautuminen poikkeusoloihin

Poikkeusolot ovat usein kaoottisia ja todellinen tilanne vaikeasti hahmotettavissa. Palvelujen, resurssien ja laitteiden saatavuus on todennäköisesti heikkoa. Poikkeusoloissa tarvitaan nopeaa päätöksentekoa ja kriisijohtamista. Normaalit komentoketjut eivät todennäköisesti päde, vaan johtamisessa siirrytään poikkeukselliseen päätöksentekomalliin ja kriisiorganisaatioon.

Viraston on varauduttava ennustettaviin ja ennustamattomiin häiriö- ja poikkeusoloihin parhaalla mahdollisella tavalla. Erityisesti edellytetään dokumentoituja ja testattuja valmiussuunnitelmia poikkeusoloissa toimimiseksi. Suunnitelmissa on syytä huomioida vaihtoehtoisia toimintatapoja – on todennäköistä, että poikkeusoloissa tulee yllätyksiä järjestelmien toimivuuden ja erityisesti henkilöiden käyttäytymisen suhteen. Henkilön toimintaa kovan paineen alla on vaikeaa ennustaa edes harjoitusten perusteella.

5.7 Järjestelmäluokkien erityispiirteet

5.7.1 Eheys, käytettävyys ja luottamuksellisuus tärkeitä

Tietojärjestelmän toipuminen häiriö- tai poikkeustilanteesta ei salli kompromisseja. Toipumissuunnitelman on oltava erityisen tarkka ja säännöllisesti harjoiteltu, koska toipumisen nopeuden lisäksi täytyy huolehtia tietoaineistoturvallisuudesta.

Häiriöihin ja poikkeuksiin on varauduttava resursseja moninkertaistamalla, huomioiden laitteet, verkkoyhteydet, sovellukset ja henkilöt. Järjestelmä voidaan hajauttaa maantieteellisesti siten, että yhden pisteen häiriöt eivät lamauta koko järjestelmää missään tilanteessa. Hajautettu järjestelmä vaatii erityistä huolellisuutta suunnitelmien ja yhteistyön organisoinnissa ja selkeää vastuunantoa kriisitilanteissa. Henkilöresursseja voidaan varmistaa ylläpitämällä osaamispooleja ja kouluttamalla ihmisiä useampiin tehtäviin siten, että osaamisalueet menevät tarvittavin osin päällekkäin.

5.7.2 Eheys ja käytettävyys tärkeitä

Tietojärjestelmäsuunnittelussa ja –toteutuksessa on painotettava häiriötilanteista toipumisen nopeutta. Häiriöihin ja poikkeuksiin on varauduttava resursseja moninkertaistamalla, huomioiden toiminta, laitteet, verkkoyhteydet, sovellukset ja henkilöt.

Järjestelmän nopea, tärkeimpien toimintojen osittainenkin toipuminen on tärkeämpää kuin järjestelmän toimiminen kokonaisuudessaan.

5.7.3 Eheys ja luottamuksellisuus tärkeitä

Häiriö- ja poikkeustilanteissa on oleellista tehdä toipuminen selkeiden ohjeiden mukaan, ennalta valittujen henkilöiden toimesta. Tietoaineistoturvallisuutta korostetaan toipumisen nopeuden kustannuksella.

6 HENKILÖSTÖTURVALLISUUS

Henkilöstöön liittyvien tietoriskien hallinta henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta. (VAHTI 4/2004: Valtionhallinnon tietoturvakäsitteistö)

Lähtötaso	
Vaatimus	Kuvaus
Henkilöllisyyden tarkastus	Uuden työntekijän henkilöllisyys tarkastetaan passista, ajokortista tai poliisiviranomaisen myöntämästä henkilöllisyystodistuksesta.
Taustatarkastus	Suositusten, koulutuksen ja työhistorian tarkastus sekä turvallisuusselvityksen teettäminen tarvittaessa.
Sopivuuden varmistus	Peruskoulutuksen ja osaamisen minimitaso sekä muu soveltuvuus tehtävään varmistetaan.
Perehdytys	Uusi työntekijä osallistuu suunniteltuun perehdytyskoulutukseen.
Salassapitositoumus	Työntekijä allekirjoittaa joko salassapitositoumuksen tai dokumentin, joka osoittaa työntekijän tuntevan lainsäädännön ja muut keskeiset velvoitteet salassapidon suhteen.

Lähtötaso	
Vaatimus	Kuvaus
Dokumentoitu tuloprosessi	Työhönotto tapahtuu etukäteen dokumentoidun prosessin mukaisesti, joka kattaa kaikki vaiheet rekrytoinnin aloittamisesta siihen, että uusi työntekijä tai viranhaltija voi aloittaa työnteon. Perehdyttämisprosessi on dokumentoitu ja on huomioitu myös jatkuva työnohjaus.
Dokumentoitu lähtöprosessi	Työsuhteen päättyminen tapahtuu etukäteen dokumentoidun prosessin mukaisesti, joka kattaa kaikki vaiheet irtisanomisesta, irtisanoutumisesta, työsuhteen purkamisesta tai virkasuhteen purkamisesta siihen, että työntekijä ei enää ole työsuhteessa tai virkamies virkasuhteessa.
Kirjallinen toimenkuva	Työtehtävistä on laadittu kuvaus, joka sisältää tehtävät, vastuut, oikeudet ja velvollisuudet.
Tehtävien eriyttäminen	Tehtävät ja vastuualueet eriytetään siten, että tiedon ja palveluiden tahattoman tai tahallisen väärinkäytön riskiä pienennetään.
Avainhenkilöiden kartoitus ja varahenkilöjärjestelyt	Toiminnan kannalta välttämättömät henkilöt ovat dokumentoidusti tiedossa ja tarvittaessa käytettävissä.
Riittävä miehitys	Tehtävien suorittamista varten on käytettävissä riittävät henkilöresurssit.
VAP-varaukset	Poikkeusolojen henkilöresurssit on turvattu.
Työsuojelu	Työsuojelulla pidetään yllä ja edistetään työntekijöiden terveyttä, turvallisuutta ja työkykyä sekä ehkäistään tapaturmia ja ammattitauteja.
Resurssipankki	Työntekijöiden osaaminen on kartoitettu, dokumentoitu ja kartoituksen tulokset ovat käytettävissä.

Lähtötaso	
Vaatimus	Kuvaus
Sertifikaatit	Henkilöiden ammattisertifikaatteja suositaan.
Ulkoisen työvoiman hallinta	Ulkoisen työvoiman tulee olla oman henkilöstön ohjauksessa ja oman henkilöstön osaamistaso tulee pystyä säilyttämään ydintehtävissä.

Perusohjeistus
VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi
VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 1/2001: Valtion viranomaisen tietoturvallisuustyön yleisohje
Laki yksityisyyden suojasta työelämässä (759/2004)

Standardit
BS7799

6.1 Henkilöstön toimenkuvat

Jokaisella valtionhallinnon keskeisten tietojärjestelmien toimintoihin osallistuvalla henkilöllä tulee olla määriteltynä kirjallinen toimenkuva. Työntekijän tulee tuntea toimenkuvansa; tämä varmistetaan siten, että työntekijä vahvistaa allekirjoituksellaan sekä vastaanottaneensa että lukeneensa toimenkuvansa.

Toimenkuvassa määritellään henkilön tehtävät, oikeudet, velvollisuudet ja vastuut. Sen on oltava selkeä ja ennen kaikkea kattava sisältäen mm. tietoturvavastuut, ja -tehtävät. Toimenkuvissa tulee noudattaa työn eriyttämistä siten, että vaarallisia työyhdistelmiä ei pääse syntymään.

Toimenkuvat tulee säännöllisesti sekä tarkastaa, jotta toimenkuva täyttää muodolliset vaatimukset, että tarkistaa, jotta toimenkuva kattaa kaiken tarpeellisen eikä siinä ole yli-

määräisiä tehtäviä. Tarkistettu toimenkuva tulee saattaa todistetusti työntekijän tietoon.

Henkilön toimenkuvan perusteella tehdään riskianalyysi, jonka pohjalta mitoitetaan turvallisuutta lisäävät toimenpiteet. Vain kriittisimmät toimenkuvat edellyttävät esimerkiksi luottotietojen tarkastusta tai jatkuvaa terveydentilan seurantaa sekä näille asetettavia reunaehtoja. Tarvittavia toimenpiteitä arvioitaessa on kuitenkin otettava huomioon mm. laki yksityisyyden suojasta työelämässä (759/2004), henkilötietolaki (523/1999), työterveyshuoltolaki (1383/2001), laki yhteistoiminnasta valtion virastoissa ja laitoksissa (651/1988) sekä muu valtion virkamiehiä koskeva lainsäädäntö.

6.2 Henkilöstön soveltuvuus

Henkilöstöturvallisuuden yhtenä kulmakivenä on toimenkuviinsa soveltuva henkilöstö. Keskeisten tietojärjestelmien toiminnoista vastaaville henkilöille tulee olla määriteltynä tarkat toimenkuvat, ja rekrytointimenettelyjen tulee olla sellaiset, että tehtäviä saadaan hoitamaan toimenkuvaan soveltuvat henkilöt.

Rekrytointiprosessiin tulee pääsääntöisesti kuulua prosessin loppupuolella muutamalle parhaimmalle kandidaatille heidän suostumuksellaan tehtävä soveltuvuustestaus. Soveltuvuustesti kartoittaa hakijan sopivuutta haettuun tehtävään mittaamalle puolueettomasti esim. älykkyyttä, paineensietokykyä, persoonallisuutta ja oppimiskykyä. Soveltuvuustestin sisältö vaihtelee toimenkuvittain. Soveltuvuustesteissä on käytettävä luotettavia, ammattitaitoisia ja sertifioituja yrityksiä ja henkilöitä. Testatulle on annettava tämän pyynnöstä soveltuvuusarvioinnissa annettu lausunto maksutta.

Rekrytointiprosessin loppupuolelle voi kuuluu myös hakijan mahdollisten suosittelijoiden kuuleminen ja näiden aitouden varmistaminen.

Valitun työntekijän tausta tarkastetaan työtehtävien edellyttämässä laajuudessa. Henkilön työhistoria varmistetaan vähintään pistokokein. Koulutus- ja tutkintotodistusten alkuperäiskappaleille tehdään visuaalinen tarkastus ja tarvittaessa aitous varmistetaan todistuksen antaneelta instanssilta. Mikäli toimenkuva vaatii, valitusta työntekijästä teetetään turvallisuusselvitys.

Työntekijän luottotietojen tulee olla kunnossa, jos tehtäviin liittyy joko rahan tai vähintään salaiseksi luokiteltujen tietojen käsittely. Luottotiedot tulee tarkastaa rekrytointivaiheessa ja niitä on seurattava säännöllisesti. Mikäli luottotiedot eivät ole kunnossa kasvavat riskit sekä lahjottavuuden että epätoivoisten tekojen osalta.

Työntekijälle tulee tehdä terveystarkastus työhöntulovaiheessa. Jatkossa terveystarkastus tehdään tarvittaessa jopa vuosittain. Terveystarkastuksiin tulee sisältyä, lainsäädännön puitteissa, tarvittavat testit sekä itsearvioinnit työntekijän työkyvystä tehtäväänsä. Huumetestiä koskevan todistuksen työnantaja voi edellyttää työntekijältä siten kuin laissa yksityisyyden suojasta työelämässä säädetään.

6.3 Henkilöstön osaamisen varmistaminen

Työhöntulovaiheessa jokaisen työntekijän tulee osallistua ennalta suunniteltuun perehdytyskoulutukseen, joka antaa valmiudet toimia työyhteisön jäsenenä.

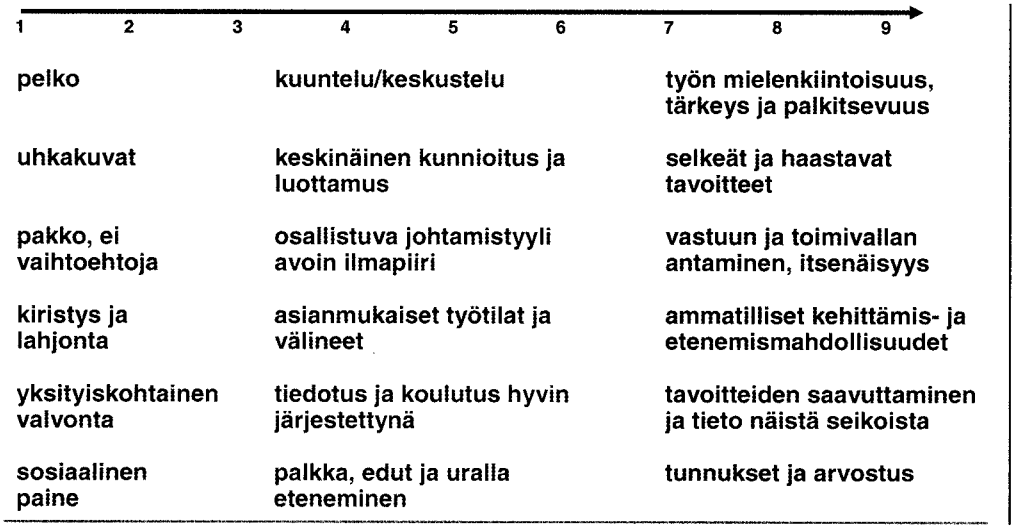
Jokaiselle työntekijälle laaditaan tehtäviin ja toimenkuvaan linkitetty koulutussuunnitelma, joka kattaa sekä ammatillisen koulutuksen että tietoturvakoulutuksen. Tietoturvakoulutuksen tulee olla säännöllistä, suunniteltua ja pakollista.

Osaamisen varmistamista tulee systemaattisesti seurata ja valvoa.

6.4 Avainhenkilöstö

Avainhenkilöiden kartoitus tehdään arvioimalla toimenkuvista tehtävän kriittisyysaste. Kriittistä osaamista pyritään levittämään siten, että saadaan toimiva varahenkilöjärjestelmä. Avainhenkilöasemassa olevat pyritään sitouttamaan mahdollisuuksien mukaisesti esim. palkka- ja palkkiopolitiikan sekä työsuhde-etujen avulla.

Henkilöstön omaehtoisen osaamisen ja organisaation toiminnan kehittämiseen tulee kehittää soveltuvat menettelyt. Kuvassa 3 on esitetty henkilöiden motivaatioita suhteessa henkilöiden käsittelyyn.



KUVA 3: Motivaatiosuora, tuloksia suhteessa henkilöiden käsittelyyn.

6.5 Työhöntuloprosessi

Työhöntuloprosessi tulee dokumentoida ja tarkistaa säännöllisesti. Prosessissa kuvataan toimet, jotka tulee tehdä uuden työntekijän aloittaessa työt. Prosessiin tulee kuulua ainakin seuraavat asiat:

- Ohjeistus työsopimuksen tekemiseksi
- Ohjeistus salassapitositoumuksen tai vastaavan tekemiseksi
- Ohjeistus tiedottamisesta uudesta työntekijästä
- Ohjeistus esittelykierroksen järjestämisestä
- Ohjeistus siitä, miten uusi työntekijä saa kulkuoikeudet ja tarvittavat avaimet
- Ohjeistus siitä, miten uusi työntekijä saa henkilökortin
- Ohjeistus siitä, miten uusi työntekijä saa käyttöoikeudet järjestelmiin
- Ohjeistus uuden työntekijän perehdytyskoulutuksen järjestämisestä
- Ohjeistus uuden työntekijän työssään tarvitsemien laitteiden hankintaa varten

Osa työhöntuloprosessin toimenpiteistä tehdään vasta työntekijän aloitettua työt. Suurin osa tehtävistä on kuitenkin sellaisia, että uuden henkilön esimiehen tai henkilöstöhallinnon tulee hoitaa ne ennen työn aloitusta.

6.6 Prosessi työsuhteen päättyessä (tai keskeytyessä pitkäksi ajaksi)

Terminointiprosessi sisältää tehtävät toimenpiteet työsuhteen päättyessä. Prosessi tulee dokumentoida ja tarkistaa säännöllisesti. Työsuhde (tai vastaava) voi päättyä usealla eri tavalla: mm. irtisanoutumiseen, irtisanomiseen, sopimuksen purkuun, eläkkeelle siirtymiseen tai kuolemaan. Jokaiselle vaihtoehdolle tulee luoda omat prosessit. Prosesseihin tulee kuulua ainakin seuraavat asiat:

- Ohjeistus tiedottamisesta
- Ohjeistus käyttöoikeuksien poistamiseksi
- Ohjeistus kulkuoikeuksien poistamiseksi ja avaimien palauttamiseksi tai takaisin saamiseksi
- Ohjeistus henkilökortin palauttamiselle tai takaisin saamiselle
- Ohjeistus laitteiden ja muun organisaation omaisuuden palauttamiselle tai takaisin saamiselle
- Ohjeistus työnantajan tarjoamien sähköisten identiteettien sulkulistausta varten
- Ohjeistus sähköpostin ja muun postin käsittelyä varten

Mikäli työsuhteen päättyminen on ennakoitavissa, prosessiin tulee lisätä vielä seuraavat:

- Ohjeistus tehtävien siirtämiseksi
- Ohjeistus osaamisen siirtämiseksi

6.7 Sijais- ja väliaikaisjärjestelyt

Sijaisjärjestelyjä tarvitaan pitkäaikaisia poissaoloja varten. Tällaisia poissaoloja ovat mm. komennukset, virkavapaat ja hoitovapaat. Väliaikaisjärjestelyjä tarvitaan lyhyempiä poissaoloja varten. Tällaisia poissaoloja ovat mm. kertausharjoitukset ja sairauslomat.

Sijais- ja väliaikaisjärjestelyille tulee luoda prosessit, jotka kattavat vastuiden siirrot ja käyttöoikeuksien muutokset näiden järjestelyjen aikana. Prosesseihin tulee kuulua ainakin seuraavat asiat:

- Ohjeistus tiedottamisesta
- Ohjeistus sijaisen käyttöoikeusjärjestelyistä
- Ohjeistus poissaolijan käyttöoikeusjärjestelyistä

6.8 Työnkierto ja lomat

Toimenkuviin, joihin kuuluu esimerkiksi merkittävien rahasummien kirjaus ja käsittely, tulee liittää formaali työnkierto. Työnkierrolla estetään työntekijää rakentamasta järjestelmiä, joiden avulla voidaan peittää pitkäaikaisesti epäselvyydet hoidetuissa asioissa.

Formaali työnkierto on prosessi, joka tulee dokumentoida ja saattaa työntekijöiden tietoon. Työnkiertoon kuuluu määräaikainen tehtävien vaihto. Tehtävävaihto voi olla joko kokonaan uusi toimi tai sitten käsiteltävien tietojoukkojen tai asiakaskunnan vaihto. Tehtäviin, joihin liittyy formaali työnkierto, tulee liittyä myös lomanpitovelvollisuus.

Mikäli mahdollista, formaali työnkierto tulisi toteuttaa siten, että tehtävät eivät vaihdu, mutta käsiteltävä tieto, esimerkiksi asiakaskunta, vaihtuu. Mikäli työntekijöitä kierrätetään useissa eri tehtävissä, syntyy uusi henkilöriski siitä, että työntekijät oppivat tuntemaan laaja-alaisesti kontrollijärjestelmät ja väärinkäyttömahdollisuudet kasvavat. Tällaisia riskejä saattaa syntyä pitkäaikaisissa, stabiileissa johtamis- ja asiantuntijatehtävissä.

