VALTIOVARAINMINISTERIÖ
Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI

Valtion tietoturvallisuuden kehitysohjelman toimeenpano

TIETOLIIKENNE- JA PÄÄTELAITTEET-TYÖRYHMÄN LOPPURAPORTTI

23.5.2006

ESIPUHE

Valtiovarainministeriö (VM) vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTIssa ovat edustettuina eri hallinnonalat ja -tasot.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi valtionhallinnon kaikkea toimintaa.

Valtionhallinnon tietoturvallisuuden johtoryhmä käsittelee valtionhallinnon tietoturvallisuutta koskevat määräykset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset.

Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynnetään laajasti myös kunnallishallinnossa, yksityisellä sektorilla, kansalaistoiminnassa ja kansainvälisessä yhteistyössä. VAHTI on tunnettu muun muassa tietoturvajulkaisuista ja –ohjeista sekä tietoturvahankkeistaan.

Sisältö

1 Johdanto

Matkapuhelimet ovat muuttumassa mobiileiksi päätelaitteiksi ja ne ovat tulossa arkiseen käyttöön kaikissa työyhteisöissä puhekäytön lisäksi myös organisaation tietojenkäsittelyvälineinä. Kämmenmikrot ja kannettavat tietokoneet ovat jalostumassa mobiilikäyttöön yhä paremmin sopiviksi. On tarpeellista selvittää mobiiliteknologian tuomat todelliset hyödyt ja niihin liittyvät kustannukset ja riskit ennen niiden ottamista työprosessin kiinteäksi ja organisoiduksi osaksi. Mobiiliteknologian oleellinen hyöty on riippumattomuus paikasta, usein myös ajastakin. Työtehtäviin käytettävän työkalun käyttö yksityisiin tarkoituksiin ja yksityisen välineen käyttö työtehtäviin tulee määritellä.

Raportin tavoitteina on:

- kuvata viestinnän irtautumista vanhoista välinekäsitteistä,
- kiinnittää huomiota etäkäytön tavoitteiden arviointiin ja niiden suhteuttamista todellisiin riskeihin,
- kuvata oikea kysymyksenasettelu, välineiden valinta ja ohjeistaminen lähivuosina
- antaa eväitä visiointiin tehokkaasta paikkariippumattomasta tulevaisuudesta, sekä
- tarjota välineitä siihen, miten etäkäytettävät palvelut kannattaa vyöhykkeistää tai turvaluokitella.

Raportti on tarkoitettu henkilöille, joiden tehtäviin kuuluu organisaatio- tai toimintokohtaisten tietoliikenne- ja viestintälinjauksien ja ohjeiden valmistelu tai niistä päättäminen, joilla on perustiedot raportin käsittelemästä teknologiasta ja joille VAHTI-ohjeet ovat tuttuja. Raportti ei kohdeorganisaatioiden moninaisuuden vuoksi ole ratkaisuiltaan ja suosituksiltaan yksityiskohtainen.

Raportin rajaus:

- VAHTI 2/2003 (turvallinen etäkäyttö turvattomista verkoista) on käyttökelpoinen. Tämä raportti käsittelee samaa problematiikkaa ajankohtaisella käytännön tasolla.
- Raportti koskee oman fyysisesti rajatun toimitilan ulkopuolelle ulottuvaa viestintää (mukaanlukien radioaallot, joiden liikkuminen valvotun tilan ulkopuolelle on estettävissä vain kalliin kuorisuojauksen avulla).
- Raportti keskittyy organisaation sisäisiin toimintoihin. Asiakkaille tarkoitetut viestinnän muodot on jätetty tarkastelun ulkopuolelle.

2 Hankkeen toteutus

Hanke toteutettiin virkatyönä ja se on osa valtionhallinnon tietoturvallisuuden kehitysohjelmaa 2004-2006 (VAHTI 1/2004). Pääasiallinen työmuoto oli työpaja-muotoiset kokoukset, joita

pidettiin 4 kappaletta keväällä 2005. Toissijaisena työmuotona oli sähköpostitse toimitettu tekstin viimeistely. Työryhmä on työskennellyt VAHTIn ohjauksessa ja alaisuudessa.

Puheenjohtaja:
tietoturvapäällikkö Mats Kommonen, Turun yliopisto

Jäsenet:
erikoissuunnittelija Jorma Huttunen, Etelä-Suomen lääninhallitus
tietoliikenneasiantuntija Tuomo Huuppola, Ilmailulaitos
tietoturva-asiantuntija Pasi Hänninen, Viestintävirasto
luokkavastaava Toni Härkönen, Helsingin kauppakorkeakoulu
tietoverkkoasiantuntija Martti Jokipii, Tampereen tekninen yliopisto
erikoistutkija Kari Karlsson, Ilmatieteen laitos
kehityspäällikkö Leo Kaunisto, Tampereen tekninen yliopisto
tietoturvapäällikkö Sami O. Koskinen, Teknillinen korkeakoulu
järjestelmäasiantuntija Kari Likovuori, työministeriö
majuri Perttu Luhtakanta, Pääesikunta
tietoliikenneasiantuntija Petri Ollikainen, Ilmailulaitos
tietoliikenneasiantuntija Ilkka Peräläinen, valtiovarainministeriö
projektipäällikkö Olli-Pekka Rissanen, valtiovarainministeriö
osastoinsinööri Pekka Ylitalo, Pääesikunta
tietoturvapäällikkö Mauri Rosendahl, Helsingin yliopisto
tutkija Ilkka Uusitalo, VTT Elektroniikka
tietohallinnon päällikkö Heikki Sinervo, Elinkeinoelämän Keskusliitto EK
tietotekniikkapäällikkö Seppo Perkiö, Elinkeinoelämän Keskusliitto EK

Työryhmän toimeksianto oli kohtuullisen laaja, sen tarkentamiseksi työryhmä aloitti työnsä nykyisen VAHTI-ohjeiston läpikäymisellä ja perusteellisella keskustelulla annetun tehtäväalueen yleisestä problematiikasta. Keskustelun perusteella työryhmä teki VAHTIlle tarkentavan esityksen tehtävänannosta ja rajaukseksi sovittiin organisaatioiden oman toiminnan ja erilaisten mobiilikäyttötekniikoiden välinen suhde ajankohtaisesta näkökulmasta.

