VALTIOVARAINMINISTERIÖ

Valtion-hallinnon 24/7-tieto-turva-valvonnan hanke-ehdotus

5/2008 VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

Valtionhallinnon 24/7-tietoturvavalvonnan hanke-ehdotus

Valtionhallinnon tietoturvallisuuden johtoryhmä 5/2008 VAHTI

Painotuote

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 09 16001 (vaihde)
Internet: www.vm.fi
Taitto: Anitta Heiskanen /VM-julkaisutiimi

ISSN 1455-2566
ISBN 978-951-804-894-0 (nid)
ISBN 978-951-804-884-1 (pdf)
Helsinki 2008

Esipuhe

Tämän ehdotuksen on laatinut Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTIn alainen valtion ympärivuorokautisen tietoturvatoiminnan hankesuunnitteluryhmä. Ehdotuksessa kuvataan valtionhallinnon ympärivuorokautisen tietoturvatoiminnon tarpeita, tehtäviä sekä hanke-ehdotus alustavine suunnitelmineen. Raportti on käsitelty ja saanut yksimielisen tuen VAHTIn kokouksissa elo- ja syyskuussa 2008.

Hanke-ehdotuksen mukainen eteneminen on saanut vahvan tuen myös valtioneuvoston kansliapäälliköiden kokouksessa 6.10.2008 ja valmiuspäälliköiden kokouksessa syyskuussa 2008 sekä valtiovarainministeriön johdon ja asiantuntijoiden tapaamisissa sisäministeriön ja liikenne- ja viestintäministeriön johdon ja asiantuntijoiden kanssa.

Valtiovarainministeriö (VM) vastaa julkishallinnon tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTIssa käsitellään kaikki merkittävät valtionhallinnon tietoturvalinjaukset ja tietoturvatoimenpiteiden ohjausasiat. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTI edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

VAHTIn toiminnalla on parannettu valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä, kansalaistoiminnassa ja kansainvälisesti. VAHTIn toiminnan tuloksena muun muassa on aikaansaatu erittäin kattava yleinen tietoturvaohjeisto (www.vm.fi/VAHTI). Valtiovarainministeriön ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita. VAHTI on saanut

kolmena perättäisenä vuotena tunnustuspalkinnon esimerkillisestä toiminnasta Suomen tietoturvallisuuden parantamisessa.

VAHTI on valmistellut, ohjannut ja toteuttanut valtion tietoturvallisuuden kehitysohjelman, jossa on aikaansaatu merkittävää kehitystyötä yhteensä 26 kehityskohteessa yli 300 hankkeisiin nimetyn henkilön toimesta. Osana kehitysohjelmaa selvitys valtion ympärivuorokautisesta tietoturvatoiminnasta valmistui vuonna 2006 (VAHTIn julkaisu 4/2006).

Sisältö

1 Tausta

Valtion ympärivuorokautisen tietoturvavalvonnan hankkeen tausta on määritelty Selvitys valtion ympärivuorokautisen tietoturvavalvonnan järjestämisestä – ohjeessa (Liite 1, poimintoja VAHTI 4/2006-ohjeesta).

Tämän työryhmän tehtävänä on valtionhallinnon organisaatioiden ympärivuorokautiseen tietoturvavalvontaan liittyvän hankesuunnitelman valmistelu ja hanke-ehdotus. Tämän työn perusteella voidaan tehdä päätöksiä varsinaisesta toteutushankkeesta. Tässä työssä ympärivuorokautisesta tietoturvavalvonnasta on käytetty nimeä 24/7.