Mikäli toimenkuvaan ei ole liitetty formaalia työnkiertoa, pienimuotoinen työkierto voidaan toteuttaa loma-aikojen sijaisjärjestelyillä.

6.9 Ulkopuolinen työvoima

Ulkopuoliselta työvoimalta vaaditaan tietoturvamielessä vähintään samaa kuin omalta henkilöstöltä. Valtion työntekijöitä koskevat velvoitteet tulevat lainsäädäännöstä; vastaavat velvoitteet tulee tarvittaessa asettaa ulkopuoliselle työvoimalle sopimusteitse. Ulkopuolisesta työvoimasta kuten konsulteista tulee tarvittaessa tehdä työtehtävän edellyttämän laajuinen tuvallisuusselvitys.

6.10 Varautuminen poikkeusoloihin

Valmiussuunnitelmaan tulee kuulua osana henkilöstön varaussuunnitelma. Varaussuunnitelmassa määritellään keskeisten järjestelmien toimintojen turvaamiseksi tarvittavat henkilöresurssit. Asevelvollisille henkilöille tehdään VAP-varaukset (vapautus aseellisesta palveluksesta) viraston kotipaikan sotilaslääninn esikunnasta. VAP varaukset tulee tarkistaa ja päivittää säännöllisesti. Huolimatta mahdollisuudesta henkilövarauksiin poikkeusolojen organisaatioon tulisi mahdollisuuksien mukaan mahduttaa ei-asevelvollista henkilöstöä.

6.11 Järjestelmäluokkien erityispiirteet

6.11.1 Eheys ja käytettävyys tärkeitä

Henkilöstön valmiustaso tulee olla korkealla tasolla. Tähän päästään riittävällä resursoinnilla sertifioidulla henkilöstöllä.

6.11.2 Eheys ja luottamuksellisuus tärkeitä

Henkilöstön tulee sisäistää julkisuuslain salassapitomääräykset.

7 FYYSINEN TURVALLISUUS

Henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden. (VAHTI 4/2004: Valtionhallinnon tietoturvakäsitteistö)

Lähtötaso	
Vaatimus	Kuvaus
Kulunvalvonta	Kulunvalvonta on järjestetty siten, että kukaan ei pääse saapumaan tai poistumaan tulematta rekisteröidyksi.
Tunkeutumis- ja ilkivaltasuojaus	Tila on ikkunaton ja sijoitettu rakennuksen keskelle. Rakenteet, ovet ja lukot tarjoavat riskianalyysin mukaisen suojauksen.
Palosuojaus	Tiloissa on paloilmoituslaitteisto ja sammutinlaitteisto.
Lämpösuojaus	Jäähdytys- ja ilmastointilaitteisto on riittävä pitämään jatkuvasti ilman lämpötilan ja kosteuden sopivina.
Savusuojaus	Savun kulkeutuminen ilmanvaihtojärjestelmän kautta osastosta toiseen on estetty.
Vesivahinkosuojaus	Tiloissa ei ole putkistoja, jotka voisivat aiheuttaa vesivahingon. Tilat on rakennettu alapohjan päälle, jonka alla on kosteusanturit.

Lähtötaso	
Vaatimus	Kuvaus
Pölysuojaus ja puhtaus	Pinnoitemateriaalit eivät muodosta pölyä. Tuloilmasta suodatetaan epäpuhtaudet. Siivous on säännöllistä ja riittävää.
Laitteistojen kunnossapito	Laitteistot huolletaan säännöllisesti ja niille on toiminnan takaava huoltosopimus.
Henkilöstö ja koulutus	Henkilöstö on osaava ja sitä koulutetaan säännöllisesti.
Palo-osastointi	Tilat on palo-osastoitu käyttötarkoitusten mukaisesti.
Sähkön saannin varmistaminen	Sähkön saanti on varmistettu vähintään UPS-tasoisilla laitteilla ja varavoimalla.

Perusohjeistus
VAHTI 1/2002: Tietoteknisten laitetilojen turvallisuussuositus
VM 1/01/99: Suositus toimitilaturvallisuuden huomioonottamisesta valtionhallinnossa

Standardit
BS7799

7.1 Yleistä

Keskeisten tietojärjestelmien sijoituspaikan on tarjottava korkean käytettävyyden turvasuojattu konesalitila sekä muut tätä toimintaa tukevat turvalliset tilat. Tilojen tulee olla VAHTI 1/2002 –dokumentin määritelmän mukaan täyssuojattuja. Tällainen täyssuojattu kiinteistö pitää sisällään paljon rakenteellisia erikoisratkaisuja ja turvatekniikkaa.

Tilojen ulkopuolisten osien turvasuojaus on suunniteltava kokonaisuutena kohteen muiden käyttäjien kanssa. Toimitilaturvallisuussuosituksen mukaan täyssuojatun kohteen osalta on pyydettävä suunnitteluvaiheessa suojelupoliisin lausunto kohteen erityisriskeistä ja suojautumistoimenpiteistä.

7.2 Tilat

Konesalitilat tulee osastoida niin, että kahdennetut tietojärjestelmät voidaan sijoittaa eri konesaleihin. Konesalien tulee olla erillisiä palotiloja.

Käyttöolosuhteiden konesaleissa tulee olla samanlaiset yhteisten teknisten olosuhdejärjestelmien varmistamina, mutta konesalien tulee silti toimia toisistaan riippumattomina.

Tiloilta edellytetään käytettävyyttä keskeytyksettä normaali- ja poikkeusoloissa ja soveltuvuutta käyttöhenkilöstön jatkuvaan työskentelyyn myös poikkeusoloissa.

Käyttöhenkilöstön on pystyttävä jatkamaan työskentelyä myös yksittäisen osaston tai osajärjestelmän vikaantuessa.

Tilojen tekniset järjestelmät tulee mitoittaa toimimaan täydellä henkilöstöllä ja maksimaalisella käyttökuormituksella normaali-, suodatus- ja sulkutilassa.

Tilat muodostuvat kahdesta EMP-suojatusta perusosasta, konesalitiloista ja käyttö- ja valvontatiloista. Tilat osastoidaan käyttötarkoituksen, olosuhteiden hallinnan, palosuojauksen ja kulunrajoitusten mukaisesti. Konesaliosaan tulee kuulua ainakin tallennearkisto sekä kaksi erillistä konesalia.

Tilat ja sen toimintaa tukevat järjestelmät on suunniteltava siten, että sen käyttötarkoitus kriittisten tietojärjestelmien turvallisena toimintatilana mahdollisimman hyvin täyttyy. Suunnitteluvalintojen on suosittava varmatoimisia, huollettavia ja häiriöttömiä käyttöolosuhteisiin soveltuvia toteutuksia. Käytettävien materiaalien tulee olla ensisijaisesti palamattomia ja vähän palokaasua kehittäviä.

Vesivuotojen riski on hallittava kaikissa vettä sisältävissä järjestelmissä ja vesivuodot on estettävä tarvittaessa suojaavalla koteloinnilla tai muilla vastaavilla ratkaisulla.

7.3 Olosuhdehallinta

Tilojen olosuhteiden teknisten hallintajärjestelmien, ilmanvaihdon, jäähdytyksen, sähkönsyötön ja turvasuojausjärjestelmien tulee olla jatkuvakäyntisiä, varmennettuja ja käytön aikana huollettavissa ilman tiloissa olevien atk-laitteiden toimintakatkoa.

Olosuhteet on oltava hallittuja kaikissa keskeisten tietojärjestelmien toimintaa tukevissa konesali- ja käyttötiloissa sekä normaali- että poikkeusoloissa. Olosuhteiden hallinta toteutetaan osastoittain siten, että yhden osaston toiminta ei vaikuta toiseen osastoon tai sen toimintaan. Osaston sisällä olosuhteet ovat kaikille siellä oleville järjestelmille yhteiset. Erikoislaitteiden olosuhteita voidaan hallita kohdekohtaisella toteutuksella.

Sähkönsyötön, jäähdytyksen, palo- ja turvasuojauksen ja valvonnan kapasiteetit tai tasot eivät saa laskea toimitilan muuttuessa normaalioloista poikkeusoloihin tai päinvastoin. Toimintaa tukevien ulkopuolisten järjestelmien on toimittava myös poikkeavissa olosuhteissa, kuten korkeissa pakkas-, helle-, tuuli-, vesi- tai lumiarvoissa. Kunkin olosuhteita ohjaavan osajärjestelmän on kyettävä itsenäiseen toimintaan ilman toisen järjestelmän oh-

jausta. Järjestelmien tulee olla varmennettuja, valvottuja ja riittäviä katkottoman toiminnan takaamiseen. Olosuhdejärjestelmiä tulee voida ohjata sekä keskitetysti yhdestä pisteestä että paikallisesti konesalikohtaisesti.

Käyttökatkon tai turvalaukaisun jälkeinen kaikkien koneiden yhtäaikainen käynnistyminen ja tästä aiheutuvat sähkö- ja lämpökuormitusongelmat on hallittava.

7.4 Toiminta tiloissa

Kaikki tiloissa tapahtuvan toiminnan tulee olla valvottua. Käyttöhenkilöstö on paikalla pääsääntöisesti virka-aikana, mutta kohteessa on voitava työskennellä valvotusti myös muuna aikana. Poikkeusoloissa kohde on jatkuvasti miehitetty. Lisäksi on varauduttava siihen, että tiloissa on myös normaaliaikana jatkuva miehitys.

Tietojärjestelmien toiminta pyritään pitämään yllä niin pitkään kuin mahdollista. Mikäli laitteet ovat vaarassa tuhoutua konesalin toiminta on oltava katkaistavissa konesalikohtaisesti.

Käyttö- ja operointitilat rajataan siten, että osa tiloista on vierailukäyttöön ja osa on pelkästään henkilökunnalle tarkoitettua ja rajoitettua operointitilaa.

7.5 Henkilö- ja tavaraliikenne

Toimitiloissa tulee olla S3-suojausluokan mukainen valvonta ja hallinta. Kulkua konesalitiloihin valvotaan ja hallitaan sisäänkäynnin kulkuannostelijasta lähtien osastokohtaisesti kaikkialla tiloissa.

Henkilöiden kulkua valvotaan osastoittain kahteen suuntaan tapahtuvalla henkilötunnistuksella. Kulunvalvonnan hallinta on hierarkkinen. Kulunvalvonta voidaan toteuttaa siten, että pääsyyn vaaditaan vähintään kaksi henkilöä kerrallaan tai pääsy sallitaan tai evätään etäällä olevasta valvontapisteestä.

Kiinteistön kulunvalvonnan lisäksi on oltava myös tilojen ulkopuolinen kulunvalvonta ennen tavara-liikenteen päästämistä tiloihin. Saapuva ja lähtevä tavara käsitellään erillisissä tiloissa.

Kaikki lukitukset ovat valvottuja ja tilojen sisäänkäynneissä on murtovarma lukitus. Tavarankuljetusovien aukaisu on mahdollista vain lisäkontrollilla ja valvottuna.

Pakkausmateriaalin ja jätteiden käsittely suoritetaan erillisissä tiloissa.

7.6 Poistumistiet ja pelastustoimen reitit

Poistumistiet ja -reitit on suunniteltava, merkittävä ja tiedotettava kaikille tiloissa työskenteleville henkilöille. Pelastustoimen tarpeet ja rajoitukset toimitilaturvallisuuden osal-

ta on tarkastettava ja hyväksytettävä palotarkastajan kanssa erikseen osana koko kohteen turvallisuussuunnittelua.

7.7 Turvavalaistus

Tiloissa on oltava norminmukainen turvavalaistus. Kaikkialla tiloissa on oltava turvallisen työskentelyn mahdollistava varavalaistus tai vastaava varmennettu valaistus.

Kaikissa tiloissa tulee olla vähintään videovalvonnan minimitason mukainen jatkuva valaistus.

7.8 Palontorjunta

Kaikissa tiloissa on oltava osoitteellinen paloilmoitinjärjestelmä. Konesaleissa ja kaikissa teknisissä tiloissa tulee olla näytteenottava tai muu ennakoivaan paloilmoitukseen pystyvä järjestelmä. Ennakoivan paloilmoituksen välitys olosuhteidenvalvontajärjestelmään on oltava. Palosammutuksen toimintalogiikka ja muiden järjestelmien katkaisulogiikka on suunniteltava ja toteutettava tilakohtaisesti erikseen.

Kaikki tilat tulee varustaa niihin suunnitelluilla sammutusjärjestelmillä. Sammutuskapasiteetin riittävyys mitoitetaan suurimman tilan sammuttamiseen. Konesalitiloissa tulee olla konesalikohtainen sammutusjärjestelmä. Osastot suunnitellaan siten, että kukin osasto on erikseen sammutettavissa. Tilojen ollessa miehitettyinä sammutuslaukaisussa on oltava peruutusmahdollisuus. Eri osastojen järjestelmien laatua vastaavaa käsisammutuskalustoa on oltava varattuna osastokohtaisesti.

7.9 ATK- ja teletilojen pakko-ohjaukset

Tiloissa on oltava osastokohtainen katkaiseva hätäseis-toiminto sekä atk- ja datalaitteiden sähkönsyötölle että jäähdytykselle ja ilmastoinnille.

7.10 Rikosilmoitinjärjestelmät

Tilat tulee varustaa koko tilat kattavalla yhdenkertaisella rikosilmoitinjärjestelmällä. Kaikkien ovien sekä tilojen tulee olla valvottuja. Valvonta on aina päällä kun tilassa ei työskennellä. Työskentelyaika kriittisissä tiloissa on oltava aikarajoitettu. Rikosilmoitinjärjestelmään voidaan tarvittaessa liittää erillisiä kohdesuojauksia.

7.11 TV- ja videovalvonta

Kaikissa osastoissa tulee olla nauhoittava ja etäkäytettävä digitaalinen kameravalvonta, jonka tallentama aineisto siirtyy kohteen ulkopuolella olevaan etävalvomoon. Etävalvomopäivystys on jatkuvasti toiminnassa.

7.12 Tekniset henkilöturvajärjestelmät

Tiloissa tulee olla yhteishälytysmahdollisuus (hätäpainike) ja viestiyhteys operointitiloihin.

7.13 Väestönsuojat

Tiloissa tulee olla majoitusmahdollisuus käyttötoiminnasta vastaavalle henkilöstölle ulkopuolisesta huollosta riippumatonta toiminta-aikaa vastaavaksi ajaksi.

7.14 Sähkönsyötön turvaaminen

Sähkö on tuotava kahdella erillisellä varmennetulla sähkönjakelulla, jotka viedään erillisinä konesalien ryhmäkeskuksille saakka. Tasainen ja häiriötön sähkönsyöttö varmistetaan UPS-suojauksella. Sähkönsyöttö varmistetaan varavoimakoneella, joka on mitoitettu tietojärjestelmien täydelle toimintakapasiteetille.

7.15 Teletilat ja -reitit

Tiloissa on oltava kaksi erillistä EMP-suojauksen ulkopuolista valvottua kaapeloinnin järjestely- ja läpivientitilaa. EMP-suojauksen sisäpuolella tulee olla ristikytkentätila, joka voidaan tarvittaessa turvaosastoida. Telereittien tulee olla avattavat ja tarkistettavat. Konesaleihin tulee olla erilliset telereitit sekä ristikytkentätiloista että operointitiloista.

7.16 Viestijärjestelmät

Tiloissa tulee olla puhelinvaihde ja riittävä määrä kiinteitä puhelinyhteyksiä. Muita viestintäjärjestelmiä varten tulee olla varaus kaapeloinnille.

7.17 Asennuslattia

Asennuslattian rakenteet on tuettava ristiin ja maadoitettava. Lattian tulee kantaa laitesijoituksen mukaiset kuormat ja kestää niiden kuljettaminen paikan päälle. Pintamateriaalin tulee estää staattisen sähkön synty ja rakenteen tulee muodostaa maadoitettu häiriöitä vaimentava taso. Pintamateriaalin tulee olla hyvin kulutusta kestävää.

7.18 Varautuminen poikkeusoloihin

Täyssuojattu laitetila pystyy pääsääntöisesti jatkamaan toimintaansa poikkeusoloissa pitkiäkin aikoja. Viraston on määriteltävä aikavaatimus. Valmiussuunnitelmassa tulee kuitenkin varautua toimintojen siirtämiseen varatiloihin.

Valmiussuunnitelman tulee kattaa sekä toimintojen jatkaminen pääasiallisissa laitetiloissa että varatiloissa. Suunnitelma tulee testata säännöllisesti.

7.19 Järjestelmäluokkien erityispiirteet

7.19.1 Eheys, käytettävyys ja luottamuksellisuus tärkeitä

Sopimusten tulee olla kattavia ja ne tulee synkronoida sidosryhmien sopimusten kanssa.

7.19.2 Eheys ja käytettävyys tärkeitä

Palvelutasosopimusten tulee kattaa myös laitetilat.

8 TIETOLIIKENNETURVALLISUUS

Toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus. Tietoliikenneturvallisuuteen tähtääviä keinoja ovat mm. laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen. (VAHTI 4/2004: Valtionhallinnon tietoturvakäsitteistö)

Lähtötaso	
Vaatimus	Kuvaus
Verkkosegrekaatio	Eri turvatasojen tietoverkot, verkkosegmentit ja tehtävät on eristetty toisistaan.
Kiinteistönvalvontaverkon eriyttäminen	Kiinteistövalvontaverkko on eriytetty tietoverkoista loogisesti ja fyysisesti.
Dokumentointi	Tietoliikenneyhteyksistä on ajan tasalla oleva dokumentaatio.
Kaapeloinnin suojaus	Kaapelointi on suojattu fyysisiltä uhilta: katkaiseminen, häirintä, kiinnittyminen jne.
Aktiivilaitteiden suojaus ja asetukset	Aktiivilaitteet on sijoitettu fyysisesti turvattuihin tiloihin ja ne on konfiguroitu siten, että tunkeutumisen riskit ovat minimoidut.
Ulkoisten yhteyksien turvaaminen	Ulkoiset tietoliikenneyhteydet ovat pitkälle vikasietoisia ja niille on lisäksi varajärjestelyt.

Lähtötaso	
Vaatimus	Kuvaus
Tunkeutumisen havaitsemis- ja estämisjärjestelmät	Tietoverkoissa on mekanismi tunkeutumisen havainnointia ja estoa varten.
Telekopiolaitteet ja telex	Laitteet on sijoitettu turvallisesti ja niiden käyttö on dokumentoidun käyttöpolitiikan mukaista.
Etätyö- ja etäkäyttöyhteydet	Tietoliikenneyhteydet organisaation oman verkon ulkopuolelta tapahtuvaa työskentelyä varten on suojattu.
Varajärjestelyt	Tärkeimmille tietoliikenneyhteyksille on varajärjestelyt.
IP-puhelut	Puheluiden välittäminen IP-verkoissa on turvattu.

Perusohjeistus
VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi
VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003: Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003: Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 3/2002: Valtionhallinnon etätyön tietoturvallisuusohje
VAHTI 3/2001: Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus
VAHTI 2/2001 Valtionhallinnon lähiverkkojen tietoturvallisuussuositus

Standardit
BS7799

8.1 Suunnittelu

Tietoverkon turvallisuus on otettava huomioon jo suunnittelussa. Myöhemmin tehtävät turvallisuuspaikkaukset eivät useinkaan pysty korjaamaan ennen verkon rakentamista tehtyjä virheitä. Turvallisuuden lisääminen jälkikäteen on myös huomattavasti kalliimpaa kuin vastaavan tason ratkaisujen toteuttaminen alusta lähtien.