3 Yleinen problematiikka

Luvussa käsitellään ensisijaisesti työvälineitä. Tilanteessa, jossa paineet mobiilikäyttöön ovat jo kovat, erillinen mobiilikäytön suunnitteluprosessi voi auttaa.

Raporttia laadittaessa lähtökohtana on ollut joukko huomioita nykyisistä kehitystrendeistä:

- Uuden teknologian käyttöönoton helppous mahdollistaa ratkaisujen käyttöönoton jopa puutteellisen osaamisen ja harkinnan perusteella.
- Yhteiskunnan kehittyminen ja toimivuus tulee huomioida organisaatiokohtaisia ratkaisuja tehtäessä
  - Tavoite: Suomi on tietoteknisesti edistynyt ja teknologiaa kilpailukykyisesti hyödyntävä
  - Uuden teknologian käyttöönotossa pitäisi aina muistaa olla varovainen, mutta se ei estä olemasta päättäväinen. Kun se muistetaan, idea muuttuu innovaatioksi ja lopulta hyväksi tuotteeksi.
- Tämän hetken akuutti ongelma on lopputuloksen tiettyihin toivottuihin ominaisuuksiin keskittyvä suunnittelu, jossa ei oteta riittävästi kaikkia tekijöitä huomioon (esim. kattava tekninen riskianalyysi puuttuu)
- Työaseman vakioinnin merkitys työyhteisöissä on pääsääntöisesti tunnistettu ja hyväksytty. Rinnakkaisten sovelluksien käyttöä kannattaa välttää. Samaa ajattelutapaa tulee soveltaa myös mobiilipuolelle.
- Organisaation tulee tehdä rajoituksia yhteisen tavoitteen saavuttamiseksi:
  - Strategiset linjaukset tehdään ylimmän johdon tasolla. Panostus mobiiliteknologiaan ja sen tietoturvaan on strateginen päätös.
  - Vakioinnilla on merkittävä, mitattavissa oleva vaikutus organisaation toimintaan ja kustannuksiin

- Yksityiskäytön voi yhä paremmin hoitaa myös yksityisin välinein (hintatason lasku), mikä vähentää vakioinnin esteitä
- Kaikki, myös julkisessa käytössä olevat laitteistot ja prosessit, tarvitsevat vastuullisen pääkäyttäjän ja/tai hallinnoijan

§ Globaali Internet on paikallisen sääntelyn ulottumattomissa, sääntelemättömyyden vaikutuksiin on varauduttava sekä etäkäytössä, oman sisäverkon ulkorajalla että ulos tarjottavissa palveluissa
§ Tietosuojan osalta prosessien hallinnoijat ja käyttäjät tunnistavat entistä paremmin henkilökohtaisen vastuunsa käsittelemistään asioista ja toimintansa vaikutuksista tietosuojaan. Tietoisuutta tietoturvallisuuden merkityksestä ja oman toiminnan vaikutuksesta tietoturvaan tulee silti yhä nostaa.

3.1 Arvioinnin perustaksi

Päätelaitteiden käytön arvioinnissa on oleellista selvittää:
§ millä laitteilla käyttö voidaan sallia
§ missä määrin etäkäyttö on tarpeellista tai hyödyllistä organisaatiolle
§ missä määrin etäkäyttö on tarpeellista tai hyödyllistä työntekijälle
§ etäkäytön vaikutukset työntekoon
§ etäkäytön vaikutukset organisaatioon ja sen tietoturvallisuuteen

Jos esimerkiksi sähköpostin lukeminen työntekijän omalla kotikoneella on hyväksytty, ei tämän samaisen palvelun toteuttaminen organisaation tarjoamalla välineellä tarvitse olla myöskään sitä kontrolloidumpaa. Jos palvelua koskevat vaatimukset (luottamuksellisuus, eheys, käytettävyys) edellyttävät kontrollointia, työntekijälle on annettava siihen soveltuvat välineet. Riskiarviointi on suoritettava etukäteen, jos esimerkkinä käytetyllä sähköpostilla hoidetaan viranomaistoimintoja.

Koska virukset, vakoiluohjelmat ja identiteettivarkaudet usein iskevät ensin etäkäytettäviin koneisiin "tien päällä" oltaessa (esim puuttuvien käyttöjärjestelmä- tai torjuntaohjelmistopäivitysten seurauksena), täytyy harkita, onko etäkäytettävä toiminto tai aineisto sellaista, joka ei saa joutua vääriin käsiin. Jos näin on, pitää huolehtia seuraavista:

- valvontaketjun katkeamattomuus
  - valvonnan tulee olla koko prosessin kattava päätelaitteen näppäimistöstä lähtien. Päätelaitteeseen ei saa päästä vakoilu- tai MIM-ohjelmia. Esim. VPN on arvoton, jos sertifikaatit varastetaan kovalevyltä ja salasanat urkitaan näppäimistöltä
- kolmannen osapuolen vastuulla olevan prosessin osan sisältämän riskin poistaminen tai minimointi
  - suojauksen pitää olla putkimainen niin, että putken kummassakin päässä on vain omaa laitteistoa ja ohjelmistoa, ja niiden saastuminen on estettävä tehokkaasti ja jatkuvasti
- käyttäjä ei saa muuttaa prosessin ominaisuuksia
  - ei saisi antaa edes laitetta käyttävän työntekijän itsensä hallintaan
  - prosessilla on omistaja, jolla on oikeus muuttaa sen ominaisuuksia

Prosessin määrittely ja vakiointi sisältää myös päätelaitteiden vakioinnin ja sen tehokkaan valvonnan.