Hanke-ehdotusta valmistelevassa VAHTIn alaisessa työryhmässä ovat olleet mukana:

Juhani Sillanpää, VM, työryhmän puheenjohtaja
Kauto Huopio, Viestintävirasto
Pirkko Kilpeläinen, Ilmatieteenlaitos
Kimmo Aaltonen, Ilmatieteenlaitos
Henri Lehtelä, Hallinnon tietotekniikkakeskus
Reko-Aleksi Renvik, Väestöreskisterikeskus
Tero Tuominen, Merenkulkulaitos
Minna Leivo, Puolustusvoimat
Harri Mäntylä, Puolustusvoimat
Jouni Rosenlöf, konsultti, JRComplex Oy

2 Tehtävä

Työryhmän tehtävänä oli laatia hanke-ehdotus valtionhallinnon ympärivuorokautisen tietoturvatoiminnan organisoinnista.

Ympärivuorokautinen tietoturvatoiminta, 24/7, on valtionhallinnon ympärivuorokautista tietoturvatoimintaa hoitamaan perustettava toiminto. Tavoitteena on seurata olennaisia valtion järjestelmiin liittyviä tietoturvatapahtumia, poikkeamia ja muutoksia sekä tarvittaessa reagoida nopeasti olennaisiin muutoksiin tietoturvatilanteessa. Kerättävän tiedon avulla muodostetaan jatkuvasti päivittyvä kokonaistilannekuva valtionhallinnon tietoturvallisuuden nykytilasta. 24/7 pyrkii myös ennakoimaan mahdollisia olennaisia riskikeskittymiä sekä tiedottaa ja opastaa asianosaisia tietoturvatilanteesta.

3 Lopputulos

3.1 Yhteenveto 24/7-toiminnasta

Ehdotettavan 24/7-toiminnon tehtävänä on tilanneseuranta ja tiedonjako. 24/7 ja valtion yhteisen turvallisen tietoliikenneverkon myötä kysymykseen voi tulla myös operatiivinen toiminta valvonnan piirissä olevien organisaatioiden tietoturvapoikkeamatilanteissa. 24/7 ja organisaatioiden välinen yhteistyömalli määritellään valvontasopimuksella. Organisaatioilta edellytetään, että perustietoturvataso on täytetty. 24/7 ohjeistaa valvottavia ja raportoitavia asioita erillisellä dokumentaatiolla.

24/7 raportoi kokonaistilannekuvasta sekä antaa tarvittaessa tilannekohtaisia raportteja ja suosituksia. Alkuvaiheessa painopiste on olennaisen poikkeamainformaation keräämisen organisoinnissa sekä yhteistyön kehittämisessä eri sidosryhmiin. Lisäksi painotetaan valtionhallinnon eri tietoturvatoimijoiden välisen yhteistyön kehittämistä.

Tietoturvapoikkeamatieto kerätään valvontasopimuksen mukaisesti virastoilta itseltään, palveluntuottajilta sekä mahdollisista automaattisista valvontajärjestelmistä. Valvontasopimuksessa virasto antaa 24/7:lle valtuudet organisaatioiden keräämän tiedon käsittelyyn ja tarkentaviin selvityksiin.

24/7 antaman ohjeistuksen mukaisesti pyritään keräämään vain olennaisia ja organisaatiolaajuisesti ja organisaatioiden välisesti merkittäviä poikkeamia. Olennaisia poikkeamia ovat esimerkiksi havaitut tietomurrot, merkittävät tekniset vikaantumiset, palvelunestohyökkäykset tai muut merkittävät muutokset järjestelmien tai verkkojen kuormitustasoissa sekä haittaohjelmaepidemiat.

Poikkeamatietojen tunnistamisen ja analysoinnin ensimmäisen vaiheen jälkeen 24/7 suorittaa analysoinnin toisen vaiheen, jossa raportoiduista tiedoista suodatetaan vielä uudelleen olennainen informaatio sekä tehdään tapahtumien kriittisyysluokitus.

Poikkeamatietojen keräämisessä pyritään mahdollisimman määrämuotoiseen formaattiin niin, että raportoivien tahojen vaikutus tietosisältöön jää mahdollisimman vähäiseksi. Esimerkkinä mm. alasvetovalikot tms. www-lomakkeilla.

