VALTIOVARAINMINISTERIÖ
Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI

Valtion tietoturvallisuuden kehitysohjelman toimeenpano

ROSKAPOSTIN VASTAISET TOIMET-JAOSTON LOPPURAPORTTI

24.5.2006

ESIPUHE

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

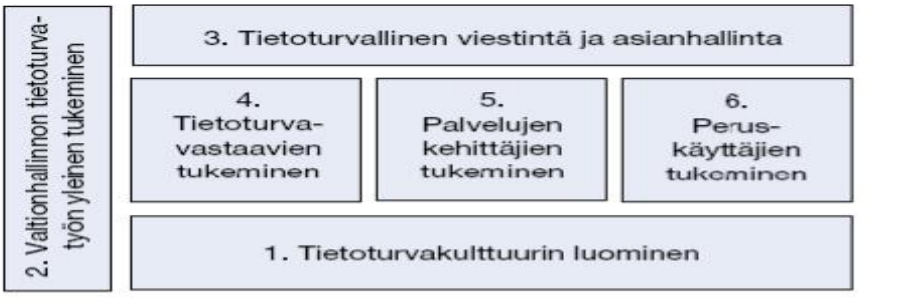
VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi valtionhallinnon kaikkea toimintaa. Valtionhallinnon tietoturvallisuuden johtoryhmä käsittelee valtionhallinnon tietoturvallisuutta koskevat määräykset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset.

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

Valtion tietoturvallisuuden kehitysohjelma on julkaistu VAHTI-julkaisusarjassa nimellä *Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006*, VAHTI 1/2004. Kehitysohjelmalla kehitetään tietoturvallisuutta laajasti osana kaikkea toimintaa. Kehitysohjelmaan sisältyy kaikkiaan 28 laajaa kehittämiskohdetta, joista osaa toimeenpannaan työryhmien tai jaostojen valmistelussa ja osaa muilla toimenpiteillä.

Kehitysohjelmaan osallistuvat laajasti kaikki hallinnonalat ja lisäksi osassa hankkeita on mukana kuntien ja elinkeinoelämän edustajia sekä ulkopuolisia asiantuntijoita. Hankkeissa on vuonna 2005 ollut mukana valtionhallintotasolla nimettyinä noin 300 osallistujaa. Osa kehitysohjelman kehitystyöstä toteutetaan hanketyöllä ja osa muulla ohjaus-, kehitys- ja yhteistyöllä. Virallisesti asetetut hankkeet löytyvät valtioneuvoston hankerekisteristä (http://www.hare.vn.fi/) VAHTIn (VM166:00/2003) alahankkeina. Seuraavassa kuvassa on esitettyinä kehitysohjelman osa-alueet. Tässä

Kaavio kehitysohjelmasta ja eri osa-alueiden hankkeet



Tässä asiakirjassa kuvataan tietoturvallinen viestintä ja asianhallinta- hankealueeseen kuuluvan VAHTIn alaisen roskapostin vastaiset toimet- toiminta ja tulokset.

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

ROSKAPOSTIN VASTAISET TOIMET -JAOSTO, LOPPURAPORTTI

1 Johdanto

1.1 Roskapostista yleisesti

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.

Spämmillä (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 tukkeutuneet. Eräiden arvioiden mukaan jopa 30–50% kaikesta sähköpostiliikenteestä liittyy spämmiin, ja että späm aiheutti lokakuussa 2003 enemmän taloudellista vahinkoa kuin virukset ja hakkerit yhteensä.

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.

1.2 Hankkeen taustatiedot

Tietoturvallisuus on olennainen osa valtionhallinnon toimintaa. Tietoturvallisuudella varmistetaan hallinnon toiminnan luotettavuus ja sujuvuus. VM vastaa valtionhallinnon tietoturvallisuuden yleisestä ohjauksesta ja kehittämisestä. Näissä tehtävissä keskeisenä koordinaatioelimenä ja VM:tä tukevana ryhmänä toimii VM:n asettama ja johtama Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. VAHTI:lla on keskeinen rooli hallinnon tietoturvallisuuden kehittämisessä ja ohjauksessa. Valtiovarainministeriö on käynnistänyt valtionhallinnon tietoturvallisuuden kehitysohjelman (VM:n VAHTI-julkaisu 1/2004, www.vm.fi/vahti) toimeenpanon ministeri Wideroosin kirjeellä 3.3.2004 (VM 7/01/2004). Ohjelma on käsitelty pääministeri Vanhasen johtamassa tietoyhteiskuntaohjelman ministeriryhmässä sekä ministeri Mannisen johtamassa hallinnon ja aluekehityksen ministeriryhmässä. Laajaan ohjelmaan sisältyy 28 kehittämiskohdetta ja tällä päätöksellä asetetun roskapostien vastaiset toimet - jaoston toiminta ja tehtävät ovat tärkeä osa kehitysohjelmaa.

1.3 Hankkeen tavoitteet

Tavoitteena on tehostaa ja yhteen sovittaa hallinnon toimijoiden toimintaa roskapostin vastaisessa toiminnassa sekä kehittää ja edistää roskapostin vastaisen toiminnan hyviä käytäntöjä.

Osatavoitteet:

- Roskapostin hallinnan yleisohjeen laatiminen
- Kansallisen lainsäädäntötyön tukeminen ja toimeenpanon edistäminen
- Kansainvälinen roskapostin vastaiseen toimintaan liittyvä yhteistoiminta
- Roskapostin torjuntaohjelmistojen puitesopimusten valmistelu yhteistyössä kauppatalo Hanselin kanssa
- Yhteistoiminta operaattoreiden ja muiden keskeisten elinkeinoelämän toimijoiden sekä niitä edustavien järjestöjen kanssa

- Valtionhallinnon sähköpostivastaavien verkoston luonti ja yhteistyön kehittäminen
- Roskapostin määrän mittaaminen ja reaaliaikaisen seurannan luominen
- Loppukäyttäjille yksinkertaiset pelisäännöt, miten toimia

2 Hankkeen toteuttaminen

2.1 Organisointi

VM perusti jaoston Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI alaisuuteen ja ohjaukseen. Sen organisointi oli aluksi seuraava:

Puheenjohtaja:

tietojärjestelmäpäällikkö	Kari Keskitalo, kauppa- ja teollisuusministeriö

Varapuheenjohtaja:

projektipäällikkö	Olli-Pekka Rissanen, valtiovarainministeriö

Sihteeri:

avustaja	Rauni Vuorensola, kauppa- ja teollisuusministeriö

Jäsenet:

erityisasiantuntija	Juhani Ahvenainen, Verohallitus
järjestelmäasiantuntija	Jan Elho, liikenne- ja viestintäministeriö
suunnittelija	Rolf Eklund, Suomen ympäristökeskus
järjestelmäasiantuntija	Ville Hagelberg, valtiovarainministeriö
tietohallintopäällikkö	Timo Haurinen, Valtiokonttori
tietoturvapäällikkö	Aku Hilve, Helsingin poliisilaitos
tietohallintopäällikkö	Pekka Kallio, Opetushallitus
tietotekniikka-asiantuntija	Vesa-Matti Kari, Helsingin yliopisto
tietoturva-asiantuntija	Sami Kilkkilä, Viestintävirasto
johtaja	Kaarina Koskinen, Ulkomaalaisvirasto
atk-suunnittelija	Jens Kristianssen, oikeusministeriö
pääsuunnittelija	Jari Lehtonen, Turun yliopisto
asiantuntija	Olavi Manninen, Kuopion yliopisto
ylitarkastaja	Heikki Partanen, Tietosuojavaltuutetun toimisto
tietoturvapäällikkö	Kaisu Rahko, Oulun yliopisto
yli-insinööri	Tapani Tarvainen, Jyväskylän yliopisto
tietotekniikka-asiantuntija	Tuuli Tuominen, Helsingin yliopisto
jaospäällikkö	Christa Winqvist, Helsingin kauppakorkeakoulu

17.6.2004 tietoturvapäällikkö Kaisu Rahko, Oulun yliopisto pyytänyt vapautusta jaoston jäsenyydestä.