- vakioinnin tarpeellisuus on perusteltava aukottomasti sekä prosessin että laitteen osalta
- laitteen käyttötarkoitus ja mahdollinen muu hyväksytty käyttö on yksilöitävä riittävällä tarkkuudella
- muun käytön osalta määriteltävä joko kielto, tekninen este tai toinen laite

Vakiointiprosessiin liittyviä mahdollisia ongelma-alueita:

- Jos vakiointi tapahtuu organisaatiossa "kaukana" käyttäjätasosta, se toimii innovaatiota potentiaalisesti haittavana tekijänä. Vakiointi on lähtökohtaisesti sovellusten kehitystahtiin nähden jäykkää, silti vakioidun laitteiston kehittämispotentiaalia on hyödynnettävä aktiivisesti
- Vakiointi reagoi markkinoiden kehitykseen yleensä viiveellä
- Mobiililaitteet ovat voimakkaasti henkilökohtaisia välineitä, käyttövapauden rajoittaminen voi aiheuttaa vastareaktion (kuten haluttomuuden käyttää ko. välinettä)
- Vakiointiin pitäisi luoda eri tasoja käyttäjän innovointipotentiaalin mukaan; käytännössä tällainen jaottelu on vaikeaa mutta tarpeellista. Vakioinnista vastaavat tahot ovat harvoin samoja, jotka keksivät uudet käyttötavat.

3.2 Käyttäjän yksityisyyden ja välineiden käytön suhde

Tarkastelu on jaettava ensin työnantajan hallitsemaan välineeseen ja muihin. Työnantajan hallintapiiriin kuulumattomat laitteet ovat henkilön yksityisasia (vaikka ne voivat toki olla myös esim. jollekin toiselle työnantajalle kuuluvia). Organisaation vieraaksi saapuvat muun organisaation työntekijät muodostavat oman ryhmänsä, heillä voi olla sellaisia viestinnällisiä velvoitteita omaa työnantajaansa kohtaan, joihin isäntänä toimivan organisaation voi olla vaikeaa puuttua. Organisaatiolla on kuitenkin omissa tiloissaan oikeus määrätä sinne tuotavista ja siellä käytettävistä laitteista.

Mobiililaite on yhä kiinteämpi osa henkilön **yksityistä** toimintaympäristöä. Oletetaan, että hän on jatkuvasti perheensä ja ystäviensä tavoitettavissa ja että hänellä on käytettävissään teknisiä apuvälineitä, joilla hän hallitsee elämäänsä, harrastuksiaan ja sosiaalista verkostoaan. Tällaisen välineen käytön rajoittaminen työympäristössä saattaa olla entistä vaikeampaa tapahtuvassa yhteiskuntakehityksessä. Vaikka työntekijä itse ymmärtäisi yksityisten yhteyksien rajoittamisen, hänen sosiaalinen verkostonsa voi kokea asian eri tavalla. Kuvaus-, äänitys- ja tiedonsiirto-ominaisuudet löytyvät kohta kaikista mobiililaitteista. Tämä edellyttää uudenlaisen ajattelutavan omaksumista asioiden hallinnassa ja siinä, miten työntekijöitä arvioidaan ja ohjataan. Yksityisyyden ja viestintä-/tallennuskontrollin välinen ongelma täytyy erityisesti pitää mielessä tilanteissa, joissa ulkopuolisia vierailijoita otetaan kontrolloituihin tiloihin.

Työnantajan antamien mobiililaitteiden osalta on joko kiellettävä yksityinen käyttö kokonaan tai saavutettava todellinen yhteisymmärrys siitä, mitkä ovat käyttäjän yksityisen käytön raamit suhteessa työnantajan itsellään pitämään hallinnointioikeuteen. Organisaatio määrittelee turvalliset viestintätavat ja huolehtii siitä, että viestinnän turvallisuus pysyy linjassa organisaation toimintaan kohdistuvien tietosuoja- ja tietoturvavaatimusten kanssa.

Yksittäinen käyttäjä pyrkii yleensä yksinomaan siihen, että palvelunsaanti onnistuu. Onnistumiseen tarvittavien toimenpiteiden turvallisuuden arviointi voi jäädä joko toissijaiseksi tai kokonaan pois tilanteessa, jossa kaikki ei suju valmiin ohjeen mukaisesti. Vaihtoehtoisia käyttöasetuksia kokeillaan haluttuun lopputulokseen pääsemiseksi usein siinä määrin, ettei käyttäjä enää tiedä, avaako se esim. potentiaalisen salakuuntelu- tai murtomahdollisuuden.

Koska päätelaitetta käyttävän henkilön näkökulmasta eri viestintätavat eroavat yhä vähemmän toisistaan, hänelle voi myös tuottaa vaikeuksia hahmottaa eri viestintätapojen välisiä eroavaisuuksia ja erilaisia turvallisuusriskejä. Koska päätelaitteisiin ei ole standardoitu mitään tapaa, jolla viestintäkanavan tarjoaja voisi välittää palveluun liittyvää informaatiota yhteyden käyttöönoton yhteydessä, jää oppi usein saamatta ja yhteyttä käytetään täsmälleen samalla varovaisuudella tai varomattomuudella, millä aikaisempiakin yhteystapoja on käytetty.

Tieto- ja viestintäteknologia tulee vielä pitkään olemaan sellaista, ettei muu kuin ICT-alan turvallisuusaspekteihin perehtynyt ammattilainen välttämättä pysty tai halua yksin huolehtia käyttämiensä välineiden turvallisuudesta täydellisesti. Organisaation pitää pystyä

(ennaltaehkäisevästikin) kontrolloimaan sitä, ettei sellaisia potentiaalisia vuoto- tai murtoväyliä ilmesty, joita organisaatio ei itse saa valvoa.

Pitkän tähtäimen tavoite on, että mobiililaitteeseen voitaisiin suhtautua kuten asiakirjasalkkuun, ja sen sisältämiin (tai sillä etäteitse käsiteltäviin) tietoihin kuin paperilla oleviin asiakirjoihin. Samalla halutaan mahdollistaa se, että kyseistä "asiakirjasalkkua" on mahdollista kantaa suhtkoht huolettomasti, koska sen turvallisuudesta on huolehdittu teknisin keinoin. Koska teknologiaan perehtymättömälle turvaongelmien vakavuuden arvioiminen on yleensä vaikeaa, on löydettävä selkeä ja molempien osapuolten kunnioittama raja organisaation hallintaoikeuden ja yksityisen hallintaoikeuden välillä.

Organisaation tiedonhallinnan suojausvaatimusten ja työntekijän yksityisyyden yhteen sovittamien tulee olemaan lähivuosien merkittävä haaste mobiilin tiedonkäsittelyn yleistyessä.

