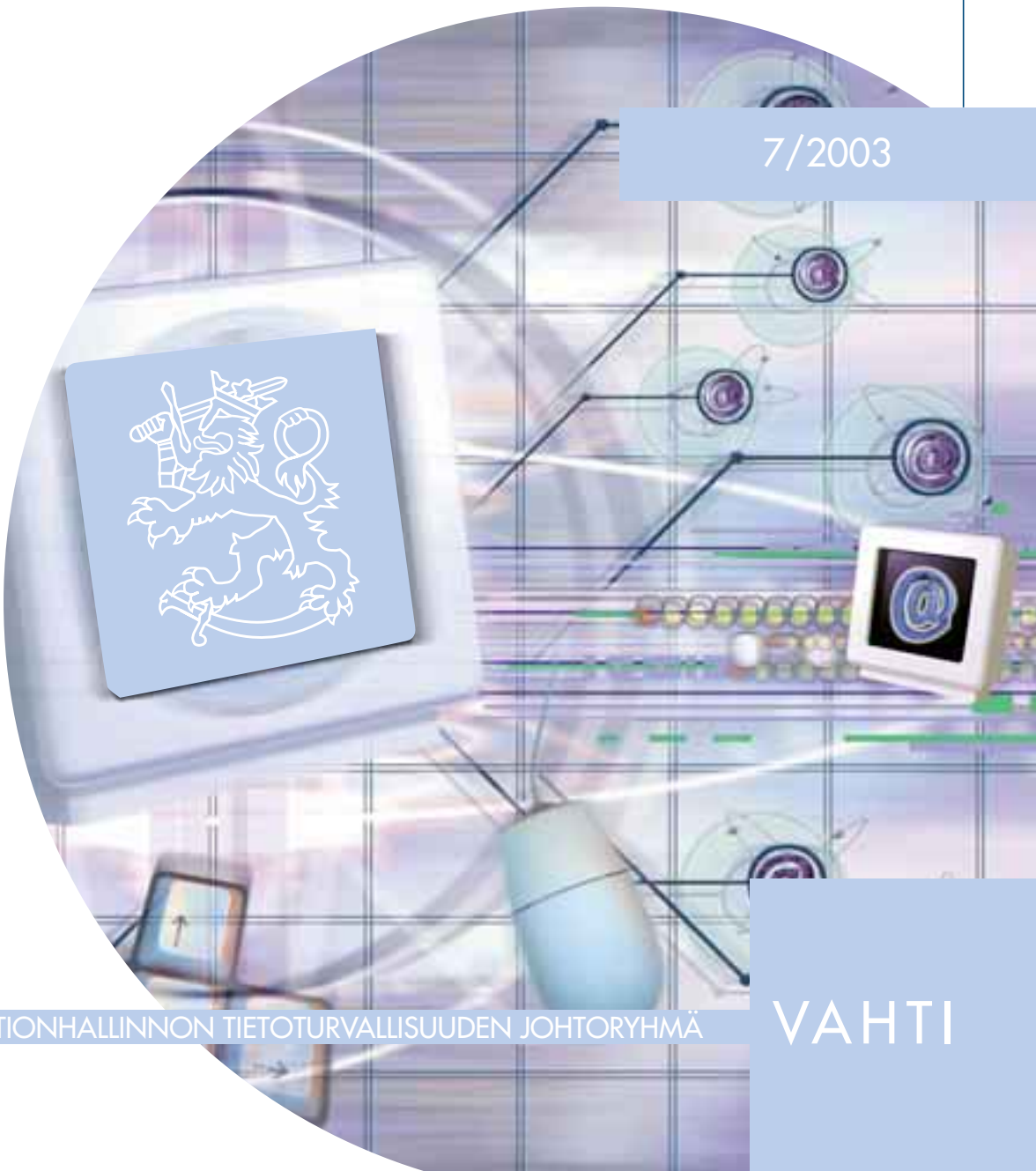
VALTIOVARAINMINISTERIÖ

OHJE RISKIEN ARVIOINNISTA TIETOTURVALLISUUDEN EDISTÄMISEKSI VALTIONHALLINNOSSA



7/2003

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

OHJE RISKIEN ARVIOINNISTA TIETOTURVALLISUUDEN EDISTÄMISEKSI VALTIONHALLINNOSSA

7/2003

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
Puh. (09) 160 33 222

Sähköposti: vahtijulkaisut@vm.fi

ISSN 1455-2566
ISBN 951-804-408-2

Edita Prima Oy
HELSINKI 2003

VALTIOVARAINMINISTERIÖ

VM 41/01/2003

OHJE
3.12.2003

Ministeriöille, virastoille ja laitoksille

OHJE RISKIEN ARVIOINNISTA TIETOTURVALLISUUDEN EDISTÄMISEKSI VALTIONHALLINNOSSA

Valtiovarainministeriö antaa oheisen tietoturvaohjeen (jäljempänä ohje), joka on laadittu valtiovarainministeriön asettaman ja johtaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimesta. Ohje täydentää laajaa olemassa olevaa valtiovarainministeriön antamaa tietoturvaohjeistoa. Ohjeen kohderyhmänä ovat erityisesti organisaation johto, tietoturva-, tietohallinto ja turvallisuusvastaavat sekä muut tietoturvariskien hallinnan kannalta keskeiset henkilöt.

Riskien arviointi on hyvin tärkeä osa organisaation riskien hallintaa ja myös keskeinen osa jatkuvaa tietoturvatyötä. Riskien arvioinnilla tarkoitetaan niitä suunnitelmallisia toimenpiteitä, joilla pyritään tunnistamaan uhkia ja haavoittuvuuksia sekä arvioimaan mahdollisesti toteutuvien uhkien seurauksia.

Valtionhallinnon organisaatioissa riskien hallintaa ja arviointia tulee hoitaa suunnitelmallisesti ja laaja-alaisesti siten, että eri toimintojen näkökulmat ja turvaamistarpeet tulevat katetuiksi. Riskien hallinnan ja arvioinnin tulee sisältää myös varautuminen vakaviin häiriötilanteisiin ja valmiuslaissa (1080/1999) määriteltyihin poikkeusoloihin.

Ohjeessa on esitetty välineitä ja keinoja, joiden avulla tietoriskejä voidaan arvioida. Ohjeessa kuvataan myös lainsäädännön riskienhallintaa koskevia velvoitteita, riskien arvioinnin merkitystä ja organisointia sekä riskienhallinnan keinoja, uhkien tunnistamista, riskien suuruuden arviointia, toimenpiteiden määrittelyä ja jatkokehitystä. Riskien arvioinnin menetelminä voidaan käyttää muun muassa ohjeen luvussa 3 kuvattuja menetelmiä sekä useiden VAHTI-ohjeiden tarkistuslistoja. Ohjeen liitteenä on myös laaja tarkistuslista tietoturvauhkien tunnistamiseksi. Erityisen tärkeätä on muun muassa uhkan todennäköisyys- ja seurausten vakavuus- analyysien pohjalta tunnistaa merkittävimmät ja kiireellisimpiä toimenpiteitä vaativat riskit.

Ohje tulee VAHTIn Internet-sivuille, jotka ovat osoitteissa *www.vm.fi/tietoturvallisuus ja www.vm.fi/vahti*. Ohjetta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi).

Lisätietoja antaa neuvotteleva virkamies Mikael Kiviniemi (etunimi.sukunimi@vm.fi).

Ministeri Ulla-Maj Wideroos

Ylijohtaja Jorma Karjalainen

Liite Ohje riskien arvioinnista tietoturvallisuden edistämiseksi valtionhallinnossa (VAHTI 7/2003)

ESIPUHE

Riippuvuus tietojärjestelmistä on tehnyt hallinnosta erittäin haavoittuvan turvallisuutta uhkaaville tekijöille. Lisäksi hallinnon ja yksityisten verkkojen yhdistäminen sekä palveluiden ulkoistaminen ovat heikentäneet virastojen mahdollisuuksia tehokkaaseen tietoturvallisuuden valvontaan.

Tietoturvallisuus ja siihen kohdistuvien riskien merkitys vaihtelee toimialoittain eri hallinnon sektoreilla. Tavallisesti ajatellaan, että tietoriskit ovat tietoihin ja niiden käyttöön kohdistuvia tapahtumien todennäköisyyksiä. Tietoriski on tilanne, jolloin tieto tai tietojärjestelmä ei ole käytettävissä, tieto on muuttunut jonkin tapahtuman kautta tai päätynyt ulkopuolisten haltuun. Tietoriskit ovat vahinkoriskejä, joiden toteutumiseen liittyy aina menetyksiä, niin taloudellisia kuin imagoon liittyviä.

Riskejä voivat aiheuttaa ihmiset, tekniset viat tai sääilmiöt, ja näihin liittyvä teko voi olla tahallinen tai tahaton. Ammattimainen hyökkäys on yhtä todennäköinen kuin tahaton virhe ja tästä syystä molempiin on varauduttava. Tietoriskiin on varauduttava tiedon luottamuksellisuuden, käytettävyyden ja eheyden turvaamiseksi.

Tietoriskien hallinta on normaalia päätöksentekotoimintaa josta organisaation johto vastaa. Tavoitteena on taata toiminnan jatkuvuus.

Oikean tason löytäminen on tärkeää, koska tieto on yksi suojattavista kohteista ja sillä voi olla merkitystä myös muiden organisaatioiden toiminnalle verkottuvassa hallinnossa. Huolellinen tai huolimaton tapa käsitellä tietoa kuvaa organisaation kulttuuria ja tapaa toimia.

Riskikartoituksen tavoitteena on löytää uhkatekijät sekä arvioida uhkien todennäköisyys ja niiden seurausten vakavuus. Tietoriskien arvioinnissa voidaan käyttää samoja menetelmiä kuin muidenkin riskien arvioinnissa unohtamatta kuitenkaan tietoriskien erityisominaisuuksia. Tiedon käsitteellisen luonteen vuoksi riskien arvioinnille asettavat haasteita tietoverkot, tiedon säilytysmuodot ja laaja-alaisuus joka liittyy tietoturvallisuuteen. Kun riskit on arvioitu, organisaatiolla on tiedossaan tunnistetut riskit. Riskien hallintasuunnitelmalla päätetään kuinka riskeihin suhtaudutaan.

Valtionhallinnon tietoturvallisuuden johtoryhmän näkemyksen mukaan valtionhallinnon tietoriskien arviointiin voidaan käyttää esimerkiksi tämän suosituksen luvussa 3.2 mainittuja menetelmiä. Lisäksi useissa VAHTI-ohjeissa on tarkistuslistoja joita voidaan hyödyntää riskien arvioinnissa.

SISÄLLYS

1 JOHDANTO 9
1.1 Tiedon ja tietojärjestelmien merkitys organisaatiolle 9
1.2 Tietoturvallisuuden johtamisen tavoitteet 10
1.3 Johdon rooli riskienhallinnassa 10
1.4 Sisäisen valvonnan määräykset ja mallit 11
1.5 Suosituksen laatiminen 11

2 LAINSÄÄDÄNNÖN RISKIENHALLINTAA KOSKEVAT VELVOITTEET 13

3 RISKIEN ARVIOINNIN MERKITYS JA ORGANISOINTI 15
3.1 Riskien arvioinnin merkitys 15
3.2 Riskien arviointi osana riskienhallintaa 16
3.3 Riskien ja arviointi ja valmiussuunnittelu 17
3.4 Riskien arvioinnin suunnittelu ja toteutus 17
3.5 Riskien arvioinnin organisointi 18
3.6 Riskien arvioinnin suhde tietoturvallisuuden hallintajärjestelmän arviointiin 19

4 RISKIENHALLINNAN KEINOT 21
4.1 Tietoturvastandardit osana riskienhallintaa 22

5 UHKIEN MÄÄRITTELY JA TUNNISTAMINEN 25
5.1 Menetelmän valinta 25
5.2 Uhkien tunnistamismenetelmiä 25
5.2.1 Potentiaalisten ongelmien analyysi 26
5.2.2 Uhkapuut 27
5.2.3 Skenaariomenetelmä 27
5.2.4 Haavoittuvuusanalyysi 27
5.2.5 Tarkistuslistat 29
5.3 Uhkien tunnistaminen 29
5.3.1 Hallinnollinen tietoturvallisuus 30
5.3.2 Henkilöstöturvallisuus 31
5.3.3 Fyysinen turvallisuus 32
5.3.4 Tietoliikenneturvallisuus 33
5.3.5 Laitteistoturvallisuus 35
5.3.6 Ohjelmistoturvallisuus 35
5.3.7 Tietoaineistoturvallisuus 37
5.3.8 Käyttöturvallisuus 39

6 RISKIEN SUURUUDEN ARVIOINTI 41
6.1 Uhkan todennäköisyyden arviointi 41
6.2 Seurausten vakavuuden arviointi 42
6.3 Riskin suuruus 43
6.4 Kvantitatiivinen ja kvalitatiivinen riskien suuruuden arviointi 44

7 TOIMENPITEIDEN MÄÄRITTELY 45

8 JATKOKEHITYS- JA SEURANTASUUNNITELMAT 45

LÄHTEET JA VIITEAINEISTOT 49

LIITTEET
Liite 1. Luettelo ohjaavasta lainsäädännöstä. 51
Liite 2. Tietoturvauhkien tunnistamisen tarkistuslistoja 55
Liite 3. Potentiaalisten ongelmien analyysi 69
Liite 4. Esimerkkejä toteutuneista riskeistä 75
Liite 5. Määritelmät 77
Liite 6. Valtiovarainministeriön ja VAHTIn tietoturvaohjeistoa 79

1 JOHDANTO

1.1. Tiedon ja tietojärjestelmien merkitys organisaatiolle

Jokaisessa organisaatiossa on sen toiminnalle kriittisiä tietoja, kuten asianhallinnan tiedot tai organisaation toimintaan liittyvät tiedot. Tieto on pääomaa, jonka suojaaminen on varmistettava. Organisaation toiminnan kannalta on tärkeää, että:

- Tiedot ovat oikein ja ajantasalla
- Tiedot ja tietojärjestelmät ovat aina oikeiden henkilöiden saatavilla
- Tiedot eivät joudu vääriin käsiin.

Valtioneuvoston tietoturvallisuutta koskevassa periaatepäätöksessä (VNp 11.11.1999) todetaan, että viranomaisilla tulee olla tietoturvallisuuden hallintaa ja ohjausta varten ajantasainen tiedonkäsittelyn turvaamissuunnitelma, vahinkojen varalta toipumissuunnitelma ja poikkeusolojen varalta tiedonkäsittelyn valmiussuunnitelma. Suunnitelmiin sisältyy organisaation tiedonkäsittelyriippuvuuden, tietotekniikan käyttöön liittyvien uhkatekijöiden ja riskien arviointi sekä niiden hallinnan edellyttämien turvaamis-, toipumis- ja varautumistoimenpiteiden määrittely ja toteuttamissuunnitelmat.

Tietoturvallisuusjärjestelyiden tavoitteena on suojata tiedon luottamuksellisuus, eheys ja käytettävyys. Tietoriskien hallinnan ensimmäinen vaihe on kartoittaa organisaation toiminnalle tärkeät tiedot ja tietojärjestelmät ja niiden merkitys toiminnan kannalta. Sen jälkeen tulee tunnistaa tietoihin liittyvät keskeiset uhkat ja arvioida niiden merkitys. Tässä ohjeessa on esitetty välineitä ja keinoja, joiden avulla tietoriskejä voidaan arvioida. Ohjeen kohderyhmänä ovat organisaation johto sekä tietohallinnon ja tietoturvallisuuden asiantuntijat.

1.2 Tietoturvallisuuden johtamisen tavoitteet

Tietoturvallisuus on osa johtamistoimintaa. Sen tavoitteet ja kehittäminen sisällytetään tulosohjaukseen. Tietoturvallisuuden ensisijaisena tavoitteena on tarjottavien palvelujen perustana olevan tietoaineiston ja käytössä olevan tietotekniikan turvallisuuden sekä toimintakyvyn ja käytettävyyden varmistaminen kaikissa oloissa.

Tietoturvallisuuden perusta on tunnistaa ja arvioida organisaation toimintaan liittyvät tietoriskit. Tämän pohjalta voidaan tehdä päätökset siitä, mitä toimenpiteitä pitää toteuttaa. **Riskejä hallittaessa lähtökohdaksi on otettava organisaation toiminnan kehittäminen, kuten esimerkiksi toimintatavat, osaaminen ja johtaminen. Sen jälkeen tulevat tekniset suojauskeinot.**

Johdolla tulee olla oikea kuva organisaation toimintaan kohdistuvista tietoriskeistä ja tietoturvallisuuden tasosta. Toimintaan ja palvelujen tietoturvallisuuteen kohdistuvien riskien arviointiin tarvitaan järjestelmällinen riskianalyysimenettely. Riskianalyysin tarkoituksena on (VAHTI 1/2001, kohta 4.3.1, s. 25):

- Selvittää toiminnan ja palvelujen tietoturvatarpeet ja vaatimukset
- Arvioida ulkoiset ja sisäiset riskit
- Selvittää säädöksistä ja määräyksistä johtuvat vaatimukset
- Arvioida toiminnan ja tietotekniikan muutoksien vaikutukset tietoturvallisuuteen
- Selvittää sidosryhmien odotukset
- Edellä mainittujen perusteella määritellä tietoturvallisuuden tarpeet, periaatteet ja toteutustapa.

Johdon tulee voida perustaa tietoturvapolitiikkaa ja -periaatteita koskevat päätökset riskianalyysin osoittamiin tarpeisiin. Samoin tietoturvallisuutta koskevat yksityiskohtaiset suunnitelmat perustuvat riskianalyysin tuloksiin.

1.3 Johdon rooli riskienhallinnassa

Tietoturvallisuus on osa organisaation johtamistoimintaa. Jokaisen organisaatiotason tehtävänä on huolehtia oman organisaationsa toiminnan ja hankkimiensa palvelujen tietoturvallisuudesta, määritellä tarvittavat periaatteet sekä laatia ja antaa tarvittavat ohjeet. Tietoturvaratkaisujen valinnassa tulee riskianalyysien perusteella ottaa huomioon ratkaisujen taloudellisuus ja tarkoituksenmukaisuus. Ylimmän johdon päätöksiä tarvitaan erityisesti silloin, kun ratkaisut on valittava taloudellisuusvaatimuksista poiketen (VAHTI 1/2001, s. 8).