4.10.2004 tietotekniikkapäällikkö Seppo Perkiö, EK nimetty jaoston jäseneksi

21.1.2005 järjestelmäsuunnittelija Jyrki Tuohela Kansainvälisen henkilövaihdon keskuksesta (CIMO) ja tietoturvapäällikkö Mats Kommonen Turun yliopistosta nimetty jaoston jäseniksi.

30.3.2005 IT suunnittelija Mikko Pitkänen Oikeusministeriöstä Jens Kristianssenin sijaiseksi työkiireiden takia.

1.8.2005 tietotekniikka-asiantuntija Tuuli Tuominen Helsingin yliopistosta jätti jaoston tehtävät

2.2 Hankkeen aikataulu ja kokoukset

Hankkeen toimikausi oli 7.6.2004 – 30.10.2005.

Kokoukset toimikauden aikana:

1/2004 - 25.8.2004
2/2004 - 21.9.2004 Seminaari Katajanokan kasinolla, jossa perustettiin alatyöryhmät
3/2004 - 23.11.2004
4 (1)/2005 – 20.1.2005
5 (2)/2005 – 17.3.2005
6 (3)/2005 – 19.5.2005
7 (3)/2005 – 18.8.2005
8 (5)/2005 – 27.10.2005

Keskimääräinen kokouksiin osallistumisprosentti oli 59 %.

2.3 Yritysvierailut ja tuote-esittelyt

23.11.2004 Symantec Oy Finland
17.3.2005 SYKE:ssä käytössä olevan roskapostin torjuntaohjelmiston esittely, Rolf Eklund
19.5.2005 Kauppakorkeakoulun roskapostin torjuntaohjelmiston esittely Christa Winqvist
18.8.2005 Deltacon/VNTHY roskapostin torjunta

2.4 Koulutus

Jaosto järjesti halukkaille jäsenilleen yhteistyössä Teleware Oy:n kanssa 16.6.2005 koulutuspäivän aiheena: ”Roskapostilta suojautuminen.” Kurssille osallistui 10 henkilöä.

3. Hankkeen saavutukset

Roskapostin hallinnan yleisohjeen laatiminen
Jaos laati puheenjohtaja Christa Winqvistin johdolla sähköpostin suodatusohjeen, joka julkaistiin VAHTI:n julkaisun Valtionhallinnon sähköpostien käsittelyohjeen (2/2005) liitteessä 1 (ks. liite 1).

Kansallisen lainsäädäntötyön tukeminen ja toimeenpanon edistäminen
Jaos oli aktiivisesti yhteydessä LVM:n virkamiehiin, joiden kautta päästiin vaikuttamaan osittain kansalliseen lainsäädäntötyöhön, jaoksen tavoitteiden mukaisesti. Puheenjohtajana tässä työssä toimi Christa Winqvist (ks. liite 2).

Kansainvälinen roskapostin vastaiseen toimintaan liittyvä yhteistoiminta
Jaoksen jäsenistä Juhani Ahvenainen osallistui OECD:n roskapostinvastaisen toiminnan kokoukseen 8.-9.9.2004 Buranissa Koreassa ja Kari Keskitalo 22.10.2004 Pariisissa. OECD:n Work on Spam sivusto löytyy osoitteesta www.oecd.org/sti/spam.

Alatyöryhmässä, jonka puheenjohtajana toimi Tapani Tarvainen tutkittiin myös laajasti kansainvälisten roskapostiaiheisten linkkien käyttökelpoisuutta (liite 3).

Roskapostin torjuntaohjelmistojen puitesopimusten valmistelu yhteistyössä kauppatalo Hanselin kanssa
Jaos on antanut Hanselille teknistä asiantuntemustaan valtionhallinnon laajuisen puitesopimuksen laatimiseksi. Ryhmän vetäjä Ville Hagelberg jatkaa työtään vielä työryhmänsä kanssa jaoksen toiminnan loputtuakin, kunnes puitesopimus gateway-tason haittaohjelmien torjuntaohjelmista saadaan aikaiseksi.

Yhteistoiminta operaattoreiden ja muiden keskeisten elinkeinoelämän toimijoiden sekä niitä edustavien järjestöjen kanssa
Työryhmä on kokonaisuudessaan jaoksen toiminnan aikana verkostoitunut keskenään sekä lukuisten muiden organisaatioiden edustajien kanssa erilaisissa tilaisuuksissa. Tämä on osaltaan edesauttanut roskapostivastaisen kulttuurin edistämistä.

Valtionhallinnon sähköpostivastaavien verkoston luonti ja yhteistyön kehittäminen
Työryhmä, vetäjänään Vesa-Matti Kari laati sähköpostivastaaville postituslistan, jonka avulla sähköpostin ylläpitotehtävissä työskentelevät voivat jakaa kokemuksiaan ja hyviä käytänteitään (ks. liite 4).

Roskapostin määrän mittaaminen ja reaaliaikaisen seurannan luominen
Olavi Manninen oli tämän alatyöryhmän puheenjohtaja. Ryhmä kehitti mittausmenetelmät, joilla kyetään esittämään organisaatioiden roskapostin määrät yhteismitallisina vertailukelpoisina graafisina esityksinä (liite 5). Tätä työtä jatketaan vielä jaoksen työn päätyttyäkin ja siitä tullaan laatimaan erillinen muistio valtionhallinnon organisaatiolle.

Loppukäyttäjille yksinkertaiset pelisäännöt miten toimia

Jaos laati loppukäyttäjän ohjeet, jotka VAHTI hyväksyi omassa kokouksessaan. Huoneentaulusta on vielä tarkoitus tehdä myöhemmin VAHTI-hiirimatto, joka osaltaan edesauttaa roskapostin vähentämistä käyttäjien postilaatikoissa (liite 6).

LIITE 1

Liite 1 Roskapostin hallinnan yleisohjeen laatiminen – loppuraportti

Työryhmän tehtävä

Alatyöryhmän 6 alkuperäinen tehtävä ”Roskapostin hallinnan yleisohjeen laatiminen” rajattiin alatyöryhmän kohdalla kattamaan valtionhallinnon sähköpostiylläpitäjien suodatusohje. Työryhmän tehtävänä oli tuottaa tekninen yleisohje valtionhallinnon sähköpostin suodatukseen.

Työryhmän jäsenet

Christa Winqvist, Helsingin kauppakorkeakoulu, puheenjohtaja
Juhani Ahvenainen, Verohallitus
Jan Elho, LVM
Timo Haurinen, Valtiokonttori
Aku Hilve, Helsingin poliisilaitos
Vesa-Matti Kari, Helsingin yliopisto
Jari Lehtonen, Turun yliopisto
Olavi Manninen, Kuopion yliopisto
Tapani Tarvainen, Jyväskylän yliopisto
Tuuli Tuominen, Helsingin yliopisto

Työryhmän työskentely

Työryhmä kokoontui kolme kertaa työskentelynsä aikana. Laaditun yleisohjeen pohjana käytettiin Suomen yliopistojen UCIRT–työryhmän laatimaa suodatusohjetta, jota työstettiin myös sähköpostin välityksellä ryhmän keskuudessa.

Suodatusohje

Työryhmän tuottama sähköpostin suodatuksen yleisohje integroitiin VAHTI:n ”Valtionhallinnon sähköpostien käsittelyohje” ohjeeseen (2/2005), liitteeksi 1.

Liite 2 Sähköpostin suodatusohje

Tässä ohjeessa täsmennetään, miten sähköpostiviestejä organisaatiossa suodatetaan. Suodatuksen tulee aina tapahtua ohjelmallisesti ja viestintäsalaisuuden säilyttäen. Tämä ohje on julkinen ja sen tulee olla julkisesti saatavilla. Suodatetut viestit voidaan tapauskohtaisesti jättää välittämättä (kohdat 1-7), tuhota (kohta 9), eristää erilliselle karanteenialueelle määräajaksi, jonka jälkeen ne voidaan tuhota (kohdat 8-11), tai välittää vastaanottajalle roskapostiksi merkittynä (kohta 11). Haittaohjelmat tulee poistaa välitettävistä viesteistä. Suodatetuista viesteistä lähettäjälle tai lähettävälle postipalvelimelle ja/tai vastaanottajalle lähetettävien virheilmoitusten tulee olla RFC 2821 -standardin mukaisia. Virheilmoitukseen voidaan myös liittää käyttäjäystävällinen kuvaus virheestä silloin kuin se on mahdollista.