Organisaatioille tuotetaan säännöllisesti kokonaistilanneraportti, joka koostuu tarkastellun aikajakson tapahtumista. Päivittäin toimitetaan päiväkohtainen raportti. Lisäksi tuotetaan sopimuksen mukaisesti erityisiä tilanneraportteja erityisorganisaatioille.

Hankkeen hyödyt:

- mahdollistetaan kokonaistilannekuvan saaminen ongelmatilanteissa
- reagointikyvyn tehostuminen
- järjestelmien käyttökatkot pienempiä
- ongelmatilanteiden rajaus ja vahinkojen minimoiminen
- kustannustehokkuuden parantaminen karsimalla päällekkäisiä toimintoja
- vastuiden ja valtuuksien selventäminen
- luottamuksen säilyttäminen valtionhallinnon toimintaan
- menettelytapojen yhtenäistäminen
- tietoturvatietoisuuden nostaminen
- tarve lisätä tietoturvaihmisiä organisaatioissa pienenee
- yhteistyö valtionhallinnon tietoturvatoimijoiden välillä tiivistyy.

3.2 Selvitettäviä asioita

Voiko organisaatioita velvoittaa liittymään 24/7-valvontaan valvontasopimuksessa määritellyillä erilaisilla toimintatasoilla?

Toiminta tilanteessa, jossa edellytettyä valvontatietoa ei saada? Valvontasopimuksessa määriteltyjä asioita on sisällytettävä organisaatioiden SLA-sopimuksiin.

Voiko tai haluaako joku organisaatio antaa toimivaltaa poikkeamatilanteissa? Mikä muu operatiivinen toiminta on mahdollista?

Kuka johtaa , kuka vastaa, miten toiminta rahoitetaan?

Selvitettävä tehtävänjako valtion tietohallinnon, 24/7, CERT-FI ja virastojen välillä.

Selvitettävä kaikkien tiedon keräysten ja käytön osalta laillisuus.

Sähköisen viestinnän tietosuojalaki: verkkoliikenteen valvonta?

Millä edellytyksillä 24/7:lle voidaan antaa tietoja tietoturvapoikkeamatilanteissa?

Valtion yhteinen verkko: mitä voidaan tehdä jo ennen sitä ja mitä vasta sitten jälkeen?

Selvitettävä tietojärjestelmien luokittelun soveltaminen 24/7-toimintaan.

Eri poikkeamatilanteiden reagointi, toiminta ja vastuut?

Miten 24/7 keräämät tiedot, järjestelmät ja verkot tulee suojata ?

Selvitettävä mahdollisuus reaaliaikaiseen tapahtumatietojen vaihtamiseen valtionhallinnon tietoturvapalveluja tuottavien viranomaisten välillä.

4 Rajaus

24/7-valvonta koskee valtionhallinnon tietoteknistä toimintaympäristöä .

24/7-asiakkaana ei voi olla muu kuin valtionhallinnon organisaatio.

24/7-toiminta pitää olla valtionhallinnon organisaation tuottamaa, eikä sitä voida ostaa palveluna ulkopuolisena palveluntuottajalta.

24/7-ei suorita alkuvaiheessa asiakasorganisaatioiden tietoturvaan liittyvää operatiivista toimintaa.