Eräs tärkeimmistä ja helposti unohtuvista suunnittelukriteereistä on tiedonsiirron tarve: onko reaaliaikainen tiedonsiirto järkevin vaihtoehto? Usein reaaliaikaisella tiedonsiirrolla vältetään redundantti tietoaineisto ja siitä johtuvat ylläpitohankaluudet. On kuitenkin tilanteita, joissa eräsiirtoratkaisut ovat kokonaiskustannuksiltaan edullisempia kuin reaaliaikaratkaisut.

Tietoverkon suunnitteluvaiheessa on tehtävä tietovirta-analyysi, analyysi turvallisuustavoitteista ja suunniteltava niiden pohjalta tietoverkon turva-arkkitehtuuriratkaisut, turvakomponenttien sijoitteluratkaisut sekä mitoitettava verkon siirtokapasiteetti ja huomioitava tarvittavien tietoliikenneprotokollien mahdolliset erikoistarpeet. Suunnitteluvaiheeseen kuuluu myös verkon valvonnan suunnittelu sekä testaussuunnitelman laadinta. Suunnittelun pohjana ovat tiedot, joita siirretään ja niiden turvaluokka.

Verkon käytettävyysasteen korkeana pitämiselle on tärkeää, että jo suunnitteluvaiheessa otetaan huomioon vaihtoehtoisten tiedonsiirtoreittien ja –resurssien käyttö. Kahdennetut yhteydet ja varayhteydet tulee suunnitella siten, että ne eivät missään kohdassa ole riippuvaisia yksittäisestä toimivasta komponentista. Järjestelyt tulee tarkastaa päästä päähän sekä loogisella että fyysisellä tasolla. Huomiota tulee kiinnittää erityisesti sellaisiin paikkoihin, joihin kaapeleiden vetäminen on vaikeaa. Tällöin saattaa paljastua, että useat kaapelit saattavat kulkea joko jopa samassa kaapelitunnelissa tai erittäin lähellä toisiaan.

Hallinta- ja valvontayhteydet tulee erottaa fyysisesti varsinaisesta tuotantoverkosta.

Sekä tilaajan että toimittajan velvollisuuksiin kuuluu kaikkien tietoliikenneyhteyksien testaus päästä päähän.

8.2 Dokumentaatio

Tietoverkon omistaja asettaa tietoverkolle dokumenttivastaavan, joka huolehtii siitä, että tietoverkko on asianmukaisesti dokumentoitu ja dokumentointia myös ylläpidetään ja valvotaan.

Tietoliikenneyhteyksistä tulee dokumentoida myös käyttö; dokumenteista tulee ilmetä tietovirrat, tietojen omistajuus sekä tietojen käyttäjät. Tietoliikenteeseen liittyvät rajapinnat ja tiedonsiirtoprotokollat on dokumentoitava varayhteyksineen ja manuaalisine varajärjestelmineen.

Tietoliikennedokumentaatiosta tulee olla sekä sähköiset että paperiset turvakopiot hajautetusti tallennettuina.

8.3 Palomuurit

Palomuurin tehtävänä on erottaa toisistaan kaksi tai useampi verkkosegmentti ja kontrolloida näiden verkkosegmenttien välistä liikennettä asennetun sääntökannan mukaisesti. Palomuuri voi olla joko sovellus, jota ajetaan normaalissa tietokonelaitteistossa tai erillinen laite, joka sisältää laitealustan, käyttöjärjestelmän ja palomuurisovelluksen.

Palomuuri tulee asentaa kovennettuna tarkan asennussuunnitelman mukaisesti käyttöjärjestelmästä ja protokollapinosta alkaen.

Palomuurin sääntökanta konfiguroidaan toteuttamaan tietoliikennepolitiikan mukaiset suodatukset. Säännöt tulee testata.

Palomuurin sääntöjen hallintaa varten tulee rakentaa prosessi, joka kuvaa vastuut ja tehtävät muutospyyntöjen käsittelylle. Prosessin tulee varmistaa, että palomuuridokumentaatio on aina ajantasainen.

Jos verkko on kriittinen, palomuurin on oltava korkean käytettävyyden ratkaisu. Tämä toteutetaan yleensä kahdentamalla palomuuri siihen liittyvine verkkokomponentteineen. Kahdennetut verkkokomponentit vaativat huolellista valvontaa, koska yhden komponentin vikaantuminen ei näy toiminnallisena häiriönä. Kahdennettu ratkaisu tulee myös tarkastaa, jotta järjestelmään ei jää ainuttakaan yksittäisvikapistettä (SPOF, Single Point of Failure).

8.4 Verkon varmistukset ja varajärjestelyt

Varmistukset ja varajärjestelyt tulee suhteuttaa verkon kriittisyyteen; kriittisen verkon tulee olla mahdollisimman vikasietoinen ja turvattu varajärjestelyin vikasietoisuuden pettämisen varalta.

Varmistusten ja varajärjestelyjen tila tulee selvittää myös sidosryhmien osalta silloin, kun ollaan riippuvaisia näistä. Mikäli tilanne ei ole tyydyttävä, joko asianomaisen sidosryhmän on korjattava tilanteensa hyväksyttävälle tasolle tai riskialttiit järjestelyt on turvattava muunlaisin varajärjestelyin.

Varayhteyksien on oltava joko jatkuvassa käytössä osana tuotantojärjestelmää tai ne on testattava säännöllisesti. Varajärjestelyt tulee mitoittaa siten, että ne takaavat riittävän palvelutason.

8.5 Operointi ja valvonta

Viraston tulee laatia tietoverkolle tietoliikennepolitiikka. Politiikassa tulee dokumentoida mm. sallitut tietoliikenneyhteydet verkkojen välillä, valvonta- ja koestusvälineiden asennus ja käyttö, verkon pääsynvalvonta, verkon käyttö sekä sallitut käyttäjäryhmät.

Verkon operointi- ja valvontayhteydet tulee eriyttää varsinaisesta tuotantoverkosta – mielellään fyysisellä tasolla. Operointi- ja valvontajärjestelmät tulee suojata luvattomalta käytöltä ja kaikesta käytöstä on jäätävä riittävät lokimerkinnät, joiden perusteella käyttö voidaan jälkikäteen jäljittää.

Verkon valvonnan tulee kattaa sekä verkon fyysisen valvonnan (topologia, komponentit, jne.) että liikenteen valvonnan (profiili, protokollat, jne.). Fyysistä valvontaa tekevien järjestelmien tulee pystyä havaitsemaan ainakin luvattomat laitteet, luvattomat kiinnitäytymiset verkkoon sekä näiden yritykset. Liikenteen valvontaan tulee kuulua tunkeutumisen havainnointi- ja estojärjestelmä. Valvonta- ja varajärjestelyt tulee toteuttaa siten, että myös heikentynyt toiminta havaitaan.

Keskeisten järjestelmien käyttämissä tietoverkoissa tulee suosia pysyviä, yksikäsitteisiä verkko-osoitteita, kuten kiinteät IP-osoitteet sekä vianmäärityksen helpottamiseksi että turvapolitiikasta poikkeavan toiminnan paikallistamisen helpottamiseksi. Aitojen kiinteiden IP-osoitteiden sijasta voidaan myös käyttää verkkokorttitunnisteeseen sidottuja dynaamisia IP-osoitteita; tällöin laite saa ensimmäisellä kerralla verkkoon liittyessään IP-osoitteen verkon osoiteavaruudesta ja jatkossa aina saman osoitteen.

8.6 Langattomat tietoliikenneyhteydet

Langattomien tietoliikenneyhteyksien suurimmat riskit ovat liikenteen luvattomassa kuuntelussa, liikenteen häirinnässä ja luvattomassa liittymisessä langattomaan verkkoon. Keskeisten tietojärjestelmien kriittisissä yhteyksissä tulee suosia langallisia tiedonsiirtokanavia.

Yritystason laitteilla toteutetun langattoman verkon palvelunestohyökkäykseen tarvitaan riittävän tehokas sopiva lähetin. Mikäli kriittinen yhteys on langaton, sillä tulee olla käytettävyyden turvaamiseksi varayhteys, joka ei ole langaton.

Langattomia yhteyksiä käytettäessä todennusmekanismien tulee olla riittäviä, koska langattomaan verkkoon voi lähettää dataa kuka tahansa sopivan lähettimen omistava. Riittävä todennusmekanismi määritetään verkon käyttöpolitiikassa riskianalyysin perusteella.

Koska langatonta yhteyttä voi kuunnella sopivalla vastaanottimella, tulee luottamuksellinen liikenne salata. Salausvaatimukset tulee määritellä riskianalyysin perusteella.

8.7 Ulkopuoliset yhteydet ja palvelut

Ulkopuoliset yhteydet tulee toteuttaa siten, että ne noudattavat tietoverkolle määriteltyä turvallisuus- ja käyttöpolitiikkaa. Ulkopuoliset yhteydet ovat aina tietoriskejä; toteutuksen, suojauksen ja valvonnan tulee pohjautua tehtyihin, dokumentoituihin riskianalyyseihin.

Internet-yhteyden toteuttaminen tulee tehdä siten, että liityntä on suojattu palomuurilla, joka toteuttaa turvallisuus- ja käyttöpolitiikan mukaiset säännöt.

Kumppaniyhteydet ovat tarveharkintaisia. Niitä voidaan toteuttaa useilla erilaisilla ratkaisuilla, kuten Internet-yhteys, VPN, Frame Relay -yhteys, dedikoitu kaapeli jne. Yhteyksien salaus-, tunnistus-, todentamis-, käytettävyys- ja eheysratkaisut tulee toteuttaa riskianalyyseihin pohjautuen.

Etähuoltoyhteydet tulee määritellä siten, että järjestelmiin ei ole avointa pääsyä ulkopuolelta. Laitteisto voi vikaantumistapauksessa ottaa yhteyttä etähuoltoon ja ilmoittaa viasta. Huoltoa varten järjestelmävastaava voi sallia ja avata etähuoltoyhteyden. Etähuollon tekevä taho on todennettava tietoturvapolitiikan vaatimukset täyttävällä todennusratkaisulla.

Etähuollolle tulee määrätä oman organisaation vastuuhenkilö, joka tarvittaessa valvoo huoltotoimenpiteitä. Huolto-ohjelmistot ja -laitteet eivät saa mahdollistaa tunkeutumista muuhun tietoverkkoon. Toimittajan huoltodokumentaation on huomioitava tietoturvallisuus myös tältä osin.

Keskeisten järjestelmien etäkäyttöä tulee pyrkiä välttämään. Jos etäkäyttö sallitaan, sen tulee toteuttaa etäkäyttöpolitiikan vaatimukset ja käyttö mahdollistetaan vain rajattuun, ei-tietoturvakriittiseen osaan. Muu käyttö on estettävä.

8.8 Varautuminen poikkeusoloihin

Tietoliikenneratkaisut tulee suunnitella siten, että ne ovat tarvittavassa laajuudessa ja käyttötarkoituksessa hyödynnettävissä myös poikkeusoloissa.

8.9 Järjestelmäluokkien erityispiirteet

8.9.1 Eheys, käytettävyys ja luottamuksellisuus tärkeitä

Tietoliikenneyhteydet on rakennettu sidosryhmät huomioiden. Palvelutasosopimukset kattavat yhteydet päästä päähän myös sidosryhmien osalta.

8.9.2 Eheys ja käytettävyys tärkeitä

Käytettävyyttä voidaan varmistaa käyttämällä eri toimittajien tietoturvaratkaisuja samaan tehtävään joko peräkkäin tai verkon eri pisteissä. Näin varmistetaan, ettei yhdessä tuotteessa oleva ongelma vaaranna koko verkkoa. Rinnakkaisia tuotteita voidaan käyttää esim. reititykseen, palomuureina, haittaohjelmien ja roskapostin torjuntaan ja hyökkäysten havainnointiin ja torjuntaan.

8.9.3 Eheys ja luottamuksellisuus tärkeitä

Tiedon eheyden varmistamiseksi tulee lähettäjä todentaa vahvasti ja tietoliikenne tulee toteuttaa sellaisten protokollien avulla, jotka varmistavat tiedon muuttumattomuuden. Riittävän vahva todennus tulee määritellä riskianalyysin perusteella. Vahvasti suojatuissa ympäristöissä riittävä todennus voi olla se, että lähettäjä pääsee lähettämään ja riittävä eheyden varmistava protokolla voi pohjautua tarkastussummaan siirtovirheen havaitsemiseksi. Tällaista ratkaisua voidaan käyttää esimerkiksi sarjaliikenneyhteyksissä, joissa sekä laitteet että siirtotie ovat fyysisesti turvattuja. Toinen ääritapaus on julkisen verkon käyttö: todennuksen tulee olla vähintään kahteen tekijään perustuva (two factor authentication, esim. toimikortit tai kertakäyttösalasanan generoivat laitteet) ja tiedon muuttumatto-

muuden varmistamiseksi tulee käyttää kryptografiaan perustuvia protokollia.

Tiedon luottamuksellisuuden varmistamiseksi tulee vastaanottaja todentaa vahvasti ja siirrettävä tieto tulee salata tai siirtää dedikoitua, salakuuntelulta suojattua siirtoyhteyttä käyttäen. Todennus- ja salausratkaisujen taso valitaan riskianalyysin perusteella.

Yhdensuuntaista tiedonsiirtoa voidaan käyttää silloin, kun tietojärjestelmään halutaan siirtää tietoa ulkopuolelta, mutta samalla halutaan varmistua siitä, että tietojärjestelmästä ei pystytä lukemaan tietoa tai päinvastoin.

Yhdensuuntaisuus voidaan toteuttaa yksinkertaisimmillaan pakettisuodatuksen avulla. Riskien pienentämiseksi on mahdollista kytkeä peräkkäin useita laitteita, joissa vastinkomponentit, kuten käyttöjärjestelmä ja pakettisuodatusohjelmisto, ovat eri toimittajilta. Tämäntyyppinen suojaus on teoreettisesti mahdollista murtaa.

Täysin varmistettu yhdensuuntaisuus voidaan toteuttaa sellaisella ratkaisulla, jossa tiedonsiirto toiseen suuntaan on estetty siten, että toista lähetyskomponenttia ei ole laitteistossa ollenkaan. Tällainen ratkaisu on esimerkiksi datadiodi. Tämän tyyppisen ratkaisun ongelma on se, että siirtoprotokolla tulee rakentaa täysin yhdensuuntaiseksi. TCP-IP-protokollaperheessä se tarkoittaa TCP-protokollasta luopumista ja siirtymistä esimerkiksi UDP:n käyttöön. Tarkastussummien avulla voidaan estää korruptoituneen tiedon tallennus, mutta uudelleenlähetyspyyntöjä ei voida välittää.

Välimuotoinen ratkaisu yhdensuuntaisuudelle on esimerkiksi sarjaliikenne. Sarjaliikenteessä voidaan rajoittaa paluulähetykset kuittauksiin ja uudelleenlähetyspyyntöihin. Ratkaisu ei kuitenkaan kokonaan poista piilokanavia (covert channel) eikä estä ohjelmistovirheistä aiheutuvia tietoturva-aukkoja.

Valitulle tiedonsiirtoratkaisulle saadaan lisäturvaa siten, että yhteys kytketään päälle vain tiedonsiirtotarpeen ajaksi ja yhteydenaikaisia prosesseja seurataan. Kun yhteyttä ei tarvita, tiedonsiirtokanava puretaan fyysisesti - yksinkertaisimmillaan irrottamalla tietoverkkokaapeli.

9 LAITTEISTOTURVALLISUUS

Tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden toteuttamiseksi. (VAHTI 4/2004: Valtionhallinnon tietoturvakäsitteistö)

Lähtötaso

Vaatimus	Kuvaus
Omistajuus	Jokaisella laitteella on yksiselitteinen omistaja, joka vastaa laitteesta.
Rekisteröinti ja turvamerkinnät	Jokainen laite on turvamerkitty ja luetteloitu laiterekisterissä.
Turvaluokittelu	Kaikki laitteet kuuluvat johonkin turvaluokkaan.
Huoltosopimukset	Niille laitteille on huoltosopimukset, jotka riskianalyysin perusteella sitä tarvitsevat.
Ennakoiva kapasiteetin suunnittelu	Tietojenkäsittelykapasiteetin tarve ennakoidaan ja hankinnat tehdään ajoissa.
Säännöllisen ylläpidon suunnittelu	Laitteiden ylläpito tehdään suunnitelmallisesti.
Asennusvaatimusten noudattaminen	Laitteet on asennettu suunnitelmallisesti ja sekä toimittajan että omistajan asennusvaatimuksia noudattaen.
Aikasynkronointi	Laitteistojen kellot ja kalenterit ovat oikeassa ajassa.

Lähtötaso	
Vaatimus	Kuvaus
Käytöstä poisto	Laitteiden käytöstä poisto on suunnitelmallista.
Haittaohjelmilta suojautumien	Laitteistoilla on asianmukainen ja säännöllisesti päivittyvä suojaus haittaohjelmia vastaan.

Perusohjeistus
VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi
VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 6/2001: Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista

Standardit
BS7799
ISF

9.1 Käytettävyys

Käytettävyyssuunnittelu tulee tehdä dokumentoitujen käytettävyysvaatimusten ja riskianalyysin perusteella. Riskianalyysin tuloksena saadaan (jollakin tarkkuustasolla) todennäköisyydet erilaisille käyttökatkon aiheuttaville tapahtumille. Näitä tapahtumia ovat tyypillisesti laiterikot, sähkökatkot ja onnettomuudet, kuten tulipalo tai vesivahinko. Osa tapahtumista on sellaisia, että jatkaminen samoilla laitteilla samoissa tiloissa on mahdotonta. Näiden tapahtumien varalta tulee virastolla olla jatkuvuussuunnitelma ja toipumissuunnitelma.

Varalaitteiden ja varaosien optimaalinen määrä voidaan laskea vikaantumisvälien odotusarvoista ja käytettävyystavoitteista. Alhaisilla käytettävyystasoilla riittävä käytäntö voi olla tyytyminen huoltosopimuksiin ja toimittajan varaosatoimituksiin. Mikäli omia varaosavarastoja ei pidetä, hankintasopimuksessa tulee olla toimittajalle velvoite varaosien saatavuudelle.

Korkean käytettävyyden järjestelmät voidaan monentaa. Vaihtoehtoisina ratkaisuina on usein joko palvelun monentaminen useisiin redundantteihin laitteisiin, vikasietoisen laitteiston hankinta tai yhdistelmä näistä. Ratkaisuvalinta on riippuvainen useista tekijöistä: sovelluksen tuki hajautukselle, sovelluksen ajon mahdollisuus vikasietoisella laitteistolla, liittyvien sovellusten arkkitehtuuri, kustannukset jne.

9.2 Toiminta, seuranta ja laajennettavuus

Laitteistojen toimivuus turvataan ennakoivien toimenpiteiden avulla. Laitteistojen tilaa tulee valvoa jatkuvasti ja automaattisesti mitattaville suureille tulee asettaa hälytysrajat. Mittausarvoista ja hälytyksistä voidaan usein päätellä, että tietty komponentti on joko rikkoutumassa tai liian pieni kapasiteetiltaan. Komponentti voidaan tällöin vaihtaa hallitusti.

