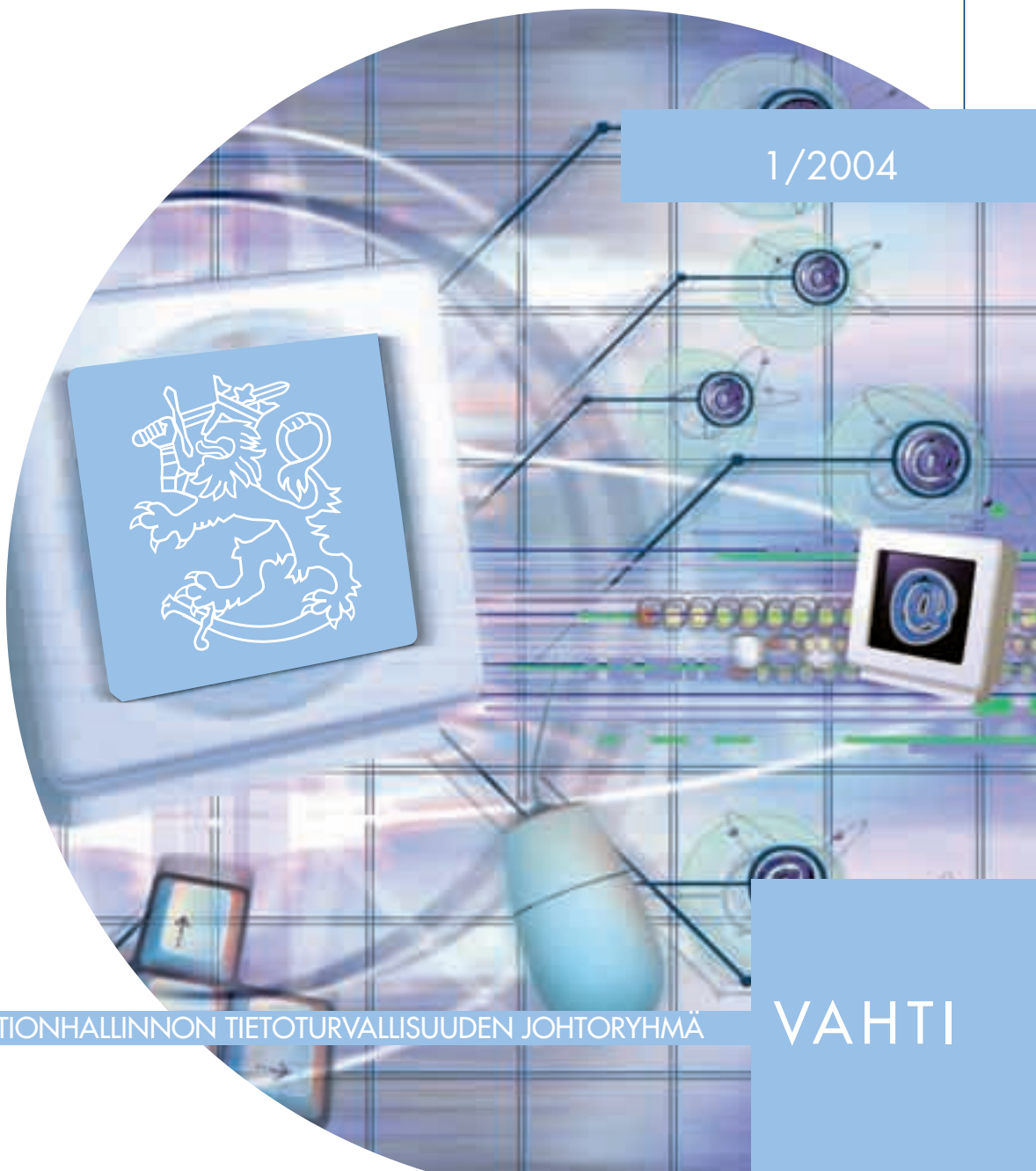
VALTIOVARAINMINISTERIÖ

VALTIONHALLINNON TIETOTURVALLISUUDEN KEHITYSOHJELMA 2004–2006



1/2004

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

VALTIONHALLINNON TIETOTURVALLISUUDEN KEHITYSOHJELMA 2004–2006

1/2004

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI 1/2004)

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
vahtijulkaisut@vm.fi

Taitto

ISSN 1455-2566
ISBN 951-804-425-2

Edita Prima Oy
HELSINKI 2004

VALTIOVARAINMINISTERIÖ VM 7/01/2004

3.3.2004

Ministeriöille, virastoille ja laitoksille

VALTIONHALLINNON TIETOTURVALLISUUDEN KEHITYSOHJELMAN TOTEUTTAMISEN KÄYNNISTÄMINEN

Valtiovarainministeriö (VM) jakaa tiedoksi ja toimenpiteitä varten valtion tietoturvallisuuden kehitysohjelman (jäljempänä ohjelma), joka on laadittu VM:n asettaman ja johtaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimesta. Ohjelmalla vastataan nykyisiin tietoturvahaasteisiin ja ennakoidaan tulevia, vahvistetaan tietoturvallisuuden yhteistoimintaa ja kehitystyötä sekä kannustetaan resurssien suuntaamista tietoturvallisuuden kannalta keskeisiin kohteisiin.

Valtionhallinnon jokaisella tasolla tulee varmistaa nykyisten resurssien riittävä kohdentaminen tietoturvatyöhön ja tietoturvallisuuden jatkuvan kehittämisen korkea prioriteetti. Ministeriöitä, virastoja ja laitoksia pyydetään toiminta- ja taloussuunnitelmissa sekä tulosohjaus- ja kehysprosesseissa ottamaan huomioon tietoturvallisuuden ja ohjelman edellyttämät resurssit.

Kehitysohjelmaan sisältyy 28 priorisoitua ja aikataulutettua kehityskohdetta, joiden osallistujatahoja on kuvattu kehitysohjelman liitteessä. Osallistujia ei rajata liitteessä mainittuihin, vaan myös muiden organisaatioiden osallistumista hankkeisiin toivotaan.

VM pyytää ministeriöitä ja virastoja ilmoittamaan osallistumisestaan kehitysohjelman lukujen 5 ja 6 hankkeisiin. Ilmoittautumisissa tulee yksilöidä ohjelman hankkeet, joihin ministeriö tai virasto osallistuu sekä ilmoittaa yhteyshenkilöt.

Osallistumisilmoitukset pyydetään toimittamaan VM:öön korkeimman prioriteetin (eli luvun 6.3) hankkeisiin 1.4.2004 ja muihin hankkeisiin 15.4.2004 mennessä:

- **valtiovarainministerio@vm.fi tai**
- **Valtiovarainministeriö, kirjaamo, PL 28, 00023 VALTIONEUVOSTO.**

Tietoturvallisuuden kehitysohjelman vastuuministeriö on valtiovarainministeriö, jonka tukena käytännön valmistelusta, koordinoinnista, seurannasta ja yhteensovittamisesta huolehtii VAHTI. Ohjelma tulee VAHTIn Internet-sivuille *www.vm.fi/vahti*. Ohjelma on tarkoitus esitellä tietoyhteiskuntaohjelman ministeriryhmälle ja ministeriöiden kansliapäälliköille sekä hallinnon ja aluekehityksen ministeriryhmälle.

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

Toinen valtiovarainministeri Ulla-Maj Wideroos

Ylijohtaja Jorma Karjalainen

Liite Valtionhallinnon tietoturvallisuuden kehitysohjelma (VM:n VAHTI-julkaisu 1/2004)

ESIPUHE JA TIIVISTELMÄ

Valtiovarainministeriö (VM) vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynnetään laajasti myös kunnallishallinnossa ja yksityisellä sektorilla.

VAHTIssa ovat edustettuina eri hallinnonalat ja -tasot. Ryhmä on tunnettu tietoturvajulkaisuista ja ohjeista. Tuore selvitys osoittaa VAHTIn menestyksellisyyden hallinnon tieto- ja viestintätekniikan sekä tietohallinnon ohjauksessa.

VAHTI muodosti elokuussa 2003 työryhmän valmistelemaan Suomen valtionhallinnon tietoturvallisuuden kehittämisohjelmaa. Tämä asiakirja esittää suunnitelman.

Tietoturvallisuuden kehitysohjelmaa sisältää 6 kehittämisaluetta, joissa on yhteensä 28 kehittämiskohdetta. Kehittämiskohteet on priorisoitu ja aikataulutettu.

Tietoturvallisuuden kehitysohjelman vastuuministeriö on valtiovarainministeriö, jonka tukena käytännön valmistelusta, koordinoinnista, seurannasta ja yhteensovittamisesta huolehtii VAHTI

FOREWORD AND ABSTRACT

Ministry of Finance is responsible for steering and development of information security in the Finnish Government and has set up The Government Information Security Management Board VAHTI[1] for co-operating, steering and developing Government information security. The results of VAHTI co-operation are also widely utilised in local government and private sector as well, besides the Finnish Government.

Members of VAHTI represent various administrative sectors and levels of public administration as well as broad information security experience. The group is well known for its data security publications and guidelines. A recent study acclaimed VAHTI as the best working organisation of cross-government ICT and information management coordination.

In autumn 2003 VAHTI set up a task force to draw a development plan for information security in the Finnish government. This document presents the plan.

The Finnish Government Information Security Development Plan covers 6 main development areas, including altogether 28 development initiatives. Development initiatives have been prioritized and implementation has been scheduled.

The Ministry of Finance has the overall responsibility for the Development Program. VAHTI group assists the Ministry in the preparation, coordination, control and alignment of the program.

[1] www.financeministry.fi/security

1 YHTEENVEDOT

1.1 Johdon yhteenveto

Tietoturvallisuus on olennainen osa tietoyhteiskunnan ja valtionhallinnon toimintaa. Sillä varmistetaan toiminnan luotettavuus ja sujuvuus kaikissa tilanteissa. Siksi tietoturvallisuutta ei tule ajatella erillisenä toimintona, vaan saattaa kiinteäksi osaksi kaikkea toimintaa.

Tietoturvallisuuteen liittyvät uhat saattavat lamauttaa viraston tai laitoksen, pahimmillaan jopa koko yhteiskunnan toiminnan. Uhat ilmaantuvat aiempaa nopeammin ja vaativat niiden torjumiseksi tarkoitetuilta vastatoimilta entistä enemmän. Tämän vuoksi on laadittu valtionhallinnon tietoturvallisuuden kehitysohjelma, jolla vastataan nykyisiin tietoturvahaasteisiin ja ennakoidaan tulevia.

Virastokohtaisesti tietoturvatyötä tulee ohjata viraston strategialla sekä toiminta- ja taloussuunnitelmilla, joiden laadinnassa tietoturvakysymykset on otettava huomioon. Toimintastrategian pohjalta laadittavalla tietoturvapolitiikalla varmistetaan tietoturvallisuus kehitettäessä ja ylläpidettäessä organisaation prosesseja ja palveluita. Ohjauksessa tulee käyttää myös tulosohjauksen keinoja, josta on valmisteilla VAHTI[2] -ohje.

Tietoturvallisuuden avulla parannetaan sekä henkilöstön että asiakkaiden luottamusta julkishallintoon, mikä osaltaan edistää verkkopalveluiden käyttöä ja siten parantaa viraston palvelutasoa, vaikuttavuutta ja tehokkuutta. Tietoturvallisuuden kehittäminen edellyttää samanaikaista kehittämistä palveluprosesseissa, toimintatavoissa, henkilöstön ja muiden käyttäjien koulutuksessa sekä teknisissä ratkaisuissa.

Tietoturvallisuuden merkitys on korostunut sähköisten palvelujen ja tietoverkkojen

[2] Valtion tietoturvallisuuden johtoryhmä VAHTI. (http://www.vm.fi/vahti) .

laajamittaisen käytön kautta. Valtionhallinnossa on tehty kattavaa tietoturvallisuuden kehittämistyötä, jonka tuloksia hyödynnetään myös kunnallishallinnossa ja yrityksissä. Tietoturvatyölle on ominaista, että se on jatkuvaa muuttuvien uhkien vuoksi. Uudet tekniikat mahdollistavat uusia toimintatapoja, mutta toisaalta järjestelmien monimutkaistuminen vaikeuttaa turvallisten järjestelmien toteuttamista.

Tietoturvallisuuden tilanne Suomessa on kansainvälisesti katsottuna varsin hyvä. Lainsäädännössä on tietoturvallisuus ja tietosuoja otettu huomioon hyvin, vaikkakin useisiin eri lakeihin hajautuneena. Joidenkin tietoturvallisuuden erityisalueiden kehittäminen ja valvonta on annettu nimettyjen virastojen vastuulle.

Lopullinen vastuu tietoturvallisuuden toteuttamisesta on jokaisella virkamiehellä, virastolla ja laitoksella. Virastoilla on kuitenkin käytettävissä hyvin erilaiset resurssit turvallisuuden hallitsemiseksi. Useimmilla suurilla virastoilla on ammattitaitoa sekä taloudellisia ja henkilöresursseja toteuttaa asioita tarvittaessa itsenäisesti. Monet pienet virastot sen sijaan tarvitsevat enemmän konkreettisia toimintaohjeita, valmiiksi neuvoteltuja puitesopimuksia sekä ulkopuolisten asiantuntijoiden hyödyntämismahdollisuuksia.

Panostaminen tietoturvallisuuteen on riippunut paljon myös viraston toimialasta ja tietovarantojen luonteesta. Virastojen välisellä yhteistyöllä ja hallinnon yhtenäisillä ratkaisuilla päästään parempaan lopputulokseen ja taloudellisuuteen kuin puhtaasti virastokohtaisilla ratkaisuilla.

Syksyllä 2003 tehdyn kyselyn[3] mukaan ajankohtaisia ongelmia virastojen tietoturvallisuudessa ovat resurssien puute, henkilöstön asenteet sekä virukset ja muut haittaohjelmat. Kaikkein akuuteimpana ongelmana kyselyssä nousi esiin roskapostin aiheuttamat sähköpostin häiriöt.

Sähköisen tiedon turvallisuuden korostuessa saattavat kuitenkin muut tietoturvan alueet, kuten paperimuotoisten asiakirjojen käsittely, jäädä liian vähälle huomiolle.

Tässä kehittämisohjelmassa on eri kehittämishankkeet koottu erilaisiin laajempiin loogisiin kokonaisuuksiin. Näitä hankealueita ovat:

1. Tietoturvakulttuurin luominen, joka sisältää tulosohjauksen käyttämisen tietoturvallisuuden kehittämiskeinona sekä monipuolista eri tahojen tuottamaa tietoturvakoulutusta. Toteutumista tulee seurata arviointien avulla.
2. Valtionhallinnon tietoturvatyön yleinen tukeminen, jota toteutetaan valtiovarainministeriön (VM) tietoturvaohjausta vahvistamalla. Erityisesti menestyksekkään VAHTIn toimintaedellytykset tulee turvata ja virastojen välistä yhteistyötä tulee tukea. Myös sitovien normien antamismahdollisuuksia parannetaan.

[3] Kehitysohjelman laadinnan tueksi tehty selvitys.

3. Tietoturvallinen viestintä ja asianhallinta, jossa painotetaan sähköisen viestinvälityksen sujuvuutta ja turvallisuutta sekä luotettavia tunnistamismenettelyjä.
4. Tietoturva- ja tietojärjestelmävastaavien työn tukeminen on tärkeä asia, sillä suuri osa tietoturvatyöstä tehdään usein joko vähäisin resurssein tai siten, että resurssit on kohdistettu tietoturvallisuuden kehittämisen sijasta muihin tavoitteisiin. Yhteishankkeilla ja hankintayhteistyöllä (kuten puitesopimukset ja yhteishankinnat) sekä sisällöltään konkreettisilla tietoturvaohjeilla pyritään helpottamaan tietoturva- ja tietojärjestelmävastaavien työtä. Resurssien kohdentamisessa vaikutetaan virastojen johtoon.
5. Toiminnan ja palvelujen kehittäjien työn tukeminen siten, että tietoturvallisuus ja yksityisyyden suoja otetaan huomioon jo palvelujen ja järjestelmien suunnitteluvaiheessa. Näin voidaan varmistaa, että toiminta on laadukasta ja säädösten mukaista.
6. Peruskäyttäjän tietoturvatyön tukeminen, jossa painottuu koulutus ja turvallisen toimintaympäristön tarjoaminen sekä johdon esimerkki ja kannustus tietoturvallisiin toimintatapoihin.

Tietoturvallisuus edellyttää virastoilta riittävää panostusta ja osaamista. Pelkkä laitteiden ja ohjelmistojen hankinta ei riitä, vaan lisäksi tarvitaan koko henkilöstön valmiuksien kehittämistä, tietohallinnon osaamisen kasvattamista sekä tietoturvallisuuden sisällyttämistä palvelusopimuksiin. Hallinnonala- ja virastokohtaisista budjeteista tulee varata riittävästi varoja tietoturvatoimien toteuttamiseksi.

Tietoturvallisuuden kehitysohjelman vastuullinen ministeriö on valtiovarainministeriö, jonka tukena käytännön koordinoinnista, seurannasta ja yhteensovittamisesta huolehtii VAHTI.

1. 2. Ledningens sammandrag

Datasäkerheten är en väsentlig del av informationssamhällets och statsförvaltningens verksamhet. Den garanterar pålitlig och smidig service i alla situationer. Därför skall datasäkerheten inte ses som en separat funktion, utan den skall integreras i all verksamhet.

De hot som anknyter till datasäkerheten kan lamslå en myndighet eller ett verk, och i värsta fall till och med alla samhällsfunktionerna. Hoten uppstår snabbare än förr och kräver allt mera av de motåtgärder som är avsedda att avvärja dem. Därför har man utarbetat ett utvecklingsprogram för datasäkerheten inom statsförvaltningen, med vars hjälp de nuvarande utmaningarna för datasäkerheten bemöts och de kommande utmaningarna förutspås.

Det myndighetsspecifika datasäkerhetsarbetet skall styras genom myndighetens strategi, samt genom verksamhets- och ekonomiplanerna, som skall utarbetas med beaktande av datasäkerhetsfrågorna. Då organisationens processer och service utvecklas och underhålls säkerställs datasäkerheten genom en säkerhetspolitik som utarbetas utgående från verksamhetsstrategin. Även resultatstyrningsmedel skall användas vid styrningen. En VAHTI-anvisning[4] om detta bereds som bäst.

Datasäkerheten förbättrar både personalens och kundernas förtroende för den offentliga förvaltningen, vilket för sin del främjar användningen av nättjänster och således förbättrar myndighetens servicenivå, samhällelig inverkan och effektivitet. Utvecklandet av datasäkerheten förutsätter samtidig utveckling av serviceprocesserna, förfaranden, utbildningen av personalen och de övriga användarna, samt av de tekniska lösningarna. Datasäkerheten har blivit allt viktigare på grund av den omfattande användningen av elektroniska tjänster och datanät. Statsförvaltningen har bedrivit omfattande datasäkerhetsutveckling, och resultaten av arbetet utnyttjas även inom kommunalförvaltningen och i företagen. Datasäkerhetsarbetet är kontinuerligt till sin karaktär på grund av de varierande hotbilderna. Nya tekniker möjliggör nya handlingssätt, men å andra sidan gör de allt mera komplicerade systemen det svårare att förverkliga säkra system.

Datasäkerhetssituationen i Finland är rätt bra i internationell jämförelse. Datasäkerheten och dataskyddet iakttas väl i lagstiftningen, även om de föreligger utspridda i flera olika lagar. Utvecklandet och övervakningen av vissa specialområden inom datasäkerheten har ålagts vissa utsedda myndigheter.

Det slutliga ansvaret för att datasäkerheten förverkligas ligger hos varje tjänsteman, myndighet och verk. Myndigheterna har dock mycket olika resurser när det gäller att administrera om säkerheten. De flesta stora myndigheterna har yrkeskompetens samt ekonomiska resurser och nödvändig personal för att vid behov genomföra saker självständigt. Många mindre myndigheter behöver däremot mera konkreta handlingsanvisningar, färdigt förhandlade ramavtal och möjligheter att utnyttja utomstående experter.

Insatser i datasäkerhet har även i hög grad varit beroende av en myndighets verksamhetsområde och karaktären av dataresurserna. Samarbete myndigheterna emellan och gemensamma lösningar för hela förvaltningen leder till bättre resultat och större ekonomisk nytta än rent myndighetsspecifika lösningar.

Enligt en förfrågan[5] som gjordes under hösten 2003 utgör otillräckliga resurser, personalens attityder samt virus och andra skadeprogram de aktuella problemen för

---

4 Ledningsgruppen för datasäkerhet i statsförvaltningen VAHTI (http://www.finansministeriet.fi/datasakerhet.

5 En utredning som gjordes till stöd för utarbetandet av utvecklingsprogrammet.

myndigheternas datasäkerhet. Störningarna i e-posten, som orsakades av skräppost, visade sig vara det allra mest akuta problemet. Då den elektroniska datasäkerheten framhävs kan dock andra områden inom informationssäkerheten, t.ex. behandlingen av pappersdokument, förbli utan tillräcklig uppmärksamhet.