5 Hankkeen jaottelu

5.1 Hankkeen jaottelu

1. Nykytilan kartoitus
2. Projektisuunnitelman teko
3. Projektisuunnitelman hyväksyminen
4. 24/7-toimintamallin ja dokumentaation tekeminen ja hyväksyttäminen
5. 24/7-vetäjän rekrytoiminen
6. Ohje poikkeamatietojen tunnistamisesta ja analysoinnin ensimmäisestä vaiheesta – laadinta
7. 24/7-toiminnan sisäinen toimintaohje
8. 24/7-toiminnan pöytätestaus
9. Valvontasopimuksen laadinta
10. Toimintaan liittyvien uhkien ja riskien kartoitus
11. 24/7-pilotti-projektiin osallistuvien perehdytys
12. 24/7-toiminnan pilotti-projekti rajatulla joukolla
13. 24/7Pilotin raportointi, tarkastaminen ja hyväksyminen
14. 24/7-Toiminnan ja rahoituksen hyväksyminen
15. 24/7-organisaation perustaminen
16. Tarvittavien tietoteknisten ympäristöjen hankinnan suunnittelu ja toteutus
17. 24/7-valvonnan roll-out

5.2 Hankkeen toteutus

Hanke toteutetaan kolmessa osassa:

- **Ensimmäisen osa**: painopiste on toiminnan ja menettelytapojen suunnittelu sekä tarvittavan dokumentaation tuottaminen
- **Toinen osa**: painopiste on simuloida 24/7-toimintaa ja saada menettelytavat jatkuvan valvontatoiminnan edellyttämälle tasolle
- **Kolmas osa**: painopiste on saada käynnistettyä 24/7-valvonta.

Konsultit on valittava kuhunkin osaan erikseen, koska osaamisaluetarpeet ovat osittain erilaiset eri osissa. Lisäksi on pyrittävä välttämään sidonnaisuuksia nykyisiin palvelutoimittajiin.

24/7-toimintaa ei saada kerralla valmiiksi, vaan kehittämisessä on hyvä noudattaa evoluutiota ja tarkentaa menettelytapoja saatujen kokemusten myötä.

Huomioitavia rinnakkaisia hankkeita:

- varautuminen
- tietoturvatasot
- valtion yhteinen tietoliikenneverkko
- Valtion IT-palvelukeskus
- muut valtionhallinnon merkittävät palvelukeskukset
- VAHTI-ohjeiden päivityshankkeet
- kansallisen tietoliikenneturvallisuuden kehittäminen, NCSA

6 Hankeorganisaatio

Hankeorganisaatiossa on oltava laaja näkemys eri hallinnonaloilta huomioiden turvallisuusviranomaiset, keskisuuret organisaatiot, joilla on jo 24h-palveluita sekä pienet organisaatiot, joilla ei välttämättä ole 24/7-tyyppisiä palveluita. Ehdotuksia mukaan tarvittavista organisaatioista:

- valtiovarainministeriö
- Puolustusvoimat
- Hallinnon tietotekniikkakeskus
- Viestintävirasto
- Valtion IT-palvelukeskus
- liikenne- ja viestintäministeriö
- valtioneuvoston kanslia
- tietosuojavaltuutetun toimisto
- suojelupoliisi
- keskisuuret ja pienet organisaatiot (käyttäjänäkökulma)

Hankkeen ohjausryhmä:

- valtion IT-johtaja
- VAHTIn edustus
- kansliapäälliköitä
- tietohallintojohtajia
- hallintojohtajia
- tietoturvajohtajia
- hankevetäjä sihteerinä

Ulkopuolisia konsultteja:

- 2-3 esimerkiksi projektin tilanteen ja tarpeen mukaan erillisiin työvaiheisiin
- järjestelmä/tietoliikennetausta
- tietoturvatausta
- ei valmiiden tuotteiden myyjiä, ei organisaatioista, jotka yrittävät saada 24/7-toimintoa oman firman hoitoon

7 Kustannusarviot

7.1 24/7-hankkeen suunnittelun ja käynnistysvaiheen kustannusarvio

Suunnittelu- ja käynnistysvaihe:

- jäsenet virkatyönä
- kokopäivätoiminen projektipäällikkö valtionhallinnosta 50 – 80 k€ / vuosi
- konsultit 150 – 300 htp / 150-300 k€
- simulointivaiheen laite ja ohjelmistokustannuksia (voidaan hyödyntää varsinaisessa toiminnassa)
- yhteensä > 300-540 k€ ajalla 9/2008-1/2012

7.2 Valtionhallinnon 24/7-tietoturvatoiminnon toimintakustannusten kustannusarvio

24/7-toiminnon kustannusarvio lähtee siitä, että 24/7 toimii jonkin jo olemassa olevan organisaation puitteissa, eikä sitä varten perusteta omaa virastoa. 24/7-kustannukset jaetaan toimintaan osallistuvien organisaatioiden kesken.