Laitekokoonpanoja tulee seurata automaattisten järjestelmien avulla, jotka kirjaavat keskitetysti yksityiskohtaiset tiedot.

Uusien laitteiden tulee olla laajennettavia. Niissä on oltava vapaita korttipaikkoja, mahdollisuus keskusmuistin ja massamuistien lisäämiselle sekä vapaita oheislaiteliityntöjä. Varautumisella laajennuksiin taataan laitteelle pitkä käyttöikä.

9.3 Käyttöönotto

Riippumatta siitä missä ja miten laitteisto on koottu se on asennusvaiheessa tarkastettava. Toimitettujen laitteiden määrä ja laatu verrataan tilaus- ja toimitusasiakirjoihin. Lisäksi ne laitteistot, joiden kotelo voidaan avata, avataan ja tarkastetaan vähintään silmämääräisesti, jotta kotelossa ei ole mitään ylimääräistä eikä sieltä puutu mitään.

Keskeisten tietojärjestelmien sovellukset tulee asentaa joko sellaisille laitteistoille, joihin järjestelmästä vastaava organisaatio on itse asentanut käyttöjärjestelmän ja varusohjelmiston, tai sellaisille laitteistoille, joiden käyttöjärjestelmä-. ja varusohjelmistoturvallisuus on huomioitu sopimuksin. Käyttöjärjestelmä, varusohjelmisto ja sovellus tulee asentaa tarkan asennussuunnitelman mukaan, tarpeelliset kovennukset on toteutettava ja asennus on dokumentoitava.

Järjestelmä tulee ottaa ensiasennuksen myötä organisaation muutoksenhallintaprosessiin mukaan. Alkupisteen määrittää asennusdokumentaatio. Kaikki muutokset jatkossa tulee tehdä suunnitelmallisesti ja dokumentoidusti.

9.4 Kunnossapito

Organisaatiolla tulee olla kunnossapitojärjestelmä, jonka avulla suunnitellaan laitteistojen ja niiden komponenttien huollot sekä seurataan ja pyritään ennakoimaan vikaantumisia.

Kunnossapitoon kuuluu myös säännöllinen arviointi kapasiteetin riittävyydestä.

9.5 Käytöstä poisto

Laitteiston käytöstä poisto voi tapahtua kolmesta syystä: järjestelmästä luovutaan, järjestelmän käyttöä jatketaan uusitulla laitteistolla tai järjestelmä korvataan. Käytöstä poistosta

on laadittava tarkka suunnitelma, joka ottaa huomioon kunkin tilanteen vaatimukset. Mikäli kyseessä ei ole järjestelmästä luopuminen, suunnittelussa on erityisesti paneuduttava ongelmatilanteiden hallintaan ja selkeästi määriteltävä ne vaiheet, joista voidaan vielä palata takaisin, sekä ne toimenpiteet, joilla kustakin vaiheesta takaisin päästään.

Keskeisten tietojärjestelmien laitteistojen käytöstä poisto tarkoittaa useasti laitteiston siirtoa sellaisiin tehtäviin, joihin soveltuu jo elinkaarensa loppupuolella oleva laitteisto. Tällaisia tehtäviä ovat mm. laboratoriokäyttö, testikäyttö ja vähemmän kriittinen palvelinkäyttö. Suunnittelun tulee kattaa laitteiston perusteellinen tyhjennys, jotta luottamuksellista jäännösdataa ei pääse karkaamaan.

9.6 Laadunvarmistus

Laitteiston laatu ja soveltuvuus koostuvat monista tekijöistä. Laitteistojen ylläpidettävyyttä voidaan arvioida laajennettavuudella ja toimittajan tekemän kehityssuunnitelman pohjalta. Luotettavuuden arvioinnin pohjana voidaan käyttää tuotteen sijaintia elinkaarellaan: keski- ja loppupään tuotteista lastentaudit ovat yleensä karsiutuneet. Myös kokemukset toimittajasta, puolueettomat tuotevertailut sekä kumppanien kokemukset auttavat luotettavuuden arvioinnissa.

Hankinnoissa tulisi suosia laitteita, joista organisaatiolla tai muilla virastoilla on kokemusta ja osaamista. Uusia teknisiä ratkaisuja tai laitetyyppejä hankittaessa tulee niiden laatu ja muut tarvittavat ominaisuudet varmistaa sekä hyödyntää tässä tarvittavaa ulkopuolista asiantuntemusta ja virastojen välistä yhteistyötä.

9.7 Laitetyyppien erityisvaatimuksia

9.7.1 Palvelimet

Palvelinkäyttöön tulee valita vain tähän tarkoitukseen suunniteltuja laitteita. Laitteet tulee mitoittaa riittäviksi. Palvelinlaitteistot tulee sijoittaa asianmukaisiin laitetiloihin ja mielellään lukittaviin telineisiin. Palvelinverkot tulee eristää turvatason ja toiminnallisuuden mukaan. Valvonta-, hallinta- ja varmistusverkot tulee eristää varsinaisesta tuotantoverkosta. Palvelimien valvontatilaan tulee olla tiukka pääsynvalvonta. Varsinainen palvelintila tulee eristää valvontatilasta ja sinne tulee olla erittäin rajattu pääsy.

9.7.2 Päätelaitteet

Päätelaitteiden tulee olla mahdollisimman pitkälle standardoituja laitteiston, käyttöjärjestelmän ja varusohjelmiston osalta. Käyttäjällä ei tule olla pääkäyttäjäoikeuksia (root, administrator, jne.) työasemaan kuin hyvin perustelluissa poikkeustapauksissa. Päätelait-

teilla tulee olla valvontaohjelmisto, joka lähettää keskitettyyn tietokantaan tiedot laitteisto- ja ohjelmistokokoonpanosta.

Ohjelmistoasennukset ja -päivitykset tulee tehdä keskitetysti etäylläpito-ohjelmistojen avulla. Erityisesti tietoturvapäivitysten osalta organisaatiolla tulee olla testattu ja dokumentoitu prosessi, jonka mukaisesti tietoturvapäivitykset asennetaan hallitusti ilman turhia viivytyksiä.

Viraston keskitetyn hallinnon hyväksymättömät ja käyttäjien omat asennukset tulee kieltää ja kieltoa valvoa.

Varmistuksilla taataan käyttäjien tietojen katoamattomuus. Päätelaitteiden varmistusten tulee noudattaa organisaation varmistuspolitiikkaa ja olla käyttäjille mahdollisimman näkymättömiä ja automaattisia. Käyttäjien tulee olla tietoisia varmennuspolitiikasta.

Kannettaville tietokoneille pätevät kaikki päätelaitteita koskevat suositukset. Mikäli kannettavalla tietokoneella on jotain tietoa, joka ei ole julkista, koneella tulee olla käytössä levysalaus koneen katoamisen varalta. Toimistokäytössä kannettava tulisi kiinnittää työpisteeseen lukituksella.

Kämmentietokoneet ja älypuhelimet ovat toiminnoiltaan täysiverisiä tietokoneita. Myös ne ovat alttiita haittaohjelmille ja niille on saatavissa tietoturvaohjelmia, kuten haittaohjelmien torjuntaa tai VPN-asiakasratkaisuja. Näiden laitteiden käytön salliminen keskeisten järjestelmien yhteydessä tulee perustua riskianalyysiin.

9.7.3 Verkkolaitteet

Verkon aktiivilaitteet ovat kriittisiä komponentteja tietoverkon toiminnan kannalta. Monessa suhteessa ne ovat verrannollisia palvelinlaitteisiin. Laitteille tulee järjestää valvonta. Niille tulee laatia päivitysprosessit sekä turvapäivitysten että versiovaihdosten osalta.

Kriittisen verkon komponentit tulee monentaa siten, että minkään yksittäisen laitteen vikaantuminen ei estä verkon toimintaa. Valvonta tulee suunnitella huolellisesti, koska yksittäisen laitteen vikaantuminen näkyy vain valvontatiedoissa eikä toiminnallisuuden puutteena. Varalaitteiden hankinta tulee suhteuttaa verkon kriittisyyteen.

9.7.4 Levyjärjestelmät

Keskeisten järjestelmien levyratkaisuissa tulee suosia vikasietoisia vaihtoehtoja. Valinta tulee tehdä käytettävyysvaatimusten ja riskianalyysin perusteella. Levyjärjestelmä voidaan monentaa joko paikallisesti tai hajauttaa hyvinkin pitkien etäisyyksien päähän. Levyjärjestelmiä tulee valvoa, koska rikkoutunut levyasema ei välttämättä näy toiminnallisuudessa mitenkään.

9.8 Varautuminen poikkeusoloihin

Valtion atk-varakeskus tarjoaa valtion-, kuntien- ja yksityisen sektorin organisaatioille toiminnan jatkuvuuden turvaamiseen soveltuvia palveluita poikkeusolojen ja erilaisten tietojenkäsittelyjär-jestelmiä kohdanneiden katastrofitilanteiden varalle. Palvelut kohdistuvat kahteen eri toiminta-alueeseen, atk-varakeskukseen ja palvelinhotelliin.

Toiminta perustuu korkean turvatason laitetilaan, joka sijaitsee pääkaupunkiseudun ulkopuolelta. Palveluyhteistyön perusteena on asiakasorganisaation tietojärjestelmien kriittisyys ja tärkeys yh-teiskunnan toiminnan kannalta. Toimintaa johtaa ja ylläpitää Huoltovarmuuskeskus.

Huoltovarmuuskeskus on julkaissut turvaluokitellun dokumentin kriittisten tietojärjestelmien varaosahuollosta ja sovellusten siirrettävyydestä.

9.9 Järjestelmäluokkien erityispiirteet

9.9.1 Eheys ja käytettävyys tärkeitä

Tietojärjestelmäalustoiksi tulee valita vikasietoiset laitteet, joille on saatavissa nopeasti sekä huolto että varaosia. Valintakriteerinä tulee myös käyttää skaalautuvuutta ja kykyä sietää erilaisia palvelunestohyökkäyksiä.

9.9.2 Eheys ja luottamuksellisuus tärkeitä

Tietoverkossa olevan järjestelmän laitteistovalinnassa on huomioitava laitteistotoimittajan reagointinopeus tietoturvaongelmiin.

10 OHJELMISTOTURVALLISUUS

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. (VAHTI 4/2004: Valtionhallinnon tietoturvakäsitteistö)

Lähtötaso	
Vaatimus	Kuvaus
Tietoturvallisuuden huomioiva tietojärjestelmän elinkaariprosessi	Ohjelmistojen hankintaan, kehitykseen, käyttöönottoon ja ylläpitoon jne. on tietoturvallisuuden huomioiva prosessi.
Dokumentointi	Dokumentointi on kattavaa: vaatimukset, määrittelyt, tuotevertailut, testisuunnitelmat, testiraportit, asennukset, jne.
Standardiratkaisujen ja -rajapintojen käyttö	Valitut ratkaisut, tuotteet ja palvelut ovat keskenään yhteensopivia. Yleisesti hyväksyttyjä standardeja suositaan ja niiden käyttöä vaaditaan.
Lisenssien hallinta	Ohjelmistolisenssit ovat ajan tasalla ja hallinnassa.

Lähtötaso	
Vaatimus	Kuvaus
Arkkitehtuuriyhteensopivuus	Ohjelmistot sopivat viraston verkko-, sovellus- ja tietoturva-arkkitehtuuriin. Liitynnät sidosryhmien järjestelmiin ja arkkitehtuureihin huomioidaan.
Tietoturvalliset asennukset	Kaikissa asennuksissa huomioidaan tietoturvallisuus. Oletusarvoiset asennukset ymmärretään turvattomiksi.
Huolellinen ylläpito	Ylläpito on suunniteltua ja dokumentoitua.
Muutosten hallinta	Korjaus- ja tietoturvapäivityksiä varten on oma dokumentoitu prosessinsa.
Käyttäjätietojen hallinta, käyttäjien todennus ja pääsyoikeudet.	Ohjelmistojen vaatimat käyttäjätiedot ja pääsyoikeudet säilytetään ja hallitaan huolellisesti ja turvallisesti. Käyttäjien todennuksen tietoturvataso valitaan suojattavien tietojen turvaluokituksen perusteella.
Tukipalvelut	Ohjelmistoille on saatavilla riittävät tuki- ja päivityspalvelut.
Koulutus	Ylläpitäjät ja käyttäjät saavat riittävän koulutuksen ohjelmiston hallintaan ja käyttöön. Sovellushankintaan ja -kehitykseen osallistujille on järjestetty riittävä tietoturvakoulutus.
Varmistukset ja niiden toimivuuden testaus	Ohjelmistojen käsittelemät tiedot ja ohjelmiston käyttöasetukset varmistetaan säännöllisesti ja varmistusten oikeellisuus testataan.
Jäljitettävyys ja kontrollin sisäänrakennettuna ohjelmistoissa, tietojenkäsittelyssä ja prosesseissa	Ohjelmistot ja niiden hallinta ja käyttö tukevat monipuolisia kontrolleja ja jäljitettävyyttä ja ne on dokumentoitu.
Haittaohjelmien torjunta	Haittaohjelmien torjumisesta on huolehdittu.

Lähtötaso	
Vaatimus	Kuvaus
Merkistöjen vaikutukset	Eri merkistöt ja niiden riippuvuudet käyttöjärjestelmästä, käyttöliittymästä ja tiedostojärjestelmästä on huomioitu.

Perusohjeistus
VAHTI 3/2004: Haittaohjelmilta suojautumisen yleisohje
VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi
VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 3/2000: Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus
VM työryhmämuistio 27/2001: Valtion tietotekniikan rajapintasuosituksia

Standardit
TCSEC
ITSEC
Common Criteria
SSE-CCM
ISF
COBIT
ISO 15504 (SPICE)

10.1 Ohjelmistot

10.1.1 Käyttöjärjestelmät

Käyttöjärjestelmä tulee valita ohjelmiston käyttötarkoituksen ja sopivuuden perusteella, huomioiden kuitenkin organisaation osaaminen ja kokemus käyttöjärjestelmien käytön ja ylläpidon osalta.

Työasemissa tulee käyttää mahdollisimman standardoitua käyttöympäristöä. Palvelimissa on erityisesti huomioitava käyttöjärjestelmän kovennus eli turhan toiminnallisuuden poistaminen ja turvattomien oletusarvojen muuttaminen turvallisiksi. Keskeisten järjestelmien palvelinasennuksiin laaditaan sekä asennussuunnitelma että asennusdokumentaatio.

10.1.2 Tietoliikenneohjelmistot

Käytettävien tietoliikenneohjelmistojen tulee olla huolellisesti testattuja ja valittuja. Ohjelmistojen tulee tukea vahvaa salausta ja käyttäjätodennusta.

10.1.3 Tietoturvaohjelmistot

Käytettävien tietoturvaohjelmistojen tulee sopia viraston tietoturva-arkkitehtuuriin ja standardeihin. Tietoturvaohjelmistojen hallittavuutta ja yhteen toimivuutta tulee korostaa ja välttää ”tietoturvasaarekkeiden” syntymistä. Viraston tietoturvapolitiikkamuutokset tulee voida viedä mahdollisimman vaivattomasti tietoturvaohjelmistojen asetuksiin.

Ohjelmistotoimittajan tulee esittää tietoturvaohjelmiston tietoturvakriittisten osien dokumentoidut suunnitteluperiaatteet ja ratkaisumallit. Ohjelmistotoimittajan tulee olla valmis kolmannen osapuolen suorittamaan ohjelmiston auditointiin viraston näin vaatiessa. Auditointia valmisteltaessa kannattaa varmistaa mahdollisesti aiemmin tehdyt auditoinnit ja yhteistyömahdollisuudet. Tietoturvaohjelmistolle hankittu tietoturvasertifiointi, kuten Common Criteria tai FIPS, on etu.

10.1.4 Valmissovellukset

Valmissovellusten valinnassa tulee varmistaa sovelluksen toiminnallinen soveltuvuus, yhteensopivuus sekä olemassaolon ja jatkokehittämisen jatkuvuus.

Valmissovellusten tulee tukea viraston tietoturvapolitiikkaa, tietoturva-arkkitehtuuria ja standardeja. Valmissovelluksen tietoturvaominaisuuksien on täytettävä riskianalyysin perusteella asetetut vaatimukset ja sen tulee integroitua viraston valitsemiin käyttäjien todennus- ja valtuutustoimintoihin. Valmissovellukset eivät saa vaatia viraston kannalta erillisiä tai epästandardeja turvaratkaisuja, ellei se ole sovelluksen kannalta välttämätöntä esim. erityissuojausten toteuttamiseksi. Hallittavuuteen ja ylläpidon helppouteen on kiinnitettävä huomiota. Valmissovelluksessa on oltava riittävät loki-ominaisuudet tapahtumien jäljitettävyyden takaamiseksi.

Valmissovelluksen dokumentaatiosta on käytävä ilmi tietoturvaominaisuudet ja niiden käyttö sekä ohjeet sovelluksen tietoturvalliseen asennukseen ja vain tarpeellisten/välttämättömien ominaisuuksien käyttöönottoon. Tuotetoimittajan on tarvittaessa annettava erillinen selvitys valmissovelluksen sopivuudesta viraston tietoturvavaatimuksiin.

10.1.5 Räätälöidyt valmissovellukset

Räätälöintiä vaativilta valmissovelluksilta edellytetään vähintään samaa kuin valmissovelluksilta. Lisäksi räätälöinti on tehtävä suunnitelmallisesti projektityönä, jossa myös arvioidaan räätälöinnin vaikutus tietoturvallisuuteen. Räätälöinnin toteutuksesta on laadittava kattava dokumentaatio siten, että jatkossa räätälöintiä voi jatkaa uusi taho. Räätälöidyn osuuden on kuuluttava valmissovelluksen tuen piiriin.

10.1.6 Teetetyt sovellukset

Sovellusten teettäminen ulkopuolisella taholla on haasteellinen projekti myös virastolle ja vaatii käytännössä viraston asettamaa omaa projektipäällikköä toimittajan sovellusprojektipäällikön pariksi. Projektin alussa on määriteltävä selkeät vastuut, rajapinnat ja työnjako mm. vaatimusmäärittelylle, asennuksille, testauksille, osa- ja kokonaisprojektien hyväksymiselle, raportoinnille, kustannusseurannalle ja eskaloinnille.

Viraston nimeämän projektipäällikön tehtävänä on mm.:
- Toimia projektin ohjausryhmän jäsenenä
- Huolehtia oman organisaation resurssien riittävyydestä projektin aikana
- Seurata projektin etenemistä ja varmistaa aikataulun ja kustannusten pitävyys sekä resurssien riittävyys.
- Varmistaa viraston vaatimusten toteutuminen
- Valvoa hyväksymispisteiden saavuttamista
- Valvoa lopullista hyväksymistestausta
- Varmistaa riittävän dokumentaation syntyminen
- Eskaloida ongelmatilanteet

Sovellustoimittajilla on usein oma työskentely- ja projektimallinsa, joka ei välttämättä sovellu keskeisten, tietoturvakriittisten järjestelmien toteuttamiseen. Viraston on joko vaadittava sovellustoimittajalta selvitystä tietoturvavaatimusten huomioimisesta toimittajan omassa projektimallissa tai edellytettävä viraston oman, toimivaksi todetun projektimallin käyttöä. Käytettäessä sovellustoimittajan omaa projektimallia, toimittajan on osoitettava normaalia tiukempien tietoturvavaatimusten huomioiminen aikataulun, resurssien ja kustannusten suhteen. Toimittajan on myös varauduttava lisäresurssien saatavuuteen, mikäli normaalista poikkeavaa työtä ei oltu osattu arvioida oikein. Viraston tulee varmistaa sopimuksin, että sovellustoimittaja vastaa käyttämiensä alihankkijoiden resursseista ja sitoutumisesta viraston esittämiin vaatimuksiin.