Henkilöstön jaksaminen ja keskittymiskapasiteetti on otettava huomioon mobiilisovelluksia kehitettäessä. Jatkuvasti "ajan hermolla" oleminen ei aina ole yksinomaan hyvä asia, se voi haitata työstä irrottautumista ja latautumista. Jos työntekijän oletetaan vastaanottavan työhön liittyvää informaatiota jatkuvasti, on harkittava, minkä tasoisiin asioihin työntekijän oletetaan reagoivan vapaa-aikanaan. Myös virkamatkoilla jatkuva yhteys omaan organisaatioon kannattaa arvioida sen pohjalta, auttaako se virkamatkan onnistumista kokonaisuutena vai ei.

3.3 Mobiiliteknologian kiivaan kehitystahdin vaikutukset

Tieto- ja viestintäsovellukset kehittyvät ja monimutkaistuvat nopeasti ja niitä käytetään lähes kaikissa arkielämän ja työnteon vaiheissa. Ne edellyttävät yhä nopeampitahtista oppimista ja omaksumista. Eri sukupolvet näkevät teknologian eri silmin ja ihmisten oppimismetodit ovat erilaisia, eri tavoin teknologiaoppimiseen soveltuvia.

Tämän kehityksen vaikutukset korostuvat erityisesti mobiililaitteissa ja niiden käytössä, koska niissä käytettävät viestintäsovellukset kehitetään ja tuotteistetaan nopeasti. Vastaavasti niiden käyttöikä lyhenee uusien sovellusten korvatessa aikaisemmat. Kehitystahdin kiivaus ei kuitenkaan oleellisesti vähennä kunkin sovelluksen yksilöllisiä, erillistä opettelua vaativia ominaispiirteitä ja käyttötapoja. Näin ollen mobiilisovellusten käyttäjien on pakko käyttää oppimiskapasiteetistaan yhä suurempi osuus viestintälaitteidensa hallintaan. Tällä hetkellä kehitys on havaittavissa siitä, että varttuneempi väestö on vasta hiljalleen omaksumassa tekstiviestien käytön viestintätapana, kun nuoremmat ikäryhmät ovat siirtyneet siihen jo viimeisen kymmenen vuoden aikana. Seuraavaksi alkanee siirtyminen pikaviestinsovellusten ja puhelinverkosta irrallisten VoIP-sovellusten (yms.) laajamittaiseen hyödyntämiseen mobiililaitteissa. On nostettava esille kysymys siitä, onko muodostumassa sukupolvien välisiä kuiluja myös työelämässä sitä mukaa, kun uutta teknologiaa otetaan osaksi työntekoprosessia.

On myös huomioitava uusien viestintäsovellusten kehitysmekanismin vaikutus itse tuotteisiin. Mobiiliviestintään kohdistuva tuotekehityspanostus on valtavaa ja pyrkii luonnollisesti turvaamaan kehittäjän elinkeinon jatkumisen. Uusia teknologioita hyödyntävä organisaatio puolestaan poimii massiivisesta kehitysvirrasta parhaiten omaan toimintaansa sopivat välineet. Koska teknologian yksittäinen loppukäyttäjäorganisaatio harvoin on suorassa kosketuksessa tuotteen kehittäjään, on vaikeaa varmistaa, että valittu teknologia tulee olemaan oikea valinta pitkällä tähtäimellä, ja että sen ominaisuuksia tullaan kehittämään tätä valintaa jatkossakin tukeviin tarkoituksiin.

Tekijänoikeuksien valvontaan tarkoitetut teknologiat (Digital Rights Management, Trusted Computing Platform) on otettava huomioon arvioitaessa mobiililaitteiden tulevaisuutta ja sovelluskehitystä. Tällaisten teknologioiden pitkän aikavälin vaikutus mobiiliviestintään on vielä tuntematon, mutta asiaa pitää seurata lähivuosina erityisen tarkasti.

4 Viestintätapoja yhdistäviä ja erottavia piirteitä

Päätelaitteiden tulevaisuus ja integroitumiskehitys

- Tietokoneen ja puhelimen raja ei kohta enää ole relevantti, ominaisuudet lähentyvät toisiaan nopeasti. Molemmista tulee sovellusalusta, jossa on radioviestintäominaisuudet.
- Työelämään on saapumassa sukupolvi, jolle vanhat laitearkkitehtuurien, käsitteiden ja käyttötarkoitusten väliset raja-aidat ovat tuntemattomia.
- Päätelaitteissa on yleensä useita vaihtoehtoisia liitäntöjä; GSM, Bluetooth, WLAN, IR, Ethernet yms. On pyrittävä tehokkaasti huolehtimaan joko siitä, ettei päätelaitteessa ole tarpeettomia radiolaitteita päällä, koska ne voivat tarjota reitin asiattomalle pääsylle, tai siitä, että kukin näistä yhteyskanavista on ohjelmallisesti hyvin suojattu asiattomalta hyväksikäytöltä.

Päätelaitteiden integroitumiskehitys tuo mukanaan joukon ongelmia, jotka johtuvat täysin erilaisten perinteiden yhteensovittamisesta. Teletoiminta on raskaasti kontrolloitua ja perustuu lainsäädäntöön ja kansainvälisiin sopimuksiin, liikenne kulkee suljetuissa, kontrolloiduissa tähtimäisissä verkoissa, joissa operaattori huolehtii koko viestintäketjusta päätelaitteiden välillä, noudattaa tiukkoja käytettävyysvaatimuksia ja on velvoitettu varautumaan häiriötilanteisiin. Internet taasen on avoimiin standardeihin, vertaiskontrolliin sekä informaation monipuoliseen ja laajasti verkottuneeseen liikkumiseen perustuva hajautettu ympäristö. Molempien omat tyypilliset ominaisuudet voidaan nähdä sekä vahvuuksina että heikkouksina. Avoimissa verkoissa mahdollisuudet ja joustavuus tuovat myös riskejä, televerkoissa kontrolli tuo ennakoitavuutta erityisesti saavutettavuuden ja käytettävyyden osalta.

