VALTIOVARAINMINISTERIÖ

HAITTAOHJELMILTA SUOJAUTUMISEN YLEISOHJE

3/2004

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

HAITTAOHJELMILTA SUOJAUTUMISEN YLEISOHJE

3/2004

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

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

ISSN 1455-2566
ISBN 951-804-443-0

Edita Prima Oy

HELSINKI 2004

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 15/01/2004

OHJE
23.6.2004

Ministeriöille, virastoille ja laitoksille

HAITTAOHJELMILTA SUOJAUTUMISEN YLEISOHJE

Valtiovarainministeriö antaa oheisen tietoturvaohjeen (jäljempänä ohje), joka on laadittu valtiovarainministeriön asettaman ja johtaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimesta. Ohje korvaa VM:n antaman ohjeen "Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje" (VM:n VAHTI-ohje 4/2000) ja täydentää laajaa valtion tietoturvaohjeistoa.

Ohje on tarkoitettu johdolle, tietoturva-, tietohallinto-, tietoverkko- ja tietojärjestelmävastaaville sekä kaikille työasemakäyttäjille. Ohjeessa on kuvattu tiiviissä muodossa haittaohjelmilta suojautumisen yleiset periaatteet ja toiminnan organisoimisen merkitys osana johtamista. Ohjeeseen sisältyy myös pikaopas käyttäjille.

Organisaation johdon on varmistauduttava, että haittaohjelmien torjunnan tekniset ja hallinnolliset toimet on suoritettu ja niitä kehitetään jatkuvana tehtäväalueena osana laajapohjaista tietoturvatyötä. Järjestelmät on rakennettava, kehitettävä ja ylläpidettävä niin, että saavutetaan riittävä suoja haittaohjelmia vastaan.

Työasemien versionhallinnasta ja korjauspäivityksistä tulee huolehtia mahdollisimman keskitetysti jatkuvaluonteisena tehtäväalueena. Erityistä huomiota tulee kiinnittää muun muassa kannettaviin tietokoneisiin sekä etätyökoneiden ohjelmistopäivityksiin ja organisaation verkkoon liittämisen turvallisuuteen.

Riittävän syvän, kerroksellisen haittaohjelmatorjunnan saavuttamiseksi tulee sisäverkko suojata sekä yhdyskäytävä- että työasematasolla haittaohjelmien torjuntaohjelmilla ja huolehtia ohjelmapäivityksistä. Erityisesti kriittiset palvelimet, testi- ja tuotantojärjestelmät tulee erottaa omiin segmentteihinsä.

Ohje tulee VAHTIn Internet-sivuille, jotka ovat osoitteissa *www.vm.fi/tietoturvallisuus ja www.vm.fi/vahti*. Ohjetta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi).

Lisätietoja antavat neuvotteleva virkamies Mikael Kiviniemi ja tietoturva-asiantuntija Juhani Sillanpää (etunimi.sukunimi@vm.fi).

Toinen valtiovarainministeri Ulla-Maj Wideroos

Ylijohtaja Jorma Karjalainen

Liite Haittaohjelmilta suojatumisen yleisohje (VM:n VAHTI-ohje 3/2004)

HAITTAOHJELMILTA SUOJAUTUMISEN YLEISOHJE

Tiivistelmä

Kansalaisten ja palvelujen käyttäjien näkökulmasta tarkastellen hallinnon tehtävänä on tuottaa sellaisia sähköisiä palveluja, joiden käytettävyyteen asiakas voi luottaa.

Palveluita tuotettaessa on huomioitava kansalaisten perusoikeudet ja rakennettava järjestelmät siten, että saavutetaan riittävä suoja haittaohjelmia vastaan niin teknisesti kuin hallinnollisestikin kuvaamalla palvelun tietoturvapäivityksien prosessit.

Tietoturvallisuuden merkitys organisaation johtamisessa ja toimintakyvyn varmistamisessa sekä häiriöttömän ja tuloksellisen toiminnan ylläpitämisessä on jatkuvasti korostunut palveluiden tuottamisessa.

Yleisohjeessa on esitetty tiiviissä muodossa haittaohjelmilta suojautumisen yleiset periaatteet ja toiminnan organisoimisen merkitys osana johtamista.

Organisaation johdon on varmistauduttava, että haittaohjelmien torjuntaan liittyvät niin tekniset kuin hallinnollisetkin toimet on suoritettu ja niihin osallistuva henkilöstö on tietoinen velvoitteistaan. Johdon tulee vaatia tulosohjaukseen liitettynä korkeatasoista tietoturvallisuuden hallintaa ja antaa siihen riittävät voimavarat.

Yleisohjeessa on haittaohjelmiin liittyvää kysymysten asettelua tarkasteltu TCP/IP – protokollaa (Transmission Control Protocol / Internet Protocol) käyttävien tietoverkkojen näkökulmasta eikä niinkään turvalähtöisistä, toimittajakohtaisista verkoista tai työasemista, jotka ovat verkkopäätteitä.

Sisäverkon työasemien versionhallinnasta ja korjauspäivittämisestä tulee huolehtia mahdollisimman keskitetysti. Erityistä huomiota tulee kiinnittää kannettaviin tietokoneisiin ja etätyökoneiden ohjelmistojen päivittämiseen sekä niiden liittämiseen etäkäytön jälkeen organisaation verkkoon.

Älykkään puhelimen arkkitehtuurista johtuen on laitteesta tulossa houkutteleva kohde haittaohjelmille, jotka voivat levitä esimerkiksi pelien välityksellä, ladattavissa soitto-äänissä ja logoissa. Haittaohjelma voi hyödyntää myös laitteen turvatonta oheislaite-yhteyttä. Merkittävä riski on laitteen Internet-toiminnot ja synkronointi organisaation käytössä olevaan työasemaan. Kaikkiin näihin riskeihin on varauduttava suunnittelulla ja hallitulla käyttöpolitiikalla.

Riittävän syvän, kerroksittaisen puolustuksen saavuttamiseksi tulee sisäverkko suojata sekä yhdyskäytävä- että työasematasolla torjuntaohjelmistoilla.

Vähintäänkin organisaation sisäverkon kriittiset palvelimet, testi- ja tuotantojärjestelmät sekä työasemat tulee erottaa omiin segmentteihinsä.

Version hallinta

Versio	Muutettu kohta ja sivu (huomautus)	Päivämäärä
0.1	Laadittu ohjeen runko ensimmäisessä kokouksessa	02.12.2003
0.2	Kirjoitettu ohjeen runko ja alakohdat	16.12.2003
0.3	Laitettu ryhmälle jakeluun puheenjohtajan esitys sisällysluettelosta	02.01.2004
0.4	Muutettu asioiden ryhmittely kokouksessa kaksi	09.01.2004
0.5	Kirjoitettu ohjetta jaettujen kirjoitusosuuksien mukaan sekä uusittu asioiden jaottelua	20.01.2004
0.6	Koottu tekstit yhteen. Vaihdettu kohta 2.7 kohtaan 4.2 ja kohta 2.8 kohtaan 4.1. Aku Hilve	04.02.2004
0.7	Kokouksen 10.2. palautteesta kohdat 5.3 5.3 ja 5.4 sekä kohta 4. Poistettu kohta 4.2.1. Lisätty toimintaprosessikuva.	11.02.2004
0.8	Risto Heinosen toimittama luku 2.6 uusittu	17.03.2004
0.9	Täydennetty luku 5.5 ja lukua 2.6 sähköpostin viivästyksen osalta.	26.03.2004
0.95	Kari Keskitalon tarkennukset lukuun 5.5. Eeva Björklundin kommentit.	13.04.2004
0.96	Mikael Kiviniemen kommentit	18.05.2004
0.97	VAHTI-kommentointikierros	10.06.2004
1.0	Hyväksytty VAHTI kokouksessa	18.06.2004

SISÄLLYS

Tiivistelmä 5
1. JOHDANTO 9
1.1 Tietojen merkitys organisaatiolle 9
1.2 Johtamisen tavoitteet 9
1.3 Haittaohjelmien torjunnan edellytykset 9
1.4 Ohjeen kohderyhmät ja rakenne 10
1.5 Ohjeen laatiminen 11

2. HAITTAOHJELMA 13
2.1 Mitä haittaohjelmat ovat 13
2.2 Haittaohjelman komponentit ja vaikutukset 15
2.3 Miten haittaohjelma toimii 16
2.4 Miksi haittaohjelmat ovat vaarallisia 19
2.5 Haittaohjelmien käyttötarkoituksia 20
2.6 Haittaohjelmien sääntely 21

3. SUOJATTAVAT KOHTEET JA VALVONTA 25
3.1 Työasemat ja palvelimet 25
3.2 Tietoverkko 25
3.3 Mobiililaitteet 26

4. TOIMENPITEIDEN ORGANISOINTI JA TORJUNTAPROSESSI 27
4.1 Tietoteknisen ympäristön hallinta ja tietotekninen valvonta 27
4.1.1 Organisointi 27
4.1.2 Hallinta ja valvontatehtävien suorittaminen 27
4.1.3 Yleinen verkon ja laitteistojen tietoturvan valvonta 28
4.1.4 Turvallisuustason selvitysohjelmistojen hallittu käyttö 29
4.1.5 Hankinnat ja ulkoistetut käyttöpalvelut 29
4.2 Torjunnan suunnittelu ja toiminnan jatkuvuuden varmistaminen 30
4.3 Havainnosta torjuntaan 30
4.3.1 Haittaohjelman havaitseminen 31
4.3.2 Tilanneanalyysi ja reagointiaika 31
4.3.3 Haittaohjelmatapauksen käsittely 31
4.4 Korjaus- ja jälkitoimenpiteet 34
4.5 Haittaohjelmiin liittyvä tiedottaminen ja raportointi osana valvontaa 34
4.6 Kustannukset ja niiden mittaaminen 35

5. KUINKA VÄLTTÄÄ TARTUNTA 37
5.1 Työaseman turvalliset asetukset 37
5.1.1 Työaseman BIOS tason suojaukset 37
5.1.2 Työaseman perusasetukset 38
5.1.3 Selaimen turva-asetukset 38
5.1.4 Sähköpostin turva-asetukset 40
5.1.5 Kannettavien työasemien turvaaminen 41
5.2 Ohjelmistohaavoittuvuudet ja korjauspäivitykset 41
5.2.1 Haittaohjelmien hyväksikäyttämät ohjelmistohaavoittuvuudet 42
5.2.2 Haavoittuvien järjestelmien päivittäminen ja suojaaminen 42
5.2.3 Puuttuvien korjauspäivitysten havaitseminen 44
5.2.4 Haavoittuvuuksien ja korjauspäivityksien seuraaminen 44
5.3 Torjuntaohjelmat, niiden päivitykset ja seuranta 45
5.3.1 Torjuntaohjelmistojen konfigurointi 45
5.3.2 Torjuntaohjelmiston päivitykset 46
5.4 Organisaation verkon suojaaminen 47
5.4.1 Verkon ulkorajojen suojaaminen 47
5.4.2 Sisäverkon sisäiset suojautumismenetelmät 48
5.5 Työskentely organisaation ulkopuolella 48

6. TOIMINNAN KEHITTÄMINEN JA KOULUTUS 51
6.1 Kehittämissuunnitelma 51
6.2 Koulutus 51

7. LIITTEET
Liite 1. Toiminta haittaohjelmatapauksessa
Liite 2. Selaimen asetukset
Liite 3. Käyttäjän pikaopas
Liite 4. Sisäisten ja ulkoisten velvoitteiden luettelo

1. JOHDANTO

1.1 Tietojen merkitys organisaatiolle

Useat lait ja asetukset edellyttävät valtion viranomaisen huolehtivan tietoturvallisuudesta. Haittaohjelmat ovat yksi tietoturvallisuuden uhka-alue. Vahinkojen varalle tulee rakentaa torjunta- ja toipumismenettelyt sekä organisoida toimintoja suorittava henkilöstö.

Tietoturvajärjestelyjen tavoitteena on suojata tiedon luottamuksellisuus, eheys ja käytettävyys. Työasemissa saa käyttää vain luotettavista lähteistä hankittuja ohjelmia ja niiden asentaminen on keskitettävä tietohallinnolle.

1.2 Johtamisen tavoitteet

Viranomaisen tietojärjestelmät ja tietojen käsittelymenetelmät tulee rakentaa lähtökohtana riittävä suoja haittaohjelmia vastaan. Osana tietojärjestelmien, -verkkojen ja -palveluiden suunnittelua ja toteutusta on oltava etukäteen suunnitellut toimenpiteet, jotka tarvitaan haittaohjelmien aiheuttaman riskin minimoimiseksi.