Sovellustoimittajan laatujärjestelmä on syytä huomioida ja sovittaa se yhteen tarvittavin osin viraston omaan laatujärjestelmään. Panostamalla sovelluksen laatuun yleisesti, parannetaan samalla sovelluksen tietoturvallisuutta.

Projektityössä on huomioitava mm.
- Dokumentoitu sovelluskehitysmalli
- Laadun ohjaus ja varmistus
- Projektityön tietoturvallisuus
- Sovelluksen tietoturvallisuuden huomioiminen läpi koko projektin
- Sovelluksen vaikutukset muiden osa-alueiden tietoturvallisuuteen
- Testattavuuden huomioiminen
- Laajennettavuuden huomioiminen

- Raportointi
- Dokumentoinnin sopivuus viraston dokumentointistandardiin
- Käyttäjien ja ylläpidon koulutus

Viraston on joka tapauksessa selkeästi vaadittava sovelluksen sopeutumista viraston tietoturvapolitiikkaan, standardeihin, arkkitehtuureihin, tietoturvavaatimuksiin ja aiemmin valittuihin tietoturvaratkaisuihin. Sovelluksesta riippuen tietoturvavaatimuksiin kuuluvat esim. kirjausketju, salaus, todennus, valtuutus, hallinta, valvonta, lokit, lokien salaus tai aikaleimaus, sovelluspalveluiden sijoittelu, tietoturvapolitiikka, palomuurit, käytettävyys, toipuminen, varautuminen verkkohäiriöihin ja off-line tiedonsiirtoon. On huomattava, että pelkkä vaatimus tietoturvamekanismeista ei riitä, vaan myös haluttu tietoturvataso on määriteltävä.

Sovellustoimittajan on tietoturvaratkaisujen osalta esitettävä projektissa mm. seuraavat dokumentit:

- Sovelluksen määrittely huomioiden viraston tietoturvavaatimukset
- Tietoturvaratkaisut yksityiskohtaisesti
- Tietoturvaratkaisujen riskianalyysi
- Perustelut tietoturvaratkaisujen sopivuudesta viraston esittämiin vaatimuksiin
- Tietoturvaratkaisujen testisuunnitelma ja -tulokset

Teetetyissä sovelluksissa dokumentaation kattavuus ja tarkkuus korostuu. Dokumentaatioon hyväksyminen tulee olla oma projektitehtävänsä ja kriteereinä käytetään mm. kattavuutta, selkeyttä ja tietoturvakriittisten osuuksien yksityiskohtaisuutta. Dokumentaatiossa on otettava kantaa myös asennuksiin, kovennuksiin, valvontaan ja kriittisiin resursseihin. Virastolle toimitettavan dokumentaation perusteella jonkun muun kuin alkuperäisen sovellustoimittajan on kyettävä ylläpitämään ja jatkokehittämään sovellusta. Dokumentaation hyväksymisen yhteydessä on varmistettava myös lähdekoodin riittävä kommentointi.

Sovellusprojektin lopullinen hyväksymistestaus tulee tehdä viraston omassa testiympäristössä käyttäen mahdollisimman oikeanlaista testidataa. Testaus on tehtävä myös oletettua normaalikäyttöä suuremmalla kuormituksella. Ennen lopullista hyväksymistä sovellus on auditoitava kolmannen osapuolen toimesta. Minimissään auditoidaan suunnitelmat, dokumentaatio, asennukset ja tietoturvatoiminnallisuus, mutta tietoturvakriittisimmissä sovelluksissa on syytä auditoida sovelluksen tietoturvatoteutukset myös sovelluskooditasolla.

Sovellusprojektin päättyessä sovelluksen lähdekoodi ja omistusoikeus siirtyvät virastolle. Mikäli sovellukseen liittyy toimittajan omia tuotteita tai komponentteja, joiden omistusoikeutta ei voi siirtää, tehdään näiden osalta Escrow-sopimus. Virastolle annetaan oikeus lähdekoodiin, mikäli sovellustoimittaja häviää markkinoilta.

Teetetyn sovelluksen tuki on varmistettava sopimuksin toimittajan kanssa. On sovittava myös ohjelmointiresurssien saatavuudesta ongelmatapauksissa ja jatkokehityksen osalta.

10.1.7 Itse tehdyt sovellukset

Itse tehdyillä sovelluksilla on samat vaatimukset kuin teetetyillä sovelluksillakin. Lisävaatimuksena on, että virastolla tulee olla ammattimainen sovelluskehitysmalli ja omia osaavia ohjelmistoalan ja projektityön ammattilaisia. Sovellusprojektiosaamista tulee virastossa myös jatkuvasti kehittää.

Ylläpidon mahdollisesti hallintaa helpottamaan kehittämät pienimuotoiset ohjelmat ja skripit sekä käyttäjien työtä helpottamaan tekemät makrot, skriptit, yms. on hallittava vastaavasti kuin muutkin sovellukset. Näiden apuohjelmien tekijän lähtö organisaatiosta ei saa vaarantaa keskeisen tietojärjestelmän toimintaa, ylläpitoa tai tietoturvallisuutta.

10.1.8 Välitason sovellukset

Välitason sovelluksiksi (middleware) lasketaan kaikki tietojärjestelmäkomponentteja yhdistävät ohjelmistot, kuten web-palvelimet, sovelluspalvelimet ja integraatiotyökalut. Välitason sovellusten on luonnollisesti sovittava viraston arkkitehtuuriin ja toisaalta valitut ratkaisut ovat viraston arkkitehtuurin komponentteja, joiden käyttöön sovellusten on sopeuduttava.

Välitason sovellustuotteet ovat usein monimutkaisia ja vaativat erityisosaamista käytön, tietoturvapiirteiden ja hallinnan kannalta. Uuden välitason sovellustuotteen käyttöönottamisessa tulee noudattaa kriittisyyttä ja huolellisuutta. Joskus on parempi käyttää tuttua tuotetta, jonka tietoturvapiirteet ja -puutteet tunnetaan ja hallitaan sen sijaan, että vaihdetaan uuteen tuotteeseen.

Sovellussuunnittelussa on huomioitava, että eri turvallisuustason sovellusten käyttäessä samaa välitason sovelluskomponenttia, on välitason sovellus suunniteltava ja asennettava korkeimman tietoturvaluokituksen omaavan sovelluksen ehdoilla.

Dokumentaatioissa ja asennuksissa on huomioitava myös välitason sovellukset. Ohjeistuksen ja tietoturvakovennuksen tulee kattaa tietojärjestelmä tai sovellus kokonaisuudessaan, mukaan lukien välitason komponentit.

10.1.9 Sovelluskehitystyökalut

Tuotantojärjestelmissä ei saa olla asennettuna sovelluskehitystyökaluja. Sovelluskehitystyökalujen käyttö on rajattava erityisiin kehitysympäristön laitteisiin, jotka on kokonaan eristetty tuotantojärjestelmistä. Sovelluskehityksessä on vältettävä työkaluja, joissa ei ole erillistä ajoaikaista ympäristöä.

10.1.10 Tietoturvallinen ohjelmointi

Sovelluskehitystyössä on varmistettava suunnittelijoiden ja ohjelmoijien osaaminen ja kyky tuottaa tietoturvallista koodia. Sovellussuunnittelijoilla on oltava tietämys sovellusten

tietoturvasuunnitteluperiaatteista ja ohjelmoijilla tietämys käyttämiensä työvälineiden tietoturvapiirteistä, mahdollisuuksista ja heikkouksista.

Tietoturvakriittiset sovellusosiot on syytä eristää muusta toiminnallisuudesta.

10.2 Ohjelmistoasennukset

Virastolla täytyy olla toisistaan eristetyt testi- ja tuotantoympäristöt. Mikäli virasto tekee sovelluskehitystä, tarvitaan lisäksi erillinen kehitysympäristö. Uudet sovellukset ja sovellusmuutokset viedään tuotantoon aina suunnitelmallisesti testiympäristön kautta. Toiminnan varmistamiseksi testiympäristön tulee olla identtinen tuotantoympäristön kanssa. Testiympäristössä on mallinnettava myös tuotantoympäristön tietoturvakomponentit, kuten reitittimet, palomuurit, tietomurtohälytinjärjestelmät, kuormanjakolaitteet, kahdennetut laitteet, yms. ympäristöön monimutkaisuutta ja mahdollisia virhetekijöitä tuovat komponentit.

Asennuksissa on erityisesti huomioitava tietoturvakovennukset tietojärjestelmän kaikkien komponenttien osalta. Normaalisti asennus oletusarvoilla ei ole hyväksyttävää. Asennukset tulee suunnitella huolellisesti ja laatia asennussuunnitelma. Asennustapahtuma ja mahdolliset poikkeamat kirjataan asennusdokumenttiin. On huomattava, ettei alihankkijoiden ja sovellustoimittajien normaalit asennusrutiinit välttämättä riitä keskeisten tietojärjestelmien asennukseen ja siksi heidän suunnitelmiensa ja työnsä taso on tarkistettava.

Samaa laitealustaa tai välitason sovellusta käyttävistä sovelluksista korkeimman tietoturvaluokituksen omaava sovellus määrää myös jaetun laitteen ja välitason sovelluksen tietoturvavaatimukset.

Sovellusasennukset on syytä auditoida ensimmäisen kerran jo testiympäristössä. Tuotantoasennus on auditoitava ennen käyttöönottoa ja sen jälkeen säännöllisesti – erityisesti muutosten yhteydessä.

10.3 Turvallisuustoimet

Keskeisissä tietojärjestelmissä on kiinnitettävä erityistä huomiota tietoturvatoimiin ja -menetelmiin, niiden valintaan ja toteutuksen laatuun. Tietoturvatason määrää tietojärjestelmässä käsiteltävän tiedon turvaluokitus ja itse tietojärjestelmän tärkeysluokitus. Erityishaasteena on huomioida tietojärjestelmä kokonaisuutena.

Seuraavassa huomioita tärkeimmistä ohjelmistojen tietoturvamenetelmistä keskeisten tietojärjestelmien osalta:

Tietoturvamenetelmä	Kuvaus
Tietoturvaluokittelu	Palvelut, sovellukset ja komponentit on kaikki luokiteltava niiden käsittelemien tietojen turvaluokituksen pohjalta.
Tietoturvavaatimusten määrittely	Tämä on olennainen osa sovelluksen toteutus- tai hankintaprojektia ja se alkaa jo esitutkimuksesta. Ilman kunnollista vaatimusmäärittelyä riittävää tietoturvatasoa ei saavuteta. Vaatimusmäärittelyn tueksi tehdään sovelluskohtainen riskianalyysi.
Tietoturvaratkaisujen tekninen määrittely ja kuvaus	Vaatimusten mukaiset tietoturvaratkaisut tulee dokumentoida yksityiskohtaisesti. Teknisen määrittelyn pohjalta voidaan todentaa ratkaisujen soveltuvuus ja riittävyys ja toisaalta tekninen määrittely toimii ohjeena sovellusohjelmoijille.
Käyttäjätietojen hallinta	Käyttäjätiedot on hallittava ajantasaisesti ja mahdollisimman keskitetysti. Hallintaprosessit ja työnkulku on dokumentoitava. Sovelluksiin liittyvät käyttäjätiedot on kyettävä kytkemään yhteiseen käyttäjähallintamenettelyyn.
Käyttäjätodennus	Käyttäjätodennustapa valitaan käsiteltävien tietojen luokituksen perusteella. Käyttäjätietojen hallinta ja todennus on pyrittävä erottamaan sovelluksesta erilliseksi, yhteiskäyttöiseksi toiminnoksi. Vahvoja todennusmenetelmiä, kuten kertakäyttösalasanoihin ja toimikortteihin perustuvia menetelmiä tulee suosia. Sovelluksilta tulisi minimissään vaatia mahdollisuutta nostaa todennusmekanismin tasoa tarvittaessa.
Pääsynvalvonta	Sovellusten on tuettava monipuolista pääsynvalvontaa ja mahdollisuutta käyttää erillistä pääsynvalvontaan keskittynyttä palvelua.
Käyttöoikeudet	Käyttäjille on annettava vain tarvittavat oikeudet sovelluksiin. Samoin sovelluksia tulee aja vain tarvittavilla minimioikeuksilla.
Istunnon hallinta	Sovellusistunto on toteutettava huolellisesti varmistaen, ettei istuntoa voida kaapata, väärentää eikä luvattomasti nauhoittaa ja toistaa. Joutilas istunto on aikakatkaistava ja aika on oltava määriteltävissä.
Kirjausketju	Sovelluksen tiedon käsittely, mukaanlukien tietojen katselu, on pystyttävä jäljittämään.

Tietoturvamenetelmä	Kuvaus
Lokit	Sovelluksen on tuotettava lokitietoa sovelluksen käytöstä ja ylläpidosta. Vaatimuksena voi jopa olla lokitietojen salaus ja sähköinen allekirjoitus lokitietojen muuttumattomuuden takaamiseksi.
Palveluiden eristäminen	Eri tietoturvatason omaavat palvelut ja komponentit tule eristää toisistaan teknisesti ja hallinnollisesti. Samoin eristetään toisistaan kehitys-, testi-, koulutus- ja tuotantoympäristöt.
Tehtävien eriyttäminen	Seuraavat tehtävät on eriytettävä toisistaan: kehitys-, testaus, ylläpito ja auditointi.
Syötteen tarkastus ennen käyttöä	Kaikki sovelluksen tai sovelluskomponentin ulkopuolelta tullut syöte on tarkastettava ennen käyttöä. Tarkistusvastuuta ei voi jättää esim. client-sovellukselle tai toiselle komponentille. Sähköisillä allekirjoituksilla voidaan myös varmistaa tiedon aitous ja muuttumattomuus siirron aikana.
Salaus	Tietoliikenne tulee salata minimissään käyttäjän laitteesta sovelluspalvelimelle. Vaatimuksena voi olla myös tietojen salaaminen tietokantaan asti.
Testattavuus	Sovellussuunnittelussa on huomioita tietoturvapiirteiden testattavuus.
Käytettävyys	Käytettävyyttä voidaan parantaa monin eri tavoin ja sovelluksessa on varauduttava vikatilanteisiin ja toipumiseen valitun käytettävyysratkaisun avulla. Sovellussuunnittelussa on otettava kantaa toipumisen nopeuteen ja päätettävä priorisointi nopean toipumisen ja tietojen ehdottoman luottamuksellisuuden välillä.
Ylläpitomekanismit	Sovelluksen ja erityisesti sen tietoturvaominaisuuksien ylläpitomekanismit on suunniteltava ja turvattava huolella.
Virhetilanteiden hallinta	Sovelluksessa on varmistettava virhetilanteiden hallinta. Vakavassa tai yllättävässä virhetilanteessa sovelluksen tulee varmistaa, ettei ylimääräisiä tietoturvariskejä synny. Erityisesti tietoturvakomponenttien tulee noudattaa ”fail-closed”-mallia eli yllättävän virheen sattuessa komponentin ja sovelluksen käyttö estetään mieluummin kokonaan kuin annetaan mahdollisuus luvattomaan käyttöön.
Auditointi	Sovellus ja sen tietoturvallisuuden hallinnointi on auditoitava ennen käyttöönottoa.

10.4 Tarkkailu- ja paljastustoimet

Ohjelmistoissa on oltava kattavat mekanismit ohjelmiston käytön ja ylläpidon tarkkailuun sekä väärinkäytösten havainnointiin. Käytännössä tämä tarkoittaa kattavia ja monipuolisia loki- ja raportointitoimintoja. Tapahtumalokiin on sisällytettävä aikaleima ja kriittisimmissä sovelluksissa on varauduttava lokitietojen salaamiseen ja/tai sähköiseen allekirjoittamiseen.

Viraston on pyrittävä yhdenmukaiseen ja keskitettyyn lokien käsittelyyn. Lokien soveltuvuutta oikeuskäsittelyyn voidaan parantaa huolellisilla lokien käsittelyprosesseilla ja eriyttämällä lokien käsittely normaalista sovelluskäytöstä ja -ylläpidosta. Lokien keräämisessä ja käsittelyssä on luonnollisesti huomioitava yksityisyydensuoja.

Sovelluksen tulee havaita selkeät väärinkäyttöyritykset ja kirjata tapahtumat lokiin sekä hälyttää tapahtumasta. Sovelluksen käsittelemiin tietoihin voidaan mahdollisesti sijoittaa dataa, jota normaalissa toiminnassa ei tarvita, mutta jonka käsittely aiheuttaa hälytyksen.

10.5 Varautuminen poikkeusoloihin

Sovellussuunnittelussa on varauduttava verkkokatkoksiin ja suunniteltava välttämättömien tietojen saantimahdollisuus sovellukseen eräsiirtoina tietovälineiden, esim. DVD-levyjen avulla.

Riittävä sovellustoimittajan tuki ja oma osaaminen on varmistettava.

10.6 Järjestelmäluokkien erityispiirteet

10.6.1 Eheys ja käytettävyys tärkeitä

Korkea käytettävyys vaatii tyypillisesti vikasietoisia tai monennettuja järjestelmiä. Käytettävyys voidaan varmistaa usealla eri tavalla ja tasolla laitteita ja sovelluskomponentteja monistamalla ja hajauttamalla. Sovellus tulee alun perin suunnitella toipumaan virhetilanteista ja mahdollistamaan sovelluksen osittaisen käytön, mikäli jossain tilanteessa täydellinen toipuminen on mahdotonta. Käytettävyyden olleessa ensiarvoisen tärkeää, sovellus pitää suunnitella toipumaan mahdollisimman nopeasti.

Sovellusten kannalta on oleellista testata toiminta häiriö- ja poikkeustilanteissa. On huomattava testata koko tietojärjestelmä kaikkine komponentteineen: verkko, hakemistot, käyttäjärekisterit, todennuspalvelimet, tietokannat, jne. Ei riitä, että sovellus on käynnissä – sen on myös oltava käytettävissä ja tietojen saatavilla. Käytettävyyden suunnittelussa tulee huomioida kaikki osa-alueet.

Tietojärjestelmään voi miettiä myös vaihtoehtoisia, rajoitettuja käyttötapoja. Häiriö-

tilanteessa tietoja voidaan ehkä käyttää hankalakäyttöisemmin, rajoitetuimmalla käyttöliittymällä, jolloin vain kriittisimmät toiminnot ovat käytettävissä.

Käytettävyyden kannalta tärkeää on tietojärjestelmän skaalautumiskyky. Mitoitus on tehtävä siten, että yllättävä normaalia suurempi käyttö ei lamauta järjestelmää. Kovan kuormituksen varalle tulee etukäteen miettiä käyttäjien priorisointia eri kriteereillä ja varmistaa tärkein käyttö.