Linjajohdon on tarpeellista omaksua riskienhallinnan toimintamallit ja viedä ajattelua eteenpäin kaikilla organisaatiotasoilla. Riskienhallinta ei toimi riittävän tehokkaasti, jos se jätetään vain riskienhallinnan ammattilaisten hoidettavaksi (Suominen 2003, s. 28).

1.4 Sisäisen valvonnan määräykset ja mallit

Asetus valtion talousarviosta edellyttää johdon huolehtivan siitä, että virastossa toteutetaan sen talouden ja toiminnan laajuuteen ja sisältöön sekä niihin liittyviin riskeihin nähden asianmukaiset sisäisen valvonnan menettelyt. Nämä menettelyt varmistavat talouden ja toiminnan laillisuuden ja tuloksellisuuden, varojen ja omaisuuden turvaamisen sekä johtamisen ja ulkoisen ohjauksen edellyttämät oikeat ja riittävät tiedot viraston taloudesta ja toiminnasta.

Asetus edellyttää lisäksi, että sisäisen valvonnan menettelyissä otetaan huomioon sitä koskevat yleiset standardit ja suositukset. Asetukseen perustuvassa Valtiokonttorin ohjeessa näiksi standardeiksi on mainittu COSO ja INTOSAI. Näissä standardeissa on keskeistä se, että valvontatoimet ovat riskeihin suhteutettuja. Tieto-omaisuuden turvaamisen ja tietojen oikeellisuuden valvontamenettelyiden ohjaaminen edellyttää riskien arviointia.

1.5 Suosituksen laatiminen

Suositus laadittiin valtionhallinnon tietoturvallisuuden johtoryhmän alaisuudessa ja ohjauksessa. Tehtävään nimetyn työryhmän kokoonpano oli seuraava:

Puheenjohtaja:
Seppo Sundberg, Valtiokonttori

Jäsenet:
Aaro Hallikainen, Poliisin tietohallintokeskus
Risto Heinonen, Tietosuojavaltuutetun toimisto
Aku Hilve, Helsingin poliisilaitos
Matti Huvila, Åbo Akademi
Kalevi Hyytiä, Pääesikunta
Pentti Mykkänen, Valtiontalouden tarkastusvirasto
Juhani Sillanpää, Valtiovarainministeriö
Keijo Vehmas, Verohallitus
Raija Viljanen, Huoltovarmuuskeskus

Työryhmän konsultti ja sihteeri:
Teuvo Uusitalo, VTT Tuotteet ja tuotanto

Valtionhallinnon tietoturvallisuuden johtoryhmä käsitteli ohjetta 18.9. pitämässään kokouksessa ja antoi ohjausta ohjeen jatkotyölle. Suositusta valmistellut työryhmä viimeisteli saatujen kommenttien pohjalta suosituksen yhteistyössä valtiovarainministeriön hallinnon kehittämisosaston kanssa. Suositus hyväksyttiin valtionhallinnon tietoturvallisuuden johtoryhmässä marraskuussa 2003.

2 LAINSÄÄDÄNNÖN RISKIENHALLINTAA KOSKEVAT VELVOITTEET

Useat lait, asetukset sekä määräykset ja ohjeet sisältävät viranomaisia koskevia tietoturvallisuusvelvoitteita, jotka on otettava huomioon myös arvioitaessa tietoturvariskejä. Lait on listattu liitteessä 1.

LAKI VIRANOMAISEN TOIMINNAN JULKISUUDESTA (621/1999)

Viranomaisen on hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehdittava asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä. Viranomaisen on suunniteltava ja toteutettava asiakirja- ja tietohallintonsa samoin kuin ylläpitämänsä tietojärjestelmät ja tietojenkäsittelyt niin, että asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavoin ja tietoturvallisuusjärjestelyin ottaen huomioon tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvallisuustoimenpiteistä aiheutuvat kustannukset.

ASETUS VIRANOMAISTEN TOIMINNAN JULKISUUDESTA JA HYVÄSTÄ TIEDONHALLINTATAVASTA (1030/1999)

Hyvän tiedonhallintatavan toteuttamiseksi viranomaisen on selvitettävä ja arvioitava tietojen saatavuuteen, käytettävyyteen, laatuun ja suojaan sekä tietojärjestelmien turvallisuuteen vaikuttavat uhat sekä niiden vähentämiseksi ja poistamiseksi käytettävissä olevat keinot ja niiden kustannukset sekä muut vaikutukset.

HENKILÖTIETOLAKI (523/1999)

Rekisterinpitäjän on toteutettava tarpeelliset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat

tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.

VALMIUSLAKI (1080/1991)

Valtioneuvoston, valtion hallintoviranomaisten, valtion liikelaitosten ja muiden valtion viranomaisten sekä kuntien on valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muin toimenpitein varmistettava tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa.

3 RISKIEN ARVIOINNIN MERKITYS JA ORGANISOINTI

3.1. Riskien arvioinnin merkitys

Riskienhallinnalla on selkeät päävaiheet. Ensin uhkat on tunnistettava ja niiden merkitys arvioitava. Sen jälkeen suunnitellaan riskien torjunta ja tarvittavat toimenpiteet. Kolmannessa vaiheessa suunnitellaan miten vahingon sattuessa toimitaan ja miten vahingoista toivutaan. Tämän jälkeen tilannetta seurataan. Mahdollinen toteutunut riski analysoidaan ja tapahtuneesta otetaan opiksi.

Riskien arvioinnilla tarkoitetaan niitä järjestelmällisiä toimenpiteitä, joilla pyritään tunnistamaan tietoturvallisuuden uhkia ja haavoittuvuuksia sekä arvioimaan mahdollisesti toteutuvien uhkien seurauksia. Käytettävät menetelmät ja työvälineet voivat olla samoja kuin muidenkin riskien arvioinnissa käytetään.

Riskien arvioinnissa pyritään vastaamaan seuraaviin kysymyksiin.

- Mitä kaikkea voi sattua?
- Miksi?
- Mitä siitä voi seurata?
- Miten suuri on aiheutuva riski?
- Mitkä riskit ovat suurimmat?

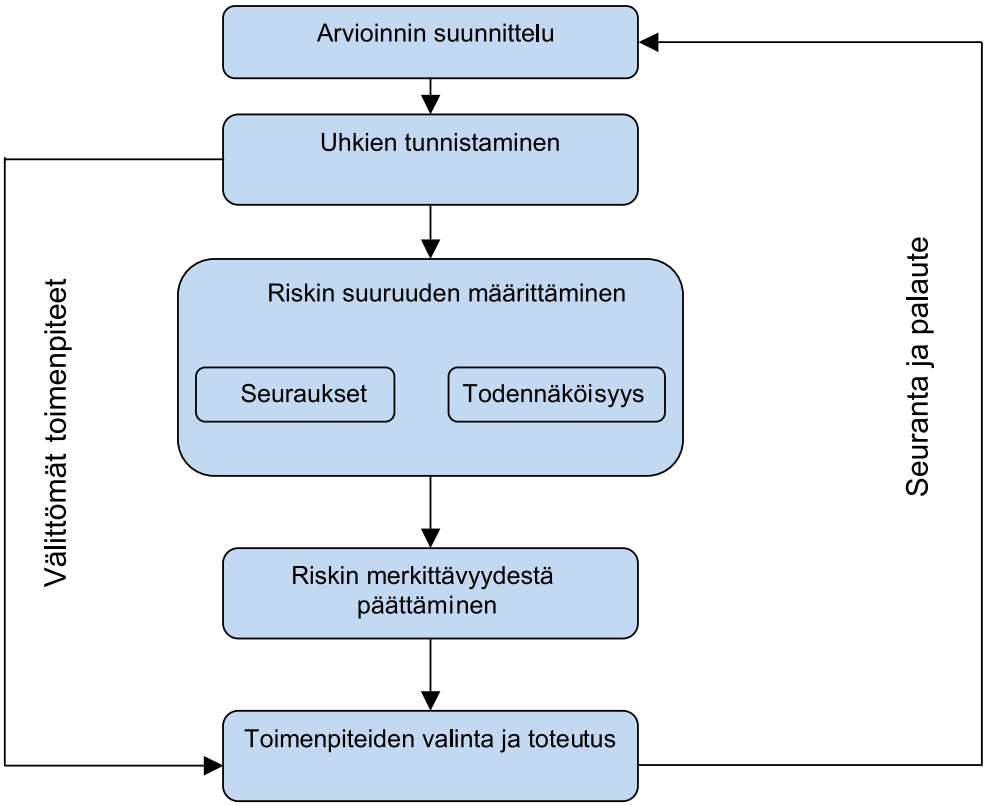
Riskien arviointiin sisältyy myös tulosten raportointi perusteluineen. Riskien arvioinnin ja hallinnan vaiheet on esitetty kuvassa 1.

3.2 Riskien arviointi osana riskienhallintaa

Kriittinen ja ennakkoluuloton asenne on hyvä uhkien tunnistamisen ja riskien arvioinnin lähtökohta. Lisäksi tarvitaan apuvälineitä, joilla varmistetaan tarkastelun kattavuus ja järjestelmällisyys. Tunnistamisen tueksi on kehitetty erilaisia menettelytapoja ja välineitä. Valtionhallinnossa on käytetty esimerkiksi Pk-yrityksen riskienhallinta -työvälinesarjaa, Secgo Manageria ja BSI-menetelmää. Liitteessä 3 on kuvattu potentiaalisten ongelmien analyysi, jota voidaan käyttää myös tietoturvariskien arvioinnissa.

Uhkien tunnistaminen voidaan aloittaa karkeilla kartoitusmenetelmillä. Niillä saadaan kokonaiskuva tilanteesta ja löydetään ne riskialueet, joita on seuraavassa vaiheessa tarkoituksenmukaista tutkia yksityiskohtaisemmilla menetelmillä. Tunnistaminen etenee tällä tavoin yleisestä yksityiskohtaisempaan. Aika ajoin on syytä arvioida kokonaistilanne uudelleen ensimmäisessä vaiheessa käytetyllä karkealla kartoitusvälineellä.

Kuva 1. Riskien arvioinnin ja hallinnan vaiheet (Murtonen 2003)



3.3 Riskien ja arviointi ja valmiussuunnittelu

Viranomaisilla on lakiin perustuva velvollisuus varautua toiminnan jatkuvuuteen myös poikkeusoloissa. Varautuminen perustuu etukäteen tehtäviin valmiussuunnitelmiin. Huoltovarmuuskeskus ja puolustustaloudellinen suunnittelukunta ovat julkaisseet valmiussuunnittelua koskevia ohjeita.

Riskien arvioinnin tulee kattaa myös varautuminen poikkeusoloihin. Tällöin pitää erityisesti kiinnittää huomiota poikkeusolojen erityisolosuhteisiin ja miettiä miten niihin on varauduttu. Poikkeusolojen riskien arvioinnissa on tärkeää ottaa huomioon tietoturvallisuus ja varautuminen informaatiouhkiin. Viime vuosina esiin nousseita uhkia ovat mm. tietokonevirukset, palvelunestohyökkäykset ja tietojärjestelmämurrot. Poikkeusolojen valmiuden ja haavoittuvuuden arvioinnissa voidaan hyödyntää puolustustaloudellisen suunnittelukunnan (PTS) tietojärjestelmäjaoston ohjetta 1/2002.

3.4 Riskien arvioinnin suunnittelu ja toteutus

Riskien arvioinnin huolellinen suunnittelu edesauttaa sen sujuvaa toteutusta. Hyvän suunnittelun avulla riskien arvioinnin toteutus helpottuu ja nopeutuu. Arviointi kannattaa pyrkiä pitämään mahdollisimman yksinkertaisena.

Riskien arviointi kannattaa tehdä ryhmätyönä, johon osallistuu organisaation toiminnan tuntevia henkilöitä. Analyysin onnistumisen edellytyksenä on sitä varten nimetty vastuullinen vetäjä, jonka tehtävinä ovat mm.

- Kohteesta tarvittavan tiedon hankkiminen
- Työryhmän kokoaminen
- Työryhmän perehdyttäminen analyysimenetelmään
- Työryhmäkokousten vetäminen
- Tulosten raportointi ja tiedottaminen

Yhteistyössä työryhmässä käsitellään analyysin laajuus ja rajaus, laaditaan toteutussuunnitelma ja kokousaikataulu sekä suunnitellaan jatkotoimenpiteiden organisointi.

Riskien arvioinnin ensimmäisenä tehtävänä on tunnistaa suojattavat kohteet, jotka ovat organisaation toiminnalle tärkeitä ja joita ilman organisaatio ei voi toimia. Tällaisia suojattavia kohteita ovat mm. tietoaineistot, turvaluokitellut asiakirjat, holvit, asiakastilat, laitehuoneet, toimistohuoneet, neuvottelutilat, arkistot, paperien hävitys, tietojärjestelmät, sovellukset ja tietoliikenneyhteydet.

Varsinainen analysointi tehdään työryhmässä. Sen suositeltava koko on vetäjän lisäksi 3–6 henkeä. Ryhmään valitaan henkilöitä, joilla on hyvä käsitys kohteen toiminnasta, valmius keskustella asioista rakentavassa hengessä ja joille on varattu riittävästi aikaa osallistua analyysiprojektiin. Ryhmän kokoonpano vaihtelee sen mukaan, minkä alueen riskianalyysin tekemisestä on kysymys, esimerkiksi tehdäänkö riskianalyysi koko organisaation tietoturvallisuudesta vai jostakin tietoturvallisuuden osa-alueesta. Tärkeää kuitenkin on, että ryhmässä ovat kattavasti mukana kaikki tarvittavat tahot.

3.5 Riskien arvioinnin organisointi

Riskien arvioinnin tulee olla säännöllistä ja jatkuvaa toimintaa. Tietoturvallisuusriskien arviointia voidaan käyttää esimerkiksi toiminnan suunnittelussa, projekteissa, tietotekniikkahankkeissa, toiminnan tarkastuksessa ja päivittäisessä johtamisessa toimialalähtöisesti. Tarkat, riskien hallinnan kokonaisuuden järjestelyt voivat vaihdella organisaatiokohtaisesti. Keskeistä on laaja-alainen riskien arviointi ja hallinta.

Tietoturvallisuus tulee ottaa huomioon organisaatiossa laaja-alaisesti siten, että se kattaa toiminnan ja yhteistyön organisaation johdosta, sovellusten ja käyttöpalvelun vastuuhenkilöistä palvelujen loppukäyttäjiin ja toiminnan vastuuhenkilöihin asti (VAHTI 1/2001). Eri tahojen tietoturvallisuusriskien arviointiin liittyviä vastuita ja tehtäviä on esitetty taulukossa 1.

Taulukko 1. Tietoturvallisuusriskien arvioinnin tehtäviä ja vastuita

Ylin johto	• Vastaa kokonaisvastuun osana tietoturvallisuuden toteutumisesta • Sisällyttää tietoturvallisuuden osaksi riskienhallintaa • Luo edellytykset ja takaa tietoturvallisuuden toteuttamiseksi tarvittavat resurssit • Hyväksyy tietoturvapolitiikan ja siihen liittyvät periaatteet • Edellyttää toimintojen tietoturvapriorisointia • Asettaa vaatimukset raportoinnille
Tietohallintojohto	• Valmistelee tietohallintoon ja tietotekniikkaan liittyvän tietoturvapolitiikan • Ohjaa organisaation tietoturvallisuuden kehittämistoimenpiteitä • Varmistaa tietoturvallisuuden toteutumisen tietohallinnossa • Huolehtii riskien arvioinnista tietojärjestelmäkehityksessä ja tietotekniikkahankkeissa • Arvioi elintärkeiden tietojärjestelmien haavoittuvuutta • Käynnistää arvioinnin esiintuomat kehittämistoimenpiteet
Tietoturvallisuusjohto	• Osallistuu tietoturvapolitiikan ja -periaatteiden määrittelyyn • Kehittää tietoturvallisuutta turvallisuuspolitiikan mukaisesti • Ohjaa tietoturvallisuuden käytännön toteutusta ja siihen liittyvää riskienhallintaa

	• Luo ja valitsee menettelyt tietoriskien arvioimiseksi • Hankkii arvioinnissa tarvittava asiantuntemuksen • Kouluttaa toiminnasta vastaavan henkilöstön käyttämään arviointimenetelmiä • Osallistuu asiantuntijana riskien arviointiin
Operatiivinen johto	• Vastaa toimialansa tietoturvallisuuden kehittämistoimenpiteiden toteuttamisesta • Ottaa huomioon tietoturvavaatimukset johtaessaan toimialaansa
Esimiehet	• Toteuttavat tietoturvatoimenpiteitä asetettujen tavoitteiden mukaisesti • Raportoivat tietoturvallisuudesta ja siihen kohdistuvista uhkista ja häiriöistä
Tietoturva-asiantuntijat	• Avustavat johtoa ja yksiköitä tietoturvallisuuden edellyttämien toimenpiteiden kehittämisessä ja siihen liittyvässä päätöksenteossa • Toteuttavat osaltaan päätetyt tietoturvatoimenpiteet • Toimivat asiantuntijoina riskien arvioinnissa
Tietopalveluista ja asiakirjahallinnosta vastaavat	• Raportoivat havaitsemistaan uhkista ja häiriöstä • Osallistuvat tarvittaessa oman alansa asiantuntijoina riskien arviointiin
Tietojärjestelmän pääkäyttäjät	• Seuraavat tietojärjestelmien toimintaa tietoturvallisuuden kannalta • Raportoivat tietoturvallisuutta vaarantavista uhkista ja häiriöistä • Osallistuvat tarvittaessa oman alansa asiantuntijoina riskien arviointiin
Käyttäjät	• Raportoivat tietoturvallisuutta vaarantavista uhkista ja häiriöistä • Osallistuvat tarvittaessa oman alansa asiantuntijoina riskien arviointiin

Organisaation johdon tulee saada tiedot arvioinnin keskeisistä tuloksista, kuten:

- Tietojenkäsittelyn merkitys elintärkeille toiminnoille
- Häiriöiden seuraukset sekä vahinkojen suuruus ja vaikutukset eri tilanteissa
- Turvallisuuden ja valmiuden taso ja siinä havaitut puutteet
- Toimenpiteet turvallisuuden ja valmiuden parantamiseksi

3.6 Riskien arvioinnin suhde tietoturvallisuuden hallintajärjestelmän arviointiin

Riskien arviointi ja tietoturvallisuuden hallintajärjestelmän arviointi poikkeavat toisistaan. Tietoturvallisuuden hallintajärjestelmän arvioinnilla selvitetään täyttääkö tietty kohde sille asetetut vaatimukset kaikilta osin. Tietojärjestelmää voidaan esimerkiksi arvioida tietoturvavaatimusten kannalta. Arvioinnin tekijä ottaa kantaa toteamiinsa havaintoihin. Arviointi voi perustua siihen noudatetaanko arvioinnin kohteessa ennalta luotuja kriteereitä. Arviointi voi ottaa myös kantaa siihen, onko jokin asian tila

hyvä tai huono, kuinka merkittävä jokin on jne. Arviointiprosessi kattaa tarvittavat toimet arvioinnin suunnittelusta arvioinnin tulosten raportointiin ja jälkiarviointiin saakka. Tietoturvallisuuden hallintajärjestelmän arviointia on käsitelty ohjeessa VAHTI 3/2003.