Organisaation palvelimet ja tietoverkkoihin liitetyt työasemat ja kannettavat työasemat sekä mobiililaitteet tulee olla varustettuina haittaohjelmien torjuntasovelluksilla.

Torjuntaohjelmistojen toiminnan ja turvapäivityksien asennustoimien on oltava riittävän automaattista lähtökohtana ratkaisu, joka ei pääsääntöisesti edellytä tietotekniikan peruskäyttäjiltä tietoteknisiä ylläpitotoimia.

1.3 Haittaohjelmien torjunnan edellytykset

Johdon tehtävänä on huolehtia haittaohjelmilta suojautumisen edellytyksistä ja tehtävien vastuuttamisesta ja valvonnan järjestämisestä varmistamalla tarvittavan käyttöpolitiikan ja tietoturvaohjeistuksen olemassaolo sekä niiden kattavuus.

Esimiesten tulee valvoa, että tässä ohjeessa ja organisaation omassa tarkemmassa ohjeistuksessa annettuja ohjeita noudatetaan koko henkilöstön osalta ja näistä toimista vastaava tietotekninen henkilöstö saa riittävän koulutuksen tehtävästä suoriutumiseksi.

Haittaohjelmien havaitsemisesta on oltava raportointimenettely tietoturvalli-suudesta ja tietohallinnosta vastaaville sekä ylimmälle johdolle. Virastoissa tulee huolehtia, että henkilöstö on saanut koulutusta tietoverkkoihin ja haittaohjelmiin liittyvistä uhkista ja niiltä suojautumisesta.

Esimiesten tulee varmistua, että työasemissa käytetään vain organisaation määrittämiä asetuksia eikä loppukäyttäjille saa antaa ylläpito-oikeuksia esimerkiksi ohjelmistojen asennuksia tai tietoliikenneasetuksien muuttamista varten.

Tietojärjestelmien ylläpidosta vastaavien tulee ottaa huomioon tietoverkkojen ja palveluiden toteutuksessa ne toimenpiteet, jotka tarvitaan haittaohjelmien aiheuttamien riskien pienentämiseksi. Tietoverkoissa tämä tarkoittaa verkon segmentointia ja palomuurien käyttöä leviämisen rajoittamiseksi.

1.4 Ohjeen kohderyhmät ja rakenne

Ohje on tarkoitettu johdolle, tietohallinnosta, tietoturvallisuudesta ja tietojärjestelmistä vastaaville sekä kaikille työasemien käyttäjille.

Ohjeen luku kaksi, jossa kuvataan erilaisia haittaohjelmia ja niiden toimintaa, on suunnattu johdolle ja käyttäjille. Luvussa kolme, joka on suunnattu tietohallinnolle, kuvataan suojattavat kohteet yleisellä tasolla torjunnan kerroksellisuuden toteuttamiseksi. Luvussa neljä kuvataan toiminnan organisointi tietohallinnossa osana johtamisprosessia.

Ohjeen tietotekniselle henkilöstölle suunnatussa luvussa viisi on kuvattu turvalliset asetukset, haavoittuvuudet, torjuntaohjelmien päivitys ja verkon suojaaminen sekä liitteessä kaksi esimerkkiä selaimen asetuksista.

Henkilöstön koulutukseen liittyvät asiakohdat on esitetty luvussa kuusi ja liitteessä kolme on loppukäyttäjälle suunnattu pikaopas.

Ohjeesta on rajattu pois palvelunestohyökkäys ja roskaposti huolimatta siitä, että roskapostia käytetään haittaohjelmien kuljettamiseen työasemaan ja haittaohjelmia roskapostin levitykseen.

Ohjeessa esitetään yleiset suositukset haittaohjelmilta suojautumiseksi ja torjuntaprosessin kuvaus toimenpiteineen.

Valtionhallinnon organisaatioiden tulee kehittää haittaohjelmien aiheuttamien vahinkojen torjunta- ja toipumismenettelyjä jatkuvaluonteisina toimintoina osana tietoturvallisuuden tulosjohtamista.

Ohje korvaa valtiovarainministeriön antaman ohjeen ”Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje, VAHTI 4/2000” (1.12.2000).

1.5 Ohjeen laatiminen

Ohje laadittiin valtionhallinnon johtoryhmän alaisuudessa ja ohjauksessa. Tehtävään nimetyn työryhmän kokoonpano oli seuraava:

Puheenjohtaja:	Seppo Sundberg, Valtiokonttori
Jäsenet:	Petri Laitinen, Puolustusvoimien tietotekniikkalaitos
	Risto Heinonen, Tietosuojavaltuutetun toimisto
	Aku Hilve, Helsingin poliisilaitos
	Mats Kommonen, Turun yliopisto
	Juhani Sillanpää, Valtiovarainministeriö
	Arsi Heinonen, Viestintävirasto
	Kari Keskitalo, Kauppa- ja teollisuusministeriö

Työ suoritettiin virkatyönä.

Valtiohallinnon tietoturvallisuuden johtoryhmä (VAHTI) käsitteli ohjetta maaliskuun kokouksessaan. Johtoryhmän kommenttikierros päättyi huhtikuun lopussa. Luonnoksesta tiedotettiin laajasti hallinnossa ja yrityksille ja se oli kommentoitavana VAHTI:n kotisivuilla ja siihen saatiin 11 kommenttia. VAHTI hyväksyi ohjeen 18.6. pitämässään kokouksessa.

2. HAITTAOHJELMA

2.1 Mitä haittaohjelmat ovat

Haittaohjelmilla tarkoitetaan ihmisen tarkoituksellisesti tekemiä vahingollisia tietokoneohjelmia. Haittaohjelmista tyypillisimpiä ovat virukset, madot ja troijalaiset.

Virukset

Tietokonevirus on ohjelmakoodia, joka pystyy kopioimaan ja levittämään itseään uusiin kohteisiin. Tietokonevirus tarvitsee levitäkseen ja aktivoituakseen aputiedoston samalla tavoin kuin biologinen virus tarvitsee avukseen isäntäsolun.

Virukset voidaan jakaa niiden tartuttamien kohteiden perusteella neljään päätyyppiin, joita ovat:

- tiedostovirukset,
- makrovirukset,
- komentojonovirukset ja
- käynnistyslohkovirukset.

Virus voi kuulua samalla useampaan kuin yhteen edellä mainituista tyypeistä. 2000-luvun jakomalli on kahdeksanosainen.

Tiedostovirukset tarttuvat suorituskelpoisiin ohjelmatiedostoihin, joista tyypillisimpiä ovat Windows-käyttöjärjestelmässä .com, .exe, .pif ja .scr –päätteiset tiedostot. Leviäminen tapahtuu aina kun saastunut ohjelma suoritetaan koneen muistissa. Tiedostovirukset voivat levitä kaikilla tiedonsiirtotavoilla, joissa siirretään ohjelmatiedostoja.

Makrovirukset on ohjelmoitu toimisto-ohjelmissa käytettävien makrokielten avulla. Makrovirusten leviäminen tapahtuu dokumenttien mukana ja ne saatetaan suorittaa automaattisesti kun dokumentti avataan toimisto-ohjelmassa. Makrovirukset voivat levitä käyttöjärjestelmästä riippumatta, mikäli käytössä on sama toimisto-ohjelma. Toimisto-ohjelmiin on lisätty sisäänrakennettuja ominaisuuksia, joilla makrojen tahatonta suorittamista pyritään estämään.

Komentojonovirukset on tehty käyttäen hyväksi kohdejärjestelmän tarjoamia komentokieliä, kuten Windows-käyttöjärjestelmässä oleva Visual Basic Scripting. Komentojonoja pystytään luomaan tavallisella tekstieditorilla.

Käynnistyslohkovirukset tarttuvat tietovälineen, kuten kiintolevyn tai levykkeen, käynnistyslohkoon, josta tietokone etsii käynnistykseen tarvittavia tietoja. Virus voi tarttua levykkeeltä kiintolevyn käynnistyslohkolle ja tämän jälkeen saastuttaa tietokoneessa käytettävät muut kirjoitussuojaamattomat levykkeet. Käynnistyslohkovirukset leviävät hitaasti, koska ne siirtyvät käytännössä vain levykkeeltä toiselle. Ne ovatkin nykyään erittäin harvinaisia.

Madot

Madoiksi kutsutaan haittaohjelmia, jotka kykenevät leviämään itsenäisesti ilman aputiedostoa. Madot voivat levitä nopeasti esimerkiksi sähköpostin avulla.

Sähköpostimadot voivat olla liitetiedostoina tai osana itse viestiä. Liitetiedostoina leviävät madot vaativat yleensä aktivoituakseen käyttäjän avaavan tiedoston. Eräät madot aktivoituvat tietyillä sähköpostiohjelmilla jo viestin esikatselutilassa. Aktivoiduttuaan sähköpostimato etsii kohdekoneesta sähköpostiosoitteita, joihin se voi lähettää itsensä edelleen. Sähköpostimadot voivat väärentää lähettämänsä viestin lähetys- tai vastaanotto-osoitteen käyttämällä löytämiään osoitteita. Viestit eivät kuitenkaan useimmiten ole suomenkielisiä.

Verkkomadot leviävät tietokoneverkossa tarvitsematta sähköpostin tai tietokoneen käyttäjän apua. Ne käyttävät hyväkseen reaaliaikaista verkkoyhteyttä tietokoneiden välillä. Verkkomatojen leviämiselle otollisia ovat jatkuvasti verkossa kiinni olevat, puutteellisesti ylläpidetyt palvelimet tai kotitietokoneet, joissa on madon leviämisen mahdollistavia paikkaamattomia tietoturvahaavoittuvuuksia.

Troijalaiset

Troijalaiset ovat ohjelmia, jotka tekevät ohjelman käyttäjältä salassa jotain arvaamatonta. Troijalaiset leviävät jollain tapaa houkuttelevan tai hyödyllisen ohjelman mukana tai ovat osa itse ohjelmaa sisältäen dokumentoimattomia toimintoja. Troijalaisissa itsessään ei ole leviämismekanismia, vaan niitä käytetään tyypillisesti muun haittaohjelman haittakuormana.

Troijalaiset voivat avata kohdekoneelle takaportin, jonka kautta luvaton tunkeutuja voi päästä murtautumaan tietokoneelle ja etähallitsemaan sitä jopa organisaation palomuurin läpi. Murrettua tietokonetta voidaan käyttää roskapostitukseen, palvelunestohyökkäyksiin tai tietomurtoihin. Troijalaiset voivat myös kerätä ja lähettää verkossa eteenpäin salasanoja, sähköpostiosoitteita, näppäinpainalluksia tai tietoa kyseisestä tietokoneesta tai käyttäjän toimista, kuten vierailuista verkkosivuilla.

Vakoilu- ja mainosohjelmat

Jotkut ilmaiset ja jopa maksullisetkin hyöty- tai apuohjelmat sisältävät vakoilukomponentteja, jotka keräävät ja lähettävät tietoa koneen käytöstä eteenpäin. Kerättävät tiedot voivat olla tietoja käyttäjän vierailemista www-sivuista tai jopa verkkopalvelujen salasanoja. Ohjelmat voivat pakottaa selaimen aloitussivun omalle kotisivulleen siten, että aloitussivua on vaikea muuttaa takaisin halutuksi sivuksi tai ne saattavat avata lukuisia mainosikkunoita selainta käytettäessä.

Näistä vakoiluohjelmista saatetaan kertoa ohjelmaa ladattaessa tai ohjelman lisenssisopimuksessa. Koska joillekin vakoiluohjelmille saadaan asennettaessa käyttäjän suostumus, näitä ohjelmia ei välttämättä tunnisteta virustorjunta-ohjelmalla, vaan ne vaativat tähän tarkoitukseen kehitetyn oman torjunta-ohjelmansa. Osa vakoiluohjelmista asentuu työasemalle salaa käyttäjän tietämättä ja lupia kysymättä.

Huijausviestit (Hoax), ketjukirjeet ja pilailuohjelmat

Huijausviestit eivät ole ohjelmia, vaan sähköpostiviestejä, jotka leviävät hyväuskoisten käyttäjien lähettäminä. Näissä viesteissä saatetaan varottaa vaarallisesta viruksesta ja kehottaa käyttäjää lähettämään viesti eteenpäin mahdollisimman monelle, kuten vaikkapa tietohallinnon ylläpitäjille. Viestistä saa informoida vain omaa tietohallintoa.