Sovellus on kyettävä varmistamaan, ylläpitämään ja päivittämään sovelluskäytön häiriintymättä.

10.6.2 Eheys ja luottamuksellisuus tärkeitä

Luottamuksellisuuden säilymisen perusta on huolellinen käyttäjätietojen hallinta ja seuranta sekä asiattomien pääsyn estäminen luottamuksellisiin tietoihin.

Luottamuksellisuutta voidaan parantaa käyttämällä vain vahvoja käyttäjätodennusmenetelmiä, kuten sähköisiin varmenteisiin perustuvaa todennusta. Samoin pääsynvalvontatekniikoihin ja pääsyoikeuksien myöntöprosesseihin tulee kiinnittää erityishuomiota.

Tietojen luottamuksellisuus ja eheys voidaan varmistaa käytettävien tietojen ja lokien salauksella ja sähköisellä allekirjoituksella. Tämä vaatii sovellukselta erityistoiminnallisuutta.

Sovelluksissa tulee olla sisäänrakennettu hälytysjärjestelmä väärinkäytösten estämiseksi. Ennakoimattomassa vikatilanteessa, jossa tietojen luottamuksellisuus tai eheys saattaa olla uhattuna, sovelluksen käyttö tulee estää kokonaan.

11 TIETOAINEISTOTURVALLISUUS

Tietoturvallisuuteen tähtäävät toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen. (VAHTI 4/2004: Valtionhallinnon tietoturvakäsitteistö).

Lähtötaso	
Vaatimus	Kuvaus
Tietojen luokittelu ja tietovälineiden luokittelumerkinnät	Tiedot on luokiteltu julkisuuslain ja -asetuksen sekä VAHTI-ohjeiden mukaisesti sekä asiakirjoihin ja tietovälineisiin on merkitty luokitus.
Käsittelysäännöt	Tiedolle on luokituksittain käsittelysäännöt, joista käy ilmi vaatimukset tiedon koko elinkaarelle.
Omistajuus	Jokaisella tiedolla on omistaja, joka vastaa tiedon luokituksesta, jakelusta ja käytöstä sekä määrittelee tietoturvavaatimukset.
Rajattu pääsy vain työssä tarvittaviin tietoihin ja hallintavälineisiin	Tiedot ja tietojärjestelmät on suojattu pääsynvalvontamekanismein siten, että työntekijöillä on pääsy vain niihin tietoihin ja järjestelmiin, jotka ovat välttämättömät työtehtävien hoitamiseksi.
Käyttöoikeusprosessit	Käyttöoikeuksien myöntämiseksi on olemassa dokumentoidut prosessit.

Lähtötaso	
Vaatimus	Kuvaus
Tietovälinepolitiikka	Tiedon tallennusvälineiden ja erityisesti siirrettävien tallennusvälineiden (esim. CD-ROM, levyke, flash-muisti) käyttö ja käyttörajoitukset on ohjeistettu.
Lukittavat säilytystilat	Salassa pidettävien asiakirjojen ja salassa pidettävää tietoa sisältävien siirrettävien tallennusvälineiden säilytystä varten on omat, sitä varten suunnitellut lukitut säilytystilat.
Tietoaineistoin turvallinen hävitys	Tietoaineiston turvallinen ja luokituksen mukainen hävitys on ohjeistettu.
Henkilökohtaiset tunnukset ja jäljitettävyys	Kaikki tietojärjestelmäkäyttö tapahtuu henkilökohtaisilla tunnuksilla. Yhteiskäyttöisiä tunnuksia ei sallita.
Salassapitosopimukset	Salassapitosopimuksilla täydennetään laista johtuvaa salassapitovelvollisuutta elleivät lain säädökset kata kaikkea toimeksisaajalle luovutettavaa tietoa tai jos halutaan liittää salassapitoon esimerkiksi sopimusoikeudellisia sanktioita.
Salaustekniikka	Salaustekniikka on valittu siten, että käytettävät salausalgoritmit ovat vahvoiksi tunnettuja ja niiden implementaatiot tarkastettuja.
Arkistointi	Arkistoinnissa noudatetaan dokumentoitua arkistonmuodostussuunnitelmaa.
Dokumenttien tunnistetiedot	Dokumenteissa on yksikäsitteiset tunnistetiedot, jotka vastaavat dokumentinhallintajärjestelmän tunnistetietoja.
Tietosuoja	Henkilötietojen käsittelyn tulee täyttää henkilötietolain vaatimukset. Syytä on huomioida henkilötietokäsitteen laajuus.

Perusohjeistus
VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi
VAHTI 4/2003: Arkaluonteiset kansainväliset tietoaineistot
VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointisuositus

VAHTI 1/2001: Valtion viranomaisen tietoturvallisuustyön yleisohje
VAHTI 2/2000: Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje
VM 21/01/2000 Tarpeettomaksi tulleiden tietoaineistojen hävittäminen
Arkistolaitoksen määräys ja ohje 216/40/2003: Valtionhallinnon asiakirjojen seulonta ja hävittäminen
Arkistolaitoksen määräys ja ohje 195/40/2003: Asiakirjojen ja tietojen rekisteröinti asiankäsittelyjärjestelmissä tai asiakirjarekistereissä.
Arkistolaitoksen ohje 62/40/2003: Asiakirjojen suojaaminen poikkeusoloissa.
Arkistolaitoksen määräys 284/40/2001: Asiakirjojen siirtäminen arkistolaitokseen
Arkistolaitoksen määräys ja ohje 126/40/2001: Sähköisten tietojärjestelmien ja aineistojen käsittely

Standardit
BS7799

11.1 Tietojen luokitus ja tietojärjestelmien luokittelu käytettävien tietojen perusteella

Tietojen luokitusvaatimukset määräävät sekä laki viranomaisten toiminnan julkisuudesta eli julkisuuslaki (621/1999) että tämän lain perusteella annettu asetus (1030/1999).

Suomella on kansainvälisiä sopimuksia mm. WEU:n ja NATO:n kanssa, joissa on sovittu ulkomaisten asiakirjojen salassa pidosta. Kansainväliset turvaluokitukset ovat verrannollisia Suomessa käytettyjen luokitusten kanssa.

Jos tietojärjestelmässä käsitellään turvaluokiteltua tietoa, käyttäjän on oltava siitä tietoinen. Mikäli tietoaineistossa on sekä julkista että salassa pidettävää tietoa, salassa pidettävät tiedot on selvästi merkittävä salassa pidettäviksi. Tietojärjestelmän suojaukset on mitoitettava turvaluokitukseltaan vaativimman käsiteltävän tiedon mukaisiksi.

Tiedoille tulee olla käsittelysäännöt luokittain. Näistä tulee käydä ilmi vaatimukset tiedon koko elinkaaren ajaksi: luomiselle, tallennukselle, jakelulle, käytölle, ylläpidolle ja tuhoamiselle. Käsittelysääntöjen noudattamista tulee valvoa.

Tiedon salassapitoajat määrätään lainsäädännössä.

11.2 Omistajuus ja käyttöoikeudet

Jokaisella tiedolla on oltava omistaja, joka päättää tiedon luokituksesta, käytöstä ja jakelusta.

Käyttöoikeudet tulee mahdollisuuksien mukaan luoda siten, että käyttäjällä on ainoastaan tarvittavat oikeudet tehtäviensä hoitamiseen. Käyttöoikeudet tulee jakaa siten, että vaarallisia yhdistelmiä ei pääse syntymään; käyttäjällä ei esimerkiksi saa olla oikeuksia oman työnsä hyväksyntään tai tarkastamiseen.

Käyttöoikeudet tulee sitoa työtehtäviin. Kun henkilön työtehtävät vaihtuvat, käyttöoikeudet tulee päivittää vastaaviksi. Virastolla tulee olla dokumentoidut työtehtävien muutosprosessit (sisältäen työhöntulon ja työsuhteen päättymisen), jotka huomioivat myös muutokset käyttöoikeuksissa.

11.3 Salassapitosopimukset

Salassapitosopimuksien tarkoitus on täydentää laissa määrättyä salassapitovelvollisuutta. Salassapitovelvollisuus saadaan täten koskemaan kaikkea vaihdettavaa materiaalia. Salassapitosopimuksien avulla voidaan tiedon paljastamiseen lisätä esimerkiksi rahallisia sanktioita. Salassapitosopimus koskee molempia osapuolia. Salassapitositoumus on mahdollista tehdä, jos halutaan yksipuolinen salassapitovelvollisuus.

Usein erillistä salassapitosopimusta tai -sitoumusta ei tarvitse tehdä, koska lainsäädäntö kattaa tietojen salassapidon. Varsinaisissa sopimuksissa on kuitenkin hyvä tuoda kirjallisesti esille lain vaatimukset.

11.4 Dokumenttien hallinta

Dokumenttien hallinta tulee mahdollisuuksien mukaan toteuttaa tietojärjestelmien avulla, jolloin dokumentteihin kohdistuvia toimintoja voidaan automatisoida ja käyttäjätoimintoja monipuolistaa.

11.5 Tietoaineiston eheyden varmistaminen

Tietoaineiston eheys tulee varmistaa jo tietoaineistoa luotaessa. Lähteet tulee varmistaa, kuten myös viittaukset muuhun tietoaineistoon. Tietoaineiston käsittelysääntöjen tulee ohjeistaa eheyden varmistus manuaalitasolla. Tietojärjestelmissä tiedon käsittelysäännöt tulee dokumentoida ja toteuttaa dokumentoinnin mukaisesti. Viite-eheys tulee pyrkiä varmistamaan jo sovellustasolla mutta viimeistään tiedonhallintajärjestelmän asetuksilla.

11.6 Tietovälineiden käsittely

Viraston tietoturvapolitiikan on otettava kantaa siirrettävien tallennusvälineiden, kuten levykkeiden, flash-muistien ja optisten muistien käyttöön. Siirrettäviä tallennusvälinei-

tä, joissa on salassa pidettävää tietoa tulee käsitellä samojen vaatimusten mukaisesti kuin salassa pidettävää paperiasiakirjaa. Tietovälineitä tulee käsitellä huolellisesti, vaikka niille olisi tallennettu pelkästään julkista aineistoa, koska kadotettu tietoväline tekee helposti vahinkoa julkisuuskuvalle.

Salassa pidettävää aineistoa, joka ei kuulu kahteen korkeimpaan turvaluokkaan, on luvallista käsitellä verkkoon kytketyssä työasemassa. Tällöin on varmistuttava siitä, että sekä tilapäiset työtiedostot että jäännösdata säilyvät luottamuksellisina.

11.7 Tietoaineiston säilytys ja arkistointi

Tietoaineisto voidaan säilyttää ja arkistoida joko sähköisessä tai manuaalisessa muodossa.

Tietoaineiston säilytystilojen turvallisuus tulee mitoittaa säilytettävän aineiston kriittisyyden mukaan riskinanalyysin pohjalta. Huomioitavia asioita ovat riittävä murtosuojaus, paloturvallisuus, lämpötila, ilman kosteus, pöly, valo jne. Eri tietovälineillä on säilytyksen osalta erityisvaatimuksia.

Säilytettävä tietoaineisto tulee kopioida ja kopiot tallentaa fyysisesti eri tiloihin. Säilytettävä tietoaineisto on luetteloitava.

Tietoaineiston arkistoinnin tulee pohjautua arkistointisuunnitelmaan, jonka puolestaan tulee perustua arkistolakiin (831/1994). Suunnitelmien toteutumista tulee myös valvoa. Tietoaineistoon sisältyy myös tietojärjestelmiin liittyvä dokumentaatio.

11.8 Tietoaineiston varmuuskopiointi

Tietojärjestelmissä oleva tieto tulee varmuuskopioida säännöllisesti. Varmuuskopiointiväli määritellään riskianalyysin perusteella. Pääsääntöisesti ainakin yksi varmuuskopio tulee sijoittaa fyysisesti eri palotilaan kuin alkuperäinen aineisto; selkeä maantieteellinen välimatka varmuuskopion ja alkuperäisen välillä olisi erittäin suotava. Tallennusvälineitä, joissa varmuuskopioita säilytetään voidaan kierrättää ja käyttää uudelleen varmuuskopiosuunnitelman puitteissa.

Mikäli varmuuskopioiden luottamuksellisuus halutaan turvata, voidaan kopioitava materiaali salata. Varmuuskopion eheys voidaan varmistaa sähköisellä allekirjoituksella. Tarvittaessa voidaan käyttää sekä salausta että allekirjoituksia.

11.9 Tietoaineiston jakelu, luovutus, tulostus

Tietoaineistoa voidaan jaella sähköisesti tai manuaalisesti.

Tietoaineiston jakelu- ja luovutuskäytännöt riippuvat tietoaineiston luokituksesta. Turvaluokiteltu materiaali jaetaan laadinnan yhteydessä tehdyn jakelulistan mukaan ja materiaalista on käytävä ilmi kenelle sitä saa jakaa. Turvaluokitellun materiaalin luovutus ja vastaanotto on dokumentoitava.

11.10 Tietoaineiston hävittäminen

Tarpeettoman tietoaineiston hävittäminen tulee tapahtua suunnitelmallisesti. Hävitettävän materiaalin valinta ja hävittämisaikataulu tulee määritellä viraston prosesseissa. Julkisen materiaalin hävitys tulee olla kustannustehokasta. Salassa pidettävän materiaalin hävityksen tulee olla riittävän turvallista; käytettävät menetelmät riippuvat turvaluokituksesta, hävitettävästä materiaalista ja tietoaineiston olomuodosta.

Salassa pidettävä materiaali on erotettava muusta hävitettävästä materiaalista ja hävittämisen saavat tehdä vain siihen oikeutetut. Hävittämistä on valvottava ja korkeimpien turvaluokkien materiaalin hävityksestä on pidettävä kirjaa.

Salassa pidettävä paperimateriaali tulee silputa. Silppukoko on riippuvainen turvaluokituksesta.

Mikrofilmit tulee silputa, polttaa ongelmajätelaitoksessa tai niistä tulee poistaa hopea erikoisliikkeessä. Tarkempi menettely on riippuvainen hävitettävän tiedon turvaluokituksesta.

Sähköiset ja magneettiset tietovälineet joko tyhjennetään päällekirjoituksella tai tuhotaan fyysisesti. Tarkempi menettely on riippuvainen hävitettävän tiedon turvaluokituksesta.

Optiset tietovälineet hävitetään rikkomalla.

11.11 Yksityisyyden suoja

Henkilötietolaki (523/1999) säätää henkilörekisterien ja henkilötietojen käsittelystä. Rekisterinpitäjän tulee laatia rekisteriseloste sekä noudattaa huolellisuutta käsittelyssä. Arkaluonteisille tiedoille on käsittelykielto. Henkilötunnusten käsittelyä rajoitetaan. Henkilöllä on pääsääntöisesti tarkastusoikeus omiin tietoihinsa. Rekisteritietojen siirto on rajoitettava vain välttämättömään.

11.12 Varautuminen poikkeusoloihin

Virastojen on määriteltävä pokkeusoloja varten minimitietovaatimukset. Tiedot on priorisoitava, jotta voidaan hallitusti säilyttää tärkeimpien tietojen saatavuus viimeiseen asti resurssien vähentyessä.

11.13 Järjestelmäluokkien erityispiirteet

11.13.1 Eheys ja luottamuksellisuus tärkeitä

Tietojenkäsittelyteknisesti luottamuksellisuus voidaan turvata käyttämällä jonkin formaalin luottamuksellisuusmallin toteuttavaa tietojärjestelmää. Tunnetuin luottamuksellisuusmalli on Bell-LaPadula-malli. Vastaavasti on olemassa eheysmalleja, joita toteuttavat järjestelmät turvaavat tiedon eheyden. Eheysmalleja ovat mm. Biba ja Clark-Wilson.

Hajasäteily on riski, joka tulee ottaa huomioon, kun halutaan turvata tiedon luottamuksellisuus korkeimmalla mahdollisella tasolla. Pääsääntöisesti hajasäteily yhdistetään näyttölaitteisiin mutta eri tasoista hajasäteilyä lähtee useista muistakin laitteista. Hajasäteily voidaan lukea melkoisen kaukaa. Suojaamattoman PC-laitteen monitorin kuva on mahdollista saada katsottavaksi jopa kilometrin etäisyydeltä. Hajasäteilystä aiheutuvaa riskiä voidaan pienentää valitsemalla vähän säteileviä laitteita ja käyttämällä rakennusmateriaaleja, jotka eivät läpäise (juurikaan) sähkömagneettista säteilyä.

12 KÄYTTÖTURVALLISUUS

Tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvät keinot tietoturvallisuuden parantamiseksi . (VAHTI 4/2004: Valtionhallinnon tietoturvakäsitteistö)

Lähtötaso	
Vaatimus	Kuvaus
Dokumentoidut käytettävyysvaatimukset	Käytettävyysvaatimukset ovat selkeitä, yksikäsitteisiä ja koko järjestelmän kattavia. Dokumentti on perusta käytettävyysratkaisun toteutukselle ja mittaamiselle.
Jatkuvuus- ja toipumissuunnitelmat	Häiriö- ja poikkeustilanteita varten on selkeät vastuut, suunnitelmat ja toimintaohjeet. Suunnitelmien toimivuutta testataan säännöllisillä käytännön harjoituksilla.
Valmiussuunnitelmat	Poikkeusoloihin on varauduttu etukäteen laatimalla valmiussuunnitelma. Valmiussuunnitelman toimivuus on testattu käytännössä.
Palvelutasosopimukset	Sopimuksissa on selkeät pykälät palvelutasovaatimuksista. Palvelutaso on määritelty selkeästi ja mitattavasti. Palvelutason toteutumista seurataan ja sopimuksessa on huomioitu riittävät sanktiot.

Huoltosopimukset	Huoltosopimusten vasteajoista, varaosien saatavuudesta ja huoltopalvelun henkilöresursseista on sovittu sekä häiriötilanteet että poikkeusolot huomioiden. Huoltotarpeet on huomioitu jatkuvuus-, toipumis- ja valmiussuunnitelmissa.
Käyttäjien ja pääsyoikeuksien todentaminen	Käyttäjien todentaminen sekä pääsyoikeuksien varmistaminen tehdään luotettavasti ja turvallisesti.
Käyttäjätietojen hallinta	Käyttäjätietojen koko elinkaari hallitaan huolellisesti: käyttäjätietojen luonti, käyttöoikeuksien antaminen, käyttöoikeuksien muuttaminen, väliaikaiset käyttöoikeudet, käyttöoikeuksien väliaikainen ja lopullinen poisto.
Käytön valvonta	Tietojärjestelmien ja hallintajärjestelmien käyttöä valvotaan. Järjestelmät on suunniteltu siten, että valvonta ja auditointi on mahdollista ja luotettavaa.
Istuntojen aikakatkaisu	Käyttäjien avaamat istunnot tietojärjestelmiin katkaistaan automaattisesti tietyn ajan kuluttua. Aika on määriteltävissä käyttötapauskohtaisesti ja ominaisuutta vaaditaan sovellustoimittajilta.
Kriittisten tehtävien eriyttäminen ja kierrättäminen	Tehtävien eriyttämisellä ja kierrättämisellä on varmistettu, ettei tietojärjestelmän hallinta ja valvonta ole samoissa käsissä eikä liian pienellä joukolla ole koko järjestelmä totaalisessa hallinnassaan.
Etäkäyttöpolitiikka	Organisaation oman verkon ulkopuolelta tapahtuva järjestelmien käyttö on huolellisesti suunniteltu, ohjeistettu ja suojattu. Erityistä huomiota on kiinnitetty etäkäyttölaitteen ja sen käyttöympäristön turvallisuuteen.
Tietojärjestelmän tilan valvonta	Tietojärjestelmän tilaa valvotaan suunnitelmallisesti ja jatkuvasti. Mahdolliset toiminnalliset ongelmat pyritään havaitsemaan ja ennakoimaan mahdollisemman aikaisessa vaiheessa.