Valtionhallinnon tietoturvatoiminnon toimintakustannukset:

- alussa minimi 8 henkilöä, (jos olemassa olevassa organisaatiossa, josta hallinto- ym. palvelut). Arviot perustuvat VAHTI 4/2006:
- 8 x 4000 e/kk + sivukulut = 640 000 € / vuosi
- jos operatiivista toimintaa, kustannukset palvelua saavilta organisaatioilta
- järjestelmä- ja laitekustannukset
- tietoliikennekustannukset
- mikäli 24/7 ryhtyy tekemään operatiivista toimintaa, tarvitaan lisää henkilöitä, mutta vastaava työ on samalla pois kohde organisaatioista
- yhteensä < 1000 k€/vuosi

Kustannus-hyöty-analyysi:

- tietoturvavalvonnan järjestäminen on hyvän tiedonhallintatavan mukainen vaatimus, kustannussäästöjä saadaan keskittämällä toimintoja nyt suunnitellulla tavalla. Samalla tietoturvaosaajien ja päällekkäisen toiminnan tarve vähenee
- poikkeamatilanteiden kustannusvaikutusta voidaan rajoittaa ja normaalitilaan palautuminen nopeutuu
- palveluiden käytettävyyttä voidaan parantaa
- luottamusta julkisiin sähköisiin palveluihin voidaan parantaa
- voidaan muodostaa valtionhallinnon järjestelmien tietoturvallisuuden kokonaistilannekuva.

8 Hankkeen työskentely ja ohjausmenetelmät

Työskentelyssä tulee noudattaa normaaleja projektityömalleja ja käytäntöjä. Erityisesti tulee painottaa perusteellista määrittelytyötä hankkeen vaihesuunnitelman mukaisesti. Projektikäytännöt ovat:

- kokopäiväinen projektipäällikkö
- konsultit tilanteen ja tarpeen mukaan
- jäsenet 8 htp / kk
- projektikokous 1 x 2h / vko
- ohjausryhmän palaveri 1 / kk
- ohjausryhmän raportointi sähköpostilla viikoittain

9 Riskit ja uhat

Riskit ja uhat hankkeen toteutukseen ja tavoitteisiin:

- Mikäli hanketta ei toteuteta riittävässä laajuudessa, hyödyt jäävät saamatta
- Saadaanko oikeat ihmiset ja organisaatiot mukaan
- Organisaatioiden kanssa ei saada sovittua poikkeamatietojen luovuttamisesta
- Mukaan ei saada riittävän kattavaa joukkoa organisaatioita
- Projekti ryhtyy valitsemaan tuotteita liian aikaisessa vaiheessa
- Poikkeamadatan/raportoinnin laatu on liian heikkoa laadukkaaseen toisen vaiheen analyysiin tai kokonaistilannekuvaan
- Pilotti-projekti ei saa kerättyä riittävää määrää poikkeamadataa
- Ei saada rekrytoitua riittävää määrää sopivan osaamistaustan ihmisiä
- Valvonta suorittavien henkilöiden työnkuvaa ei saada riittävissä määrin vastaamaan osaamistaustaa (vaihtuvuus).