Huijausviestien, samoin kuin ketjukirjeiden, välittämisen seurauksena kuluu sekä lähettäjän, että vastaanottajan työaikaa. Pahimmillaan huijausviestit erehdyttävät käyttäjän toimimaan virheellisesti, kuten poistamaan käyttöjärjestelmälle tärkeitä tiedostoja viruksina.

Internetistä on saatavana paljon erilaisia vitsi- ja pilailuohjelmia, joilla säikytellään tavallisia käyttäjiä. Ohjelmat voivat antaa kummallisia virheilmoituksia, olla alustavinaan käyttäjän kiintolevyä tai tuhoavinaan tiedostoja. Tietokoneen hiiren tai näytön toimintaa voidaan manipuloida siten, että ne vaikuttavat olevan rikki. Nämä ohjelmat eivät yleensä ole vihamielisiä, mutta niiden mukana voi levitä vaarallisia haittaohjelmia ja ne voivat kuluttaa henkilöresursseja laitteiden tarkastukseen.

2.2 Haittaohjelman komponentit ja vaikutukset

Haittaohjelmissa on erotettavissa erilaisia komponentteja, kuten leviämismekanismi ja haittakuorma (payload).

Leviämismekanismin tarkoituksena on muodostaa haittaohjelmasta kopio ja levittää se eteenpäin uuteen kohteeseen. Leviämisessä hyödynnetään tietoverkkoa, ohjelmistojen aukkoja sekä tietoverkon ja käyttäjien toimia.

Haittakuorma voi kohdejärjestelmässä esimerkiksi:

- asentaa takaoven, jota kautta tietokone on ulkopuolisten tunkeutujien hallittavissa myös palomuurin läpi
- lisätä, tuhota tai muuttaa tiedostoja
- näyttää erilaisia viestejä käyttäjälle
- estää järjestelmän hyötykäytön
- muuttaa järjestelmän epästabiiliksi
- tallentaa ja lähettää ulkopuolisille näppäinpainalluksia tai salasanoja
- postittaa luottamuksellisia tietoja ulkopuolisille
- poistaa virustorjunnan tai muita turvamekanismeja käytöstä

Haittakuorma voi aiheuttaa sen, että kohdejärjestelmää käytetään välineenä:

- tietomurtoihin
- palvelunestohyökkäyksiin
- roskapostin massalähetyksiin
- tarpeettoman, ylimääräisen verkkoliikenteen luomiseen

Kaikissa haittaohjelmissa ei ole mukana vahingollista haittakuormaa, vaan ne ainoastaan kopioivat ja levittävät itsensä uusiin kohteisiin.

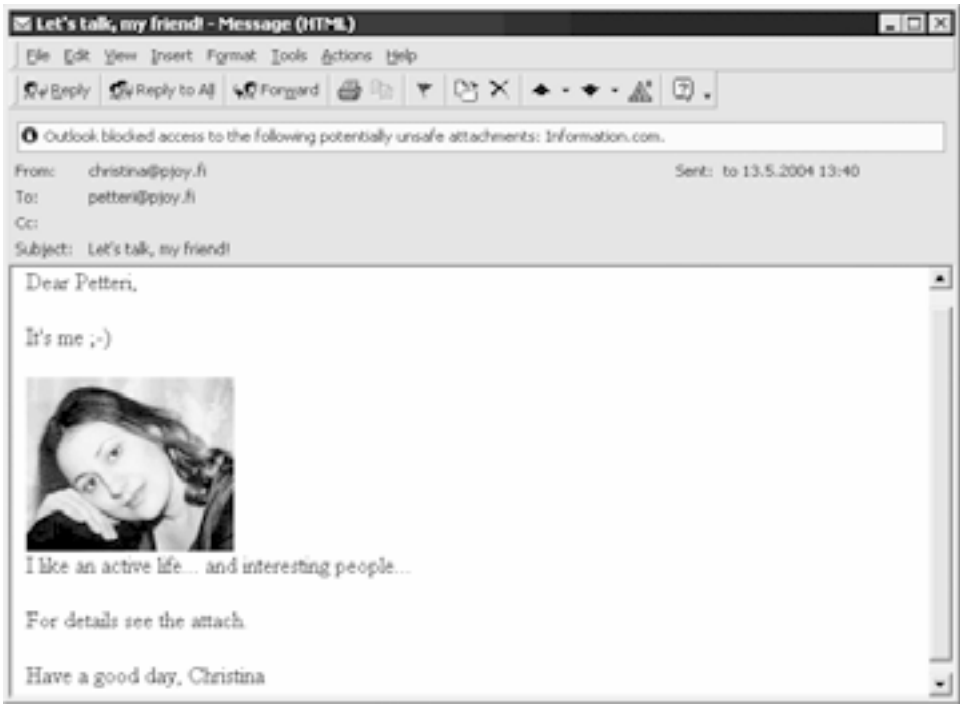
2.3 Miten haittaohjelma toimii

Virus vaatii yleensä käyttäjän toimenpiteitä aktivoituakseen ja levitäkseen. Tyypillisesti käyttäjä suorittaa saastuneen ohjelman omalla tietokoneellaan tai lataa sen vierailemaltaan verkkosivulta tahi avaa saastuneen sähköpostin liitetiedoston.

Virusten tekijät pyrkivät käyttämään hyväksi ihmisten uteliaisuutta, kokeilunhalua ja luottavaisuutta. Sähköpostin liitteenä leviävä virus pyritään saamaan vaikuttamaan jollakin tavalla houkuttavalta.

Se saattaa olla naamioitu kuvatiedostoksi, vitsiksi, kiertokirjeeksi, tekniseksi korjauspäivitykseksi, palkinnoksi, tms.

Kuvassa on tekniseksi korjauspäivitykseksi naamioitunut Swen virus. Oikeita turvapäivityksiä ei jaeta sähköpostilla.



Kuvassa BagleY2 –viruksen saastuttama sähköpostiviesti, joka houkuttaa avaamaan liitetiedoston.

Saastunut sähköposti näyttää tulevan luotettavasta lähteestä. Tällöin on yleensä kyseessä viruksen tekemä osoitehuijaus. Haittaohjelma kerää saastuttamiensa tietokoneiden tiedostoista sähköpostiosoitteita, joita se käyttelee lähettämiensä viestien lähde- ja kohdeosoitteina. Sähköpostin vastaanottajan tai lähettäjän kone ei siis välttämättä ole saastunut, kummankin osoite on vain löytynyt saastuneen osapuolen kiintolevyltä.

Liitetiedoston nimessä saattaa olla kaksoispääte (tiedosto.jpg.exe), jolla yritetään saada käyttäjä luulemaan tiedostoa sellaiseksi, että sen voi turvallisesti avata ilman virustarkistusta. Lisäksi liitetiedoston kuvake voi myös näyttää sähköpostinlukuohjelmassa turvalliselta.

Haittaohjelmien pääasiallisia leviämisteitä ovat:

- sähköposti, roskaposti
- tiedostonjako-ohjelmien muodostamat vertaisverkot (P2P, **P**eer-**t**o-**P**eer)
- IRC-keskustelukanavat (**I**nternet **R**elay **C**hat)

- jaetut verkkoresurssit
- www-sivut
- verkosta ladattavat ohjelmat
- käyttöjärjestelmä- ja ohjelmistohaavoittuvuudet

Viruksia leviää verkosta ladattavien ohjelmien ja komentojonojen (skriptien) mukana. Tämän vuoksi on tärkeää, etteivät käyttäjät asenna koneelleen itse hankkimiaan tai kopioimiaan ohjelmia. Työasemissa on käytettävä ainoastaan tietohallinnon hyväksymiä lisensoituja ohjelmia.

Verkkosivujen aktiivisen sisällön, kuten Java, javascript ja ActiveX-komponenttien, mukana voi levitä haittaohjelmia. Osa haittaohjelmista tarttuu huomaamatta, osa tarttuu sen vuoksi, että käyttäjä hyväksyy erilaisista ilmoituksista ja varoituksesta huolimatta ohjelmakomponentin asentamisen koneelleen.

Esimerkkinä tämäntyyppisistä haittaohjelmista ovat modeemin soitto-ohjelmat, jotka vaihtavat modeemikäyttäjän oletuksena olevan Internet-yhteyden kalliiksi ulkomaiseksi palvelunumeroksi. Verkkosivuilla olevien komentojonojen eli skriptien avulla leviää myös troijalaisohjelmia. Troijalaiset avaavat koneelle takaoven, jota käyttäen hyökkääjän on mahdollista etähallita konetta jopa organisaation palomuurin läpi.

Madot kopioituvat itsenäisesti ilman isäntätiedostoa ja voivat levitä tietokoneelle tietoturvahaavoittuvuutta hyväksikäyttäen ilman, että käyttäjä mitenkään osallistuu niiden aktivoitumiseen.

Sähköpostimato voi levitä sähköpostin välityksellä jopa ilman, että käyttäjä avaa sähköpostia tai sen liitetiedostoa. Eräissä sähköpostinlukuohjelmissa on ollut haavoittuvuuksia, jotka mahdollistavat haittaohjelman aktivoitumisen jo viestin esikatselutilassa.

Verkkomato voi levitä tietoturvahaavoittuvuuden kautta, joita voi olla esimerkiksi tietokanta- tai www-palvelinohjelmistossa tai se voi levitä selaimen kautta verkkosivulta, tiedostonjako-ohjelman avulla taikka jaetuilla verkkoresursseilla.

Haavoittuvuuksia voi olla yllättävissä kohteissa. Esimerkiksi työasemalle asennettu sähköinen tietosanakirjasovellus saattaa sisältää haavoittuvan tietokantaohjelmiston kevytversion.

2.4 Miksi haittaohjelmat ovat vaarallisia

Kun organisaation tietoturvallisuus pettää, seuraukset ovat usein taloudellisia ja ajallisia menetyksiä, työtehon ja -motivaation laskemista, kilpailukyvyn heikentymistä, imagohaittoja, laadun ja luotettavuuden heikentymistä,

lakien tai sopimusten rikkomista mahdollisine korvausvastuineen sekä henkilöiden yksityisyyden suojan kärsimistä.

Haittaohjelmat aiheuttavat aina joitakin edellä mainituista seurauksista. Myös hyvän tiedonhallintatavan edellyttämään haittaohjelmien torjuntaan kuluu pakostakin ajallisia ja taloudellisia resursseja. Nämä kulutetut resurssit voidaan laskea kuuluviksi haittaohjelmien aikaansaamiksi haitoiksi. Haittaohjelmien aiheuttamista kustannusvaikutuksista kerrotaan luvussa 4.6.

Haittaohjelmat tekevät käyttäjältä lupaa kysymättä ei-toivottuja toimenpiteitä. Ne voivat aiheuttaa merkittäviä seurauksia kohdejärjestelmän ja sen tietojen luottamuksellisuudelle, eheydelle ja käytettävyydelle.

Haittaohjelmien saastuttamia järjestelmiä voidaan käyttää laittomiin tarkoituksiin ja ne voivat altistua tietomurroille. Saastunutta tietokonetta käytetään usein massiiviseen roskasähköpostin lähettämiseen muille käyttäjille tai tietomurtoihin ja palvelunestohyökkäyksiin muita järjestelmiä vastaan. Virustartunta voi siis pahimmillaan aiheuttaa joutumisen poliisitutkinnan kohteeksi.

Useat virukset asentavat saastuttamalleen tietokoneelle takaoven, jota kautta hyökkääjä pääsee käsittelemään kaikkea koneella olevaa tietoa.

Haittaohjelmat voivat kuluttaa kohdekoneen tai tietoverkon resursseja merkittävästi. Samalla ne muodostavat uhkan tietojen käytettävyydelle muuttamalla järjestelmän epästabiiliksi. Haittaohjelmat voivat hidastaa varsinaista toimintaa ja jopa estää sen.

Haittaohjelmat voivat olla uhka tietojärjestelmän sisällölliselle eheydelle. Ne voivat lisätä, muuttaa tai tuhota tietoja. Muutetut tai tuhotut tiedot voivat olla tärkeitä tietokoneen toiminnalle tai ne saattavat sisältää arvokasta informaatiota.

Eräät haittaohjelmat keräävät kohdekoneelta tiedostoja ja postittavat näitä uusille uhreille. Tiedostoissa saattaa olla hyvinkin arkaluonteista tietoa, joka tällöin leviää asiattomille tahoille.

2.5 Haittaohjelmien käyttötarkoituksia

Haittaohjelma voi toimia tietomurron apuvälineenä. Murtautujien kannalta kiinnostavia tietoja voivat olla esimerkiksi salasanat, käyttöoikeudet, luottokorttitiedot, turvamekanismit, henkilötiedot, patentit tai muut salassa pidettävät asiat.

