Valtionhallinnon tietoturvallisuuden johtoryhmä

3/2002

VALTIONHALLINNON ETÄTYÖN TIETOTURVALLISUUSOHJE

SISÄLLYSLUETTELO

JOHDON YHTEENVETO

Etätyö on yleistynyt ja tulee edelleen yleistymään. Samalla on etätyön tietoturvallisuus noussut aiempaa merkittävämmäksi tekijäksi. Tekninen ja yhteiskunnallinen kehitys on nopeaa, joten uusia etätyömuotoja ja tietoturvallisuutta edistäviä ratkaisuja kehittyy jatkuvasti. Kehityksen seuranta auttaa toteuttamaan tietoturvallisen kokonaisuuden.

Lähtökohtana on, että etätyön tulee olla yhtä tietoturvallista kuin työn tekeminen viraston toimitiloissa.

Etätyön tietoturvallisuuden tulee olla osa normaalia tietoturvallisuustyötä: viraston johto määrittelee tietoturvallisuuspolitiikan, jonka toteuttamisessa viraston tietohallinto on keskeisessä asemassa.

Henkilöstön osaaminen, selkeät toimintamallit sekä toimivat, helppokäyttöiset ja helposti hallittavat tietoturvallisuusratkaisut luovat hyvät edellytykset tietoturvalliselle etätyölle.

Etätyön tietoturvallisuus aiheuttaa laite- ja palvelukustannuksia sekä saattaa vaatia toimintatapojen ja prosessien merkittävääkin uudistamista.

Joidenkin tehtävien hoito etätyönä ei ole mahdollista ja joidenkin tekeminen puolestaan vaatii erityisjärjestelyjä. Tehtävien soveltuvuuden arviointi on tehtävä tapauskohtaisesti ottaen huomioon käsiteltävien tietojen luonne, etätyöympäristö sekä tietoturvallisuutta tukevien ratkaisujen sovellettavuus.

Etätyön tietoturvallisuus on laaja kokonaisuus, jonka voidaan katsoa toteutuvan vasta, kun koko ketju etätyöntekijästä ja etätyöympäristöstä viraston järjestelmiin ja tietoihin on turvattu. Turvallisuuden tasoa on valvottava teknisillä menetelmillä sekä hallinnollisilla toimilla, etenkin tarkastuksilla.

Tietoturvallisuutta on arvioitava riskianalyysillä. Ihminen on useimmiten kaiken tietoturvallisuuden heikoin lenkki, ja etätyössä tämä korostuu. Etätyöntekijän on tiedostettava vastuunsa koko viraston tietoturvallisuuden kannalta. Johdon on tuettava etätyöntekijää koulutuksella ja asianmukaisilla tietoturvallisuusratkaisuilla.

1 JOHDANTO

1.1 Hankkeen tausta

Valtiovarainministeriön asettama ja vetämä valtion tietoturvallisuuden johtoryhmä nimitti työryhmän valmistelemaan Valtion etätyön tietoturvallisuussuosituksen (1/1999) uusimista. Tarve ohjeen uusimisille on tullut teknisen kehityksen, etätyön yleistymisen ja etätyömuotojen monipuolistumisen myötä. Etätyön hallinnollisen tietoturvallisuuden osalta kehitys on ollut hitaampaa, eikä uudistustarve tältä osin ole ollut yhtä suuri. Ohjeen uusimisessa on näin ollen painotettu teknisiä asioita.

1.2 Ohjeen laatiminen

Ohjeen laatineen VAHTI:n alaisen työryhmän muodostivat:

Juhani Sillanpää	Valtiovarainministeriö	puheenjohtaja
Heikki Haukirauma	Työministeriö	
Risto Heinonen	Tietosuojavaltuutetun toimisto	
Anssi Juuti	Ilmatieteen laitos	
Kari Keskitalo	Kauppa- ja teollisuusministeriö	
Timo Larmela	Teknillinen korkeakoulu	
Minna Romppanen	Maa- ja metsätalousministeriön tietopalvelukeskus	
Pertti Saloranta	Oikeusministeriö	
Timo Tuomaila	Verohallitus	
Matti Viirret	Suojelupoliisi	

Konsulttityöstä vastasivat:

Tuomo Muhonen	HM&V Research Oy	
Petri Tötterman	HM&V Research Oy	
Olli-Pekka Soini	HM&V Research Oy	sihteeri

Työryhmä haastatteli etätyöntekijöitä, etätyön hallinnoinnista vastaavia sekä teknisiä asiantuntijoita. Haastattelun lisäksi tehtiin sähköpostikysely, jolla selvitettiin tietoturvallisuusohjeistuksen nykytilaa eri virastoissa ja tietoturvallisuusratkaisuista saatuja kokemuksia sekä saatiin taustatietoa.

VAHTI käsitteli ohjeluonnosta ja linjasi ohjeen valmistelua kokouksessaan toukokuussa 2002. Luonnokseen 31.5.2002 saatiin 44 lausuntoa, joiden pohjalta viimeisteltiin lopullinen ohje. VAHTI päätti ohjeen julkaisemisesta syyskuussa 2002.

1.3 Ohjeen tarkoitus ja rajaus

Ohje antaa suosituksia etätyön ja tietojärjestelmien etäkäytön tietoturvalliseen toteuttamiseen, mutta ei ota kantaa etätyön työoikeudellisiin, henkilöstöhallinnollisiin tai muihin vastaaviin kysymyksiin. Pääpaino on tietojärjestelmien turvallisessa etäkäytössä, mutta myös työpisteen fyysistä turvallisuudesta sekä paperimuodossa olevan tiedon käsittelystä annetaan ohjeita.

Ohjeistuksessa ei käsitellä puhelimen ja telekopiolaitteen käytön turvallisuuskysymyksiä.

Etätyötä tehdään hyvin monenlaisissa virastoissa. Etätyön menettelyt, etätyötä tekevien henkilöiden tietotekninen osaaminen ja virastojen toimintakulttuuri poikkeavat suuresti toisistaan. Ohjeessa annetut suositukset eivät kaikilta osin sovellu tilanteisiin, joissa etätyöntekijän tietotekninen ja tietoturvallisuusosaaminen on korkeatasoista. Toisinaan voi olla perusteltua poiketa tämän ohjeen suosituksista, mutta tämä on tehtävä tietoisesti: tietoturvallisuusvaatimukset vaihtelevat niin virastokohtaisesti kuin viraston sisällä työtehtävittäin.

Ohjeen suositukset on laadittu tasolle, josta ilmenee tietty tavoitteellisuus: työryhmä on esittänyt tietoturvallisuutta edistäviä ratkaisuja, jotka eivät vielä ole laajamittaisessa käytössä, mutta joiden käyttöönotto on suotavaa.

VAHTI:n olemassa olevaa ohjeistusta on hyödynnetty soveltuvin osin. Erityisesti Valtion viranomaisen tietoturvallisuustyön yleisohjetta (1/2001) sekä sähköpostin keskeisen merkityksen vuoksi Valtionhallinnon sähköpostien ja lokitietojen käsittelyohjetta (5/2001) suositellaan hyödynnettäväksi tämän ohjeen rinnalla.

1.4 Ohjeen rakenne

Ohjeessa käytetään termiä "virasto", jolla tarkoitetaan kaikkia valtionhallinnon organisaatioita niiden virallisista nimistä riippumatta.

Tietoturvallisuuden minimitason toteuttamiseen liittyvät asiat on ohjeessa esitetty käskevässä muodossa ja virastokohtaisesti harkittavat täydentävät asiat on ilmaistu lievemmällä kieliasulla.

Ohjeen rakenne on kolmikantamalli, jossa kullekin etätyön keskeisimmistä osapuolista (työntekijä, tietohallinto ja johto) on suunnattu oma lukunsa. Tietohallinnon edustajille tarkoitetuissa luvuissa tietoturvallisuutta on käsitelty valtionhallinnossa vakiintuneen kahdeksankohtaisen jaottelun mukaan.

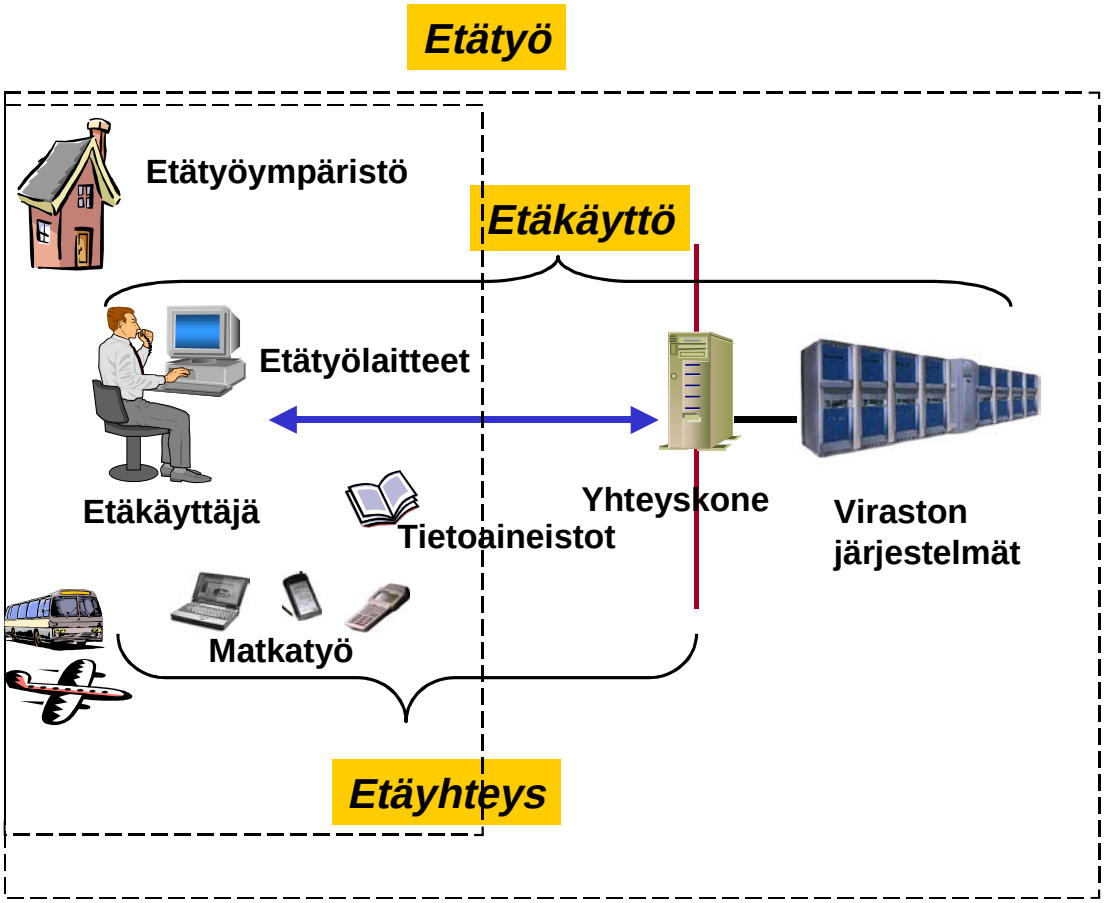
Luku 2 on suunnattu viraston johdolle. Siinä otetaan esiin etätyön ja etäkäytön yhteydet muuhun tietoturvallisuustyöhön ja viraston muuhun toimintaan. Johdon osuuteen on koottu keskeisimmät seikat, joita tulee arvioida etätyötä harkittaessa.

Tietohallinnolle on laadittu luku 3, jossa asioita käsitellään laajasti, esitellään erilaisia vaihtoehtoja sekä arvioidaan niiden hyviä ja huonoja puolia. Tietohallinnon on kyettävä toteuttamaan etätyön ja etäkäytön tarvitsemat tietotekniset tietoturvalliset ratkaisut. Tietohallinnon on myös voitava avustaa viraston johtoa tietoturvallisuuteen liittyvissä linjaratkaisuissa.

Etätyöntekijälle on luvussa 4 tiivis yksinkertainen ohjeistus.

1.5 Käsitteet

Etäyhteys	=	Tietoliikenneyhteys viraston sisäverkon ulkopuolelta
Etäkäyttö	=	Tietoteknisten palvelujen käyttö etäyhteyden avulla
Etätyö	=	Muualla kuin viraston vakituisessa toimipisteessä suoritettava työ
Uhka	=	Tietoihin tai tietojärjestelmään kohdistuvan vahingon tai häiriön mahdollisuus
Riski	=	Uhan toteutumisesta aiheutuvan menetyksen odotusarvo, johon vaikuttavat uhan realisoitumisen todennäköisyys ja tällöin tapahtuvien vahinkojen arvo



Kuva 1. Käsitteiden etätyö, etäkäyttö ja etäyhteys erot. Etätyö ei kuitenkaan edellytä viraston järjestelmien etäkäyttöä, ja on mahdollista etäkäyttää järjestelmiä tekemättä etätyötä.

2 ETÄTYÖN TIETOTURVALLISUUSPERIAATTEET

Viraston johdon tehtävänä on määritellä tietoturvallisuuspolitiikka, antaa politiikan totuttamisesta vastaaville riittävät resurssit tämän toteuttamiseen ja valvoa politiikan toteutumista. Etätyön kannalta tämä tarkoittaa, että etätyön tietoturvallisuuden erityiskysymykset on ratkaistava viraston tietoturvallisuuspolitiikan mukaisesti.

Etätyössä on enemmän tietoturvallisuusuhkia kuin toimistotyössä ja niiden hallinta on vaikeampaa.

2.1 Etätyön edellytykset

Etätyön tietoturvallisuuden edellytykset vaihtelevat virastokohtaisesti. Tässä käsitellään yleisiä vaatimuksia, jotka soveltuvat useimmissa tapauksissa arvioinnin pohjaksi.

Kaikkea virastossa tehtävää työtä ei voida tehdä tietoturvallisesti etätyönä. Nämä työt on kyettävä tunnistamaan. Töiden erottelu asettaa vaatimuksia paitsi etätyötä tekeville henkilöille myös asian- ja asiakirjojen käsittelyjärjestelmille, joihin on tarvittaessa rakennettava tätä tukevia ominaisuuksia. Töiden jaottelu niissä käsiteltävän tietoaineiston luottamuksellisuuden perusteella on eräs mahdollinen luokitteluperuste.

Etätyötä tekevän henkilöstön on kyettävä toimimaan annettujen ohjeiden mukaan ja osattava soveltaa ohjeita uusiin tilanteisiin. Henkilöiden on kyettävä tekemään itsenäiset arviot etätyöympäristön tietoturvallisuudesta ja heidän on omattava ainakin kohtuulliset valmiudet etätyön vaatiman tietotekniikan hallintaan. Henkilöille on annettava riittävästi koulutusta ennen etätyön aloittamista. Tietotekniikan kehitys tulee ratkomaan tämän päivän ongelmia, mutta todennäköisesti syntyy uusia turvallisuusuhkia. Käyttäjille asetettavat vaatimukset muuttuvat ja todennäköisesti kasvavat. Kun epäillään tietoturvallisuuden vaarantuneen, on työntekijöiden toimittava tilanteesta annettujen ohjeiden mukaan.

Käyttäjille on järjestettävä riittävän kattava etätyön käyttäjätuki. Minimissään tämä on päivystävä puhelinnumero, mutta mitä laajempaa ja yleisempää etätyö on, sitä suuremmat ovat tarpeet käyttäjätuelle.

Tietohallinto vastaa yleensä etätyössä tarvittavien laitteiden ja ohjelmien hankinnasta, ylläpidosta ja hävittämisestä. Tietohallinnon on kyettävä hallitsemaan etäkäytön vaatimien teknisten ratkaisujen hallinnointi. Koulutus, yhteistyö muiden virastojen kanssa ja ratkaisujen kokeilu ovat keinoja tämän saavuttamiseen. Tilanteessa, jossa etäkäytön vaatimien teknisten ratkaisujen hallinnointi on ulkoistettu, tietohallinnon on kyettävä valvomaan tietoturvallisuuden toteutumista.