I detta utvecklingsprogram har de olika utvecklingsprojekten samlats i olika, mera omfattande logiska helheter. Dessa projektområden utgörs av

1. Skapandet av en datasäkerhetskultur som innefattar utnyttjandet av resultatstyrningen som ett sätt att utveckla datasäkerheten, samt mångsidig datasäkerhetsutbildning med hjälp av olika producenter. Förverkligandet skall följas upp med hjälp av evalueringar.
2. Allmänt stödande av datasäkerhetsarbetet inom statsförvaltningen, vilket förverkligas genom att finansministeriets (FM) datasäkerhetsstyrning stärks. Speciellt den framgångsrika VAHTIs verksamhetsförutsättningar skall säkerställas och samarbetet myndigheterna emellan skall stödas. Även möjligheterna att utfärda bindande normer förbättras.
3. Datasäker information och ärendehantering, där den elektroniska kommunikationens smidighet och säkerhet samt pålitliga identifieringssätt betonas.
4. Stödandet av datasäkerhets- och datasystemansvarigas arbete är viktigt, eftersom en stor del av dataskyddsarbetet ofta sköts antingen med otillräckliga resurser eller så att resurserna har riktats mot andra mål än utvecklandet av datasäkerheten. Datasäkerhets- och datasystemansvarigas arbete underlättas med hjälp av gemensamma projekt och anskaffningssamarbete (såsom ramavtal och gemensamma anskaffningar) samt datasäkerhetsanvisningar med ett konkret innehåll. När det gäller allokeringen av resurser påverkar man myndigheternas ledning.
5. Stödandet av deras arbete, som utvecklar verksamheten och tjänsterna, på ett sådant sätt att datasäkerheten och integritetsskyddet tas i beaktande redan då tjänsterna och systemen planeras. På så sätt kan det garanteras att verksamheten håller hög klass och uppfyller bestämmelserna.
6. Stödandet av vanliga användares datasäkerhetsarbete, där utbildning och en säker verksamhetsomgivning betonas, samt ledningens exempel och uppmuntran till datasäkra handlingssätt.

Datasäkerheten förutsätter tillräcklig satsning och kompetens av myndigheterna. Det räcker inte endast med att apparater och program skaffas. Hela personalens färdigheter måste dessutom utvecklas, dataadministrationens kompetens bör ökas, och datasäkerheten skall inkluderas i serviceavtalen. Förvaltningsområds- och myndighetsspecifika budgetar skall innehålla tillräckliga anslag för genomförande av datasäkerhetsåtgärder.

Finansministeriet ansvarar för utvecklingsprogrammet för datasäkerheten. VAHTI stöder ministeriet när det gäller praktisk koordinering, uppföljning och harmonisering av programmet.

1.3 Executive Summary

Information security plays an important role in the information society and in government. Everyday operations of public authorities depend on systems and people working in a data secure way. Therefore, information security should not be considered as a separate activity but as an integral part of all processes and services and developed as such.

Information security incidents may have serious effects on a government agency, and in the worst case they may bring activities of the society into a halt. Security threats occur more and more frequently, and counter measures are increasingly difficult to take. In order to deal with all this and to prepare for future threats The Government Information Security Management Board, VAHTI has prepared The Development Plan for Finnish Government's Information Security.

Development of information security should be based on each government agency's strategy and it should be linked to agency's operational and financial planning (*toiminta- ja taloussuunnittelu).* Otherwise, data security may not be taken into account when processes and services are being developed. Management by results and performance of government agencies (*tulosjohtaminen*) should be employed when appropriate. A guide on this is being prepared by VAHTI.

Public administration needs to be trusted by its clients and its employees. A high level of information security is an all-important ingredient in building of trust in public services and eGovernment in general. Furthermore, a good level of information security properly implemented will not impede improvement on efficiency and service level. To accomplish this, processes, systems and know-how have to be developed in concert.

Information security has gained in importance as the eGovernment services have proliferated and the number of customers has picked up rapidly. Consequently, government has completed many information security development activities, many of which embrace local government. The results of these are also utilized in private sector as well.

Information security is characterised by rapidly changing threats, which call for prompt, precise and well organised counter-measures. New technologies have a dual effect. On one hand, new more efficient services and ways of working become available. On the other hand, they introduce new data security problems and add to an ever increasing complexity of system management.

Compared to many other countries, the level of information security in Finland is high. Data security and privacy have been a concern to legislators, but the number of laws governing data security and privacy is high and increasing, and the overall situation in data security legislation can be considered as rather perplexing. Responsibility for certain areas of information security have been given to selected government agencies.

Each civil servant and each government agency should assume the final responsibility for data security. Ability to develop data security varies from one agency to another. Some may be self-sufficient and have the necessary expertise and resources to carry out major development projects on their own. Others, especially small agencies, rely more on external help and services. They need how-to -guides, outside IT and consulting services and government joint procurement schemes more than their big counterparts.

Investment in data security depends on nature of agency's activities and services, and on the confidentiality of information in its possession.Co-operation between government agencies will yield better results at less cost than every agency working on their own.

As a part of preparations for the development plan a survey on data security in the Finnish government was conducted. The survey revealed that the most acute problem at hand is e-mail spamming. Other topical areas include the lack of resources devoted to information security, negligence toward data security and malicious programs, especially viruses.

Traditional data security, especially that of printed documents, should not be neglected, but it should be developed along with Internet-related security issues.

The six main development areas to guide the overall development of data security are

1. **The creation of culture for data security**. This includes various initiatives ranging from use of management by results and performance (*tulosohjaus)* to security training programs. Various metrics should be developed and employed to monitor the development of data security. They should be accompanied by security audits.
2. **The general strengthening of government information security development**. This is done mainly by assuring that both the Ministry of Finance and the Government Information Security Management Board VAHTI have enough resources to meet the growing demand for data security information. Along with VAHTI other means of co-operation and coordination will be promoted. The need for and methods of regulation for Government on data security issues will be investigated.

3. **Data security in communication and IT-systems** will become increasingly important. This development area includes fighting against spam, introducing new secure means of communications, and other ways to assure that the information technology of eGovernment will operate smoothly.
4. **IT and data security professionals work** in the front line of data security. Their time is scarce and all too often their valuable know-how is sidelined by assigning them with responsibilities which are of secondary importance. This problem will be tackled by providing them with first class and ready-to-use information security guides and by use of cross government procurement and project schemes in data security products and services.
5. **Service and process developers work needs to be supported**, so that data security and privacy protection are taken into consideration from the initial phases of service development. This minimises the possibility that a new eService would infringe privacy or data security laws.
6. **The end user data security. D**ata security training and efficient and transparent data security environment are important ingredients in end user data security as well as managers' practice-what-you-preach -attitude.

Good level of information security cannot be attained without adequate investments and expertise. Having computer security programs installed and devices up and running is a must, but information security development should not be stopped once this has been achieved. Employee computer literacy, IT managers cutting edge knowledge and service agreements inclusive data security are a prerequisite for the information security development. Funding for information security and its development programs have to be included in budgeting process.

The Ministry of Finance has the overall responsibility for the Development Program. VAHTI group assists the Ministry in the preparation, coordination, control and alignment of the program.

2 JOHDANTO

2.1 Tausta

Valtiovarainministeriö (VM) ohjaa ja yhteensovittaa valtionhallinnon tietoturvallisuutta ja sen kehittämistä. Ohjeistusta kehittää valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI), joka on VM:n asettama ja johtama, tietoturvallisuuden asiantuntemusta laajapohjaisesti edustava ryhmä.

VM on antanut tietoturvaohjeita noin 20 vuotta, ja ohjeistamista on vahvistettu vuodesta 1999 vastaamaan lisääntynyttä kysyntää ja tarvetta. Ohjeet ovat tunnettuja tietoturvatiedon lähteitä valtionhallinnossa ja niitä käytetään myös kunnallishallinnossa sekä yksityisellä sektorilla. Käytetyimpiä ohjeita ovat uusimmat, laajalle joukolle suunnatut ja erityisen ajankohtaisia tietoturva-asioita käsittelevät julkaisut. Tällaisia ovat mm. Sähköpostien ja lokitiedostojen käsittely, Lähiverkkojen tietoturvasuositus, Viranomaisen tietoturvatyön yleisohje ja Etätyön tietoturvaohje[6].

Ohjeet ovat osoittautuneet hyväksi tavaksi edistää tietoturvallisuutta valtionhallinnossa. Tiiviit ja aihe huomioon ottaen helppolukuiset ohjeet helpottavat tietoturvatyössä hyväksi havaittujen ratkaisujen, menettelytapojen ja muiden asioiden soveltamista valtionhallinnossa. Ohjeiden lisäksi tarvitaan useita muitakin toimenpiteitä ja ohjausmuotoja tietoturvallisuuden kehittämiseksi.

2.1.1 Tietoturvallisuutta koskevat normit

Suomessa ei ole yhtenäistä tietoturvalainsäädäntöä, vaan tietoturvaan liittyviä säädöksiä on kymmenissä eri laeissa. Yksittäisen viraston kannalta keskeisiä ovat perustuslaki, julkisuuslaki, henkilötietolaki, arkistolaki ja rikoslaki.

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta on annettu 11.11.1999. Periaatepäätöksen tarkoituksena on parantaa organisaatioiden toimin-

[6] Tietoja valtion tietohallinnosta ja tietotekniikasta 2002.

tojen ja tiedonkäsittelyn tietoturvallisuuden sekä henkilötietojen tietosuojan tasoa. Lisäksi päätös täsmentää tietoturvallisuuden työnjakoa ja vastuita sekä yksilöi keskeisiä viranomaisten tehtäviä. Tietoturvallisuuden parantaminen tapahtuu kehittämällä valtionhallinnon tietoturvaperiaatteita ja antamalla tietoturvallisuuden hallintaa ja kehittämistoimenpiteitä koskevia suosituksia.

Valtioneuvoston periaatepäätös kansallisesta tietoturvastrategiasta on tehty 4.9.2003. Strategiaan on koottu linjauksia ja toimia, joilla tietoturvallisuutta ja yksityisyyden suojaa voidaan parantaa.

2.1.2 Kansainvälinen kehitys

Tietoturvallisuuden kehitys on suuressa määrin riippuvainen kansainvälisestä kehityksestä. Uhat ovat kansainvälisiä, mutta myös vastatoimia suunnitellaan monikansallisena yhteistyönä. Tämän merkitys on noussut voimakkaasti viime vuosien aikana, jolloin EU, OECD[7] ja muut kansainväliset toimijat ovat tuoneet tietoturvallisuutta esiin niin itsenäisenä asiana kuin osana muuta toimintaa, etenkin tietoyhteiskuntakehitystä.

VM:n ja VAHTIn rooli kansainvälisen tietoturvatyön tulosten tuomisessa Suomen julkishallintoon korostuu. Tulokset on välitettävä nopeasti, niistä on tiedotettava ja niiden vaikutukset on arvioitava. Tämä korostaa tietoturvatiedon nopean jakamisen ja sitä kautta jakelukanavien merkitystä.

Suomi on monessa suhteessa tietoturvatyössä kansainvälisessä kärjessä, joten tiedon välittäminen suomalaisesta tietoturvatyöstä kansainvälisiin järjestöihin on jo ajankohtaista.

EU:n tietoturvaviraston perustaminen ja muu Eurooppa-tasoinen tietoyhteiskuntakehitys on merkittävä vaikuttaja suomalaisessa tietoturvakehityksessä.

Kansainvälisen standardointitoiminnan profiili on noussut, ja toiminta on laajentunut teknisestä standardoinnista toiminnallisten asioiden standardointiin. Puhtaiden tietoturvastandardien lisäksi on laaja joukko tietoturvallisuuteen merkittävästi vaikuttavia standardeja.

Hyvä esimerkki kansainvälisestä ja voimakkaasti verkostoituneesta tietoturvatoiminnasta on CERT-toiminta, johon Suomessa toimiva CERT-FI aktiivisesti osallistuu.

---

[7] Valtiovarainministeriö ja muut valtionhallinnon tietoturvatoimijat osallistuvat OECD:n tietoturvatyöhön (http://www.oecd.org/) . VM on kääntänyt OECD:n linjauksia suomeksi (http://www.vm.fi/) .

2.2 Työryhmä ja -menetelmät

Jotta valtionhallinnon tietoturvatyö pystyisi vastaamaan nykyisiin ja tuleviin haasteisiin, VAHTI perusti elokuussa 2003 työryhmän suunnittelemaan tietoturvatyön kehittämistä. Työryhmän muodostivat seuraavat henkilöt:

Mikael Kiviniemi	Neuvotteleva virkamies	valtiovarainministeriö (pj)
Reijo Aarnio	Tietosuojavaltuutettu	Tietosuojavaltuutetun toimisto
Ari Uusikartano	Neuvotteleva virkamies	kauppa- ja teollisuusministeriö
Antero Taimiaho	Tietohallintopäällikkö	sosiaali- ja terveysministeriö
Seppo Sundberg	Tietoturvapäällikkö	Valtiokonttori
Kaarlo Korvola	Tietohallintopäällikkö	sisäasiainministeriö
Risto Yrjönen	Neuvotteleva virkamies	maa- ja metsätalousministeriö
Kalevi Hyytiä	Tietoturvallisuuspäällikkö	Pääesikunta
Irma Nieminen	Tietohallintopäällikkö	opetusministeriö
Pekka Sinkkilä	Tietohallintopäällikkö	liikenne- ja viestintäministeriö

Työryhmää ovat avustaneet HM&V Research Oy:n konsultit:

Tapani Seppänen	
Tuomo Muhonen	
Olli-Pekka Soini	työryhmän sihteeri

Työryhmän työn ensisijaisena tavoitteena oli valtionhallinnon ministeriöiden, virastojen ja laitosten tietoturvallisuuden parantaminen, mutta tämän tavoitteen rinnalla pohdittiin keinoja, joilla virastot ja laitokset voivat parantaa myös koko suomalaisen yhteiskunnan tietoturvallisuuden tasoa.

Työn lopputulokseksi haluttiin laaja kehitysohjelma, joka sisältää myös uusia toimintatapoja ja -muotoja. Kehitysohjelma nivoutuu muuhun julkishallinnon kehittämiseen.

Verkkopalveluilla, tietojärjestelmillä ja sähköisellä kommunikoinnilla on entistä suurempi rooli julkishallinnon toiminnassa. Yhä useampi palvelu on saatavilla sähköisesti ja yhä useammin tietojen ensisijainen formaatti on sähköinen. Tästä huolimatta työryhmä käsitteli myös perinteisen toiminnan ja paperimuotoisten dokumenttien tietoturvallisuuden kehittämistarpeita.

Työryhmäkokousten lisäksi haastateltiin tietoturvatoimijoita, -asiantuntijoita sekä valtionhallinnon tietoturvatyön asiakkaita: virastoja, laitoksia ja muita julkishallinnon yksiköitä. Osa haastatteluista tehtiin henkilöhaastatteluna, osa sähköpostilla. Työryhmä halusi saada mahdollisimman laajan ja syvän ymmärryksen tietoturvallisuuden kehittämisen tilanteesta valtionhallinnossa, joten haastattelun kohderyhmää laajennettiin kattamaan niin tietoturvavastaavat, palvelujen kehittämisestä vastuulliset, yksiköiden johdon edustajat kuin peruskäyttäjät.

Työryhmäkokouksia, kirjallista ja sähköistä materiaalia ja haastatteluja täydennettiin aivoriihellä (*brainstorm*), jossa ideoitiin kehityskohteita, ruodittiin ehdotuksia ja arvioitiin tietoturvan kehitystä.

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) käsitteli kehitysohjelman luonnosta joulukuussa 2003 ja evästi työryhmää työn loppuunsaattamisesta. Valtionhallinnon tietoturvallisuuden kehitysohjelma esiteltiin Valtioneuvoston tietohallinnon johtoryhmälle (VATI) tammikuussa 2004, jolloin VATIn jäsenillä oli mahdollisuus kommentoida työryhmän työn tuloksia. VAHTI päätti kehitysohjelman julkaisusta helmikuussa 2004.

2.3 Ohjelman tarkoitus, kohderyhmä ja rajaus

Kehitysohjelma pyrkii omalta osaltaan konkretisoimaan tietoyhteiskuntaohjelmia ja kansallista tietoturvastrategiaa ehdottamalla yksinkertaisia, toteuttamiskelpoisia ja käytännönläheisiä hankkeita, joista useat voidaan käynnistää nopeasti. Osa toimenpide-ehdotuksista on aloitteita, joiden toteuttaminen tullee mahdolliseksi lähitulevaisuudessa.

Ohjelman ulkopuolelle on rajattu julkishallinnon yksikköjen sisällä tapahtuva tietoturvatyö, paitsi siltä osin kuin sitä voidaan tukea ohjeilla, valtionhallinnon hankkeilla tai muilla toimenpiteillä.

Tietoturvatyössä oikean, nopean ja sisällöltään korkeatasoisen tiedotuksen merkitys on suuri. Jokaisen valtionhallinnon toimijan on huolehdittava tietoturvallisuuden toteuttamisesta omalla vastuualueellaan, mutta otettava huomioon myös julkishallinnon yhteistyö ja eri osapuolten tietoturvallisuus. Toimijoiden selkeä ja tarkoituksenmukainen vastuunjako ja roolit vaikuttavat suotuisasti myös tietoturvatyöhön.

Nopeasti muuttuvassa ympäristössä on erittäin vaikeaa, jopa mahdotonta, ennustaa tulevaisuutta. Tietoturvallisuuden kehitysohjelman laatinut työryhmä totesi, että kehitysohjelman arviointi sen puolivälissä lisää joustavuutta ja mahdollistaa painopisteiden muuttamisen ohjelman kuluessa, mikäli tähän ilmenee tarvetta.

2.4 Tämän dokumentin rakenne ja käyttö

Tämän raportin luvussa 3 kuvataan lyhyesti valtionhallinnon nykyistä tietoturvatyötä, yleistä tietoturvakehityksen ohjaamista sekä muita tähän liittyviä asioita.

Raportin laadintaan liittyneen kyselytutkimuksen tärkeimmät tulokset on analysoitu luvussa 4.

Luvussa 5 esitetään keskeiset hankealueet eli ”korit” kuten niitä työn aikana nimitettiin. Ne (6 kpl) koostuvat yleisestä, asiaa ja tavoitteita kuvaavasta johdannosta, sekä tarkemmista, yksityiskohtaisemmista kehityskohteista, joita on pyritty konkretisoimaan.

Koreissa esitetyt kehityskohteet eivät ole ainoat, joita tarkastelukaudella toivotaan toteutettavan, vaan työryhmä uskoo, että raportissa esitettyjen kehityskohteiden lisäksi toteutetaan myös muita. Tietoturvan kehittäminen edellyttää myös nopeita toimenpiteitä, joita ei kehittämisohjelmassa voi ennakkoon yksilöidä.

Kehityskohteiden toteutukseen liittyvän asiat ovat luvun 6 aihe. Vastuutus ja priorisointi on käsitelty sillä tarkkuudella, kuin se kehitysohjelman tässä vaiheessa oli mahdollista. Luvussa käsitellään myös työryhmän esitys kehitysohjelman seurannasta.

3 VALTIONHALLINNON TIETOTURVAHANKKEET

3.1 Tietoturvahankkeiden merkitys

Julkisten palvelujen siirtyessä enenemässä määrin tietoverkkoihin korostuu tietoturvallisuuden merkitys jokaiselle asiakkaalle ja virkamiehelle, kansalaiselle ja yritykselle. Tietoturvaongelmat ovat saaneet huomiota tiedotusvälineissä. Suomalainen valtionhallinto nauttii kansainvälisissä vertailuissa korkeaa arvostusta omien asiakkaittensa – kansalaisten – keskuudessa. Luottamuksen säilyttäminen nopeasti muuttuvassa ympäristössä on suuri haaste. Haastavuutta lisää, että tietoturvallisuuteen vaikuttavat asiat ovat usein nopeimmin muuttuvien joukossa.

3.2 Kansallinen tietoturvastrategia

Keskeinen kansallinen tietoturvallisuuden kehittämistä ohjaava toimintasuunnitelma on kansallinen tietoturvastrategia, jota on arvosteltu konkreettisten tietoturvallisuutta edistävien hankkeiden puutteesta. Valtionhallinnon tietoturvallisuuden kehitysohjelma pyrkii omalta osaltaan edistämään strategian toteutumista jalkauttamalla ylätason tavoitteita.

Kansallista tietoturvastrategiaa laati tietoturvallisuusasioiden neuvottelukunta. Neuvottelukunnan työn pohjalta Valtioneuvosto teki periaatepäätöksen kansallisesta tietoturvastrategiasta syksyllä 2003. Strategiassa esitetään viisi keskeistä toimintaperiaatetta, joihin kuhunkin liittyy 2–4 toiminnallista tavoitetta:

1. Kansainvälinen ja kansallinen yhteistyö.
2. Yhteiskunnan kehityksen ja kansallisen kilpailukyvyn tukeminen tietoturvaa edistämällä.

3. Tietoturvariskien hallinnan kehittäminen.
4. Yksilön ja muiden toimijoiden perusoikeuksien turvaaminen.
5. Tietoturvatietoisuuden ja osaamisen kehittäminen.

Kansallisessa tietoturvastrategiassa ei käsitelty julkishallinnon sisäiseen tietoturvallisuuteen liittyviä kysymyksiä, mutta valtionhallinnon tietoturvallisuuden kehitysohjelmassa on kansallisen strategian tavoitteet pyritty ottamaan huomioon.

Kansalliseen tietoturvastrategian toteuttamisen seurantaan liikenne- ja viestintäministeriö on asettanut uuden tietoturvallisuusasioiden neuvottelukunnan, jonka toimikausi on 17.10.2003–31.5.2007.