Integroitumiskehityksessä kannattaa pyrkiä hyötymään kunkin ympäristön tunnetuista vahvuuksista yhtaikaa ja tukea niiden kehitystä ja elinvoimaisuutta. Teleyritysten näkökulmasta nämä kaksi markkinaa ovat jo pitkälti yhdistyneet (esim. yhteiset runkoverkot huolehtivat lähes kaikesta tiedonsiirrosta), mutta eroavaisuudet päätelaiteyhteyksien tasolla tulevat vielä pysymään niin kauan, kunnes ajatusmaailmat ovat yhdistyneet. Eri asia on, kuinka pitkälle näitä ajatusmaailmoja lopulta kannattaa yhdistää.

Yhteiskunnan toimivuus on jo huomattavan riippuvainen yleisten tiedonvälitysverkkojen toiminnasta. Mikäli kaikki yleiset verkot lamaantuvat, tilanne on joka tapauksessa äärimmäisen vakava ja myös viranomaiset joutuvat siirtymään "vaikeutettuun tiedonvälitykseen" hyvin nopeasti. Näin ollen tämä raportti käsittelee normaalioloja ja lieviä häiriötilanteita, vakavimmat häiriötilat ja poikkeusolot jäävät tämän ulkopuolelle. Voidaan olettaa, että häiriötilanteessa energiansaanti ja yleisten tietoverkkojen ylläpito ovat automaattisesti korkean prioriteetin asioita ja yhteiskunta ponnistelee tässä raportissa kuvattujen kanavien toimivuuden varmistamiseksi.

Tilannekuvia arvioinnin pohjaksi:

- normaali arki
- ruuhka (yleisötapahtuma, juhlapäivä, sähkökatko, onnettomuus jne)
- tietomurto, palvelunesto, kohteena:
  - päätelaite
  - viestintäyhteys
  - organisaatio
- katastrofi
  - yhteinen ponnistelu viestintäyhteyksien pystyssä pitämiseksi
- informaatiosodankäynti
  - joku ponnistelee viestintäyhteyksien lamauttamiseksi paikallisesti tai globaalisti

Näissä eri tilanteissa mobiilikäytön onnistumiseen vaikuttavat tekijät ovat yleensä samat riippumatta siitä, mitä tiettyä ratkaisua käytetään. Kunkin tilanteen vaikutus yksittäiseen yhteystapaan on vaikea arvioida kategorisesti etukäteen.

5 Katsaus eri teknologioihin ja sovelluksiin

5.1 WLAN

5.1.1 Yleistä

Tietotekninen kehitys mahdollistaa yhä suorituskykyisempiä ratkaisuja langattomaan tiedonsiirtoon. Käyttäjäystävällisyyden lisäksi niiden etuna voi olla myös säästö verkkoinfrastruktuurin rakennuskustannuksissa. Langaton, radiotiellä tapahtuva tiedonsiirto tuo kuitenkin mukanaan riskejä, joita kaapeliverkossa ei ole. Valintoja tehtäessä nämä riskit tulisi ajoissa tiedostaa, analysoida ja hallita siten, että käsiteltävälle tiedolle taataan kaikissa olosuhteissa riittävä tietoturva. Tehty riskianalyysi tulisi myös päivittää säännöllisesti, sillä voimakkaasti lisääntyvän langattoman tiedonkäsittelyn rinnalla lisääntyy myös motiivi näitä päätelaitteita, verkkoja ja protokollia hyödyntävien haittaohjelmien tekoon ja muuhun epälojaaliin toimintaan.

Langattomalla lähiverkolla tarkoitetaan tässä 802.11-standardien mukaisia radiolähetintekniikalla toteutettuja ethernet-verkkoja (WLAN). Langaton lähiverkko on nimensä mukaisesti vain yksi mahdollinen siirtoalusta tietoliikenteelle, muilta ominaisuuksiltaan se ei teknisesti poikkea tavallisesta johtimia pitkin kulkevasta ethernet-liikenteestä. Tässä ohjeessa paneudutaan langattomuuden aiheuttamiin erityispiirteisiin.

Langattomuuden tärkein hyöty on käyttömukavuus. Kannettavaa tietokonetta ei tarvitse kytkeä johtoihin, vaan sitä voidaan käyttää tukiaseman läheisyydessä vapaasti liikutellen. Erityisesti taskukokoisia laitteita (kämmentietokoneet, puhelimet) käytettäessä käyttömukavuus korostuu.

Langaton verkko on käytettävissä täysin turvallisesti, kunhan
- sen erityispiirteet on huomioitu,
- on sovittu, millä tavalla/tasolla kukin käytettävä sovellus suojataan salakuuntelulta,
- käyttäjät on asianmukaisesti ohjeistettu, ja he noudattavat annettuja ohjeita
- verkon tietoturvallisuutta seurataan.

Arvioinnin lähtökohtana pitää olla verkossa käytettävät palvelut ja järjestelmät, ei itse verkko. Langaton verkko on vain väline, ei palvelu. (Poikkeuksena langattoman verkon tarjoaminen, mikä taasen on vierailijoille suunnattu tai yleisöpalvelu, joka pitää suunnitella ja rakentaa erikseen tämän raportin huomioita soveltaen.)

5.1.2 Erityispiirteitä

Radioteitse kulkeva tietoliikenne voidaan siepata välittömän käyttöympäristön ulkopuolelta. Parhaimmilla antenneilla tämä voidaan tehdä jopa kilometrien etäisyydeltä. Tavanomaisillakin laitteilla se on välittömästä ympäristöstä täysin tehtävissä, esimerkiksi viereisestä rakennuksesta. Paikallisverkoissa käytettävää Ethernet-protokollaa ei ole suunniteltu muun muassa salakuuntelua tai viestinnän väärentämistä vastaan. Sen langattomissa paikallisverkoissa käytettävään versioon tällaisia on kuitenkin lisätty. Toteutukset ovat kuitenkin iältään niin nuoria, ettei niiden luotettavuudesta ole vielä ollut mahdollista riittävästi varmistua. Lisäksi merkittävä osa nyt käytettävissä olevista päätelaitteista ei välttämättä osaa näistä uusimpia.

On huomattava, että langattomassa verkossa kulkeva salaamaton liikenne on aina kenen tahansa siepattavissa. Vahti 2/2000:n ohjeiden asettamissa rajoissa langatonta verkkoa voidaan käyttää, mikäli on huolehdittu siitä, että liikenne on suojattu sen luonteen edellyttämällä tavalla. Myös salattu liikenne voidaan siepata talteen etäältä, jolloin sen suojausta voidaan myöhemmin yrittää purkaa paremmin välinein ja paremmalla ajalla.