4 RISKIENHALLINNAN KEINOT

Riskienhallinnan ensimmäinen vaihe on uhkien tunnistaminen. Kun uhkat on tunnistettu ja niiden toteutumisen todennäköisyys ja seurausten vakavuus arvioitu, voidaan suunnitella ja päättää toimenpiteistä riskien hallitsemiseksi. Riskejä voidaan hallita monin keinoin. Keskeiset toimintavaihtoehdot ovat:

- **Riskin välttäminen.** Tämä on usein mahdollista vain, jos ko. toiminnasta pidättäydytään kokonaan.
- **Riskin poistaminen.** Yksittäinen riski voidaan mahdollisesti poistaa kokonaan. Poistaminen saattaa kuitenkin aiheuttaa uusia riskejä.
- **Riskin pienentäminen.** Ensisijaisesti on pyrittävä estämään vahinkojen syntyminen tai vähentämään niiden seurauksia. Riskin seurausten pienentämiseksi voidaan erilaisilla kontrolleilla pyrkiä vähentämään seurausten vakavuutta tai tapahtuman todennäköisyyttä
- **Riskin siirtäminen** esimerkiksi sopimuksin tai vakuuttamalla.
- **Riskin pitäminen omalla vastuulla.** Osa riskeistä joudutaan tai kannattaa pitää omalla vastuulla. Tällöin otetaan tietoinen riski siitä, että uhka voi toteutua

Toimet riskien pienentämiseksi voivat olla mm:

- **Teknisiä** toimenpiteitä, kuten uudet laite- tai työtilaratkaisut, konesuojauksen kehittäminen, tekniset varmistukset, hälytinjärjestelmät tai huollon ja kunnossapidon parannukset.
- **Organisaation toimintaan** liittyviä toimenpiteitä, kuten yhteisistä pelisäännöistä sopiminen, toimintaohjeiden laatiminen, valvonnan tai seurannan kehittäminen, tiedonkulun ja työnsuunnittelun parantaminen tai vastuista sopiminen.
- **Yksilöiden** toimintamahdollisuuksia parantavia toimenpiteitä, kuten uu-

sien työvälineiden hankinta, ohjeistus, perehdyttäminen ja koulutus, uudet työaika- tai työparijärjestelyt.

Kaikkia riskejä ei voida poistaa. Riskienhallintatoimenpiteet on syytä aloittaa suurimmiksi arvioiduista riskeistä ja ulottaa niin laajalle kuin mahdollista. Riskienhallintaan liittyy aina arviointi toimenpiteiden kustannuksista. On mietittävä kuinka paljon vakuuttamiseen ja erilaisiin riskiä pienentäviin toimenpiteisiin voidaan taloudellisesti panostaa.

4.1 Tietoturvastandardit osana riskienhallintaa

Viime vuosina on laadittu useita tietoturvastandardeja, joiden avulla organisaatiot voivat kehittää tietoturvallisuuttaan ja arvioida omien järjestelmiensä toimivuutta ja tehokkuutta. Tässä luvussa on lyhyesti esitetty kolme keskeistä standardia. Nämä edustavat erilaista lähestymistapaa tietoturvariskien käsittelyyn ja hallintaan.

BS 7799 (ISO 17799) on British Standard Institution'in (BSI) julkaisema tietoturvallisuuden hallintajärjestelmiä koskeva standardi, joka on julkaistu kahdessa osassa:

- BS 7799-1: Tietoturvallisuuden hallintajärjestelmiä koskeva menettelyohje.
- BS 7799-2: Tietoturvallisuuden hallintajärjestelmiä koskevat vaatimukset

Standardi tarjoaa mallin tietoturvallisuuden hallintajärjestelmän rakentamiseen ja hallintaan. Standardin mukaan organisaation turvallisuusvaatimusten tunnistamisessa ensimmäinen lähde on riskianalyysi, jonka avulla tunnistetaan suojattaviin kohteisiin kohdistuvat uhat sekä arvioidaan alttius vahingoille, vahingon todennäköisyys ja vahingon mahdolliset vaikutukset.

Luotaessa standardin mukaista tietoturvallisuuden hallintajärjestelmää organisaation tulee määritellä hallintajärjestelmän kattavuus ja systemaattinen riskien arvioinnin menettelytapa, tunnistaa ja arvioida riskit, tunnistaa ja arvioida riskien käsittelyn vaihtoehdot, valita valvontatavoitteet ja turvamekanismit riskien käsittelyyn sekä valmistella soveltamissuunnitelma.

Common Criteria for Information Technology Security Evaluation (ISO 15408) on tietojärjestelmien ja tietoteknisten tuotteiden tietoturvallisuuden vahvuuden arviointiin ja luokitteluun kehitetty arviointikriteeristö. Järjestelmille ja tuotteille voidaan laatia tietoturvaprofiili, joka kuvaa järjestelmän tietoturvallisuuden toiminnalliset vaatimukset. Kriteeristöä voidaan myös käyttää apuna omia järjestelmiä kehitettäessä ja hankintapäätöksiä tehtäessä. Arvioinnin tuloksia voidaan hyödyntää pohdittaessa täyt-

tääkö tietojärjestelmä tietoturvallisuudelle asetettavat vaatimukset. Nämä vaatimukset on tyypillisesti tunnistettu riskianalyyseissa ja tietoturvapolitiikassa.

Common Criteria jakautuu kolmeen osaan seuraavasti:

- Osa 1: Johdanto ja yleinen malli. Määrittelee CC:n yleiset käsitteet ja periaatteet tietoteknisten tuotteiden tai järjestelmien arvioinnille.
- Osa 2: Tietoturvan funktionaaliset vaatimukset. Esittelee joukon toiminnallisia komponentteja, joilla ilmaistaan standardoidulla tavalla arvioitavan kohteen funktionaaliset vaatimukset. Vaatimukset on taulukoitu komponenteittain, perheittäin ja luokittain.
- Osa 3: Tietoturvan luottamusvaatimukset. Esittelee joukon luottamuskomponentteja, joilla ilmaistaan standardoidulla tavalla arvioitavan kohteen luottamusvaatimukset.

ISO 21827 -standardi (Information technology – Systems Security Engineering – Capability Maturity Model) arvioi tuotteiden ja operatiivisten järjestelmien sijaan organisaation kykyä (kypsyyttä) toteuttaa tietoturvan hallintajärjestelmän prosesseja. Standardi jakautuu viiteen kypsyystasoon (Taponen, 2003)

Tasolla 1 tarkastellaan organisaatiota tai projekteja ja sitä suorittavatko ne tiettyjä toimintoja, jotka katsotaan mallin mukaisesti kuuluvaksi ns. peruskäytäntöihin. Tasolla 2 keskitytään projektityöskentelyn määrittely-, suunnittelu- ja suorituskykyasioihin. Tasolla 3 määritetään toimintaprosessit organisaation laajuisesti. Määrittelyn seurauksena erilaisia projekteja voidaan alkaa räätälöidä hallitusti. Tasolla 4 toiminnan mittarit pyritään sitomaan organisaation (liike)toiminnallisiin tavoitteisiin. ISO 21827-standardin korkeimmalla tasolla vahvuus saavutetaan kaikista alempien tasojen hallinnan parannuskeinoista. Painopiste on siirretty toimintakulttuurin muutoksiin, joilla ylläpidetään aikaisempien tasojen saavutuksia.

5 UHKIEN MÄÄRITTELY JA TUNNISTAMINEN

5.1. Menetelmän valinta

Uhkien tunnistamiseen on olemassa erilaisia menetelmiä, joita voidaan käyttää rinnakkain. Menetelmää valittaessa huomioon otettavia seikkoja ovat:

- Tiedon keruu (kysymykset)
- Menetelmän ominaisuudet ja sopivuus siihen ympäristöön, jossa sitä on tarkoitus käyttää
- Tulosten esitystapa ja kattavuus
- Tulosten selkeys ja yksiselitteisyys
- Käytön helppous
- Menetelmän omat turvaominaisuudet
- Raportointimahdollisuudet

5.2 Uhkien tunnistamismenetelmiä

Riskianalyysimenetelmillä voidaan uhkia tunnistettaessa ottaa huomioon monia luonteeltaan erilaisia tekijöitä ja tarkastella yksityiskohtaisesti niiden välisiä riippuvuussuhteita. Analyysissä tarkasteltava kohde jaetaan yleensä osiin ja riskejä tunnistetaan osakohtaisesti. Usein tunnistuksessa käytetään apuna tarkistuslistoja tai avainsanaluetteloita.

Uhkien ja vaarojen tunnistamiseen on kehitetty useita riskianalyysimenetelmiä, kuten esimerkiksi seuraavat:

- Poikkeamatarkastelu
- Potentiaalisten ongelmien analyysi
- Toimintovirheanalyysi
- Työn turvallisuusanalyysi
- Vaarallisten skenaarioiden analyysi
- Vika- ja vaikutusanalyysi

Yksityiskohtaiset kuvaukset näistä menetelmistä ovat saatavissa esimerkiksi www-sivuilta 'Riskianalyysin menetelmät' osoitteessa http://riskianalyysit.vtt.fi/.

5.2.1 Potentiaalisten ongelmien analyysi

Potentiaalisten ongelmien analyysi (POA) on tehokas uhkien tunnistusmenetelmä. Uhkien tunnistaminen edellyttää avointa mieltä ja eri kokemusten yhdistämistä. Tavallinen keskustelu tai tarkistuslistojen käyttö ei täytä näitä vaatimuksia. POA on tehokas menetelmä riskien luovaan ideointiin ja käsittelyyn työryhmässä.

Potentiaalisten ongelmien analyysissa on useita vaiheita. Analyysi laaditaan ryhmätyönä vastuullisen vetäjän johdolla. Kohteen koosta riippuen joudutaan pitämään useampiakin analyysikokouksia, joiden tyypillinen kesto on 2–4 tuntia kerrallaan.

Analyysin toteutuksen edellytyksenä on, että viraston johto antaa tukensa ja myöntää resurssit analyysin laadintaan. POA aloitetaan valitsemalla ja rajaamalla tarkasteltava kohde. Valintaperusteet ja kohteen rajaukset on hyvä esitellä tarkastelun loppuraportissa. Esimerkiksi tietojärjestelmän osaan kohdistuva riskianalyysi voi koskea seuraavia osatekijöitä:

- Tietoturva-arkkitehtuuri
- Tietojen säilyttäminen ja käyttö
- Sovellus tai sovellukset, ohjelmat
- Käyttöympäristö (palvelimet, työasemat, tietoliikenne)
- Fyysinen ympäristö
- Henkilöstö
- Ulkoisten palveluiden käyttö
- Hankinnat.

POA-menetelmän yksityiskohtainen kuvaus on esitetty liitteessä 3.

5.2.2 Uhkapuut

Uhkapuut on menetelmä, jossa uhkat jaetaan järjestelmällisesti pieniin osiin. Menetelmässä tietoturvaa koskevat uhkia jaetaan yhä pienempiin osiin niin kauan kuin mahdollista. Näin syntyvä puumalli kuvaa rakenteellisesti kaikkia tietoturvaa koskevia uhkia.

Uhkapuiden rakentaminen vaatii tarkastelun kohteen selkeää rajausta ja huolellista tarkastelun kohteena olevan toiminnon tai tietojärjestelmän analyysia (Suominen 2003, s.86).

5.2.3 Skenaariomenetelmä

Skenaarioanalyysissä käydään läpi erilaisia tapauksia, joiden avulla pyritään tunnistamaan mahdollisia uhkia. Analyysi aloitetaan skenaarioiden luomisella. Tähän vaiheeseen kannattaa ottaa mukaan henkilöstöä eri osastoilta ja yksiköistä sekä eri alueiden erityisosaajia. Skenaarioiden laadinnassa on hyvä hyödyntää tietoja aiemmin sattuneista tietoturvavahingoista tai läheltä piti -tilanteista. Apuna voidaan käyttää myös tietoturvaan liittyvää yleistä aineistoa. Analyysin seuraavassa vaiheessa laadittujen tapausten pohjalta pyritään saamaan kuva suojausten nykytilasta sekä mahdollisista tietoturvapuutteista (Suominen 2003, s. 88).

5.2.4 Haavoittuvuusanalyysi

Haavoittuvuudella tarkoitetaan riskien hallintaan liittyvää epävarmuutta, joka uhkaa organisaation toimintaa. Haavoittuvuusanalyysin näkökulma on tulevaisuuspainotteinen. Siinä pyritään tarkastelemaan, miten jatkossa selvitään. Myös kokemuksista kannattaa ottaa opiksi. Tarkastelemalla itselle ja muille sattuneita tilanteita ja vahinkoja saadaan vinkkejä omista vahvuuksista ja heikkouksista.

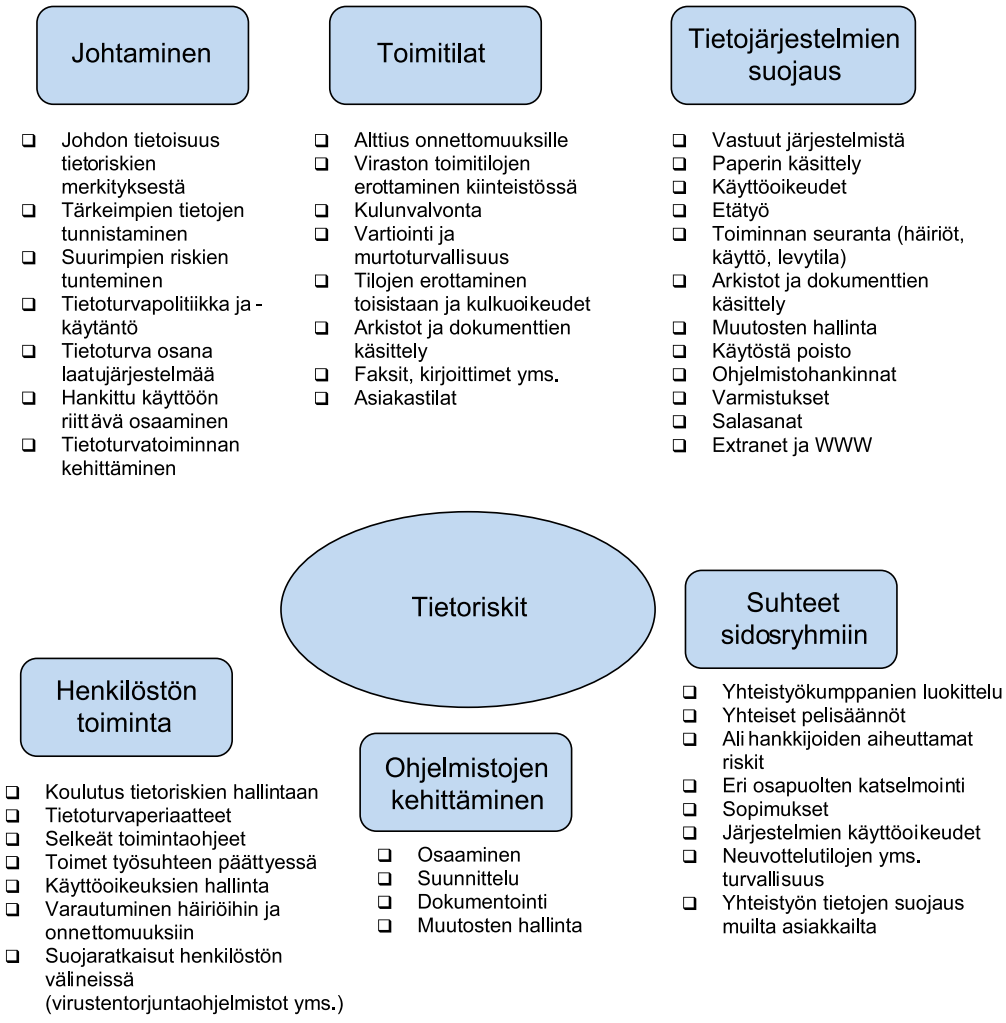
Haavoittuvuusanalyysissä voidaan tarkastella toimintaa kokonaisuutena, jolloin siihen voi sisältyä seuraavia asioita:

- Henkilöt
- Omaisuus ja keskeytykset
- Toimintaedellytykset
- Toiminnan organisointi
- Sidosryhmät
- Talous

Haavoittuvuusanalyysillä tunnistetaan ne osa-alueet, joihin liittyvät suurimmat riskit ja siten selvittää riskejä tarkemmin ja toteuttaa riskejä vähentäviä toimenpiteitä.

Tietoturvallisuutta koskevassa haavoittuvuusanalyysissä voidaan hyödyntää kuvan 2 mukaista tietoriskikarttaa. Riskikartan avulla tarkastellaan tietoturvallisuuden osa-alueita ja mietitään organisaation toimintaan mahdollisesti liittyviä uhkia.