Etätyöntekijöiden vaatima tuki sekä etätyössä käytettävien laitteiden ja ohjelmien ylläpito sitoo tietohallinnon resursseja. Tämä seikkaa saattaa olla aluksi merkitykseltään vähäinen, mutta etätyön yleistyessä se saattaa kuormittaa tietohallinnon resursseja merkittävästi.

2.2 Riskianalyysi[1]

Etätyön riskianalyysissä arvioidaan etätyöhön kohdistuvia riskejä, näiden todennäköisyyksiä ja vaikutuksia sekä valitsemaan vastakeinot, joilla riski kyetään saattamaan halutulle tasolle. Mikäli riskejä ei saada riittävän pieniksi, ei kyseistä työtä voida tehdä etätyönä. Erityisen huolellisesti tulee ar-

[1] Riski- ja haavoittuvuusanalyysiä on käsitelty Valtion viranomaisen tietoturvallisuustyön yleisohjeessa (VAHTI 1/2001).

vioida mahdollinen henkilötietoihin liittyvä etätyö.

Viraston johdon ei yleensä tule arvioida yksittäisten työtehtävien soveltuvuutta vaan pitäytyä yleisissä kriteereissä, joiden perusteella työtehtävien arviointia voidaan tehdä.

Riskien arvioinnissa voidaan hyödyntää tärkeimpiä etätyön tietoturvallisuusuhkia käsittelevää liitettä.

On kuitenkin arvioitava, millaisiin toimenpiteisiin hyökkääjä on valmis ryhtymään saadakseen salasanoja tai viraston salassa pidettäviä tietoja haltuunsa.

2.3 Politiikka

Etätyölle voidaan laatia erillinen etätyön tietoturvallisuuspolitiikka, mutta useissa tapauksissa voidaan soveltaa viraston yleistä tietoturvallisuuspolitiikkaa. Etätyön tietoturvallisuuspolitiikan ja muiden dokumenttien laadinta suositellaan tehtäväksi yhteistyössä tietohallinnon kanssa. Politiikan tekotavasta riippumatta viraston johto kantaa lopullisen vastuun sen toteutuksesta ja toteutuksen valvonnasta. Mikäli laaditaan erillinen politiikka voidaan siinä käsitellä seuraavia asioita:

- Ketkä saavat etätyötä tehdä sekä millaista työtä etätyönä saa tehdä ja mitä ei saa tehdä? Tietoturvallisuuden kannalta etätyöhön soveltuvia ovat esimerkiksi työt, joissa käsitellään vain julkisia tietoaineistoja.
- Etätyössä käytettävien järjestelmien osalta on ratkaistava, saako niihin ottaa yhteyden muulta kuin työnantajan laitteelta. Mikäli saa, on ratkaistava kysymys vaaditaanko laitteelta samoja turvallisuusominaisuuksia kuin viraston laitteilta. Kuitenkin työntekijä vastaa laitteen tietoturvallisuudesta. Tietohallinnon on tällöin annettava tukea tarvittavien ohjelmistojen asennukseen ja ylläpitoon.
- Käyttäjä-, laitteisto- ja ohjelmistotuen järjestäminen on ratkaistava. Tuki voidaan ulkoistaa, se voidaan antaa osana normaalia tietotekniikkatukea, tai se voidaan antaa yhteistyössä jonkin toisen viraston kanssa.
- Tietoaineistojen käsittely kolmannen osapuolen hallussa olevilla ohjelmilla on yleistynyt. Etätyön tietoturvallisuuspolitiikassa voidaan ottaa kantaa, millaisen aineiston käsittely Internetissä tarjottavilla palveluilla on sallittua.
- Etätyöntekoa voidaan ajallisesti rajoittaa tietoturvallisuusseikkojen perusteella.
- Etätyöhön käytettävälle laitteelle ja siihen asennetuille ohjelmille voidaan asettaa vaatimuksia, joita voidaan tarvittaessa porrastaa. Tietokoneessa tarvitaan virustentorjuntaohjelma, jonka päivitykset on syytä hoitaa automaattisesti. Hajautettua palomuuria ja kovalevyn salausta voidaan edellyttää, mikäli riski luvattomasta tietojärjestelmiin tunkeutumisesta tai laitteen anastamisesta on suuri.
- Sallitut yhteysmuodot ja niiden edellyttämät turvatoimet on ratkaistava. Virasto voi rajoittaa tai kieltää tietoliikenneyhteyksiä etätyöhön käytettävään laitteeseen. Mikäli työntekijälle sallitaan muita kuin etätyön tekemiseen käytettäviä yhteyksiä (yleinen Internet-yhteys, yhteydet muiden virastojen järjestelmiin), on näistä sovittava tapauskohtaisesti.
- Etäkäyttäjien tunnistamisessa vaadittavat menettelyt voivat vaihdella käytettävän järjestelmän mukaan. Yksinkertaisen käyttäjätunnus-salasana -tunnistautumisen antama suoja on varsin heikko. Tämän menetelmän sijaan suositellaan käytettäväksi vaihtuvia tai kertakäyt-

töisiä salasanoja. Vahvan tunnistuksen menetelmiä tulee suosia, mikäli käytettävien järjestelmien tietoturvallisuusvaatimukset ovat korkeat ja mikäli vahvan tunnistuksen käytännön toteutus kyetään tekemään riittävän toimivaksi. Toimivuuden arvioinnissa on painotettava järjestelmän käytettävyyttä etäkäyttäjän kannalta.

2.4 Etätyöstä ja etäkäytöstä sopiminen

Etätyön tekemiselle on oltava asialliset perustelut, ja sen on oltava viraston toimintastrategian ja tietoturvallisuuspolitiikan mukaista.

Etäkäyttöyhteys avataan ja etätyö voidaan aloittaa työnantajan ja työntekijän sovittua asiasta. Työnantaja voi edistää etäkäyttöä ja etätyötä, jolloin aloite näiden aloittamiseen tulee virastosta.

Etäkäytöstä sovittaessa on käsiteltävä ainakin seuraavat kohdat:

- Etäkäyttäjän velvollisuus on noudattaa virastossa etäkäytöstä annettuja tietoturvallisuusohjeita. Etäkäyttäjä on tutustunut ao. ohjeisiin ja ymmärtää ne. Viraston ohjeiden lisäksi etätyöntekijän on tunnettava Valtion viranomaisen tietoturvallisuustyön yleisohjeen (VAHTI 1/2001) ja Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohjeen (VAHTI 4/2000) sekä tapauskohtaisesti muiden ohjeiden suositukset.
- Järjestelmät, jotka ovat etäkäytön piirissä. Etäkäyttöä voidaan rajoittaa hallinnollisilla tai teknisillä toimenpiteillä.
- Etäkäytön lopettamiseen liittyvät menettelyt.
- Työnantajan hallinnointioikeus etätyölaitteeseen ja sovelluksiin.
- Työnantajan etätyöympäristöön ulottuva valvontaoikeus.
- Etäkäytön muut rajaukset.

Etätyössä on lisäksi sovittava muussa kuin sähköisessä muodossa olevan tietoaineiston käsittelystä.

Tieto etätyön aloittamisesta, päättymisestä ja muutoksesta on toimitettava tietohallinnolle, joka pitää yllä rekisteriä etätyöyhteyksistä. Nämä menettelyt koskevat kaikkea käyttöoikeuksien hallintaa, mutta niiden tärkeys korostuu etäkäytössä.

Etätyön valvontaan liittyvistä menettelyistä on sovittava yt-menettelyn mukaisesti.

2.5 Tehtävien soveltuvuus etätyöhön

Virastokohtaisesti on ratkaistava, mitkä työt ja järjestelmät halutaan rajata vain normaalissa työympäristössä tehtäviksi. Näiden lisäksi on töitä, joiden tekeminen etätyönä on mahdollista, mutta edellyttää normaaleja tiukempia tietoturvallisuustoimia. Tällaisia töitä ja järjestelmiä ovat:

- Järjestelmien etähallinta ja etähuolto
- Ohjelmistopäivitykset ja järjestelmien kehitystyö
- Henkilötietojen käsittely
- Viraston, sen asiakkaiden tai kolmansien tahojen kannalta luottamuksellisten tietojen käsittely
- Taloushallinnon järjestelmät, erityisesti maksuliikenne

Näiden etäkäyttö edellyttää tietoliikenteen vahvaa salausta sekä käyttäjien riittävän vahvaa tunnistusta. Myös etätyöympäristön on oltava tehtävien vaatimalla tasolla.

Kokonaan kiellettyä on:

- Salaisten ja erittäin salaisten tietojen käsittely

2.6 Tietoturvallisuus osana etätyön muita järjestelyjä

Etätyöntekijöiden koulutus voidaan hoitaa osana muuta koulutusta. Koulutuksessa suositellaan käytävän läpi seuraavia asioita:

- Etätyön käytännön järjestelyt (sopimukset, laitteet, ohjelmat, kustannukset).
- Etätyöhön liittyvät ohjeet ja suositukset. Koulutuksessa voidaan käsitellä etätyön tietoturvallisuus esimerkiksi selittämällä, miksi tiettyjä toimintatapoja suositellaan.
- Etätyöntekijälle tulee selvittää keskeisimmät etätyön tietoturvallisuusongelmat sekä toiminta tilanteissa, joissa tietoturvallisuus on pettänyt. Erityisesti on korostettava fyysiseen tietoturvaan ja tietoaineistoihin liittyviä kysymyksiä.
- Selvitetään etätyöhön liittyvien tukipalveluiden käyttö (keneen otetaan yhteyttä, miten tunnistaudutaan jne.), sekä käsitellään etätyössä olevien laitteiden hallinnoinnin vaikutukset (ohjelmien asennukset, käytön valvonta jne.).

Tietoturvallisuuden seurannan on katettava etäyhteyksien tietoturvallisuus. Turvallisuuden toteutumisen valvonnan on oltava säännöllistä. Tuloksista on syytä raportoida osana muuta tietoturvallisuuden raportointia. Suositeltavaa on, että etätyön tietoturvallisuudesta esitetään erillinen arvio, vaikka etätyöhön liittyviä teknisiä ratkaisuja arvioitaisiin osana kokonaisuutta.

Etätyön tietoturvallisuus saattaa edellyttää, että etätyöntekijältä virastoon suuntautuvan yhteyden lisäksi viraston tietohallinto saa oikeuden ottaa yhteyden etätyössä käytettävään laitteeseen. Tämä voi olla tarpeen laitteen hallinnoinnin (ohjelmien asennus ja päivitys, inventointi) tai tietoturvallisuuden valvonnan takia (IDS, lokitietojen siirto). Näiden menettelyjen osalta on sääntöjen oltava mahdollisimman selkeitä, yksinkertaisia ja etätyöntekijän yksityisyyden suojaa loukkaamattomia.

Etätyön lopettamisesta on oltava selkeät menettelyt. Menettelyn tulee sisältää etätyössä käytettyjen laitteiden ja ohjelmien luovutuksen, tarpeettomiksi tulleiden käyttöoikeuksien poistamisen sekä etätyössä käsitellyn materiaalin luovuttamisen takaisin työnantajalle. Tietohallinnon ja henkilöstöhallinnon on syytä laatia tarkistuslista työtä helpottamaan.

2.7 Jatkuva ylläpito

Tietoturvallisuuden ylläpito vaatii myös etätyössä jatkuvaa ylläpitoa, josta osa voidaan automatisoida. Etätyössä käytettävien laitteiden ja ohjelmistojen ylläpito suositellaan sisällytettäväksi osaksi normaalia ylläpitoprosessia.

2.8 Etätyö- ja etäkäyttömuotoja

Etätyö ja etäkäyttö on jatkuvasti yleistynyt. Uudet teknologiat mahdollistavat uusia ratkaisumalleja ja usein työn luonne edellyttää etäkäyttöä. Tässä yhteydessä hahmotellaan erilaisia etätyön ja -käytön tilanteita, mutta esimerkit eivät pyrikään kattamaan kaikkia tilanteita.

Yleisimmät etätyössä käytettävät ohjelmat ovat sähköposti, toimisto-ohjelmat ja Internet-selain, jota käytetään etenkin tiedonhakuun.

Etätyötä voidaan tehdä paikasta riippumatta ilman tietotekniikkaakin. Työskentely voi perustua vi-

rastosta mukaan otettuun aineistoon tai se voi olla kokonaan uuden luomista. Tässä yhteydessä tietoturvallisuus liittyy etupäässä käsiteltävän aineiston fyysiseen turvallisuuteen.

Tyypillinen etätyö on kotoa tehtävää toimistotyötä. Tällöin työskentely perustuu osittain virastosta tuotuihin paperimuotoisiin aineistoihin, osin sähköiseen aineistoon ja osin tietoliikenneyhteyksiin viraston tietojärjestelmiin. Kotoa tapahtuvassa etätyössä voidaan vaikuttaa fyysisen turvallisuuden tasoon sopimalla etätyöntekijän kanssa turvallisuutta edistävistä menettelyistä. Tietoliikenteen turvallisuus voidaan ratkaista yksinkertaisin perinteisin keinoin, jolloin vältetään Internetin tuomat ongelmat.

Etätyötä voidaan tehdä toisen viraston tiloissa, jolloin ollaan kyseisen viraston turvallisuusmenettelyjen piirissä. Omalla virastolla ei juurikaan ole vaikutusmahdollisuuksia turvallisuuteen.

Joissakin paikoissa kunta tai muu yhteisö tarjoaa etätyöntekijöille yhteistä työskentelytilaa. Näissä järjestelyissä henkilökohtainen työympäristö ja sen tietoturvallisuuskysymykset on toteutettu erilaisilla ratkaisuilla, joten työntekijän oman harkintakyvyn merkitys kasvaa.

Etätyö voi olla matkalla tehtävää työtä, jolloin käyttöympäristöt vaihtelevat eikä ympäristön turvallisuuteen voida juurikaan vaikuttaa. Käytettävät tietoliikenneyhteydet ovat langattomia tai ne tulevat satunnaisista puhelinnumeroista. Tietojärjestelmien etäkäyttöä voi tapahtua myös viraston toimitilojen sisällä, mikäli käytetään langattomia yhteyksiä. Tällöin tietoliikenneyhteys käy välillä viraston ulkopuolella.

Etätyöhön voidaan käyttää perinteisten tietokonelaitteiden lisäksi kämmentietokoneita ja matkapuhelimia, joiden ei aina mielletä kuuluvan viraston tietotekniseen ympäristöön. Niillä käsitellään kuitenkin viraston tehtäviin kuuluvia asioita, joten tietoturvallisuuden on oltava etätyön edellyttämällä tasolla. Laitteista on pidettävä kirjaa, ja niissä on oltava käytössä asianmukaiset salaus- ja suojausohjelmistot.

Etäkäyttöä on myös virastojen tietojärjestelmien käyttäminen muista virastoista ja yrityksistä käsin.

3 ETÄTYÖN TIETOTURVALLISUUSRATKAISUT

Tässä luvussa käsitellään tietohallinnon tehtäviä viraston tietoturvallisuuspolitiikan kannalta.

Etätyön kannalta tärkeimmät tietoturvallisuusasiat liittyvät käyttäjän tunnistamiseen, tietoliikenteen suojaukseen ja tietojen luottamuksellisuuteen. Etätyöpisteen sijainti toimitilojen ulkopuolella on riskitekijä, sillä normaaleja tietoturvallisuustoimenpiteitä ei kyetä sellaisenaan ulottamaan etätyöympäristöön. Etätyön suorittamista varten voidaan joutua avaamaan viraston tietoverkkoa. Tähän on valmistauduttava analysoimalla riskitekijät ja suunnittelemalla niiden varalle toimenpiteet.