On myös muistettava, että langattomien yhteyksien häirintä on helppoa, ja siltä suojautuminen on vaikeaa. (VAHTI 5/2004, s. 58) Näin ollen tärkeät sovellukset eivät saa olla vain langattoman yhteyden varassa.

Mikäli langatonta verkkoa halutaan käyttää, on välttämätöntä huolehtia sen eristämisestä omaksi verkon osakseen, organisaation muu verkkoliikenne ei saa vahingossa reitittyä kuulumaan langattomassa verkossa.

Jos langatonta verkkoa käytetään yleisöpalvelun tarjoamiseen, on muistettava suojata muu verkko asiattomalta käytöltä; sen tulee ehdottomasti olla oma, eristetty vyöhykkeensä. Langattoman verkon asiaton käyttäjä voi olla esim. piiloutuneena valvottavien tilojen ulkopuolella tai muulla tavoin vaikeasti valvottavissa.

Langattomia verkkoja mietittäessä on hyvä muistaa, että suuren käyttäjäkunnan saaminen tietoiseksi verkkoliikenteen ominaisuuksista ja tietoturvaongelmista on hyvin vaikeaa. Keskivertokäyttäjä on palvelu- ja lopputulosorientoitunut, ja kokee turvallisuuteen liittyvät detaljit toimintaa vaikeuttavina, hankalina ja joskus pelottavinakin. Siksi on yleensä kannattavampaa opastaa käyttäjät turvallisiin käyttötapoihin positiivisin sanakääntein ja hyvään lopputulokseen tähtääviksi, ja jättää tarkempi informaatio erillisiin dokumentteihin, jotka ovat kiinnostuneempien käyttäjien saatavilla.

Käytettävissä olevia suojaus- tai rajoitusmenetelmiä

- Liikenteen salaus IP-tasolla (VPN-ratkaisut)
- Liikenteen salaus sovellustasolla (SSL, TLS jne)
- Liikenteen salaus WLAN-tasolla ("Level 2 –tasolla") (WPA, WEP)
- Suljettu WLAN (access list)
- Piilotettu SSID
- Käytön rajoittaminen sisäänkirjautumissivun avulla

Näistä erityisesti piilotettu SSID ja suljettu WLAN voivat antaa väärän turvallisuudentunteen, koska ne eivät anna suojaa liikenteen salakuuntelulta ja ovat päättäväisen tulijan kierrettävissä melko yksinkertaisin toimin. Käytön rajoittaminen sisäänkirjautumissivun avulla ei suojaa langatonta verkkoa itseään eikä myöskään siinä kulkevaa liikennettä millään tavoin. Sillä tavallisesti kontrolloidaan sitä, etteivät käyttäjä pysty ottamaan ko. verkon kautta yhteyksiä edelleen muualle ennen kirjautumista. Tämä on yleisesti käytetty tapa suurissa vierailija- ja henkilökuntaverkoissa. Näissä varsinaisen liikenteen salaaminen on oleellista.

5.1.3 Suosituksia eri käyttötarkoituksiin

Pääsääntö: Langattomassa verkossa ei koskaan saa tarjota sellaisia palveluja, jotka eivät saa olla käytettävissä myös oman sisäverkon ulkopuolelta. (Langaton verkkohan ulottuu omien tilojen ulkopuolelle, jollei tila ole radioeristetty)

Suojauksen kannattaa olla monikerroksinen. Liikenteen salaaminen L2-tasolla (802.11-protokollaperheen omat suojaustavat, WPA, WEP) tuo myös oikeudellisen suojan salakuuntelua vastaan, so. oikeudettoman kuuntelijan täytyy tehdä tietoisia toimia salauksen murtamiseksi ja rikoksen tunnusmerkistö täyttyy yksiselitteisesti. WPA- ja WEP-salaukset estävät ulkopuolisia käyttämästä verkkoa vahingossa.

Käyttäjän vahva todentaminen on ensiarvoisen tärkeää kaikissa sellaisissa järjestelmissä, joissa viranomainen käsittelee asioitaan. Vahvan todentamisen välinetarjonta paranee ja monipuolistuu ajan mittaan.

- § Hallinnolliset sovellukset; taloushallinto, henkilöstöhallinto, rekisterit, viranomaisen asianhallintajärjestelmät
  - o Ei suositeltavaa
  - o Oltava ylläpidon tiukassa kontrollissa (käyttöpolitiikka, liikennevirran valvonta)
  - o Tietoliikenteen oltava täysin salattua, yksittäiset liikennetapahtumat eivät saa olla tunnistettavissa (VPN-putki, thin client -sovellus)
- § Sähköposti
  - o Käytettävä SSL/TLS-salausta sekä vastaanotossa että lähetyksessä. Missään nimessä ei pidä käyttää salaamatonta yhteyttä. Ohjeistettava jokaiselle käyttäjälle.
- § WWW

- Vähintään WPA-suojauksen käyttö suositeltavaa. Sellaisissa vierailijaverkoissa, joissa minkäänlaista salausta ei ole käytössä, kannattaa palvelun info- tai käyttäjäntunnistussivulla erikseen mainita, ettei "normaali www-käyttö" ole välttämättä suojassa salakuuntelulta.

5.2 Matkaviestintä

Matkaviestintä: matkapuhelimet, PDA:t, kannettavat tietokoneet, **kun** niitä käytetään "tien päällä".

Lähivuosina matkaviestinnän painopiste tullee olemaan GSM/3G-pohjaisten ratkaisujen puolella.

Urbaaneissa ympäristöissä langattomia lähiverkkoja tulee olemaan vaihtelevasti saatavilla; esimerkiksi pysähdys kahvilaan saattaa samalla avata langattoman pääsyn Internetiin. Kukaan ei kuitenkaan takaa langattoman verkon palvelujen turvallisuutta (eikä edes oikeellisuutta) samalla tasolla, kuin millä teleyritys takaa GSM:n luotettavuuden. Langattomien lähiverkkojen radiotaajuuksien vähäisyys, häiriöherkkyys ja keskinäinen kontrolloimattomuus tekevät niistä huonosti "katukäyttöön" soveltuvia.