Väärinkäytösten havaitseminen ja hallintamenettelyt	Tietojärjestelmän käyttöä ja tilaa seurataan väärinkäytösten, rikkomusten ja vahinkojen varalta. Toimenpiteet havaintojen varalta on suunniteltu ja dokumentoitu etukäteen. Henkilökunta on tietoinen rikkomusten seuraamuskäsittelystä.
Eriytetyt kehitys-, testaus - ja tuotantoympäristöt	Tuotantoympäristö on eristetty kehitys- ja testausympäristöstä myös henkilöresurssien osalta. Testausympäristö on identtinen tuotantoympäristön kanssa, jotta toimivuus voidaan varmistaa ennen käyttöönottoa. Kehitys-testaus-tuotanto-elinkaari on dokumentoitu ja sen noudattamista vaaditaan myös alihankkijoilta ja toimittajilta.
Haittaohjelmistoilta suojautuminen	Haittaohjelmilta suojautumiseksi on olemassa mm. hyvä tietoturva-arkkitehtuuri, suojausohjelmistot, sujuvat päivitysrutiinit, rajatut järjestelmien ja palvelujen käyttöoikeudet, haittaohjelmatilanteen jatkuva seuraaminen ja yhteistyötä muiden virastojen ja organisaatioiden kanssa.
Palvelutoimittajien luotettavuus ja niiden henkilöstön henkilöstöturvallisuus	Keskeisten tietojärjestelmien kanssa tekemisiin joutuvien palvelutoimittajien sekä palvelutoimittajan henkilöiden taustatiedot on tarkistettu ja osaamistaso varmistettu.
Dokumenttien ja ohjeiden säilytys sekä saatavuus	Tietojärjestelmään liittyvä dokumentaatio on henkilökunnan ja palvelutoimittajien saatavilla kunkin tarpeen ja dokumentin luottamuksellisuuden mukaisesti. Dokumentaatio pidetään ajan tasalla ja arkistoidaan. Versiohistoria säilytetään. Tietojärjestelmiin liittyvästä dokumentaatiosta on tehty oma ohjeensa mallidokumentteineen.
Testauksen hallinta	Testauksessa huomioidaan kokonaisuuden toimivuus, vaikka varsinaisen testin kohteena olisikin yksittäinen komponentti tai toiminnallisuus.

Perusohjeistus
VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi
VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003: Turvallinen etäkäyttö turvattomista verkoista
VAHTI 7/2001: Toimet tietoturvaloukkaustilanteessa
VAHTI 1/2001: Valtion viranomaisen tietoturvallisuustyön yleisohje
VAHTI 2/1999: Valtionhallinnon tietohallintotoimintojen ulkoistamisen tietoturvasuositus
PTS Tietojärjestelmäjaoston ohje 1/2002: Tietotekniikan turvallisuus ja toiminnan varmistaminen

Standardit
BS7799

12.1 Ulkoistaminen ja sopimukset

Toimintojen ulkoistaminen aiheuttaa erityishaasteita palvelujen toimivuudelle ja niiden palvelutasolle sekä ulkoistettujen osien käyttöturvallisuudelle. Ulkoistaminen vaatii virastolta erityisosaamista ja strategian suunnittelua. Ulkoistamiseen on otettava kantaa viraston tietoturvastrategiassa ja -politiikassa sekä riskianalyysissä. Ulkoistamista pohdittaessa on hyvä miettiä erilaisia skenaarioita riskianalyysin kautta

Oleellista ulkoistamisessa on oman toimintaympäristön ja ulkoistettavan toiminnon täydellinen ymmärtäminen. Tällöin palveluntarjoajalle osataan esittää riittävät vaatimukset ostettavasta palvelusta, vasteajoista, tarvittavista resursseista ja vastuunjaosta. On huomattava, että keskeisten järjestelmien osalta tietoturva- ja käytettävyysvaatimukset ovat todennäköisesti kovempia kuin mitä palveluntarjoaja normaalisti tarjoaa. Neuvottelut todennäköisesti kestävät normaalia kauemmin.

Palveluntarjoajalta edellytetään:

- Sitoutumista viraston tietoturvavaatimuksiin ja -politiikkaan
- Sitoutumista valtionhallinnon tietoturvaohjeistukseen
- Laatu- ja/tai tietoturvasertifiointia
- Korkeintaan vuoden vanhaa, virastolle tarjottavan palvelun tietoturvallisuuden auditointiraporttia
- Suostumusta viraston tarvittaessa järjestämään erilliseen auditointiin
- Henkilöstön taustatarkistuksia
- Selvitystä henkilöstöturvallisuudesta

- Henkilöstön tietoturvallisuuden ammattisertifikaatteja tai muuta selvitystä henkilöstön tietoturvallisuuden riittävästä osaamistasosta
- Palveluun liittyvien tietoturvaratkaisujen kuvaukset
- Kuvaus pääsyoikeuksien hallinnasta
- Kuvaus mahdollisista tietoturvallisuutta parantavista lisäpalveluista
- Palveluun liittyvät prosessikuvaukset
- Palveluun liittyvät jatkuvuus- ja toipumissuunnitelmat viimeisimpine testiraportteineen
- Sitoutumista jatkuvuus-, toipumis- ja valmiussuunnitelmien kehittämiseen ja testaamiseen yhdessä viraston kanssa
- Nimetyt yhteyshenkilöt ja kuvatut yhteyskäytännöt
- Kuvaus palvelun toimivuuden seurantamenetelmistä ja -ryhmistä
- Kuvaus ongelmien käsittely- ja eskalointiprosessista
- Kuvausta palvelun siirtämisestä kolmannelle osapuolelle tai takaisin virastolle.

Viraston on huolehdittava siitä, että tietämys ulkoistetusta toiminnosta säilyy riittävänä siten, että tietoturvallisuus ei muilta osin vaarannu, ja että ulkoistettu toiminto on mahdollista tarpeen vaatiessa ottaa takaisin omaan haltuun.

Viraston vastuulla on huolehtia palvelukokonaisuuden hallinnasta ja toimittajien koordinoinnista. Tietoturvallisuuden kokonaisvastuuta ei voi ulkoistaa, vaikka toimintoja ja niihin liittyvien osien tietoturvavastuita voidaankin. Viraston on säännöllisesti ja kattavasti arvioitava kumppaneiden tietoturvakäytäntöjä viraston omien tietoturvavaatimusten kannalta.

12.2 Etäkäyttö, etätyö ja etähallinta

Etäyhteydet on normaalistikin suunniteltava turvallisiksi huomioiden erityisesti etäyhteyteen käytettävän laitteen suojaukset, etäyhteyden avaamiseen vaadittava käyttäjän todennusmekanismi ja tietoliikenteen salaus. Etäyhteydet myönnetään suunnitellun lupamenettelyn kautta ja etäyhteyksien hallinnointiin ja käytön seurantaan on oltava dokumentoitu prosessi.

Keskeisten järjestelmien etäkäyttöön ja etähallintaan on suhtauduttava erittäin kriittisesti ja näiden osalta käytössä on tiukennettu käyttöpolitiikka. Pääsääntöisesti keskeisiin järjestelmiin ei myönnetä etäkäyttöoikeuksia.

Mikäli jokin erityistapaus ehdottomasti vaatii etäyhteyttä keskeisiin järjestelmiin joko käyttöä tai hallintaa varten, tulee noudattaa seuraavia periaatteita:

- Etätyökone on dedikoitava vain tähän käyttötarkoitukseen
- Etätyökoneen ja sen käyttöympäristön täytyy vastata varsinaisen kohdejärjestelmän ja sen ympäristön turvatasoa

- Etäyhteyden muodostamiseen vaaditaan vahva käyttäjätodennus, johon tarvitaan salasanan tai PIN-koodin lisäksi fyysinen elementti, kuten toimikortti tai kertakäyttösalasanoja generoiva laite
- Etäyhteyden tietoliikenteen täytyy olla vahvasti salattua
- Etäyhteyksistä täytyy jäädä kattava audit-loki.

Etähallintamahdollisuus on normaalia tietojärjestelmän etäkäyttöä kriittisempi toiminto, siksi etähallintaan käytettävät erityisohjelmistot on valittava erityisen huolellisesti ja vaadittava toimittajalta sopivuuden osoittamista. Oleellisia toiminnallisuuksia ovat:
- Vahvan käyttäjätodennuksen käyttömahdollisuus
- Tietoliikenteen vahva salaus
- Kattava audit-loki
- Hallintaoikeuksien rajoittaminen vain välttämättömään.

12.3 Prosessien hallinta

Tietojärjestelmien käytettävyyteen vaikuttavat oleellisesti operointi- ja hallintarutiinit mukaan lukien häiriö- ja poikkeustilanteiden hallinta. Tietojärjestelmien kaikki normaalit operointi- ja hallintatoimet on ohjeistettava:
- Operointi- ja hallintavastuu on selkeästi ja dokumentoidusti osoitettava ja rajoitettava sopiville henkilöille.
- Operointi- ja hallintaoikeuksien myöntöprosessi on erotettava normaalista käyttöoikeuksien myöntöprosessista.
- Operointi- ja hallintaoikeuksia on rajattava henkilöiden toimenkuvan mukaan.
- Kriittisimmissä operaatioissa on vaadittava kahden tai useamman henkilön aktiivinen osallistuminen ja käyttöoikeudet.
- Myönnetyistä oikeuksista on oltava ajantasainen kirjanpito ja sen valvonta.
- Operointi- ja hallinnolliset toimet on erotettava toisistaan ja tarkastus- ja auditointitoimista.
- Tietojärjestelmien operoinnista ja hallinnasta on jäätävä selkeä lokitieto, jonka pohjalta tehdyt toimenpiteet voidaan jäljittää.
- Tehdyt operointi- ja hallintatoimenpiteet on kirjattava: päivämäärä, aloitusaika, lopetusaika, tekijä(t), toimenpiteet, syy ja kuittaus.

Vakavissa häiriö- ja poikkeustilanteissa ei välttämättä voida toimia normaalirutiineiden mukaan. Häiriö- ja poikkeustilanteisiin tulee kuitenkin varautua ja valmistautua toimimaan hallitusti.

Häiriö- ja poikkeustilanteisiin varautumisessa huolella tehty ja testattu tietojärjestelmän toipumissuunnitelma on tietysti avainasemassa. Erityisesti on syytä huomioida:

- Ennalta määritellyt vastuut
- Eskalointiprosessi paitsi omassa organisaatiossa myös palveluntarjoajille ja sidosryhmille
- Palveluntarjoajien tukiprosessien toiminta
- Normaalista poikkeavien käyttöoikeuksien hallittu saantimahdollisuus
- Kriteerit tietojärjestelmän pysäyttämiselle tai eristämiselle. On huomioitava myös se mahdollisuus, että muiden järjestelmien häiriöt vaativat keskeisen tietojärjestelmän eristämisen.

Havaitut tietoturvaloukkaukset vaativat vielä oman erityisprosessinsa. Viraston on muodostettava sisäinen CERT-ryhmä, jonka vastuulle tietojärjestelmä ja sen suojaaminen siirtyy vakavan tietoturvaloukkauksen tai -riskin havaitsemisen jälkeen. Toimintaohjeet ja valtuudet on selkeästi dokumentoitava ja tiedotettava, samoin kriteerit erityistilanteen alkamiseen ja päättymiseen.

12.4 Muutosten hallinta

Muutokset tietojärjestelmässä, henkilöstön vaihtuminen, vastuiden muutokset, ulkoistaminen, jne. vaativat analyysin tietojärjestelmän uudesta riskitilanteesta. Toimintaympäristön muutokset todennäköisesti vaikuttavat riskeihin ja suojautumiskeinoihin. Muutoksiin varaudutaan suunnitelmallisuudella ja kattavalla dokumentaatiolla.

12.4.1 Päivitykset

Isot päivitysoperaatiot, kuten sovelluksen, käyttöjärjestelmän, tietokannan, välitason ohjelmistojen, tms. versiovaihdokset tehdään varmistamalla toimivuus ensin testiympäristössä. Normaalipäivitykset voidaan projektoida ja suunnitella tapauskohtaisesti sekä aikatauluttaa ja tiedottaa hyvissä ajoin etukäteen. Suunnitelman tulee sisältää testaussuunnitelma ja hyväksymiskriteerit.

Versiovaihdoksissa on varmistettava tietojärjestelmän koko tietojenkäsittelyketjun toimivuus. Yhden komponentin muutos voi aiheuttaa muutostarpeita yllättävissäkin kohteissa. Käyttöönottovaihe on suunniteltava siten, että nopea palaaminen vanhaan versioon on mahdollista määrätyn ajan puitteissa.

Erityisesti on huomioitava uuden version muutokset tietoturvaominaisuuksiin ja niiden vaikutukset kokonaisuuteen.

12.4.2 Korjauspäivitykset

Korjauspäivityksiin tulee yleensä suhtautua kuten versiovaihdoksiin ja siksi toimintatapa on sama kuin edellä.

Korjauspäivitysten asennuksiin ja hallintaan tulee ottaa käyttöön työkalu, joka mahdollistaa asennukset, automatisoinnin, asennusten onnistumisen seurannan, asennuksen peruuttamisen ja raportoinnin. Uudessa uhkatilanteessa on tärkeää saada nopeasti selville tietojärjestelmän tila.

12.4.3 Tietoturvakorjaukset

Tietoturvakorjaukset ovat korjauspäivitysten erityistapaus. Tietoturvakorjaukset voidaan pahimmassa tapauksessa joutua asentamaan hyvinkin kiireellisellä aikataululla ilman perusteellista testausta. Tietoturvakorjausten kiireellisestä asennuksesta päättää viraston CERT-ryhmä, joka arvioi tilanteen, riskit ja mahdolliset toimenpiteet.

Tietoturvakorjaustenkin toimivuus on pyrittävä ensin todentamaan testiympäristössä. Testien laajuudesta päättää viraston CERT-ryhmä. Mikäli CERT-ryhmä ei pidä tietoturvakorjausta kiireellisenä, se asennetaan, kuten normaalit korjauspäivitykset.

12.4.4 Järjestelmäintegroinnit

Järjestelmäintegroinnit suunnitellaan ja projektoidaan erillisenä kehityshankkeena ja kyseessä on uuden sovelluksen tai toiminnallisuuden käyttöönotto. Oleellista on huomioida muuttuva käyttöympäristö ja päivittää tietojärjestelmäkokonaisuuden riskiarvio uutta tilannetta vastaavaksi ja huomioida integroinnin vaikutukset kokonaistietoturvaan.

Järjestelmäintegrointi voi aiheuttaa yllättäviä muutoksia tai tietoturvatarpeita varsinaisen integrointityön ulkopuolella muilla osa-alueilla.

12.4.5 Toimittajavaihdokset

Uuden sovelluksen, toimittajan tai palvelutarjoajan mukaan tuominen keskeisen tietojärjestelmän käytön piiriin vaatii aina huolellista suunnittelua ja aikaa. Yhteensopivuus vanhan tuotteen tai palvelun kanssa on varmistettava huolellisesti ja arvioitava uuden tuotteen tai palvelun riskivaikutukset. Tuote- ja toimittajavaihdoksista aiheutuu paljon dokumentointityötä ja koulutustarpeita.

12.5 Varautuminen poikkeusoloihin

Poikkeusoloihin varaudutaan etukäteen laatimalla valmiussuunnitelma, jonka toimivuutta säännöllisesti testataan. Poikkeusoloissa on varauduttava rajallisiin resursseihin ja toi-

minnan siirtämiseen varakeskukseen. Ihmishenkien pelastaminen on tärkein tehtävä, joten henkilökunnan evakuointi vaaran uhatessa on suunniteltava ja säännöllisesti harjoiteltava – samoin turvallinen siirtyminen varakeskukseen.

Varakeskuksen toimivuutta tilojen, laitteiden, verkkoyhteyksien, sovellusten ja tietojen osalta on testattava säännöllisesti. Normaali varaosahuolto katkeaa pahimmassa tapauksessa kokonaan viikossa tai kahdessa, joten omassa varastossa on oltava riittävä määrä tärkeimpiä varaosia ja varalaitteita.

Valmiussuunnittelussa on huomioitava tietojärjestelmän toimivuus kokonaisuutena ja tuotantotietojen turvallinen siirto varalaitteisiin tarvittaessa.

12.6 Järjestelmäluokkien erityispiirteet

12.6.1 Eheys ja käytettävyys tärkeitä

Käytettävyyden ollessa luottamuksellisuutta tärkeämpää, voidaan toipumissuunnitelmissa ja päivitysohjeissa korostaa nopeaa toimintaa.

Etähallinta saattaa olla mahdollista.

12.6.2 Eheys ja luottamuksellisuus tärkeitä

Luottamuksellisuuden säilyminen häiriö- ja poikkeustilanteissa vaatii erityisen hyvin suunniteltua käyttöoikeuksien hallintaa ja eriyttämistä.

Etäkäyttö ja -hallinta kiellettyä.

13 TIETOTURVALLISUUDEN ARVIOINTI

VAHTI-ohje 3/2003, Tietoturvallisuuden hallintajärjestelmän arviointisuositus, antaa hyvät perustiedot arviointiprosessista.

13.1 Itsearviointi

Keskeisten tietojärjestelmien tietoturvallisuuden itsearviointi on hyvä lähtökohta tietoturvatason mittaamiselle. Säännöllisillä, suunnitelluilla itsearvioinneilla voidaan seurata organisaation tietoturvallisuuden kehitystä ja tehtyjen tietoturvatoimenpiteiden vaikutusta. Itsearvointia voidaan tehdä myös jatkuvasti henkilötasolla.

Virastojen yhteistyö mahdollistaa vertaiskehittämisen ja oman tilanteen mittaamisen muihin virastoihin verrattuna.

13.2 Ulkoinen arviointi

Säännöllinen ulkoinen arviointi antaa uutta näkökulmaa organisaation tilanteeseen. Ulkoinen arviointitaho saattaa löytää organisaatiosta tietoturvallisuutta heikentäviä toimintatapoja ja ratkaisuja, joita itsearvioinneissa ei ole huomattu esim. valittujen mittareiden tai tahattoman tuloshakuisuuden takia.

Ulkoisissa arvioinneissa viraston on itse selkeästi rajattava mitattava kokonaisuus ja määriteltävä mittauksen tavoitteet.

13.3 Sisäinen tarkastus

Sisäisellä tarkastuksella on tärkeä rooli viraston toiminnan laadukkuuden ja turvallisuuden sekä sääntöjen, ohjeiden ja lakien noudattamisen tarkastamisessa. Sisäinen tarkastus

valvoo yleensä asioita tietoturvallisuutta laajemmasta näkökulmasta ja näin saatetaan löytää yllättäviäkin tietoturvanäkökohtia.