Etätyön tietoturvallisuusratkaisut kehittyvät nopeasti, mikä tarjoaa uusia mahdollisuuksia lisätä etätyön tietoturvallisuutta. Kehityksen tiivis seuraaminen ja tietohallinnon ammattitaidon kehittäminen lisäävät mahdollisuuksia etätyön tietoturvallisuuden onnistuneeseen toteutukseen.

3.1 Hallinnollinen turvallisuus

Tietohallinnon tehtävänä on toteuttaa viraston tietoturvallisuuspolitiikka siten, että tietojenkäsittelyjärjestelmien turvallinen käyttö viraston toimitilojen ulkopuolella on mahdollista.

Etätyön turvallisuus vaatii virastolta panostuksia teknisiin järjestelyihin ja etätyöntekijän tarvitsemiin tukipalveluihin. Erityistä huomiota on kiinnitettävä etätyöpisteen ja viraston välisen tietoliikenteen luottamuksellisuuden turvaamiseen. Etätyön käyttöönotto saattaa vaatia muutoksia myös lähiverkon turvallisuusmäärityksiin, jos verkossa on tietoturvallisuudeltaan kriittisiä resursseja.

Tietohallinto valvoo tietojärjestelmien etäkäyttöä ja tarvittaessa raportoi tietoturvallisuustilanteesta viraston johdolle. Käytettävät valvontamenettelyt on käsiteltävä henkilöstön kanssa lain edellyttämällä tavalla.[2] Etätyön tietoturvallisuudessa havaitut tarpeet tulee kirjata, ne tulee poistaa ja puutteiden poistamista tulee valvoa. Tietohallinnon tehtäviin voi kuulua myös käyttäjien koulutusta ja opastusta.

Etätyön päätyttyä työnantajan laitteistot ja tietoaineisto palautetaan. Tietoliikenneyhteydet puretaan ja etätyössä käytetyt tunnukset, salasanat ja oikeudet poistetaan.

3.2 Henkilöstöturvallisuus

Normaalit henkilöstöturvallisuuden menettelyt yleensä kattavat myös etätyön tarpeet.

Etätyöntekijän sijaisjärjestelyjen toimiminen on varmistettava. Sijaisjärjestelyyn sisältyy etätyönä tehtävässä työssä tarpeellisten työvälineiden ja tietoaineiston siirto tai kopioiminen viraston tiloihin.

Pysyvää etätyötä tekevien mahdollisuudesta osallistua tietoturvallisuus- ja muuhun koulutukseen tulee huolehtia, vaikka etätyöpiste sijaitsee etäällä viraston koulutukseen käyttämistä tiloista.

Suositellaan, että uudet työntekijät eivät aloita etätyötä ennen kuin he ovat tehneet työtään virastossa jonkin aikaa.

3.3 Fyysinen turvallisuus

Etätyöympäristön fyysistä turvallisuutta ei kyetä valvomaan, kun etätyötä tehdään kotona, matkalla tai muussa tilapäisessä etätyöympäristössä. Etätyöntekijöille voidaan antaa hyvinkin yksityiskohtai-

[2] Laki yksityisyyden suojasta työelämässä (477/2001)

sia ohjeita, mutta työpisteiden turvallisuustarkastukset eivät ole käytännössä mahdollisia. Muiden virastojen tiloissa vakituisesti tehtävän työn osalta fyysisestä turvallisuudesta vastaa kyseinen virasto. Virastojen välillä voi olla poikkeavia turvallisuusvaatimuksia, jotka saattavat rajoittaa sallittuja työtehtäviä. Fyysisen turvallisuuden hallinnan vaikeuden vuoksi muut tietoturvallisuustoimenpiteet tulee toteuttaa siten, että tietoturvallisuuden kokonaisriski hallitaan.

3.4 Tietoliikenneturvallisuus[3]

Etätyöpisteen ja viraston tietoverkon välisen tietoliikenteen turvaaminen on keskeisessä asemassa etätyön tietoturvallisuuden kannalta. Tietoliikenneturvallisuus muodostuu molempien osapuolten tunnistamisesta ja yhteyden salaamisesta siten, että:

1. Viraston järjestelmissä on varmuus, että yhteyden on ottanut siihen oikeutettu käyttäjä.
2. Ulkopuolinen ei voi saada selville tai muuttaa siirrettäviä tietoja.
3. Etäkäyttäjä on varma, että on yhteydessä juuri oikean viraston järjestelmiin

Myös yleisessä puhelinverkossa on mahdollista kaapata yhteyksiä esimerkiksi kytkeytymällä suoraan talojohtoon ja tekeytymällä viraston järjestelmäksi ja näin saada järjestelmien käyttöön oikeuttavia salasanoja.

Kaikissa käyttötavoissa turvallisinta on salata koko tietoliikenneyhteys. Tähän tarkoitukseen suositellaan VPN (Virtual Private Network) -ratkaisuja, joita käsitellään liitteessä 2. Kokonaisuuden ja kustannusten hallinnan kannalta yhtenäiset etäyhteysratkaisut ovat suositeltavia.

Kansainvälisessä etäkäytössä on varmistettava, että käytettävät tietoliikenteen turvaratkaisut ovat kyseisen maan säädösten mukaiset.

3.4.1 Puhelinverkkoyhteydet

Modeemiyhteys suoraan järjestelmään on perinteisesti käytetty yhteystapa. Modeemipooli voidaan liittää yhden järjestelmän sijasta viraston lähiverkkoon ja tarjota käyttäjille usean järjestelmän palveluja. Tällöin vaaditaan käyttäjän tunnistamisen lisäksi pääsyn valvonta, jonka perusteella käyttäjä päästetään palveluihin. Modeemiyhteyslaitteista kerrotaan tarkemmin liitteessä 2. Modeemipalvelut voidaan myös ostaa teleoperaattorilta.

Puhelinverkkoyhteyksiin suositellaan takaisin soittavaa modeemia, mikäli yhteydet voidaan rajata vain tiettyihin paikkoihin tai matkapuhelimeen. Yhteydenottoon ja sisäänkirjautumiseen käytetään yleisesti PPP-protokollaa.

3.4.2 Kiinteät yhteydet

Mikäli etätyö on jatkuvaa yhdessä pisteessä tapahtuvaa työtä, jossa tietoliikenne on merkittävässä asemassa, on harkittava kiinteän yhteyden hankkimista teleoperaattorilta. Yhteysnopeus on sovittavissa tarpeen mukaan. Käytännössä näin saadaan viraston lähiverkko laajennetuksi myös etätyöpisteeseen ja verkonvalvonta voidaan tehdä normaalein menettelyin.

Tämä tietoliikenneratkaisu altistaa viraston lähiverkon etätyöpisteen fyysisen turvallisuuden uhille.

[3] Etätyöympäristön lähiverkon tietoturvallisuuden arvioinnissa tulee hyödyntää Valtionhallinnon lähiverkkojen tietoturvallisuussuositusta (VAHTI 3/2001).

3.4.3 Internet-yhteydet

Yhteys viraston järjestelmiin Internetin kautta on monella tavalla joustava yhteysmuoto. Internet-operaattoriin otetaan yhteys modeemilla tai ISDN-sovittimella, jolloin yhteyskulut ovat paikallispuhelun tasoa. Pysyvään etätyöpisteeseen voidaan joissakin tapauksissa hankkia kiinteä laajakaistainen Internet-yhteys. Kiinteä laajakaistayhteys on suositeltavin vaihtoehto, jos pysyvässä etätyöpisteessä joudutaan toistuvasti siirtämään suuria tietomääriä tai yhteysaikaa käytetään paljon.

Mikäli etäkäyttö tapahtuu Internet-verkon välityksellä, on yhteyden turvaamiseen kiinnitettävä erityistä huomiota. Koska yhteys muodostetaan julkisen verkon yli, tulee yhteys salata yhteyden alkaessa, ennen kuin salasanoja, käyttäjätunnuksia tai muita vastaavia tietoja siirretään. Ulkopuolisten tunkeutuminen työasemaan on estettävä palomuurin avulla. Internet-yhteyksien turvaratkaisuja ja eri yhteysvaihtoehtoja käsitellään tarkemmin liitteessä 2.

3.5 Laitteistoturvallisuus

Viraston tietoverkko liittymineen tulee dokumentoida ja kaikki sen laitteet rekisteröidä. Rekisterin tulee sisältää laitteiden teknisten tietojen lisäksi niiden haltija, sijoituspaikka sekä kaikki verkkoon määritellyt etäyhteydet.

Etätyössä tulee käyttää työnantajan hallitsemia laitteita. Muu käytäntö on mahdollista vain poikkeustapauksissa viraston päätöksellä. Ilman selkeää tietohallinnon ohjausta laitteiden ja ohjelmistojen turvallisuuden hallinta muodostuu ylivoimaiseksi. Monissa laitteissa on sisäänrakennettuja turvaominaisuuksia laitteen käynnistämiseen, tiedostojen salaamisen tai varastamisen varalle. Nämä ominaisuudet on syytä ottaa käyttöön, elleivät ne aiheuta merkittäviä hallintaongelmia.

Laitehuolto tulee järjestää myös etätyövälineistölle. Huollon turvallisuusseikat eivät poikkea muusta laitteistosta. Mikäli joudutaan käyttämään muita kuin vakituisia huoltopalveluja, on käyttäjälle annettava ohjeet tällöin noudatettavista menettelyistä tietojen suojaamiseksi.

Etätyölaitteet on hyvä turvamerkitä. Erityisesti tämä koskee pienikokoisia laitteita kuten matkapuhelimia ja kämmentietokoneita. Turvamerkinnän antama suoja on rajallinen, mutta se vaikeuttaa anastetun omaisuuden jälleenmyyntiä ja helpottaa löytötavaran palautusta omistajalleen.

3.6 Tietoaineistoturvallisuus[4]

Etätyön tietojenkäsittely on rajattava aineistoon, jonka paljastuminen ei vaaranna viraston tietoturvallisuutta eikä loukkaa yksityisyyden suojaa ellei muilla menettelyillä voida varmistaa tietojen turvallisuutta. Mikäli aineistot voidaan säilyttää sähköisessä muodossa vahvasti salattuna, on niiden säilyttäminen etätyöpisteessä mahdollista.

Yleisesti on asetettava samanlaiset, käsiteltävästä aineistosta riippuvat tietoturvallisuusvaatimukset kaikille etätyössä käytettäville tietoteknisille ratkaisuille.

Mikäli tietoaineistoja viedään Suomen ulkopuolelle, on varmistettava, että niiden vieminen ei ole kiellettyä minkään säädöksen nojalla. Esimerkiksi henkilötietolaki sääntelee aineiston vientiä ulkomaille.

Tietoaineistojen varmuuskopiointimahdollisuus tulee tarjota myös etäkäyttäjille. Suositeltavinta on

[4] Tietoaineistoturvallisuutta on käsitelty tarkemmin Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohjeessa (VAHTI 2/2000).

aineistojen siirto viraston tietoverkon palvelimelle, josta otetaan säännölliset varmuuskopiot. Mikäli tämä ei ole mahdollista tai se ei ole tarkoituksenmukaista, käyttäjän on itse huolehdittava varmuuskopioiden ottamisesta ja säännöllisestä toimittamisesta virastoon. Käyttäjän hoitamaa varmuuskopiointia varten on hyvä olla ohjelmistot, jotka samalla salaavat varmuuskopion.

Järjestelmien transaktiohallinnan pitää toimia myös etäkäytössä. Asiakirjojen eheyden on oltava todennettavissa esimerkiksi salausohjelmiston avulla.

Salaamattomana sähköpostissa saa lähettää vain julkista aineistoa. Suositeltava ratkaisu on salakirjoittaa kaikki sähköpostiliikenne, mikäli vastaanottajalla on mahdollisuus käsitellä salakirjoitetut sanomat. Työtehtäviin liittyvän sähköpostin automaattinen ohjaus turvattomiin postipalveluihin, kuten Internetissä käytettäviin palveluihin, tulee kieltää.

Muita kuin julkisia tietoja ei tule tallentaa kovalevylle tai levykkeelle ilman salausta. Salausohjelmia käytettäessä on suunniteltava salauksessa käytettävien avainten hallinta, jotta tietohallinto voi tarvittaessa avata etätyöntekijän salaamat tiedot. Tämä voi kuitenkin tapahtua vain poikkeustilanteissa, esimerkiksi henkilön kuoltua.

Mikäli etätyönä tehdään tietojärjestelmien hallintaa, huoltoa, kehitystyötä, ohjelmistopäivityksiä, näihin rinnastettavia töitä tai näihin töihin liittyviä tietoja käsitellään etätyönä, tarvitaan vahva salaus sekä tietoliikenteessä että tietojen tallentamisessa.

3.7 Ohjelmistoturvallisuus

3.7.1 Etäkäyttäjien ohjelmistot

Lähtökohtaisesti tarvitaan:

- Virustorjunta, mieluiten automaattisesti viraston järjestelmistä päivittyvä. Toissijaisesti voidaan käyttää ohjelmistotoimittajan päivityspalvelua. Haittaohjelmien torjunnassa tulee soveltaa Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohjetta (VAHTI 4/2000).
- Salaava tietoliikenneohjelmisto yhteydenottoa ja pääte-emulointia varten[5].
- Viraston käyttämään toimisto-ohjelmistoon kuuluva tai sen kanssa yhteensopiva sähköposti ja kalenteri.
- Internet-selainohjelma, joka tukee viraston tietoturvallisuusvaatimuksia.
- Turvallisuusasetusten omatoiminen muuttaminen tulee estää tai kieltää.

Suositeltavia etäkäytön ohjelmistoja ovat tiedostojen salausohjelmat. Kiintolevyn salaavat ohjelmistot saattavat vaikeuttaa päivityksiä ja muita huoltotoimenpiteitä, jotka edellyttävät salauksen avaamista.

Tehtäväkohtaisesti voidaan edellyttää muita ohjelmistoja.

Ohjelmistojen osalta on huolehdittava, että käyttö on lisenssiehtojen mukaista.

Osa tarvittavista ohjelmistoista voi olla osana käyttöjärjestelmää, jolloin erillistä hankintaa ei tarvita.

[5] Ks. Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001

3.7.2 Etäylläpito

Etätyössä käytettävien ohjelmistojen päivitys tulee suunnitella etukäteen. Etäkäyttäjille voidaan esimerkiksi osoittaa palvelin ohjelmistopäivityksiä varten. Virustorjuntaohjelmistojen päivitykset ovat keskeisessä asemassa, joten automaattista päivitystä suositellaan. Käyttäjän tulee mahdollisuuksien mukaan välttää etätyölaitteiden ja -ohjelmien asetusten muuttamista, ja tietoturvallisuusasetuksien muuttamisen estoa tai kieltoa on harkittava.

Käyttötukeen yhteydessä oleva etäkäyttäjä tulee tunnistaa. Tunnistus voi perustua esimerkiksi haaste-vaste -tyyppiseen järjestelmään. Tietohallinnon henkilöstön ei tule missään olosuhteissa kysyä etätyöntekijän salasanoja, vaan tukea omalla toiminnallaan salasanojen pysymistä henkilökohtaisena tietona.

3.7.3 Erityiset toimenpiteet etäkäyttäjiä varten

Jotkin järjestelmäasetukset saattavat olla tavallisesta käytöstä poikkeavia varsinkin järjestelmiin pääsyn ja tietoliikenteen osalta.

Etätyön salasanakäytäntö voi olla toimistokäyttöä tiukempi.

3.8 Käyttöturvallisuus

Käytettävyys heikkenee, mikäli viraston resurssit ja tukipalvelut eivät ole etätyöntekijän käytettävissä, mutta myös mikäli etätyöympäristön resurssit eivät ole viraston käytettävissä, tietoliikenneyhteydet eivät toimi tai varmistusten ottaminen on puutteellista.