3.3 VAHTI-ohjeet

VAHTIa pidetään valtion tietohallinnon koordinointiryhmistä kaikkein onnistuneimpana[8]. VAHTIn tietoturvatyön tärkeimmät muodot ovat olleet yhteishankkeet sekä VAHTI-ohjeiden julkaisu, joita on yhteensä 25 (tilanne joulukuussa 2003). Sähköisessä muodossa ohjeet on saatavilla valtiovarainministeriön verkkosivuilla (http://www.vm.fi/vahti, http://www.vm.fi/tietoturvallisuus ja http://www.vm.fi/vahti-ohjeet).

Työryhmän tekemässä selvitystyössä ilmeni, että VAHTI-ohjeeet arvioitiin sisällöltään korkeatasoiseksi ja kattavaksi kokonaisuudeksi. Ohjeet ovat tarkoituksenmukainen tapa levittää tietoturvatietoutta: ne ovat tiiviitä esityksiä ja ne on sovellettu valtionhallinnon erityiskysymyksiin. Useimmat ohjeet ovat tietoturvaohjeeksi pitkäikäisiä, sillä niiden tarkastelukulma ei yleensä ole rajoittunut tekniikkaan. Ohjeita hyödynnetään laadittaessa virastokohtaisia toimintaohjeita kuten tietoturvapolitiikkoja ja -ohjeita.

Useille valtionhallinnon loppukäyttäjille VAHTIn tietoturvaohjeet eivät sellaisenaan ole tuttuja, vaikka heidän käyttämänsä ohjeet on usein laadittu vastaavien VAHTI-ohjeiden pohjalta. Tämä organisaatiokohtainen soveltaminen on oleellinen osa VAHTI-ohjeissa esitettyjen asioiden ja toimintatapojen soveltamista käytäntöön, sillä valtionhallinnon yksikköjen väliset erot ovat suuret.

Valtionhallinnon tietoturvallisuuden kehitysohjelman laatinut työryhmä ei rajoittunut tarkastelemaan vain uusien ohjeiden tarvetta, vaan ohjeet nähtiin yhtenä, joskin keskeisenä keinona tietoturvatyön tavoitteiden saavuttamiseksi. Tämä näkyy luvussa 5, jossa on käsitelty työryhmän tärkeimpinä pitämiä tietoturvallisuuden kehityskohteita:

[8] Valtion tietohallinnon kehittämisen arviointi - loppuraportti, Cap Gemini Ernst & Young, 2003 sekä Valtion tietohallinnon kehittämisen arviointi -selvitys, 5/2003.

osassa lopputuloksena on ohje, mutta merkittävässä osassa jotain muuta. Tämä on luonnollinen jatko VAHTIn työn monipuolistumiselle ja laajenemiselle.

Ohjeiden määrän lisääntymisestä ja tietoturvaympäristön nopeasta muuttumista seuraa tarve päivittää nykyistä tietoturvaohjeistusta entistä tiiviimmin.

3.4 Muu tietoturvatyö

Valtiovarainministeriön vetämissä valtionhallinnon tietoturvallisuuden yhteishankkeissa useat virastot ja laitokset toimivat yhdessä tietoturvallisuuden kehittämiseksi. Useita yhteishankkeita on järjestetty vuodesta 2001 lähtien, ja yhteishanke tullaan järjestämään myös vuonna 2004. Työryhmän tekemien haastattelujen perusteella yhteishankkeita pidetään erittäin onnistuneena tietoturvatyön muotona ja niitä halutaan lisää. Yhteishankkeita toivottiin myös koko valtionhallintoa suppeampina: alakohtaisesta yhteistyöstä oli haastatelluilla hyviä kokemuksia.

Myös yhteishankintoja ja puitesopimuksia toivottiin lisää. Näillä on merkitystä etenkin pienille virastoille, joiden resurssit ovat rajalliset.

Internet on erittäin tärkeä tietoturvatiedon jakelukanava, joten useat työryhmän haastattelemista mainitsivat sen tärkeimpien tietoturvatiedon lähteiden joukossa. VAHTIn sivujen kehittäminen tukee paitsi ohjeiden myös muun tietoturvatiedon jakelua ja nostaa VAHTIn profiilia julkishallinnon tietoturvatyön keskeisenä vaikuttajana.

3.5 Valtionhallinnon verkkopalvelujen kehittäminen

Sähköiset palvelut ovat nopeassa kasvuvaiheessa. Suurin osa valtion virastoista ja laitoksista tarjoaa sähköisiä palveluita, joista pääosa on yksinkertaisia peruspalveluita, mutta kehittyneiden, interaktiivisten palveluiden yleistyminen on voimakasta. Asiakkaalle suunnattujen palveluiden rinnalla kehittyvät hallinnon sähköiset prosessit ja näiden liittäminen sähköisiin palveluihin. Tämä on edennyt hitaammin kuin asiakkaiden palvelujen sähköistäminen, mutta vauhti kiihtynee.

Palveluiden ja prosessien sähköistäminen luo tietoturvahaasteita. Prosessien ja palveluiden uhat ovat sähköisessä maailmassa toisenlaisia kuin perinteisessä. Uhkien realisoituminen saattaa johtaa nopeasti suuriin vahinkoihin, mikä ei perinteisissä palveluissa ole yhtä todennäköistä.

3.6 Meneillään olevat hankkeet

Valtionhallinnon tietoturvallisuuden kehittämisen pääpaino on ministeriöissä, virastoissa ja laitoksissa tapahtuva tietoturvatyö. Ammattitaitoisesti tehty ja oikea-aikainen ohjeiden laadinta, uhkiin vastaaminen ja muu kehitystyö on ratkaisevassa asemassa, joten sitä pyritään tukemaan hallinnon yhteisillä toimenpiteillä.

VAHTIn ohjeita ja suosituksia on julkaistu tarpeen mukaan ja tähän pyritään jatkossakin. Valtionhallinnon salausohjelmistojen yhteishankinta etenee ja VM:n yhteishankkeissa on käsitelty tietoturva- ja valmiussuunnittelua, riskien hallintaa ja tietoturvapolitiikkaa sekä muita ajankohtaisia aiheita. Turvatun sähköpostin käyttöä on testattu ja kokeiltu käytännössä.

Viestintäviraston CERT-FI-yksikkö kehittää tietoliikenteen turvallisuutta yhteistyössä operaattorien ja muiden toimijoiden kanssa. Myös CERT-FI:n toiminnassa on oleellisen tärkeää yhteistyö niin julkishallinnon sisällä kuin yksityissektorin toimijoiden kanssa.

3.7 Tietoturvatoimijat

Tietoturvallisuuden kehittäminen on kunkin hallinnonalan ja viime kädessä jokaisen viraston ja laitoksen vastuulla, mutta tietoturvallisuuden edistämisessä korostuu neljän ministeriön rooli.

Valtiovarainministeriö on vastuussa valtionhallinnon yleisestä tietoturvallisuuden ohjaamisesta ja kehittämisestä. Ministeriön sisällä vastuullinen yksikkö on hallinnon kehittämisosasto. Valtiovarainministeriön asettama valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI laatii ohjeita ja suosituksia. Toinen tärkeä toimintamuoto on yhteishankkeet ja -hankintapuitteet, joista vuoden 2004 kattava tietoturvallisuuden yhteishanke on valmisteluvaiheessa ja salaustuotteiden yhteishankinta on edennyt loppusuoralle. Näiden lisäksi ministeriö on järjestänyt tietoturvaseminaareja sekä osallistuu tietoturvatyöhön kansainvälisissä järjestöissä. Lisäksi valtiovarainministeriössä toimii valtioneuvoston tietohallintopalveluja varten Valtioneuvoston tietohallintoyksikkö (VNTHY), jossa on käynnissä mm. virkakortin käyttöönottohanke.

Liikenne- ja viestintäministeriö (LVM) vastaa sähköisen viestinnän ja teletoiminnan säätelystä. LVM:n alaisella Viestintävirastolla on vuoden 2002 alusta lähtien ollut vastuu tietoliikenneturvallisuudesta ja tietoturvaloukkausten käsittelystä. Osa tietoturvaloukkauksista johtaa rikosilmoitukseen, jolloin asiaa selvittää poliisi. Ministeriön nimittämä tietoturvallisuusasioiden neuvottelukunta edistää kansallisen tietoturvastrategian toimeenpanoa.

Oikeusministeriö valmistelee hallintoon liittyvät monet yleislait. Monet näistä sivuavat tietoturvallisuutta ja yksityisyyden suojaa.

Sisäasiainministeriön hallinnonalalla on monta valtionhallinnon tietoturvallisuuden kannalta keskeistä toimijaa. Väestörekisterikeskuksen ja Keskusrikospoliisin tietoturvarikosyksikön palveluita voidaan hyödyntää kaikkialla julkishallinnossa. Suurta kiinnostusta on herättänyt hallinnonalan virkakorttikokeilu, jonka tuloksia odotetaan.

Tietoturvallisuuden merkityksen lisääntymisen myötä yhä useammalla toimijalla on ollut rooli yhteisissä tietoturvatehtävissä. Toimijoiden roolia on kuvattu mm. valtioneuvoston periaatepäätöksessä valtion tietoturvallisuudesta 11.11.1999.

3.8 Kehittämisohjelma osana tietoyhteiskunnan kehitystä

Julkishallinnon palveluiden tarjoamisesta Internetissä ja sisäisten prosessien sähköistymisestä käytetään nimitystä eHallinto. Muutos perinteisesti suljetuista hallinnon järjestelmistä eHallintoon on ollut nopea, mikä puolestaan on altistanut viranomaisten tietojärjestelmät avoimien tietoverkkojen uhille.

Hyvin hoidettu tietoturvallisuus ja sen jatkuva kehittäminen ovat keskeiset edellytykset, jotta kansalaiset luottavat sähköisiin palveluihin ja niitä tarjoaviin viranomaisiin.

Sähköisessä ympäristössä osa tietoturvauhista on nopeatempoisia ja edellyttää välitöntä reagointia, osa puolestaan on altistavia uhkia, jotka suurentavat varsinaisten tietoturvauhkien todennäköisyyttä ja uhkien toteutuessa niistä syntyviä vahinkoja.

4 TIETOTURVATYÖN HAASTEET JA KIPUPISTEET

Onnistuneen kehittämisohjelman edellytys on riittävän luotettava arvio valtionhallinnon tietoturvallisuuden nykytilasta, kehityshankkeista sekä käsitys tilanteen kehityksestä. Tämän tavoitteen saavuttamiseksi työryhmä teki haastatteluja ja sähköpostikyselyn[9]. Haastattelut ja kyselyn vastaukset olivat korkeatasoisia ja niiden analysoinnista oli suuri apu työryhmälle.

4.1 Nykyiset ongelmat

Työryhmän näkemyksen mukaan tärkeimmät tietoturvallisuutta uhkaavat asiat valtionhallinnossa ovat:

- tietoturvatyöhön kohdennettujen resurssien puute, joka on seurausta tietoturvallisuuden liian alhaisesta priorisoinnista suhteessa muihin tavoitteisiin
- henkilöstön tietoturvatietoisuus[10]
- virukset ja muut haittaohjelmat

Tietoturvatyön keskeinen haaste julkishallinnossa on riittävien resurssien kohdentaminen tietoturvatyöhön. Ensisijaisesti resurssien allokoinnista johtuvaa puutetta ilmentää ammattitaitoisten tietoturvaihmisten työpanoksen suuntaaminen muihin töihin, mutta toissijaisesti myös rahan puute. Joissakin virastoissa määrärahoja jää käyttämättä, kun omia henkilöresursseja ei ole riittävästi.

Resurssien puutteen tasolla oleva ongelma koskee virastojen omaa henkilöstöä, joskin tilanne vaihtelee organisaatiosta toiseen. Joissain yksiköissä tietoturvallisuutta ei

[9] Tarkemmat tiedot haastatteluista ja kyselystä liitteessä.
[10] Työryhmän tekemän kyselyn perusteella joissakin yksiköissä henkilöstön asenteet ovat ongelma.

pidetä riittävän tärkeänä, eikä johto ei ole sitoutunut tietoturvallisuuteen tai on sitoutunut siihen vain nimellisesti.

Konkreettisista tietoturvauhista selkeimmin esiin tuodut ovat virukset (ja muut haitta-ohjelmat) ja roskaposti (späm, engl. *spam*). Virukset ovat vakava uhka niin tietoturvatyöntekijöiden kuin tavallisten käyttäjien mielestä, mutta palveluiden kehittämisestä vastaavat eivät koe asiaa yhtä vakavaksi. Virusuhan arvioidaan pahenevan tulevaisuudessa, vaikka tehokas virustorjunta on yleistä.

Roskaposti on vasta hiljakkoin noussut merkittäväksi tietoturvauhaksi, joka saattaa kaataa tietojärjestelmiä, eikä enää ainoastaan aiheuta pientä kiusaa sähköpostin käyttäjille. Roskapostin osalta tilanne muistuttaa viruksia: ongelman eteen joutuvat tietoturvatyötä tekevät ja tavalliset käyttäjät, eivät niinkään palveluita kehittävät. Roskapostista toivottiin VAHTIlta nykyistä ohjeistusta (5/2001) täydentävää ohjetta.

4.2 Lähitulevaisuuden haasteet

Tietoturvallisuuden lähitulevaisuus nähtiin varsin samanlaisena kuin nykyisyys. Virukset, roskapostit ja riittämättömät resurssit ovat tietoturvauhkia myös lähitulevaisuudessa. Uusina tai nykyistä merkittävästi vakavampina uhkina esiin tuotiin tietomurrot, verkkoterrorismi sekä yhteiskunnan yleisen tietotekniikkariippuvuuden aiheuttamat uhat, kuten Internetin mahdollinen lamautuminen.

4.3 Valtionhallinnon nykyinen tietoturvatyö

VAHTIn toimintaa ei kyselyssä pyydetty arvioimaan, mutta useat vastaajat antoivat palautetta: VAHTIn työ koettiin onnistuneeksi tai erittäin onnistuneeksi ja ohjeiden tasoa pidettiin enimmäkseen hyvänä. Kehityskohteet liittyvät kahteen alueeseen: tietoturvaympäristön muuttumiseen ja VAHTIn työn edelleen vahvistamiseen.

Tietoturvauhat muuttuvat nopeasti ja uhkien torjunnan keinovalikoima kehittyy jatkuvasti. Vastaajat toivoivat olemassa olevien VAHTI-ohjeiden riittävän nopeaa päivittämistä vastaamaan muuttuneita olosuhteita. Lisäksi toivottiin uusia, interaktiivisia toimintamuotoja, kuten keskustelupalstaa VAHTIn verkkosivuille.

Ohjeiden sisältöä ja määrää pidettiin hyvänä, kehittämiskohteina nähtiin helppolukuisten, yksinkertaistettujen ohjeiden määrän lisääminen. Lisäksi nähtiin tarvetta käytännönläheisemmille, soveltamista ja tietoturvatyön jalkauttamista tukeville ohjeille.

Kysyttäessä uusia toimintamuotoja tietoturvallisuuden edistämiseen tähtäävät yhteishankkeet ja -hankinnat saivat useita mainintoja. Ilmeinen tarve on myös ympärivuo-

rokautiselle help-desk -toiminnalle (CERT-FI:n resurssit riittävät tällä hetkellä vain virka-aikana tapahtuvaan päivystykseen). Tietoturvaseminaareja, koulutustilaisuuksia ja yhteistyötä yritysten kanssa haluttiin myös lisää.

Valtionhallinnossa tietoturvallisuuden kehittämisen tärkeä toimintamuoto on tietoturvaohjeiden, -politiikkojen ja muiden vastaavien dokumenttien päivittäminen. Etätyö ja etäkäyttö sekä näiden kehittäminen ovat monissa organisaatioissa keskeinen tietoturvahuolia aiheuttava asia.

4.4 Tietoturvaongelmat vastaajaryhmittäin

Tietoturvavastaavat, toimintaa ja palveluja kehittävät sekä loppukäyttäjät mieltävät tietoturvaongelmat hieman toisistaan poikkeavasti: salasanojen suuri lukumäärä on ongelma keskivertokäyttäjälle, palvelujen kehittäjälle puolestaan verkkokäyttäjän tunnistaminen. Tietoturvatyötä tekevä koettaa ratkoa etäkäyttäjien verkkoon kirjautumista. Sama asia - käyttäjien tunnistaminen ja oikeuksien hallinta - ilmenee eri tavalla eri ryhmille.

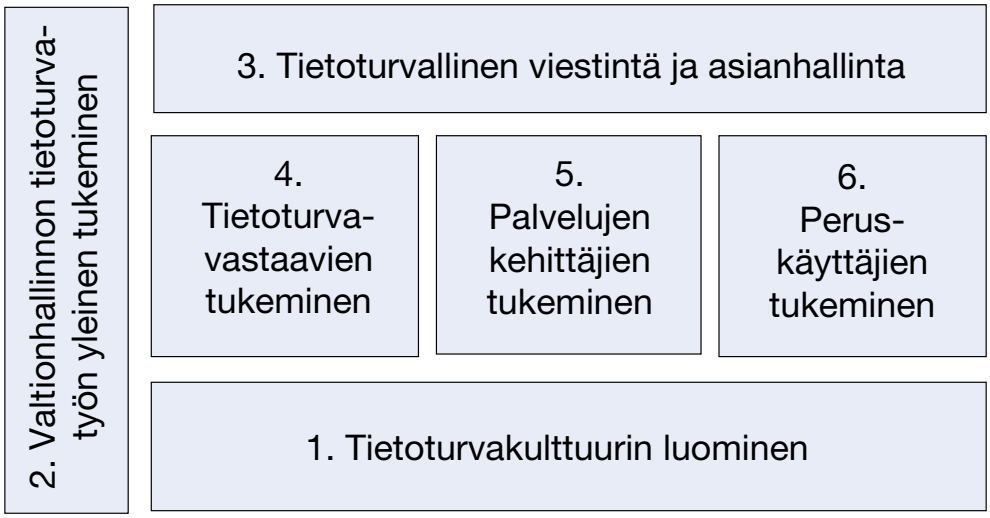
Mielenkiintoinen havainto on, että useimmat loppukäyttäjät pitivät organisaationsa tietoturvaohjeistusta melko hyvänä, joskin saatavuutta keskinkertaisena. Tietoturvavastaavat puolestaan toivoivat VAHTIlta enemmän loppukäyttäjälle suunnattua ohjeistusta ja helppokäyttöisempiä ohjeita. Tietoturvavastaavat tekevät onnistunutta työtä VAHTI-ohjeiden muokkaamisessa organisaatioidensa käyttöön, mutta resurssien vähäisyyden vuoksi he toivoisivat loppukäyttäjälle valmiimpia ohjepaketteja. VAHTI on jo tiedostanut asian ja ryhtynyt toimenpiteisiin: käyttäjän tietoturvaohje (VAHTI 5/2003) ja opas tietoturvakoulutuksesta (VAHTI 6/2003) on julkaistu kyselyn jälkeen, ja lisää materiaalia (mm. multimediaa hyödyntävää) on valmisteilla.

Tietoturvavastaavat ja palveluita kehittävät törmäävät ohjelmien tietoturva-aukkoihin. Kehittäjiä huolestuttaa palvelujen tietoturvallisuus, kun taas tietoturvaihmisten vaikeutena on tarvittavien päivitysten nopean jakelun varmistaminen.

5 TÄRKEIMMÄT KEHITYSKOHTEET

Kehityshankkeet on jaettu kuuteen hankealueeseen eli kehityskoriin. Koreista kolme on toimenpiteiden kohderyhmän mukaan nimettyjä, kaksi kaikkia kohderyhmiä tukevia ja yksi koko valtionhallinnon tietoturvatyötä tukeva.

Hankkeiden jako korien välillä voisi olla toinenkin kuin tässä esitetty, sillä useat hankkeet edistävät tietoturvallisuutta monilla eri tavoilla.



5.1 Tietoturvakulttuurin luominen

Tietoturvakulttuurin luominen ei tapahdu hetkessä, vaan edellyttää pitkäjänteistä ja määrätietoista työtä, johon valtiovarainministeriö ja VAHTI ovat omalta osaltaan osallistuneet. Tietoturvallisuuden kehitysohjelman yhteydessä tehdyssä tutkimuksessa virastojen ja laitosten tietoturvallisuudesta kävi selkeästi ilmi, että usein tietoturvakulttuuri joko puuttuu tai on vasta muodostumassa. Kulttuurin muodostuminen on paljon pidempi ja mutkikkaampi prosessi kuin yksittäisen tietoturvaongelman ratkaisu.

Jotta virastoissa kyettäisiin muodostamaan tietoturvallisuudesta samanlainen turvallisia toimintatapoja suosiva asenne kuin työturvallisuudessa vallitsee, on asiaan pyrittävä vaikuttamaan seuraavin keinoin, joita on käsitelty muualla tässä dokumentissa:

- Henkilöstön kouluttaminen.
- Johdon tietojen ja valmiuksien parantaminen.
- Avainhenkilöiden kouluttaminen ja koulutuksen suosiminen.
- Tietoturvallisuuden ottaminen mukaan tulosohjaukseen.