GSM:n kehityssuunta:

- Puheliikenne ja tekstiviestit (SMS) pysyvät erillisinä toimintoina, mikä on hyvä asia kriisitilanteissa (erityisesti SMS:n toimintavarmuus ja pieni kaistankulutus). Ongelmana on osapuolten todentaminen.
  - salattujen puheyhteyksien hoitamiseen omassa hallinnassa olevat VoIP-yhteydet tai muu vahvasti salattavissa oleva laitekohtainen tapa on tarpeen luottamuksellisuuden varmistamiseksi. Tämä tarkoittaa sitä, että puhelimessa on oltava erillinen sovellus, joka on suorassa salatussa datayhteydessä organisaation omassa hallinnassa olevaan yhdyspalvelimeen. Puheliikennettä ei siis hoideta tällöin normaalina gsm-puheluyhteytenä, vaan datasiirtona.
- On kova paine siirtää myös matkapuheliikenne IP-pohjaiseksi (lankapuhelinliikennettä välitetään jo laajamittaisesti IP-protokollien avulla), mutta toistaiseksi maailmanlaajuisilla operaattorimarkkinoilla on ollut ilmeisesti muutosvastarintaa helposti laskutettavien äänipuhelujen siirtymisestä dataliikenteeksi, joka on heikommin kontrolloitavissa (laskutettavissa). On vaikea ennakoida, käynnistyykö muutos lähimpänä parina vuotena laajamittaisesti. Tämänsuuntaisia yritysratkaisuja alkaa olla jo tarjolla.
- IP-pohjaisessa matkapuhelinviestinnässä pitää huomioida, että viestintäpalvelun tarjoajana saattaa olla joku muu kuin matkapuhelinoperaattori, tai erillistä viestintäpalvelun tarjoajaa ei ole lainkaan (internet-viestintä, joka ei välity tavanomaisen puhelinverkon numerovalinnoin). Tällöin normaalisti palvelun tarjoajalle kuuluvat viestinnän luottamuksellisuuteen liittyvät vastuut kuuluvatkin joko ohjelmistoa tarjoavalle yritykselle tai käyttäjälle itselleen.
- Multimediaviestipalvelujen (MMS) kehittymistä kannattaa seurata lähivuosina. Se voi jäädä "välikausiteknologiaksi" samalla tavalla kuin WAP, koska muut viestintäpalvelutavat kehittyvät tällä hetkellä nopeasti.
- Operaattorit ja laitevalmistajat suunnittelevat jatkuvasti vapaasti liikkuvalle Internet-liikenteelle ja –standardeille vaihtoehdoiksi tehokkaampia, mutta myös paremmin kontrolloitavissa olevia viestintätapoja. Kontrolli on tarpeen tekijänoikeuksien turvaamiseksi tai yleisömäärän rajaamiseksi (sopimusvelvoitteet).
- Laajempiin yleisiin viestintätarpeisiin GPRS/EDGE & 3G (tai HSCSD)
  - Täysin riippuvainen tukiasemien kapasiteetista, kriisikuormitus katkaisee datayhteyden siinä missä puheluyhteydenkin.

Muut matkaviestimet (satelliittiyhteydet, analogiset viestimet, Virve)

- Jätetään tämän tarkastelun ulkopuolelle.

6 Internet yleisesti

Kaikessa Internet-liittymien kautta tapahtuvassa ja internet-protokollia hyödyntävässä etäkäytössä oleellisinta on vahva käyttäjätodentaminen ja vahvasti salattu yhteys, ilman näitä ei siirtoyhteydellä ole mainittavaa arvoa viranomaismielessä. (VPN, SSL-suojattu Thin Client –sovellus, SSH-putkitus tms.)

Käytettävissä olevien Internet-liittymien ominaisuuksia palveluja käyttävän näkökulmasta:

- Modeemipankit ovat pääosin "menneisyyden tuotteita", mutta niiden vahvuudeksi voi laskea sen, että hyvin monissa kannettavissa tietokoneissa on edelleen vakiovarusteena V.90-modeemi.
    - Modeemipankki voi olla taloudellisesti kannattava etäkäyttötapa paikasta, jossa on käytettävissä edullinen lankapuhelinliittymä.
    - V.90- ja V.110/120-modeemit ovat jo oleellisesti hitaampia kuin GPRS/EDGE/3G-yhteydet, mutta koska laskutus tyypillisesti perustuu yhteysaikaan eikä liikutettuun datamäärään, voi modeemiyhteydelle edelleen löytyä oma perustelunsa käytössä, jossa yhteyden varmuus on tärkeämpi kuin tiedonsiirtonopeus tai tiedonsiirtomäärä on koko ajan siirtonopeuden ylärajoilla.
    - Sopii hyvin varakanavaksi tilanteessa, jossa analogiset puhelinyhteydet ovat ainoa (turvallinen) käytettävissä oleva kanava. Näin ollen modeemikäyttöä ei vielä kannata unohtaa omasta etäkäyttövalikoimasta, jos käytettävyys vaihtelevissa olosuhteissa on tärkeää.
    - Jos modeemipankki on organisaation oma, se on ominaisuuksiltaan melko sama kuin VPN-putki; erona vain se, että VPN-ohjelmiston salausjärjestelyjen sijaan putkena toimii puhelinyhteys. Tällöin suojaus on puhelinliikenteen luottamuksellisuuden varassa.
- Yritysten, virastojen ja yhteisöjen public-verkot (WLAN/Ethernet/Bluetooth/jne.)
    - Public-verkkojen suurin ongelma on pääsynvalvonta. Jos anonymiteetti on sallittu, kuka ottaa moraalisen vastuun liittymän kautta tehdyn rikoksen lähes mahdottomasta jäljitettävyydestä?
    - Jos tällainen verkko on tarjolla, sen käyttökelpoisuus riippuu tietysti yhteyttä tarjoavan isännän harjoittamasta suojauspolitiikasta.
- ADSL/kaapelimodeemi/tms. "joka kodissa ja pajassa"
    - Suhteellisen avoin verkko
    - Saattaa olla helpohkosti häirittävissä operaattorin ratkaisuista riippuen, keskimäärin melko vikasietoinen
    - Yhteys saattaa olla rajoitettu operaattorin politiikasta riippuen. Esim. vertaisverkko-ohjelmien rajoituspolitiikka tai valmispaketteina kuluttajille tarjotut tietoturvaratkaisut saattaa vaikuttaa yhteyksien saatavuuteen.
- GPRS & 3G
    - Kokonaisuutena nykyoloissa melko luotettava väline etäyhteyksien hoitamiseen, arkikäytön eturintamaa liikkuvalle työntekijälle
    - Ruuhkautuu helposti, ainakin vielä. Riippuvainen tukiasemaverkon paikallisesta kattavauudesta.
    - Salakuunneltavissa tai häirittävissä, jos asialla on hyvin varustettu ja päättäväinen vastapuoli (vaatii ammattimaiset välineet)
    - Palvelun taso on kovin vaihteleva paikasta ja operaattorista riippuen; paranemaan päin (kilpailutekijänä nopeasti tärkeämpi kuluttajamarkkinoilla)
    - Kallis, jos liikutellaan muutakin kuin tekstiä.
- Julkiset päätteet (nettikahvilat, kirjastopäätteet jne.)
    - Ei voida käyttää viestintään, jossa identiteettikaappausta tai salakuuntelua ei saa tapahtua
    - Yleensä vain WWW-käyttö tarjoajan valitsemalla selaimella
    - Soveltuu yksityisluontoiseen viestintään
    - Yhteys saattaa olla rajoitettu tiettyihin osoitteisiin tai tiettyihin protokolliin, saattaa pakottaa käyttämään välityspalvelinta