Tehtävien ja vastuiden kohdennettavuudesta huolehditaan mm. käyttöoikeuksien määrittelyn sekä tapahtuma- ja käyttäjäkirjausten avulla viraston tietoturvallisuuspolitiikan mukaisesti. Käyttöoikeuksia annetaan vain sellaisille henkilöille, jotka tarvitsevat niitä työtehtävien hoidon takia ja vain työtehtävien edellyttämässä laajuudessa.

Viraston ulkopuolelta hankittavissa palveluissa tulee ulkopuolisilta toimittajilta edellyttää käyttöturvallisuuden osalta samalla tasolla olevat turvallisuusrutiinit, mitä virasto itse noudattaa omassa toiminnassaan.

Turvajärjestelmien toimivuus sekä turvallisuus on tarkistettava säännöllisesti. Kaikki määrittelyt on kirjattava tarkasti ja talletettava turvalliseen paikkaan. Tähän tarkistukseen on olemassa apuvälineitä, jotka tutkivat heikkouksia ja antavat niistä raportteja. Järjestelmiin tunkeutumisen havaitsevia ohjelmia tulee mahdollisuuksien mukaan käyttää, jotta voidaan reagoida tapahtuneisiin hyökkäyksiin ja virhetilanteisiin välittömästi.

3.8.1 Tunnistaminen

Etäkäytössä käyttäjän luotettava tunnistaminen ja todentaminen on tärkeää. Kirjautumisen nykyisiä ratkaisuja ovat mm. TACACS+ ja RADIUS. Koska etäyhteyttä voidaan salakuunnella, heikko salasana ei ole riittävä todennuskeino. Suositeltavia ratkaisuja ovat varmennepohjainen tunnistaminen ja kertakäyttösalasanat. Ihannetapauksessa käyttäjä tunnistetaan verkossa vain kerran istunnon alussa.

3.8.2 Pääsyn rajoitus

Pääsynvalvonnan avulla valvotaan järjestelmiin kytkeytymisiä sekä mahdollisia kytkeytymisyrityksiä. Pääsynvalvonta perustuu yleensä tunnistamiseen ja pääsynvalvontalistoihin. Eri menetelmiä esitetään liitteessä 2.

Luotettavan yhteyden luominen käyttäjälle sallittuihin tietojärjestelmiin edellyttää henkilökohtaisia

käyttöoikeuksia. Pääsynvalvonta hakee käyttöoikeudet pääsynvalvontalistalta (ACL, Access Control List).

Kaikkia tietojärjestelmien käyttöoikeuksia ei automaattisesti tule myöntää etäkäyttäjille. Siksi on pystyttävä erottamaan käyttäjän rooli joko käyttäjätunnusten, yhteydenotto-osoitteen tai muiden tietojen avulla. Palomuurin avulla on mahdollista rajoittaa käyttäjän pääsyä eri laitteille, jolloin ei välttämättä tarvita eri käyttäjätunnuksia. Lopulliset menettelytavat on ratkaistava tapauskohtaisesti tietojärjestelmien luokituksen, tietoverkon rakenteen ja yhteystapojen mukaan.

3.8.3 Käyttäjien seuranta

Etäkäytön seuranta on toteutettava siten, että toimenpiteitä ei voida suorittaa ilman, että jälkikäteen on tietoturvallisuuskirjanpidosta selvitettävissä toimenpiteen sisältö, suorittaja sekä tapahtuman ajankohta. Seuranta parantaa myös etäkäyttäjien oikeusturvaa, kun toimenpiteet voidaan kohdistaa tiettyyn käyttäjätunnukseen ja ajankohtaan.

Etäyhteyksien toteuttamistavoista riippuu, pystytäänkö etäkäyttöä kontrolloimaan eri tavalla kuin toimistosta tapahtuvaa käyttöä.

Työntekijää on informoitava käytettävistä valvontamenettelyistä ja niiden mahdollisesta vaikutuksesta yksityisyyden suojaan.

3.8.4 Sallitut käyttöajat

Järjestelmien käyttöä on mahdollista rajoittaa kellonajan, kalenterin tai muiden seikkojen perusteella. Asiasta on tiedotettava varsinkin ulkomailta tapahtuvaa etäkäyttöä ajatellen. Rajoittaminen on perusteltua esimerkiksi mikäli verkon valvontaa ei voida tehdä jatkuvasti, käytettävät sovellukset vaativat huolto- tai muita taukoja tai mikäli välttämätöntä käyttäjätukea ei voida tarjota ympärivuorokautisesti.

3.8.5 Lokitiedostot ja seuranta[6]

Kaikki tärkeimpien ohjelmistojen käytön tapahtumatiedot, esimerkiksi sisäänkirjaantuminen, poistuminen järjestelmästä ja konfiguroinnin muutokset, tulee kirjata suojattuun lokitiedostoon tietosuojasäädökset huomioon ottaen. Erityisesti epäonnistuneet tapahtumat tulee kirjata. Lokitiedostojen käyttö muihin kuin teknisiin, toimintaa tai turvallisuutta kontrolloiviin tarkoituksiin on kielletty.

Tietokoneen kello on pidettävä oikeassa ajassa transaktiohallinnan, lokitiedostojen ja muiden tarkkaa aikaa edellyttävien toimintojen vuoksi.

3.8.6 Viraston ohjelmistot

Viraston sovellusten ja palvelujen varmistamiseksi suositellaan roolipohjaisten pääsylistojen käyttöä. Tällöin voidaan käyttäjälle antaa erilaiset käyttöoikeudet etäkäyttöä ja virastossa tapahtuvaa käyttöä varten. Sähköpostipalvelimiin tulee harkita virusten suodatusohjelmistoa estämään virusten ja muiden haittaohjelmien leviämistä. Selainpohjaisten sovellusten yleistyessä on harkittava SSL/TLS-protokollan käyttöä, joka on VPN:ää täydentävä, eikä tätä korvaava tietoturvallisuusratkaisu.

[6] Lokitiedostojen käsittelystä lähemmin ks. Valtionhallinnon sähköpostien ja lokitietojen käsittelyohje (VAHTI 5/2001).

3.9 Ongelmatilanteet

3.9.1 Etäkäyttäjän tuki

Etätyön onnistumisen kannalta viraston on järjestettävä riittävät tukipalvelut etätyöntekijälle. Käytännössä tämä tarkoittaa normaalin työajan ulkopuolisina aikoina toimivia tukipalveluja. Etätyöntekijä tarvitsee mahdollisesti tukipalvelua ohjelmistojen ja laitteiden käyttöön liittyvissä ongelmissa, tietoliikenteeseen liittyvissä asioissa ja laitteiden vikaantuessa. Tukipyynnöissä on otettava huomioon etäkäyttäjän luotettava tunnistaminen. Tämä voidaan järjestää esimerkiksi takaisinsoitolla ennalta sovittuun puhelinnumeroon tai esittämällä henkilölle henkilöllisyyden varmistamia kysymyksiä.

Kattavaa tukea ei aina voida tarjota, jolloin käyttäjän osaamiselle asetetaan lisävaatimuksia ja on hyväksyttävä, että ongelmatilanteissa etätyö häiriintyy merkittävästi.

3.9.2 Hälytykset[7]

Havaittaessa tietokonevirus tai järjestelmään tunkeutuminen on käyttäjiä varoitettava ja järjestelmän käyttö suljettava tarvittavilta osin. Epäillyt tietoturvarikokset on ilmoitettava poliisille. Kaikki merkittävät tietojärjestelmien turvallisuutta uhkaavat tapahtumat ilmoitetaan Viestintäviraston CERT-FI -yksikölle.

Hälytystilanteita varten on virastossa oltava etätyöntekijöiden puhelinnumerot. On suotavaa, että etätyöntekijällä on samanaikaisesti käytettävissä puhelinyhteys ja tietokoneen käyttämä tietoliikenneyhteys.

3.9.3 Vikatilanteet

Kun järjestelmien käyttö estyy osittain tai kokonaan, voidaan varautua vastaamaan toistuviin puhelinsoittoihin. Ensisijaisesti on varmistettava tietoaineiston eheys ja luottamuksellisuus.

[7] Vastatoimien suunnittelussa on syytä hyödyntää VAHTI:n asiasta antamaa ohjetta Toimet tietoturvaloukkaustilanteissa (7/2001).

4 ETÄTYÖNTEKIJÄLLE

Tämän luvun ohjeet on tarkoitettu etätyöntekijälle. Tarkoituksena on kiinnittää huomio niihin tietoturvallisuusasioihin, joihin etätyöntekijä voi vaikuttaa. Etätyöntekijän toimet ratkaisevat tietoturvallisuuden tason.

4.1 Toiminta etätyöntekijänä

- Vastuusi viraston tietoturvallisuudesta lisääntyy etätyön myötä.
- Kiinnitä kaikessa toiminnassasi huomiota tietoturvallisiin menettelytapoihin. Erityisen tärkeää tämä on toimittaessa vakituisten toimistotilojen ulkopuolella.
- Noudata viraston johdon antamia ohjeita.
- Tarkkaile mahdollisia tietoturvallisuutta vaarantavia seikkoja ja raportoi niistä.
- Etätyöhön liittyvien turvallisuusriskien vuoksi toimintaasi saatetaan joutua valvomaan toisin kuin toimistotyöskentelyssä.
- Käytä sovittuja käyttäjätunnistusmenettelyjä. Älä missään tilanteessa luovuta tunnisteitasi kenenkään muun käyttöön äläkä jätä niitä muiden saataville.
- Varmistu, että sivulliset, kuten perheenjäsenesi, eivät saa otetuksi yhteyttä viraston tietojärjestelmiin.
- Huolehdi, että tiedät miten toimit erilaisissa ongelmatilanteissa. Todennäköisiä tilanteita ovat tietoliikenneyhteyden ongelmat sekä laitteiden ja tietoaineiston varastaminen tai katoaminen.
- Kehitä tietotekniikkaosaamistasi.

4.2 Laitteet ja ohjelmistot

- Varmista, että asiattomat eivät pääse käyttämään tietokonettasi.
- Käytä etätyössäsi ainoastaan sovittuja tietoliikennetapoja ja varmista, että sovitut salaus- ja suojausmenettelyt ovat käytössä.
- Käytä vain työnantajan tarkoitusta varten osoittamaa laitteistoa. Oman laitteiston käyttöoikeudesta on aina erikseen sovittava.
- Laitteistoa ei saa käyttää mihinkään sellaiseen toimintaan, joka voi vaarantaa sen turvallisuuden. Tällaisia voivat olla tietokonepelit, epäluotettavien Internet-sivujen selailu ja ohjelmien lataaminen.
- Huolehdi työnteossa käyttämiesi puhelinten, kommunikaattoreiden ja kämmentietokoneiden turvallisuudesta. Älä säilytä niissä ylimääräistä tietoa ja käytä tiedon salausta.
- Etätyöhön käytettävässä työnantajan laitteessa saa käyttää vain hyväksyttyjä ohjelmistoja. Älä asenna siihen itse mitään ohjelmia.
- Käytä sovittuja suojausohjelmia ja varmista, että ne ovat ajan tasalla.
- Viraston tietojärjestelmien etäkäyttöä voidaan tietoturvallisuus- tai muista syistä rajoittaa. Siksi sinulla ei välttämättä ole kaikkia samoja oikeuksia etäkäytössä kuin toimistossa työs-

kenneltäessä tai et voi käyttää kaikkia järjestelmiä.

- Muista, että virkapostin automaattinen edelleen ohjaus esim. henkilökohtaiseen sähköpostiin on kielletty. Hallittu sähköpostin siirto on sallittu, mikäli noudatetaan tietoaineiston käsittelystä annettuja ohjeita ja määräyksiä.
- Huolehdi, että laitteesi on ja pysyy turvallisena.

4.3 Tietoaineisto

- Vältä salassa pidettävien tietojen tulostamista paperille tai tallentamista levykkeille. Jos tulostat tai tallennat, huolehdi tiedon asianmukaisesta käsittelystä ja hävittämisestä.
- Käsittele etätyössä ainoastaan sellaista tietoaineistoa, jonka salaisuusaste vastaa käyttämääsi työskentely-ympäristöä. Etätyössä ei voi käsitellä kaikkea tietoa.
- Tarvittaessa käytä tiedostojen salausta.
- Lukitse aineistojen säilytyspaikka.
- Vie toimistotilojen ulkopuolelle vain työn suorittamisen kannalta välttämätöntä tietoaineistoa. Palauta se mahdollisimman pian.
- Huolehdi tietoaineistosi varmuuskopioinnista. Suositeltavaa on siirtää aineistot viraston ympäristöön varmuuskopioitavaksi. Tällöin varmuuskopion palauttaminen on kuitenkin hidasta.
- Huolehdi tietoaineistojen virustarkastuksista

4.4 Etätyöympäristö

- Työskentelytilojen on vastattava käsiteltävän tietoaineiston turvallisuusvaatimuksia
- Varmista, että tiloissa on riittävä murtosuojaus. Varkaus voi kohdistua laitteisiin tai työssä käytettävään tietoaineistoon.
- Jos etätyössä käsitellään alkuperäisiä asiakirjoja, palosuojauksen järjestäminen on välttämätöntä.
- Jos teet etätyötä Suomen ulkopuolella, varmista, että käyttämäsi tekniset ratkaisut ovat kyseisessä maassa sallittuja ja tietoaineiston vienti kyseiseen maahan on luvallista.

5 MUUTA HUOMIOON OTETTAVAA

5.1 Asiakirjojen käsittely

Asiakirjojen käsittelystä on annettu Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje (VAHTI 2/2000). Tätä ohjetta tulee noudattaa myös etätyönä tehtävään asiakirjojen käsittelyyn. Kyseinen ohje rajoittaa merkittävästi salassa pidettävien tietoaineistojen käsittelyä etäkäyttönä.

Virastokohtaisesti voidaan harkita VAHTI:n ohjetta täydentävien tai sitä tiukempien ohjeiden antamista etätyössä käsiteltävien asiakirjojen käsittelyyn. Tämä tulee kyseeseen erityisesti tapauksissa, joissa viraston käsittelemien asiakirjojen tai viraston toiminta näin edellyttää.

Mikäli edellä kuvattu ohjeistus ei ole tarpeen, on etätyötä koskevassa yleisessä ohjeistuksessa otettava huomioon ainakin seuraavat seikat:

- Asiakirjojen käsittelyssä on noudatettava samoja periaatteita kuin normaalisti, etätyön erityisriskit huomioon ottaen.
- Asiakirjan haltijan on itse arvioitava, onko etätyöskentely-ympäristö sellainen, että asiakirjan tietoturvallisen käsittelyn edellytykset täyttyvät. Epävarmoissa tapauksissa on suositeltavaa olla varovainen ja olettaa, etteivät turvallisen käsittelyn edellytykset täyty. On myös muistettava, että liikuteltavan tietokoneen mukana tietoaineisto voi vahingossa siirtyä turvattomaan ympäristöön.
- Asiakirjan elinkaari voi alkaa tai se voi päättyä etätyössä. Tällöin on noudatettava asiakirjojen käsittelystä sekä asiakirjan turvallisesta hävittämisestä annettuja ohjeita[8] sekä viraston arkistonmuodostussuunnitelmassa määriteltyjä asiakirjojen säilytysaikoja. Tarpeettomaksi tulleiden sähköisten tietovälineiden tuhoamista etätyöympäristössä ei suositella, vaan tältä osin tulee noudattaa viraston normaalia sähköisten tietovälineiden tuhoamismenettelyä.