5.1.1 Tietoturvallisuuden tulosohjaus ja mittaaminen

Tietoturvallisuus tulee nähdä osana normaalia palvelujen ja toiminnan kehittämistä ja sen on näin ollen oltava mukana tulosohjausprosessissa. Varhaisin VAHTI-ohjeistus aihepiiristä on laadittu jo vuonna 1997. Tietojenkäsittelyn merkitys tuotannontekijänä on jatkuvasti kasvanut ja virastojen johtamisjärjestelmien kehittyminen on ollut nopeaa, joten aiheeseen liittyvän ohjeistuksen uudistaminen on ajankohtaista. VAHTI onkin valmistelemassa vuonna 2004 julkaistavaa uutta suositusta tietoturvallisuuden tulosohjauksesta.

Valtiovarainministeriön työryhmäraportin Tulosohjauksen terävöittäminen (9/2003; http://www.vm.fi/tiedostot/pdf/fi/36817.pdf) mukaan organisaation kokonaistuloksellisuus koostuu neljästä osasta: yhteiskunnallinen vaikuttavuus, toiminnan tehokkuus, laadunhallinta ja henkisten voimavarojen hallinta. Näistä tietoturvallisuudella voidaan vaikuttaa varsinkin laadunhallintaan, mutta merkittävästi myös toiminnan tehokkuuteen.

Kaiken seurannan on oltava johdettavissa yksikön toiminnallisista tavoitteista, ja tämä yhteys on oltava ymmärrettävä sekä yksikön johdolle että koko organisaatiolle. Mikäli yksikön tietoturvasuunnitelmat on laadittu toimintastrategian pohjalta, voidaan tietoturvamittarien valinnassa lähteä tietoturvasuunnitelmista. Tulee kuitenkin huomata, että suorat mittarit ovat luonteeltaan kvantitatiivisia, kun taas tietoturvallisuuden parantamisessa pyritään pääsääntöisesti laadulliseen lopputulokseen, mikä edellyttää useiden suorien mittareiden yhdistelyä.

Tietoturvallisuuden mittaamista voidaan edistää osana organisaation johtamista. Tietoturvallisuuden tasoa kuvaavat mittarit on sisällytettävä yksikön tulosten seurantaan. Tällöin tietoturvallisuus nähdään toimintaa tukevana asiana, joten se nivoutuu luontevaksi osaksi organisaation tavoitteiden seurantaa, esimerkiksi Balanced Scorecard -tyyppistä mittaristoa. Tällöin seurannan kohteena voi olla esimerkiksi sähköisen palvelun käytettävyysaste tai vasteaika.

Tietoturvallisuutta voidaan mitata suorilla ja epäsuorilla mittareilla. Suoria toiminnallisia mittareita voivat olla esimerkiksi virustorjunta ja palomuuri asennettuna ja ajan tasalla (% työasemista) ja etätyöntekijöillä VPN-yhteys (%).

Tietoturvallisuuden luonteen vuoksi epäsuorien mittarien merkitys korostuu. Epäsuorista mainittakoon:

- Tietoturvakoulutusta saaneiden henkilöiden määrä ja koulutustuntien määrä.
- Tietoturvasuunnitelmien, -ohjeiden ja muun dokumentaation kattavuus, ajantasaisuus (esim. päivitetty vuoden sisällä) ja saatavuus.

Tietoturvallisuuden mittaamista on käsitelty mm. NIST:n julkaisussa SP 800-55 Security Metrics Guide for Information Technology Systems, July 2003 (http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf).

Toimenpiteet:

- Tietoturvallisuuden sitominen tulossopimuksissa viraston toiminnallisiin tavoitteisiin.
- Valtionhallinnon tietoturvamittariston ja mittaamisperiaatteiden valmistelu ja ohjeistaminen.

5.1.2 Tietoturvallisuuden sitominen virastojen palveluihin ja prosesseihin

Tietoturvakulttuurin muodostuminen edellyttää paitsi virkamiesten ja johdon asenteiden muutosta, myös tietoturvasta vastaavien ihmisten uudenlaista asennoitumista tietoturvallisuuden ja toiminnan suhteeseen. Tietoturvallisuuden kehittäminen on muun tietohallinnon tavoin saatava aiempaa luontevammin osaksi toiminnan muuta kehittämistä ja tietoturvallisen toimintatavan tarjoamien etujen aktiivista esilletuomista. Esimerkiksi käyttäjiä vaivaavaan salasanojen runsauteen korttipohjainen tunnistaminen ja käyttäjäoikeuksien tehostunut hallinta tarjoavat mielenkiintoisia mahdollisuuksia.

Virastojen ja laitosten palvelujen ja prosessien kannalta tietoturvallisuus on liian usein erillinen kokonaisuus, jota käsittelevät tietotekniset ihmiset. Tietoturvamittarien sitominen toiminnan mittareihin on eräs varteenotettava vaihtoehto liian tekniikkakeskeisyyden välttämiseksi. Palvelun käytettävyys (*availability*) ja kehittyneitä, interaktiivisia palveluita käyttävien asiakkaiden määrä ovat mittareita, jotka ovat ensisijaisesti toiminnallisia, mutta joiden hyvän tason saavuttaminen ei ole mahdollista ilman toimivia tietoturvaratkaisuja. Parhaillaan on käynnissä VM:n johdolla tehtävä verkkopalvelun laatukriteeristö, joka sisältää myös tietoturvanäkökohtia.

Toimenpiteet:

- Kaikissa tietojärjestelmähankkeissa tulee määrittelyvaiheessa ottaa huomioon tietoturvavaatimukset.
- Palvelujen kehittämishankkeissa tullaan aktiivisesti ottamaan huomioon tietoturvallisuutta edistävien, hyväksi havaittujen ratkaisujen tarjoamat mahdollisuudet. Virkakorttihankkeista saaduista tuloksista tullaan tiedottamaan aktiivisesti.
- Hyviä, erityisesti käytettävyyttä edistävien tietoturvaratkaisujen saamaa julkisuutta tullaan edistämään tarjoamalla niitä aiheiksi ammattilehtiin.
- Tietoturvariskien hallintaa kehitetään osana toimintojen jatkuvuuden varmistamista.
- Tietoturva-asiat otetaan entistä paremmin huomioon hankintoja ja sopimuksia tehtäessä. Soveltuvin osin noudatetaan VAHTIn Valtion tietotekniikkahankintojen tarkistuslistaa (VAHTI 6/2001).

5.1.3 Tietoturva-asioiden kouluttaminen

Kansalaisten tietoturvatiedot ja taidot vaikuttavat valtionhallinnon tietoturvallisuuteen. Kansalaisten tietoturvaosaamisen parantamisen lisäksi on panostettava erityisesti korkeakoulujen tietoturvakoulutukseen, jotta tulevien verkkopalvelujen kehittäjien osaaminen vastaa valtionhallinnon tietoturvavaatimuksia.

Osana valtionhallinnon tietoturvallisuuden edistämistä tietoturvakoulutusta pyritään lisäämään kaikilla koulutuksen tasoilla. Nopein vaikutus on organisaatiokohtaisella koulutuksella sekä tietoturvahenkilöiden ammatillisella koulutuksella. Tietoturvahenkilöiden tietoturvatutkintojen suorittamista edistetään ottamalla asia esiin tulos- ja kehityskeskusteluissa. Ammatillinen tietoturvakoulutus voi olla myös hankinta- tai muun yhteistyön kohde.

Korkeakoulutasoisessa opetuksessa edistetään tietoturvallisuuden opetusta ja tutkimusta. Tietoturvallisuuteen liittyviä koulutuksen ainevalintoja tulee lisätä tietoteknisen koulutuksen ohessa myös kaupallisessa ja teknisessä korkeakouluopetuksessa. Tässä korostuu opetusministeriön rooli. Tietoturvallisuus pyritään saamaan osaksi peruskoulujen opetusohjelmaa sekä keskiasteen koulutusta.

Opetuksen edistäminen tukee selkeästi kansallista tietoturvastrategiaa ja kansalaisten yleisiä tietoyhteiskuntavalmiuksia.

Virastoja kannustetaan antamaan koko henkilöstölleen tietoturvakoulutusta. Toteutuksessa voidaan käyttää myös sopimuksia kaupallisten koulutusyritysten kanssa.

Toimenpiteet:

- Vaikutetaan tietoturvallisuusasioiden neuvottelukunnassa koulutusasioiden edistämiseksi.
- Tiivistetään yhteyksiä tietoyhteiskuntaohjelman vaikuttajiin.
- Tiivistetään viranomaisten koulutusyhteistyötä esim. valtionhallinnon yhteishankkeiden ja VM:n ohjeiden avulla.

5.1.4 Tietoturvaverkostot, -seminaarit ja hyvät toimintatavat

Tietoturvaseminaarit

Valtionhallinnossa järjestetyistä seminaareista on saatu positiivista palautetta ja niiden voidaan arvioida edistäneen verkottumista ja tietoturvakulttuurin luomista.

Seminaaritarjontaa halutaan lisätä ja laajentaa. Aiempien yleisseminaarien rinnalle halutaan kohdennettuja seminaareja. Kohdentaminen voi olla aiheen mukainen (kuten varmenteet, virkakortti tai olemassa olevien ohjeiden hyödyntäminen), henkilöstöryhmän mukainen (kuten johto tai henkilöstöhallinto) tai hallinnonalakohtainen. Tietoturva-aiheisia luentoja annetaan myös osana muita julkishallinnon seminaareja, ja tätä pyritään lisäämään.

Seminaarit tukevat useiden tässä kehitysohjelmassa esitettyjen tavoitteiden toteuttamista, sillä ne:

- Nostavat tietoturvallisuuden arvostusta virastojen johdossa työskentelevien keskuudessa.
- Tukevat verkottumista.
- Tukevat tietoturvakulttuurin muodostumista.

Toimenpiteet:

- Järjestetään seminaareja.
- Vaikutetaan kaupallisiin toimijoihin, jotta ne järjestäisivät valtionhallinnon tarpeisiin soveltuvia seminaareja.

Tietoturvaverkostot

Tehokas tietoturvatyö edellyttää ihmisten verkottumista. Valtionhallinnon tietoturvatyötä tekevien ytimellä on tiivis verkosto, jonka sisällä kommunikointi toimii hyvin. Verkoston laajentamiselle on olemassa selkeä tarve.

Verkostojen syntymistä edistetään myös hallinnonalan sisäisillä tai tietyn toiminnon poikkihallinnollisilla yhteistyöhankkeilla, joita edistetään julkishallinnon yhteishankkeiden rinnalla. Verkostoja pyritään laajentamaan myös yksityiselle sektorille.

Toimenpiteet:

- Valtionhallinnon tietoturvallisuuden yhteishankkeisiin osallistuvien verkottumista edistetään seminaareissa.
- Perustetaan tietoturva-aiheinen keskustelufoorumi, joka toimii verkossa.
- Teemakohtaiset verkostot, joiden muodostumista edistetään mm. keskustelufoorumilla ja seminaareilla. Teemoja voisi olla esimerkiksi tunnistaminen, biometriset menetelmät, SSO (kertakirjaus eli Single Sign-On) ja IDS (tietomurtohälytin eli *Intrusion Detection System*).[11]

Parhaat käytännöt

Hallituksen tietoyhteiskuntaohjelman tavoitteisiin kuuluu hyvistä toimintatavoista (*best practices*) kertovan Internet-sivuston perustaminen. Vastaavalle tietoturvaan keskittyvälle sivustolle ei ole tarvetta, mutta VM pyrkii siihen, että perustettavalla tietoyhteiskuntasivustolla esitellään myös:

- Parhaita sähköisiin palveluihin liittyviä tietoturvakäytäntöjä.
- Parhaita sähköisiä palveluita, joissa tietoturvallisuus on ollut tärkeässä mahdollistavassa roolissa.

Parhaisiin käytäntöihin liittyvässä pääministerin jakaman palkinnon arvioinnissa pyritään vaikuttamaan siten, että tietoturvallisuuden erinomaisesti toteuttavat palvelut sijoittuisivat mahdollisimman hyvin.

Parhaiden käytäntöjen syntymisessä ja tiedon leviämisessä tietoturvaihmisten verkottuminen on tärkeä osatekijä. Palkinnoilla ja muilla julkisuutta saavilla asioilla voidaan lisäksi vaikuttaa koko tietoturvallisuuden tärkeyteen.

Toimenpiteet:

- Tietoyhteiskuntaohjelman *best practices* -sivujen käyttäminen tietoturva-asioiden esittelemiseen.
- Laadittavissa ohjeissa tuodaan esiin parhaita käytäntöjä.

5.1.5 Keskustelufoorumi tietoturva-asioista

Kyselyn vastauksissa tuotiin esiin toive tietoturva-asiantuntijoiden keskustelupalstas-

[11] Tietoturvaan liittyvistä termeistä ks. Valtionhallinnon tietoturvakäsitteistä (VAHTI 4/2003).

ta, joka tukisi verkottumista ja mahdollistaisi nopean vastauksen saamisen akuuttiin tietoturvaongelmaan. Internetin kaikille avoimet keskustelupalstat ovat suosittuja, mutta niillä ei voida käsitellä arkaluontoisia asioita.

Valtionhallinnon tietoturvallisuudesta vastaaville suunnattu keskustelufoorumi, johon pääsy edellyttää vahvaa tunnistamista sekä ennakkorekisteröintiä, tarjoaisi mielenkiintoisia mahdollisuuksia. Käyttäjiksi pääsisi vain ennakkorekisteröinnin perusteella valikoitu tietoturvavaikuttajien ryhmä, jotka tunnistettaisiin laatuvarmenteella (esim. virka- tai HST-kortilla) ennen keskustelupalstalle tuloa.

Onnistuessaan palsta lisää vahvan tunnistamisen suosiota ja siitä voidaan tulevaisuudessa kehittää yhteistyön tukemiseen tarkoitettua välinettä (*kollaboraatio).*

Toimenpiteet:

- Perustetaan keskustelupalsta ja tiedotetaan siitä valtionhallinnon tietoturvavastuullisille.
- Keskustelupalsta voidaan toteuttaa aloittaa erillisenä hankkeena, tai VAHTIn sivustolla.

5.1.6 Kansainvälisen tietoturvayhteistyön kehittäminen

Tietoturvauhat ovat kansainvälisiä eivätkä tunne kieli-, kulttuuri- tai muita muureja edes siinä määrin kuin muut turvallisuusuhat. Myös vastatoimet ovat luonteeltaan samankaltaisia tai täysin samanlaisia eri maissa. Eräät tietoturvallisuutta edistävät toimenpiteet eivät edes ole mahdollisia kansallisella tasolla, vaan edellyttävät kansainvälistä, hyvin koordinoitua ja organisoitua toimintaa. Verkottuvassa maailmassa kansainväliset vaatimukset yhteisistä toimista yhteisiä uhkia vastaan lisääntyvät koko ajan.

Kansainvälistä tietoturvayhteistyötä tapahtuu monella tasolla. Tietoliikenteen, Internetin hallinnan ja ohjelmistojen tietoturva -standardointi koskee kansallisesti eri toimijoita kuin yleisten tietoturvaperiaatteiden laadinta.

Jotta valtionhallinnon tietoturvallisuutta voitaisiin kehittää, tulee kansainvälisen yhteistyön edellytyksiä parantaa ja työn tulosten soveltamista edistää.

Toimenpiteet:

- Valtionhallinnon toimijoiden sektori- ja hallinnonalakohtaista osallistumista kansainväliseen tietoturvayhteistyöhön edistetään sekä parannetaan osallistuvien tahojen välistä koordinointia.
- Kansainvälisen yhteistyön tuloksista tiedottamista tehdään yhteistyöverkostojen toiminnalla, kääntämällä tärkeimpiä yhteistyön tuloksena syntyneitä raportteja suomeksi, informoimalla valmistelussa olevista asioista valtion-

hallinnon asianosaisille tahoille sekä aktiivisesti tiedottamalla kansallisista tietoturvatoimista, joista muille maille saattaa olla hyötyä.

- Kansainvälisen tietoturvatyön kannalta keskeisimpiä aineistoja käännetään tarpeen mukaan englannin- ja ruotsinkielelle.

5.2 Valtionhallinnon tietoturvatyön yleinen tukeminen

5.2.1 VAHTIn toiminnan vahvistaminen

Vuonna 2003 tehty selvitys ja työryhmän tekemä kysely osoittavat VAHTIn toiminnan olleen menetyksellistä. VAHTIn tietoturvaohjeet ovat tunnettuja ja arvostettuja ja itse VAHTIa pidetään vakiintuneena osana valtionhallinnon tietoturvatyötä ja siihen liittyvää yhteistyötä.

Positiivisten tulosten, tietoturvatyön lisääntyvän kysynnän ja VAHTIn myötä syntynyt tietoturva-asiantuntijoiden verkottuminen ovat lisäsyitä VAHTIn toiminnan vahvistamiselle. Valtionhallinnon tietoturvallisuuden ammattitaidon ja verkottumisen lisäksi VAHTIn toiminnan sivutuotteena Suomessa on useita valtionhallinnon tietoturvallisuuden erityiskysymyksiin perehtyneitä asiantuntijoita VAHTIa avustaneissa, VAHTIn ohjeita soveltaneissa sekä valtionhallinnon kanssa toimineissa yrityksissä.

VAHTIn pääasiallisena toimintamuotona ovat olleet ohjeiden ja suositusten julkaisu sekä yhteishankkeet. Tässä kehitysohjelmassa esitetään ideoita ja aloitteita, jotka täydentävät ja tukevat näitä.

Toimenpiteet:

- Julkishallinnon sisäistä yhteistyötä tiivistetään VAHTIssa tapahtuvan kehittämisen osalta.
- Tiedottamisella, resurssien varmistamisella ja yhteistyön tiivistämisellä pyritään varmistamaan, että kaikki VAHTIn tehtäviin ja toimialaan kuuluvat tietoturvallisuuden kannalta tärkeät asiat käsitellään ryhmässä.
- Mahdollinen VM:n toimivaltuuksien laajentaminen sitovien tietoturvanormien ja määräysten antamisen osalta edellyttäisi myös VAHTIn toiminnan edelleen vahvistamista.
- VAHTIn sihteeristön toimintaa vahvistetaan.
- Valtiovarainministeriön ja VAHTIn tietoturvatyön vaatimat resurssit turvataan. VM, VAHTI, ja VAHTIssa mukana olevat tuovat aktiivisesti esiin työn

tuloksia ja työstään saamaansa positiivista palautetta.

- Valmisteilla olevien VAHTI-ohjeiden laadinnassa otetaan tarpeiden ja mahdollisuuksien mukaan yksityisen sektorin edustajia nykyistä enemmän mukaan.
- VAHTIn profiilin nostoa harkitaan. VAHTI-toiminnan esittely tietoturvamessuilla ja aktiivinen haastattelujen antaminen ovat harkittavia keinoja.

5.2.2 Tietoturvaohjeistuksen kehittäminen

Valtiovarainministeriön VAHTI-tietoturvaohjeet ovat tunnettuja ja arvostettuja. Ohjeet on yleensä laadittu hallinnollisen tietoturvan näkökulmasta ja sellaisiksi, etteivät niissä esitetyt asiat vanhene nopeasti. Näin perusohjeiden rinnalle on tullut käytännönläheisempiä, usein teknisluontoisempia ohjeita ja suosituksia. Työryhmän tekemän kyselyn mukaan vastaajat olivat tyytyväisiä ohjeistuksen määrään ja laatuun.

Nopeasti muuttuvassa ja kehittyvässä tietoturvaympäristössä tarve uusien tietoturvaohjeiden laadintaan ja olemassa olevien päivittämiseen tulee lisääntymään.

Tietoturvatiedon kysynnän jatkuva kasvu ja uhkien nopea muuttuminen edellyttää myös jatkossa useiden VAHTI-ohjeiden julkaisua vuosittain. Valtionhallinnon tietoturvallisuuden kannalta on ensiarvoisen tärkeää, että ohjeiden korkea taso ja ajanmukaisuus kyetään ylläpitämään, ja ohjeisiin liittyvät kehitysehdotukset voidaan toteuttaa.

Perinteisten ohjeiden julkaisun ohella kehitetään virastoissa tapahtuvan ohjeiden laadinnan tukemista ja julkaistujen VAHTI-ohjeiden muodostaman kokonaisuuden käytettävyyttä.

Roskapostin hallintaan, arviointeihin, käyttöoikeuksien hallintaan, sähköinen valvontaan ja yksityisyyden suojaan, käyttäjien tunnistukseen, tietoturvallisuuden hallintajärjestelmään ja riskien hallintaan toivottiin työryhmän tekemissä haastatteluissa VAHTI-ohjetta. VM on tiedostanut kyseisten ohjeiden tarpeen, ja tietoturvallisuuden hallintajärjestelmää (VAHTI 3/2003) ja riskien hallintaa (7/2003) käsittelevät ohjeet on julkaistu haastattelujen tekemisen jälkeen.

Toimenpiteet:

- Jatketaan ohjeiden laatimista. Julkaistavien ohjeiden nimistä ja sisällöstä päätetään erikseen.
- Ohjeissa hyödynnetään Internetin suomia mahdollisuuksia.
- Nykyistä ohjeistokokonaisuuden käytettävyyttä parannetaan lisäämällä sähköinen hakemisto, joka kertoo, missä VAHTI-ohjeissa asioita on käsitelty.

- VAHTI tukee osaltaan valtionhallinnon XML-strategian toteuttamista ja selvittää mahdollisuuden hyödyntää XML:ää VAHTI-ohjeissa ja muussa VAHTIn työssä.