Suodatusmenetelmät

1. Third party open relay -esto, eli releointihyökkäysten esto organisaation koneiden kautta.
Organisaation ei välitä ulospäin sellaisia viestejä, jotka eivät ole lähtöisin organisaation osoiteavaruudesta ja joiden vastaanottajan osoite ei ole organisaation sähköpostiosoite. Lisäksi organisaatio estää palomuurin konfiguraatiossaan SMTP-yhteydet muihin kuin pääasiallisiin postipalvelimiinsa internetistä käsin.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: *”550 Relaying denied”*

2. Postin välitys tuntemattomista toimialueista tai koneista
Organisaation postipalvelin tekee nimipalvelutarkastuksen lähettäjätoimialueen tai –koneen olemassaolon varmistamiseksi. Mikäli lähettävä toimialue tai kone ei selviä nimipalvelukyselystä, voidaan postitus estää tilapäisesti kunnes lähettävän koneen tai toimialueen nimipalvelutietueet ovat kunnossa.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: ”451 *Sender domain must resolve”*

3. Mustat listat (Black Lists)
Organisaatio ei välitä postia sellaisista postikoneista, joita voidaan käyttää releointihyökkäyksiin (ks. kohta 1). Organisaatio saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja. Esimerkkejä:

MAPS (Mail Abuse Prevention System)
ORDB (Open Relay DataBase)
DSBL (Distributed Server Boycott List)
SPAMHAUS (The Spamhaus Project)

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: *”550 Mail from <lähettäjä> rejected as spam; see http://www.käytettävä_musta_lista.domain”*

4. Postin välitys sellaisista postikoneista, joiden kautta tunnetusti lähetetään roskapostia
Organisaatio ei välitä postia sellaisista koneista, joiden kautta tunnetusti lähetetään roskapostia tai joita ylläpitävä organisaatio tunnetusti tukee roskapostittajia. Tähän organisaatio saa käyttää apunaan kansainvälisten, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja. Esimerkiksi NJABL-tietokanta (Not Just Another Bogus List).

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: *”550 Mail from <lähettäjä> rejected as spam; see http://www.njabl.org”*

5. Postin välitys sellaisista koneista, joilla on dynaamisesti varattu verkko-osoite
Organisaatiolla on oikeus olla välittämättä postia sellaisista koneista, joiden verkko-osoite kuuluu dynaamisesti varattaviin osoiteavaruuksiin. Organisaatio saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja, esimerkiksi NJABL Dynablock.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: *”550 Mail from <lähettäjä> rejected as spam; see http://www.njabl.org/dynablock.html”.*

Kohdissa 3, 4 ja 5 organisaatio saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja. Tietokantoja käytettäessä tulee varmistua niiden asianmukaisuudesta mm. tarkastamalla periaatteet, joilla osoitteita kantaan lisätään. Tietokantoja ylläpitävän palveluntarjoajan on tarjottava helppokäyttöinen mekanismi, jolla osoitteita voi pyytää poistettavaksi kannasta. Poistopyynnöt on käsiteltävä kohtuullisen ajan kuluessa niiden tekemisestä. Tietokantoja käytettäessä tarkastus voi olla reaaliaikainen tai organisaatio voi ylläpitää omaa kopiotaan tietokannoista, jota kuitenkin tulee päivittää kohtuullisin väliajoin.

6. Palvelinkohtainen pääsylista
Organisaatio käyttää tarvittaessa haittapostin torjumiseen itse ylläpitämiään palvelinkohtaisia pääsylistoja (access list). Listan avulla voidaan sulkea tilapäisesti tai pysyvästi erillisiä toimialueita, lähettäjiä, vastaanottajia, yksittäisiä verkko-osoitteita tai kokonaisia aliverkkoja, mikäli se on muun liikenteen turvaamiseksi välttämätöntä.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: *”550 Mail from <lähettäjä> rejected as spam” tai ”550 Access Denied”*

7. Liikennemääriin perustuva suodatus
Liikenneanalyysisuodatuksessa voidaan esimerkiksi sähköpostipalvelimen lokeja reaaliaikaisesti tarkkailemalla huomata poikkeamat normaalissa postinkulussa. Tällaisia roskapostitukseen viittaavia poikkeamia voivat olla epätavallisen pitkät yhteysajat postipalvelimeen, poikkeuksellinen määrä viestejä samasta isännästä tai suuri määrä vastaanottajia samassa viestissä. Liikennemääriä voi kontrolloida myös proaktiivisesti esimerkiksi hidastamalla yhteysnopeuksia tai rajoittamalla yhteysaikaa. Rajoituksia tulee kuitenkin aina käyttää harkiten, jotta esimerkiksi sähköpostilistojen toiminta ei häiriytyisi.

8. Viestien koko ja liitetiedostojen määrä
Organisaatiolla on oikeus rajoittaa välittämiensä viestien kokoa ja niiden mahdollisesti sisältämien liitetiedostojen määrää. Tiedon viestin kokoon ja liitetiedostojen määrään liittyvistä rajoituksista tulee olla julkisesti saatavilla.

9. Haittaohjelmien poistaminen
Organisaatio poistaa välittämistään viesteistä haittaohjelmat mahdollisuuksiensa mukaan tai tarpeen vaatiessa tuhoaa koko haittaohjelman sisältävän viestin.

10. Liitetiedostojen tiedostotyypit
Organisaatiolla on oikeus olla vastaanottamatta / välittämättä riskialttiita, haittaohjelmien kuljetukseen tyypillisesti käytettäviä tiedostotyyppejä sisältäviä viestejä. Esimerkkejä tiedostotyypeistä:

*.ade, *.adp, *.bas, *.bat, *.chm, *.cmd, *.com, *.cpl, *.crt, *.dll, *.exe, *.hlp, *.hta,
*.inf, *.ins, *.isp, *.js, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.ocx, *.pcd,
*.pif, *.reg, *.scr, *.sct, *.shs, *.url, *.vb, *.vbe, *.vbs, *.wsc, *.wsf, *.wsh

Ajantasainen lista tiedostotyypeistä, joita organisaation postipalvelin ei vastaanota / välitä, tulee aina olla julkisesti saatavilla. Välittämättä jätettävät tiedostot on eristettävä määräajaksi karanteenialueelle ja ne on saatettava vastaanottajan tai lähettäjän tietoon ennen niiden tuhoamista. Tiedosto voidaan toimittaa vastaanottajalle tämän sitä pyytäessä, edellyttäen että tiedosto ei sisällä esim. haitalliseksi katsottua koodia.

11. Sähköpostin sisältöön perustuva suodatus
Organisaatio voi suodattaa roskapostia ohjelmallisesti sisällölliseen automaattiseen analyysiin perustuen, esimerkiksi pisteytykseen perustuvilla suodatusohjelmilla (Spam Assassin, IMF). Sisällöllisessä analyysissa roskapostiksi luokiteltu viesti tulee aina merkitä roskapostiksi ja toimittaa vastaanottajan sähköpostilaatikkoon, suodattaa erilliselle karanteenialueelle, josta se on vastaanottajan luettavissa tai muutoin saattaa vastaanottajan tietoon kohtuullisen ajan kuluessa viestin vastaanottamisesta.

12. Viivästäminen
Organisaatiolla on oikeus tarvittaessa viivästää viestien toimittamista kohtuullisen ajan tunnistaakseen mahdolliset liikenteen mukana tulevat haittaohjelmat.

13. Muuta
Organisaation tulee palomuurin konfiguraatiossaan tai muutoin, mahdollisuuksiensa mukaan, estää sähköpostin lähettäminen muihin toimialueisiin muiden kuin virallisten postipalvelimiensa kautta. Postin suodatusta on mahdollista tehdä sähköpostiasiakkaaseen asennettavassa lisäohjelmassa, keskitetyssä suodatuspalvelimessa tai yhdyskäytävässä. Suodatusohjeen kohdat 1–8 suositellaan tehtäväksi jo sähköpostiyhdyskäytävässä, kohta 9 keskitetyssä suodatuspalvelimessa ja asiakkaassa, kohta 10 keskitetyssä suodatuspalvelimessa sekä kohta 11 keskitetyssä suodatuspalvelimessa ja / tai asiakkaassa.