5.2 Etätyö useaan eri virastoon

Virastojen väliset yhteydet tulevat lisääntymään ja näin tulee tapahtumaan myös niiden henkilöiden määrälle, jotka ovat etäyhteydessä useampaan kuin yhteen virastoon. Sellaiset yhteydet toisiin virastoihin, jotka ovat jatkuvia ja joita käyttää huomattava määrä viraston henkilökunnasta, suositellaan järjestettäviksi siten, että etätyöntekijät ottavat yhteyden omaan virastoonsa, josta muodostetaan yhteys toisen viraston palveluihin. Mikäli tällainen järjestely ei ole tarkoituksenmukaista, on etäyhteysasiasta toteutettava yhteistyössä kohdeviraston kanssa.

5.3 Etätyön tietoturvallisuuden suhde muuhun tietoturvallisuuteen

Tietoturvallisen etätyön toteuttaminen on oleellisesti helpompaa, mikäli virastossa on toimiva tietoturvallisuuden johto ja toteutus. Tietoturvallisuuden puutteista aiheutuvan riskin merkitys saattaa kasvaa merkittävästi etätyön myötä. Viraston turvallisuusvyöhyke laajenee ja se muuttuu vaikeammin hallittavaksi, kun työympäristöjen ja työssä käytettävien laitteiden määrä kasvaa.

Etätyön tietoturvallisuuden toteutuksen valittavien teknisten ratkaisujen valinta ja niiden hallinta vaatii osaamista, jota pienillä virastoilla ei välttämättä ole. Ratkaisuissa on lähdettävä viraston toiminnallisista tarpeista.

[8] Tarpeettomaksi tulleiden tietoaineistojen hävittäminen (VM 21/01/2000, 18.4.2000).

Tietoturvallisuustarkastusten on katettava myös etätyön tietoturvallisuusratkaisut. Tarkastus on suositeltavaa tehdä aina merkittävien muutosten jälkeen, eikä se saa rajoittua vain teknisen tietoturvallisuuden arviointiin.

5.4 Tekninen kehitys

Tekninen kehitys tulee vaikuttamaan etätyön tietoturvallisuuteen erityisesti kolmella tavalla: uudet verkkoyhteydet tulevat lisäämään etätyöntekoa, tietoturvallisuusohjelmistojen tekninen kehitys tulee tarjoamaan uusia ja entistä toimivampia ratkaisuja tietoturvallisuuden parantamiseksi sekä uudet laitteet, ohjelmat ja verkot tulevat asettamaan uusia tietoturvallisuusvaatimuksia osin suoraan (tekniset asiat) ja osin epäsuorasti (uudet käyttötavat).

Toimikortit tulevat yleistymään. Niiden käyttö ei toistaiseksi ole yleistynyt odotetusti. Syitä tähän on lukuisia, mutta vaikuttaa ilmeiseltä, että tulevan viiden vuoden aikana toimikorttien avulla tapahtuva vahva tunnistaminen ja sähköinen allekirjoitus lisääntyvät. Kehitys on ilmeisesti nopeinta suurissa organisaatioissa. Toimikorttipohjaisella tunnistamisella voidaan lisätä tietoturvallisuutta erityisesti hyvää tietoturvallisuutta vaativissa kohteissa.

Toimikorttiratkaisuista tulevat valtionhallinnossa ensi sijassa kyseeseen HST- ja virkamieskortti. Virkamieskortin laaja käyttöönotto on alkanut sisäasiainministeriön hallinnonalalla.

Kolmannen sukupolven matkapuhelinverkkojen yleistyminen ei sekään ole vastannut odotuksia. Nämä ns. 3G verkot tarjoavat nykyisiä verkkoja nopeamman tiedonsiirtoyhteyden. Yhteyden kustannukset jäänevät alhaisemmiksi kuin nykyisillä ns. 2G (GSM) ja 2.5G (GPRS) verkoilla, mikä edesauttaa mobiilisti tapahtuvan etäkäytön yleistymistä. Verkkojen tietoturvallisuusominaisuudet kehittyvät, mutta etätyön tietoturvallisuuden kannalta tällä ei ole suurta merkitystä. Etätyön tietoturvallisuuden kannalta tärkeämpää on langatonta tietoliikenneyhteyttä hyödyntävien sovellusten tietoturvallisuus sekä etätyön muut tietoturvallisuusasiat.

Nopeat, halvat tietoliikenneyhteydet muuttavat etätyötä kohti mobiilia työntekotapaa. Etätyön tietoturvallisuuden kannalta tämä tarkoittaa, että tarve suojata etätyöhön käytettävä laite ja etäkäytettävä järjestelmä tulevat lisääntymään. Etäkäyttäjien määrän lisääntyessä etäkäyttäjiksi tulevat entistä laajemmat käyttäjäjoukot. Tämän johdosta tietoturvallisuuskoulutuksen ja tietoturvallisuusohjeiden merkitys tulee kasvamaan.

Matkapuhelinverkkojen rinnalla ja osin näitä täydentämään tulevat muut langattomat verkot. Etätyön tietoturvallisuuden kannalta merkittävää tulee olemaan ainakin langattomien lähiverkkojen (WLAN) laajamittainen käyttöönotto sekä mahdollisesti ns. vertaisverkkojen (peer-to-peer – networks) synty Bluetooth-protokollaa hyödyntävien laitteiden yleistyessä. Langattomat lähiverkot aiheuttavat etätyön tietoturvallisuudelle samankaltaisia vaikutuksia kuin 3G verkkojen käyttöönotto.

Nykyisellään langattomien tietoverkkojen tietoturvallisuuden taso on heikko, mutta oletettavasti lähitulevaisuudessa tilanne jossain määrin paranee. Langattomat lähiverkot sitovat työntekijää entistä vähemmän etätyöpisteeseen. Etätyötä tehdään entistä useammin ympäristössä, johon ei voida vaikuttaa ja jonka tietoturvallisuus ei ole hyvä. Tämän johdosta etätyön tietoturvallisuudessa tulee korostumaan sovellusten tietoturvallisuus, luotettavat tunnistusmenettelyt sekä etätyössä käytettävien laitteiden tietoturvallisuus. Myös etätyöntekijöiden on entistä useammin kyettävä tekemään itsenäiset arviot etätyöympäristön turvallisuudesta.

Langattomissa lähiverkoissa ominaiset lyhytkestoiset ja satunnaiset verkkoyhteydet ovat tyypillisiä myös vertaisverkoissa. Bluetooth tulee ilmeisesti olemaan yleinen menetelmä tilapäisesti muodos-

tettavien vertaisverkkojen kommunikointimenetelmänä. Vertaisverkkojen tietoturvallisuuteen liittyvistä erityisongelmista on vasta vähän tietoa, mutta luultavaa on, että näiden tietoturvallisuuden kannalta merkittävämpää on verkkojen käyttötapaan liittyvät ongelmat kuin itse protokollan mahdolliset tietoturvaheikkoudet.

Biometriseen tunnistukseen käytetyt menetelmät ovat kehittyneet ja niiden käyttö on yleistynyt. Tällä ei tule lähitulevaisuudessa olemaan merkittäviä vaikutuksia etätyön tietoturvallisuusongelmien ratkaisuun, vaan biometristen sovellusten käyttö rajautuu kokeiluihin ja mahdollisesti yksittäisiin suurta tietoturvallisuutta vaativiin tapauksiin. Tällöin voidaan hyödyntää esim. hiireen sijoitettua sormenjälkitunnistusta käyttäjän tunnistukseen. Biometriset tunnistusmenetelmät eivät tule korvaamaan ns. PKI-ratkaisuja, eivätkä suoranaisesti toimikorttejakaan, vaan niitä tultaneen käyttämään näitä ratkaisuja täydentävinä tietoturvallisuusvälineinä.

Uusia tietoturvallisuusratkaisuja kehitetään ja jo olemassa olevien toimivuutta parannetaan. Kehityksen seuranta on tärkeää, jotta kyetään arvioimaan, millaisia toimivia ja hyväksi havaittuja ratkaisuja on saatavilla.

6 ETÄTYÖN TIETOTURVALLISUUTEEN LIITTYVÄÄ SÄÄNTELYÄ

6.1 Yleistä

Lainsäädäntö asettaa velvoitteita etätyön tietoturvallisuudelle. Etätyössä on varmistettava tietojen luottamuksellisuus, käytettävyys ja eheys. Etätyötä koskevat myös työlainsäädännön etätyöntekijälle asettamat velvoitteet ja antamat oikeudet. Perusoikeudet turvaavat esimerkiksi kotona tehtävää työtä ulkopuoliselta tunkeutumiselta ja asiattomalta valvonnalta.

6.2 Viraston velvollisuudet

Hyvä tiedonhallintatapa edellyttää, että viranomainen huolehtii tietojenkäsittelynsä turvallisuudesta ja tietojensa asianmukaisesta suojaamisesta etätyössä (JulkL, JulkA). Henkilötiedot on myös etäkäytössä suojattava asiattomalta muuttamiselta, tuhoamiselta tai anastukselta (HetiL). Henkilötietolain velvoitteet koskevat myös sitä, joka rekisterinpitäjän toimeksiannosta käsittelee henkilötietoja, joko etäyhteyden välityksellä tai muuten.

Viranomaisen tulee huolehtia tietojärjestelmien ja tietojensa käytettävyydestä (JulkL, JulkA). Henkilörekisterissä olevien tietojen on oltava käytettävissä, kun tehdään rekisteröityjä koskevia arvioita ja päätöksiä, riippumatta siitä käytetäänkö tietoja virastosta käsin tai ollaanko tietoihin etäyhteydessä (HetiL). Viranomaisen on lisäksi huolehdittava tietojensa eheydestä ja oikeellisuudesta (JulkL, JulkA).

Etätyössä on otettava huomioon asiakirjojen säilyttämistä ja hävittämistä koskevat säädökset ja määräykset (AL). Viraston arkistonmuodostussuunnitelmaan on sisällytettävä myös etätyössä syntyvät asiakirjat ja tiedot. Henkilötietojen säilytyksessä ja hävittämisessä on etätyössä noudatettava erityistä huolellisuutta (HetiL).

6.3 Työntekijän velvollisuudet

Työntekijä ei saa sopimussuhteen aikana ilmaista muille työnantajan liike- ja ammattisalaisuuksia (TyösL), eikä virkamies ei saa luvatta ilmaista muille asemassaan tietoon saamaansa salassa pidettävää seikkaa (VirkamL). Virkamies ja työntekijä eivät saa luvatta ilmaista sivullisille yhteistoimintalain nojalla salassa pidettävää asiaa (YhteistL). Henkilötietojen käsittelijä ei saa ilmaista sivullisille rekisterin etäkäytön yhteydessä saamiaan tietoja (HetiL).

Työntekijän on noudatettava etätyön edellyttämää varovaisuutta ja ilmoitettava työnantajalle etäkäytössään olevissa laitteissa ja järjestelmissä havaitsemistaan vioista tai puutteista. Virkamiehen on suoritettava tehtävänsä asianmukaisesti ja noudatettava työnjohto- ja valvontamääräyksiä myös etätyössä. Rekisterinpitäjän alaisuudessa toimivan henkilötietojen etäkäsittelijän on toimittava rekisterinpitäjän ohjeiden mukaisesti (TyösL, Valtion virkamL, HetiL).

6.4 Telepalveluyrityksen velvollisuudet

Telepalvelujen tarjoajan on varmistettava palvelujensa käytettävyys. Myös telepalvelun käyttäjän tulee huolehtia liittymiensä turvallisuudesta. Telepalvelujen turvallisuutta ja käytettävyyttä vaarantava telepäätelaite voidaan poistaa yleisestä televerkosta. Teleyritysten on huolehdittava televiestien ja tietojen siirron eheydestä (TTsL).

Tele- tai postilaitoksen palveluksessa oleva tai ollut ei saa ilmaista, mitä tehtävässään on saanut tietää tele- tai postitoiminnassa välitetyn tiedon sisällöstä, mikäli tämä loukkaa tieto- ja viestintä- tai

kirjesalaisuutta (TTsL, PostiL).

6.5 Etätyön järjestäminen ja etätyön valvonta

Työnjohto- ja valvontavaltansa nojalla työnantajalla ei ole oikeutta mennä etätyötä tekevän asuntoon vastoin tämän tahtoa (PL). Työnantajalla on oltava erityinen syy voidakseen tarkastaa, miten työntekijä noudattaa kotonaan työtä koskevia määräyksiä. Etätyön valvonnalla ei saa tarpeettomasti loukata työntekijän yksityisyyttä, eikä vaarantaa hänen yksityisten luottamuksellisten viestiensä salaisuutta. Etätyön teknisen valvonnan tarkoituksesta, käyttöönotosta ja menetelmistä sekä sähköpostin ja tietoverkon käytöstä on tiedotettava henkilöstölle ja asiassa on noudatettava yhteistoimintamenettelyä (TyöelämänTSL, YhteistL).

6.6 Tietorikostyyppejä

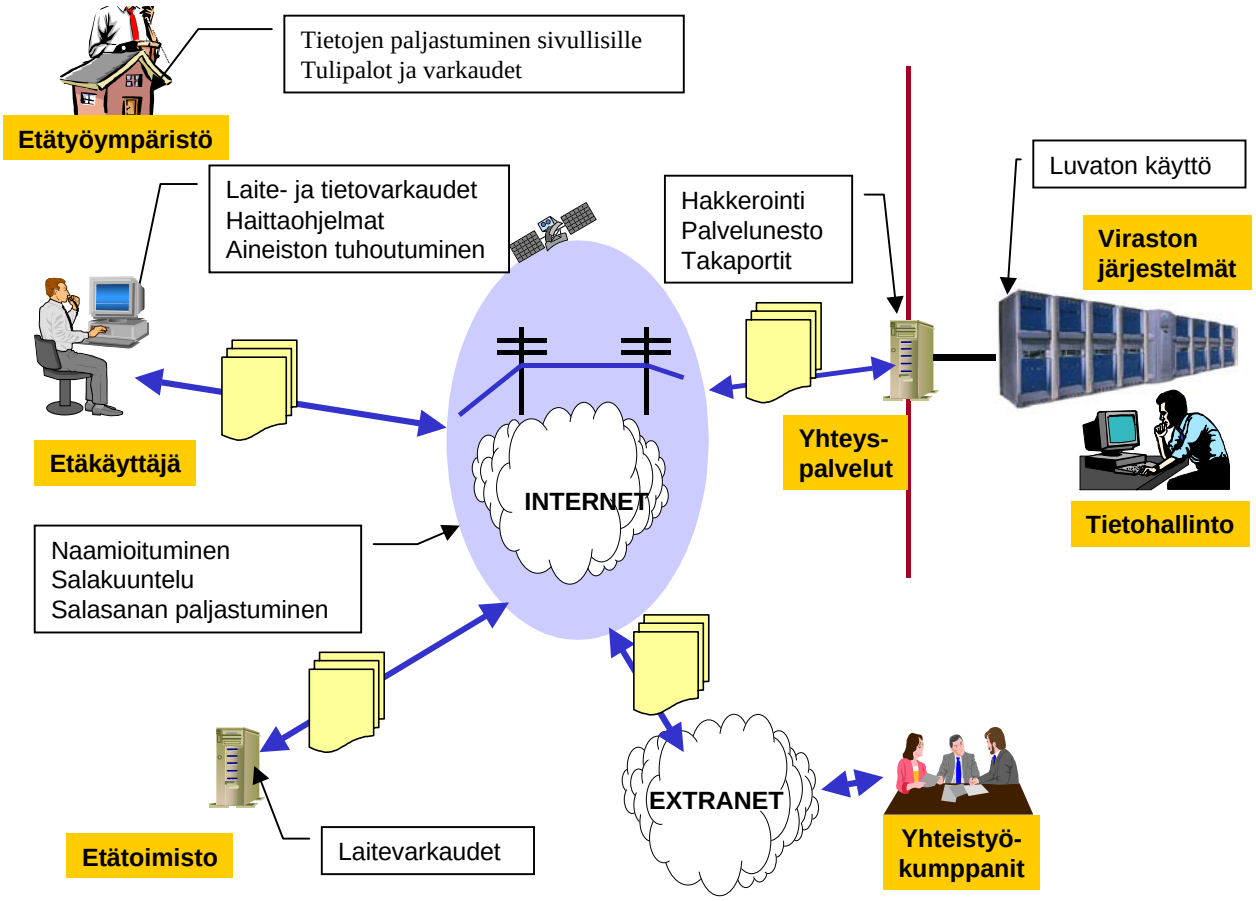
Tietomurtoon tai henkilörekisteririkokseen, esimerkiksi tietojen asiattomaan tuhoamiseen tai muuttamiseen syyllistynyt tuomitaan sakkoon tai vankeuteen. Palvelunestohyökkäykseen, tietoliikenteessä välitettävien tietojen muuttamiseen tai muuhun tietoliikenteen häirintään syyllistynyt tuomitaan sakkoon tai vankeuteen. Haitallisten ohjelmistojen, esimerkiksi virusten levittämiseen syyllistynyt tuomitaan sakkoon tai vankeuteen (RL luvut 35, 38). Tietoturvallisuuteen kohdistuvat rikokset saattavat olla rangaistavia myös muiden lain kohtien perusteella, esimerkiksi yritysvakoiluna.