Kuva 2. Esimerkki tietoriskikartasta



5.2.5 Tarkistuslistat

Tarkistuslistojen avulla voidaan uhka kerrallaan miettiä, liittyykö tämä oman organisaation toimintaan. Tarkistuslista on hyvä väline karkeaan uhkien tunnistamiseen ja ongelmakohtien paikallistamiseen. Tarkistuslistoja voidaan käyttää muistilistoina, kun mietitään eri uhkien vaikutusta omassa organisaatiossa. Tarkistuslistat eivät ole koskaan täydellisiä, joten niitä käytettäessä on syytä miettiä, kattavatko ne organisaation toimintaan liittyvät keskeiset uhat. Liitteessä 2 on tietoturvauhkien tunnistamisen tarkistuslistoja. Lisäksi useissa VAHTI-ohjeissa on julkaistu tarkistuslistoja, joita voidaan käyttää apuna uhkien tunnistamisessa:

- VAHTI 2/1999 Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, Liite 4, Keskeiset uhkat
- VAHTI 3/2000 Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, Liite 3, Tietojärjestelmäkehityksen elinkaaren eri vaiheiden tietoturvallisuustarkistuslistat
- VAHTI 4/2001 Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, Liite 3, Sähköisen palvelun turvallisuusanalyysi
- VAHTI 6/2001 Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista
- VAHTI 3/2002 Valtionhallinnon etätyön tietoturvallisuusohje, Liite 1, Uhkia etäkäytön turvallisuudelle
- VAHTI 3/2003 Tietoturvallisuuden hallintajärjestelmän arviointi, Liite 5, Arviointityökalu – tarkistuslista

5.3 Uhkien tunnistaminen

Uhkien tunnistamisen tulee kattaa tietoturvallisuuden kaikki osa-alueet, jotka ovat:

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

Uhkien tunnistamisessa voidaan käyttää apuna esimerkiksi VAHTI-ohjeiden tarkistuslistoja.

Tässä luvussa on kunkin osa-alueen kohdalla esitetty keskeisiä seikkoja, joihin uhkien tunnistamisessa tulee ottaa kantaa. Lisäksi on esitetty esimerkkejä tyypillisistä uhkista.

5.3.1 Hallinnollinen tietoturvallisuus

Hallinnollisen tietoturvallisuuden perustana on tietoturvapolitiikka, jonka avulla johto määrittelee tietoturvallisuuden periaatteet ja toimintatavat (VAHTI 1/2001).

Johdon tietoisuus tietoriskeistä on tietoriskien hallinnan perusta. Johtamisen käytännön välineitä ovat hallittu tietoturvatyö, osaamisen hyödyntäminen ja riskienhallinnan muiden lähtökohtien luominen. Uhkien tunnistamisessa tulisi käsitellä seuraavia asioita:

- Johdon tietoisuus tietoturvauhkista
- Tietoturvallisuuden johtaminen
- Tietoturvallisuuden hallintamenettelyt
- Henkilöstön koulutus riskitietoisuuteen

SUHTEET ASIAKKAISIIN JA SIDOSRYHMIIN

Hallinnolliseen turvallisuuteen kuuluvat myös organisaation suhteet asiakkaisiin ja sidosryhmiin. Uhkien tunnistamisen yhteydessä tulisi käsitellä seuraavia suhteisiin liittyviä seikkoja.

- Suhteiden suunnittelu
- Toiminnan tietoriskien tunnistaminen
- Verkosto- ja alihankintasuhteiden käynnistys
- Tietoturvaratkaisut
- Asiakkaiden ja yhteistyökumppanien käynnit organisaatiossa

Uhkien tunnistamisen apuna voidaan käyttää esimerkiksi liitteen 2 tarkistuslistoja tietoriskien hallinnan johtaminen ja organisointi sekä tietoriskit suhteissa asiakkaisiin ja sidosryhmiin.

Tyypillisiä hallinnolliseen tietoturvallisuuteen liittyviä uhkia ovat seuraavat puutteellisin toimintatapoihin liittyvät:

- Tietoturvaohjeistuksen, sääntöjen ja koulutuksen puutteet
- Tietoturvasopimusten ja -selvitysten puutteet
- Riittämättömät tai sopimattomat resurssit
- Valvonnan puutteellisuus (käytönvalvonta, fyysinen valvonta, huolto)
- Pääsyoikeuksien virheellinen hallinnointi

HANKINNAT

Hankinnat liittyvät kaikkiin tietoturvallisuuden osa-alueisiin. Hankintoja koskevan riskianalyysin teossa voidaan hyödyntää valtion tietotekniikkahankintojen tarkistuslistaa (VAHTI 6/2001). Tämä tarkistuslista on jaettu hankinnan kohteen mukaan seuraaviin pääkohtiin:

- Laitehankinnat ja huolto
- Valmisohjelmistohankinnat
- Sovelluskehitys
- Käyttö-, hallinta- ja tietojenkäsittelypalvelut
- Konsultointi- ja asiantuntijapalvelut

5.3.2 Henkilöstöturvallisuus

Henkilöstöturvallisuus on henkilöstöön liittyvien riskien hallintaa. Tarkasteltavia seikkoja ovat mm. henkilöstön soveltuvuus, toimenkuvat, sijaisjärjestelyt, tiedonsaanti- ja käyttöoikeudet, suojaaminen, turvallisuuskoulutus ja valvonta. Henkilöstön käytännön toimissa tietoriskit joko hallitaan tai ne toteutuvat. Tietoisuus uhkista ja osaaminen luovat pohjan onnistuneelle riskienhallinnalle. Henkilöstön käyttöön on luotava sopivat välineet riskien hallitsemiseksi.

Henkilöstön toimintaan liittyvien uhkien tunnistamiseen voidaan käyttää esimerkiksi liitteen 2 tarkistuslistaa henkilöstön tietoisuus ja toimintatavat tietoriskien hallinnassa.

Tyypillisiä henkilöstöturvallisuuteen liittyviä uhkia:

- Puutteelliset toimintatavat
  - Tietoturvaohjeistuksen, sääntöjen tiedottamisen ja valvonnan sekä koulutuksen puutteet
- Tahattomat teot
  - Käyttövirheet
  - Operointivirheet

- Virusten tahaton levittäminen
- Henkilöstön ylikuormittuminen
- Ylläpitovirheet
- Huoltotoimenpiteet

- Tahalliset teot
  - Tiedon tuhoaminen
  - Tietokantoihin tunkeutuminen
  - Tietojen anastus
  - Tiedon muuttaminen
  - Tietoverkon salakuuntelu
  - Toisten käyttöoikeuksilla toimiminen
- Ylivoimainen este
  - Avainhenkilöstön menetys

5.3.3 Fyysinen turvallisuus

Fyysinen turvallisuus sisältää organisaation tuotanto- ja toimitilojen fyysiseen suojaamiseen liittyvät asiat, joilla pyritään estämään organisaation tarvitsemien tietojen tuhoutuminen, vahingoittuminen tai joutuminen vääriin käsiin. Tähän tietoturvallisuuden osa-alueeseen kuuluvat mm. kulunvalvonta, tekninen valvonta ja vartiointi, palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunta sekä tietoaineistoja sisältävien lähetysten turvallisuus (VAHTI 1/2002). Uhkien tunnistamisessa läpikäytäviä kohtia ovat seuraavat:

- Kiinteistön turvallisuus
- Toimitilojen turvajärjestelyt
- Tietojen ja järjestelmien käyttöperiaatteet
- Asiakaspalvelutilat
- Varavoimajärjestelmät

Tyypillisiä fyysiseen turvallisuuteen liittyviä uhkia ovat esimerkiksi seuraavat:

- Puutteelliset toimintatavat
  - Tietoturvaohjeistuksen, sääntöjen ja koulutuksen puutteet
  - Valvonnan puutteellisuus (käytönvalvonta, fyysinen valvonta, huolto)

- Kulunvalvonnan puutteellisuus
- Tekniset viat
  - Kaapelointiin liittyvät vauriot
  - Laiterikko
  - Jännitehäiriö
  - Sähkökatkot
- Tahattomat teot
  - Inhimillinen erehdys
- Tahalliset teot
  - Murtautuminen toimitiloihin
  - Varkaus
  - Ilkivalta
- Ylivoimainen este
  - Poikkeustilanteet
  - Tulipalot
  - Vesivahingot

5.3.4 Tietoliikenneturvallisuus

Tietoliikenneturvallisuuteen sisältyvät mm. tietoliikennelaitteiston kokoonpano, luettelointi, ylläpito ja muutosten valvonta, ongelmatilanteiden kirjaus, käytön valvonta, verkon hallinta, viestinnän salaus ja varmistaminen, tietoturvallisuuden kannalta merkityksellisten tapahtumien tarkkailu, kirjaus ja selvittäminen sekä tietoliikenneohjelmien testaus ja hyväksyminen. Lähiverkkojen uhkien tunnistamisessa voidaan hyödyntää lähiverkkojen tietoturvallisuussuositusta VAHTI 2/2001. Sähköiseen asiointiin liittyviä uhkia on esitetty ohjeessa VAHTI 4/2001. Internetin tietoturvallisuuteen liittyviä riskejä on käsitelty ohjeessa VAHTI 1/2003.

Uhkien tunnistamisessa käsiteltäviä asioita ovat:

- Reititykset, verkon valvonta ja hallinta
- Salaus
- Palomuuri
- Verkon varmistukset, varajärjestelyt
- Ulkopuoliset yhteydet ja palvelut

Tyypillisiä tietoliikenneturvallisuuteen liittyviä uhkia ovat mm. seuraavat:

- Puutteelliset toimintatavat
  - Tietoturvaohjeistuksen, sääntöjen ja koulutuksen puutteet
  - Valvonnan puutteellisuus (käytönvalvonta, fyysinen valvonta, huolto)
  - Pääsyoikeuksien virheellinen hallinnointi
  - Dokumentaation puutteet
- Tahattomat teot
  - Inhimilliset vahingot
  - Osaamattomuus
  - Kokemattomuus (esim. Nopean kehityksen mukanaan tuoma uusi teknologia)
  - Kommunikaation puute (esim. Ei tiedetä mitä muutoksia joku toinen on tehnyt)
- Tekniset viat
  - Häiriöt tietoliikenneyhteyksissä ja tietoverkoissa
  - Levyrikko
  - Laiteohjainvika
  - Verkkokorttivika
  - Verkon komponentin vika
- Tahalliset teot
  - Ilkivalta, varkaus
  - Luvaton käyttö
  - Salakuuntelu
  - Toisena laitteena tai käyttäjänä esiintyminen
  - Virukset
  - Palvelunestohyökkäykset
- Ylivoimainen este
  - Tulipalo
  - Räjähdys
  - Vesivahinko

5.3.5 Laitteistoturvallisuus

Laitteistoturvallisuus käsittää tietojenkäsittely- ja tietoliikennelaitteiden käytettävyyden, toiminnan, kokoonpanon, kunnossapidon ja laadunvarmistuksen. Lähiverkkoihin liittyvää laitteistoturvallisuutta on käsitelty suosituksessa VAHTI 2/2001.

Tyypillisiä laitteistoturvallisuuteen liittyviä uhkia ovat mm. seuraavat:

- Puutteelliset toimintatavat
  - Tietoturvaohjeistuksen, sääntöjen ja koulutuksen puutteet
  - Valvonnan puutteellisuus (käytönvalvonta, fyysinen valvonta, huolto)
  - Pääsyoikeuksien virheellinen hallinnointi
- Tekniset viat
  - Komponenttiviat
  - Levyrikko
  - Laiteohjainvika
  - Verkkokorttivika
  - Sähkökatkot
- Tahalliset teot
  - Varkaus
  - Ilkivalta
  - Pommiuhat
  - Terroriteot
- Ylivoimainen este
  - Häiriö toimitusketjussa
  - Poikkeustilanteet
  - Tulipalot
  - Vesivahingot

5.3.6 Ohjelmistoturvallisuus

Ohjelmistoturvallisuuteen kuuluvat käyttöjärjestelmät, ohjelmistot sekä sovellus- ja tietoliikenneohjelmat. Tähän alueeseen kuuluvat myös ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt, ohjelmistojen laadunvarmistus sekä turvallisuustoimet. Ulkoistamiseen

liittyvien uhkien tunnistamisessa voidaan hyödyntää valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositusta (VAHTI 2/1999).

JÄRJESTELMÄKEHITYS JA KÄYTTÖÖNOTTO

Järjestelmäkehityksessä tietoturvallisuus tulee ottaa huomioon toisaalta kehityksen aikaisena tietoturvana ja toisaalta turvallisena lopputuotteena. Kehityksen aikaisessa tietoturvassa tulee ottaa huomioon mm. dokumenttien turvallinen käsittely, niiden käytettävyys, testausaineiston luottamuksellisuus. Tietojärjestelmän kehityksessä tulee pyrkiä siihen, että lopputuotteena oleva tietojärjestelmä vastaa niitä vaatimuksia, joita asetetaan kyseisen tehtävän hoidossa tietojen eheydelle, luottamuksellisuudelle ja käytettävyydelle.

Järjestelmäkehityksessä riskien arviointi on tärkeää kaikissa vaiheissa. Esitutkimusvaiheessa riskianalyysin ja alustavien tietoturvallisuusvaatimusten avulla arvioidaan vaadittavien tietoturvallisuuteen liittyvien toimintojen kustannus-, hyöty- sekä kuormitusvaatimukset, joiden pohjalta määritetään tärkeimmät tietoturvallisuusvaatimukset.

Määrittelyvaiheessa tarkennetaan tietoturvavaatimukset. Tässä vaiheessa riskianalyysi toistetaan tarkemmalla tasolla. Riskianalyysin lisäksi tässä vaiheessa tuloksena on yleinen kuvaus jäännösriskistä sekä arvio tietoturvakriittisten kohteiden jäännösriskeistä.

Uhkien tunnistamisen apuna voidaan käyttää valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuosituksessa julkaistuja tietojärjestelmän elinkaaren eri vaiheiden tietoturvallisuustarkistuslistoja (VAHTI 3/2000). Nämä tarkistuslistat kattavat seuraavat elinkaaren vaiheet:

- Esitutkimus
- Määrittely
- Suunnittelu
- Toteutus
- Käyttöönotto
- Ylläpito
- Tuotantoaikainen käyttö
- Version vaihto
- Poisto käytöstä

Tyypillisiä ohjelmistoturvallisuuteen liittyviä uhkia ovat mm. seuraavat:

- Puutteelliset toimintatavat

- Tietoturvaohjeistuksen ja sääntöjen puutteet
- Puutteellinen tai riittämätön koulutus
- Käyttöoikeusmenettelyjen puuttuminen
- Dokumentaation puute

- Tahattomat teot
  - Inhimilliset vahingot
  - Kokemattomuus (esim. Nopean kehityksen mukanaan tuoma uusi teknologia)
  - Kommunikaation puute (esim. Ei tiedetä mitä muutoksia joku toinen on tehnyt)
- Tekniset viat
  - Levyrikko
  - Verkkokorttivika
  - Verkon komponentin vika
- Tahalliset teot
  - Ilkivalta, varkaus
  - Luvaton käyttö
  - Salakuuntelu
  - Toisena laitteena tai käyttäjänä esiintyminen
  - Virukset
  - Palvelunestohyökkäykset
- Ylivoimainen este
  - Tulipalo
  - Räjähdys
  - Vesivahinko

5.3.7 Tietoaineistoturvallisuus

Tietoaineistoturvallisuus käsittää asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden. Keinoina ovat mm. tietoaineistojen luokitus ja luettelointi ja tietovälineiden asianmukainen hallinta, käsittely, säilytys ja hävittäminen. (VAHTI 2/2000, VAHTI 4/2002).

Uhkien tunnistamisen tulisi kattaa seuraavat seikat:

- Tietojen luokitus
- Käyttöoikeudet
- Salassapitosopimukset
- Tarpeettoman tietoaineiston hävittäminen
- Dokumenttien hallinta
- Tietovälineiden käsittely, käytöstä poisto
- Tietoaineiston säilytys ja arkistointi
- Aineiston jakelu, luovutus, tulostus
- Salassapitosopimusten lisäksi julkisuus/salassapitosäädökset
- Yksityisyyden suoja.

Tyypillisiä tietoaineistoturvallisuuden uhkia ovat esimerkiksi seuraavat:

- Puutteelliset toimintatavat
  - Puutteellinen, epäyhtenäinen luokittelu
  - Vanhentuneet käyttöoikeudet
  - Dokumenttien hallinnan puutteet
  - Puuttuvat salassapitosopimukset
  - Salassapito-/julkisuussäädösten tuntemattomuus
  - Henkilötietojen käsittelyn ohjeistuksen puutteet
  - Puutteelliset hävittämismenetelmät
  - Puutteelliset aineiston jakelun, luovutuksen, tulostuksen ohjeet
- Tahattomat teot
  - Tietovälineiden epäluotettava hävitys
- Tekniset viat
  - Puutteelliset säilytys- ja arkistointivälineet
- Tahalliset teot
  - Ilkivalta, varkaus
  - Luvaton käyttö
  - Salakuuntelu

- Ylivoimainen este
  - Tulipalo
  - Räjähdys
  - Vesivahinko

5.3.8 Käyttöturvallisuus

Käyttöturvallisuus kattaa tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvän turvallisuuden. Käyttöturvallisuuteen liittyvät mm. varusohjelmien asetusten turvallisuus, käyttöoikeudet, vahvat käyttöoikeudet, varmuuskopioinnit ja välineiden säilytys sekä laitteiden huollot.

ULKOISTAMINEN JA SOPIMUKSET

Riskianalyysin tulee kattaa myös viraston ulkoistamat palvelut. Ulkoistamisessa korostuvat erityisesti hallinnolliset ja käyttäjiin liittyvät riskit. Uhkat koskevat sekä ulkoistettua palvelua että palvelun ulkoistanutta virastoa ja palvelua hyödyntäviä osapuolia. Ulkoistaminen ei välttämättä lisää riskejä. Tyypillisiä esimerkkejä ulkoistamisen lisäämistä riskeistä ovat luottamuksellisiin aineistoihin perehtyneiden henkilöiden lukumäärän kasvu ja viraston oman järjestelmäosaamisen väheneminen.

Uhkien tunnistamisessa voidaan hyödyntää valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositusta (VAHTI 2/1999).