Haittaohjelmia on myös käytetty massiivisiin palvelunestohyökkäyksiin valittua kohdetta vastaan.

Jotkut haittaohjelmat käyttävät kohdettaan massasähköpostitukseen, palvelunesto-hyökkäyksiin, tietomurtoihin tai muuhun laittomaan toimintaan.

Massamaiseen roskapostitukseen käytettävien haittaohjelmien takana on arveltu olevan ammattimaista liiketoimintaa.

Haittaohjelmia voidaan käyttää harhautuksena peittämään jotain muuta rikollista toimintaa luomalla hämminkiä.

Osa haittaohjelmista on tarkoitettu pelkkään kiusantekoon, vitsiksi tai maineen ja arvonannon saamiseksi omassa alakulttuurissa. Ammattitaitoisia ohjelmoijia on kuitenkin tarvittu edistyksellisimpien virusten luomisessa ja niitä on todennäköisesti kehitetty tiimityönä. Näitä haittaohjelmia käytetään usein taloudellisen hyödyn tavoitteluun.

Haittaohjelmien tekijöitä voivat olla niin kokeilunhaluiset nuoret kuin ammattirikollisetkin.

2.6 Haittaohjelmien sääntely

Useat lait ja asetukset sekä määräykset ja ohjeet asettavat viranomaisille velvoitteen arvioida haittaohjelmien riskejä ja eliminoida haittaohjelmia ja niiden seurauksia. Säädösten perusteella viranomaisille voi koitua myös oikeudellisia seuraamuksia, mikäli ne laiminlyövät haittaohjelmien torjunnan.

Keskeisiä voimassa olevia lakeja ovat rikoslaki, laki yksityisyyden suojasta televiestinnässä ja tulossa olevat sähköisen viestinnän tietosuojalaki sekä työelämän tietosuojalainsäädännön täydennys. Säädöksiä on laajalti kuvattu Valtion viranomaisen tietoturvallisuustyön yleisohjeessa VAHTI 1/2001.

Viranomaisella on velvollisuus torjua haittaohjelmat

Viranomaisen toiminnan julkisuudesta annetun lain (621/1999) mukaan viranomaisen on suunniteltava ja toteutettava tietohallintonsa samoin kuin ylläpitämänsä tietojärjestelmät ja tietojenkäsittelyn niin, että tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavoin ja tietoturvajärjestelyin ottaen huomioon haittaohjelmien tietojärjestelmille ja tietojenkäsittelylle aiheuttamat uhat.

Viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta annetun asetuksen (1030/1999) mukaan viranomaisen on hyvän tiedonhallintatavan toteuttamiseksi selvitettävä ja arvioitava haittaohjelmien uhat tietojärjestelmien turvallisuudelle sekä uhkien vähentämiseksi ja poistamiseksi käytettävissä olevat keinot ja niiden kustannukset sekä muut vaikutukset.

Rekisterinpitäjän on henkilötietolain (523/1999) perusteella suojattava henkilötiedot haittaohjelmien aiheuttamalta tietojen asiattomalta hävittämiseltä, muuttamiselta tai muulta käsittelyltä. Rekisterinpitäjän on toteutettava haittaohjelmien torjumisen ja poistamisen edellyttämät toimenpiteet siten, että ei perusteettomasti loukata käyttäjien yksityisyyttä.

Viranomaisen on sähköisestä asioinnista annetun lain (13/2003) § 5:n mukaan pyrittävä käyttämään asiakkaan kannalta teknisesti mahdollisimman yhteensopivia ja helppokäyttöisiä laitteistoja ja ohjelmistoja. Viranomaisen on lisäksi varmistettava riittävä tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa. Saman lain § 6:n mukaan viranomaisen tulee huolehtia siitä, että sen sähköiset tiedonsiirtomenetelmät ovat toimintakunnossa ja mahdollisuuksien mukaan käytettävissä muulloinkin kuin viraston aukioloaikana.

Viranomaisten on toimittava yhteistyössä haittaohjelmien torjumiseksi

Sähköisen viestinnän tietosuojaa koskevan lain (125/2003) mukaan viranomaisen, joka tilaajana hallinnoi käyttäjien liikennetietoja oman toimintansa mahdollistamiseksi, on huolehdittava palvelujensa ja käyttäjiensä tietoturvasta. Tietoturvan toteuttaminen on suhteutettava haittaohjelmien uhkien vakavuuteen.

Jos tietoturvaan kohdistuu erityinen uhka haittaohjelmien takia, viranomaisen on tilaajana saatava teleyritykseltä ja lisäarvopalvelujen tarjoajalta viipymättä ilmoitus siitä sekä haittaohjelmien uhan torjumiseksi käytettävistä toimenpiteistä. Lisäarvopalveluja tarjoavan viranomaisen on ilmoitettava Viestintävirastolle merkittävistä haittaohjelmien aiheuttamista tietoturvaloukkauksista sekä kerrottava toimista, joihin se on ryhtynyt haittaohjelmien johdosta.

Haittaohjelmien poistamiseen ja sen edellyttämiin toimenpiteisiin saa ryhtyä vain, jos toimet ovat välttämättömiä verkko- tai viestintäpalvelujen taikka viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi. Viestin sisältöön saa puuttua vain, jos on todennäköisiä syitä epäillä viestin sisältävän haittaohjelman tai ohjelmakäskyjen sarjan. Toimenpiteet on toteutettava huolellisesti ja luottamuksellisesti viestin ja yksityisyyden suojaa tarpeettomasti vaarantamatta.

Haittaohjelmien poistamisesta viesteistä on sovittava työnantajan ja työntekijän kesken

Mikäli toiminnan jatkuvuutta vaarantavien haittaohjelmien poistaminen ja levittämisen estäminen edellyttää työnantajan hakevan tai avaavan työntekijän sähköisen viestin, sovelletaan yksityisyyden suojaa työelämässä koskevaa lainsäädäntöä.

Yksityisyyden suojaa työelämässä säädellään lailla (477/2001), jossa sähköpostin valvonta kuuluu YT-menettelyn piiriin.

Yksityisyyden suojaa työelämässä koskevan lain täydentämishanke (HE 162/2003) mukaan työnantajan on suunniteltava ja järjestettävä työntekijälle tämän nimellä lähetettyjen ja tämän lähettämien sähköisten viestien suojaamisen edellyttämät toimenpiteet myös haittaohjelmien estämiseksi ja poistamiseksi.

Työnantajalla on oikeus tietojärjestelmän pääkäyttäjän valtuuksia käyttävän henkilön avulla ottaa selville, onko työntekijälle lähetetty tämän poissa ollessa tai onko työntekijä välittömästi ennen poissaoloaan vastaanottanut työnantajalle kuuluvia viestejä, jotka todennäköisesti sisältävät haittaohjelmia, jos työntekijän suostumusta ei voida saada kohtuullisessa ajassa ja asian selvittäminen ei kestä viivytystä. Tietojärjestelmän pääkäyttäjän valtuuksia käyttävä henkilö saa samoin edellytyksin avata toisen henkilön läsnä ollessa työntekijälle tulleen työnantajalle kuuluvan viestin. Tästä on informoitava työntekijää mahdollisimman pian.

Työntekijöihin kohdistuvan haittaohjelmia koskevan teknisen valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät kuuluvat yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin. Työnantajan on tiedotettava työntekijöille haittaohjelmia koskevan teknisen valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä.

Haittaohjelman tahallinen levittäminen ja perusteeton hallussapito on rangaistava teko

Rikoslain muuttamista koskevan ehdotuksen (OM 2003:3) mukaan henkilö, joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle tai tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle tuo maahan, valmistaa, myy tai muuten levittää taikka asettaa saataville sellaisen haittaohjelman tai ohjelmakäskyjen sarjan, joka on suunniteltu tai muunnettu ensisijaisesti vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa tai tietojärjestelmän suojauksen murtamiseen taikka levittää tai asettaa saataville haittaohjelman tai ohjelmakäskyjen sarjan valmistusohjeen, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, vaaran aiheuttamisesta tietojenkäsittelylle sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Henkilö, joka ilman hyväksyttävää syytä pitää hallussaan edellä tarkoitettua haittaohjelmaa tai ohjelmakäskyjen sarjaa, on tuomittava tietoverkkorikosvälineen hallussapidosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Viranomainen on myös oikeushenkilönä vastuussa haittaohjelmien aiheuttamasta vaarasta tietojenkäsittelylle tai haittaohjelmien hallussapidosta.

Sähköpostin viivästys

Kun haittaohjelmilta suojautumisessa ja niiden poistamisessa viivästetään sähköisten asiakirjojen perille tuloa tai muuten vaikutetaan siihen, sovelletaan sähköisestä asioinnista viranomaistoiminnassa annettua lakia (13/2003). Sähköinen viesti katsotaan lain 10 §:n mukaan saapuneeksi viranomaiselle silloin, kun se on viranomaisen käytettävissä vastaanottolaitteessa tai tietojärjestelmässä siten, että viestiä voidaan käsitellä. Mikäli viestin perille tuloa viivästetään, on varmistettava, että sille asetetut määräajat eivät tämän takia ylity.

Viranomaisen on lain 12 §:n mukaan viipymättä ilmoitettava lähettäjälle sähköisen asiakirjan vastaanottamisesta. Asiakirjan viivästäminen tai muu käsittely ei saa vaikuttaa ilmoittamiseen lähettäjälle sen vastaanottamisesta.

Lain 13 §:n mukaan kirjaus- tai muista vastaavista merkinnöistä on käytävä ilmi asiakirjan saapumisajankohta. Asiakirja ja sen saapumisajankohta on kirjattava siten, että asiakirjan viivästämisestä tai muusta käsittelystä riippumatta asioijan oikeudet varmistetaan.

Hyvin todennäköisesti viivästykset eivät kohdistu edellä esitettyihin viesteihin, mutta on kuitenkin huomioitava, että ohjeistus istuu esitettyihin normeihin ja organisaatioissa pitää tämä asia tiedostaa.

3. SUOJATTAVAT KOHTEET JA VALVONTA

Tietoteknisen ympäristön tulee olla ajanmukaisesti dokumentoitu sekä tarvittavat hallinta-, valvonta- ja muutosprosessit kuvattu. Tehtävän suorittamisesta vastaavat verkon ja laitteiden hallinnoinnista vastaava(t) henkilö(t) yhdessä organisaation tietoturvapäällikön tai tietoturvasta vastaavan henkilön kanssa.

Organisaation johto vastaa, että tietoturvariskit on kartoitettu ja niille on laadittu hallintasuunnitelmat ja toiminnan jatkuvuuteen liittyvät jatkuvuussuunnitelmat.

Tietoturvatilanteen valvonta on osa johdon tietoturvallisuuden tulosjohtamista.

3.1 Työasemat ja palvelimet

Työasemia (ml kannettavat) saa ylläpitää vain tehtävään nimetty tukiorganisaatio, joka on ohjeistettu ylläpitämään dokumentaatiota työsuorituksistaan sekä ilmoittamaan tietoturvavastaavalle tietoturvaa vaarantavat tekijät.

Kaikki sovellus-, tietokanta-, sähköposti- ja lähiverkon palvelimet kuten työasematkin (ml kannettavat) tulee varustaa haittaohjelman paljastamiseen kykenevällä ohjelmistolla.

3.2 Tietoverkko

Tietoverkon (organisaation lähiverkko ja käyttöpalvelun toimittajan lähiverkko) valvonnassa suositetaan käytettäväksi IDS-järjestelmää (**I**ntrusion **D**etection **S**ystem), joka automaattisesti hälyttää poikkeavasta toiminnasta. IDS ei tässä tarkoita välttämättä tuotetta, vaan se voi olla menetelmä, jonka avulla organisaatio voi seurata verkkonsa tilaa ja reagoida ongelmiin kuten hyökkäyksen havainnointi tai sen esto.

Organisaation lähiverkko on suojattava ulkoisista yhteyksistä teknillisillä ratkaisuilla. Yksi käytetyin menettelytapa on rakentaa eri paikoissa sijaitsevien verkkojen

liittymäpisteisiin haittaohjelmatorjunnalla varustettu palomuuri ja käyttää reitittimen turvallisuusominaisuuksia.

3.3 Mobiililaitteet

Matkaviestimiä ja PDA-laitteita (**P**ersonal **D**igital **A**ssistant) saavat ylläpitää vain tehtävään nimetty tukiorganisaatio. Laitteet on varustettava samoilla haittaohjelmien torjuntatuotteilla kuin kannettavat työasemat sekä muistin salauksella ja tulevaisuudessa laitekohtaisella palomuurilla.