5.2.3 Perusinfrastruktuurin tietoturvallisuus

Yhteiskunnan perusinfrastruktuurin toimivuuden varmistaminen kuuluu kansallisen tietoturvastrategian ja yleisen varautumisvelvoitteen piiriin. Tähän perusinfrastruktuuriin kuuluvat mm. sähköverkko, valtakunnalliset tietoliikenneverkot, pankkitoiminta ja liikenneinfrastruktuuri, jotka kaikki hyödyntävät tietotekniikkaa. Näiden kehittäminen ei kuulu tämän kehittämisohjelman piiriin.

Tässä yhteydessä perusinfrastruktuurilla tarkoitetaan organisaatioiden omia tietoverkkoja, tärkeimpiä tietojärjestelmiä laitteineen sekä yhteiskunnan toiminnan kannalta tärkeimpiä perusrekistereitä.

Perusinfrastruktuurin käytettävyyteen voidaan vaikuttaa varmistamalla valtionhallinnon tietoverkkojen kehittäminen ja ylläpito sekä osallistumalla aktiivisesti Internetin hallinnoinnin kehittämiseen kansainvälisissä organisaatioissa.

Yhteistyön lisääminen yksityisen sektorin kanssa tukee tätä kehityskohdetta, sillä yksityisen sektorin merkitys infrastruktuurin ylläpidossa on suuri.

Perusrekisterien tietoturvallisuus kuuluu perusinfrastruktuurin turvallisuuteen, vaikka niiden tietoturvaongelmat ovat jossain määrin erilaisia. Kaikkia tietoturvallisuuden osia kehitetään, ja eheyden varmistaminen perusrekistereissä on erittäin korkealla prioriteetilla.

Valtionhallinnon kriittisten järjestelmien turvaamiseksi käynnistetty hanke muodostaa erinomaisen pohjan perusinfrastruktuurin turvaamisesi. Hankkeen resurssien turvaaminen ja toiminnan mahdollinen laajentaminen ovat keskeisiä vaatimuksia.

Toimenpiteet:

- Turvataan valtionhallinnon viranomaisverkkojen toiminta.
- Kehitetään perusrekisterien eheyttä tukevia toimia.
- Jatketaan kehitystyötä VAHTIn käynnistämän keskeisten tietojärjestelmien turvaamishankkeen pohjalta.

5.2.4 Sitovien julkishallinnon tietoturvaa koskevien normien anto

Valtiovarainministeriö ohjaa ja koordinoi valtionhallinnon tietoturvatyötä. Ministeriö on panostanut tietoturvallisuuden kehittämiseen, mikä näkyy ohjeina ja suosituksina

sekä valtionhallinnon yhteishankkeina. Ohjeiden määrä on lisääntynyt tasaisesti, niiden laatua ja ajankohtaisuutta on kehitetty entisestään, ja yhteisten seminaarien, hankintojen ja muiden hankkeiden avulla on tuettu valtionhallinnossa tapahtuvaa kehitystyötä uusilla toimintatavoilla. Palaute on ollut positiivista ja ulkopuoliset arvioijat ovat päätyneet samankaltaiseen arvioon: valtionhallinnon sisällä tapahtuvasta tietohallintoyhteistyöstä tietoturvayhteistyö on eräs kaikkein tuloksekkaimmista.

Valtionhallinnon tietoturvatyön tulokset on nähtävä laajempina kuin vain julkiseen sektoriin rajoittuvina. Ohjeita ja suosituksia hyödynnetään yksityisellä sektorilla joko sellaisenaan tai sovellettuna, ja valtionhallinnossa omaksutut käytännöt vaikuttavat yritysten tietoturvaratkaisuihin. Valtionhallinnon tietoturvatyön yhteiskunnallinen vaikuttavuus on siis suuri, mikä asettaa vaatimuksia sen korkean tason säilyttämiselle.

Tietoturvalain tarve on kartoitettu aiemmin[12]. Lisäksi Valtiovarainministeriö on selvittänyt hallinnon tilannetta ja kartoittanut muutostarpeita vuonna 2001.

Tilanne on muuttunut etenkin viimeisten vuosien aikana. Tietoturvallisuus vaatii entistä nopeampaa reagointia, tietoturvatyö on kansainvälistynyt ja toimijoiden keskinäinen riippuvuus on toista luokkaa kuin muutamia vuosia sitten.

Ilman yleistä tietoturvalakia on selvitty, eivätkä lain puuttumisesta aiheutuneet ongelmat ole sinällään estäneet menestyksellistä tietoturvatyötä. Valtionhallinnossa on useita tietoturvatoimijoita, joiden toimivaltuudet perustuvat eri säädöksiin. Tietoliikenteestä, henkilötiedoista ja tietoaineistojen käsittelystä on lakeja, mutta säädösten muodostama kokonaisuus alkaa olla melko mutkikas. Erillislakien määrän mahdollinen kasvu vaikeuttaisi tietoturvatyötä tai ainakin sen yhteensovittamista.

Virastojen välinen yhteistyö helpottuisi, mikäli ne voisivat luottaa kaikkien noudattavan yhteistä tietoturvallisuuden minimitasoa ja mikäli toimivaltuudet tietoturva-asioissa olisi selkeästä säädelty.

Siirtyminen sitoviin normeihin ja määräyksiin (jäljempänä ”sitovat tietoturvanormit”) ei olisi niin suuri muutos kuin miltä se saattaa aluksi vaikuttaa. Tietoturvatyötä on valtionhallinnossa tehty laajasti, sillä tietoturvastrategia on yleisempi kuin tietohallintostrategia[13]. Merkittävä osa työstä perustuu VAHTI-ohjeisiin, jotka eräissä organisaatioissa on nostettu sisäisen, sitovan ohjeistuksen tasalle.

Sitovien tietoturvanormien tarve on esitetty useissa VAHTI-työryhmissä, ja myös tämän työn haastatteluissa asia on otettu vahvasti esiin.

Sitovien tietoturvanormien anto voi perustua joko tulevaisuudessa säädettävään tie-

---

12 Saarenpää et al: Tietoturvallisuus ja laki, näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä, Valtiovarainministeriö ja Lapin yliopisto, 1997

13 Tietoja valtion tietohallinnosta 2002. Tietohallintostrategia oli 68% virastoista ja laitoksista, tietoturvasuunnitelma 73%:lla.

toturvalakiin tai voimassa olevien säädösten muuttamiseen. Vaihtoehtojen selvittäminen ja arvioiminen on tehtävä pikaisesti, jotta mahdollinen lainvalmistelutyö voidaan aloittaa.

Käytännössä sitovien tietoturvanormien anto tarkoittaisi kahta asiaa. Ensinnäkin valtionhallinnon keskeisten tietoturvatoimijoiden keskinäiset vastuut tulisi määritellä selkeästi. Toiseksi, osa nykyisissä ohjeissa olevista asioista siirtyisi asteittain sitovaan normistoon normien annosta säätelevässä laissa säädetyllä menettelytavalla. Tämä puolestaan edellyttäisi monta valmistelevaa asiaa: vaikutusten arviointi, siirtymäajasta päättäminen ja resurssien vahvistaminen sitovien määräysten valmistelutyössä. Myös sitovien normien toteuttaminen virastoissa edellyttää tarvittavien taloudellisten ja henkilöresurssien lisäämistä sekä asiaan liittyvien ohjeiden antamista.

Toimenpiteet:

- Selvitetään tarpeet ja keinot valtionhallintoa koskevan sitovan tietoturvaohjauksen tiivistämiseen. Osana selvitystä käsitellään valtionhallinnon yleisen tietoturvalain säätämisen tarve.

5.2.5 Yhteistyö tietoyhteiskuntaohjelman kanssa

Yhteistyö hallituksen tietoyhteiskuntaohjelman kanssa mahdollistaa hallinnon sisäisen tietoturvatyön ohjaamisen tietoyhteiskuntakehityksen strategisten tavoitteiden mukaisesti. Vastavuoroisesti valtiovarainministeriö ja VAHTI pystyvät edistämään tietoturvallisuutta eräänä kaikkein keskeisimpänä luottamusta edistävänä tekijänä.

Eräs hallituksen tietoyhteiskuntaohjelman kohdista on kansallisen tietoturvastrategian toimeenpano. Kansallinen tietoturvastrategia on keskeinen suomalaisen tietoyhteiskunnan turvallisuuteen vaikuttava dokumentti. Tietoturvastrategiassa tehdyn rajauksen mukaan se ei käsittele hallinnon sisäistä tietoturvallisuutta, missä taas valtiovarainministeriön rooli on merkittävä. Tietoturvastrategiassa on kuvattu ylätason tavoitteita tietoyhteiskunnan turvallisuudesta, mutta konkreettisia toimenpide-ehdotuksia on vähän, mikä nostaa toteutusta lähempänä olevan VAHTIn ja tietoturvastrategiasta vastaavien tahojen yhteistyön merkitystä. VAHTIssa ja tietoturvallisuusasioiden neuvottelukunnassa on edustettuna useita samoja organisaatioita, joten yhteistyö ja tiedon välittyminen näiden elinten välillä on helppoa.

Toimenpiteet:

- Vaikuttaminen tietoyhteiskuntaneuvostossa oleviin ja tietoyhteiskuntaohjelman hankkeissa mukana oleviin henkilöihin.
- Tietoyhteiskuntaohjelman ja VAHTIn riittävä yhteistyö.

5.2.6 Yhteistyö virastojen valmiustoiminnan kanssa

Monissa virastoissa valmiussuunnittelu on eri henkilön vastuulla kuin tietoturva-asiat, eikä näiden välinen yhteistoiminta välttämättä ole kovin tiivistä. Viraston kannalta tietohallinnon ja tietoturvallisuuden varautumistoiminnan ei tulisi jakautua selkeästi normaaliajan häiriöihin ja poikkeusoloihin, vaan siirtymän tulisi olla jatkumo. Siten poikkeusolojen järjestelyjen tulisi olla liitetty osaksi normaaliolojen ratkaisuja.

Varautuminen poikkeusoloihin on monesti merkinnyt investointia laitteisiin ja tiloihin, joita ei normaaliolojen häiriötilanteissa käytetä. Tämä on lisännyt kustannuksia sekä aiheuttanut päällekkäisyyksiä. Lisäksi nopeasti vanhenevien tietoteknisten laitteiden varastointiaika on lyhyt.

Esimerkiksi Huoltovarmuuskeskuksen ATK-varakeskuksella on valmius toimia helposti käyttöönotettavana varapaikkana ja tätä mahdollisuutta jotkut virastot ovat hyödyntäneet. Kehittämisessä tärkeintä on saada virastojen sisällä valmius- ja tietohallinto- ja tietoturvaihmiset yhteistoimintaan.

Toimenpiteet:

- Ohjeistuksissa otetaan esiin varautumistoiminnan liittäminen normaaliolojen tietohallintoon ja tietoturvatyöhön, mikä edistää virastojen sisäistä yhteistyötä.

5.2.7 Tietoturva-arvioinnit

Arviointeja hyödynnetään erilaisissa tilanteissa, joissa halutaan varmistaa keskeisen laatu-, kirjanpito-, ympäristö- tai muun järjestelmän toimivuus. Tietoturvallisuus on nousemassa näiden veroiseksi järjestelmäksi virastojen toiminnan kannalta.

Tietoturva-arviointeja voi tapahtua usealla tasolla. Laajimmat, koko tietoturvallisuuden hallintajärjestelmän kattavat arvioinnit saattavat tähdätä tietoturvasertifikaatin saamiseen, mutta pienimmät arvioinnit vain verkkolaitteiden asetusten todentamiseen.

Arviointeja voi tehdä ulkopuolinen tarkastaja (joka puolestaan voi olla yksityinen yritys tai virasto), yksikön omat tietoturvavastaavat tai yksiköt voivat ristiinarvioida toisiaan. Oikea metodi riippuu tavoitteista.

Valtionhallinnon hankintayhteistyö (kuten puitesopimukset ja yhteishankinnat) on keino, jolla tietoturva-arviointeja voidaan edistää: pienten yksikköjen mahdollisuudet paranevat ja kynnys arvioinnin tekemiseen madaltuu. Tulosohjaus ja VAHTI-ohjeet ovat myös keinovalikoimassa ja yksiköiden toinen toisilleen tekemiä ristiinarviointeja voidaan edistää tietoturvakulttuurin muodostumisella.

Toimenpiteet:

- Täydennetään arvioinneista julkaistua VAHTI-ohjetta muilla ohjeilla tai tarkistuslistoilla.
- Perustetaan valtionhallinnon arviointipooli tietoturva-arvioinnin yhteistyön edistämiseksi.

5.2.8 Yhteistoiminta ja jaetut resurssit

Niukkojen resurssien vuoksi virastojen välistä yhteistoimintaa tietoturva-asioissa tulee edistää. Tätä voidaan edistää henkilöiden verkostoitumisella, yhteisillä foorumeilla ja ohjeilla. Yksi mahdollisuus resurssien säästöön on usean viraston yhteiset tietoturvahenkilöt; ratkaisu, jollaisia on jo toteutettu. Etenkin pienissä virastoissa ei välttämättä ole tarvetta täysipäiväiselle tietoturvahenkilölle, jolloin sama henkilö voi palvella useampaa virastoa samalla hallinnonalalla tai alue-/paikallishallinnossa. Samalla virastojen tietoturvaratkaisut tullevat varsin yhdenmukaisiksi.

Toimenpiteet:

- Tuetaan tietoturvaverkostojen muodostumista.
- Selvitetään mahdollisuus hyödyntää tulosohjausta jaettujen resurssien käytön edistämisessä ja resurssien yhteiskäytössä.

5.3 Tietoturvallinen viestintä ja asianhallinta

5.3.1 Roskaposti eli späm

Sähköpostin merkitys niin operatiivisena järjestelmänä kuin asiakaspalvelukanavana on lisääntynyt merkittävästi. Monessa virastossa sähköposti on tärkeimpiä järjestelmiä ja sen käyttökatkokset aiheuttavat nopeasti ongelmia, joten roskapostin tukkima sähköpostipalvelin on saatava nopeasti takaisin käyttöön.

Spämillä (engl. *spam)* tarkoitetaan roskapostia eli sähköpostia, jota postin vastaanottaja ei ole tilannut, ei halua ja jonka lähettämistä käyttäjä ei yleensä pysty estämään. Aiemmin roskapostista aiheutui käyttäjille pelkästään ylimääräistä vaivaa, kun he joutuivat poistamaan kyseisiä viestejä postilaatikostaan. Viime aikoina tilanne on pahentunut: roskapostitulva, haittaohjelmia sisältävien postien yleistyminen ja spämmillä toteutetut palvelunestohyökkäykset (*Denial of Service Attack* eli *DoS)* ovat tulleet niin yleisiksi, että jopa suurten palveluntarjoajien sähköpostipalvelut ovat tukkeu-

tuneet. Eräiden arvioiden mukaan jopa 30-50% kaikesta sähköpostiliikenteestä liittyy spämmiin, ja että späm aiheutti lokakuussa 2003 enemmän taloudellista vahinkoa kuin virukset ja hakkerit yhteensä[14].

Roskapostinvastaisia toimia on valmisteilla useita. Suomessa ja useissa muissa maissa ollaan säätämässä lakeja, joilla pyritään parantamaan vastaanottajien mahdollisuuksia rajoittaa heille tulevaa postia ja lisäämään palveluntarjoajien mahdollisuuksia puuttua akuuttiin roskapostiongelmaan. Roskaposti on kansainvälinen ongelma: saman ongelman parissa painivat useat maat, eikä roskaposti tunne maa- eikä kielirajoja.

Ongelma koskettaa yhtä lailla yksityisiä henkilöitä, yrityksiä kuin julkista hallintoa, joskin vaikutukset viimeksi mainitussa ovat sikäli suuremmat, että tukkeutunut sähköposti vaikeuttaa sähköistä asiointia (jossa usein on määräaikoja) ja täten heikentää luottamusta viranomaisiin ja tietoyhteiskuntaan.

Toisin kuin virukset, laajamittainen roskaposti on melko uusi ilmiö, eikä vastatoimiin ole samanlaista rutiinia.

Toimenpiteet:

- Roskapostin hallinnan yleisohjeen laatiminen.
- Kansallisen meneillään olevan lainsäädäntötyön tukeminen, ja työn päätyttyä lakien implementoinnin varmistaminen.
- Osallistuminen kansainväliseen roskapostia rajoittavaan sopimus-, standardointi-, organisointi- ja muuhun työhön.
- Roskapostin torjuntaohjelmistojen puitesopimusten teko.
- Viestintäviraston yhteistyö operaattoreiden kanssa.

5.3.2 Varmenteiden käytön edistäminen sähköpostissa

Palvelukanavana sähköposti on nopea ja joustava, mutta sellaisenaan tietoturvallisuudeltaan heikko. Koska tietoturvallisuuden heikkoudet eivät ole asiakkaiden tiedossa, välitetään salaamattomassa sähköpostissa arkaluontoisia tietoja. Julkishallinnon asiakkaat lähettävät usein sähköpostiviesteissä tietoja, joiden tulisi olla vahvasti suojattuja ja vain vastaanottajan luettavissa. Monet sähköpostin käyttäjät eivät tiedosta tähän liittyviä vaaroja tai ottavat tietoisen riskin, sillä sähköpostiviestin salaamista pidetään joko hankalana tai käytännössä mahdottomana.

Varmenteiden avulla pystytään myös allekirjoittamaan sähköpostiviestit, jolloin voidaan varmistua lähettäjän henkilöllisyydestä. Nykyisin sähköpostin lähettäjän vää-

[14] www.mi2G.com ja The Washington Post 10.10.2003

rentäminen on jokseenkin helppoa, mitä käytetään hyväksi roskapostin ja virusten lähettämisessä. Allekirjoitus lisää käyttäjien luottamusta sähköpostiin, ja allekirjoitusten käytön lisäännyttyä riittävästi sitä voitaisiin hyödyntää myös roskapostin suodattamisessa.

Ongelmaa pyritään ratkaisemaan rakentamalla turvallisen sähköpostiasioinnin vaatimia perusratkaisuja ja tiedottamalla niin asiakkaille kuin viranomaisille tästä mahdollisuudesta sekä opastamalla heitä sen käyttämisessä.

Turvallisessa sähköpostiasioinnissa julkinen sektori voi toimia suunnan näyttäjänä, ja toisaalta sen tulee toimia näin, sillä asiakkaan yksityisyyden suoja saattaa merkittävästi vaarantua suojaamattomassa sähköpostiliikenteessä. Uhkana ei ole ainoastaan väärään osoitteeseen menneet sähköpostit tai sähköpostiliikenteen salakuuntelu vaan myös mahdollinen virushyökkäys (toiset virukset lähettävät saastuneessa koneessa olevia vanhoja sähköposteja uusiin osoitteisiin) ja monet täysin tavalliset järjestelmähallintoon liittyvät toimenpiteet, kuten varmuuskopiointi ja järjestelmän pääkäyttäjätoimet.

Toimenpiteet:

- Toimikortinlukijoiden ja tarvittavien ohjelmistojen yhteishankinta.
- Varmenteiden ja toimikorttien hankinnan yhteinen puitesopimus.
- Varmenteiden käyttöönoton toteuttaminen yhteishankkeena.
- Loppukäyttäjien ja julkishallinnon asiakkaiden opastaminen varmenteiden käyttöön.

5.3.3 Tunnistaminen ja oikeuksien hallinta

Pääsääntönä tunnistamisessa on, että käyttäjä tunnistetaan ainoastaan, kun siihen on erityinen tarve. Tällöinkin on harkittava mahdollisuutta tunnistukseen, jossa palvelun asiakkaan tunnistaa kolmas osapuoli ja palvelun tarjoajalle asiakas esiintyy anonyyminä.

Tunnistaminen ei liity vain ulkoisten asiakkaiden tunnistamiseen vaan myös sisäisten käyttäjien tunnistamiseen. Monet käyttäjät kokevat, että heillä on liikaa salasanoja; varsinkin kun niitä pitää vaihtaa.

Interaktiivisten kehittyneiden verkkopalvelujen kehittäminen tuo esiin tarpeen tunnistaa asiakas. Aloite tunnistuspalveluiden käyttöön tulee usein palvelujen kehittäjiltä, jotka haluavat tarjota personointia, luotettavaa tunnistamista edellyttäviä palveluita tai parantaa palvelun tietoturvallisuutta. Käytettävissä olevien vaihtoehtojen määrä tunnistamisessa on lisääntynyt: perinteisten salasanojen ja HST-kortin rinnalle on tullut uusia tapoja, joista suosituin on pankkien tarjoama tunnistuspalvelu.

Luotettava tunnistaminen on tärkeää identiteettivarkauksien estämisessä ja muussa digitaalisen identiteetin suojaamisessa[15]. Luotettavan tunnistamisen lisäksi tunnistamistietojen asianmukainen käsittely ja suojaaminen ovat tärkeitä. Tämä korostuu vahvan tunnistamisen yleistyessä.

Biometrisen tunnistamisen kehitystä seurataan aktiivisesti muutamissa virastoissa, mutta toistaiseksi asian yleinen prioriteetti ei ole niin korkea, että se edellyttäisi välittömiä toimia tässä kehittämisohjelmassa. Asiaa seurataan ja aihetta käsitteleviä tutkimuksia analysoidaan, jotta kehitysjakson puolivälissä voidaan arvioida, tarvitaanko biometrisen tunnistamisen hanke.