Tyypillisiä ulkoistamiseen liittyviä uhkia ovat:

- Puutteellisuudet toimintatavoissa tai toimintaedellytyksissä
- Tahattomat teot, kuten käyttövirheet ja virukset
- Tekniset viat
- Tahalliset teot, tiedon urkinta tai tuhoaminen
- Toimitushäiriöt
- Ylivoimainen este toimittajalla tai ympäristössä

ETÄKÄYTTÖ JA ETÄTYÖ

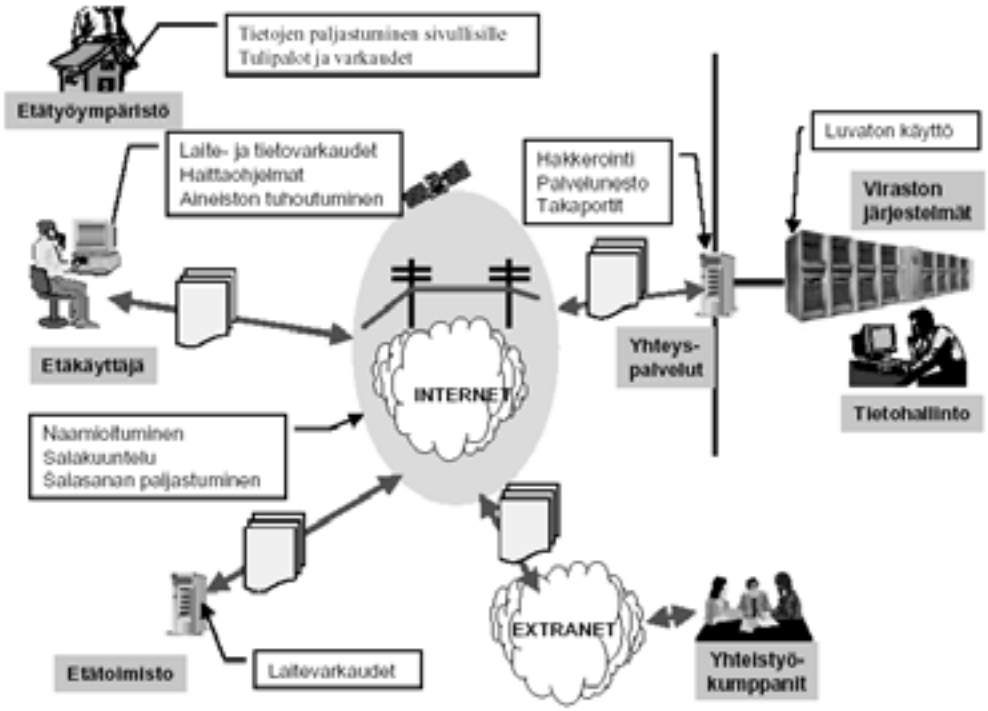
Etätyön riskianalyysissä arvioidaan etätyöhön kohdistuvia uhkia, näiden todennäköisyyksiä ja vaikutuksia sekä valitaan toimenpiteet, joilla riski saadaan halutulle tasolle. Erityisen huolellisesti tulee arvioida mahdollinen henkilötietoihin liittyvä etätyö. Etätyön turvallisuusohjeessa (VAHTI 3/2002) on esitetty havainnollisesti etätyöhön

liittyviä tyypillisiä uhkia. Ohjeessa esitettyä kuvaa voidaan hyödyntää etätyön riskien arvioinnissa (kuva 3).

Uhkien tunnistamisessa tulisi käydä läpi seuraavat etätyöhön liittyvät kohdat:

- Etätyöympäristö
- Etätyössä käytettävät laitteet
- Etätyössä käytettävät ohjelmistot
- Tietoaineistot
- Tietoliikenne
- Tunnistaminen
- Käytettävät järjestelmät ja palvelut
- Tukipalvelut
- Hallinnolliset riskit

Kuva 3. Etätyöhön kohdistuvia uhkia (VAHTI 3/2002)



6 RISKIEN SUURUUDEN ARVIOINTI

Riskin suuruuteen vaikuttavat mahdollisten seurausten vakavuus ja todennäköisyys. Uhkia löytyy usein niin paljon, että kaikkia ongelmia on mahdoton hoitaa yhdellä kertaa. Tärkeää onkin tunnistaa ne isoimmat riskit, jotka kiireisemmin vaativat ratkaisua. Tämän vuoksi määritellään ensin riskin suuruus arvioimalla uhkan seurauksena mahdollisesti syntyvien vahinkojen suuruus ja vahingon todennäköisyys. Riskin suuruuden arviointi antaa perusteet toimenpiteiden suunnittelulle ja suuntaamiselle.

Tässä luvussa esitetään yksi malli riskin suuruuden arviointiin. Myös muita tapoja riskin suuruuden arviointiin on olemassa.

6.1 Uhkan todennäköisyyden arviointi

Kaikkiin vaarojen ja uhkien tunnistamismenetelmiin voidaan liittää myös riskin määrittely karkealla tasolla. Kun uhkan syyt on tunnistettu ja seuraukset arvioitu, voidaan kyseisen riskin suuruus määritellä. Riskin suuruuteen vaikuttavat tapahtuman todennäköisyys ja seurausten vakavuus. Yksinkertainen karkea luokittelu on usein helpompi laatia ja antaa hyvän kuvan eri riskien keskinäisistä eroista. Uhkien luokitteluun voidaan käyttää esimerkiksi taulukossa 1 esitettyä asteikkoa. Asteikon soveltamisessa pitää käyttää harkintaa ja soveltaa sitä oman organisaation tilanteen mukaisesti.

Taulukko 2. Esimerkki uhkan todennäköisyyden arvioinnin asteikosta.

Korkea	**3**	• Toiminto tai järjestelmä on heikosti valvottua • Toimintoon tai järjestelmään pääsy on helppoa • Toimintoa tai järjestelmää kohtaan on suurta mielenkiintoa • Toiminnon ohjeistusta ei ole • Tapahtuma ilmenee kerran kuukaudessa • Uhkan toteuttaminen on mahdollista suurelle määrälle käyttäjiä (oma henkilöstö, yhteistyökumppanit, ulkopuoliset)

Keskimääräinen	**2**	• Toiminto on osittain valvottua • Toiminnon ohjeistus on puutteellista • Tapahtuma ilmenee 1–2 kertaa vuodessa • Uhkan toteuttaminen on mahdollista tietyille käyttäjäryhmille (atk-tuki)
Alhainen	**1**	• Toiminto on hyvin valvottua ja siihen pääsy on hallittua. • Toiminto on hyvin ohjeistettu • Toimintoa kohtaan ei ole mielenkiintoa • Tapahtuma ilmenee kerran vuodessa • Uhkan toteuttaminen on mahdollista vain yksittäisille työntekijöille (asiantuntijat)
Ei merkitystä	**0**	• Todennäköisyys on tasan nolla. Tämä uhka ei voi toteutua missään olosuhteissa

6.2 Seurausten vakavuuden arviointi

Seurausten vakavuuden arviointi kattaa mahdollisesti esiintyvän haitallisen tapahtuman vaikutusten analysoinnin. Taulukossa 2 on esitetty esimerkki seurausten vakavuuden luokittelusta. Asteikon soveltamisessa pitää käyttää harkintaa ja soveltaa sitä oman organisaation tilanteen mukaisesti.

Taulukko 3. Esimerkki seurausten vakavuuden luokittelusta

Erittäin vakavat	**3**	• Seuraukset koskevat kaikkia tietojen tai palveluiden käyttäjiä • Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä • Uhkan toteutuminen aiheuttaa raportoinnin ministeriölle ja tiedotusvälineille • Uhkan toteutuminen aiheuttaa toiminnan keskeytymisen tunneista useisiin päiviin • Uhkan toteutuminen aiheuttaa suuria taloudellisia kustannuksia • Uhkan toteutuminen aiheuttaa vakavan häiriön organisaation toiminnassa (useiden avainhenkilöiden menetys) • Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen • Toiminta on lainsäädännön velvoitteiden vastaista.
Vakavat	**2**	• Seurauksilla on vaikutuksia organisaation sisällä, esimerkiksi yksittäisten työntekijöiden työmäärät kasvavat (avainhenkilön menetys) • Seuraukset koskevat useita tietojen tai palveluiden käyttäjiä • Seurauksilla on vaikutus organisaation toimintaan (saatava kuntoon tunneissa) • Uhkan toteutuminen aiheuttaa tiedotteen tekemisen • Uhkan toteutuminen aiheuttaa merkittäviä taloudellisia kustannuksia

Vähäiset	**1**	• Seuraukset koskevat muutamia tietojen tai palveluiden käyttäjiä • Uhkan toteutuminen ei aiheuta välittömästi toimenpiteitä • Uhkan toteutuminen aiheuttaa sisäisen raportoinnin • Uhkan toteutuminen aiheuttaa vähäisiä taloudellisia kustannuksia • Toiminnan keskeytyminen on muutaman minuutin pituinen

Seurausten vakavuutta mietittäessä kannattaa pohtia seuraavia kysymyksiä.

- **Mitä vahingosta voi pahimmassa tapauksessa aiheutua?** Mitä vahingosta normaalisti aiheutuu?
- **Mihin kaikkeen vahinko vaikuttaa?** Miten monia ihmisiä, töitä, koneita, asiakkaita tai esimerkiksi yhteistyötahoja vahinko ja sen seuraukset koskevat? Mihin kaikkeen vahinko voi vaikuttaa?
- **Mitkä ovat vahingon välilliset seuraukset?** Välilliset seuraukset voivat olla paljon suuremmat kuin välittömästi seuraava vahinko.

6.3 Riskin suuruus

Käytännöllinen apuväline arviointiin on esimerkiksi alla oleva riskitaulukko. Riskitaulukossa seurausten vakavuudelle ja uhkan todennäköisyydelle on kolme eri tasoa. Tehtyjen selvitysten perusteella valitaan ensiksi seurausten vakavuus taulukon ylimmältä riviltä ja sen jälkeen tapahtuman todennäköisyys ensimmäisestä sarakkeesta. Riski on valittujen kohtien leikkauspisteessä olevan arvon suuruinen. Riskin suuruus saa pienimmillään arvon 1 (merkityksetön riski) ja suurimmillaan arvon 5 (sietämätön riski). Myös muunlaisia asteikkoja on mahdollista käyttää.

Taulukko 4. Esimerkki riskitaulukosta

Kriittisyys		Seurausten vakavuus		
		Vähäinen (1)	Vakava (2)	Erittäin vakava (3)
Uhkan todennäköisyys	Korkea (3)	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski
	Keskimääräinen (2)	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski
	Alhainen (1)	1.Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski

Välittömät toimenpiteet pitää toteuttaa kuitenkin heti, jos tilanne niin vaatii..

6.4 Kvantitatiivinen ja kvalitatiivinen riskien suuruuden arviointi

Riskianalyysin alkaa aina ensin kvalitatiivisella uhkien ja vaaratekijöiden tutkimisella. Tämän jälkeen voidaan uhkien seurauksia ja niiden todennäköisyyttä luokitella subjektiivisiin arvioihin perustuen. Tässä luokittelussa voidaan käyttää apuna edellä esitettyjä taulukkoja tai muita vastaavia apuvälineitä. Usein tällainen analyysi on riittävän tarkka riskienhallinnan kannalta.

Analyysia voidaan jatkaa merkittävimpien uhkien seurausten ja tapahtumistaajuuden kvantitatiivisella arvioinnilla, mikäli tarvitaan tarkempia arvioita päätöksenteon pohjaksi. Uhkien todennäköisyyden arviointi perustuu tällöin komponenttien vioittumistietoihin ja ihmisen toiminnan virhetietoihin. Seurausten kuvaamiseen voidaan käyttää laskentamenetelmiä, jotka kuvaavat järjestelmän käyttäytymistä häiriötilanteessa.

Courtneyn riskianalyysimenetelmä on hyväksytty Yhdysvaltain valtion virastojen viralliseksi riskianalyysistandardiksi, ja sen pohjalta on toteutettu lukuisia riskianalyysiohjelmistoja. Menetelmän kehitti Robert Courtney Jr IBM:n palveluksessa 1970-luvulla.

Menetelmä perustuu ei-toivottujen tapahtumien odotetun esiintymistaajuuden sekä rahallisten vahinkojen suuruuden avulla laskettavaan vahingon odotusarvoon. Laskennan lopputuloksena saadaan tarkka numeerinen arvo (odotetun vahingon suuruus euroina). Tämä mahdollistaa tarvittavien suojausten priorisoinnin ja hyöty- / kustannusarviot suojauksia suunniteltaessa. Courtneyn menetelmän ongelmana on tilastollisen tiedon puute. Lähtötiedot ovat arvioita.

7 TOIMENPITEIDEN MÄÄRITTELY

Tunnistettuja riskejä voidaan hallita monilla keinoilla. Ensisijaisesti on pyrittävä estämään vahinkojen syntyminen tai vähentämään niiden seurauksia. Tarvittavat toimenpiteet riippuvat riskin suuruudesta. Toimenpiteet voidaan suunnitella esimerkiksi seuraavan taulukon avulla.

Merkityksetön riski

- Riski on niin pieni, että toimenpiteitä ei tarvita.

Vähäinen riski

- Toimenpiteitä ei välttämättä tarvita.
- Harkitaan parempia ratkaisuja, jotka eivät aiheuta lisäkustannuksia.
- Tilannetta seurataan ja varmistetaan, että riski pysyy hallinnassa.

Kohtalainen riski

- On ryhdyttävä toimiin riskin pienentämiseksi. Toimenpiteiden toteutukselle voidaan suunnitella sopiva aikajänne.
- Toimenpiteiden kustannuksia on mietittävä tarkasti.
- Jos riskiin liittyy erittäin haitallisia seurauksia (esimerkiksi vakava henkilövahinko tai tulipalo), on tarpeen selvittää tapahtuman todennäköisyys tarkemmin.

Merkittävä riski

- Riskin pienentäminen on välttämätöntä. Toimenpiteet tulee aloittaa nopeasti.
- Riskialtista toimintaa ei pidä aloittaa ennen kuin riskiä pienennetty.
- Riskialtista toimintaa voidaan jatkaa, mutta kaikkien on tunnettava riski ja toiminta pitää saada loppumaan nopeasti.

Sietämätön riski

- Riskin poistaminen on välttämätöntä. Toimenpiteet tulee aloittaa välittömästi
- Riskialtista toimintaa ei pidä aloittaa
- Riskialtis toiminta pitää keskeyttää, kunnes riski on poistettu

Riskien arvioinnin tavoitteena on löytää tehokkaimpia toimenpiteitä tietoturvallisuuden parantamiseen. Riskin suuruutta voidaan käyttää perusteena toimenpiteiden kohdistamiseen. Suurimpien riskien poistamisen tai pienentämisen tulee olla etusijalla toimenpiteitä toteutettaessa. Riskien suuruusjärjestys ei kuitenkaan ole suoraan toimenpiteiden järjestys vaan toimenpiteiden valinnassa pitää päätyä kokonaisuuden kannalta optimaalisiin ratkaisuihin.

8 JATKOKEHITYS- JA SEURANTASUUNNITELMAT

Riskien arvioinnissa laadittujen toimenpide-ehdotusten toteuttamiseksi tulee analyysin lopuksi sopia, mitä ehdotuksia ja miten ryhdytään viemään eteenpäin. Samalla sovitaan asioiden hoidolle vastuuhenkilöt ja karkea aikataulu. Edistymistä seurataan sopivin, esimerkiksi puolen vuoden välein pidettävissä seurantakokouksissa.

Kaikkia kehitettyjä parannustoimenpiteitä ei voida toteuttaa välittömästi. Riskin arvioinnin avulla on tunnistettu suurimmat riskit. Yleensä kannattaa aloittaa näiden poistamisella tai pienentämisellä. Joskus parannustoimenpiteet vaativat jatkoselvityksiä, lisäsuunnittelua ja investointeja. Ei kuitenkaan kannata jäädä odottamaan suurimpien riskien poistamista, vaan samanaikaisesti voidaan hoitaa pieniä parannuksia pienempien riskien hallitsemiseksi. Usein toimenpiteet voidaan toteuttaa helposti ja pienin panostuksin. Tällaisia ovat esimerkiksi uudet toimintatavat ja henkilökunnan koulutus. Taulukossa 5 on esitetty esimerkki yksittäisen riskin hallintasuunnitelmasta.

Taulukko 5. Esimerkki yhden riskin hallintasuunnitelmasta.

Riski	**Internet palvelimen tietoturvariski (murto)**
Tavoite	Tavoitteena on sekä riskin todennäköisyyden että seurausten vakavuuden pienentäminen.
Syy riskin olemassaoloon	Käyttöjärjestelmän suunnittelussa on unohdettu riittävästi huomioida tietoturvallisuuteen liittyviä tekijöitä tai toiminnallisuuden takaamiseksi on turvaominaisuuksista osittain luovuttu. Testauksessa ei ole löydetty kaikkia aukkoja joita hyökkääjä voi hyödyntää.
Toimenpide-ehdotus	Toimintaympäristön tapahtumia seurataan. Palvelimen ohjelmisto päivitetään usein. Hankitaan seurantatyövälineitä joilla mahdollinen murto voidaan havaita.
Aikataulu ja vastuuhenkilö	Toiminnan seuranta on jatkuvaa. Hankitaan tarvittavat ohjelmistot kahden kuukauden aikana. Vastuuhenkilö on MM

Tarkastelun tulokset on saatettava asianomaisten tietoon. Sekä viraston johtoa että kohteen henkilöstöä tulee informoida tuloksista ja kertoa jatkotoimenpiteistä. Tiedottaminen voidaan hoitaa organisaation normaalin tiedotuskäytännön mukaisesti järjestämällä tiedotustilaisuuksia, tiedottamalla asiasta sopivissa kokouksissa, julkaisemalla keskeiset tulokset esimerkiksi henkilökuntalehdessä tai laatimalla erillinen tiedote.

Riskienhallintaharjoitus on yksi mahdollisuus suunnitella organisaation toimintaa eri uhkatilanteissa. Osana jatkokehitystoimenpiteitä voidaan testata organisaation valmiutta toimia esimerkiksi virushyökkäystilanteessa. Harjoitus valmistellaan suunnitteluryhmässä, joka laatii skenaarion tapahtuman kehittymisestä. Varsinaisessa harjoituksessa käydään läpi eri tahojen toiminta skenaarion mukaisessa tilanteessa. Harjoituksen jälkeen arvioidaan tulokset ja laaditaan suunnitelmat tarvittavista korjaavista toimenpiteistä.