Käyttäjille on annettava riittävä koulutus laitteiden turvallisesta käytöstä ja teknilliselle henkilöstölle niiden haavoittuvuuksista ja käyttöjärjestelmissä olevista tietoturva-aukoista siten, että luvaton tunkeutuminen laitteelle voidaan estää.

Älykkään puhelimen arkkitehtuuri on hyvin lähellä työaseman rakennetta. Laitteessa on jatkuva yhteys ja siksi siitä on tulossa houkutteleva kohde haittaohjelmille, jotka voivat levitä esimerkiksi pelien välityksellä, ladattavissa soittoäänissä tai logoissa. Haittaohjelma voi hyödyntää myös laitteen turvatonta oheislaiteyhteyttä. Merkittävä riski on laitteen Internet-toiminnot ja synkronointi organisaation käytössä olevaan työasemaan.

4. TOIMENPITEIDEN ORGANISOINTI JA TORJUNTAPROSESSI

4.1 Tietoteknisen ympäristön hallinta ja tietotekninen valvonta

Tärkeintä haittaohjelmien torjunnassa on huolehtia, että torjunnan kerroksellisuus kuten torjuntaohjelmistot, työasemien asetukset, selainten asetukset, automaattiset päivitykset, tietoverkon segmentointi ja henkilöstön koulutus on hoidettu ja niiden ajantasaisuutta valvontaan.

4.1.1 Organisointi

Tietoteknisten järjestelmien hallinnasta ja valvonnasta tulee sopia kirjallisesti järjestelmien omistajien ja järjestelmiä valvovan ja hallinnoivan organisaation kesken. Riippuen organisaation ohjausmallista (esimerkiksi konserni) on sopimusta käytettävä eri sisäisten organisaatio-osien kesken ja aina jos organisaation sisäverkon ylläpitopalvelut on ulkoistettu.

Toteutuksen tulee sisältää sekä järjestelmähallintatoiminnot että tietoturvallisuuden valvonnan. Nämä toisiaan tukevat toiminnot, joissa voidaan ristiin hyödyntää käytettäviä hallinta- ja valvontajärjestelmiä sekä henkilöstön ammattitaitoa, muodostavat yhden toisiaan tukevan toiminnon, joka tulee huomioida toimintaa organisoitaessa.

4.1.2 Hallinta ja valvontatehtävien suorittaminen

Tavoitteena on turvata tietoteknisten järjestelmien palvelut mahdollistamalla tietoturvallisuuden valvonta ja mahdollinen tapahtumiin reagointi ja tarvittavat korjaukset sekä ohjata teknisiä korjaustoimenpiteitä ja muutoksenhallintaa.

Tietoteknisen ympäristön valvonnan ja hallinnan teknisen ja organisatorisen toteutuksen on kyettävä tuottamaan organisaatiolle tilannekuva tietoteknisen ympäristön käytettävyydestä ja tietoturvatilanteesta.

Tietoturvallisuuden valvonta sekä järjestelmähallinta- ja valvontaprosessit on määriteltävä ja kuvattava. Mikäli organisaation tietoturvallisuutta tai järjestelmiä valvovaan tekniseen toteutukseen tunkeudutaan, on tunkeutujalla erinomainen mahdollisuus aiheuttaa erittäin merkittävää vahinkoa kohdeorganisaatiolle. Tästä syystä sekä tietoturvallisuus- että järjestelmien hallinta- ja valvontatoteutusten suojaamiseen on kiinnitettävä erityistä huomiota.

Valvonta- ja hallintatoimeen osallistuvan henkilöstön on tinkimättä noudatettava organisaation turvallisuusohjeistusta.

4.1.3 Yleinen verkon ja laitteistojen tietoturvan valvonta

Keskitetysti hallittavien tietoteknisten laitteiden ja järjestelmien osalta tulee laatia tarvittava ohjeistus käyttötunnusten ja salasanojen vaihtorutiineiden ja jakelumenetelmien osalta. Niissä hallinta- ja valvontajärjestelmissä, missä on mahdollisuus useampaan salasanaan, tulee olla määritelty hallinta- ja valvontaorganisaation käyttöön sekä asiantuntija- että käyttösalasana.

Asiantuntijasalasana ei saa olla päivittäisessä käytössä ja se on tarkoitettu vain asiantuntijoiden tietoon. Asiantuntijasalasanalla on käytettävään hallinta- tai valvontajärjestelmään laajemmat oikeudet kuin käyttösalasanalla. Mikäli on epäiltävissä, että joku hallinta- tai valvontajärjestelmän salasana on vuotanut ulkopuolisten henkilöiden tietoon, tulee salasana vaihtaa välittömästi.

> Työasemia ylläpitää tehtävään nimetty tukiorganisaatio. Käyttöympäristön tulee olla mahdollisimman pitkälle vakioitu. Tietoteknisen ympäristön tulee olla ajanmukaisesti dokumentoitu sekä tarvittavat hallinta-, valvonta- ja muutosprosessit kuvattuna.

Laajoissa organisaatioissa on tarkoituksenmukaista luoda tietoturvan hallinnoinnin prosessinohjausjärjestelmä. Sen toteutustavasta riippuen siihen on mahdollista integroida mm. seuraavia tietoturvallisuuden valvonnan kannalta oleellisia toimintoja:

- Käyttäjähallinta
- Vikaraportointi
- Tietoturvaloukkausepäily- ja raportointilomakkeet
- Työnohjaus ja raportointi

- Tietoteknisen tilanteen seuranta- ja esitysjärjestelmä:
    1. Haittaohjelmahavainnot
    2. Vikatilanne
    3. Tunkeutumisen havainnointi

Prosessinohjausjärjestelmää luotaessa tulee kiinnittää erityisesti huomiota järjestelmän tekniseen toteuttamiseen, sillä siihen tunkeutuminen saattaa mahdollistaa vastatoimenpiteiden edistymisen seurannan ja tapahtumatietojen väärentämisen.

4.1.4 Turvallisuustason selvitysohjelmistojen hallittu käyttö

Luvan turvallisuustason selvitysohjelmistojen käyttöön myöntää tietoturvallisuuden valvonnasta vastaava organisaatio. Käytettäessä kyseisiä ohjelmia tulee niiden ominaisuudet ja toiminta testata ensin suljetussa testiympäristössä ennen niiden käyttöä tuotantoympäristössä.

4.1.5 Hankinnat ja ulkoistetut käyttöpalvelut

Kokonaisvastuu toiminnoista ja tietoturvallisuudesta säilyy virastolla ulkoistuksesta huolimatta, vaikka palveluntoimittaja vastaa virastolle tuottamistaan palveluista sovituilta osin. Tämä koskee myös haittaohjelmien torjuntaa.

Hyvän tietoturvallisuustason saavuttaminen ja säilyttäminen virastoissa ja laitoksissa edellyttää omaa tietoteknistä osaamista, selkeää organisointia ja vastuuttamista sekä toimivaa viraston ja toimittajan välistä työnjakoa. Tähän liittyy sopimuksen kautta mahdollisuus varmistua, että palvelun toimittajan toimintaprosessit haittaohjelmien torjunnassa ovat kunnossa ja täyttävät viraston asettamat vaatimukset.

Palveluntoimittajan toimittamaan palveluun liittyviä tietoturva-asioita on seurattava säännöllisesti palvelun seurantaryhmässä osana johdon tarvitsemaa tietoturvallisuuden tilannekuvaa.

Hankittaessa organisaation käyttöön tuotteita haittaohjelmien torjuntaan on ensisijaisesti hyödynnettävä valtiovarainministeriön ja Hanselin puitesopimuksia kokonaisedullisuuden saavuttamiseksi. Tällöin tuotteiden vertailua ja kilpailutusta ei virasto- ja tuotekohtaisesti ole tarpeen suorittaa.

Ulkoistamiseen liittyviä tietoturva-asioita on kuvattu laajemmin VAHTI-ohjeessa 2/1999 (Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuus).

4.2 Torjunnan suunnittelu ja toiminnan jatkuvuuden varmistaminen

Organisaation tulee olla varautunut eri tilanteita, kuten esimerkiksi haittaohjelmien torjuntaa varten määrittämällä ja toteuttamalla tarvittava ohjeistus sekä suunnittelemalla ja harjoittelemalla tarvittavat toimintamallit.

Poikkeamat voidaan luokitella esimerkiksi seuraavasti:

1. Henkilöstöuhka
2. Fyysinen turvallisuusuhka
3. Toiminnan jatkuvuuden vaarantava uhka

Haittaohjelmat ovat yksi toiminnan jatkuvuuden vaarantava uhkatekijä. Toiminnan jatkuvuussuunnittelun tulee huomioida kyseiset tietoturvaan kohdistuvat uhat. Haittaohjelmiin reagoimiseksi nopeasti on määritettävä etukäteen organisaatiokohtaisesti tarvittavat tehtävät ja niiden toteuttajat.

Suunnitellut toimintamallit tulee testata käytännössä ja niitä on harjoiteltava säännöllisesti. Tietoturvahäiriöihin voidaan varautua laatimalla taulukko, johon on kuvattu organisaatiossa tehtävät toimenpiteet sekä niiden suorittajat.

Liitteessä yksi on esimerkki vastuutaulukosta haittaohjelmatapauksessa. Kyseinen taulukko on esimerkki ja kussakin organisaatiossa on erikseen määritettävä tarvittavat vastuut ja tekijät välittömien järjestelmällisten torjunta- toimenpiteiden käynnistämiseksi.

Organisaation luoma reagointimalli on testattava sen toimivuuden varmistamiseksi käytännössä ja harjoiteltava säännöllisesti.

4.3 Havainnosta torjuntaan

Havainto haittaohjelmasta voi tulla organisaatiolle ennen kuin virustorjuntaa tuottava yritys on siitä antanut varoituksen tai saanut valmiiksi ohjelmisto-päivityksen, jolla torjunta voidaan suorittaa. Näissä tapauksissa voi olla hyödyllistä käynnistää toimenpiteet, joilla voidaan viivästyttää esimerkiksi sähköpostiliikennettä.

Toimenpide on perusteltu, koska haittaohjelma voi keskimäärin olla kahdesta kolmeen tuntia liikkeellä sähköpostin liitteinä ennen torjuntapäivitysten saapumista.

Esimerkki haittaohjelman torjuntaprosessista on kuvattuna liitteessä kaksi. Torjuntaprosessin vaiheet on kuvattu myöhemmissä kappaleissa.

4.3.1 Haittaohjelman havaitseminen

Haittaohjelmasta tulevat havainnot organisaation tietohallintoon automaattisesti käytettävien tuotteiden antaman tiedon perusteella. Jos laite ei ole kytketty organisaation verkkoon ja tartunta on saatu esimerkiksi siirrettävän tiedontallennusvälineen kautta, saadaan tieto yksittäisen käyttäjän toimittamana tietona.

4.3.2 Tilanneanalyysi ja reagointiaika

Organisaation tietohallinto tai palvelun palvelinvastaava (organisaatiokohtaisesti sovittava henkilö) ilmoittaa havainnoista etukäteen sovitun menettelyn mukaisesti ja ryhtyy toimenpiteisiin joilla voidaan rajoittaa vahinkojen vakavuutta. Menettelyt kohdistuvat tietoverkkoon ja palvelimiin. Reagointiaika on lyhyt ja moni toiminta pitää käynnistää ilman, että odotetaan paikalle muita päätöksentekijöitä kuin mikrotuen päivystäjä.

4.3.3 Haittaohjelmatapauksen käsittely

Analysoitaessa haittaohjelmatapauksen vakavuusastetta, on huomioitava useita vaikuttavia tekijöitä. Määritettäessä tapahtuman vakavuutta ja oikeaa toimintatapamallia, tulee valvovan organisaation määrittää vastaukset alla lueteltuihin kysymyksiin:

- Miten laaja tapahtuma on?
- Mikä on sen vaikutus toimintakykyyn ja operatiivisiin järjestelmiin?
- Kuinka vaikeaa on rajoittaa tapahtumaa?
- Miten nopeasti tapahtuma laajenee?
- Mikä on sen arvioitu taloudellinen vaikutus?
- Mikä on sen arvioitu vaikutus organisaation julkisuuskuvaan?

Alla olevassa taulukossa on kuvattu esimerkki vakavuusluokittelusta, jota voidaan käyttää apuna tarvittavien vastatoimenpiteiden määrittelyssä.