Suodatussuosituksen tekohetkellä ei-suositeltaviksi suodatusmenetelmiksi katsottiin sellaiset menetelmät, jotka olennaisesti rajoittavat sähköposti-arkkitehtuurin luontaista avoimuutta, esim. challenge/response, graylisting tai jotka ovat vielä toistaiseksi kokeellisessa käytössä, esim. RMX, SPF, DMP. Edellisten käyttö on hyväksyttävää arviointimielessä, mutta niitä ei tulisi käyttää pääasiallisina suodatusmenetelminä. Sähköpostipalvelua tarjoavan organisaation tulee huolehtia siitä, että sähköpostitoimialueen ylläpitoon liittyvät sähköpostiosoitteet ovat olemassa ja että ne ohjautuvat oikealle taholle. Tällaisia osoitteita ovat mm. postmaster@toimialue.fi ja abuse@toimialue.fi. Tiedon organisaation käyttämistä suodatusmenetelmistä tulee aina olla julkisesti saatavilla.

Liite 3 Kansallisen lainsäädäntötyön tukeminen ja toimeenpanon edistäminen – loppuraportti

Työryhmän tehtävä

Alatyöryhmän 7 (KLT) tehtäväksi rajautui ensimmäisessä kokouksessa sähköisen viestinnän tietosuojalain (516/2004) ongelmakohtien tunnistaminen ja analysoiminen.

Työryhmän jäsenet

Christa Winqvist Helsingin kauppakorkeakoulu, puheenjohtaja
Aku Hilve Helsingin poliisilaitos
Mats Kommonen Turun yliopisto
Kaarina Koskinen Ulkomaalaisvirasto
Jens Kristiansen Opetusministeriö
Seppo Perkiö Elinkeinoelämän Keskusliitto
Tapani Tarvainen Jyväskylän yliopisto

Työryhmän työskentely

Työryhmä kokoontui neljä kertaa työskentelynsä aikana sekä kommunikoi aiheeseen liittyen sähköpostin välityksellä. Ryhmän edustajat (Kari Keskitalo, Mats Kommonen, Jens Kristiansen, Christa Winqvist) tapasivat Juhapekka Ristolan 3.6.2005 liikenne- ja viestintäministeriössä. Tapaamisessa keskusteltiin keskeisimmistä ryhmän havaitsemista ongelmakohdista sähköisen viestinnän tietosuojalain ja roskapostin suodatuksen osalta. Mats Kommonen lähetti Juhapekka Ristolalle oheisen muistion aiheeseen liittyen 8.6.2005.

Asia: Ehdotuksia sähköisen viestinnän tietosuojalain tiimoilta

Ehdotusten keskeiset tavoitteet

- Sähköpostin välitystoiminnassa yleisesti käytettävien menettelyjen laillisuuden varmistaminen
- Yhteisötilaajan ja käyttäjän oikeuksien tasapainon kehittäminen kumpaakaan heikentämättä
- Automaattisen sisältöanalyysin ja sähköpostinvälityksen laadunvalvonnan nimenomainen salliminen viestinnän osapuolien oikeuksia loukkaamatta.

Tuon samalla esille sähköpostiviestintään ja toisaalta myöskin yhteisötilaajan asemaan liittyviä muita huomioita, jotka tukevat alussa esitettyjä tavoitteita. Pykälään 20 ehdotetut muutokset ovat erityisesti sähköpostiviestintään liittyviä, mutta muut ehdotetut muutokset tukevat sitä oleellisesti ja ne kannattaisi ottaa prosessiin mukaan. (Hakasulkeissa [] olevat termit tarvitsevat mahdollisesti muuntoa lakikieleen paremmin sopiviksi.)

2§ 5 kohta: "*verkkopalvelulla viestintäverkon tarjoamista käytettäväksi viestien siirtoon, jakeluun tai tarjolla pitoon; ” ja 6 kohta: ”viestintäpalvelulla viestien siirtämistä, jakelemista tai tarjolla pitämistä viestintäverkossa;*".

Nykyinen 5 ja 6k käytännössä kuvailevat 'yleistä verkkopalvelua ja yleistä viestintäpalvelua', joiden erotteleminen omaksi ryhmäkseen ei liene tarpeellista lain nykysisällön kannalta, koska yleinen viestintäverkko on jo määritelty. Termin on parempi kuvailla kaikkea viestintäpalvelua, koska sekä teleyritysten että muiden harjoittamat viestintäpalvelut tarvitsevat yhtäläistä suojaa ja velvoitteita. Esimerkiksi palaverihuoneessa vierailijalle annettava langaton verkko-

yhteys on verkkopalvelun tarjoamista, mutta vain rajatulle käyttäjäjoukolle. On päätettävä kuuluuko se lain soveltamisalaan ja jos, niin miltä osin. Soveltamisalaa ei kannata rajata vielä määritelmissä, vaan vasta pykälässä 3.

3.2§: Soveltamisalan rajaus jättää nykyisellään tulkinnanvaraa. Tavoiteltu uusi rajaus olisi jotakin tämänkaltaista: "*Tätä lakia ei sovelleta sisäisiin ja muihin rajoitetuille käyttäjäpiireille tarkoitettuihin viestintäverkkoihin muiden kuin yleiseen viestintäverkkoon yhteydessä olevien viestintäpalvelujen osalta.*" Tällöin esimerkiksi yhteisötilaajan verkossa olevat taloushallinnolliset järjestelmät kuuluvat vain 4§ ja 5§ osalta lain piiriin, mutta samassa verkossa toteutettavat Internetiin kytkeytyvät viestintäpalvelut kuuluvat soveltamisalaan. Käytännössä samassa verkossa liikkuu yleensä aina sekä sisäistä että Internet-liikennettä.

19§: Korjausehdotus alkuun: "*[Kaikkien] on huolehdittava tarjoamiensa palvelujen tietoturvasta.*" Huolehtimisvelvoitetta ei kannata rajata vain tiettyihin toimijoihin, tämän pitäisi olla jokeripykälä samaan tapaan kuin 4§ ja 5§. **Vaihtoehtoinen** (ehkä parempi) **muotoilu:** "*Verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun tarjoajan on huolehdittava palvelujensa sekä harjoittamiensa tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta. Palvelun ja käsittelyn ...*" Onko jokin tietty syy nykyiseen muotoiluun? Teleyrityksethän (ja kaikki muutkin toimijat) käsittelevät tunnistamis- ja paikkatietoja siinä missä yhteisötilaajatkin. Kun 2§:n palvelumääritelmät on päivitetty, tämä muotoilu kattaa kaikki palvelut ja toimijat, niin kuin pitääkin.

20§: Yleisenä huomiona, pykälän velvoitteet tähtäävät ainoastaan siihen, että käyttäjän viestintä pysyy häiriöttömänä. Toivomus olisi, että tässä pykälässä huomioitaisiin myös yhteisötilaajan tarve huolehtia palvelujensa tasapuolisesta ja häiriöttömästä toiminnasta yhteisötilaajan oman toiminnan turvaamiseksi, ei ainoastaan siihen kuuluvien käyttäjien henkilökohtaisten oikeuksien turvaamiseksi. Tällä hetkellä tämä oikeus on käytännössä turvattu sallimalla viestintä- tai verkkopalvelun turvaaminen (edellyttäen, että yhteisötilaaja laajennetaan 2§:ssä näiden palvelujen tuottajaksi kuten yllä on ehdotettu), mutta ei olisi pahitteeksi että lain tasolla yhteisötilaajan oikeutettu oma etu olisi vähintään todettuna (kuten tietosuojadirektiivissä on). Useimmat yhteisötilaajat ovat tarkoittaneet viestintäpalvelut nimenomaan omaksi hyväkseen, ja toissijaisesti käyttäjien hyväksi. Käyttäjät saavat sen yleensä sivutuotteena tai työ- tai virkaoikeudellisen vastuun myötä ja heidän ensisijainen lojaliteettivelvoitteensa on työnantajaa kohtaan. Asia tulee huomioiduksi jos ehdotetut 2§:n muutokset tehdään, muussa tapauksessa (yhteisö)tilaajan oikeutettu etu täytyy lisätä esim. 20.4§:ään.