LÄHTEET JA VIITEAINEISTOT

Arkaluontoiset kansainväliset tietoaineistot. Käsittelyperiaatteet valtionhallinnossa. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 4/2002. Valtiovarainministeriö.

BS 7799-1. 2000. Tietoturvallisuuden hallinta. Osa 1. Tietoturvallisuuden hallintaa koskeva menettelyohje. Suomen standardisoimisliitto SFS. Helsinki.

BS 7799-2. 2003. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset ja soveltamisohjeet. Suomen standardisoimisliitto SFS. Helsinki.

ISO 15408-1:1999. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model.

ISO 15408-2:1999. Common Criteria for Information Technology Security Evaluation. Part 2: Security functional requirements.

ISO 15408-3:1999. Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance requirements.

Kyrölä, T. 2001. Esimies ja tietoriskien hallinta. WSOY. Juva.

Murtonen, M. 2003. Riskien arviointi työpaikalla. Työkirja. Sosiaali- ja terveysministeriö, työsuojeluosasto, Tampere.

Pk-yrityksen riskienhallinta -työvälinesarja. 2000. VTT. www.pk-rh.com

Suominen, A. 2003. Riskienhallinta. WSOY. Helsinki.

Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 4/2001. Valtiovarainministeriö.

Taponen, V, Tietoturvastandardit puolustusvoimien tietoturvaprosessien sekä ekstranet-ratkaisun kehittämisessä. 2003. Diplomityö. Teknillinen korkeakoulu. Espoo.

Tietoteknisten laitetilojen turvallisuussuositus. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 1/2002. Valtiovarainministeriö.

Tietotekniikan turvallisuus ja toiminnan varmistaminen. Puolustustaloudellinen suunnittelukunta. Tietojärjestelmäjaoston ohje 1/2002.

Tietoturvallisuuden hallintajärjestelmän arviointi. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 3/2003. Valtiovarainministeriö.

Valtion tietohallinnon Internet-tietoturvallisuusohje. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 1/2003. Valtiovarainministeriö.

Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 2/1999 Valtiovarainministeriö.

Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 6/2001. Valtiovarainministeriö.

Valtion viranomaisen tietoturvallisuustyön yleisohje. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 1/2001. Valtiovarainministeriö.

Valtionhallinnon etätyön tietoturvallisuusohje. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 3/2002. Valtiovarainministeriö.

Valtionhallinnon lähiverkkojen tietoturvallisuussuositus. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 2/2001. Valtiovarainministeriö.

Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 2/2000. Valtiovarainministeriö.

Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus. Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI 3/2000. Valtiovarainministeriö.

LUETTELO OHJAAVASTA LAINSÄÄDÄNNÖSTÄ

(VAHTI 1/2001, s. 17–18)

Toiminnan ohjausta koskevat

- valtioneuvoston ohjesääntö (1522/1995)
  - VM ohjaa valtionhallinnon tietoturvallisuutta (19§)

Tietoaineistoa koskevat

- perustuslain perusoikeussäännökset (731/1999)
  - yksityiselämän suoja (10 §)
  - sananvapaus ja julkisuus (12 §)
- laki viranomaisen toiminnan julkisuudesta (621/1999)
  - julkisuusperiaate (1 §)
  - velvoite hyvään tiedonhallintatapaan (3 §)
  - tiedonsaanti salassa pidettävästä asiakirjasta (10 §)
  - viranomaisen velvollisuudet edistää tiedonsaantia ja hyvää tiedonhallintatapaa (17 §)
  - hyvä tiedonhallintatapa (18 §)
  - salassapitovelvoitteet (22 §–25 §)
  - asiakirjasalaisuus (22 §)
  - vaitiolovelvollisuus ja hyväksikäyttökielto (23 §)
  - salassa pidettävät viranomaisen asiakirjat (24 §)
  - salassapidosta poikkeaminen ja sen lakkaaminen (26 §–32 §)
- 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 §)

- asetus valtionhallinnon tietohallinnosta (155/1988 ja muutos 1401/1992)
  - tietojärjestelmät taloudellisia, turvattuja, toiminnallisesti yhteensopivia sekä tietosuojan vaatimukset täyttäviä (1 §)
  - valtionhallinnon tietojenkäsittelyn ja tietohallinnon ohjaus ja yhteensovittaminen (2 §)
  - velvoite pyytää merkittävästä tahi useaa virastoa tai laitosta koskevasta tietotekniikan soveltamiseen liittyvästä hankkeesta valtiovarainministeriön lausunto (3 §)
  - tietojenkäsittelyä ja tietohallintoa koskeva kehittämissuunnitelma (3 §)
- arkistolaki (831/1994)
  - käytettävyys ja säilyminen, tarpeettoman aineiston hävittäminen (7 §)
  - turvaaminen tuhoutumiselta, vahingoittamiselta ja asiattomalta käytöltä (12 §)
- laki valtion talousarviosta annetun lain muuttamisesta (217/2000)
  - velvollisuus hoitaa sisäinen valvonta (24 §)
- asetus valtion talousarviosta (1243/1992)ja sen muutos (263/2000)
  - taloushallinnon järjestelmien tietoturvallisuusmääräykset taloussäännössä (26 §)
  - riskeihin nähden asianmukainen sisäinen valvonta (69 §, 69a §)
  - sisäinen tarkastus (70 §)
  - koneellisin menetelmin pidetty kirjanpito ja sen menetelmäkuvaus (47 §)
- henkilötietolaki (523/1999)
  - tarkoituksena toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia (1 §)
  - tietoturvallisuus ja tietojen säilytys (32–35 §)
- henkilökorttilaki (829/1999)
- laki yksityisyyden suojasta työelämässä (477/2001)
- väestötietolain muutos (527/1999)
  - väestörekisterikeskuksen varmenneviranomaistoiminta
- tekijänoikeuslaki (344/2000)

- ohjelmistojen tekijänoikeudet

Tietoaineistoa ja tietotekniikkaa koskevat

- laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)
  - televiestinnän turvallisuus (4 §)
  - teleyrityksen tietoturvallisuusvelvoitteet (6 §)
  - teleoperaattorien vaitiolovelvollisuus (7 §)
  - rajoitukset suoramarkkinoinnille (21 §)
- edellisen lain nojalla annettu asetus (723/1999)
- telemarkkinalaki (396/1997) ja laki telemarkkinalain muuttamisesta (566/1999)
  - suojauksen purkujärjestelmien kielto (25 §)
- 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 §)
- laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- laki sähköisistä allekirjoituksista (14/2003)
- valtion virkamieslaki (750/1994)
  - virkasuhteen päättäminen, purkuperusteet, kirjallinen varoitus (7 luku)

Poikkeusolojen valmiutta koskevat

- valmiuslaki 22.7.1991/1080
- laki huoltovarmuuden turvaamisesta (18.12.1992/1390)
- valtioneuvoston päätös huoltovarmuuden tavoitteista (8.5.2002/350)
- laki Puolustustaloudellisesta suunnittelukunnasta (20.5.1960/238)

Valmisteilla olevat säädökset

- hallituksen esitys sähköisen viestinnän tietosuojalaiksi (HE 125/2003)
- työelämän tietosuojalainsäädännön täydentämishanke, Työministeriö

TIETOTURVAUHKIEN TUNNISTAMISEN TARKISTUSLISTOJA

Tässä liitteessä on esitetty esimerkkejä tietoturvallisuusuhkien tunnistamisen tarkistuslistoista. Seuraavat tarkistuslistat on sovellettu valtionhallintoon Pk-yrityksen riskienhallinta -työvälinesarjassa julkaistuista tarkistuslistoista:

1. Tietoriskien hallinnan johtaminen ja organisointi
2. Tietoriskit suhteissa asiakkaisiin ja sidosryhmiin
3. Henkilöstön tietoisuus ja toimintatavat tietoriskien hallinnassa
4. Toimintaympäristön, työ- ja palvelutilojen tietoturvallisuus
5. Tietojärjestelmien suojaus

Tarkistuslistojen soveltamisessa tulee muistaa, että tarkistuslistat eivät koskaan ole täydellisiä, joten niitä käytettäessä on syytä miettiä kattavatko ne organisaation toimintaan liittyvät keskeiset uhkat ja tehdä tarvittavat täydennykset.

1. Tietoriskien hallinnan johtaminen ja organisointi

Tarkistuslista tietoriskien hallinnan johtamiseen liittyvistä asioista ja johdon toimiin liittyvien riskien tunnistamiseen.

Organisaatio:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa organisaation toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

1.1 Hallinnollinen tietoturvallisuus

1.1.1 Johdon tietoisuus tietoriskeistä

	Kyllä	Ei	Ei koske meitä
Onko organisaation johto tietoinen tietoriskien vaikutuksista liiketoimintaan?	☐	☐	☐
Onko tunnistettu ne organisaation tiedot, jotka ovat toiminnalle elintärkeitä?	☐	☐	☐

1.1.2 Oireita tietoriskeistä

	Kyllä	Ei	Ei koske meitä
Onko toimitilojen rikosturvallisuudesta huolehdittu?	☐	☐	☐
Ovatko työntekijät sitoutuneet työhönsä ja työnantajaansa eivätkä ole esim. siirtymässä kilpailijalle?	☐	☐	☐
Voiko luottaa siihen, että organisaation palveluksesta lähteneet tai irtisanotut henkilöt eivät levitä tietoja organisaatiosta?	☐	☐	☐
Onko laitteistojen tai toimitilojen paloturvallisuudesta huolehdittu?	☐	☐	☐
Toimiiko koko henkilöstö huolellisesti ja rehellisesti?	☐	☐	☐
Seurataanko edellä mainittuja erilaisia häiriötilanteita?	☐	☐	☐

1.1.3 Tietoriskien hallinnan johtaminen

	Kyllä	Ei	Ei koske meitä
Onko toiminnan turvallisuudesta huolehtiminen vastuutettu nimetylle henkilölle organisaation johdossa?	☐	☐	☐
Onko organisaation omaisuuden ja tietojen suojaamistahto konkretisoitu tietoturvapolitiikaksi ja käytännöiksi?	☐	☐	☐
Arvioidaanko tietojen käsittelytapoja ja turvajärjestelyjä laatujärjestelmän auditointien yhteydessä?	☐	☐	☐

	Kyllä	Ei	Ei koske meitä
Onko johdolla valmius vakuuttaa sidosryhmille tietojen ja tietämyksen säilyvyys organisaatiossa?	☐	☐	☐
Onko laadittu tietoturvasuunnitelma?	☐	☐	☐
Raportoidaanko tietoturvasta suoraan ylimmälle johdolle?	☐	☐	☐

1.1.4 Tietoriskien tunteminen

	Kyllä	Ei	Ei koske meitä
Onko tunnistettu tilanteet, jotka saattavat lamauttaa toiminnan?	☐	☐	☐
Onko tunnistettu tilanteet, jotka häiritsevät ja haittaavat toiminnassa tarvittavien tietojen saantia?	☐	☐	☐
Onko tunnistettu tilanteet, jotka voivat aiheuttaa tietojen häviämisen tai muuttumisen?	☐	☐	☐
Onko arvioitu em. tilanteiden menetyksiä tai vahinkoja?	☐	☐	☐
Onko turvakäytäntöjen kehittämiskustannukset suhteutettu toiminnan keskeytymisestä aiheutuviin menetyksiin?	☐	☐	☐

1.1.5 Tietoriskien hallintamenettelyt

	Kyllä	Ei	Ei koske meitä
Onko turvaamisen tavoitteet määritelty?	☐	☐	☐
Onko turvatyön mittarit määritelty?	☐	☐	☐
Onko organisaatiolla toiminnan turvaamisen strategia osana toimintastrategiaa?	☐	☐	☐
Onko organisaatiolla käytettävissä laaja-alaista turva-asioiden osaamista?	☐	☐	☐
Onko olemassa toimintamalli tietokonevirusten hallitsemiseksi?	☐	☐	☐
Onko olemassa toipumissuunnitelma ja toimintaohjeet, jotka ohjaavat vastuuhenkilöitä ja muuta henkilöstöä varajärjestelyjen käyttöönotossa ja toiminnassa häiriötilanteissa?	☐	☐	☐
Onko peruskäyttäjille laadittu ja tiedotettu tietoturvaohjeet?	☐	☐	☐
Seurataanko järjestelmien käyttöä esimerkiksi etäkäyttöä epämääräisinä kellonaikoina, tärkeiden tietojen kopiointia tai lähettämistä?	☐	☐	☐
Onko olemassa tiedottamismenettely, jolla kerrotaan organisaatiossa tapahtuneesta häiriötilanteesta tarvittaville osapuolille?	☐	☐	☐
Vastaako joku turvakäytäntöjen kehittämisestä?	☐	☐	☐
Onko organisaatiossa tietoturvaryhmä?	☐	☐	☐
Onko poikkeusolojen tietojenkäsittelyn valmiussuunnitelma?	☐	☐	☐
Onko laadittu ennakkosuunnitelmat häiriötilanteisiin ja tietoturva-hyökkäysten/haittaohjelmien varalle?	☐	☐	☐

2. Tietoriskit suhteissa asiakkaisiin ja sidosryhmiin

Tarkistuslista organisaation ja sen asiakkaiden ja sidosryhmien välisen yhteistyön tietoriskien tunnistamiseen.

Organisaatio:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa organisaation toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

2.1 Hallinnollinen tietoturvallisuus

2.1.1 Asiakas ja sidosryhmäsuhteiden suunnittelu

	Kyllä	Ei	Ei koske meitä
Onko yhteistyökumppanit luokiteltu toiminnan jatkuvuuden kannalta elintärkeisiin, tärkeisiin ja tarpeellisiin?	☐	☐	☐
Onko eri osapuolten valinnassa otettu myös tietoriskit huomioon? (Tahojen luotettavuus, kyky hallita heille luovutettuja tietoja jne.)	☐	☐	☐
Onko kaikilla osapuolilla sama käsitys yhteistyösuhteiden luonteesta?	☐	☐	☐

2.1.2 Toiminnan tietoriskien tunnistaminen

	Kyllä	Ei	Ei koske meitä
Onko arvioitu kumppaneilla tapahtuvat tilanteet, jotka aiheuttavat haittaa organisaation toiminnalle?	☐	☐	☐
Onko kumppaneilla kirjallinen tietoturvapolitiikka ja toimintamallit tietojen käsittelyyn?	☐	☐	☐
Onko omassa organisaatiossa tietoturvapolitiikka dokumentoitu siten, että dokumentti voidaan luovuttaa kumppaneille ja kumppanit saavat sen perusteella kuvan toiminnan luotettavuudesta?	☐	☐	☐
Onko kaikkien kumppanien tietoturvallisuustoiminta katselmoitu yhteistyössä?	☐	☐	☐

2.1.3 Verkosto- ja alihankintasuhteiden käynnistys

	Kyllä	Ei	Ei koske meitä
Onko yhteistyöhön luotu yhteiset tietoturvaperiaatteet?	☐	☐	☐
Onko yhteistyökumppanien välisiin sopimuksiin liitetty organisaation tietoturvavaatimukset sekä tietojen siirron ja käsittelyn menettelyohjeet?	☐	☐	☐

	Kyllä	Ei	Ei koske meitä
Sovitaanko erilliskäytäntöjä luottamuksellisten, kuten tuotekehityksen, tietojen käytöstä, siirto- ja suojaustavoista?	☐	☐	☐
Onko kaikki osapuolet koulutettu yhteisiin tietojärjestelmiin?	☐	☐	☐
Onko yhteistyössä edellytettävät tietoturvaperiaatteet, menettelytavat ja järjestelmät koulutettu alihankkijoille?	☐	☐	☐
Onko suunniteltu, miten hallitaan yhteistyösuhteen päättyminen?	☐	☐	☐

2.2 Fyysinen turvallisuus

2.2.1 Asiakkaiden ja yhteistyökumppanien käynnit toimitiloissa

	Kyllä	Ei	Ei koske meitä
Syntyykö asiakaskäynneillä tai yhteistyökontakteissa kuva oman organisaation luotettavuudesta ja luottamuksellisuudesta?	☐	☐	☐
Pidetäänkö muiden asiakkaiden, yhteistyötahojen ja projektien tiedot suojassa? (Ei neuvotteluhuoneissa, ei asiakaspalvelutiloissa)	☐	☐	☐
Onko neuvottelutilat ääni- ja näköeristetty?	☐	☐	☐
Selvitetäänkö uusien vierailijoiden taustat riittävän huolellisesti? (Koskee sekä kotimaisia että ulkomaisia vierailijoita).	☐	☐	☐

2.3 Käyttöturvallisuus

2.3.1 Tietoturvaratkaisut

	Kyllä	Ei	Ei koske meitä
Onko olemassa käytäntö, jolla käsitellään kumppanin henkilöstön tarve päästä organisaation tietoliikenneverkkoon ja järjestelmiin?	☐	☐	☐
Onko sovittu osapuolten toimenpiteet eri häiriötilanteiden hoitamiseksi?	☐	☐	☐
Arvioidaanko kumppanien turvakäytäntöjä?	☐	☐	☐

3. Henkilöstön tietoisuus ja toimintatavat tietoriskien hallinnassa

Tarkistuslista arkipäivän tietojenkäsittelytapojen riskien tunnistamiseksi.