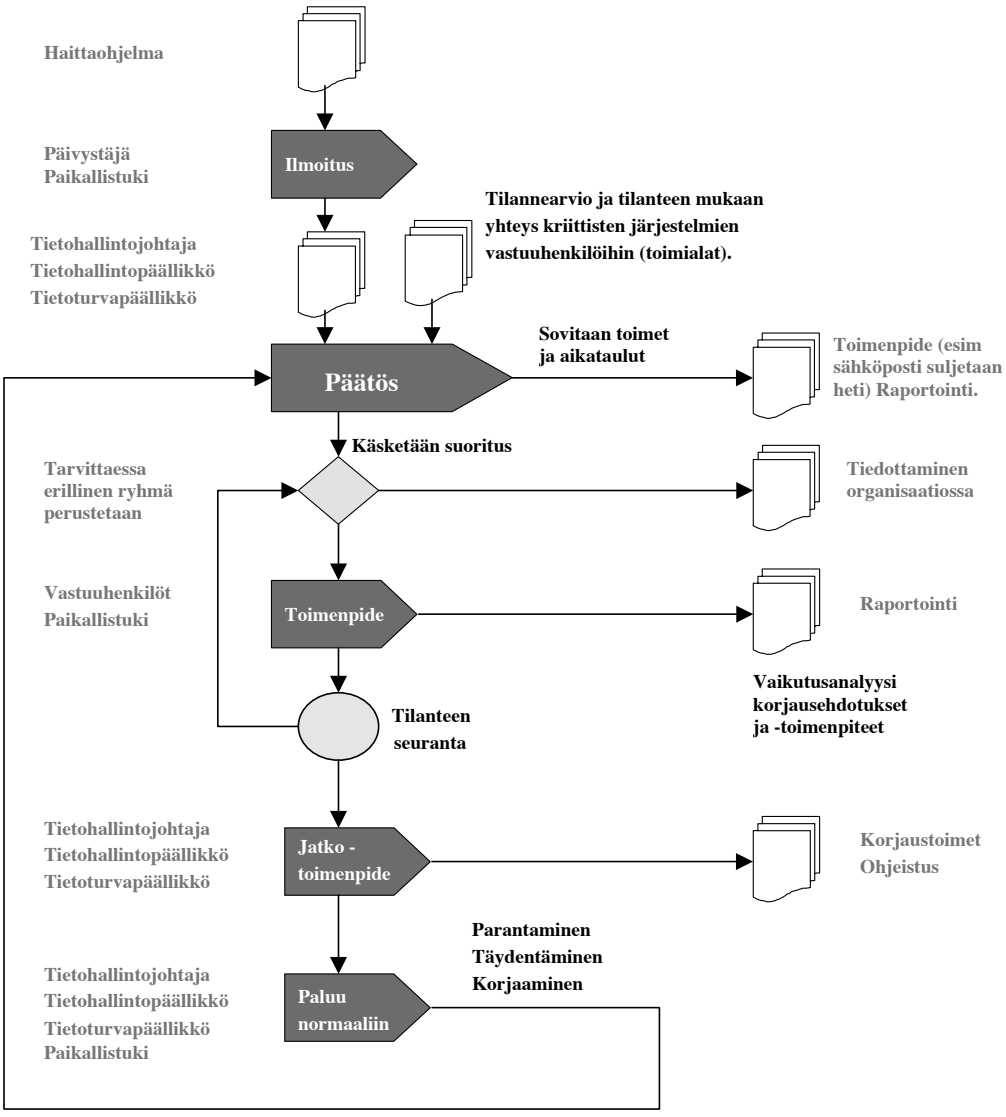
Vakavuusluokka / -vaikutus	**Kuvaus**
0 Normaalitilanne	Normaalitilanne, ei poikkeamia
1 Alhainen / haittaava	Tapahtuma, jonka **vaikutus on pieni**. Esimerkiksi virustartunta on eristetty yhteen työasemaan, yksittäisessä sovelluksessa on tilapäinen käyttökatkos, lyhytaikainen tietoliikennekatkos jne.
2 Keskinkertainen / rajoittava	Tapahtuma, jonka **vaikutus on merkittävä**. Esimerkiksi toimintahäiriö, joka vaikuttaa eri organisaatioiden toimintaan tai jonka arvioidaan ylittävän sovitun / sallittavan käyttökatkosajan. Tällaisia ovat kaikki tietoliikenne- sähköposti ja kriittisten sovellusten katkot, joiden kestoaika tiedetään tai on ennalta arvioitavissa. Haittaohjelmien toiminta, joka häiritsee tai estää yksittäisen työaseman käyttöä tai henkilön työn suorittamista.
3 Korkea / estävä	Tapahtuma, jonka **vaikutus on vakava**. Esimerkiksi kaikki operatiivisten sovellusten häiriöt sekä kriittisten järjestelmien häiriöt, jotka ylittävät tai arvioidaan ylittävän sallitun käyttökatkoksen ajan tai joiden käyttökatkos aikaa ei tiedetä. Haittaohjelmat, joiden vaikutusaluetta ei kyetä rajaamaan tai tilanteet, joissa eri järjestelmien tietojen oikeellisuus on vaarassa tai tiedot voivat joutua sellaisten henkilöiden haltuun, jotka eivät ole niihin oikeutettuja.

Vakavuusluokaltaan korkeiksi (luokka 3) luokitellaan mm. seuraavat tapahtumat:

- Toiminnan estävät, operatiivisiin tietojärjestelmiin vaikuttavat katkokset.
- Tietoliikenneverkkojen infrastruktuuriin, kuten nimipalveluihin ja runko verkkoon kohdistuvat hyökkäystilanteet sekä niiden yritykset.
- Automaattiset ja laajalle levinneet infrastruktuuriin tai Internet sivustoille kohdistuvat hyökkäystilanteet sekä niiden yritykset.

- Televerkkoon, kiinteään tai liikkuvaan, kohdistuvat vakavat hyökkäykset sekä niiden yritykset.
- Uudentyyppisten (=ei tunnettujen) hyökkäystapojen havainnot tai niiden yritysten havainnot.

Haittaohjelman torjuntaprosessi



4.4 Korjaus- ja jälkitoimenpiteet

Kaikki korjaus- ja jälkitoimenpiteet on suunniteltava huolellisesti osana kuvan yksi toimintaprosessia.

Tiedostetut aukot on korjattava ja tarvittavat kehittämistoimet toteutettava ennen järjestelmän uudelleen käyttöönottoa. On pyrittävä siihen, ettei samaa haavoittuvuutta voida hyödyntää uudelleen. Turvallisuusprosesseissa ilmenneet puutteet on korjattava.

Tapahtuma on aina analysoitava. Analysoinnin yhteydessä on vakavien tilanteiden sattuessa arvioitava toipumissuunnitelmien toimivuus. Mikäli epäillään, että tietojen eheys on vaarantunut, on varmistukset tarkastettava ja palautettava tiedot tapahtumaa edeltäneeseen tilanteeseen.

4.5 Haittaohjelmiin liittyvä tiedottaminen ja raportointi osana valvontaa

Tiedottamisen kolme tasoa:

1. Sisäinen tiedottaminen
Kohderyhmänä ovat organisaation omat työntekijät.

2. Ulkoinen tiedottaminen
Kohderyhmänä ovat mm. asiakkaat ja julkinen sana. Ulkoisessa tiedottamisessa otetaan huomioon oman organisaation eri sisäiset toimijat, alihankkijat, joukkoviestimet ja operaattorit.

3. Eri viranomaiset
Viranomaisten välinen tiedottaminen, kuten esimerkiksi rikosilmoitusten tekeminen tai yhteistyö Viestintäviraston kanssa tarvittavien CERT-FI:n (**C**omputer **E**mergency **R**esponse **T**eam – **F**icora) luomien tilanneilmoitusten seuraamiseksi tai kansallista turvallisuutta uhkaavien havaintojen ilmoittamiseksi CERT-FI:lle.

Merkittävistä tapauksista tulee ilmoittaa valtion tietoturvaohjauksesta vastaavalle (VM/HKO, valtiovarainministeriön hallinnon kehittämisosasto). Kaikista tapauksista tulee informoida ainakin niitä henkilöitä, joiden toimintaan tapahtuma vaikuttaa.

Tapahtuman vakavuusluokan mukaisesti tiedotetaan vaikutuksen kohteena olevil-le henkilöille ja yksiköille toimenpiteistä, vaikutuksista ja palautumisen tilanteesta. Mikäli organisaatiossa on tiedotuksesta vastaava yksikkö, niin sitä tulee informoida tarvittaessa vakavuusluokaltaan korkeista tapahtumista sekä kaikista tapahtumista,

joista haittaohjelmien aiheuttamista ongelmista on mahdollista näkyä toiminnassa organisaatiosta ulospäin. Luonteeltaan toteutetun viestinnän tulee olla informoivaa, ohjaavaa, ohjeistavaa ja rauhoittavaa. Tiedottamisen tulee tapahtua ennen väärien tietojen leviämistä.

Tietoturvallisuuden valvonnasta vastaavan organisaation osan toteuttaman tiedottamisen tarkoitus on pitää sekä tiedottamisesta vastaava että oma organisaatio tietoisena tosiasioista ja tehdyistä toimenpiteistä.

4.6 Kustannukset ja niiden mittaaminen

Haittaohjelmien aiheuttamat kustannukset jakaantuvat kahteen pääluokkaan: seuraukset haittaohjelmatartunnoista, johon kuuluvat menetetty työaika ja paljastuneen tiedon arvo sekä haittaohjelmien torjuntatyön kustannukset.

Tartunnan aiheuttamien kustannuksien laskeminen on vaikeaa. Useimmat työsuoritteet ovat enemmän tai vähemmän sidoksissa atk-laitteistoon. Mikäli työasemaa tai verkkoa ei voi käyttää, työteho alenee tai pahimmillaan työnteko estyy hetkellisesti kokonaan.

> Jos työsuoritus on kokonaan riippuvainen atk-laitteiston käytettävyydestä, esimerkiksi 300 käyttäjän menetetty työaikakustannus on luokkaa 100 €/min.

Käytännössä atk-käyttökatkon vaikutus riippuu sen hetkisestä työvaiheesta ja mahdollisuudesta suorittaa tuottavaa työtä muin välinein.

Samalla tavoin voidaan laskea, että haittaohjelmatorjunta käyttäjien itsensä suorittamana tulee nopeasti erittäin kalliiksi, jos jokainen käyttäjä joutuu tekemään aktiivisia toimenpiteitä esimerkiksi 15 minuutin verran ennen kuin omaa työtä voidaan jatkaa.

Haittaohjelmatartunnan muut seuraukset ovat vielä vaikeammin ennakolta mitattavia. Haittaohjelma, joka lähettää satunnaisia kiintolevylle talletettuja tiedostoja postiliitteinä, voi aiheuttaa vakavia taloudellisia tai muita vahinkoja, jos tiedosto sisältää salassa pidettäviä tietoja, joiden paljastuminen sivullisille voi aiheuttaa korvausvastuun. Hyvä tiedonhallintatapa edellyttää, että tämän tyyppisiä vahinkoja vastaan tulee varautua ennalta, mutta haittaohjelmien nopea kehitys voi edelleen aiheuttaa tilanteita, missä kohtuullisen hyvänäkään pidettävä ennaltaehkäisy ei riitä estämään vahingon syntymistä.

Keskitetyn haittaohjelmatorjunnan kustannukset on helpompi laskea, koska kyseessä on ylläpito- ja tukihenkilöstön mitattavissa oleva työpanos sekä erilliset ohjelmisto- ja laitteistohankinnat:

- Torjuntajärjestelmien hankinta- ja ylläpitokustannukset
- Torjuntajärjestelmien ylläpitoon, jatkuvaan torjuntatehon analysoimiseen ja kehittämiseen käytetty työaika
- Haittaohjelmien poistamiseen ja toimintakyvyn palauttamiseen käytetty työaika (yksittäiset työasemat)
- Verkko- ja työasemaylläpidon käyttämä työaika saastuneiden työasemien eristämiseen ja verkkoliikenteen (ml. sähköpostiliikenne) turvaamiseen

Torjuntajärjestelmien hankesuunnittelussa on aina pyrittävä tekemään luotettava ja totuudenmukainen arvio sen ylläpitämiseen kuluvista henkilötyömääristä. Usein ne mitoitetaan optimistisen alhaisiksi ja nykyisessä kiivaasti kehittyvien ja laajalle automaattisesti leviävien haittaohjelmien ympäristössä muuhun verkko- ja työasemaylläpitoon käytettävissä oleva työaika kärsii.