20.1§: lisätään uusi kohta 3: "*rajoittamalla viestintäverkon tai viestintäpalvelun käytön määrää tai siinä käytettäviä yhteystapoja;*". Vaihtoehtoisesti voi arvioida, kattaako 1-kohtaan lisättävä "estämällä *tai rajoittamalla*" saman tarpeen. Tällä tarkoitetaan esimerkiksi tilannetta, jossa jokin yhteydenottotapa (vaikkapa POP-protokolla tai jokin varmennus-/tunnistuskäytäntö) osoittautuu vaarallisen heikkouden sisältäväksi ja sen käyttö on estettävä varsinaiseen viestien välittämiseen sen kummemmin puuttumatta. Toisekseen se tarkoittaa tilannetta, jossa jonkin liikennöintitavan määrällinen tai laadullinen kasvaminen uhkaa estää muita liikennöintitapoja. Kolmanneksi, tavoitteena on sallia esim. kiintiöiden tiukentaminen tilanteessa, jossa vaikkapa levytilaa on käytettävissä normaalia vähemmän. Tällaiset rajoitukset voidaan joutua tekemään tilanteessa, jossa siitä ei voida "sopia" käyttäjän kanssa aikataulusyistä etukäteen, ja siksi siitä pitää olla ennakkovaroitus laissa. Välttämättömyysvaatimus ja ViVi/TSV-valvonta turvannevat pykälän asiatonta käyttöä vastaan.

20§ uusi momentti: "*Viestintäpalvelussa välitettäväksi otetuille viesteille saa suorittaa automaattisen analyysin sen tarkastamiseksi, onko viesti rakenteellisesti [viestintätapaa koskevien välitysstandardien mukainen], sisältääkö viesti [3 momentissa tarkoitetun haittaohjelman] tai onko se roskapostia. Tarkastamisesta ja sen tuloksesta on lisättävä merkintä viestin otsikkotietoihin, jos se on mahdollista. Sisältöön perustuvasta analyysista ei saa jäädä palvelimen lokeihin merkintöjä, jotka paljastavat viestin luottamukselliseksi tarkoitetun sisällön, ellei [8–14§:sta] muuta johdu. "* Tälle momentille paras paikka olisi ehkä nykyisen 2 ja 3 momenttien väliin. Huom. Kyseinen momentti sisältää oikeuden sekä sähköpostin tarkastamiseen viruksien, roskapostin ja "rikkinäisyyden" havaitsemiseksi (varsinaisiin esto- ja poistotoimiin tulee mandaatti 20.1-3§:ssa ja 29§:ssä), että muun verkkoliikenteen automaattiseen analysointiin (esim. www-välityspalvelimiin oikeus etsiä ja poistaa haittaohjelmat www-selailusta). Molemmat ovat kaikkien toimijoiden turvallisuuden kannalta tarpeellisia. Huom2: ehdotuksessa oleva " *ellei [8–14§:sta] muuta johdu."* ei välttämättä riitä sellaisenaan, koska hyväksyttävän toiminnan osana IDS-järjestelmät ("Intrusion Detection System") yleensä tallentavat näytteen epäilyttävästä liikenteestä jatkoanalyysia varten. Tällöin ei siis tallenneta tunnistamistietoja 9-14§:n mukaisesti, vaan koko viesti tai merkittävä osa siitä. Silloin ei kuitenkaan ole yleensä kyse mistään ihmisten välisestä kommunikoinnista, vaan palvelimien ohjauskäskyistä ja muusta vastaavasta liikenteestä. Ne kuitenkin voivat olla myös käyttäjän tarkoituksellisesti liikkeelle saattamaa viestintää, jonka pitäisi nauttia lain suojaa. Tässä on edelleen ongelmana "viestin" ja "sisällön" määrittelyn monimerkityksellisyys. Tässä pykälässä (tai 13§) pitäisi myös sallia liikennevirran tallentaminen mahdollista väärinkäytöksen selvittämistä varten. Pelkkä tunnistamistietojen käsittely ei riitä, koska uhka piilee itse viestissä, ei sen tunnistamistiedoissa. Mandaatin käyttöä pitäisi tietty kontrolloida ennalta ja tarkoitussidonnaisuuden tulee olla hyvin määritelty, emmehän halua että liikennettä täysin mielivaltaisesti tallennellaan. Lisäksi kannattaa harkita, pitääkö tässä yhteydessä erotella tallentaminen ja muu käsittely siten, että väliaikaiseen tallentamiseen on oikeus kevyemmin perusteluin, muuhun käsittelyyn vaaditaan jo vahvempi epäilys.

20.3§ muutetaan: "*[Viestin tai sen osan] saa poistaa, jos on todennäköisiä syitä epäillä viestin sisältävän sellaisen tietokoneohjelman tai ohjelmakäskyjen sarjan, jota tarkoitetaan rikoslain (39/1889) 34 luvun 9 a §:n 1 kohdassa tai jos on todennäköisiä syitä epäillä, että viestiä käytetään rikoslain 38 luvun 5 §:ssä [tarkoitettuun] tietoliikenteen häirintään. Viestin tai sen osan poistamiseen johtavasta toimenpiteestä on jäätävä lokiin merkintä, josta käy ilmi poistamisen syy."* Voi olla harkitsemisen arvoista miettiä, pitääkö em. lisäykseen lisätä toiseksi viimeiseksi virkkeeksi vielä: "*Jos viesti sisältää [merkityksellisiä] osia, jotka voidaan välittää vastaanottajalle [em. toimenpiteen jälkeen], viestiä ei saa poistaa kokonaan."*

29§: Kannattaa tehdä pesäero 26–28§:n tarkoittaman _laillisen_ suoramarkkinoinnin ja selkeän "roskapostin" välillä. Roskaposti on yleensä automaattisesti lähetettyä Suomen lainsäädännöstä piittaamatonta "kohinaa", jonka määrä rasittaa postipalvelimia kohtuuttomasti, muttei kuitenkaan 20§:n "välttämättömyys-kynnystä" ylittävästi. Koska roskapostin aiheuttamat kustannukset nousevat vääjäämättä, pitää oikeusperiaatteeksi ottaa se, että maksaja päättää. Tämä on tilaajan oikeutettu etu (tietosuojadirektiivin artikla 13.5). **Uusi momentti** tai uusi virke nykyisen perään: "*Tilaajalla on oikeus estää roskapostin vastaanottaminen.*" Roskaposti voitaneen jättää joko yleiskielisesti ymmärrettäväksi sanaksi tai tarvittaessa viestintäviraston määriteltäväksi. Jos se on määriteltävä suoraan tässä laissa, määritelmän muotoilemisesta tulee äärimmäisen vaikeaa ja virheherkkää.