Organisaatio:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa organisaation toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

3.1 Henkilöstöturvallisuus

3.1.1 Henkilöstön tietoisuus tietoriskeistä

	Kyllä	Ei	Ei koske meitä
Onko henkilöstölle koulutettu toiminnan luottamuksellisuuteen ja tietosuojaan liittyviä yleispiirteitä?	☐	☐	☐
Tunteeko henkilöstö organisaation vastuut tietojen luotta-muksellisuuden ja muun tietoturvallisuuden suhteen?	☐	☐	☐
Onko kaikille selvää, millaiset tiedot ovat kaikkein tärkeimpiä ja joiden suojaaminen on erityisen tärkeää?	☐	☐	☐
Onko kaikille selvää, mitä organisaation toiminnasta saa kertoa ulkopuolisille?	☐	☐	☐
Onko organisaatiolle määritelty tietoturvaperiaatteet ja laadittu niiden toteuttamiseksi ohjeet?	☐	☐	☐
Kattavatko ohjeet sähköisten tietojärjestelmien lisäksi suullisen viestinnän ja paperidokumenttien käsittelyn ja jakelun?	☐	☐	☐
Onko henkilöstö koulutettu tunnistamaan tietoriskejä ja noudattamaan turvakäytäntöjä?	☐	☐	☐
Onko olemassa menettely tietoturva-asioiden käsittelyä varten?	☐	☐	☐
Onko jokainen työntekijä allekirjoittanut tietojen käyttösäännöt?	☐	☐	☐
Onko tietojen luokittelu ja ohjeet osa arkipäivän käytäntöä?	☐	☐	☐
Tietääkö henkilöstö, minne ilmoittaa havaitsemistaan tietoturva-rikkeistä tai käytäntöjen puutteista?	☐	☐	☐

3.1.2 Uudet työntekijät ja työsuhteen päättyminen

	Kyllä	Ei	Ei koske meitä
Tarkistetaanko uusien työntekijöiden taustat ennen työsuhteen alkamista?	☐	☐	☐
Ovatko tietoturva-asiat mukana uusien työntekijöiden perehdyttämisessä?	☐	☐	☐
Selvitetäänkö myös uusille ja väliaikaisille työntekijöille yrityksen tietoturvapolitiikan ja vaitiolositoumuksen merkitys?	☐	☐	☐
Allekirjoittavatko työntekijät erillisen sitoumuksen tietojen ja järjestelmien käytöstä sekä tietojen palauttamisesta työsuhteen jälkeen?	☐	☐	☐

3.1.3 Työsuhteen päättyminen

	Kyllä	Ei	Ei koske meitä
Onko henkilön irtisanoutumistilanteessa esimiehellä tieto kaikista henkilön käyttäjätunnuksista ja käyttöoikeuksista, joiden voimassaolo tulee poistaa?	☐	☐	☐
Onko suunniteltu muut toimet tietoturvallisuuden varmistamiseksi työsuhteiden päättyessä?	☐	☐	☐

3.1.4 Henkilöstön toimintatavat

	Kyllä	Ei	Ei koske meitä
Käsittelevätkö työntekijät luottamuksellisia tietoja vain työnsä kannalta tarkoituksenmukaisella tavalla?	☐	☐	☐
Onko organisaation keskeiset tiedot suojattu mm. rajaamalla niiden saatavuus ja määrittelemällä niiden käyttöoikeudet?	☐	☐	☐
Onko minimoitu mahdollisuus myydä tai luovuttaa ulos organisaatiosta sille keskeisiä tietoja ja dokumentteja?	☐	☐	☐
Ovatko organisaation sisäiset valvontajärjestelmät kunnossa (työnvalvonta, tilojen valvonta, tietojen käytön ja tietojärjestelmien valvonta)?	☐	☐	☐
Onko työntekijöiden omin töiden tekeminen työpaikalla hallittua (ajat, kulkuoikeudet, valvonta)?	☐	☐	☐
Onko luottamuksellisten tietojen säilyttämiseen riittävästi lukollisia tiloja?	☐	☐	☐
Hoidetaanko jätepaperin keräys ja käsittely hallitusti?	☐	☐	☐
Ovatko puhelinkäyttäytymisen ohjeet olemassa?	☐	☐	☐
Onko tulipalon varalle toiminta ohjeistettu ja harjoiteltu?	☐	☐	☐
Onko tehtävien varahenkilöjärjestelyistä huolehdittu?	☐	☐	☐

3.1.5 Tietojärjestelmien ja tietokoneiden käyttö

	Kyllä	Ei	Ei koske meitä
Onko henkilöstöllä riittävä perusosaaminen järjestelmien käyttöön?	☐	☐	☐
Käyttääkö jokainen työntekijä työssään vain omaa käyttäjä-tunnustaan?	☐	☐	☐
Onko ohjeistettu turvallisen salasanan muodostaminen?	☐	☐	☐
Pystyvätkö muut työntekijät lukemaan tai muuttamaan käyttäjän tietoja käyttäjän huomaamatta?	☐	☐	☐
Onko varmuuskopioiden ottamiseen ja palauttamiseen olemassa toimintaohjeet?	☐	☐	☐
Valvotaanko varmuuskopioiden ottamista?	☐	☐	☐
Onko Internetin käyttö ohjeistettu?	☐	☐	☐
Onko sähköpostin käyttö ohjeistettu?	☐	☐	☐
Onko virusten torjuntamenettelyt ohjeistettu niin työkoneiden kuin kotikoneiden osalta?	☐	☐	☐
Onko virusohjelmien ja muiden vastaavien päivitykset automatisoitu?	☐	☐	☐
Salakirjoitetaanko kannettavilla tietokoneilla olevat luottamukselliset tiedot?	☐	☐	☐
Onko käyttäjiä kielletty asentamasta organisaation verkkoon ulkopuolisia ohjelmistoja tai modeemeja?	☐	☐	☐

4. Toimintaympäristön, työ- ja palvelutilojen tietoturvallisuus

Tarkistuslista toimintaympäristöön ja toimitiloihin liittyvien tietoriskien tunnistamiseen.

Organisaatio:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa organisaation toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

4.1 Fyysinen turvallisuus

4.1.1 Kiinteistön turvallisuus

	Kyllä	Ei	Ei koske meitä
Onko kiinteistö altis onnettomuuksille? Sijaitseeko se lähellä rautatietä tai isoa valtatietä?	☐	☐	☐
Onko sähkönsyötön häiriöihin varauduttu?	☐	☐	☐
Onko kiinteistöllä suojelupäällikkö ja turvasuunnitelma?	☐	☐	☐
Onko kiinteistössä organisaatioita, joissa liikkuu paljon vieraita henkilöitä?	☐	☐	☐
Onko rakenteellinen suojaus palon, murron, vesivahingon ja sabotaasin varalta hoidettu?	☐	☐	☐
Onko kiinteistössä kulunvalvonta?	☐	☐	☐
Onko kiinteistössä vartiointi?	☐	☐	☐
Onko organisaation tiloihin pääsy suojattu kulunvalvonnalla?	☐	☐	☐
Onko kiinteistön yleisiin tiloihin, kuten puhelinkeskukseen, piha-alueelle, kellariin, katolle, asiaton pääsy estetty ja valvottu?	☐	☐	☐
Onko toimitiloissa kulunvalvonta ja vartiointi?	☐	☐	☐
Onko toimitiloissa hälytysjärjestelmää?	☐	☐	☐
Ovatko takaovet ja -ikkunat lukittu?	☐	☐	☐
Säilytetäänkö avaimia huolella?	☐	☐	☐

4.1.2 Toimitilojen turvajärjestelyt

	Kyllä	Ei	Ei koske meitä
Onko kulkuoikeuksien myöntäminen nimetty vastuuhenkilölle?	☐	☐	☐
Onko kulkeminen tiloissa rajattua ja valvottua?	☐	☐	☐
Onko muilla kuin työntekijöillä kulkuavaimet tiloihin?	☐	☐	☐
Onko työntekijöiden omin töiden tekeminen työpaikalla hallittua (ajat, kulkuoikeudet, valvonta)?	☐	☐	☐
Onko vierailusäännöt ja -käytännöt olemassa?	☐	☐	☐
Onko tärkeät laitteet, kuten työasemat ja palvelimet, sijoiteltu valvottuihin tiloihin?	☐	☐	☐
Onko tärkeät tilat sijoiteltu pois viemärien ja putkistojen lähistöltä?	☐	☐	☐
Ovatko laitetilat alttiita lämpötilan vaihteluille?	☐	☐	☐
Onko alkusammutuskaluston käyttöä harjoiteltu?	☐	☐	☐
Onko tulipalon varalle harjoiteltu tiloista poistumista?	☐	☐	☐

4.2 Tietoaineistoturvallisuus

4.2.1 Asiakaspalvelutilat

	Kyllä	Ei	Ei koske meitä
Pidetäänkö luottamukselliset tiedot poissa asiakaspalvelutiloista?	☐	☐	☐
Pidetäänkö tietokonepäätteet, kirjoittimet, faksit yms. poissa kulkuväyliltä?	☐	☐	☐
Onko asiakastilat sijoitettu siten, että asiakkaiden liikkumista voidaan valvoa?	☐	☐	☐
Ovatko neuvottelutilat ääni- ja näköeristettyjä?	☐	☐	☐
Huolehditaanko neuvottelutilojen siivouksesta siten, että vanhojen palaverien asiakirjat, fläpit ja piirtoheitinkalvot eivät jää tilaan?	☐	☐	☐
Onko asiakkaita varten suunniteltu esimerkiksi puhelin sellaiseen paikkaan, että sen käyttö ei aiheuta riskiä? (Ei esimerkiksi työhuoneeseen)	☐	☐	☐

4.3 Käyttöturvallisuus

4.3.1 Tietojen ja järjestelmien käyttöperiaatteet

	Kyllä	Ei	Ei koske meitä
Onko järjestelmien käyttöoikeuksien hallinta nimetty vastuu-henkilölle?	☐	☐	☐
Onko käyttöoikeuksien käsittely ja myöntäminen ohjeistettu?	☐	☐	☐
Onko jokaisella käyttäjällä oma käyttäjätunnus ja henkilö-kohtainen salasana?	☐	☐	☐

	Kyllä	Ei	Ei koske meitä
Onko työntekijöille rajattu pääsy vain omiin työtehtävän edellyttämiin tietoihin?	☐	☐	☐
Onko luottamuksellisille asiakirjoille ja muille tietovälineille lukitut kaapit?	☐	☐	☐
Onko luottamuksellisten tietojen hävittämiseen silppurit tai lukitut paperisäiliöt?	☐	☐	☐
Sallitaanko tietojen siirtely tietolevykkeillä (korput, kirjoittavat CD:t yms.)?	☐	☐	☐
Ovatko laitteet, ohjelmistot ja tiedot kirjattu omaisuusrekisteriin?	☐	☐	☐
Onko turvalliset etätyötavat ohjeistettu?	☐	☐	☐

5. Tietojärjestelmien suojaus

Tarkistuslista tietojen ja järjestelmien teknisten suojakeinojen kehittämiseen.

Organisaatio:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Arvioi tietojen käsittely- ja menettelytapoja kaikessa organisaation toiminnassa. Arviointiasteikko: kyllä = asia on kunnossa, ei = asia täytyy selvittää. Kirjaa perustelut, lisätiedot ja päätökset asioiden hoitamisesta erilliselle paperille tai esimerkiksi työvälinesarjaan sisältyvälle riskienhallintatoimenpiteiden yhteenvetolomakkeelle, jotta ne eivät unohdu.

5.1 Tietoliikenneturvallisuus

	Kyllä	Ei	Ei koske meitä
Toimivatko modeemiyhteydet takaisinsoittoperiaatteella?	☐	☐	☐
Onko asiaton pääsy ja muu asiaton verkkoliikenne organisaation verkkoon estetty?	☐	☐	☐
Ovatko paikallisverkko, extranet- ja WWW-palvelimet eristetty toisistaan riittävästi?	☐	☐	☐
Tarkistetaanko sähköpostiliitteiden asianmukaisuus ja virukset ennen pääsyä organisaation verkkoon?	☐	☐	☐
Tarkistetaanko lähtevät sähköpostiliitteet?	☐	☐	☐
Suojataanko kannettavat tietokoneet kattavasti? (niin että varkaat eivät pääse tietoihin käsiksi)	☐	☐	☐

5.2 Ohjelmistoturvallisuus

5.2.1 Ohjelmistot

	Kyllä	Ei	Ei koske meitä
Hankitaanko ohjelmistot, laitteet ja muu tuki osaavilta toimittajilta?	☐	☐	☐
Onko käytössä vain lisensoidut lailliset ohjelmistoversiot?	☐	☐	☐
Onko laadittu järjestelmäkehityksen tietoturvasuunnitelma?	☐	☐	☐
Otetaanko hankintojen yhteydessä huomioon ohjelmistojen turvallisuus ja luotettavuus? (Tietojen hankinta luotettavuudesta, oma testaus)	☐	☐	☐
Ovatko tietojen varmistuskäytännöt vastuutettu ja suunniteltu?	☐	☐	☐
Onko harjoiteltu varmistusten palautusten onnistumista?	☐	☐	☐
Onko paloturvakaappi tietojen varmistuksille?	☐	☐	☐
Onko kaikissa työasemissa virustorjunta?	☐	☐	☐

	Kyllä	Ei	Ei koske meitä
Onko virustentorjuntaohjelmiston ajantasaisuudesta huolehtiminen vastuutettu?	☐	☐	☐
Tapahtuuko työasemien virustentorjuntaohjelmistojen ja vastaavien päivitys automaattisesti?	☐	☐	☐

5.3 Tietoaineistoturvallisuus

5.3.1 Tietojen ja järjestelmien käyttöperiaatteet

	Kyllä	Ei	Ei koske meitä
Onko järjestelmien käyttöoikeuksien hallinta nimetty vastuuhenkilölle?	☐	☐	☐
Onko käyttöoikeuksien käsittely ja myöntäminen ohjeistettu?	☐	☐	☐
Onko jokaisella käyttäjällä oma käyttäjätunnus ja henkilökohtainen salasana?	☐	☐	☐
Onko työntekijöille rajattu pääsy vain omiin työtehtävän edellyttämiin tietoihin?	☐	☐	☐
Onko luottamuksellisille asiakirjoille ja muille tietovälineille lukitut kaapit?	☐	☐	☐
Onko luottamuksellisten tietojen hävittämiseen silppurit tai lukitut paperisäiliöt?	☐	☐	☐
Sallitaanko tietojen siirtely tietolevykkeillä (korput, kirjoittavat CD:t yms.)?	☐	☐	☐
Onko laitteet, ohjelmistot ja tiedot kirjattu omaisuusrekisteriin?	☐	☐	☐
Onko turvalliset etätyötavat ohjeistettu?	☐	☐	☐

5.4 Käyttöturvallisuus

5.4.1 Teknisen ympäristön hallinta ja valvonta

	Kyllä	Ei	Ei koske meitä
Onko tietotekniset turvatehtävät vastuutettu?	☐	☐	☐
Vastaavatko teknisen ympäristön ylläpidosta henkilöt, joilla on siihen riittävä tekninen osaaminen?	☐	☐	☐
Onko sähköpostipalvelimien asennus ohjeistettu?	☐	☐	☐
Onko järjestelmien ylläpidosta vastaavat koulutettu tietoriskien hallintaan ja järjestelmien suojaamiseen?	☐	☐	☐
Ovatko varahenkilöt tietoisia nykykäytännöistä?	☐	☐	☐
Onko tietojärjestelmäsuunnittelijoilla valmius ennakoida järjestelmää uhkaavat tilanteet ja suunnitella ja arvioida tarpeellisia suojaustapoja?	☐	☐	☐
Seurataanko järjestelmän virheitä ja levytilojen täyttymistä?	☐	☐	☐
Seurataanko järjestelmän käyttöä ja puututaanko siihen tarvittaessa?	☐	☐	☐

5.4.2 Teknisen järjestelmä hankinta, huolto, muutokset ja poisto käytöstä

	Kyllä	Ei	Ei koske meitä
Otetaanko tietoturvaasiat huomioon laitehankinnoissa?	☐	☐	☐
Onko varauduttu teknisten järjestelmien rikkoutumiseen (varaosien saatavuus, kahdennus, varajärjestelmät, korvaavat toimintatavat)?	☐	☐	☐
Käytetäänkö luotettavia huoltoyrityksiä, joiden kautta tiedot eivät ole vaarassa joutua kolmansille osapuolille?	☐	☐	☐
Onko tekninen ympäristö ja sen muutokset dokumentoitu?	☐	☐	☐
Onko tietojen hävitysmenettely olemassa, jos laitteita myydään työntekijöille tai ulkopuolisille?	☐	☐	☐

5.4.3 Tekniset suojaamiskeinot

	Kyllä	Ei	Ei koske meitä
Onko suojaamiskeinojen kattavuus tarkistettu / auditoitu?	☐	☐	☐
Onko järjestelmien käyttö ilman käyttäjän luotettavaa yksilöintiä estetty?	☐	☐	☐
Ovatko tietojen varmistukset automaattiset ja aukottomat?	☐	☐	☐
Onko UPS-laitteita varasähkön varmistamiseksi?	☐	☐	☐
Salakirjoitetaanko työasemilla ja palvelimilla olevat tiedot ja sähköpostiliikenne?	☐	☐	☐
Vaatiiko käyttöä valvova ohjelmisto salasanalle tietyn määrä-muotoisuuden ja salasanan ennalta ajoitetun vaihtamisen?	☐	☐	☐
Tarkistetaanko työntekijöiden salasanojen muoto ja turvallisuus ajoittain?	☐	☐	☐
Jääkö järjestelmän lokitiedostoihin merkintä järjestelmän käyttäjistä?	☐	☐	☐
Rajataanko ulkopuolisilta pääsy organisaation verkkoon?	☐	☐	☐

POTENTIAALISTEN ONGELMIEN ANALYYSI

Potentiaalisten ongelmien analyysissa on useita vaiheita. Analyysi laaditaan ryhmätyönä vastuullisen vetäjän johdolla. Kohteen koosta riippuen joudutaan pitämään useampiakin analyysikokouksia, joiden tyypillinen kesto on 2–4 tuntia kerrallaan. Analyysin vaiheet on esitetty taulukossa 3.