5. KUINKA VÄLTTÄÄ TARTUNTA

5.1 Työaseman turvalliset asetukset

5.1.1 Työaseman BIOS tason suojaukset

Työaseman turvaaminen aloitetaan vaikuttamalla työasemaan tekemällä BIOS-asetuksiin (Basic Input/Output System) tiedonsiirtoon liittyvät turvallisuutta lisäävät rajoitukset.

Näistä kriittisimpiä ovat ilmarajapintaa hyödyntävät

- WLAN (**W**ireless **L**ocal **A**rea **N**etwork),
- Bluetooth (Lyhyen matkan radiotaajuudella toimiva avoin tiedonsiirto-protokolla laitteiden väliseen tiedonsiirtoon tai laitteiden liittämiseen Internettiin) ja
- IR-portti (**I**nfra **R**ed Led, punaista valoa käyttävä pulssilähetys).

Myös sisäinen modeemi ja verkkokortti mahdollistavat haittaohjelmien helpon pääsyn työasemaan. Sarjaportin, rinnakkaisportin ja USB-portin (**U**niversal **S**erial **B**us) käyttö on myös harkittava kukin erikseen, sillä näiden kautta voidaan kytkeytyä työasemaan.

Kannettavan työaseman käynnistys on aina suojattava salasanalla. Se voidaan toteuttaa työasemassa olevalla nk. turvapaneelilla, kiintolevyn salakirjoitus-ohjelmaan kuuluvalla käynnistyssalasanalla tai BIOS-asetuksista löytyvällä koneen käynnistyssalasanalla. Vasta salasanan syöttäminen käynnistää tietokoneen käyttöjärjestelmän ja antaa käyttäjälle kirjautumisikkunan.

Jos kannettavan kiintolevyä ei ole salakirjoitettu, on se suojattava BIOS-asetuksista löytyvällä kiintolevyn suojaussalasanalla. Menettely estää levyn käytön toisessa samanlaisessa koneessa.

Työaseman käynnistys (boot) on sallittava vain kiintolevyltä. Jos tähän turva-asetukseen on jostain syystä tehtävä kevennyksiä, suositellaan käynnistys-järjestykseksi: kiintolevy, cd-rom, muut siirrettävät mediat (levyke tai USB-laitteet).

BIOS-asetuksista kannattaa kytkeä pois mahdollinen Bluetooth, mikäli kyseinen ominaisuus laitteesta löytyy, eikä se ole käytössä.

BIOS-asetuksilla on estettävä verkkokortin etäkäynnistys, WOL (**W**akeup **O**n **L**AN) –ominaisuus. Eräistä BIOS-asetuksista löytyy myös työaseman kannen aukaisuilmaisin. Tämä, kuten monta muutakin BIOS-asetusta on syytä ottaa hallitusti käyttöön.

Kaikki BIOS-tason asetukset on suojattava muutoksilta salasanalla, jota ei saa antaa loppukäyttäjälle.

5.1.2 Työaseman perusasetukset

Turvallisuuden kannalta merkittävää on, että loppukäyttäjälle ei anneta kuin perusoikeudet työaseman käyttöön. Työasemien tietoturvakäytännöt on otettava käyttöön keskitetysti.

Työasemien turvallisuutta parannetaan käyttämällä asennuksissa vakioituja ympäristöjä joissa on käytössä viimeisimmät korjaussarjat ja turvapäivitykset. Apuohjelmistojen versioista pitää käyttää uusimpia versioita, joiden turva-aukot on tukittu. Työasemien turvapäivityksissä on hyödynnettävä automaatti-toimintoja. Päivitykset on mahdollisuuksien mukaan hoidettava keksitetysti ja valvotusti.

Työasemassa voidaan estää esimerkiksi Visual Basic Scriptien suorittaminen poistamalla Wscript.exe ohjelman suorittaminen. Perusasetuksissa karsitaan pois turhat ohjelmat (esimerkiksi messenger.exe ja msnmessenger.exe), jotka hyödyntävät HTTP (**H**ypertext **T**ransfer **P**rotocol) liikenteessä porttia 80. Muita poistettavia ohjelmia voivat olla ftp.exe, tftp.exe, debug.exe, at.exe, edlin.exe ja format.com.

Kaikissa työasemissa on oltava asennettuna virustorjuntaohjelmistot ja virustunnisteiden päivittyminen automaattisesti siten, että loppukäyttäjä ei voi näihin vaikuttaa.

Työasemissa on käytettävä ohjelmallista palomuuria, joka estää ohjelmien suorittamisen sekä kerää lokia. Uusimmat madot eivät kopio itseään kovalevylle, eikä niitä näin ollen löydetä kovalevyskannauksella. Lokitiedot ovat tarpeellisia mahdollisten haittaohjelmaepidemioiden selvittelyn kannalta. Palomuurien, kuten virustorjuntaohjelmienkin hallintaan on syytä hankkia keskitetty hallintatyöväline ja estää käyttäjää tekemästä sääntöihin muutoksia. Käyttäjällä ei saa antaa työasemissa (ml kannettavat) local admin-oikeuksia.

5.1.3 Selaimen turva-asetukset

Uusimmat haittaohjelmat ovat ottaneet yhdeksi leviämiskanavakseen selainten tietoturvattomuuden. Selaimista löytyy usein myös kriittisiä tietoturva-aukkoja, joiden

päivittäminen on tärkeää. Käyttäjät eivät valitettavasti tiedosta tarpeeksi, miten haavoittuvia selaimet ja Internetissä surffaaminen ovat.

Selaimen turvallisissa asetuksissa kannattaa lähteä sivustojen luokittelusta erilaisiin vyöhykkeisiin. Selaimet pitävät sisällään monenlaisia staattisia ja dynaamisia elementtejä. Koska näiden liikkuvien, komentokieltä hyödyntävien objektien tietoturvallisuutta ei aina voi varmistaa, pitää niihin suhtautua kielteisesti. Useat sivustot on kuitenkin laadittu siten, että ilman näitä ominaisuuksia ne ovat usein käytettävyydeltään heikkoja.

Seuraavassa on tarkasteltu vyöhykeajatusta yleisimmin käytössä oleva Microsoft Internet Explorer-selaimen kannalta:

- Internet-vyöhyke
- Intranet-vyöhyke
- luotetut sivustot
- kielletyt sivustot

Internet-vyöhyke on sellainen, jossa lähteisiin ei luoteta. Tällöin joudutaan estämään mahdollisesti haitallisten koodien suorittaminen, koska ei voida olla varmoja, mitä komentoja sivustoihin sisältyy. Näiltä sivustoilta ei myöskään oletusarvoisesti saa antaa loppukäyttäjän ladata minkäänlaisia tiedostoja.

Intranet vyöhykkeellä surffaillessa liikutaan viraston omilla, turvallisilla palvelimilla. Näihin on usein ohjelmoitu sellaisia palveluja, jotka hyödyntävät ajonaikaisen koodin suorittamista. Näitä ei ole syytä asetuksilla estää, koska niitä tarvitaan usein tiettyjen toimintojen suorittamiseksi.

Suurin osa Internetin sivustoista on kuitenkin turvallisia. Nämä sivustot pitää vain jollain tavalla käyttäjän toimenpitein kertoa selaimelle turvallisiksi. Tätä varten Explorerissa on mahdollisuus käyttää luotettujen sivujen luetteloa. Tämän vyöhykkeen asetukset voivat käytännössä olla melkein yhtä korkeat avoimuudeltaan kuin Intranet-vyöhykkeen. Sivujen määrittely vain usein jää loppukäyttäjän päätettäväksi, koska keskitetyn luotettavien sivustojen listan ylläpito osoittautuu työmäärältään liian suureksi.

Selaimessa on myös mahdollista määritellä tietyt sivut kiellettyjen listoille, mutta tässäkin törmätään usein ylläpidon vaikeuteen. Sivustojen kieltäminen onkin syytä suunnitella ja toteuttaa viraston proxy-palvelimella (välityspalvelin) tai palomuurilla.

Selaimen turva-asetuksissa kannattaa huomioida, että IE 6 (**I**nternet **E**xplorer) SP 1 (**S**ervice **P**ack) ja Exchange 2003 osaavat poistaa suojatut OWA-sivut (**O**utlook **W**eb **A**ccess) välimuistista käytön jälkeen.

Selaimen turvallisista asetuksista on tämän ohjeen liitteenä taulukko. Seuraavalta sivulta http://www.niscc.gov.uk löytyy NISCC (National Infrastructure Security Co-

ordination Centre) julkaisu 5/2003 ”Configuration and Use of Web browsers”. Julkaisusta löytyy yleisimpien selainten Microsoft Internet Explorerin, Netscapen ja Operan turvallisuuteen vaikuttavia asetuksia.

5.1.4 Sähköpostin turva-asetukset

Sähköpostiohjelmassa ei tulisi suosia postin katselua html-muodossa (**H**yper**T**ext **M**arkup **L**anguage).

Postiohjelma käyttää tällaisen postin näyttämiseen työaseman selainsovellusta, jossa olevat turvallisuusaukot mahdollistavat haitallisen koodin suorittamisen ilman käyttäjän toimenpiteitä. Jos käyttäjällä on avoinna postin esikatseluruutu, html-kieleen sisältyvä komento suoritetaan jopa ilman postin avaamista. Tällainen esikatselu on mahdollisuuksien mukaan keskitetysti estettävä tietohallinnon toimenpitein. On lisäksi huomattava, että tällä tavalla leviävät haittaohjelmat eivät käytä leviämiseen edes liitetiedostoa.

Sähköpostin viivästäminen yhdyskäytävässä ja/tai palvelimella on yksi keino torjua sähköpostiliikenteen mukana tulevat haittaohjelmat unohtamatta lähtevän sähköpostin tarkistusta haittaohjelman varalta. Valitettavasti uusien haitta-ohjelmien leviämisnopeus on jo ylittänyt niiden tunnisteiden toimitusnopeuden. Sähköpostin tallentaminen karanteenialueelle parantaa kykyä tunnistaa mahdollisesti liikenteen mukana tulevat haittaohjelmat.

Sähköpostiliikenteestä suurin osa ei sisällä liitetiedostoja. Tätä osuutta ei tarvitse viivästyttää, jolloin suuri osa postista liikkuu mahdollisimman reaaliajassa. Viivästystä voidaan käyttää viraston sisäisessä liikenteessä ja luotettavaksi todettujen muiden tahojen postille. Viivästetyn postin osalta tarkastetaan määräaika organisaatioon tulon osalta.

Liitetiedostojen käsittelyssä on syytä tehdä luokittelu tiedostotyyppien perusteella. Sähköpostin välitys/suodatusohjelmien on syytä kyetä tekemään luokittelu tiedoston otsikkotietojen eikä tiedoston tarkentimen perusteella. Sallitut tiedostotyypit ovat sellaisia, joita ei ole todettu sillä tavalla vaarallisiksi, että niitä olisi syytä viivästyttää. Ne ovat yleensä normaaleja työtiedostoja, joille tietenkin tehdään normaalit virustarkastukset.

Toiseksi luokitteluryhmäksi on määritelty sellaiset tiedostot, jotka ovat suoraan ajettavia, hyvin suurella todennäköisyydellä haittaohjelmien käyttämiä tiedostotyyppejä. Nämä kaikki on poistettava sähköpostiliikenteestä, tulevat ne sitten virastoon tai lähtevät virastosta ulospäin. Poikkeuksen muodostaa jälleen kerran luotettavat tahot, joille voidaan luoda tarvittaessa omia sääntöjä. Posti välitetään siis ilman liitetiedostoja vastaanottajalle, jolloin vastaanottajalle voidaan laittaa ilmoitus, jossa kerrotaan liitetiedoston poistamisesta turvallisuuteen vedoten.

Pakatut tiedostot muodostavat oman ryhmänsä. Tähän kuuluvat kaikki sellaiset tiedostomuodot, jotka pakkaavat yhteen pakettiin yhden tai useamman tiedoston. Sähköpostiliikenteen analysointiohjelmat kykenevät avaamaan tällaiset paketit ja ikään kuin kurkistamaan mitä tiedostoja ne pitävät sisällään. Sähköpostin käsittelyssä käytetään tämän jälkeen paketin sisältä löytyvien tiedostojen mukaista käsittelypolitiikkaa. Salasanalla suojatut pakatut tiedostot on aina laitettava karanteeniin.

Karanteeniin laitetaan kaikki loput sähköpostit. Ne ovat siis tulleet ei-luotetulta taholta, eivät pidä sisällään liitteinä sallittuja tiedostotyyppejä, eivätkä kuulu kiellettyihin tiedostoihin. Karanteeniajan eli viivästysajan jälkeen tältä alueelta voi käyttäjä erikseen niin halutessaan saada postinsa. Tänä aikana työaseman virustunnisteet ovat toivon mukaan ajan tasalla. Jos käyttäjä nyt avaa esimerkiksi salasanalla suojatun pakatun tiedoston ja liite pitää sisällään haittaohjelman, kykenee työaseman virustorjuntaohjelma estämään haitallisen koodin suorittamisen.