Muita huomioita ja perusteluja

On huomattava, että teleyrityksille ja yhteisötilaajille on edelleen perusteltua säätää eritasoisia velvoitteita esim. tunnistetietojen käsittelyssä. Tämä sillä perusteella, että teleyrityksen perusliiketoimintaan kuuluu yksityisen viestinnän välittäminen (ainakin kuluttajamarkkinoilla),
- teleyritys ei missään olosuhteissa ole viestinnän osapuoli viestejä välittävän roolinsa perusteella, vaan ainoastaan silloin, jos teleyritys on tarkoituksellisesti viestinnän nimenomainen osapuoli (yhteisötilaaja taasen useimmiten on määrätyissä olosuhteissa, vrt. perustuslakivaliokunta TETSL-asiassa),
- käyttäjällä on lähes poikkeuksetta mahdollisuus harjoittaa yksityistä viestintäänsä muun kuin yhteisötilaajan kautta (kääntyä siis tilaajana teleyrityksen puoleen),
- teleyrityksellä ei ole taloudellista perustetta rajoittaa tilaajan/käyttäjän viestintää muulla kuin 19-20§:n perusteella, koska viestinnästä aiheutuvat kustannukset se voi siirtää tilaajan maksettavaksi (tai niin sen ainakin kuuluisi tehdä). Yhteisötilaajalle on annettava mahdollisuus järjestellä sen ja käyttäjän välisiä oikeuksia sitovin määräyksin/sopimuksin (ja näille on oltava nimenomainen lupa laissa), jotta sillä on mahdollisuus turvata resurssiensa käyttö siihen viestintään, jota varten järjestelmä on tarkoitettu. Näiden valtuuksien käyttöä pitää luonnollisesti voida arvioida ja valvoa. Niiden on oltava julkisia ja/tai TSV:n suorassa valvonnassa.
Tätä asiaa ei ole vielä näissä ehdotuksissa käsitelty, mutta asia on tarpeellinen ja kiireellinen. Esim. työnantajan ja työntekijän suhdetta on käsitelty TETSL:ssa, lasten ja holhoojan suhteesta on oma lainsäädäntönsä, mutta muiden (yhteisö)tilaajien ja käyttäjän suhteesta ei ole säädelty mitään. "Harmaalla vyöhykkeellä" on oppilaitoksia, yhdistyksiä, osuuskuntia, asunto-osakeyhtiöitä ynnä muita vastaavia yhteisöjä. Koska erilaisia toimijoita on niin paljon, heitä koskeva SVTS-säännös pitäisi ottaa tähän yleislakiin muun kaikkia säätelevän lain puuttuessa. Lain lähtökohtana ei voi olla, että vain käyttäjällä on oikeuksia. Koska perusoikeuksiin puuttumisesta on oltava nimenomainen säädös laissa, ei tilaajan ja käyttäjän välistä sopimusta voi mitenkään laillisin keinoin valvoa, ellei siihen anneta tässä laissa lupaa.

Liikenteen automaattinen analysointi (mm.) vertaisverkkoliikenteen, haittaohjelmaliikenteen sekä verkkoa ylenmäärin kuormittavan liikenteen havaitsemiseksi ja rajoittamiseksi on sallittava nimenomaisesti jossain. Kyse ei ole vain tunnistamistietojen analysoinnista, vaan itse liikennevirtojen analysoinnista muun kuin niiden _merkityssisällön_ perusteella, mutta tarkemmin kuin vain 'tunnistamistietojen' perusteella. On päätettävä, kuuluuko tämä verkkopalvelu- vai viestintäpalvelukäsitteen alaisuuteen, ja huomattava että sekä teleyrityksellä että yhteisötilaajalla voi olla yhtäläinen tarve moiseen toimintoon. Jos kyse on verkkopalvelusta, on verkkopalvelun määritelmää laajennettava samaan tapaan kuin viestintäpalvelun määritelmää (aiempana dokumentissa).

Lopuksi vielä huomio luvusta 3: Viestien käsittely (ei siis pelkkien tunnistamistietojen käsittely) lienee itsestään selvästi osa viestintäpalvelun toteuttamista? Pykälät 9–14 käsittelevät vain tunnistamistietojen, ei itse viestin käsittelyä, mutta 8.2§ sisältänee viestien käsittelyvaltuutuksen osana käyttäjän ja tilaajan välistä sopimusta tai suostumusta? Asia voisi tietysti olla hyvä varmistaa vielä erillisellä maininnalla, mutta sen lisääminen sopiviin kohtiin on oman miettimisensä paikka.

Liite 4 Anti-Spam sivustoja

www.roskapostipaketti.fi LVM:n laatima laadukas kotimainen roskapostisivusto
www.oecd.org/sti/spam (OECD:n Work on Spam –sivusto)
www.irtf.org/charters/asrg.html (Internet Research Task Force - Anti-Spam Research Group)
www.cauce.org/ (Campaign against Unsolicited Commercial E-mail)
www.euro.cauce.org/ (Euro CAUCE)
www.spamcon.org/
* Englanninkielinen monipuolinen sivusto
* Tietoa loppukäyttäjille, markkinoijille, pääkäyttäjille, lakiasioissa
* Uutisia etusivulla liittyen aiheeseen
* Mielestäni ihan ok!
http://www.mail-abuse.com/
* MAPS lienee kaikille tuttu?
* Englanninkielinen
* Kelkea ostanut MAPS-palvelut http://www.kelkea.com/services/index.html
* Mielestäni ihan ok!
http://spam.abuse.net/
* Alla oleva just about says it all:
"Our aim with spam.abuse.net is to provide the best collection of anti-spam links and resources to be found anywhere on the Internet." ja "Who are we? We're Internetters with a collective century-plus of experience in the online world."
* Semi-amatöörimäinen
* Ihan ok ...
www.spamrecycle.com/
* englanninkielinen
* kaupallinen (takana firma nimeltä Mailport25)
* teknistä informaatiota, eri tekniikoiden vertailua yms
* mainostaa spammivapaita sähköposteja, kaupallisia suodatinohjelmia jne.
* tarjolla sähköinen Newsletter ("of course no spam")
* USA-keskeinen (mm. kaikkien osavaltioiden anti-spam lait koottuna)
* aktiivisuutta vaikea selvittää kun päiväyksiä ei löydy
www.nanae.org:
* NANAE, n.a.n-a.e., news.admin.net-abuse.email
* nyyssiryhmän webisivu, jolla linkkejä FAQ:hun, blokkilistoihin yms.
www.spamsites.org
* englanninkielinen sivu, joka mainostaa heti alussa, että sitä ei
päivitetä usein, projekti melko jäissä
www.spamhaus.org
* kaupallinen
* englanninkielinen
* infoa sekä pää- että loppukäyttäjille
www.fmp.com/spam_patrol
* harrastelijamaisen näköinen sivusto
* sivulla uutisia vuodelta 2000
* USA-keskeinen
* vanhoja linkkejä
www.natsma.com
* national spam mail abuse association
* uutisia viime kesältä
* tarkoituksena jäljittää spämmien lähtöpisteitä
* rikkinäisiä linkkejä, ei taida olla erityisen toiminnassa

http://sims.net/massacre/
www.gssnet.com/antispam/spam_index.htm
www.stop-spam.org/
www.caspam.org/
www.ripe.net/ripe/wg/anti-spam/
www.cauce.org/orgmember/org_list.shtml
www.caube.org.au/ (CAUCE Australia)
http://cauce.ca/ (CAUCE Canada) (was http://cauce-canada.org/)
http://india.cauce.org/ (CAUCE India)
www.spambr.org/ (Brazilian Spam Fighters)
* portugalinkielinen
* kansalaisjärjestö
* ohjeita käyttäjille, postmastereille yms. sekä teknisiä että juridisia
* ilmeisesti ei kovin aktiivinen, tuoreimmat tiedot v. 2003
www.antispam.ru/ (Russian anti-spam site)
* venäjänkielinen
www.aui.es/contraelspam/ (Spanish Association of Internet Users)
* espanjankielinen
* kansalaisjärjestö
* ei kovin aktiivinen mutta kuitenkin selvästi toimii,
uutissivulla tuoreimmat uutiset joulukuulta,
tilastot vanhoja (2002)
* ohjeita käyttäjille, web- ja postmastereille, ISP:lle jne
* "PePi-II" -projekti spammin kitkemiseksi
www.fabel.dk/ (Danish site)
* tanskankielinen
* 'vastuullisen email-käytön yhdistys'
www.spam.org.tr/ (Turkish anti-spam site)
* ilmeisesti lopettanut toimintansa (ainakaan www-sivu ei toimi)
www.antispam-argentina.8m.net/ (Argentine anti-spam site)
* espanjankielinen (hieman englantia seassa)
* kansalaisjärjestö
* ilmeisesti yrittää ylläpitää omaa mustaa listaa
* aktiivisuudesta vaikea saada selvää, ainakin tilastot ja
päivätyt tiedotteet ovat vanhoja, mutta päiväyksiä on vähän
www.spamstop.net/ (Japanese)
www.cauce.nl/ (Dutch)
www.ihatespam.biz/ (Korean)
* ei tietoa ylläpitäjästä, epämääräisen ja tyhjän tuntuinen
* englanninkielinen
www.iajapan.org/hotline/ (Japanese)
* japaninkielinen (ilmeisesti) ilman anglo-saksista kielivalintaa
www.spamstop.net/ (Japanese)
* englanninkielinen
* sisältönä linkkejä työasemakohtaisiin roskapostisuodatinohjelmiin; vaikuttaa mainossivustolta
www.nospamware.it/ (Italian)
* italiankielinen ilman muuta kielivalintaa (ilmeisesti)
www.uzice.net/yasi/ (Yugoslav Anti-Spam Initiative)
* serbokroatiankielinen? ilman muuta kielivalintaa (ilmeisesti)
http://www.kisa.or.kr/english/
* englanninkielinen sivusto koreankielisen rinnalla
* Korean Information Security Agency, valtion organisaatio
* englanninkielisellä sivustolla ei mitään erityisesti roskapostista
* linkit muihin Etelä-Korean ministeriöihin yms. valtion organisaatioihin
* paperijulkaisuna "Guide to Best Practices for Blocking Spam", 2004