Väärennykseen tai vahingontekoon, esimerkiksi tietojen ja asiakirjojen asiattomaan muuttamisen syyllistynyt tuomitaan sakkoon tai vankeuteen. Petokseen, esimerkiksi tietojenkäsittelyn harhauttamisella tietojen muuttamiseen syyllistynyt tuomitaan sakkoon tai vankeuteen. Tietoliikenteen häirintään, esimerkiksi välitettävien tietojen ja viestien asiattomaan muuttamiseen syyllistynyt tuomitaan sakkoon tai vankeuteen. Tietomurtoon tai tietojen asiattomaan muuttamiseen tuhoamiseen syyllistynyt tuomitaan sakkoon tai vankeuteen (RL luvut 33, 35, 36, 38).

Salassapitorikokseen tai viestintäsalaisuuden loukkaukseen syyllistynyt tuomitaan sakkoon tai vankeuteen. Virkasalaisuuden rikkomiseen tai asiakirjan luvattomaan paljastamiseen syyllistynyt tuomitaan sakkoon tai vankeuteen, usein myös viralta panoon (RL luvut 38, 40).

Joka asiattomasti ja vastoin toisen tahtoa tunkeutuu toisen kotiin, hänet tuomitaan sakkoon tai vankeuteen. Samoin joka asiattomasti kuuntelee tai tallettaa, mitä tapahtuu toisen kotona, tuomitaan salakuuntelusta tai -katselusta sakkoon tai vankeuteen (RL luku 24).

LIITE 1: UHKIA ETÄKÄYTÖN TURVALLISUUDELLE



Kuva 2: Etätyöhön kohdistuvia uhkia

Etätyön riskianalyysi voidaan suorittaa osana viraston yleistä riskien arviointia, mutta suositeltavaa on tehdä se erillisenä. Etätyön riskianalyysi tulee ajankohtaiseksi ennen ensimmäisten etätyölupien myöntämistä. Tärkeitä tarkistus- ja uudistuspisteitä ovat tilanteet, jossa etätyöntekijöille tarjotaan pääsy uusiin järjestelmiin, etätyö laajenee tai yleistyy merkittävästi tai kun etätyössä tapahtuu muita merkittäviä muutoksia. Viimeksi mainittuja voivat olla uusien päätelaitetyyppien käyttöönotto ja uusien tietoturvallisuusratkaisujen markkinoilletulo.

Etätyön riskianalyysissa voidaan soveltaen hyödyntää oheista tarkistuslistaa. Lisäksi voidaan käyttää hyväksi tietosuojavaltuutetun toimiston laatimaa "Tee se itse" -tarkastuslistaa (http://www.tietosuoja.fi/5940.htm), jonka osat 1 ja 2 liittyvät henkilötietojen käsittelyyn, mutta osa 3 on laaja tietoturvallisuuden tarkistuslista.

Etätyöympäristöön liittyviä riskejä:

- Ulkopuolisten liikkumista ympäristössä ei voida kontrolloida.
- Palo-, murto- tai muu fyysinen turvallisuus on heikosti järjestetty.
- Sähkönjakelussa esiintyvät häiriöt vaarantavat laiteturvallisuuden ja käytettävyyden. Laitteiden suojaus muita ulkopuolisia häiriöitä vastaan on etätyössä normaalia toimistokäyttöä hankalam-

paa järjestää.

Etätyössä käytettäviin laitteisiin liittyviä riskejä:

- Kannettavat laitteet katoavat tai ne varastetaan.
- Etätyössä käytettävien laitteiden huollon järjestelyt on hoidettu heikosti.
- Kannettavia laitteita liitetään turvattomiin verkkoihin.
- Kannettavia laitteita käytetään tai kuljetetaan ympäristössä, jonka tietoturvallisuus ei vastaa vaatimuksia.
- On yhteiskäyttöisiä laitteita, joille ei ole omistajaa ja jotka ovat normaalin laitteiden hallinnointitoimenpiteiden ulkopuolella

Etätyössä käytettäviin ohjelmistoihin liittyviä riskejä:

- Käyttäjä sivuuttaa hankaliksi kokemansa tietoturvallisuusohjelmat.
- Ohjelmistot eivät ole yhteensopivia. Tämä tulee korostetusti esiin, mikäli laitetta käytetään useaan eri tarkoitukseen tai ollaan yhteydessä useaan eri virastoon.
- Käyttäjälle annetaan pääkäyttäjäoikeudet, vaikka hän ei osaisi hallinnoida laitetta tai ohjelmistoa.
- Ohjelmistojen päivitys tai muu ylläpito jää toteuttamatta. Erityisesti tietoturvallisuusohjelmien päivityksen toimimattomuus altistaa tietoturvallisuuden rikkoutumiselle.
- Internetissä yleisesti saatavilla olevia sähköposti- tai muita ohjelmia käytetään luottamuksellisen tiedon välittämiseen tai käsittelyyn ilman asianmukaisia turvallisuusjärjestelyitä.
- Etätyössä käytettävälle laitteelle asennetaan luvattomia ohjelmia.
- Tietoturvallisuusohjelmistot eivät toimi, eikä tätä kyetä havaitsemaan.

Tietoaineistoon liittyviä riskejä:

- Tietoja voidaan etäkäytön yhteydessä helpommin käyttää muuhun kuin niiden alkuperäiseen tarkoitukseen.
- Varmuuskopiointi on puutteellisesti järjestetty.
- Mikäli käyttäjä säilyttää varmuuskopioita, on niiden hallinta ja käsittely riskialtista.
- Tietovälineiden katoaminen.
- Ulkopuolisten asiaton pääsy tietoon.
- Etätyössä olevalle laitteella on sellaista luottamuksellista tietoa, jonka olemassaolosta käyttäjä ei ole tietoinen, eikä näin ollen käsittele laitetta asianmukaisesti. Ongelma tulee esiin erityisesti käytöstä poistettavien laitteiden kohdalla.
- Tietoaineiston siirto etätyöympäristön ja viraston välillä.

- Etätyössä syntyneen tietoaineiston asianmukaisesta hävittämisestä ei ole huolehdittu.
- Yhteiskäytössä olevalle koneelle jää luottamuksellista tietoa.

Tietoliikenteen riskejä:

- Osa tietoliikenteestä kulkee suojaamattomana ei-turvallisissa verkoissa.
- Salakuuntelu, etenkin Internetissä siirrettävien tietojen.
- Turvallisuusratkaisujen negatiiviset vaikutukset tiedonsiirron nopeuteen.
- Turvallista yhteyttä ei voida kaikkialla käyttää, jolloin turvaudutaan tietoturvallisuudeltaan heikompitasoisiin yhteyksiin.
- Tietoliikennesopimuksissa ei ole riittävästi otettu huomioon kaikkia tietosuoja- ja tietoturvavelvoitteita.

Tunnistamisen riskejä:

- Käyttäjä ei vaihda salasanojaan edes niin usein kuin toimistoympäristössä.
- Kriittisten sovellusten käyttäjäntunnistus on hoidettu heikosti.
- Yhteiskäyttöiset käyttäjätunnukset ja salasanat.
- Salasanoja hallinnoidaan heikosti, eikä niitä poisteta etätyönteon loppuessa.
- Salasanojen käyttö yhteiskäytössä olevalla laitteella voi vaarantaa niiden luottamuksellisuuden.
- Muistiin kirjoitettujen salasanojen joutuminen ulkopuolisen käsiin.
- Ulkopuolinen pakottaa käyttäjän tunnistautumaan. (kiristäminen tai uhkaaminen)

Käytettäviin järjestelmiin ja palveluihin kohdistuvia riskejä:

- Järjestelmien käyttöä ei rajata, vaan järjestelmät ovat käytettävissä niin kuin ne olisivat toimistoympäristössä.

Tukipalveluihin liittyviä riskejä:

- Tukipalvelut toimivat vain virastoaikana.
- Tukipalveluiden käyttäjän tunnistaminen hoidetaan heikosti.
- Mikäli etäkäytössä käytetään tulostimia tai kopiointilaitteita, joita käyttävät muutkin kuin viraston omat henkilöt, on otettava huomioon lisääntynyt riski tietoaineiston joutumisesta vääriin käsiin. Tämä voi tapahtua joko paperien joutuessa väärään paikkaan (tulostus virheelliselle tulostimelle, telekopioiden tai kopioiden unohtaminen) tai käytettävistä laitteista johtuen (esim. digitaaliset kopiokoneet tallettavat käsiteltävät työt).

Hallinnollisia riskejä:

- Viraston tietoturvallisuuspolitiikkaa ei ole tai sitä ei osata soveltaa etätyöhön.
- Virastokohtaisia etätyön tietoturvallisuusohjeita ei ole tai ne eivät ole sovellettavissa liian tiukkuuden, vaikeaselkoisuuden tai muun syyn vuoksi.
- Viraston johto on puutteellisesti sitoutunut etätyön tietoturvallisuuden ylläpitoon.
- Etätyön tietoturvallisuutta ei valvota eikä sitä tarkasteta.
- Etätyöstä, sen sisällöstä, siihen liittyvistä valvonta- ja muista menettelyistä ei sovita.
- Etätyöhön liittyvää ohjeistusta ja koulutusta ei ole.
- Vastuut etätyön tietoturvallisuusjärjestelyissä ovat epäselvät. Tämä korostuu, mikä tietoturvallisuusratkaisuja tarjoamiseen osallistuu toimittajia tai muita viraston ulkopuolisia tahoja.
- Etätyössä sallitaan tehtäväksi töitä, jotka eivät siihen sovellu.
- Tietohallintohenkilöstöllä ei ole riittävää asiantuntemusta tietoturvallisuusratkaisujen hallintaan.
- Tietoturvallisuusratkaisut eivät skaalaudu etäkäyttäjämäärän kasvaessa.
- Tietoturvallisuusratkaisut eivät palvele viraston toiminnallisia tarpeita.

LIITE 2: TEKNISIÄ RATKAISUJA

1 YHTEYSLAITTEET

1.1 Yleisen puhelinverkon modeemit

Modeemiyhteys voidaan muodostaa valintaisen puhelinverkon yli kantoaaltomodeemilla tai nopeammalla ISDN-sovittimella. Matkapuhelinverkkoa voidaan hyödyntää GSM-data -modeemilla. Näissä tapauksissa yhteys on varattu etäkäyttäjän ja järjestelmän väliseen tiedonsiirtoon.

Pakettikytkentäinen GSM-data (GPRS) toimii GSM-verkon periaatteessa suojatulla ilmarajapinnalla, mutta tukiasemakeskuksesta yhteys ohjataan operaattorin palvelimien kautta Internet-verkkoon. Tästä syystä yhteys tulee suojata päästä päähän jollakin luotettavalla ja helppokäyttöisellä salausmenetelmällä.

1.2 Laajakaistainen yhteys Internet-verkon yli

Yhteistä näille yhteysmuodoille on, että verkkoyhteys on pysyvä eli sitä ei erikseen avata ja suljeta jokaista tehtävää varten. Tiedonsiirtonopeus on ISDN-sovitinta suurempi ja saattaa lähestyä lähiverkon siirtonopeutta. Modeemiyhteyteen verrattuna laajakaistaisen liittymän perustamiskustannukset ovat korkeammat, mutta varsinkin laajamittainen käyttö halvempaa. Liikkuvaan etäkäyttöön nämä eivät sovellu WLAN:ia lukuun ottamatta.

- ADSL-liittymässä IP-data liikkuu valintaisen puhelinverkon kaapeleissa. ADSL on yleensä mahdollista alle 5 km etäisyydellä paikalliskeskuksesta, mikä rajoittaa ADSL:n käyttöä. Suomen kotitalouksista noin puolet sijaitsee ADSL-palvelun alueella.
- Kaapelimodeemissa IP-data liikkuu kaapeli-TV -verkossa. Suurimmissa taajamissa on kaapeli-TV -verkko, ja sen parissa on n. 300 000 tilaajaa.
- Langattomassa lähiverkossa (WLAN) IP-data liikkuu radioyhteydellä. WLAN-verkkoja on kokeilumielessä pystytetty lähinnä suurimpien taajamien keskuksiin, mutta myös joihinkin pienehköjen kuntien keskuksiin.

2 ERI TYYPPISET TYÖASEMAT

2.1 Microsoft Windows

Windows eri versioissaan on selvästi yleisin henkilökohtaisten tietokoneiden käyttöjärjestelmä. Windows pohjautuu edelleen jo DOS-maailmasta lähteneeseen yhden käyttäjän olettamukseen. NT4- ja 2000-järjestelmissä on useita käyttäjätilejä (user account), joista vain yksi voi kerrallaan olla koneelle kirjaantuneena. Sovellusten prosessit voivat käyttää eri tasoisia (ml. system) oikeuksia, mikä altistaa järjestelmää tietoturvaloukkauksille. Skriptivirukset ovat Windows-ympäristössä yleisiä ja leviävät nopeasti. Päivitysten ja uusien versioiden mukana järjestelmään on jouduttu lisäämään suojauskerroksia, mikä on hidastanut versioiden julkaisua ja aiheuttanut toimivuusongelmia päivityksissä. Myös laitteisto- ja muistivaatimukset ovat jatkuvasti kasvaneet.

Windows 2000:ssa on korjattu suurin osa NT4:n heikkouksista. Yhteensopivuuden säilyttämiseksi parannukset on kuitenkin tehty ohjelmakerroksia lisäämällä, joten Windows 2000 vaatii laitteistolta kaksinkertaiset resurssit NT4:n verrattuna. Käyttöjärjestelmän ytimen rakenteellisia heikkouksia

on vielä jäljellä, mutta vakautta on parannettu ylimääräisillä suojauskerroksilla ja tarkemmilla vikailmoituksilla.

Uusin kotikäyttäjille suunnattu versio Windows XP sisältää ominaisuuksia, jotka saattavat kyseenalaistaa XP:n tietoturvallisuuden. Yhteys Microsoftin omaan PassPort-pääsynvalvontajärjestelmään on uhka yksityisyydelle.

Lisäksi Outlook- ja Exchange-sähköpostijärjestelmissä ja Explorer-selaimessa on jatkuvasti ilmitulevia turvallisuusongelmia. Microsoft onkin aloittanut erityisen turvallisuusohjelman ongelmien ratkaisemiseksi.

Koska Microsoft on merkittävin toimija markkinoilla, sen tuotteisiin kohdistetaan eniten tietoturvan rikkomisyrityksiä, jolloin myös onnistumisia tulee useammin kuin muiden tuotteiden kohdalla. Microsoftin tuotteiden yleisyyden vuoksi myös pääosa Internetissä leviävistä viruksista kohdistuu niihin.