Taulukko1. Potentiaalisten ongelmien analyysin vaiheet

Uhkien ja vaarojen tunnistaminen aivoriihessä	Osa 1, hiljainen aivoriihi ● Ideointilomakkeen ja avainsanojen käyttö ● Kiinnitetään erityistä huomiota suuriin merkittäviin vaaralähteisiin ja seurauksiltaan vakaviin uhkiin Osa 2, keskustelumuotoinen aivoriihi **Järjestelmällinen eteneminen kohde kohteelta (esimerkiksi tarkasteltava prosessin tai alueen mukaan)**
	TULOSTE: Vaaraluettelo
Uhkien ja vaarojen arviointi	Osa 1, jatkokäsiteltävien uhkien valinta Osa 2, käsiteltäviksi valittujen uhkien syiden ja seurausten selvittäminen ja riskin suuruutta kuvaavan tunnusluvun arviointi ● järjestelmällinen käsittely analyysityöryhmässä ● analyysilomakkeen käyttö
	TULOSTE: Alustavat analyysilomakkeet (uhkat ja vaarat syineen ja seurauksineen sekä riskien arviointi analyysilomakkeelle kirjattuina)
Toimenpide-ehdotusten kehittäminen	**Järjestelmällinen tarkastelu arvioinnin yhteydessä tai erillisessä kokouksessa.**
	TULOSTE: Lopulliset analyysilomakkeet
Analyysin raportointi	**TULOSTE: Loppuraportti, jonka liitteinä ovat uhka- ja vaaraluettelo ja analyysilomakkeet**

Analyysin valmistelu

Analyysin toteutuksen edellytyksenä on, että organisaation johto antaa tukensa ja myöntää resurssit analyysin laadintaan. POA aloitetaan valitsemalla ja rajaamalla tarkasteltava kohde. Valintaperusteet ja kohteen rajaukset on hyvä esitellä tarkastelun loppuraportissa. Esimerkiksi tietojärjestelmän osaan kohdistuva riskianalyysi voi koskea seuraavia osatekijöitä:

- Tietoturvaarkkitehtuuri
- Tietojen säilyttäminen ja käyttö
- Sovellus tai sovellukset, ohjelmat
- Käyttöympäristö (palvelimet, työasemat, tietoliikenne)
- Fyysinen ympäristö
- Henkilöstö
- Ulkoisten palveluiden käyttö
- Hankinnat.

Analyysin onnistuminen vaatii siihen nimetyn vastuullisen vetäjän. Hänen ei tarvitse olla kohteen asiantuntija vaan ennen kaikkea POA-menetelmän asiantuntija, joka pystyy johtamaan varsinaisten kohteen asiantuntijoiden analyysityöskentelyä. Usein ns. työpaikkasokeus haittaa analyysityöskentelyä. On todettu, että ulkopuolinen vetäjä esimerkiksi naapuriosastolta, organisaation toisesta yksiköstä tai jopa ulkopuolinen konsultti pystyy johtamaan tarkastelua paremmin ilman ”*näin-on-aina-tehty*” ja *”meillä-ei-ole-koskaan-sattunut-mitään”* - asennetta.

Vetäjän tehtäviä ovat mm.

- Kohteesta tarvittavan tiedon hankkiminen
- Työryhmän kokoaminen
- Toteutussuunnitelman ja kokousaikataulun laatiminen
- Työryhmän perehdyttäminen analyysimenetelmään
- Työryhmäkokousten vetäminen
- Tulosten raportointi ja tiedottaminen
- Jatkotoimenpiteiden suunnittelun organisointi.

Tarkasteltavan kohteen laajuudesta ja monimutkaisuudesta riippuen kohde voidaan jakaa pienempiin osiin, joita tarkastellaan kutakin erikseen. Jako voidaan tehdä esimerkiksi toiminnan luonteen tai maantieteellisten tai rakennusteknisten seikkojen perusteella.

Analyysityöryhmän perustaminen

Varsinainen analysointi tehdään työryhmässä. Sen suositeltava koko on vetäjän lisäksi 3–6 henkeä. Ryhmään valitaan henkilöitä, joilla on aikaa osallistua analyysi-

projektiin ja joilla on hyvä käsitys kohteen toiminnasta ja valmius keskustella asioista rakentavassa hengessä. Ryhmän kokoonpano vaihtelee sen mukaan, minkä alueen riskianalyysin tekemisestä on kysymys, esimerkiksi tehdäänkö riskianalyysi koko organisaation tietoturvallisuudesta vai jostakin tietoturvallisuuden osa-alueesta. Tärkeää kuitenkin on, että ryhmässä ovat kattavasti mukana kaikki tarvittavat tahot.

Ryhmän kokoa ei tule paisuttaa tarpeettomasti. Jos ryhmän asiantuntemus ei riitä johonkin yksityiskohtaan, voidaan asia selvittää kokousten välillä tai kyseisen ongelman käsittelyn ajaksi paikalle kutsutaan asiantuntija.

Kun analyysityöryhmä on perustettu, voidaan yhdessä tutustua tarkasteltavaan kohteeseen. Jos kohde on pieni ja kaikille tuttu, ei erillistä tutustumista tarvita.

Analyysin laatiminen työryhmässä

Varsinainen analyysi laaditaan kahdessa vaiheessa. Ensin aivoriihessä kerätään mahdollisia ongelmia ja uhkia. Sen jälkeen ideat järjestellään ja luokitellaan. Toisen vaiheen analyysi-istunnoissa jatkokäsiteltäviksi valittuja uhkia tarkastellaan yksityiskohtaisemmin. Tässä vaiheessa mietitään uhkien syitä ja seurauksia, määritellään riskiluku sekä arvioidaan nykyisen varautumisen riittävyyttä ja kehitetään tarvittaessa parannustoimenpide-ehdotuksia.

Aivoriihi

Aivoriihen tavoitteena on saada paljon ideoita. Lennokkaat, villit ideat ovat tervetulleita. Periaatteena on, että ideoiden arvostelu on kielletty koko ideoinnin ajan. Ideoinnissa toivotaan jatkoideoita, parannuksia ja yhdistelmiä muiden ideoista. Kaikki ideat kirjataan heti paperille.

Idean pitää olla riittävän yksityiskohtainen ja siinä tulisi selvästi olla uhkan syy ja onnettomuuteen tai häiriöön johtava tapahtumaketju.

Ongelmien ja uhkien ideointiin aivoriihessä käytetään idealomaketta. Jokaiselle jaetaan lomake ja kukin kirjoittaa kolme uhkaa tai ongelmaa. Sen jälkeen lomaketta kierrätetään analyysityöryhmässä seuraavalle. Luettuaan edelliset ideat hän kirjoittaa jälleen kolme ideaa. Ne voivat olla uusia tai ne voivat olla aiemmin kirjoitetuista ideoista jatkokehiteltyjä. Näin lomakkeita kierrätetään, kunnes lomakkeet ovat täynnä tai ideat tyrehtyvät. Ideoinnin apuna voidaan käyttää avainsanoja tai tarkistuslistoja.

Normaalisti ideoinnin aikana ei kirjatuista ideoista keskustella, ainoastaan vetäjä ohjaa lomakkeiden vaihtoa ja esittelee mahdolliset avainsanat. Usein kannattaa hiljaisen aivoriihen lopuksi kuitenkin vielä yhdessä keskustellen miettiä lisää uhkia tai kehittää edelleen jo esiin tulleita vaaroja. Tässä vaiheessa ei kuitenkaan ole tarkoitus kehitellä parannustoimenpide-ehdotuksia. Syyttely ja selittely eivät kuulu tämän ana-

lyysin periaatteisiin. Keskustelussa kannattaa edetä järjestelmällisesti esimerkiksi prosessin tai materiaalien kulun mukaisesti.

Ideoiden luokittelu

Normaalisti ideoita kertyy runsaasti, ja osa niistä on käytännössä mahdottomia tai niin vähäisiä, että niitä ei kannata tarkastella yksityiskohtaisemmin. Kuitenkin myös epätodennäköisiä, lähes mahdottomina pidettäviä mahdollisuuksia tulee arvioida. Mahdottomilla asioilla on ikävä taipumus toteutua. Ideat on hyvä luokitella ja lajitella esimerkiksi seuraavan luokittelun mukaisesti:

1. Jatkokäsittelyä edellyttävät uhkat
2. Vanhat ja luotettavasti hoidossa olevat uhkat
3. Vailla käytännön merkitystä olevat uhkat.

Vaikka jatkokäsittelyyn valitaankin vain osa tunnistetuista uhkista, ei muitakaan pidä hylätä. Vähintäänkin ne esitetään analyysin loppuraportin liitteenä olevassa uhkaluettelossa. Myöhemmin esimerkiksi seurantakokouksissa on hyvä tarkistaa idealuettelo ja arvioida, onko siinä vielä sellaisia uhkia, joita tulisi käsitellä tarkemmin.

Uhkien arviointi ja riskiluvun määritys

Jatkokäsittelyyn valittuja ideoita tarkastellaan yksityiskohtaisesti analyysityöryhmässä. Analyysin vetäjä johtaa puhetta ja esittelee kulloinkin käsiteltävän uhkan. Kuten ideoinnin keskusteluvaihe, myös yksityiskohtainen tarkastelu etenee prosessin kulun tai materiaalivirtojen mukaisesti.

Analyysin tulokset kirjataan ensimmäisessä vaiheessa analyysilomakkeelle, jossa on sarakkeet uhkaa, sen syitä, varautumista, seurauksia, riskilukua ja toimenpide-ehdotuksia varten.

Ensin arvioidaan missä tilanteessa tai olosuhteissa kussakin ideassa kuviteltu uhka on mahdollinen. Tarkoitus on tunnistaa syitä, tilanteita ja olosuhteita, jotka mahdollistavat uhkan toteutumisen. Missään vaiheessa ei haeta syyllisiä. Uhkan kuvaamisen jälkeen arvioidaan seurauksia, eli kuinka suuria vahinkoja se voisi aiheuttaa. Kannattaa miettiä erikseen todennäköisiä seurauksia ja pahimpia mahdollisia seurauksia.

Riskin arviointi

Kaikkiin uhkien tunnistamismenetelmiin voi liittää myös riskin määrittelyn karkealla tasolla. Kun uhkan syyt on tunnistettu ja seuraukset arvioitu, voidaan kyseisen riskin suuruus määritellä. Riskin suuruuteen vaikuttavat tapahtuman todennäköisyys ja seurausten vakavuus.

Yksinkertainen karkea luokittelu on usein helpompi laatia, ja se antaa hyvän kuvan eri riskien keskinäisistä eroista. Riskin suuruuden määrittämiseen käytetty aika ei lisää eikä vähennä riskiä. Sen vuoksi ei kannata uhrata liikaa aikaa riskilukuihin.

Varautuminen

Riskin arvioinnin jälkeen arvioidaan tarkasteluhetken varautumista kyseiseen tilanteeseen. Jos varautumista ei joiltain osin pidetä riittävänä, tehdään parannustoimenpide-ehdotuksia. Kun yksi tunnistettu uhka on käsitelty loppuun, jatketaan käsittelyä seuraavan uhkan osalta edellä kuvatulla tavalla.

Raportointi

Jotta analyysityöstä saadaan täysi hyöty, tulee tehty työ raportoida huolellisesti. Kirjaukset analyysilomakkeisiin tulee tehdä niin, että myöhemminkin niitä lukevalle selviää mistä on kysymys. Lomakkeiden lisäksi on hyvä laatia yhteenvetoraportti, jotta myöhemmin voidaan todeta, mitä on tehty, miten on tehty, ketkä analyysin tekemiseen ovat osallistuneet ja mitkä ovat analyysin keskeiset tulokset ja jatkosuunnitelmat. Tällöin analyysin hyödyntäminen ja päivittäminen myöhemmin on helpompaa.

POA analyysilomake

	KOHDE: Laatijat:	Analyysin pvm: Raportti: Sivu ( )

Vaaraa/uhkaa aiheuttava tilanne	Seuraukset	Riski	Nykyinen varautuminen	Toimenpide-ehdotukset/ lisäkysymyksiä

ESIMERKKEJÄ TOTEUTUNEISTA RISKEISTÄ

Tietokonevika tuhosi kirjanpitotiedot

Tietokoneen kiintolevyn rikkoutumisen vuoksi kunnan taloushallinto ja kirjanpito jouduttiin päivittämään uudelleen vuoden ajalta. Tietojen varmennustallennus ei myöskään ollut toiminut, vaan nauhuriaseman nauhat olivat tyhjentyneet.

Vioittuneen kiintolevyn tietoja yritettiin palauttaa yrityksessä, joka on erikoistunut rikkoutuneiden kiintolevyjen käsittelyyn. Tämä ei kuitenkaan onnistunut.

Tapauksen jälkeen palvelimeen asennettiin kaksi identtistä kiintolevyä sekä nauhavarmistus.

Tietokonevirus aiheutti pankin konttorien sulkemisen

Kymmeniä pankin konttoreita jouduttiin sulkemaan tietokoneviruksen vuoksi. Virus aiheutti työasemien jatkuvan uudelleenkäynnistymisen ja esti näin työasemien käytön. Viruksen arvioitiin päässeen järjestelmään verkkoon kytketyn kannettavan tietokoneen kautta.

Sairastuneen tietoihin ei päästä käsiksi

Asiakkaiden sopimustietojen ylläpitäjä oli sairastunut eikä häntä tavoitettu. Hänen työasemansa kiintolevyltä oli tarve saada käyttöön pikaisesti erään asiakkaan sopimustiedot. Vastuuhenkilö oli suojannut tiedot salasanallaan.

Kopiokone ja telefax julkisissa tiloissa

Organisaation kopiokone ja telefax olivat tilanpuutteen vuoksi sijoitettuna organisaation käytävälle, jossa liikkuu jatkuvasti asiakkaita ja muiden yritysten henkilöstöä. Kopiokoneen päällä oli kopioitavaksi tarkoitettu tulevan kauden strategiat ja juuri muutetut hinnoitteluperiaatteet. Telefaxin paperikaukalo oli täynnä tulleita telekopioita.

Kutsut väärään osoitteeseen

Sihteeri lähetti kahden tilaisuuden palaverikutsuja. Osoitteet menivät ristiin, ja kutsujen liitteenä olevat luottamukselliset tiedot menivät vääriin osoitteisiin.

Projektin tiedot vuotavat

Organisaation toimintaan liittyvästä hankkeesta julkaistiin tietoja lehdistössä. Hank-

keen luottamuksellisuudesta johtuen toimittajilla ei pitäisi olla tietoa hankkeesta eikä henkilöstön tulisi kertoa tietoja hankkeesta.

Lisenssitön ohjelmistojen käyttö

Organisaatiossa on käytössä ohjelmia, joille ei ole riittävästi laillisia lisenssejä. Organisaatiosta riitaisesti eroava henkilö ilmiantaa ohjelmistojen käytön valvontaviranomaisille.

MÄÄRITELMÄT

Luottamuksellisuus

1) Tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta.

2) Se, missä määrin luottamuksellisuutta pidetään tärkeänä.

Eheys

1) Tietojen tai tietojärjestelmän aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus.

2) Ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

Käytettävyys

Ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuilla saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Todennus

1) Varmistuminen kohteen todenmukaisuudesta, oikeellisuudesta tai alkuperästä.

2) Järjestelmän käyttäjän (henkilön, organisaation tai laitteen) tai viestinnässä toisen osapuolen aitouden varmistaminen

Kiistämättömyys

Tietty henkilö on lähettänyt tietyn viestin (alkuperän kiistämättömyys),vastaanottanut tietyn viestin (luovutuksen kiistämättömyys),tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi.

Riski

1) Todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai vahingon.

2) Uhkaan liittyvän vahingon rahallinen arvo tai odotusarvo (=arvo x todennäköisyys).

Riskianalyysi

Systemaattisin menetelmin tapahtuva uhkien ja riskien arviointi.

Riskienhallinta

Järjestelmällinen toiminta riskien rajoittamiseksi niin, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun organisaation toiminnalle asetetut tavoitteet voidaan saavuttaa.

Riskienhallinnan vaiheita ovat riskianalyysi, riskienhallintamenetelmän valinta, päätös riskien poistamisesta, alentamisesta tai pitämisestä omalla vastuulla, sekä riskienhallinnan organisointi.

Tietoturvariski

Tietoon, tietoliikenteeseen tai tietojärjestelmään kohdistuva vahingon vaara.

Tietoturvallisuus

1) Tavoitetila, jossa tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa niin, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhat eivät aiheuta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille.

2) Lainsäädäntö ja muut normit sekä toimenpiteet, joiden avulla pyritään varmistamaan tietoturvallisuus (1) niin normaali kuin poikkeusoloissa.

Tietoturvallisuuden toteuttamisessa on tapana erottaa kahdeksan toimenpidealuetta: hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus.

Haavoittuvuus

Alttius tietoturvallisuutta uhkaaville tekijöille.

Uhka

Tietoihin tai tietojärjestelmään tietyltä taholta kohdistuvan vahingon tai häiriön mahdollisuus.

Vahinko

Aiheuttajaansa yhdistettävissä oleva menetys, kuten fyysisen tai aineettoman omaisuuden häviäminen, toiminnan tulosten tai edellytysten heikkeneminen, ihmisen tai luonnon elinolosuhteiden huononeminen.

VALTIOVARAINMINISTERIÖN JA VAHTIN TIETOTURVAOHJEISTOA

- Ohje riskien arvionnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
- Opas julkishallinnon tietoturvakoulutuksen järjestämisestä, VAHTI 6/2003
- Käyttäjän tietoturvaohje, VAHTI 5/2003
- Valtionhallinnon tietoturvakäsitteistö, VAHTI 4/2003
- Tietoturvallisuuden hallintajärjestelmän arviointi, VAHTI 3/2003
- Turvallisen etäkäytön arkkitehtuuri. VAHTI 2/2003
- Tunnistaminen valtionhallinnon verkkopalveluissa, VM 6/01/2003
- Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003
- Arkaluonteisten kansainvälisten aineistojen käsittelyohje, VAHTI 4/2002
- Etätyön tietoturvaohje, VAHTI 3/2002
- Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002
- Tietotekniikan turvallisuus ja toiminnan varmistaminen, VM ja PTS, 2002
- Toimet tietoturvaloukkaustilanteissa, VAHTI 7/2001
- Tietotekniikkahankintojen tietoturvallisuustarkistuslista, VAHTI 6/2001
- Sähköpostin ja lokitietojen käsittely, VAHTI 5/2001
- Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001
- Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001
- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
- Tietokoneviruksilta ja muilta haittaohjelmistoilta suojautumisen yleisohje, VAHTI 4/2000
- Tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000
- Valtion tietoaineistojen käsittelyn tietoturvaohje, VAHTI 2/2000
- Tarpeettomien tietoaineistojen hävittämisohje, VM 19.4.2000

- Valtionhallinnon tietoturvallisuuskäsitteistö, VAHTI 1/2000
- Tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje
- Tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, VAHTI 2/1999
- Suositus toimitilaturvallisuudesta, VM 31.12.1998
- Tietoturvallisuuden tulosohjaus ja kehittämisvälineet, VAHTI 2/1997

VAHTI

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

7/2003

OHJE RISKIEN ARVIOINNISTA TIETOTURVALLISUUDEN EDISTÄMISEKSI VALTIONHALLINNOSSA

ISSN 1455-2566
ISBN 951-804-408-2