RVT-jaos/VAHTI, 3.4.2006

Liite 5 Tiedoksi sähköpostivastaaville ja sähköpostiylläpidossa työskenteleville

Yksi RVT-jaoksen tavoitteista oli luoda valtionhallinnon sähköpostivastaavien yhteistyöverkosto. Verkostoitumisen tarkoituksena on, että samanlaisten ongelmien kanssa painiskelevat sähköpostiylläpitäjät eivät aina joutuisi turhaan keksimään pyörää uudestaan omilla tahoillaan. Kuten niin monessa muussakin toiminnassa, myös roskapostin torjunnassa olisi hyvä pyrkiä siihen, että voitaisiin mahdollisimman laajalti hyödyntää muualla jo saavutettuja tuloksia ja ottaa oppia muiden yrityksistä, erehdyksistä ja onnistumisista. Jos sähköpostivastaavat tekevät yhteistyötä ja jakavat avoimemmin kokemuksiaan käyttämistään postinvälitysohjelmistoista ja roskapostintorjuntamenetelmistä, niin kaikki voivat hyötyä.

Epäselvyyksien välttämiseksi on ehkä syytä tehdä pieni terminologinen tarkennus. Nykyään on hyvin tyypillistä, että haittaohjelmat levittävät roskapostia tai että roskaposti sisältää kylkiäisenä haitallisen liitetiedoston. RVT-jaosto on keskusteluissaan päätynyt sille linjalle, että pedanttisen tarkka erottelu esimerkiksi roska- ja viruspostien torjumisen välillä on usein käytännössä tarpeetonta. Paremminkin voitaisiin todeta omaksutun asenteen olevan pragmaattinen: ”Kaikki roska on käyttäjien kannalta roskaaja siitä roskasta haluamme mahdollisimman nopeasti eroon.”

Mikäli työskentelet sähköpostin ylläpitotehtävissä ja haluat olla mukana kehittämässä yhteistyötä tai vain seurata postituslistaa, niin voit liittyä postituslistalle lähettämällä viestin osoitteeseen *majordomo@helsinki.fi*. Jätä viestin otsikkokenttä tyhjäksi ja kirjoita varsinaiseen tekstiosaan viestiksi: *subscribe mail-admins@helsinki.fi oma@osoittee.si* (Huom! käytä plain text –muotoa).

Liite 6 Roskapostin määrän mittaaminen (RVT12) -alatyöryhmän toiminta

Ryhmän tehtävämäärittely

Alatyöryhmän alkuperäisenä tehtävämäärittelynä oli "Roskapostin määrän mittaaminen ja reaaliaikainen seuranta".

Ryhmän kesken käydyn keskustelun tuloksena reaaliaikaisen roskapostin seurannan luominen todettiin teknisesti niin vaikeaksi haasteeksi, että se jätettiin epärealistisena pois tavoitteesta eli ryhmän toiminnan tavoitteeksi jäi löytää keinoja roskapostin määrän seuraamiseen.

Roskapostin määrän mittaamisen tavoitteet

Alatyöryhmässä käydyssä keskustelussa roskapostin mittaamisessa ryhmän lähes yksimielinen käsitys oli, että roskapostin määrää tulee mitata

- vain viraston ulkopuolelta tulevasta postista (eli viraston sisältä tuleva liikenne jätetään tässä huomiotta)
- luokittelu tulee tehdä melko karkealla tasolla:
  roskapostin osuus / viruksia sisältävien viestien osuus / asiallisen viestien osuus
- roskapostin määrän seurantaan riittää kuukausikohtainen tilastointi

Näiden tilastojen perusteella voidaan arvioida roskapostin määrän kehitystä, suodatuksessa käytettyjen menetelmien tehokkuutta sekä tarvittavia koneresursseja.

Toinen, täysin poikkeava näkökulma olisi mitata suodatuksen läpi käyttäjien sähköpostikansioon pääsevien roskapostiviestien määrää. Tämän mittaaminen on kuitenkin vaikeaa, ja sitä voisi käytännössä toteuttaa esimerkiksi raportointilomakkeilla tai käyttäjille tehdyillä kyselyillä.

Roskapostin määrän mittaaminen kansallisella tasolla

Kansallisella tasolla sähköpostipalveluja ja niiden toiminnan varmistamista säätelee Viestintävirasto (Vivi). Vivi on tehnyt teleyrityksiä varten määräyksen Sähköpostipalvelujen tietoturvasta ja toimivuudesta (http://www.ficora.fi/suomi/document/Viestintavirasto112004M.pdf)
sekä suosituksen sen soveltamisesta
(http://www.ficora.fi/suomi/document/SMS11.pdf)

Alatyöryhmä oli yhteydessä Vivin Sähköposti- ja Internet-yhteyspalvelujen tietoturva ja toimivuus (SIT) -työryhmään. SIT-työryhmällä ei ole menossa aktiviteettia roskapostin määrän jatkuvan seurannan suhteen. Tarvitessaan tilastoja roskapostin määrästä Vivi on hankkinut niitä tietyiltä operaattoreilta.

Pilottijärjestelmä roskapostitietojen keräämiseen ja tilastointiin

Jari Lehtonen Turun yliopistosta ilmaisi kiinnostuksensa pilottijärjestelmän rakentamiseen roskapostinmäärä tietojen keräämistä ja tilastointia varten.

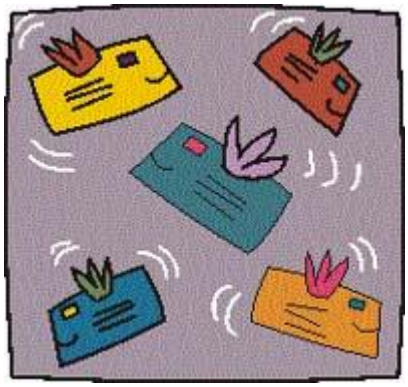
Kerättävien tietojen formaatiksi määriteltiin

- päiväkohtaisille tiedoille:
  <domain>:<päivämäärä>:<ok-postin-määrä>:<roskapostin-määrä>:<virusviestien-määrä>
  (esim. virasto.fi:20050815:11111:3333:222)
- kuukausikohtaisille tiedoille:
  <domain>:<kuukausi>:<ok-postin-määrä>:<roskapostin-määrä>:<virusviestien-määrä>
  (esim. virasto.fi:200508:11111:3333:222)

Pilottijärjestelmä valmistui syyskuussa 2005. Lokakuun alkuun mennessä kaksi virastoa oli toimittanut järjestelmään päivätason tiedot vuoden 2005 alusta lähtien. Tiedoista on toistaiseksi tuotettu päivä- ja kuukausikohtaisia graafeja roskapostin ja viruspostin määristä.

Liite 7 Pelisäännöt turvalliseen sähköpostiin

Tulviiko sähköpostilaatikkosi roskapostia? Miksi ystäväsi lopulta raivostui lähettämästäsi sähköpostikortista? Lue ohjeet turvalliseen sähköpostiin ja vältä virheet.