2.2 Unix

Eri Unix-versioita kuten Solaris ja HP-UX käytetään edelleen lähinnä raskaissa työasemasovelluksissa. Avoimen lähdekoodin Unix-johdannainen Linux on yleistynyt mm. www-palvelimissa vakautensa, edullisuutensa ja keveiden laitteistovaatimustensa ansiosta. Unix on alun pitäen suunniteltu monen käyttäjän moniprosessiympäristöksi, mikä on suureksi avuksi tietoturvallisuuspalveluiden toteutuksessa.

Unix-työasemasovelluksia ja niiden käyttäjiä on suhteellisen vähän Windowsiin verrattuna. Ilmeisesti tästä johtuen Unix-haittaohjelmistoja ei ole liikkeellä kovin usein. Moniprosessiympäristö ehkäisee tehokkaasti Windowsille tyypillisten makrovirusten ajon, mutta ns. madot ja troijalaiset ovat mahdollisia.

Heikosti suojattuun Unix-koneeseen voidaan murtautua ja sitä voidaan käyttää palvelunestohyökkäyksessä muita koneita vastaan. Laitekohtaisen palomuurin asennuksen lisäksi tulisi tärkeät järjestelmätiedostot suojata, ja ennen kaikkea varmistaa pääkäyttäjän (root) oikeuksien ja salasanan tietoturvallisuus.

2.3 Kämmentietokoneet (PDA)

Kädessä pidettävän kokoiset tietokoneet voidaan jakaa eri tavoilla lähtökohtana esim. laitteen verkkoyhteysmuoto, käyttäjärajapinta tai käyttöjärjestelmä. Useimmat etäkäyttöön soveltuvat laitteet pohjautuvat Symbian-, PocketPC- tai Palm-alustaan. Symbian on varsinkin matkapuhelinvalmistajien suosima alusta, ja Pocket PC on Windows-ympäristön pienoisversio. Palm oli ensimmäinen USA:ssa laajalle levinnyt kämmentietokone, mutta Euroopassa huomattavasti harvinaisempi.

PDA-valmistajat tarjoavat sovelluskehittäjille avoimen alustan ja kehitysvälineitä, koska olettavat laajan sovellustarjonnan houkuttelevan asiakkaita. Samalla tosin helpotetaan myös haittaohjelmien kehitystä. Haittaohjelmat eivät ole vielä yleistyneet, mutta tilanne saattaa muuttua nopeasti.

2.4 Mac-työasemat

Mac-työasemilla on noin 10% osuus markkinoista, joten Mac-haittaohjelmia esiintyy melko harvoin: PC-ympäristössä viruksia, matoja ja Troijan hevosia on löydetty noin 60 000, mutta Mac-ympäristössä alle 100. Alun perin yhden käyttäjän työasemaksi tarkoitettu Mac-ympäristö sisältää versioon 9 saakka samanlaisia puutteita kuin Windows. Versiosta 10 (Mac OS X) alkaen käyttö-

järjestelmä perustuu BSD-Unixiin, joka luultavasti on haittaohjelmien tekijöiden paremmin tuntema ympäristö. Unixin tietoturvallisuusominaisuudet ovat kuitenkin käytettävissä.

PC-haittaohjelmia ei voi ajaa Mac-ympäristössä, mutta MS Word- ja Excel-makrovirukset toimivat Mac:ssa samalla tavalla kuin PC:ssäkin. Vaikka Mac-työasema ei vioitu PC-haittaohjelmasta, se voi kuitenkin levittää tartuntaa muihin koneisiin.

Viimeisten kahden vuoden aikana Mac-ympäristössä on löydetty noin 40 vakavaa tietoturva-aukkoa, ja määrän oletetaan kasvavan. Koska haittaohjelmien torjuntavälineet on useimmiten tarkoitettu PC-koneisiin, on mahdollista, että virastolla ei ole välineitä Mac-työasemien suojaukseen. Jos Mac-työasemia käytetään, on teknisen tuen saatavuus varmistettava.

2.5 Verkkotietokoneet ja Thin Clientit

Suurten organisaatioiden rajusti kasvaneet käyttäjämäärät ovat tehneet PC-tietokoneiden ylläpito- ja päivitystehtävistä vaikeasti hallittavia. Siksi on kehitetty konsepteja, joissa työasema on mahdollisimman yksinkertainen ja sovellukset mahdollisimman pitkälti palvelimiin keskitettyjä. Työasema toimii lähinnä päätteenä, jossa tarvitaan käyttöjärjestelmän lisäksi Internet-selain tai etäkäyttöohjelma, esim. Citrix MetaFrame tai MS Terminal services, sovellusten ajoa varten.

Tietoturvan kannalta verkkotietokone ilman omaa tallennuskapasiteettia tarjoaa suuria etuja perinteiseen työasemaan verrattuna. Verkkotietokonetta ei voi käyttää itsenäisesti, vaan lähiverkko huolehtii keskitetysti sisäänkirjautumisesta, varmuuskopioinnista ja haittaohjelmien torjunnasta. Käyttäjien asetukset tallennetaan palvelimille, joten verkkotietokoneet voidaan konfiguroida yhtenäisesti. Samalla ylläpidon ja käyttäjätuen tarve pienenee. Verkkotietokoneen hankintahinta ei juurikaan poikkea tavallisesta työasemasta, mutta tavallista PC-työasemaa voidaan käyttää ”verkkotietokoneena” estämällä kovalevyn käyttö esim. BIOS-asetuksilla.

Käytännössä kovalevytön verkkotietokone sopii lähiverkkoympäristöön, jossa verkon palvelut ovat välittömästi saatavilla. Etätyössä joudutaan usein toimimaan ilman verkkoyhteyksiä, jolloin verkkotietokoneet ja Thin Client-työasemat eivät tule kysymykseen. Etäkäyttöohjelmistot puolestaan kykenevät tarjoamaan yhteyden myös Internetin tai modeemin välityksellä, jolloin kotikäyttö on mahdollista.

3 SUOJAUSOHJELMISTOT

3.1 Virustorjunta[9]

Tietokonevirukset, madot ja Troijan hevoset (eli troijalaiset) ovat tyypillisimpiä loppukäyttäjän PC-työasemaan kohdistuvia tietoturvallisuusongelmia. Virukset ovat muihin ohjelmistoihin piilotettuja ohjelmia, jotka suorittavat haitallisia toimintoja (esim. tiedostojen poisto) ja lisääntyvät kopioimalla itsensä uusiin ohjelmiin. Sähköpostin liitetiedostojen avulla virus voi levitä nopeasti koko maailmaan.

Troijan hevonen poikkeaa viruksesta vain siinä, että haittaohjelma on naamioitunut vaarattomaksi ohjelmaksi, kuten peliksi, jonka ajaminen kuitenkin käynnistää haitallisia toimintoja, esimerkiksi

[9] Haittaohjelmien torjuntaa käsitellään VAHTI:n ohjeessa Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje (4/2000).

lähettää tietoaineistoja tai avaa tietoliikenneyhteyksiä murtautujaa varten (ns. salaovi). Mato on verkon avulla leviävä ohjelma joka kopioi itseään muihin tietokoneisiin verkko-ohjelmistojen tietoturvallisuusaukkojen kautta. Vaikka puhtaat madot eivät tee muutoksia laitteistoihin, joihin ne tunkeutuvat, voidaan madoilla saada aikaan huomattavia vahinkoja esimerkiksi tekemällä palvelunestohyökkäys verkkoa kuormittavan madon avulla. Tuhoisimmat haittaohjelmat kuten Nimda ja Code Red sisältävät sekä virusten että matojen piirteitä.

Virusten torjuntaohjelmistot tunnistavat haittaohjelmia niiden bittisisällön ("sormenjälki") tai käytöksen perusteella. Koska uusia haittaohjelmia kehitetään koko ajan, ja entisiä voidaan uudistaa pienillä muutoksilla, on virustorjunnan päivitysten tiheys keskeisessä asemassa. Johtavien toimittajien ratkaisut perustuvat automaattisiin päivityksiin Internetin avulla. Keskitetty hallinta antaa tietohallinnolle edellytykset viraston laitteiston ylläpitoon.

Työasemien ohella virustorjuntaohjelmia on saatavissa kämmentietokoneisiin ja sähköpostipalvelimiin tehokkaampaa liitetiedostojen virustarkastusta varten.

3.2 Kovalevyn salaus[10]

Salakirjoittamalla tiedostojen sisältö estetään luottamuksellisten tietojen paljastuminen laitevarkauden yhteydessä. Yksittäisten tiedostojen salaamisen sijasta nykyiset salausohjelmat toimivat taustalla ja käsittelevät kokonaisia kovalevyjä tai hakemistoja ilman käyttäjän väliintuloa. Huolto- ja päivitystilanteissa tämä saattaa aiheuttaa ongelmia, mutta on loppukäyttäjän kannalta kuitenkin helpoin tapa suojata aineisto. Mikäli etätyössä käytetään laitteita, joihin virastolla ei ole hallinnointioikeuksia, voidaan harkita tiedostokohtaisen salauksen käyttöä.

Salausta ja sen purkamista varten tarvitaan avain eli salasana, joka on säilytettävä huolellisesti. Salausavaimen katoamisen ja muiden pakottavien tilanteiden varalle on oltava salasanan turvatalletus- tai muu järjestelmä, jolla tiedot voidaan tarvittaessa palauttaa.

Salausohjelmia asennettaessa on valittava riittävän turvallisuustason takaavat salausalgoritmit, avainpituudet sekä muut salausominaisuudet.

3.3 Tunkeutumisen havainnointi ja esto

Sovellustason hyökkäykset kohdistuvat yleensä jonkin palvelinohjelmiston (sähköposti, web-palvelin, ftp-palvelin, nimipalvelin) heikkouksiin, joiden avulla tunkeutuja voi hankkia sovelluksen pääkäyttäjän oikeudet. Koska nämä hyökkäykset tehdään palomuurin näille palveluille avattuihin portteihin, niiden torjuntaan tarvitaan muitakin keinoja. IDS (Intrusion Detection System) perustuu tyypillisen hyökkäyksen profiilin tunnistamiseen. IDS voidaan toteuttaa verkkopohjaisena (NIDS), jolloin tunkeutumisyritys tunnistetaan seuraamalla tietyn vyöhykkeen tietoliikennettä, tai konepohjaisena (HIDS) jolloin isäntäkoneeseen sijoitetut ns. agentit tunnistavat tunkeutumisyrityksen lokitiedostojen muutoksia seuraamalla.

3.4 VPN – Virtual Private Network

VPN:llä tarkoitetaan yleisestä tietoliikenneverkosta salauksella eriytettyä yhteyttä, jonka avulla käyttäjä näkee etäyhteyden takana sijaitsevan laitteiston omaan lähiverkkoonsa kuuluvana. Alku-

[10] Lisätietoa salausohjelmista on saataville VAHTI:n julkaisemasta Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus (3/2001).

jaan VPN:ien avulla haettiin kustannussäästöjä korvaamalla yrityksen toimipisteiden väliset kiinteät linjat edullisilla Internet-yhteyksillä. Tietoturvallisuushyödyt saatiin lisäämällä VPN-yhteyksiin salaus. Yleisimmät VPN-protokollat ovat IPSec, L2TP ja PPTP, joiden lisäksi esim. SSH:lla voidaan muodostaa suojattuja yhteyksiä. VPN voidaan toteuttaa laitteistolla ja/tai ohjelmistolla ja se on ongelmistaan huolimatta suositeltavin menetelmä etäkäyttöä varten.

VPN:n ratkaisuissa on esiintynyt yhteensopivuusongelmia: kaikki laitteet ja ohjelmat eivät toimi yhdessä niin kuin niiden pitäisi. Ongelmia on esiintynyt etenkin kun palomuuriohjelmalla ja VPN-ohjelmistolla on eri valmistajat. Ohjelmistojen yhteensopivuudesta on varmistuttava ennen hankintaa.

VPN alentaa hieman siirtonopeutta , mikä saattaa aiheuttaa ongelmia etenkin hitaimmilla yhteyksillä. Yhteyden muodostuminen kestää suojaamatonta yhteyttä kauemmin, mutta myös varsinaisen tietoliikenteen nopeus saattaa hidastua. Käyttäjän havaitsevat tämän, joten asiasta on hyvä tiedottaa VPN-yhteyksiä käyttäville.

Tyypillinen virhe VPN-hankinnoissa on kapasiteetiltään riittämättömän ratkaisun hankkiminen. Käyttäjämäärien kasvaessa todelliseen käyttömäärään nähden alimitoitettu ratkaisu saattaa alentaa palveluiden käytettävyyttä.

VPN:n toteuttamisessa käytetään seuraavia tekniikoita. *Kapseloinnin* avulla siirretään yksityisillä osoitteilla tapahtuvaa verkkoliikennettä IP-runkoverkossa. *Salauksella* suojataan siirrettävä liikenne salakuuntelulta ja väärentämiseltä. *Autentikointia* ja *auktorisointia* tarvitaan pääsynvalvontaan. *Liikenteen seurannan* avulla voidaan kohdentaa tietoliikenteen kustannukset ja havaita epätavallinen liikenne.

Viraston eri toimipisteet voidaan yhdistää intranet-VPN:llä, ja yhteydet toimittajiin ja muihin sidosryhmiin extranet-VPN:llä. Tyypillisesti tunnelointi kulkee avoimen Internetin yli. Useita erilaisia yhteystekniikoita on käytettävissä.

Etäkäyttäjiä varten voidaan soveltaa ns. access-VPN -yhteyksiä siten, että etäkäyttäjän työasema muodostaa salatun yhteyden Internet-operaattorin ja Internetin kautta viraston sisäverkkoon saakka. Toinen mahdollisuus on soittaa verkko-operaattorin palvelupisteeseen, jossa käyttäjä autentikoidaan, ja operaattori muodostaa salatun yhteyden viraston verkkoon.

Mitään tarkkaa määritelmää VPN:lle ei ole, mutta VPN-tuotteella tulee olla ainakin seuraavat ominaisuudet:

- **Autentikointi.** Yhteyspyyntö on autentikoitava ennen kuin VPN ryhtyy muodostamaan tunnelia. Autentikointi voi tapahtua ns. jaettujen salaisuuksien avulla, tai parempaa tietoturvallisuutta haettaessa IP-pakettikohtaisesti.
- **Kapselointi.** Kun tunneli on avattu, datapaketit kapseloidaan toisiin IP-paketteihin avoimen Internetin yli tapahtuvaa siirtoa varten. Kapseloinnin avulla IP-verkossa voidaan siirtää muitakin protokollia, kuten AppleTalk ja IPX. IPSec-standardiin perustuvat tuotteet pystyvät lisäksi autentikoimaan lähetyksen IP-pakettikohtaisesti.
- **Salaus.** Datapaketit salataan ennen siirtoa avoimen Internetin yli salakuuntelun estämiseksi. Tuotteet tukevat yleensä useita salausvaihtoehtoja, joista voi valita parhaiten sopiva.
- **Suodatus.** IP-pakettien suodatus auttaa todentamaan yhteyden toisen pään henkilöllisyyden.

VPN-toteutuksia on sekä laitteisto- että ohjelmistomuotoisena. Laitteistopohjaiset VPN:t ovat yleensä itsenäisiä laitteita, joiden prosessori suorittaa pelkästään VPN-toimintoja, joten niillä on VPN-toteutuksista paras suorituskyky. Laitteistoratkaisuihin voidaan lukea Virtual Access Serverit ja VPN-toiminnalliset reitittimet.

Ohjelmistopohjaiset VPN:t ovat palvelinpuolella yleensä etäkäyttö- ja reititinohjelmistojen lisävarusteita. Työasemiin VPN:n voi saada esimerkiksi tietoturvallisuuspaketin tai etäkäyttöohjelmiston osana. Ohjelmistopohjainen VPN yhdistetään usein myös palomuuriin.