Tunnistamiseen liittyy kiinteästi käyttöoikeuksien hallinta, jossa järjestelmä myöntää tunnistetulle käyttäjälle oikeuden joihinkin palveluihin. Käyttöoikeuksien hallinta on eräs tietohallintohenkilöiden kokemista ongelmista, jonka voidaan arvioida muuttuvan entistä akuutimmaksi palvelujen kehittymisen, yleistymisen ja käyttäjämäärien kasvun myötä.

Valtionhallinnon vahvan tunnistamisen kehittämisen kannalta erittäin tärkeä hanke on virkakorttipilotit, joista saatavien kokemusten myötä PKI-pohjainen vahva tunnistaminen voidaan ottaa käyttöön laajassa mittakaavassa.

Toimenpiteet:

- Hyödynnetään tunnistuksessa ja oikeuksien hallinnassa samoja varmenteita ja laitteita kuin sähköpostin salauksen ja allekirjoituksen yhteydessä.
- JULHA-hakemiston käyttöä lisätään ja sen tarjoamia palveluita monipuolistetaan.
- Laaditaan ohje modulaarisen käyttöoikeuksien hallinnan rakentamiseksi järjestelmiin.
- Yhteisen tunnistuspalvelun rakentaminen virkakorttihankkeiden kokemusten pohjalta.

5.3.4 Tietoliikenneverkkojen ja päätelaitteiden tietoturvallisuus

Langattomat lähiverkot ovat yleistyneet yrityksissä ja kotitalouksissa, vaikka valtionhallinnossa niiden käyttö on toistaiseksi vähäistä. Mobiililaitteet ovat puolestaan yleisiä kaikkialla ja niiden tietoturvallisuus on saanut osakseen huomiota. Laitteiden yhä lisääntyvä kapasiteetti ja koon pienentyminen tekee niiden hukkaamisen entistä va-

[15] Australian oikeusministerin mukaan identiteettivarkauksien (kaikissa muodoissaan) arvioidaan aiheuttavan Australiassa noin 700 miljoonan euron vuotuiset kustannukset. USA:ssa kustannusten arvioidaan olevan noin 45 miljardia euroa ja Iso-Britanniassa lähes 2 miljardia.

hingollisemmaksi ja entistä helpommaksi. Mobiililaitteiden, ja joissain tapauksissa myös langattomien verkkojen, tietoturvallisuuteen törmätään yleensä etätyön ongelmia ratkottaessa, mutta virastojen langattomat lähiverkot ovat yleensä jääneet yksittäisiksi kokeiluiksi. Asiakkaille suunnatut mobiilipalvelut ovat vielä vähäisiä, mutta niiden määrä lisääntyy.

Päätelaitteiden ja tietoliikenneverkkojen tietoturvavaatimukset kasvavat koko ajan: kovalevyjen salaus, VPN ja hajautettu palomuuri alkavat olla kannettavien laitteiden tietoturvavaatimuksia, mutta uusia tulee. Palomuurien hallinta edellyttää ammattitaitoa ja nopeaa reagointia, joita tuetaan koulutuksella, yhteistyön tiivistämisellä sekä tietoturvaohjelmiston integroinnilla.

Työryhmä arvioi, että niin mobiililaitteiden kuin langattomien lähiverkkojen tietoturvallisuuden merkitys kasvaa muutaman vuoden kuluessa. Valtionhallinnon tietoturvallisuuden kehittämisessä tärkeä ennakointi on täten mahdollista. Ohje vaikuttaa luonnollisimmalta muodolta toteuttaa tämä, mutta muitakaan vaihtoehtoja ei tässä vaiheessa suljeta pois.

Toimenpiteet:

- Laaditaan ohje langattomien lähiverkkojen tietoturvallisesta toteuttamisesta.
- Laaditaan ohje mobiililaitteiden tietoturvallisuudesta.
- Seurataan langattomien lähiverkkojen ja mobiililaitteiden tietoturvallisuuden kehittymistä ja tiedotetaan asiasta.
- Edistetään kaikkien laitteiden ja tietoliikenneverkkojen turvallisuutta tietoturvallisuuden tulosohjauksen keinoin, hankintayhteistyöllä ja koulutuksella.
- Valmistellaan sähköpostia ja tietoliikenneyhteyksien suojaamista koskevat linjaukset.

5.3.5 Asianhallinnan tietoturvallisuus

Asianhallintajärjestelmät, dokumentinhallinta- ja työryhmäohjelmistot ovat jo nyt yleisesti käytössä, ja niiden uskotaan yleistyvän edelleen. Sähköpostia käytetään yleisesti asianhallintajärjestelmänä tai tällaisen tukena, vaikka kyseessä on kommunikointiin tarkoitettu sovellus.

Toimenpiteet:

- Varsinaisten asian- ja dokumenttien hallintajärjestelmien käyttöä edistetään. Näiden valinnassa arvostetaan hyviä tietoturvaominaisuuksia.
- Kehitysjakson loppupuolella dokumenttienhallinnan ja työryhmäohjelmistojen tietoturvallisuudesta valmistellaan ohje, mikäli aihe on riittävän akuutti.

- Julkaistavissa ohjeissa tuodaan esiin, ettei sähköpostia ole tarkoitettu asianhallintaan virusvaaran, arkistointiongelmien ja muiden seikkojen johdosta.

5.4 Tietoturva- ja tietojärjestelmävastaavien työn tukeminen

Tietoturvallisuuden toteuttaminen edellyttää riittävästi osaavia tietoturvatyöhön suunnattuja resursseja. Resurssit ovat usein niukkoja, sillä ne on kohdennettu muuhun kuin tietoturvallisuuden kehittämiseen.

Työryhmän tekemissä haastatteluissa ilmeni selkeästi, että resurssien niukkuus koetaan tietoturvallisuuden kehittämistä rajoittavaksi, usein jopa estäväksi tekijäksi. Nimenomaan pätevien ihmisten ajasta on puutetta, mutta myös raha on usein rajoittava tekijä.

Rahan riittävyys ei takaa henkilöresurssien määrää, sillä henkilöstöpolitiikka voi rajoittaa uusien osaajien rekrytointia. Tietyt osat tietoturvallisuudesta ovat lisäksi sellaisia, että niiden ulkoistaminen on käytännössä vaikeaa, ja konsulttipalveluiden ostaminen ja työn ohjaaminen edellyttävät organisaation omaa työpanosta.

Pula resursseista näkyy kipeämmin tietoturvallisuuden kehittämisessä kuin jatkuvassa tietoturvatyössä. Useat tietoturvallisuuden hallintajärjestelmänsä sertifioinnista kiinnostuneet virastot sanoivat, ettei asia ole ajankohtainen niin kauan kuin tietoturvahenkilöiden kuormitus on nykyisellä erittäin korkealla tasolla.

Tietoturvavastaavien ja tietojärjestelmästä vastuullisten merkitys kokonaisuuden kannalta on kriittinen ja heidän työnsä tukemiseen tulee kiinnittää aiempaa enemmän huomiota.

Toimenpiteet tietoturvallisuuteen allokoitujen resurssien lisäämiseksi:

- Kansliapäälliköihin ja virastojen yleisjohtoon vaikuttaminen.
- Tietoturvatiedottamisen lisääminen.
- Tietoturvallisuuden tulosohjauksen edistäminen.
- Ammatillisen tietoturvakoulutuksen lisääminen.

5.4.1 Valtionhallinnon yhteishankkeet ja hankintayhteistyö

Tehdyssä kyselyssä tuotiin usein esiin tietoturvallisuuden yhteishankkeiden merkitys. Ne koetaan tehokkaana tapana edistää yhteisesti tärkeitä, ajankohtaisia asioita.

Yhteishankkeet tukevat myös tietoturvaihmisten verkottumista, parhaiden käytäntöjen leviämistä ja edistävät hyvän tietoturvallisuuden saamaa positiivista julkisuutta.

Yhteishankkeiden sisältö voi koskea mitä tahansa tietoturva-asiaa, mutta erityisesti ajankohtaisten, useita virastoja koskevien asioiden käsittelylle on kysyntää. Sähköisten palvelujen tietoturvallisuus, vahva tunnistaminen, sähköpostin turvaaminen, riskienhallinta ja tietoturvasuunnittelu ovat tällaisia asioita. Tähän mennessä on toteutettu yhteishankkeita tietoturvallisuus- ja valmiussuunnittelun tehostamiseksi sekä virastotasoisten ohjeiden laatimiseksi.

Suurten, koko julkista sektoria koskevien hankkeiden rinnalla on selkeä tarve yhden hallinnonalan, toiminnon tai muun yhdistävän asian tietoturvahankkeille.

Tietoturvatuotteiden yhteishankintoihin kohdistuu positiivisia odotuksia, vaikka esimerkiksi salaustuotteiden yhteishankintahanke ei ole vielä valmis.

Toimenpiteet:

- Toteutetaan yhteishankkeita ja hankintayhteistyötä virastojen tarpeiden ja osallistumismahdollisuuksien mukaan.
- Hankintayhteistyötä tiivistetään yhteistoiminnassa Hanselin kanssa.
- Laajennetaan tietoturvaohjelmien puitesopimuksen hyödyntämistä.

5.4.2 Ohjelmien versiopäivitysten hallinta ja jakelu

Sähköiset palvelut koostuvat useasta yhteen liitetystä tietojärjestelmästä. Yhden järjestelmän tietoturvallisuuden pettäminen saattaa vaarantaa koko palvelun tai pahimmassa tapauksessa koko viraston tietoturvallisuuden. Ohjelmien tietoturva-aukkoja paljastuu tiheästi, ja vaikka useimpiin on saatavilla korjaus (*patch, fix)* ei kaikkia ohjelmien tietoturva-aukkoja ole paikattu.

Päivitysten jakelu saattaa olla erittäin vaikeaa, mikäli järjestelmäympäristössä on laitteita, joiden fyysinen hallinta on viraston ulkopuolella. Lisääntyvä etä- ja matkatyö on tyyppiesimerkki tästä tilanteesta.

Tietoturva- ja tietotekniikkavastaavat kokevat päivitysten jakelun ja hallinnan suurena ongelmana, joka vaatii paljon resursseja ja sisältää lukuisia riskitekijöitä. Tilannetta voidaan helpottaa ohjelmilla, toimintamalleilla, selkeillä vastuilla ja mahdollisesti arvioinneilla.

Tietojärjestelmien ja etenkin niiden käyttöjärjestelmien korjauspäivitysten nopea asentaminen vaikuttaa merkittävästi tietoturvallisuuteen. Entuudestaan tunnettuja käyttöjärjestelmä- ja sovellushaavoittuvuuksia hyödynsi lähes kaksi kolmasosaa tietojär-

jestelmään suuntautuneista hyökkäyksistä, entuudestaan tuntemattomia noin joka neljäs[15].

Toimenpiteet:

- Laaditaan ohje päivitysten testaamisesta ja suorittamisesta.
- Edistetään laitteiden ja ohjelmien hallintaan tarkoitettujen ohjelmistojen käyttöä hankintayhteistyössä.

5.4.3 Tietoturvaratkaisujen integrointi

Koko tietoturvaympäristö on muuttunut entistä heterogeenisemmaksi. Päätelaitteita ja verkkoratkaisuja on monenlaisia, tietojärjestelmiä ja toimipisteitä entistä enemmän. Samassa tahdissa on tietoturvaohjelmien määrä ja niiden hallinta muuttunut mutkikkaaksi.

Tietoturvaratkaisuja tultaneen integroimaan entistä enemmän niiden hallinnan helpottamiseksi. Tämä tarjoaa yhtä aikaa niin haasteita kuin mahdollisuuksia. Mahdollisuuksia tarjoaa päivitysten nopea jakelu ja tietoturvaihmisten kuormituksen pienentäminen, haasteista mainittakoon integroidun ohjelmiston omien tietoturvaongelmien aiheuttamat vahingot sekä uuden ohjelman käyttöönotosta tulevat kustannukset.

Toimenpiteet:

- VAHTI seuraa suurimpien tietoturvaohjelmistovalmistajien suuntausta valmistaa palomuurin, virustorjunnan ja muiden tietoturvaohjelmistojen yhdistäviä kokonaisuuksia. Näiden hyöty tullaan arvioimaan.

5.4.4 Virustorjunnan ylläpito

Virustorjunta on tietoturvallisuuden tyypillisimpiä rutiineja, jonka merkitys on yleisesti ymmärretty. Virustorjunta pitäisi saada asennetuksi ja jatkuvasti ylläpidetyksi kaikkien virastojen kaikkiin tietokoneisiin, ja tästä olisi hyvä saada aikaan sitova normi. Virustorjunnan suurimpina haasteina on sen ylläpito kannettavissa tietokoneissa sekä etätyöasemissa.

Asia on aina ajankohtainen, joten VAHTI on käynnistänyt virustorjunnasta annetun ohjeen päivittämisen.

---

[15] Information Week 2003 U.S. Information Security. Hyökkäykset ovat voineet hyödyntää molempia haavoittuvuuksia. Ks http://www.internetweek.com/breakingNews/showArticle.jhtml?articleID=16100232.

Toimenpiteet:

- Huolehditaan, että virustorjunnasta on aina saatavilla ajan tasalla oleva ja mahdollisimman kattava VAHTI-ohje.
- Tuotetaan ohje ostopalveluiden sopimuksista.
- Virustorjunnan ottaminen mukaan tulosohjauksen kriteereihin (esimerkiksi monessako prosentissa laitteista on virustorjunta, joka on päivitetty viimeisen 24 tunnin kuluessa).
- Kehitetään valtionhallinnon yleistä reagointikykyä virusuhan torjumiseksi.

5.4.5 Valtionhallinnon ympärivuorokautinen tietoturvapalvelu

Tietoverkkojen tietoturvaloukkaukset eivät tapahdu vain virka-aikana, joten on olemassa tarve jatkuvaan tietoturvapalveluun. Tämän alueen toimijoita on olemassa useita, ainakin puolustusvoimilla, poliisin tietohallintokeskuksella sekä kaupallisilla toimijoilla. Yhtenä riskinä on pidettävä eri toimijoiden välisen tiedonvaihdon ongelmia laajamittaisen tietoturvahyökkäyksen torjumisessa.

Hallinnon toimijat tarjoavat palvelujaan kuitenkin vain yhdelle tai muutamalle virastolle. Useat virastot ostavat tietoverkkojensa hallinnoinnin kaupallisilta toimijoilta, joiden tulisi huolehtia akuuteista tietoturvatoimistakin. Ostopalveluiden yhteydessä kuitenkin operaattoreiden tietoturva-ammattitaito ei välttämättä ole riittävä vakavien ongelmien ilmetessä, eikä vastuista ja toimista ole sovittu.

Viestintäviraston CERT-FI toiminta on parantanut suomalaisen yhteiskunnan kykyä vastata nopeasti realisoituviin tietoturvauhkiin. CERT-FI on ollut auki vain virka-aikaan, mikä on koettu puutteeksi.

Valtionhallinnon tietoturvatyön kehittämisessä ei perusteta yksityisen palvelutarjonnan kanssa kilpailevaa toimintaa, vaan yksityissektorin palveluja hyödynnetään, milloin tämä on tarkoituksenmukaista.

Toimenpiteet:

- Selvitetään tarve ympärivuorokautiselle hallinnon tietoturvapalvelulle.
- Kehitetään yksiköiden kykyä nopeaan reagointiin ja tietoturvatietolähteiden hyödyntämiseen.
- Kehitetään tiedonvälitystä nopeaa reagointia vaativissa tietoturva-asioissa.

5.5 Toiminnan ja palvelujen kehittäjien työn tukeminen

Sähköiset palvelut eli verkkopalvelut muodostavat laajan kokonaisuuden, jonka tietoturvallisuuden kehittäminen vaatii useita toinen toisiaan täydentäviä hankkeita. Palveluiden kehitystä tapahtuu kolmella tasolla: palveluiden kehittyneisyysaste kasvaa, tarjotaan uusia verkkopalveluita ja uudet yksiköt rakentavat palveluita.

Kehittyneitä palveluita tarjoavat törmäävät teknisiin ongelmiin sekä ongelmiin, joita kukaan ei ole aiemmin kohdannut. Ensimmäistä kertaa peruspalvelujaan verkkoon vievä virasto taas löytää tukea ongelmiinsa jo olemassa olevista tietoturvaohjeista ja hankkeista, mutta ei välttämättä tiedä, mitä tehdä.

Toiminnan kehittäjien osalta tilanteen voidaan olettaa olevan hyvin samankaltainen kuin palvelun kehittäjien.

5.5.1 Asiakasnäkökulman korostaminen

Sähköisten palvelujen tietoturvallisuus ei ole riippuvainen vain palveluja tarjoavan viraston toimenpiteistä, vaan tietoturvallisuudessa on otettava huomioon asiakasnäkökulma. Käytännössä tämä tarkoittaa laajasti ymmärretyn käytettävyyden ja tietosuojan huomioon ottamista palvelujen suunnittelussa ja toteutuksessa.

Asiakasnäkökulman huomioon ottamisen edistämistä ei ole helppo kiinnittää mihinkään yksittäiseen hankkeeseen, vaan käyttäjän näkökulma on oltava mukana kaikessa tietojärjestelmäkehityksessä.

Toimenpiteet:

- Käytettävyyssuunnittelua ja käytettävyyden testaamista tullaan edistämään tekemällä tunnetuksi ohjeita ja suosituksia.
- Tulevissa VAHTI- ja muissa tietoturvaohjeissa tullaan aiempaa useammin kirjoittamaan luku, jossa arvioidaan tietoturvaohjeiden vaikutuksia käyttäjän kannalta.

5.5.2 Sähköinen valvonta ja yksityisyyden suoja

Työnantajan oikeus valvoa työntekijöiden sähköpostia on puhuttanut jo useamman vuoden ajan, ja on esimerkki uusista ongelmista, joihin vanhojen periaatteiden soveltaminen sellaisenaan ei tuo tyydyttävää ratkaisua. Ongelma on laajempi kuin pelkkää sähköpostia koskeva: uudet tietoturvallisuutta yhdeltä osa-alueelta parantavat

ratkaisut saattavat heikentää toisia. Vähitellen yleistymässä olevat IDS-järjestelmät (tietomurtohälytin eli *Intrusion Detection Systems)*, verkonvalvonta sekä muut apuvälineet saattavat epäsuorasti mahdollistaa sähköisen valvonnan. Asia ei vielä ole akuutti, mutta sen merkitys on nousussa. Lisäksi kyseessä on tilanne, jossa uudet tekniset mahdollisuudet sekä nopeasti muuttuva lainsäädäntö hankaloittavat juuri pienten virastojen asemaa.

Elektronisen valvonnan ongelmat tulevat esiin myös biometristen tunnistusten yhteydessä. Toistaiseksi biometristen tunnisteiden käyttö on vähäistä, vaikkakin kansainvälisistä seikoista johtuen lisääntymässä. Käytön yleistymistä estää moni seikka, joista eräs on epäselvyydet biometristen tunnisteiden käytön säätelystä. Eräissä tunnistusmenetelmissä on periaatteessa mahdollisuus valvoa henkilön terveydentilaan liittyviä tekijöitä. Ongelma ei ole akuutti, mutta kehitysohjelman loppupuolella asia saattaa olla tärkeä.

Toimenpiteet:

- Liikenne- ja viestintäministeriön valmistelema ja muu kansallinen ja kansainvälinen biometrisia tunnistusmenetelmiä käsittelevä aineisto analysoidaan, ja tämän pohjalta päätetään tarpeellisista toimenpiteistä.

5.5.3 Yksityisyyden suojan yleinen kehittäminen

Yksityisyyden suojaan liittyvät kysymykset koetaan usein ongelmallisiksi ennen palvelun aloittamista, mutta ei yleensä sen jälkeen kun palvelu on toiminnassa. Yksityisyyden suojaan liittyviä asioita pidetään siis yleensä vaikeampina ratkaista kuin mitä ne todellisuudessa ovat. Vastaava ilmiö esiintyy tietoturvallisuudessa yleisemmin, mutta lienee tietosuojan kohdalla korostunut.

Yksityisyyden suojan kehittäminen toteutuu kolmella toisiaan tukevalla toimenpiteellä: VM:n, VAHTIn ja muiden tietoturvatoimijoiden sekä tietosuojavaltuutetun yhteistyön ylläpitämisellä, yksityisyyden suojaan liittyvien asioiden huomioinnilla VAHTI-ohjeissa ja muissa valtionhallinnon tietoturvahankkeissa sekä erillisissä yksityisyyden suojaa käsittelevissä hankkeissa.

Yhteistyön kehittämisessä pyritään jatkamaan nykyistä linjaa, jossa tietosuojavaltuutetun toimiston edustaja osallistuu kaikkiin yksityisyyden suojan kannalta keskeisten tietoturvahankkeiden valmisteluun. Tietosuojavaltuutetun toimisto avustaa VAHTI-työryhmiä tapauskohtaisesti sovittavilla menettelytavoilla.

Myös niissä VAHTI-hankkeissa, joissa tietosuojavaltuutetun toimiston edustaja ei ole tukemassa työryhmän työtä, tulee yksityisyyden suojaan liittyvät asiat ottaa huomioon.

Uusissa tietoturvallisuuden kehittämishankkeissa tulee seurata erityisesti yksityisyyden suojan turvaamiseen tarkoitettujen ohjelmien ja tekniikoiden kehitystä (ennakointi), sekä valtionhallinnossa esiin tulevia yksityisyyden suojaa koskevia ongelmia (reagointi).