Sähköpostin luotettava toiminta tulevaisuudessa edellyttää tietoteknisiltä järjestelmiltä yhä enemmän tehoa ja älykkyyttä roskapostien ja haittaohjelmien poistamiseksi organisaation sähköpostiliikenteestä. Roskapostin vastaisessa taistelussa myös käyttäjän omilla toimenpiteillä on suuri merkitys yritettäessä vähentää tämän ylimääräisen vaivan aiheuttamaa lisätyötä.

Seuraavien pelisääntöjen noudattaminen vähentää käyttäjälle tulevaa roskapostia ja rasittaa vähemmän tietoteknisten järjestelmien resursseja.

Kymmenen kultaista ohjetta turvalliseen sähköpostiin:

1) Ilmoitan osoitteeni muodossa etunimi.sukunimi@organisaatio.fi.
Älä kerro oikeaa osoitettasi, vaan kuinka se muodostuu. Jos nimesi on Matti Virtanen, niin kerro osoitteesi olevan etunimi.sukunimi@ktm.fi. Tätä osoitetta roskapostittaja ei voi hyödyntää.

2) Harkitsen tarkkaan kenelle luovutan tai mihin verkossa syötän sähköpostiosoitteeni.
Käytä työpaikkasi sähköpostiosoitetta ainoastaan työasioiden hoitamiseen. Älä syötä sähköpostiosoitettasi epäilyttäville web-lomakkeille tai anna sitä epämääräisiin jakelulistoihin.

3) Jos tunnistan viestin roskapostiksi, tuhoan sen heti.
Älä ole turhan utelias. Roskapostien käsittely kuluttaa turhaan työaikaa, ja lisäksi se saattaa olla jopa vaarallista. Voit nimittäin vahingossa klikata esim. linkkiä roskapostissa mainostetulle www-sivulle tai avata haittaohjelman sisältävän liitetiedoston.

4) En koskaan vastaa roskapostiin.
Roskapostiin vastaaminen osoittaa roskapostittajalle, että osoitteesi on toimiva, jolloin sinulle tulevan roskapostin määrä kasvaa. Lisäksi roskapostin lähettäjäosoite on usein väärennetty, jolloin vastauksesi saattaa kuormittaa viattoman sivullisen postilaatikkoa.

5) En koskaan klikkaa linkkejä roskapostissa.
Linkki ei välttämättä johda sinne minne se näyttää. Linkin takana saattaa piileskellä haittaohjelma. Linkin takana saattaa myös olla ammattirikollinen, joka on kiinnostunut käyttäjätunnuksistasi ja salasanoistasi.

6) En tartu roskapostiviestien tarjouksiin, enkä näin tule huijatuksi.
Kysy itseltäsi: ”Miten luotettava tarjous voi olla, jos sitä pitää mainostaa roskapostin keinoin?” Tässäkin käy vanha viisaus. ”Jos tarjous on liian hyvä ollakseen totta, niin…” Kaiken lisäksi huijatuksi tuleminen on noloa ja nöyryyttävää.

7) En lähetä netistä sähköpostikortteja tai muita viestejä.
Roskapostittajat ja muut huijarit käyttävät sähköpostikortteja osoitteiden keräämiseen. Vastaanottaja ei ilahdu joutuessaan spammerin uhriksi sähköpostikorttisi takia.

8) En jatka ketjukirjeitä, vitsejä, videoleikkeitä tai muita vastaavia.
Ketjukirjeet, vitsit ja videoleikkeet ovat tyypillistä roskapostia. Myös virukset saattavat levitä näiden viestien mukana. Ethän välitä niitä eteenpäin?

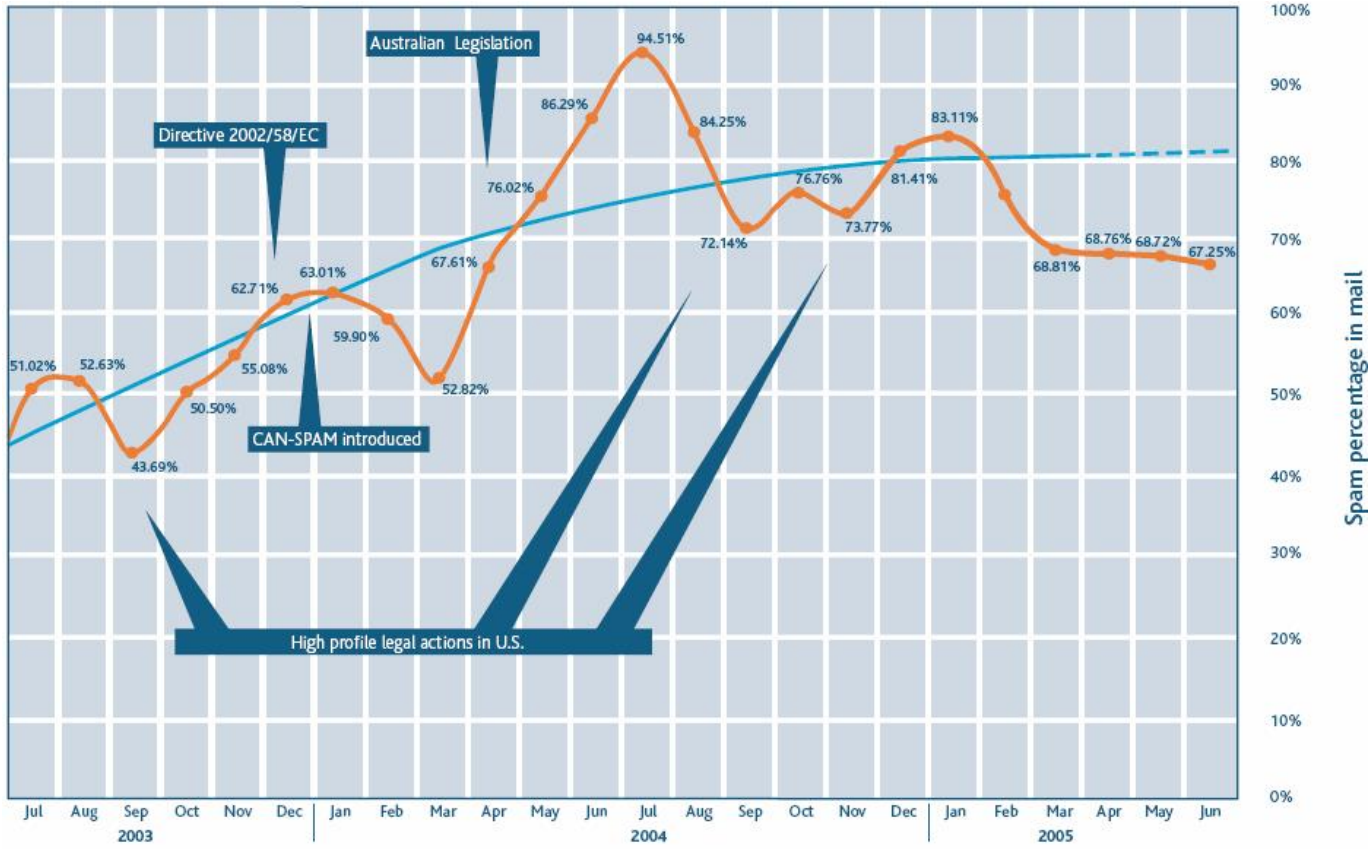
9) En käytä esikatselua.
Haittaohjelma saattaa aktivoitua koneellasi jo sähköpostin esikatseluikkunassa.

10) Opetan myös työtoverini noudattamaan näitä sääntöjä.
Nyt kun olen itse oppinut turvallisen sähköpostiviestinnän pelisäännöt, voin kertoa näistä asioista myös muille.

Teksti: Kari Keskitalo

Liite 8 Roskapostin määrän väheneminen jaoston toiminta-aikana

Jaoksen toiminta-aikana roskapostien määrä on vähentynyt heinäkuun 2004 94,5 %:n huipusta syksyn 2005 alle 70 %:n tasoon.



Lähde: www.messagelabs.com

Liite 9 **Voimassaoleva VAHTI-ohjeistus**

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

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

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