LIITE 1 Selvitys valtion ympärivuorokautisen tietoturvatoiminnan järjestämisestä

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060628Selvit/Vahti_4_06.pdf

JOHDON TIIVISTELMÄ

Selvitys on ensisijaisesti suunnattu ministeriöille, valtion virastoille ja laitoksille. Hallinnossa on laajalti kokemusta niistä vaikeuksista, jotka kohdataan, kun virka-ajan ulkopuolella sattuu viraston tietojärjestelmiin kohdistuva tietoturvapoikkeama tai kun tietoturvallisuuden ylläpitämiseen liittyvä välttämätön toimenpide on suoritettava lauantai-iltana. Työaika on muuttunut EU-toiminnan vaatimustenkin myötä pidemmäksi ja ajoittain ympärivuorokauden kestäväksi (esim. EU-kokoukset, kuten hallitusten väliset kokoukset). Kansainvälisiin kriiseihin ja katastrofeihin varautuminen vaatii myös jatkuvaa tietoturvallisuuden toimintavalmiutta. Tietoturvallisuuden vaaratilanteissa tietoliikenteen hätäpysäytystä viikonlopun ajaksi on joissain tapauksissa käytetty tuloksellisesti estämään viraston tietojärjestelmien vahingoittuminen. Sama tietoturvapoikkeama vaikuttaa helposti useaan kohdeorganisaatioon, sillä virastoissa on käytössä samankaltaisia järjestelmiä ja tietotekniikkaratkaisuita. Tietokoneet, niiden käyttöjärjestelmät, oheislaitteet, tukiohjelmistot ja jopa useat viranomaissovellukset ovat samankaltaisia sekä useiden viranomaisten yhdessä käyttämiä. Esimerkiksi poliisin ja Väestörekisterikeskuksen rekisterit ovat tällaisia yhteiskäyttöisiä palveluita.

Kustannuksia säästetään keskittämällä useiden valtion organisaatioiden tietoturvatoiminta yhteen palvelukeskukseen (=sisäinen ulkoistaminen).

Tietoturvapoikkeama on tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena rganisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut. Tällaisia poikkeamia turvallisuustilanteeseen ovat kaikenlaiset epätoivottavat tapahtumat, jotka estävät tieto- tai viestintäjärjestelmien käyttöä, aiheuttavat päätöksen tekoon käytettävien tietojen vääristymistä, mahdollistaisivat hallinnon tietojärjestelmien tietojen asiattoman käytön tai muuta haittaa viranomaisen tietohuollolle.

LIITE 2 Valtiovarainministeriön voimassaolevat VAHTI-julkaisut

Valtionhallinnon 24/7-tietoturvavalvonnan hanke-ehdotus, VAHTI 5/2008

Valtionhallinnon tietoturva-arviointipoolin toimintaraportti, VAHTI 4/2008

Valtionhallinnon salauskäytäntöjen tietoturvaohje, VAHTI 3/2008

Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008

VAHTIn toimintakertomus vuodelta 2007, VAHTI 1/2008

Tietoturvallisuudella tuloksia – valtionhallinnon tietoturvallisuuden yleisohje, VAHTI 3/2007

Äypuhelimien tietoturvallisuus hyvät käytännöt, VAHTI 2/2007

Osallistumisesta vaikuttamiseen - valtionhallinnon haasteet kansainvälisessä tietoturvatyössä, VAHTI 1/2007

Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006

Tietoturvakouluttajan opas, VAHTI 11/2006

Henkilöstön tietoturvaohje, VAHTI 10/2006

Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006

Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006

Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006

Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006

Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006

Electronic Mail-handling Instructions for State Government, VAHTI 2/2006

Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005

Valtionhallinnon sähköpostien käsittelyohje, VAHTI 2/2005

Information Security and management by Results, VAHTI 1/2005

Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004

Datasäkerhet och resultatstyrning, VAHTI 4/2004

Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004

Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004

Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006, VAHTI 1/2004

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003

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

Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista, VAHTI 6/2001

Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001

Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001

Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000

Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000

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

5/2008
VAHTI
marraskuu 2008

ISSN 1455-2566
ISBN 978-951-804-894-0 (nid.)
ISBN 978-951-804-884-1 (pdf)