Toimenpiteet:

- Tietosuojavaltuutetun toimiston yhteistyö toiminnan kehittäjien ja tietoturvaihmisten kanssa.
- Tietosuojavaltuutetun osallistuminen tietoturvan kehitysfoorumeihin.

5.5.4 PET-teknologiat

Esimerkkinä ennakoivista hankkeista mainittakoon yksityisyyden suojaamiseen tarkoitetut PET-teknologiat (*Privacy Enhancement Technology*), jotka ovat melko uusi teknisten ratkaisujen joukko, joka tarjoaa mahdollisuuden nykyistä parempaan yksityisyyden suojaan. Digitaalinen raha, nollatietotodistukset ja muut PET:iin kuuluvat ratkaisut[17] ovat tietoturva-asioita, joiden merkityksen arvioidaan nousevan seuraavien viiden vuoden kuluessa.

PET-teknologioiden tunnetuksi tekeminen tarjoaa VM:lle ja VAHTIlle mahdollisuuden ennakoivaan ja palveluja mahdollistavaan tietoturvatyöhön. Tieto mahdollisuuksista lisää halua käyttää niitä sähköisten palvelujen suunnittelussa. Tämä puolestaan vaikuttaa siihen, että kansalaiset alkavat kuluttajina vaatia PET-teknologioiden käyttöä kaupallisissa palveluissa.

Toimenpiteet:

- VAHTIn avustuksella VM tulee aktiivisesti seuraamaan PET-teknologioiden kehitystä yhdessä Tietosuojavaltuutetun toimiston kanssa
- VAHTI julkaisee PET-teknologioita käsittelevän ohjeen (tai muun julkaisun), kun niiden kypsyysasteen arvioidaan olevan riittävä.

5.6 Peruskäyttäjän tietoturvatyön tukeminen

Monet edellä kuvatuista valtionhallinnon tietoturvallisuuden kehityskohdista vaikuttavat peruskäyttäjän tietoturvallisuutta parantavasti, eikä niitä tulla tässä kohtaa käsit-

[17] Nollatietotodistuksessa henkilö kykenee vakuuttamaan toiselle, että hän tietää salaisuuden paljastamatta itse salaisuutta (esim. että hänellä on validi tarkistusnumero). Päinvastoin kuin luottokorttirahassa, ja kuten paperirahassa, digitaalisen rahan maksajaa ei liitetä maksuvälineeseen.

telemään yksityiskohtaisesti. Roskapostin (eli spämmin) vastaiset toimet, asianhallinnan tietoturvallisuus, tietoturvakulttuurin luominen ovat esimerkkejä asioista, jotka olisi voitu sijoittaa peruskäyttäjän tietoturvatyön tukeminen -koriin. Mikäli näin olisi tehty, olisi tämä kori paisunut suureksi. Koska työryhmä ei halunnut jakaa kehityskohdetta useaan koriin, eikä toisaalta toistaa samoja asioita päädyttiin ratkaisuun, jossa viitataan edellä käsiteltyihin asioihin ja käsittelemään vain aidosti uudet asiat.

Peruskäyttäjien tietoturvallisuuden kehittäminen vaatii pitkäjänteistä työtä ja ominaisuuksia, joita tietoturvatyötä tekeviltä ei ensimmäiseksi odoteta. Koulutuksen ja motivoinnin taidot, asioiden yksinkertaistaminen ja selkeä, käytännönläheinen esitystapa vievät tietoturvallisuutta eteenpäin. Loppukäyttäjät ovat heterogeeninen, laaja joukko, jonka tietoturvallisuuden edistäminen on erittäin vaativa tehtävä.

VAHTI on jo julkaissut ja tulee julkaisemaan lisää loppukäyttäjille suunnattuja aineistoja sekä tukemaan tietoturvan parissa työskentelevien heille antaman koulutuksen järjestelyjä ja koulutusmateriaalin julkaisua.

Virastojen ja laitosten tietoturvavastaavien ja henkilöstöhallinnon mahdollisuuksia tietoturvakoulutukseen lisätään. Juuri julkaistu VAHTIn koulutusopas ja siihen liittyvä piakkoin valmistuva materiaali tullaan pitämään ajan tasalla ja ohjeesta tullaan aktiivisesti hakemaan palautetta, jota hyödynnetään jatkokehityksessä. Mainittu ohje lisää myös tietoturvavastaavien mahdollisuuksia antaa tietoturvakoulutusta.

Loppukäyttäjien tietoturvakoulutuksessa tullaan hyödyntämään verkkoteknologioiden suomia mahdollisuuksia, kuten verkossa tarjottavaa koulutuspakettia ja multimediamateriaalia. Yhteistyötä Suomen Virtuaaliyliopiston tai virtuaalikursseja tarjoavan korkeakoulun kanssa tullaan harkitsemaan tarkastelujakson loppupuolella.

Loppukäyttäjille suunnatun materiaalin ulkomuotoon ja pedagogisiin asioihin tullaan kiinnittämään erityistä huomiota.

Seminaaritoiminnan lisäämisen myötä harkitaan loppukäyttäjän tietoturvallisuuden edistämiseen suunnatun tilaisuuden järjestämistä.

Varmenteiden käytön lisääminen tarjoaa mahdollisuuksia loppukäyttäjien tietoturvallisuuden parantamiseen. Toimiva virkakortti tekee mahdolliseksi kertakirjauksen (SSO eli Single Sign-On) ja tätä kautta mahdollistaa salasanojen määrän vähentämisen.

Käyttäjien kokemaa salasanojen runsautta ja niiden hallinnan vaikeutta helpotetaan virkamieskortin suomien mahdollisuuksien tiedottamisella sekä asiaan liittyvillä yhteishankkeilla. Mobiilivarmenteiden käyttömahdollisuuksia tullaan tutkimaan ja toimikortin lukijalaitteiden sekä muiden tietoturvaohjelmistojen valinnassa tullaan painottamaan käytettävyyttä.

Tietoturvakoulutusta osana muuta tietotekniikkakoulutusta tullaan lisäämään, jolloin tietoturvallisuuden sitominen osaksi normaalia päivittäistä toimintaa helpottuu.

Tietoturvakoulutuksen lisääminen peruskouluissa, keskiasteen koulutuksessa ja korkeakouluissa parantaa peruskäyttäjien tietoturvaosaamista ja valmiuksia käyttää tietoturvaratkaisuja.

Johdon esimerkin merkitystä ei voida korostaa liikaa. Käytännössä johdon osallistuminen (tai pois jäänti) tietoturvakoulutukseen viestii henkilöstölle asian todellisesta merkityksestä. Johdon asenteiden merkityksestä tullaan kertomaan kansliapäällikkökokouksessa ja valtionhallinnon tietoturvaseminaareissa.

Toimenpiteet:

- Tietoturvakoulutusta ja koulutuksen edellytyksiä lisätään.
- Virkakortin, kertakirjauksen ja muiden peruskäyttäjän tietoturvallisuutta edistävien ratkaisujen yleistymistä tuetaan.
- Vaikutetaan virastojen johtoon, jotta tietoturvallisuudesta tulee luonteva osa päivittäistä toimintaa.

6 KEHITYSOHJELMAN TOIMEENPANO

Tietoturvallisuuden kehittäminen on pitkäjänteistä työtä, jossa yhdistyy toisaalta valmius vastata nopeasti ilmeneviin akuutteihin uhkiin, toisaalta asenteita ja valmiuksia luova hitaasti vaikuttava työ.

Varsinaiset hankesuunnitelmat tehdään vasta kun kehityskohteista syntyviin hankkeisiin on nimetty vastuulliset tahot ja projektipäälliköt. Toteuttajille varataan mahdollisuus vaikuttaa hankkeen lopulliseen sisältöön, toteutustapoihin ja resurssitarpeisiin. On myös mahdollista yhdistää useita hankkeita yhdeksi kokonaisuudeksi.

Kehitysohjelman toteutus vaatii resursseja. Ensisijaisesti tämä tarkoittaa nykyisten resurssien kohdentamista tietoturvallisuustyöhön valtionhallinnon jokaisella tasolla.

Pyritään siihen, että ministeriöt ja hallinnonalat varmistavat sekä vuotta 2005 koskevassa budjettiprosessissa että TTS-prosessissa tietoturvallisuuden edellyttämät resurssit.

Tämä toimeenpanosuunnitelma on vain ehdotus, sillä tietoturvatyössä on vaikea ennakoida pitkälle tulevaisuuteen. Osa tässä esitetyistä hankkeista saattaa menettää merkityksensä ja uusia hanketarpeita voi ilmetä.

Kehitysohjelman toteuttamisen alustava aikataulu ja osallistuvat tahot on esitetty liitteessä ” Kehitysohjelman aikataulu ja toteuttajat”.

6.1 Kehitysohjelman kokonaisvastuu

Tietoturvan kehitysohjelman vastuullinen ministeriö on valtiovarainministeriö, jonka tukena käytännön koordinoinnista, seurannasta ja yhteensovittamisesta huolehtii VAHTI. VM ja VAHTI huolehtivat hankkeisiin vastuullisten tahojen nimeämisestä sekä hankkeiden etenemisen seurannasta ja yhteistoiminnan koordinoinnista.

Kehitysohjelmasta tullaan tiedottamaan laajasti. Kehitysohjelmaan kuuluvien hallinnon kehittämiseen ja tietoyhteiskunnan edistämiseen liittyvien asiakokonaisuuksien

johdosta ministeriöiden kansliapäälliköille ja muulle johdolle sekä tietoyhteiskuntaohjelman ministeriryhmälle ja johdolle tiedottaminen on poikkeuksellisen tärkeää.

Valtionhallinnon tietoturvallisuuden kehittämisohjelma toteuttamisen kannalta on tärkeää, että koko ohjelman toteutumista valvovan ja koordinoivan valtiovarainministeriön tietoturvatyön resurssit turvataan.

6.2 Kehittämisohjelman arviointi

Tietoturvatyölle luonteenomaista on uusien uhkien ilmaantuminen nopeassa syklissä. Näin ollen tietoturvaympäristön kehityksen ennustaminen pitkälle tulevaisuuteen on käytännössä mahdotonta, vaikka eräät altistavat tietoturvauhat lienevät luonteeltaan hyvin pysyviä. Valtionhallinnon tietoturvallisuuden kehitysohjelma ulottuu vuoteen 2006. Jotta kehitysohjelman kokonaisuuden tavoite - valtionhallinnon tietoturvallisuuden parantaminen - toteutuisi, on ohjelman toteutumista seurattava ja arvioitava kokonaisuutena eikä vain yksittäisinä hankkeina.

Kehitysjakson puolivälissä VAHTI tulee arvioimaan kehitysohjelman toteutumista ainakin seuraavien kriteerien osalta:

- Miten kehityskohteiden toteutus on edennyt?
- Onko tarpeen muuttaa kehityskohteiden prioriteetteja, aikatauluja, vastuullisia tahoja tai muita ominaisuuksia?
- Onko tarvetta lisätä kehityskohteita?
- Onko tarvetta poistaa kehityskohteita?

Arvioinnin perusteella VAHTI tekee tarvittavat lisäykset, poistot ja muutokset.

6.3 Korkeimman prioriteetin hankkeet ja kehittämiskohteet

Prioriteetiltaan tärkeimmiksi kehityskohteiksi työryhmä arvioi seuraavat:

- Roskaposti eli späm.
- Tietoturvallisuuden tulosohjaus ja mittaaminen.
- Tietoturvallisuuden sitominen virastojen palveluihin ja prosesseihin.
- Valtionhallinnon yhteishankkeet ja hankintayhteistyö.

- VAHTIn toiminnan vahvistaminen.
- Perusinfrastruktuurin tietoturvallisuus.
- Peruskäyttäjän tietoturvatyön tukeminen.

Näiden kaikkien läpivienti tulee aloittaa ensi tilassa, ja jo käynnissä olevien hankkeiden menestyksellinen läpivienti on varmistettava.

Roskapostin vastaisen kehittämisohjelmaan kuuluvan ohjeen laadinnasta vastaa VAHTI ja sitä valmisteleva työryhmä perustetaan vuoden 2004 ensimmäisellä neljänneksellä. Valmisteilla olevan lainsäädäntötyön resurssit varmistetaan ja työn päätyttyä asiasta tiedotetaan aktiivisesti niin valtionhallinnon sisällä kuin yrityksiin ja mahdollisuuksien mukaan yksityisille. VM aloittaa keväällä valmistelut roskapostin torjuntaan käytettävien ohjelmien liittämiseksi valtionhallinnon puitesopimuksiin. Roskapostin vastaisissa toimissa keskeisiä toimijoita ovat Viestintävirasto, LVM, VM, VAHTI ja tietosuojavaltuutettu.

Tietoturvallisuuden tulosohjauksen ja mittaamisen kehittäminen vaikuttaa positiivisesti moneen muuhun tietoturvallisuuden kehittämiskohteeseen, joten myös tämä hanke on käynnistettävä pikaisesti. Tavoitteena on viedä asiaa koskeva VAHTI-ohje käytäntöön vaikuttamalla etenkin ministeriöiden kansliapäälliköihin ja muuhun johtoon. Valtionhallinnon yleiseen ohjaukseen rinnastettavana toimena tietoturvallisuuden tulosohjauksen kehittämisen päävastuu on VM:llä. Ratkaisevaa on jokaisen ministeriön vastuulla tapahtuva hallinnonalakohtainen kehittäminen ja toteutus.

Tietoturvallisuuden sitominen virastojen palveluihin ja prosesseihin on edellisiä laajempi kokonaisuus, jossa valtionhallinnon yhteisten toimien mahdollisuudet ovat rajatummat. Tietoturvallisuutta ja palveluita edistävien ratkaisujen (varsinkin käytettävyyden parantaminen) kartoittaminen aloitetaan keväällä 2004 ja jatketaan koko kehitysjakson ajan. Hallinnonalojen sisäisten toimien onnistumista seurataan VAHTIn kokouksissa kesästä 2004 alkaen.

Valtionhallinnon yhteishankkeiden valmistelu on VM:n ja VAHTIn vastuulla. Tietoturva-arviointien ja roskapostin torjuntaohjelmistojen puitesopimuksen valmistelu aloitetaan kesällä 2004. Saatetaan päätökseen salaustuotteiden yhteishankinta ja turvataan yhteishankkeiden edellyttämät VM:n resurssit.

VAHTIn ja VM:n tietoturvaohjauksen toiminnan vahvistaminen tulee ajankohtaiseksi heti tämän kehitysohjelman toteutuksen alkaessa. Mikäli sitovien määräysten antaminen toteutuu, korostuu molempien rooli entisestään. Koko kehitysohjelman suunnittelun, toteutuksen ja valvonnan kannalta on ensiarvoisen tärkeää, että näillä on käytössä tietoturvallisuuden parhaat asiantuntijat eri hallinnonaloilta.

Perusinfrastruktuurin tietoturvallisuuden kehittämisen toiminta jakautuu useille tahoille. VM koordinoi tätä jatkuvaa toimintaa valtionhallinnon sisällä.

Peruskäyttäjien tietoturvallisuuden tukeminen on kenties laajin ja moniulotteisin tämän kehitysohjelman asioista. Toteutusvastuu hajautuu kaikille hallinnonaloille ja mitä moninaisimpiin hankkeisiin. Kehityskohde on jatkuvaa toimintaa ja toteutumisen seurannassa on luotettava virastokohtaisiin arvioihin tavoitteiden toteutumisesta.

6.4 Tärkeät hankkeet ja kehittämiskohteet

Tärkeiksi vaikutuksiltaan merkittäviksi kehityskohteiksi arvioitiin seuraavat:

- Varmenteiden käytön edistäminen sähköpostissa.
- Tunnistaminen ja oikeuksien hallinta.
- Tietoturvaohjeistuksen kehittäminen.
- Tietoliikenneverkkojen ja päätelaitteiden tietoturvallisuus.
- Asiakasnäkökulman korostaminen.
- Sähköinen valvonta ja yksityisyyden suoja.
- Valtionhallinnon ympärivuorokautinen tietoturvapalvelu.
- Sitovien julkishallinnon tietoturvaa koskevien normien anto.
- Asianhallinnan tietoturvallisuus.
- Yhteistyö tietoyhteiskuntaohjelman kanssa.
- Yksityisyyden suojan yleinen kehittäminen.
- Kansainvälisen tietoturvayhteistyön kehittäminen.

Varmenteiden käytön edistäminen sähköpostissa perustuu SM:n, VM/VNTHY:n ja VAHTIn toimikorttiprojektien kokemuksiin. Varmenteiden käyttöönoton vaatimat tekniset ja hallinnolliset toimet valmistetaan ja toteutetaan koordinoidusti hankkeessa, joka aloitetaan vuoden 2004 ensimmäisellä neljänneksellä. Tämän rinnalla laaditaan puitesopimus toimikorttien ja niiden lukijalaitteiden hankinnasta.

Tunnistamisen ja oikeuksien hallinnan kehittäminen nivoutuu sekä varmenteiden käytön hankkeeseen että SM:ssä ja VM/VNTHY:ssa käynnissä olevien virkakorttihankkeiden tuloksiin. Kehittäminen aloitetaan vuoden 2004 aikana, ja panostusta lisätään vähitellen hankkeiden edistyessä.

Päätelaitteiden ja tietoliikenneverkkojen tietoturvallisuus tulee koko ajan ajankohtaisemmaksi. Mobiililaitteiden teho niin tietojenkäsittelykapasiteetin kuin tietoliikennekapasiteetin osalta kasvaa jatkuvasti. Langattomien lähiverkkojen merkitys on tällä

hetkellä erittäin pieni, mutta lisääntynee tulevaisuudessa. Näin ollen tarvittavat toimenpiteet käynnistetään vuoden 2004 loppupuolella. Hankkeen toteutuksesta vastaa VAHTI. LVM:n, Viestintäviraston ja operaattorien rooli on merkittävä.

Asiakasnäkökulman mukanaolo on jatkuvaa toimintaa, mutta valmisteilla olevan käytettävyyttä käsittelevän ohjeen julkistaminen tarjoaa mahdollisuuden asian edistämiseen. Tietosuojavaltuutetun rooli asiakasnäkökulman huomioimisessa on tärkeää.

Myös sähköisen valvonnan vaikutusten arvioinnissa tietosuojavaltuutetun rooli on keskeinen. Yhdistämällä tämä VM:n ohjeistukseen ja Viestintäviraston, OM:n sekä muiden toimijoiden asiantuntemukseen saadaan aikaan hanke, joka käynnistetään vuoden 2005 alkupuolella.

Valtionhallinnon ympärivuorokautisen tietoturvapäivystyksen tarvetta selvittämään perustetaan VAHTIn työryhmä.

Sitovien julkishallinnon tietoturvallisuutta koskevien normien antamisen tarpeellisuuden ja mahdollisuuden selvittäminen aloitetaan. Vastuullisena ministeriönä on valtiovarainministeriö.

Asianhallinnan tietoturvallisuus liittyy läheisesti sähköpostin tietoturvallisuuteen, joten hanke käynnistetään kun roskapostin torjunta ja varmenteiden käytön edistäminen ovat valmiita tai valmistumassa. Tällöin asian tärkeys on noussut entisestään, joten tuloksille on lisää kysyntää. Kehityskohteen toteutus edellyttää poikkeuksellisen laajaa yhteistyötä, joten sen toteuttamiseen osallistuvat ainakin VM, VAHTI, Valtipa, Arkistolaitos ja Juhta.

Yhteistyö tietoyhteiskuntaohjelman kanssa tulee olla jatkuvaa. Kukin ministeriö vastaa hallinnonaloillaan yhteyden pidosta tietoyhteiskuntaohjelmaan ja ohjelmassa vaikuttaviin henkilöihin.

Yksityisyyden suojan pitäminen kansainvälisesti hyvällä tasolla on jatkuvaa toimintaa, jossa Tietosuojavaltuutetun toimistolla on päävastuu. Oikeusministeriö ja muut ministeriöt vastaavat siitä, että toimiston toimintaedellytykset turvataan, ja että tietosuojakysymykset otetaan huomioon kaikessa toiminnassa. VM vastaa, että tietosuojaan liittyvistä asioista voidaan tarvittaessa julkaista VAHTI-ohjeita. Lisäksi huolehditaan, että VAHTI-ohjeita laativissa työryhmissä on riittävä tietosuojakysymysten ammattitaito. Tietoturvallisyystyön kansainvälistyminen edellyttää myös kansallisten toimijoiden tiiviistä yhteistyötä.

Kansainvälinen yhteistyö tietoturva-asioissa lisääntyy ja saa uusia muotoja. Kehityshankkeen arvioidaan vaativan jatkuvaa panostusta, mutta resurssitarve ja toisaalta työstä saatavat hyödyt lisääntyvät kehitysjakson loppua kohti.

6.5 Muut hankkeet ja kehittämiskohteet

Muut kuin edellä luetellut kehittämiskohteet kuuluvat tähän luokkaan. Niiden toteutusprioriteetti ei tällä hetkellä ole yhtä korkea, mutta asiat ovat tästä huolimatta merkittäviä ja niiden toteuttaminen edistää valtionhallinnon tietoturvallisuutta.

Ohjelmien versiopäivitysten jakelun helpottamisesta olisi suuri apu tietohallintohenkilöstölle, mutta hankkeen toteuttaminen voi odottaa kehitysjakson loppupuolelle, jolloin hanketta tukevien ohjelmistoratkaisujen voidaan olettaa olevan nykyistä kehittyneempiä.