è Kehityssuuntana on selvästi, että jonkinlainen Internet-liittymä löytyy tulevaisuudessa kaikkialta, missä modernia asutusta on. Ratkaistavaksi vielä jää, kuinka sen käyttöä hallinnoidaan ja kuka maksaa rakentamisesta ja ylläpidosta aiheutuvat laskut.

Matkapuhelinverkoissa liittymänhallinta kohdistaa kustannukset suoraan loppukäyttäjälle, lähiverkkoratkaisuissa kustannukset jäävät lähtökohtaisesti verkon rakentajalle, joka tarjoaa verkkoa joko vieraanvaraisuudesta, muun toimintansa oheispalveluna tai markkinointitarkoituksessa.

Internetin redundanssi on suuri voimavara, jota kannattaa hyödyntää

- monta vaihtoehtoista kytkeytymispistettä lähes kaikkialla, niiden yhtäaikaiseen käyttömahdollisuuteen kannatta panostaa
- siirrettävän datamäärän skaalautuvuus on varmistettava etäkäyttösovelluksissa mahdollisten ruuhkien varalta

Erityistä huomioitavaa

Graafisesti ja toiminnollisesti monipuolinen käyttöliittymä saattaa muodostua suunnattomaksi riipaksi tilanteessa, jossa data liikkuu hitaasti. Esimerkiksi asianhallintajärjestelmä, jonka WWW-käyttöliittymä on monimutkainen, raskas ja voimakkaasti edestakaisin viestivä, saattaa olla täysin käyttökelvoton ilman jatkuvaa ja häiriötöntä yhteyttä. Käyttöyritys mobiilivälineellä saattaa ongelmatilanteissa muuttua painajaiseksi ja aiheuttaa enemmän turhautumista kuin hyötyä.

Palvelujen käyttöliittymän rakentaminen siten, että se toimii vain yhdellä ratkaisulla, estää tavallisesti sen käyttämisen muilla. Tyypillinen esimerkki on selaimella käytettävän palvelun rakentaminen toimimaan vain Internet Explorerilla, jolloin palvelu ei muilla selaimilla toimi. Tällöin esimerkiksi palvelun käyttäminen älypuhelimella rajautuu automaattisesti pois. Vahvan salauksen toteuttavan ohjelmiston valinnassa pitää myös huomioida, halutaanko palvelua voitavan käyttää myös muilla kuin sillä ohjelmistolla, jolle salausjärjestelmä on tehty. Parhaimmillaan käyttöliittymät on tehty yleisten html- tai vastaavien standardien mukaisiksi, joita lähes kaikki selaimet ja laitteet osaavat käyttää, ja vastaavasti käyttäjän tunnistaminen ja viestinnän salaaminen hoidetaan kunkin alustan tarjoamilla vaihtoehtoisilla välineillä rinnakkain.

Liite 1 Voimassaoleva VAHTI-ohjeistus

VAHTI 3/2005:	Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005:	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005:	Information Security and Management by Results
VAHTI 5/2004:	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004:	Datasäkerhet och resultatstyrning
VAHTI 3/2004:	Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004:	Tietoturvallisuus ja tulosohjaus
VAHTI 1/2004:	Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006
VAHTI 7/2003:	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 6/2003:	Opas julkishallinnon tietoturvakoulutuksen järjestämisestä
VAHTI 5/2003:	Käyttäjän tietoturvaohje Datasäkerhetsanvisning för användaren User´s Information Security Instruction
VAHTI 4/2003:	Valtionhallinnon tietoturvakäsitteistö
VAHTI 3/2003:	Tietoturvallisuuden hallintajärjestelmän arviointi
VAHTI 2/2003:	Turvallisen etäkäytön arkkitehtuuri
VAHTI 1/2003:	Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 4/2002:	Arkaluonteisten kansainvälisten aineistojen käsittelyohje
VAHTI 3/2002:	Etätyön tietoturvaohje
VAHTI 1/2002:	Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 6/2001:	Tietotekniikkahankintojen tietoturvallisuustarkistuslista
VAHTI 4/2001:	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 3/2001:	Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus
VAHTI 2/2001:	Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 1/2001:	Valtion viranomaisen tietoturvallisuustyön yleisohje
VAHTI 3/2000:	Tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 2/2000:	Valtion tietoaineistojen käsittelyn tietoturvaohje (uudistettavana)
VAHTI 2/1999:	Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus (uudistettavana)

Ohjeisto löytyy VAHTIn Internet-sivuilta www.vm.fi/vahti ja ohjeita saa myös tilattua hyvin edullisesti painotalo Editasta.

VAHTIn toiminnan kokonaisuus vuodelta 2005 on kuvattuna VAHTIn toimintakertomuksessa (VAHTI 1/2006).