VPN:n voi hankkia palveluna Internet-operaattorilta. Ratkaisut ovat yleensä laitteisto- tai palomuuripohjaisia. Tässä vaihtoehdossa on muistettava, että osa tietoturvallisuusjärjestelmästä siirtyy pois omasta hallinnasta.

3.5 IPSec

IPSec on IP-tietoliikenneprotokolla, jossa IP-paketteja välitetään turvallisesti avoimen verkon läpi. Palomuurit tunnistavat ja sallivat tällä tavalla kapseloidun ja salatun liikenteen.

3.6 SSL ja TLS – Secure Sockets Layer ja Transport Layer Security

SSL on sovellusriippumaton asiakas-palvelin (client-server) –menetelmä, jota käytetään mm. http ja ftp -protokollien suojaukseen. TLS on SSL:n standardisoitu muoto. SSL/TLS käyttää sekä julkisen että salaisen avaimen salausta, ja sitä käytetään yleensä palvelimen, varsinkin web-palvelimen autentikointiin. Asiakas (client) pyytää salattua yhteyttä ja palvelin (server) vastaa lähettämällä digitaalisen sertifikaattinsa, jossa on palvelimen julkinen avain. Asiakas muodostaa salausavaimen, joka salataan palvelimen julkisella avaimella ja lähetetään takaisin. Näin osapuolet ovat sopineet yhteisestä symmetrisestä salausmetodista.

3.7 SSH – Secure Shell

Unix-maailman etäkäyttökomentojen rlogin, rsh ja rexec tilalle on kehitetty PKI-pohjainen SSH-ohjelmisto etäkirjautumista ja komentojen suoritusta varten. SSH-ohjelmat sisältävät keinoja luotettavaan kirjautumiseen, tietoliikenteen salaukseen ja kompressointiin.

SSH on alun perin SSH Communications, Inc:n tuote. Secure Shell (”Suojattu komentotulkki”) on toisaalta yleinen käsite, ja vastaava avoimen lähdekoodin ohjelma on saman niminen, mikä on aiheuttanut sekaannuksia. Lisäksi on olemassa avoimen lähdekoodin tuote OpenSSH. Nämä kaikki sisältävät samankaltaisia toimintoja.

3.8 Henkilökohtainen palomuuri

Palomuuri rajoittaa liikennettä kahden verkon välillä. Yleisimmät palomuurin toteutukset perustuvat pakettien suodatukseen IP-osoitteen, protokollan, portin tai muun liikennetiedon perusteella. Suodattava palomuuri sopii henkilökohtaisen tietokoneen Internet-liikenteen rajoittamiseen. Palomuurin toiminta edellyttää hyvin määriteltyjä suodatussääntöjä (politiikkaa) siitä, minkälainen liikenne sallitaan kyseiselle laitteelle. Palomuuri rajoittaa liikenteen pääsyä verkkoon, mutta ei liikenteen sisältöä.

Käytännössä Internet-etäkäyttäjiä varten määritellään palvelimet ja portit joihin voidaan avata yhteys, ja asetukset monistetaan kaikille käyttäjille. Yleisesti vain tarpeelliset yhteydet avataan ja muu liikenne estetään. Palomuurien asetuksista on runsaasti kirjallisuutta saatavissa.

3.9 Salaus ja digitaalinen allekirjoitus

Asiakirjasta tehdään ainutkertainen ”sormenjälki” tiivistealgoritmilla, jolloin asiakirjan yhdenkin merkin muuttaminen muuttaa sormenjälkeä. Asiakirjan lisäksi myös sormenjälki lähetetään, ja asiakirja voidaan lähettää salattuna. Vastaanottaja purkaa tarvittaessa asiakirjan salauksen, ja laskee saamastaan asiakirjasta samalla tiivistealgoritmilla sormenjäljen. Jos laskettu ja vastaanotettu sormenjälki ovat samoja, on varmaa, että asiakirjan sisältö ei ole muuttunut.

3.10 Julkisen avaimen salaus

Asymmetrisessä eli julkisen avaimen salauksessa käytetään avainparia, jonka muodostavat julkinen ja salainen avain. Julkisella avaimella salatun viesti voidaan avata vain avainparin salaisella avaimella ja päinvastoin. Julkinen avain on yleisesti saatavilla, joten kuka tahansa voi salata tietylle henkilölle lähetettävän aineiston. Purkuavain on vain kyseisen henkilön hallussa, joten vain hän voi purkaa salauksen.

Salaisella avaimella salatun viestin voi purkaa vain julkisella avaimella, jolloin asiankirjan ja sen lähettäjän yhteys voidaan todentaa.

Digitaalisen sertifikaatin avulla voidaan kiinnittää käyttäjän henkilöllisyys julkiseen avaimeen. Sertifikaatin avulla voidaan toteuttaa esim. käyttöoikeuslistojen vaatima tunnistaminen. Viraston kirjautumispalvelin myöntää eri palvelujen vaatimat sertifikaatit, jolloin etäkäytön vaatimat tietoturvallisuuspalvelut voidaan toteuttaa samalla menetelmällä.

3.11 Kertakirjautuminen

Turvallinen kertakirjautuminen (Secure Single Sign-On) on haastavaa toteuttaa. MIT Kerberos toimii siten, että keskuspalvelin lähettää käyttäjälle “pääsylipun”, jonka sovellukset hyväksyvät. Kerberoksen käyttö edellyttää kaikkien sovellusten ”kerberisointia”, mikä on erityisen vaikeaa toteuttaa eri virastojen välillä. Koska Kerberos-avaimet talletetaan yhdelle keskuspalvelimelle, voidaan koko viraston tietoturvallisuus nujertaa murtautumalla tähän palvelimeen. Windows 2000 sisältää Kerberos-toteutuksen, jossa on laajennuksia MIT:n versioon. Julkisen avaimen salausta pidetään nykyisin Kerberosta parempana ratkaisuna.

3.12 Toimikortit

Toimikortit ovat muovisia, luottokortin kokoisia kortteja, jotka sisältävät suorittimen ja muistia tietojenkäsittelyä varten. Virtalähdettä ei ole, vaan toimintaan tarvittava virta saadaan esim. PC-tietokoneeseen liitettävästä kortinlukijasta. Toimikortti on helppo kuljettaa mukana, ja sen sisältämään tietoon on asiattomien lähes mahdotonta päästä käsiksi. Toimikorteilla on lukuisia sovellusmahdollisuuksia, mutta laajamittainen käyttö edellyttää sopimusta yhteisestä standardista. Yleisin toimikorttisovellus on matkapuhelinten SIM-kortti, jolla verkko tunnistaa puhelinliittymän haltijan. Toimikortin ominaisuudet voidaan sisällyttää myös muun kuin kortin muotoisiin laitteisiin. Erilaisia ratkaisuja on markkinoilla jo runsaasti.

Toimikortille on yleensä tallennettu käyttäjän tunnistamisessa tarvittava sertifikaatti, jota näin voidaan siirtää sovelluksesta toiseen helposti ja turvallisesti. Toimikorttia on mahdollista käyttää tunnistamiseen (virkamieskortti), digitaaliseen allekirjoitukseen, salaukseen ja asioinnin kiistämättömyyden varmistamiseen.

Vaikka toimikortteihin liittyvä fyysinen laitteisto (kortit, lukijat ja näihin välittömästi liittyvät oh-

jelmat) onkin jo olemassa, puuttuu useimmista sovelluksista toimiva tuki toimikorteille. Tämä on hidastanut esimerkiksi HST-kortin yleistymistä.

Toimikortit edellyttävät niiden hallinnoinnin järjestämistä. Korttien myöntäminen, jakelu, peruuttaminen, tarkistuslistat ja muut hallinnolliset palvelut asettavat omat haasteensa.

LIITE 3: LAITEKOHTAISIA TIETOTURVALLISUUSUHKIA JA NIIDEN RATKAISUJA

Tilanne keväällä 2002.

	Päätelaite		
Uhka	**PDA, älypuhelin**	**Kannettava PC**	**Kiinteä PC**
Laitteen katoaminen tai varastaminen	Massamuistin salaus Vahva sisäänkirjaus laitteeseen Varmuuskopionti	Kovalevyn salaus Vahva sisäänkirjaus laitteeseen Varmuuskopionti	Kovalevyn salaus Vahva sisäänkirjaus laitteeseen Varmuuskopionti (Riski merkittävästi pienempi)
Haittaohjelmat	Virustorjunta (riski toistaiseksi pieni) Käyttäjien koulutus	Virustorjunta Käyttäjien koulutus	Virustorjunta Käyttäjien koulutus
Sisääntunkeutuminen (krakkerointi)	Laitekohtainen palomuuri (riski toistaiseksi pieni)	Laitekohtainen palomuuri	Laitekohtainen palomuuri
Salakuuntelu	VPN	VPN	VPN
Laiterikot	Varmuuskopiointi Huoltosopimukset Varalaitteet	Varmuuskopiointi Huoltosopimukset Varalaitteet	Varmuuskopiointi Huoltosopimukset Varalaitteet
Muuta huomioon otettavaa	Vastakeinoja toteuttavat tuotteet melko uusia ja käyttökokemuksia vähän	Ratkaisut yleensä koeteltuja ja toimivia	Ratkaisut yleensä koeteltuja ja toimivia

LIITE 4: LYHENTEITÄ

2G, 2.5G, 3G	=	Matkapuhelintekniikoiden sukupolvia. GSM luetaan toiseen sukupolveen (2G), GPRS 2,5 ja UMTS kolmanteen sukupolveen. Uudemmilla sukupolvilla on edeltäjiään huomattavasti suurempi tiedonsiirtokapasiteetti.
ACL	=	*Access Control List.* Pääsynvalvonnassa käytetty tietokanta, joka määrittelee käyttäjän (tai muun objektin) oikeudet.
Biometrinen tunnistus	=	Ihmisen fysiologisiin ominaisuuksiin perustuva tunnistaminen. Mm. sormenjälki-, verkkokalvo- ja kasvojentunnistus ovat biometrisiä menetelmiä.
GPRS	=	*General Packet Radio Service.* GSM:n laajennus, joka mahdollistaa suuremman tiedonsiirtonopeuden.
IDS	=	*Intrusion Detection System.* Tietojärjestelmiin tapahtuvan tunkeutumisen havainnointiin tarkoitettu ohjelmisto.
ISDN	=	*Integrated Services Digital Network.* Tiedonsiirtotekniikka, joka on yleinen kotikäyttäjien Internet-yhteyksissä. ISDN:n tietoturvallisuus vastaa tavallisen puhelinyhteyden tietoturvallisuutta.
Palomuuri	=	Engl. Firewall. Yleisnimi laitteille ja ohjelmistoille, joiden tarkoituksena on erottaa kaksi verkkoa tai verkon osaa toisistaan siten, että verkkojen välistä liikennettä pystytään valvomaan. Yleisimmin palomuurilla erotetaan yrityksen sisäinen verkko Internetistä.
PKI	=	*Public Key Infrastructure.* Julkisen avaimen eli epäsymmetrisen avaimen menetelmä. Tietoturvaratkaisuja tukeva järjestelmä, jossa kullakin oliolla (henkilö, yritys, ohjelma jne.) on kaksi salakirjoitusavainta eli avainpari: julkinen ja salainen. Salaisella avaimella salattu viesti aukenee vai sitä vastaavalla julkisella avaimella ja julkisella avaimella salattu aukeaa vain salaisella avaimella. PKI mahdollistaa toisilleen entuudestaan tuntemattomien henkilöiden luotettavan tunnistamisen.
PPP-protokolla	=	*Point-to-Point Protocol.* Tietoliikenneyhteyksien tietoturvallisuuden lisäämiseen käytetty protokolla. PPP protokolla mahdollistaa tietoliikenneyhteyden osapuolten (laitteiden) tunnistamisen ja yhteyden salaamisen.
RADIUS ja TACACS	=	*Remote Authentication Dial-In User Service* ja *Terminal Access Controller Access Control System.* Etäkäyttäjän tunnistuksessa käytettäviä protokollia. TACACS:n kehittyneempi versio tunnetaan nimellä TACACS+.
TCP/IP	=	*Transmission Control Protocol/ Internet Protocol*. Internetin kuljetuskerroksella ja verkkokerroksella toimivia tiedonsiirtoprotokolla. Internet perustuu TCP/IP-protokollan käyttöön.
VPN	=	*Virtual Private Network.* Yleisnimi ratkaisuille, joilla Internetissä eriy-

		tetään näennäinen erillisverkko kahden verkkolaitteen väliseen tiedonsiirtoon.
WLAN	=	*Wireless Local Area Network.* Langaton lähiverkko. Verkkoratkaisu, jossa rajatulla alueella olevat koneet kytketään toisiinsa radioteitse kaapelin sijaan.

LIITE 5: LÄHTEITÄ

VAHTI:n suositukset ja VM:n ohjeet (http://www.vm.fi/vahti):

- Toimet tietoturvaloukkaustilanteissa VAHTI 7/2001 (VM 44/01/2001)
- Valtionhallinnon sähköpostien ja lokitietojen käsittelyohje, VAHTI 5/2001 (VM 34/01/2001)
- Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001 (VM 32/01/2001)
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001 (VM 30/01/2001)
- Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001 (VM 24/01/2001)
- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001 (VM 18/01/2001, 27.3.2001)
- Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje, VAHTI 4/2000 (VM 0024:00/02/99/1998)
- Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000 (VM 30/01/2000)
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000, (VM 23/01/2000, 18.8.2000)
- Valtionhallinnon tietoturvallisuuskäsitteistö, VAHTI 1/2000
- Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, VAHTI 2/1999
- Valtion etätyön tietoturvallisuussuositus, VAHTI 1/1999
- Tarpeettomaksi tulleiden tietoaineistojen hävittäminen (VM 21/01/2000, 18.4.2000)

Lait, asetukset ja periaatepäätökset:

- Laki julkisista hankinnoista (1505/1992)
- Asetus valtion hankinnoista (1416/1993)
- Henkilötietolaki (523/1999)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki sähköisestä asioinnista hallinnossa (1318/1999; uudistustyö meneillään)
- Asetus valtionhallinnon tietohallinnosta (155/1988, muutos 1401/1992)
- Valtioneuvoston ohjesääntö (1522/1995, muutos 730/2000)
- Arkistolaki (831/1994)
- Henkilökorttilaki (829/1999)
- Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)

- Asetus yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (723/1999)
- Telemarkkinalaki (369/1997)
- Valtion virkamieslaki (750/1994)
- Perustuslaki (731/1999)
- Laki yksityisyyden suojasta työelämässä (477/2001)
- Työsopimuslaki, TyösL (55/2001)
- Laki yhteistoiminnasta valtion virastoissa ja laitoksissa (725/1988)
- Rikoslaki (19.12.1889)
- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta (VM 0024:00/02/99/1998)

Muita lähteitä:

- Valtiovarainministeriö: Valtion tietotekniikan rajapintasuosituksia (27/2001)
- Kerttula, Esa: Tietoverkkojen tietoturva, Edita, 2000
- Nikander et al: Internet tietoturva, Suomen ATK-kustannus 1996
- Paavilainen, Juhani: Tietoturva, Gummerus, 1998
- Tipton – Krause (toim.): Information Security Handbook, Auerbach, 2000
- Obe, Olicer: Remote Access Networks and Services, John Wiley & Sons 1999
- Lierly et al (toim): Security complete, Sybex, 2001
- Kivimäki, Jyrki: Windows tietoturva, IT Press, 1999
- Northcutt, Stephen; Novak, Judy: Verkkomurtojen havaitseminen - analyytikon käsikirja, Kauppakaari, 2002.
- Scambray-Stuart, Joel - McClure, George: Hakkeroinnin torjunta, Gummerus 2001
- Tietosuojavaltuutetun toimisto: Tietosuojan ja tietoturvan "Tee se itse" -tarkastus, 2000