PET-teknologioiden edistämisessä ja tietoturvaratkaisujen integroinnissa tilanne on samankaltainen: käytännön sovellukset ovat vasta tulossa ja niiden tuomat mahdollisuudet tulevat ajankohtaisiksi kehitysjakson loppupuolella. Konkreettiset kehityshankkeet käynnistetään vasta, kun tuloksista voidaan olla varmoja. PET-teknologioiden osalta on otettava huomioon, että niissä on kyse myös palvelujen kehittäjille suunnattavasta tiedotuksesta.

Tietoturvaverkostojen, seminaarien ja hyvien toimintatapojen edistäminen toteutuu pitkälti muiden kehityskohteiden tai jo käynnissä olevien hankkeiden avulla. Verkottumisessa ja hyvien toimintatapojen edistämisessä päävastuu on vapaamuotoisella tietoturvaihmisten välisellä kommunikaatiolla, jota ei erillisellä hankkeella juurikaan voi vaikuttaa.

Arviointeja edistetään syksyllä 2003 julkaistun VAHTI-ohjeen implementoinnilla. Arviointien merkitys kasvaa, joten työryhmä päätti odottaa niiden yleistymistä ennen kuin hankkeita käynnistetään. Arviointien edistämiseen tähtäävät kehityshankkeet vaativat resursseja, jotka ovat niukkoja ja joiden kohdentaminen on harkittava tarkasti. Aiheen ajankohtaisuus arvioidaan uudelleen kehitysjakson loppupuolella.

VAHTIn sivustoille avattava tietoturva-aiheinen keskustelufoorumi on hanke, jonka menestyksekäs toteuttaminen riippuu muiden kehityskohteiden toteuttamisesta: tunnistamismenettelyiden (HST- ja virkakortti) hankkeiden on oltava pitkällä, VAHTIn resursseja on vahvistettava ja tietoturvaverkostojen syntyminen on oltava yleistä. Näin ollen työryhmä katsoi, että hankkeen prioriteetti ei ole kovin korkea, mutta sen toteuttaminen kehitysjakson loppupuolella on suotavaa.

7 YHTEENVETO

Työryhmän työn ensisijaisena tavoitteena oli valtionhallinnon ministeriöiden, virastojen ja laitosten sekä yksittäisen työntekijän tietoturvallisuuden parantaminen, mutta tämän tavoitteen rinnalla pohdittiin keinoja, joilla virastot ja laitokset voivat parantaa myös suomalaisen yhteiskunnan tietoturvallisuuden tasoa. Tämän tulee tapahtua yhteistyössä elinkeinoelämän ja kuntasektorin kanssa.

Työn lopputulokseksi haluttiin laaja kehitysohjelma, joka sisältää myös uusia toimintatapoja ja -muotoja, ja joka nivoutuu muuhun julkishallinnon kehittämiseen. Ohjelmassa otetaan kantaa tietoturvallisuuden ohjaamiseen ja painotetaan tietoturvallisen toiminnan hyötyjä toiminnan kehittämisessä.

Työryhmä keräsi laajasti tietoa tietoturvatilanteesta valtionhallinnossa. Työryhmän tekemissä haastatteluissa ja kyselyssä saatiin arvokasta palautetta, mikä analysoitiin ja otettiin huomioon kehitysohjelman laadinnassa. Haastattelujen tulosten vaikutus kehitysohjelmaan on helposti havaittavissa: tietoturvallisuuden kehitysohjelman hankealueet on pitkälti valittu juuri kehityshankkeiden loppuasiakkaiden mukaan, eikä teknologiavetoisesti uusien uhkien tai mahdollisuuksien mukaan.

Julkisten palvelujen siirtyessä enenemässä määrin tietoverkkoihin, korostuu tietoturvallisuuden merkitys jokaiselle asiakkaalle ja virkamiehelle. Tietoturvaongelmat ovat saaneet huomiota tiedotusvälineissä. Suomalainen valtionhallinto nauttii kansainvälisissä vertailuissa korkeaa arvostusta omien asiakkaittensa - kansalaisten - keskuudessa. Luottamuksen säilyttäminen nopeasti muuttuvassa ympäristössä on suuri haaste. Haastavuutta lisää, että tietoturvallisuuteen vaikuttavat asiat ovat usein nopeimmin muuttuvien joukossa.

Valtioneuvosto on 4.9.2003 hyväksynyt kansallisen tietoturvastrategian, jolla edistetään tietoturvallisuutta koko yhteiskunnassa. Tämä kehittämisohjelma tukee strategian tavoitteiden saavuttamista valtionhallinnossa.

Valtionhallinnossa tietoturvatyö on hajautunut useille eri toimijoille. Merkittävin toimija yleisessä tietoturvatyössä on valtiovarainministeriön asettama VAHTI, joka on valmistellut erittäin kattavan tietoturvaohjeiston, jota käytetään valtionhallinnon lisäksi kunnallishallinnossa ja yrityksissä.

Tässä kehittämisohjelmassa on eri kehittämishankkeet koottu erilaisiin laajempiin loogisiin kokonaisuuksiin. Näitä hankekokonaisuuksia ovat:

1. Tietoturvakulttuurin luominen, joka sisältää tulosohjauksen käyttämisen tietoturvallisuuden kehittämiskeinona sekä monipuolista eri tahojen tuottamaa tietoturvakoulutusta.
2. Valtionhallinnon tietoturvallisuuden kehittämistä tuetaan VAHTIn ja VM:n tietoturvatyötä vahvistamalla sekä virastojen välistä yhteistyötä edistämällä. Sitovien tietoturvanormien antamisen tarpeet ja mahdollisuudet selvitetään.
3. Tietoturvallinen viestintä ja asianhallinta, jossa painotetaan sähköpostiliikenteen sujuvuutta ja turvallisuutta sekä luotettavia tunnistamismenettelyjä.
4. Tietoturva- ja tietojärjestelmävastaavien työn tukeminen. Yhteishankkeilla ja puitesopimuksilla sekä konkreettisilla ohjeilla pyritään helpottamaan heidän työtään.
5. Toiminnan ja palvelujen kehittäjien työn tukeminen on tärkeää, jotta tietoturvallisuus ja yksityisyyden suoja otetaan huomioon jo palvelujen ja järjestelmien suunnitteluvaiheessa.
6. Peruskäyttäjän tietoturvatyön tukeminen, jossa painottuu koulutus ja turvallisen toimintaympäristön tarjoaminen sekä johdon esimerkki.

Tietoturvallisuuden kehitysohjelman vastuullinen ministeriö on valtiovarainministeriö, jonka tukena käytännön koordinoinnista, seurannasta ja yhteensovittamisesta huolehtii VAHTI. VM ja VAHTI huolehtivat hankkeiden vastuullisten tahojen nimittämisestä sekä hankkeiden etenemisen seurannasta ja yhteistoiminnan koordinoinnista.

Tässä ohjelmassa esitetyistä kehityskohteista osa tukee läheisesti käytännön tietoturvatyötä, osa tietoturvallisen tietoyhteiskunnan muodostumista. Kaikista kohdista on pyritty tekemään niin konkreettisia kuin se asian luonteen huomioon ottaen on mahdollista.

Kehitysohjelma toteutetaan hanketyöllä. Tietototuturvaresurssien niukkuuden vuoksi kehityshankkeet on priorisoitu ja niille on laadittu alustava aikataulu. Näin halutaan varmistaa kaikkein akuuteimpien hankkeiden, kuten roskaposti, tietoturvallisuuden tulosohjaus sekä VAHTIn toiminnan vahvistaminen, läpivienti.

Valtionhallinnon tietoturvallisuuden ohjauksen kehittäminen on ajankohtainen asia, jonka merkitys on suuri. Ohjauksen jämäköittäminen normiohjauksella on eräs keskeinen kehitysehdotus, joka aiheuttaisi muutoksia nykyiseen tilanteeseen. Yhtäältä VM:n ja VAHTIn, ja toisaalta ohjauksen virastojen tietoturvaresurssien määrää ja laatua on kehitettävä.

Hankkeiden toteuttamisaikataulu on kehittämisohjelmassa laadittu varsin tiiviiksi: useimmat hankkeet esitetään käynnistyväksi jo vuonna 2004. Tämä asettaa haasteita toteuttavien organisaatioiden resurssien hallinnalle. Hankkeille on kuitenkin niin suuri tarve, että niitä ei voi lykätä kovin pitkälle.

HAASTATTELUT JA KYSELY

Työryhmä lähetti kyselyn yhteensä 25:lle ennalta valitulle henkilölle, joiden arvioitiin kykenevän täydentämään työryhmän työtä omilla näkemyksillään. Haastatteluja sovittiin 6 kappaletta. Yksi sähköpostikysely muutettiin haastatteluksi.

Kaikki 7 haastattelua tehtiin, joten vastausprosentti oli 100. Sähköpostikyselyyn saatiin 22 vastausta, joka nostaa vastausprosentin 92:teen, mitä voidaan pitää erittäin hyvänä tuloksena.

Haastatellut edustivat yhteensä noin 63 000 työntekijää ja 63 000 työasemaa, 1 600 päätoimista IT-henkilöä ja 250 miljoonan euron ICT-budjettia.

Kyselylomake

1 Taustatiedot

1) Organisaation henkilömäärä
2) Työasemien lukumäärä
3) Tietohallintohenkilöiden määrä
4) ICT-budjetti
5) Mitkä tietohallinto- / tietotekniikkatoiminnot ostatte ulkoa?

2 Tietoturvallisuuden nykytilanne

6) Mitkä ovat merkittävimmät tietoturvaongelmanne?
7) Mitkä ovat mielestänne hyviä tietolähteitä tietoturvatyössä?
8) Mitä valtionhallinnon tietoturvallisuuden palveluita, ohjeita tai suosituksia tiedätte käyttävänne?
9) Miten arvioisitte VM/VAHTIn antamia suosituksia:
    a) Mitä kehittämistarpeita VM/VAHTIn ohjeissa on?
    b) Mitkä ohjeet ovat mielestänne olleet parhaita?
    c) Mitä uusia ohjeita kaipaatte?
10) Miten seuraatte lainsäädännön ja muiden normien vaikutuksia tietoturvatoimin-

taanne? Mikä on käsityksenne hallintoa sitovien ja yleisten tietoturvanormien kehittämistarpeista?

11) Mihin julkisen hallinnon tai oman toimialanne tietoturvallisuutta parantaviin hankkeisiin olette osallistunut v. 2002-2003 aikana?

12) Mitkä ovat olleet merkittävimmät esteet tietoturvallisuutenne kehittämiseksi? (esimerkiksi henkilöiden, osaamisen tai rahoituksen puute, johdon mielestä asia ei ole tärkeä, jalkauttaminen ei ole onnistunut)

13) Mitkä ovat näkemyksenne mukaan merkittävimmät tietoturvallisuuden kehittämisen esteet Suomessa?

14) Mitkä ovat seuraavat tietoturvahankkeenne?

3 Tietoturvallisuuden tavoitetila

15) Kuvailkaa lyhyesti organisaationne tietoturvallisuuden tavoitetilaa?

16) Mitkä näette suurimpina tietoturvaongelmina muutaman seuraavan vuoden aikana? Miten aiotte ongelmiin vastata?

17) Mitkä ovat merkittävimmät esteet haluamanne tietoturvatason saavuttamiseksi?

18) Millaista tukea omalle tietotuvallisuustyöllenne toivotte julkisen hallinnon ja erityisesti VM:n hankkeilta ja toimenpiteiltä?

19) VM:n tietoturvatyön pääasiallinen muoto on ollut VM/VAHTIn suositusten ja ohjeiden julkaisu ja yhteishankkeet. Miten VM ja VAHTI voisivat kehittää toimintaansa tai mitä muita tietoturvatyön muotoja kaipaatte?

20) Miten valtionhallinnon muut toimijat kuin VM ja VAHTI voivat edistää viranomaisten tietoturvatyötä?

21) Esityksiä mahdollisiksi hankkeiksi:

- eri hallinnonaloille
- VM:lle

22) Miten kansallista tietoturvastrategiaa tulisi edistää hallinnossa?

4 Kysymykset toiminnan kehittämisestä vastaavalle henkilölle

1) Millaista toiminnan kehittämistä teette? Suunnitteletteko uusia sähköisiä palveluita (verkkopalveluita)?

2) Onko näissä palveluissa erityisiä tietoturvaominaisuuksia tai -vaatimuksia?

3) Missä vaiheessa kehittämishankkeissa tarkastellaan tietoturva-asioita?

4) Ketkä osallistuvat tietoturvallisuuden arviointiin?
5) Haittaavatko tietoturvavaatimukset toiminnan kehittämistä? Jos haittaavat, niin miten?
6) Mitä tietoturvauhkaa pidätte kaikkein vakavimpana suunnitteilla olevien ja nykyisten palvelujen osalta?
7) Mitkä tietoturvallisuuteen liittyvät kysymykset tuottavat eniten päänvaivaa?
8) Mistä saatte tietoa verkkopalveluiden tai muun toiminnan kehittämiseen liittyvistä tietoturva-asioista? Miten haluaisitte saada?
9) Miten asiakkaan tietoturvaosaamisen taso otetaan huomioon?
10) Tuleeko palveluiden käyttäjiltä palautetta tietoturvallisuudesta? Jos tulee, niin millaista?
11) Miten tunnette VM/VAHTIn tietoturvatyötä?

5 Kysymykset loppukäyttäjälle

Tietoturvallisuudella tarkoitetaan tilaa, jossa tietojen, tietojärjestelmien ja tietoliikenteen luottamuksellisuus, eheys ja käytettävyys ovat kunnossa. Toisin sanoen oikeat tiedot ovat niiden käyttöön oikeutettujen henkilöiden (eikä kenenkään muun) käytettävissä.

1) Onko teillä selvillä organisaationne tietoturvalinjaukset ja toimintaohjeet?
2) Pystyttekö käytännössä noudattamaan ohjeita? Jos ette, niin mitkä ovat suurimmat ongelmat?
3) Ovatko ohjeet
    a. riittävän selkeät
    b. helposti saatavilla
    c. helposti sovellettavissa
    d. ajan tasalla
4) Mistä saatte tietoa tietoturva-asioissa? Tunnetteko VAHTI-ohjeita? Keneen otatte yhteyttä, mikäli haluatte lisätietoa?
5) Miten tärkeänä yksikkönne johto pitää tietoturvallisuutta?
6) Haittaavatko tietoturvallisvaatimukset päivittäistä työtä?
7) Mitä pidätte vakavimpana tietoturvaongelmana?

Aikataulu ja osallistuvat tahot

Raportin rakenteen mukainen järjestys
Osallistuvien tahoja ei ole rajattu taulukossa oleviin, vaan osallistuminen on avointa kaikille valtionhallinnon toimijoille
Aikataulutus vain kahden korkeimman prioriteettiluokan kehityskohteilla (*)

Aikataulu ja osallistuvat tahot

Raportin rakenteen mukainen järjestys
Osallistuvien tahoja ei ole rajattu taulukossa oleviin, vaan osallistuminen on avointa kaikille valtionhallinnon toimijoille
Aikataulutus vain kahden korkeimman prioriteettiluokan kehityskohteilla (*)

Valtionhallinnon tietoturvallisuuden kehitysohjelma Toteutusssunnitelma		
1 Tietoturvakulttuurin luominen		
1.1 Tietoturvallisuuden tulosohjaus	*	VM, Kansliapäälliköt, Ministeriöt
1.2 Tietoturvallisuuden sitominen virastojen palveluihin ja prosesseihin	*	Ministeriöt ja virastot, VAHTI, Johto
1.3 Tietoturva-asioiden kouluttaminen		OPM, VM, Ministeriöt ja virastot, Korkeakoulut
1.4 Tietoturvaverkostot, -seminaarit ja hyvät toimintatavat		Ministeriöt ja virastot, VM, VAHTI
1.5 Keskustelufoorumi tietoturva-asioista		VM, VAHTI, ViVi, LVM
1.6 Kansainvälinen yhteistyö tietoturva-asioissa	*	VM, TSV, OPM, Korkeakoulut, LVM, CSC
2 Valtionhallinnon tietoturvallisuustyön yleinen tukeminen		
2.1 VAHTIn toiminnan vahvistaminen	*	VM, Ministeriöt ja virastot
2.2 Tietoturvaohjeistuksen kehittäminen	*	VAHTI, VM, Ministeriöt ja virastot
2.3 Perusinfrastruktuurin tietoturvallisuus	*	Ministeriöt ja virastot, VM, PTS, HVK, LVM
2.4 Sitovien julkishallinnon tietoturvaa koskevien normien anto	*	OM, VM, VAHTI, LVM
2.5 Yhteistyö tietoyhteiskuntaohjelman kanssa	*	Ministeriöt, VM, VAHTI, JUHTA
2.6 Yhteistyö virastojen valmiustoiminnan kanssa		Ministeriöt ja virastot, HVK, PTS, VM, KTM, Valmiuspäälliköt, PV
2.7 Arviointi		Ministeriöt ja virastot, VM, VTV, VAHTI
2.8 Yhteistoiminta ja jaetut resurssit		Ministeriöt ja virastot, VM, VAHTI, Johto
3 Tietoturvallinen viestintä ja asianhallinta		
3.1 Roskaposti eli späm	*	LVM, ViVi, VM, VAHTI, TSV, Operaattorit
3.2 Varmenteiden käytön edistäminen sähköpostissa	*	SM, VM, VNTHY, VRK
3.3 Tunnistaminen ja oikeuksien hallinta	*	VM, SM, VAHTI, VNTHY, TSV, CSC
3.4 Lähiverkkojen ja päätelaitteiden tietoturvallisuus	*	LVM, ViVi, VAHTI, Operaattorit
3.5 Asianhallinnan tietoturvallisuus	*	VM, Arkistolaitos, Valtipa, JUHTA, VAHTI
4 Tietoturva- ja tietojärjestelmävastaavien työn tukeminen		
4.1 Valtionhallinnon yhteishankkeet ja hankintayhteistyö	*	VM, VAHTI, Hansel (hankinnat), KTM
4.2 Ohjelmien versiopäivitysten hallinta ja jakelu		VAHTI, VM, Ministeriöt ja virastot, IT-talot
4.3 Tietoturvaratkaisujen integrointi		VAHTI, VM, Vivi, PTHK, IT-talot
4.4 Virustorjunnan ylläpito		Ministeriöt ja virastot, VAHTI, IT-talot, Operaattorit
4.5 Valtionhallinnon ympärivuorokautinen tietoturvapalvelu	*	VAHTI, Vivi, PTHK, PV
5 Toiminnan ja palvelujen kehittäjien työn tukeminen		
5.1 Asiakasnäkökulman korostaminen	*	TSV, Ministeriöt ja virastot, Johto
5.2 Sähköinen valvonta ja yksityisyyden suoja	*	TSV, VM, ViVi, OM, LVM, TM, Työsuojelupiirit
5.3 Yksityisyyden suojan yleinen kehittäminen	*	TSV, OM, VM, LVM
5.4 PET-teknologiat		TSV, VAHTI, VM, LVM
6 Peruskäyttäjän tietoturvatyön tukeminen	*	Ministeriöt ja virastot, Tietoturvapäälliköt, Johto

Johto = Yksiköiden johto
Korkeakoulut = Yliopistot ja ammattikorkeakoulut

Vastuullinen taho tarkoittaa tahoa, joiden osallistuminen kehityskohteeseen on suotavaa; halukkaiden mukaantuloa ei rajoiteta

LÄHTEITÄ:

Kehitysohjelman sisältöön ja muotoon vaikuttivat eniten seuraavat dokumentit:

- Hallitusohjelman tietoyhteiskuntaohjelma (http://www.government.fi/tiedostot/pdf/fi/41868.pdf)
- Kansallinen tietoturvastrategia (http://www.mintc.fi/www/sivut/suomi/tele/tietoturvastrategia.pdf)
- Julkisen hallinnon sähköisen asioinnin toimintaohjelma eli ns. Backmanin työryhmän raportti (http://www.vm.fi/tiedostot/pdf/fi/40642.pdf)

VM:n ja VAHTIn tietoturvaohjeet: (www.vm.fi/vahti)

- Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
- Opas julkishallinnon tietoturvakoulutuksen järjestämisestä, VAHTI 6/2003
- Käyttäjän tietoturvaohje, VAHTI 5/2003
- Valtionhallinnon tietoturvakäsitteistö, VAHTI 4/2003
- Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003
- Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003
- Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003
- Arkaluonteiset kansainväliset tietoaineistot, VAHTI 4/2002
- Valtionhallinnon etätyön tietoturvallisuusohje, VAHTI 3/2002
- Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002
- Toimet tietoturvaloukkaustilanteissa, VAHTI 7/2001
- Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista, VAHTI 6/2001
- Valtionhallinnon sähköpostien ja lokitietojen käsittelyohje, VAHTI 5/2001
- Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001

- Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001
- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
- Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje, VAHTI 4/2000
- Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000
- Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, VAHTI 2/1999
- Tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000
- Tietoturvallisuuden tulosohjaus ja kehittämisvälineet, VAHTI 2/1997
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM 19.1.2000

VAHTI

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

1/2004

VALTIONHALLINNON TIETOTURVALLISUUDEN KEHITYSOHJELMA 2004–2006

ISBN 951-804-425-2
ISSN 1455-2566