13.4 Ulkoinen auditointi

Auditointi eli tarkastaminen eroaa arvioinnista siten, että auditoinnilla valvotaan annettujen ohjeiden ja sääntöjen toteutumista, kun taas arvioinnilla halutaan mitata kohteen tietoturvallisuuden tasoa ja etsitään mahdollisia parannuskohteita.

Ulkoisilla auditoinneilla voidaan varmistaa viraston tietoturvapolitiikan ja -ohjeiden noudattaminen ja halutun tietoturvatason toteutuminen.

Auditoinnissa löydetyt puutteet on korjattava mahdollisimman pian.

13.5 Mittaaminen

Tietoturvallisuuden tilaa ja kehitystä mitattaessa haasteena on mittareiden ja mittaustapojen valinta. Arviointi on yleensä subjektiivista, arvioijan kokemuksesta ja tiedosta riippuvaa, mutta tarkkaa seurantaa varten tarvitaan mittaamista.

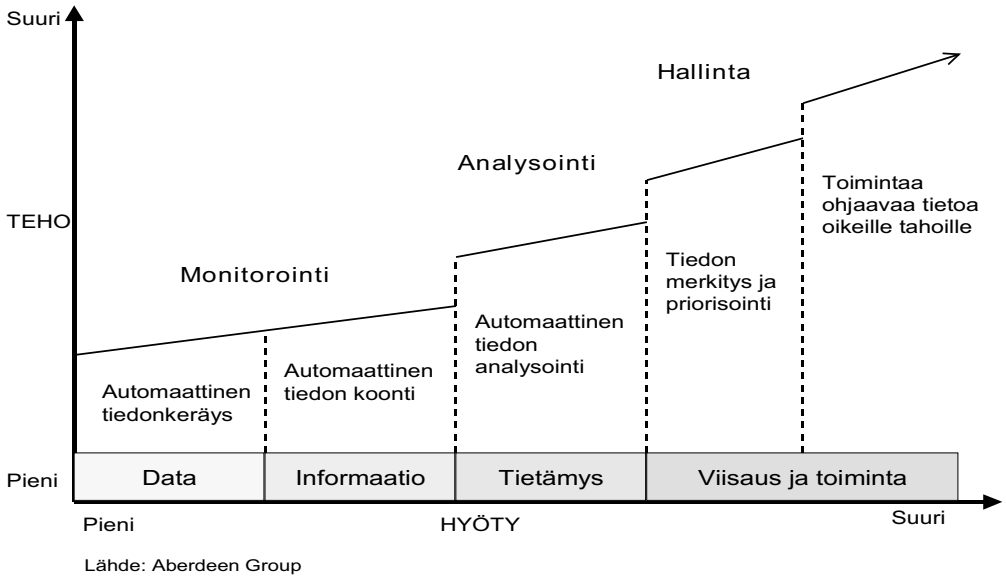
Mittaamisen on oltava jatkuvaa, toistettavaa, nopeaa, ennustettavien virhemarginaalien sisällä pysyvää ja tavoitteellista. Tulosten on oltava analysoitavissa ja verrattavissa aiempiin mittaustuloksiin. Erilliset mittaustapahtumat eivät saa olla toisistaan riippuvaisia. Mittaustuloksista on pystyttävä päättelemään tarvittavat toimenpiteet.

Mittaustapahtuman kulku:

- määritetään mittaamisen tavoitteet ja kohteet
- määritetään mittarit
- suoritetaan mittaus
- arvioidaan mittaustulosten luotettavuus ja hyöty
- tehdään johtopäätökset ja suoritetaan korjaavat toimenpiteet
- tehdään uudelleenmittaus toimenpiteiden onnistumisen varmistamiseksi
- vertaillaan mittaustuloksia ja haetaan trendejä.

Mitattavuus on huomioitava jo tietojärjestelmiä kehitettäessä tai hankittaessa. Oleellista on myös suunnitella mittaustulosten raportointi. Samasta mittaustapahtumasta tarvitaan erilaisia näkymiä. Tarvitaan sekä yhteenvetoja ja trendikuvausta että yksityiskohtaisia mittaustuloksia.

Kuva 4 esittää tavoitetta muodostaa kerätyistä yksittäisistä tiedonpalasista organisaation toimintaa ohjaavaa tietoa. Tiedon hyöty ja käyttötehokkuus kasvaa sen analysoinnin ja priorisoinnin myötä.



Kuva 4: Kerätyn tiedon arvo

13.6 Valvonta

Valvonta voidaan käsittää mittaamisen osa-alueena. Teknisin keinoin voidaan valvoa viraston toimintaa esim. sovellus- tai verkkotasolla. Hallintajärjestelmien ja sovellusten tulee hälyttää väärinkäytöksistä ja ongelmatilanteista.

Keskeisen tietojärjestelmän kokonaisturvallisuuden valvonta on huomattavasti haasteellisempaa.

13.7 Yhteistyökumppaneiden arviointi

Yhteistyökumppaneita voidaan arvioida hankittujen tietoturva- ja laatusertifikaattien perusteella. Sertifikaattien lisäksi on syytä varmistaa kumppanin sertifiointia varten asettama tavoitetila. Tyypillisesti sertifioinneilla varmistetaan, että riskianalyysin kautta asetettu tavoitetila toteutuu. Kumppanin tavoitetila ei välttämättä vastaa viraston tarpeita.

Kriittisimpien tai yksittäisten toimintojen kohdalla voidaan käyttää ulkopuolista arvioijaa. Myös yrityksen tuottama dokumentaatio toiminnastaan usein antaa kuvan yrityksen sitoutumisesta tietoturvalliseen ja laadukkaaseen toimintaan.

14 LIITTEET

Liite 1: Lainsäädäntö

Laki yksityisyyden suojasta työelämässä (759/2004)
Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
Sähköisen viestinnän tietosuojalaki (516/2004)

Valtioneuvoston ohjesääntö (262/2003)
- Valtiovarainministeriön toimialaan kuuluvat valtion tietohallinnon, tietojenkäsittelyn ja tietoturvallisuuden yleiset perusteet, hallinnon sähköinen asiointi ja valtioneuvoston yhteinen tietohallinto (17§)

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
Laki sähköisistä allekirjoituksista (14/2003)
Laki turvallisuusselvityksistä (177/2002)
Valtioneuvoston päätös huoltovarmuuden tavoitteista (350/2002)

Laki valtion talousarviosta annetun lain muuttamisesta (217/2000)
- velvollisuus hoitaa sisäinen valvonta (24 §)

Suomen perustuslaki (731/1999)
- yksityiselämän suoja (10§)
- sananvapaus ja julkisuus (12§)

Henkilötietolaki (523/1999)
- tietoturvallisuus ja tietojen säilytys (7. luku)

Laki väestötietolain muuttamisesta (527/1999)

Laki viranomaisen toiminnan julkisuudesta (621/1999)
- julkisuusperiaate (1§)
- velvoite hyvään tiedonhallintatapaan (3§)
- tiedonsaanti salassa pidettävästä asiakirjasta (10§)
- viranomaisen velvollisuudet edistää tiedonsaantia ja hyvää tiedonhallintatapaa (5. luku)
- salassapitovelvoitteet (6. luku)
- salassapidosta poikkeaminen ja sen lakkaaminen (7. luku)

Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- selvitykset hyvän tiedonhallintatavan toteuttamiseksi (1 §)
- erityissuojattavan tietoaineiston luokitus (2 §)
- erityissuojattavaa tietoaineistoa koskevat yleiset tietoturvallisuustoimenpiteet (3 §)
- ohjeet, valvonta ja seuranta (4 §)
- selosteet tietojärjestelmistä (8 §)

Henkilökorttilaki (829/1999)

Arkistolaki (831/1994)
- käytettävyys ja säilyminen, tarpeettoman aineiston hävittäminen (7 §)
- turvaaminen tuhoutumiselta, vahingoittamiselta ja asiattomalta käytöltä (12 §)

Laki huoltovarmuuden turvaamisesta (1390/1992)
Laki julkisista hankinnoista (1505/1992)
Asetus valtion hankinnoista (1416/1992)

Asetus valtion talousarviosta (1243/1992) sekä sen muutokset (263/2000 ja 254/2004)
- koneellisin menetelmin pidetty kirjanpito ja sen menetelmäkuvaus (47 §)
- sisäinen valvonta (9. luku)
- taloushallinnon järjestelmien tietoturvallisuusmääräykset taloussäännössä (69b §)

Valmiuslaki (1080/1991)

Laki rikoslain muuttamisesta (769/1990)
- luvaton käyttö (28. luku 7 § - 9 §)
- vahingonteko (35. luku 1 § - 3 §)

Laki rikoslain muuttamisesta (578/1995)
- viestintäsalaisuuden loukkaus (38. luku 3 §)

- tietomurto (38. luku 8 §)
- virkasalaisuuden rikkominen (40. luku 5a §)

Laki rikoslain muuttamisesta (951/1999)
- vaaran aiheuttaminen tietojenkäsittelylle (34. luku 9a §)

Tekijänoikeuslaki (404/1961)
- tekijänoikeus suojaa tietokoneohjelmaa (1 §)

Laki Puolustustaloudellisesta suunnittelukunnasta (238/1960)

Liite 2: Ohjeet ja määräykset

- VAHTI 3/2004: Haittaohjelmilta suojautumisen yleisohje
- VAHTI 2/2004: Tietoturvallisuus ja tulosohjaus
- VAHTI 1/2004: Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006
- VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
- VAHTI 6/2003: Opas julkishallinnon tietoturvakoulutuksen järjestämisestä
- VAHTI 5/2003: Käyttäjän tietoturvaohje
- VAHTI 4/2003: Valtionhallinnon tietoturvakäsitteistö
- VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointi
- VAHTI 2/2003: Turvallisen etäkäytön arkkitehtuuri
- VAHTI 1/2003: Valtion tietohallinnon Internet-tietoturvallisuusohje
- VM 6/01/2003: Tunnistaminen valtionhallinnon verkkopalveluissa
- Arkistolaitoksen määräys ja ohje 216/40/2003: Valtionhallinnon asiakirjojen seulonta ja hävittäminen.
- Arkistolaitoksen määräys ja ohje 195/40/2003: Asiakirjojen ja tietojen rekisteröinti asiankäsittelyjärjestelmissä tai asiakirjarekistereissä.
- Arkistolaitoksen ohje 62/40/2003: Asiakirjojen suojaaminen poikkeusoloissa.
- Valtiokonttorin määräys 280/03/2003: Koneellisten tietovälineiden käyttäminen kirjanpidossa
- VAHTI 4/2002: Arkaluonteisten kansainvälisten aineistojen käsittelyohje
- VAHTI 3/2002: Etätyön tietoturvaohje
- VAHTI 1/2002: Tietoteknisten laitetilojen turvallisuussuositus
- VM ja PTS, 2002: Tietotekniikan turvallisuus ja toiminnan varmistaminen
- VAHTI 7/2001: Toimet tietoturvaloukkaustilanteissa
- VAHTI 6/2001: Tietotekniikkahankintojen tietoturvallisuustarkistuslista
- VAHTI 5/2001: Sähköpostin ja lokitietojen käsittely
- VAHTI 4/2001: Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
- VAHTI 3/2001: Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus
- VAHTI 2/2001: Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
- VAHTI 1/2001: Valtion viranomaisen tietoturvallisuustyön yleisohje
- Arkistolaitoksen määräys 284/40/2001: Asiakirjojen siirtäminen arkistolaitokseen.
- Arkistolaitoksen määräys ja ohje 126/40/2001: Sähköisten tietojärjestelmien ja aineistojen käsittely.
- Valtiokonttorin määräys 20/03/2001: Taloussääntöjen uudistaminen
- VAHTI 3/2000: Tietojärjestelmäkehityksen tietoturvallisuussuositus
- VAHTI 2/2000: Valtion tietoaineistojen käsittelyn tietoturvaohje
- VM 17.2.2000: Tietojärjestelmäselosteen laadintasuositus

- VM 19.1.2000: Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje
- Valtiokonttorin määräys 9/03/2000: Koneellisin menetelmin pidetyn kirjanpidon menetelmäkuvaus
- VAHTI 2/1999: Tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus
- VM 1/01/99: Suositus toimitilaturvallisuuden huomioonottamisesta valtionhallinnossa

Liite 3: Standardit, parhaat käytännöt

Standardi	Kuvaus
BS 7799	Kaksiosainen standardi, joka kuvaa tietoturvallisuuden hallintajärjestelmiä koskevat menettelyohjeet (1. osa) ja vaatimukset (2. osa)
ISO 17799	BS 7799 -standardin ensimmäinen osa
ISO 15408 (Common Criteria)	Standardi tietoturvallisuuden arviointia varten.
ISO 15504 (SPICE)	Standardi ohjelmistoprosessien (hankinta, tuki, kehitys jne.) arviointia varten
ISO TR 13335	Tietoturvallisuuden hallinnan ohjeistus
ISO 9001	Vaatimukset laadunhallintajärjestelmälle
ISO 90003	Opastus ISO 9001 -standardin soveltamiseksi tietokoneohjelmistoihin ja niihin liittyviin tukipalveluihin.
AS/NZS 4360	Riskinhallintaprosessin ohjeistus
SAA/SNZ HB 231	Tietoturvariskien hallinnan ohjeistus
GAO/AIMD-00-33	Tietoturvariskien arvioinnin ohjeistus
MG-2	Tietojärjestelmien turvariskien hallinnan ohjeistus
NIST Spec Pub 800-30	Tietojärjestelmien riskinhallinnan ohjeistus
BSI PD3002	BS7799-standardin mukainen opas riskien arvioinnille ja hallinnalle
ITSEC	Standardi tietoturvallisuuden arviointia varten. Vanha, korvautumassa standardilla ISO 15408.
DoD 5200.28-STD (TCSEC)	Standardi tietoturvallisuuden arviointia varten. Vanhentunut, korvattu standardilla ISO 15408.
Systems Security Engineering Capability Maturity Model (SSE-CMM)	Kuvaa organisaation hyvään tietoturvallisuuden hallintaan kuuluvat keskeiset elementit tietoturvakäytäntöjen kypsyyden arviointia kehittämistä varten.
Information Security Forum: The Standard of Good Practice for Information Security	Liiketoimintalähtöinen ohjeistus tietoturvallisuuden hyvistä käytännöistä

ITIL	Kuvaa tietotekniikkapalvelujen hallinnan parhaat käytännöt.
COBIT	Tietohallinnon, tietotekniikan ja tietojärjestelmien valvontamalli
RFC 2828	Sanasto
ISO 2382-8	Sanasto

Liite 4: Sanasto

Sanastossa esitellään ne tässä ohjeessa käytetyt termit ja käsitteet, joita ei ole määritelty VAHTI 4/2003 Valtionhallinnon tietoturvakäsitteistö -suosituksessa.

Käsite / termi	Selite
Bell-LaPadula, BLP	Formaali luottamuksellisuusmalli, joka rajaa tiedon lukemisen ja kirjoittamisen siten, että korkeamman luottamuksellisuustason tietoa ei voida siirtää alemmalle luottamuksellisuustasolle.
Biba	Formaali eheysmalli, joka rajaa tiedon lukemisen ja kirjoittamisen siten, että heikomman eheystason tieto ei pääse saastuttamaan korkeamman eheystason tietoa. Biba-malli on analoginen BLP-mallin kanssa.
Clark & Wilson	Kaupallinen eheysmalli, joka perustuu hyvin määriteltyihin tiedonkäsittelyprosesseihin, joilla erityisesti tavoitellaan toimintojen eriyttämistä.
Kulkuannostelija	Ovi- tai kulkuporttijärjestelmä, jolla säädellään kerralla sisään päästettävien henkilöiden määrä.
Piilokanava	Tietoliikennekanava, joka mahdollistaa tiedon siirron vastoin järjestelmän turvapolitiikkaa. (covert channel)
Osoitteellinen paloilmoitusjärjestelmä	Antaa tarkan palopaikan sijainnin, jotta palokunta löytää mahdollisimman nopeasti palopesäkkeen.
S3-suojausluokka	Väestönsuojien suojatilavaatimusten luokittelu.
VAP-varaus	Henkilöstövaraus yhteiskunnan ja talouselämän kriisijan toimintoja varten.

Liite 5: Kotimaiset viitteet

- Suomen turvallisuus- ja puolustuspolitiikka, Valtioneuvoston selonteko VNS 6/2004
- Taloushallinnon tietojärjestelmien ohjesääntö, Verohallinto, 2003
- Tietoja valtion tietohallinnosta ja tietotekniikasta 2002, VM, 2002
- Tiedonkäsittelyalan tarvikkeiden huoltovarmuusselvitys, PTS, 2003
- Uhkakuvat, Huoltovarmuuskeskus, 2004
- Uhkakuvat ja varautuminen, PM, 2003
- Varaosahuoltoa ja sovellusten siirrettävyyttä käsittelevä turvaluokiteltu julkaisu, Huoltovarmuuskeskus, 2004
- Varautuminen yhteiskunnan häiriöihin ja poikkeusoloihin, Puolustusneuvosto, 1999
- Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, Valtioneuvoston periaatepäätös 27.11.2003

Liite 6: Ulkomaiset viitteet

- APEC Information Systems Security Standards Handbook, APEC-TEL, Final Draft
- Basnivå för IT-säkerhet (BITS), Krisberedskapmyndigheten, 2003
- Försvarsmaktens informationstekniska katalog, Försvarsmakten, 2001
- Improving Security Across the Software Development Lifecycle, Task Force Report, 2004
- IT-säkerheten inom den civila delen av totalförsvaret, Överstyrelsen för civil beredskap, 2000
- Ledningssystem för informationssäkerhet vid 24-timmarsmyndigheter, Statskontoret, 2003
- National Plan for Information Systems Protection, The White House, 2000
- National Plan for Information Systems Protection, U.S. Nuclear Regulatory Comission, 2000
- National Strategy for Critical Infrastructure and Cyber Space Security, I&C Sector National Strategy Input, 2002
- Operational Security Standard – Readiness Levels for Federal Government Facilities, Treasury Board of Canada Secretariat, 2002
- Recommended Security Controls for Federal Information Systems, NIST SP 800 53, 2003
- Sammanhållen strategi för samhällets IT-säkerhet, Statskontoret, 2004
- The National Strategy to Secure Cyber Space, The White House, 2003
- The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, The White House, 2003
- Vulnerability and Security in a new Era – a Summary, The Swedish Commission of Vulnerability and Security, 2001

Liite 7: Valtion ja virastojen yhteiset tietoturvaorganisaatiot

Virasto	Organisaatio
Valtiovarainministeriö	Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI)
Viestintävirasto	Tietoturvaloukkausten havainnointi ja ratkaisu (CERT-FI)

Liite 8: Liitteet

Liite 1: Toiminta haittaohjelmatapauksissa

Liite 2: Selaimen asetukset

Liite 3: Käyttäjän pikaopas

Liite 4: Sisäisten ja ulkoisten velvoitteiden luettelo (lakiliite)

Liite 5: VM:n tietoturvaohjeita ja -julkaisuja: (www.vm.fi/vahti)

VAHTI

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

5/2004

VALTIONHALLINNON KESKEISTEN TIETOJÄRJESTELMIEN TURVAAMINEN

ISBN 951-804-467-8 (nid.)
ISBN 951-804-468-6 (PDF)
ISSN 1455-2566