5.1.5 Kannettavien työasemien turvaaminen

Erityistä huomiota tulee kiinnittää kannettaviin tietokoneisiin ja etätyökoneiden ohjelmistojen päivittämiseen. Näistä on huolehdittava keskitetysti hyväksytyn prosessin mukaisesti.

Kun organisaation ulkopuolella ollut työasema palaa takaisin organisaation sisäverkkoon, on se tarkastettava erillisessä pisteessä ennen verkkoon kytkemistä. Tässä voidaan ajatella perinteistä mallia, jossa levykkeet tarkastettiin ennen niiden käyttöä. Ratkaisu on suunniteltava organisaatiokohtaisesti ja käyttöönotossa on huomioitava muiden käytössä olevien turvaratkaisuiden vaikutus.

Organisaation laitepolitiikassa on määriteltävä, että kaikki työasemat, joilla organisaation verkkoon kytkeydytään, ovat sen omistamia ja hallinnoimia. Työasemia ei saa kytkeä muihin verkkoihin (yritykset, hotellit, kotiverkko) ja etäkäytössä on noudatettava aina organisaation antamia ohjeita.

5.2 Ohjelmistohaavoittuvuudet ja korjauspäivitykset

Ohjelmistohaavoittuvuuksien hyväksikäyttö osana haittaohjelman leviämis- tai haittavaikutusmekanismia on suosittu ja jatkuvasti lisääntyvä ilmiö. Ilmiön suosioon on vaikuttanut muun muassa haittaohjelmakirjoittajien ja perinteisten hakkereiden yhteenliittyminen, sekä julkaistujen vakavien ohjelmisto-haavoittuvuuksien voimakas lisääntyminen.

Organisaation on järjestettävä turvapäivityksien aktiivinen seuranta ja toteutus työasemissa ja palvelimissa.

5.2.1 Haittaohjelmien hyväksikäyttämät ohjelmistohaavoittuvuudet

Ohjelmistohaavoittuvuuden hyväksikäyttö voi olla osa varsinaista haittaohjelman leviämis- tai aktivoitumismekanismia. Lisäksi alemman tason oikeuksilla aktivoitunut haittaohjelma voi hyväksikäyttää paikallista hyväksikäytettävää ohjelmistohaavoittuvuutta korkeamman tason oikeuksien saamiseen.

Tyypillisiä sähköpostin kautta leviävien haittaohjelmien hyväksikäyttämiä haavoittuvuuksia ovat sellaiset sähköpostiohjelmistojen tai selainten haavoittuvuudet, jotka mahdollistavat haittaohjelman aktivoitumisen ilman liitetiedoston avaamista. Hyvin tunnettuja ovat virukset, jotka ohjelmistohaavoittuvuutta hyväksikäyttämällä aktivoituvat jo sähköpostin esikatselutilassa. Lisäksi sähköpostin liitetiedostoina leviävät virukset voivat hyväksikäyttää lähes kaikkia liitetiedoston käsittelyyn käytettyjen sovellusohjelmistojen haavoittuvuuksia. Tällainen haavoittuvuus voi olla esimerkiksi toimistosovelluksessa mahdollistaen makrojen suorittamisen ohjelmiston asetusten vastaisesti.

Selainhaavoittuvuuksien hyväksikäyttö on erityisen suosittua WWW-sivujen (**W**ord **W**ide **W**eb) kautta leviäville Troijan Hevosille. Selaimen haavoittuvuutta hyväksikäyttämällä haittaohjelma voi tarttua WWW-sivujen kautta sivuja selailevan käyttäjän järjestelmään, vaikka selaimessa on käytössä turvalliset asetukset. Selaimen haavoittuvuuden hyväksikäyttö on yksi suosituimmista menetelmistä läpäistä palomuuri ja ujuttautua sisäverkon työasemaan.

WWW-sivujen kautta leviävät haittaohjelmat voivat hyväksikäyttää myös selaimen kautta käyttöjärjestelmän tai kirjaston haavoittuvuuksia tai mitä tahansa WWW-sivuilta ladattavia tiedostoja käsittelevien asiakasohjelmistojen, kuten esimerkiksi videotiedostojen katseluun tai musiikkitiedostojen kuunteluun tarkoitettujen ohjelmistojen haavoittuvuuksia.

Useimmat verkkomadot leviävät suoraan palvelinohjelmistojen haavoittu-vuuksien avulla. Verkkomadot voivat hyväksikäyttää myös verkon kautta hyväksikäytettäviä käyttöjärjestelmien ja kirjastojen haavoittuvuuksia.

5.2.2 Haavoittuvien järjestelmien päivittäminen ja suojaaminen

Haittaohjelmien leviämisen ehkäisemiseksi ja haittavaikutusten rajoittamiseksi ylläpidon tulee ryhtyä välittömästi toimenpiteisiin ohjelmistovalmistajan julkaistua korjauspäivityksen vakavaan haavoittuvuuteen organisaatiossa sovitun prosessin mukaisesti. Haittaohjelmien leviämisen näkökulmasta vakavia haavoittuvuuksia ovat erityisesti mielivaltaisten komentojen etäsuorittamisen (arbitrary remote code execution) mahdollistavat haavoittuvuudet.

On kuitenkin huomattava, että useampi vähäpätöisempi haavoittuvuus voi yhdessä muodostaa hyväksikäytettynä yhtä vakavaa haavoittuvuutta vastaavan uhan. Kussakin organisaatiossa tulee arvioida haavoittuvuuden vakavuutta organisaation näkökulmasta (haavoittuvuusikkuna), arvioiden erikseen hyväksikäytön mahdollisuutta haittaohjelman avulla.

Usein ohjelmistovalmistajat joutuvat tekemään tietoturvapäivitykset nopeasti, erityisesti julkiseen tietoisuuteen tulleisiin haavoittuvuuksiin, eikä tietoturvapäivityksiä välttämättä testata valmistajan toimesta yhtä kattavasti kuin varsinaisia ohjelmistoversioita. Korjauspäivityksen asentaminen voi aiheuttaa toimivuus- tai yhteensopivuusongelmia. Ennen tuotantojärjestelmien ja kriittisten palvelimien päivittämistä sekä sisäverkon työasemien keskitettyä päivittämistä tulee korjauspäivityksen toimivuus ja yhteensopivuus muiden organisaatiossa käytettyjen ohjelmistojen kanssa kokeilla erillisessä testiympäristössä.

Jos julkaistuun vakavaan ohjelmistohaavoittuvuuteen ei ole saatavilla korjauspäivitystä tai päivitystä ei voida asentaa esimerkiksi yhteensopivuus-ongelmien takia, tulee ylläpidon pyrkiä rajoittamaan hyväksikäyttöä muilla menetelmillä, esimerkiksi suojaamalla järjestelmä palomuurilla. Erityisesti on kuitenkin huomattava, ettei virustorjuntaohjelmisto yksin suojaa riittävästi päivittämätöntä järjestelmää saastumiselta. Esimerkiksi uusi nopeasti leviävä mato ennättää saastuttaa valtavia määriä haavoittuvia tietojärjestelmiä ennen kuin torjuntaohjelmiston valmistaja kykenee päivittämään virustunnisteet uuden madon torjumiseksi. Jos vakavan haavoittuvuuden sisältävää järjestelmää ei voida päivittää tai suojata muilla hyväksikäyttöä rajoittavilla toimenpiteillä, tulee ylläpidon tarkastella vaihtoehtoisen ohjelmiston käyttöönottoa.

Haittaohjelmien leviämisen ehkäisemiseksi tulee haavoittuvista tietojärjestel-mistä suojata ensisijaisesti suoraan niihin kytketyt tai avoimeen verkkoon palveluita tarjoavat tietojärjestelmät. Muiden järjestelmien päivittämisen prioriteettia arvioitaessa tulee tarkastella muiden suojaus-kerroksien tarjoamaa suojaa ja järjestelmän kriittisyyttä.

Erityisesti on huomattava, ettei pelkän verkkopalomuurin tuoma suoja ole useinkaan riittävä: palomuurilla suojattuun sisäverkkoon verkkomato voi päästä esimerkiksi saastuneen kannettavan laitteen tai sisäverkkoon yhteyden ottaneen etätyöaseman kautta. Sisäverkkoon päässyt verkkomato voi saastuttaa erittäin nopeasti paljon työasemia ja aiheuttaa vakavan uhan koko organisaation toiminnalle.

Sisäverkkoon liitettävien työasemien versionhallinnasta ja korjauspäivittämisestä tulee huolehtia mahdollisimman keskitetysti ja tätä varten pitää olla hyväksytty hallintaprosessi. Erityistä huomiota tulee kiinnittää kannettaviin tietokoneisiin ja etätyökoneiden ohjelmistojen päivittämiseen.

5.2.3 Puuttuvien korjauspäivitysten havaitseminen

Organisaation ylläpidon tulee tarkastella verkkoon kytkettyjen tietojärjestelmien päivitystilannetta säännöllisin väliajoin. Päivitystilannetta voidaan tarkastella joko järjestelmän ulkopuolelta toisesta järjestelmästä verkon kautta suoritettavilla teknisillä haavoittuvuustarkastuksilla tai paikallisesti järjestelmässä suoritettavilla päivitystilannetta tarkastelevilla työkaluilla.

Haavoittuvuusskannereiden toiminta perustuu tutkittavien ohjelmistojen versioiden selvittämiseen ja versiotietojen vertaamiseen haavoittuvuus-tietokannan tietoihin. Haavoittuvuustietokanta sisältää luettelon yleisimpien ohjelmistojen eri versioista löydetyistä haavoittuvuuksista. Haavoittuvuusskannerit voivat etsiä haavoittuvia ohjelmistoja myös murtokokeita tekemällä. Haavoittuvuusskannereita on saatavilla sekä ilmaisohjelmistoina, että kaupallisina ohjelmistoina.

Verkon kautta suoritettavilla teknisillä haavoittuvuustarkastuksilla voidaan havaita ohjelmistopäivitysten puuttuminen vain niistä ohjelmistoista, joihin päästään verkon kautta käsiksi. Tällaisia ohjelmistoja ovat ensisijaisesti verkkoon palveluita tarjoavat palvelinohjelmistot. Lisäksi haavoittuvuus-skannereilla voidaan havaita vain osa puuttuvista käyttöjärjestelmä- ja kirjastopäivityksistä. Verkon kautta suoritettavilla haavoittuvuustarkastuksilla ei tavallisesti havaita asiakasohjelmistoista puuttuvia päivityksiä.

Erityisesti on huomattava, että haavoittuvuusskannereita ja muita versiotietoihin pohjautuvia työkaluja käyttämällä voidaan havaita vain tunnettuja haavoittu-vuuksia. Haavoittuvuusskannerit toimivat haavoittuvuustietokannan tietojen perusteella, joten haavoittuvuustietokannan päivittäminen riittävän usein - esimerkiksi aina ennen säännöllisin väliajoin suoritettavaa teknistä haavoittuvuustarkastusta – on välttämätöntä. Suurimpien valmistajien (Qualys, CA, ISS ja NAI) tuotteet havaitsevat noin 91.000 haavoittuvuutta.

Paikallisesti suoritetuilla skannauksilla voidaan tutkia kattavasti järjestelmän päivitystilannetta, näin havaitaan myös asiakasohjelmistoista puuttuvat päivitykset. Monet ohjelmistovalmistajat tarjoavat ilmaiseksi työkaluja, joilla voidaan tutkia valmistajan ohjelmistojen asetuksia ja puuttuvia korjauspäivityksiä. Työkaluja, joilla voidaan keskitetysti hallita ja valvoa eri ohjelmistojen päivitystilannetta, voidaan käyttää tehokkaasti apuna puuttuvien päivitysten havaitsemiseen.

5.2.4 Haavoittuvuuksien ja korjauspäivityksien seuraaminen

Ohjelmistovalmistajat julkaisevat korjauspäivityksiä ja tiedotteita omista tuotteista löydetyistä haavoittuvuuksista omilla WWW-sivuillaan. Jotkut ohjelmistovalmistajat tar-

joavat haavoittuvuustiedotteita myös sähköposti-jakeluna. On kuitenkin huomattava, etteivät valmistajat normaalisti lähetä loppukäyttäjille korjaustiedostoja sähköpostin liitetiedostona, vaan käyttäjän on ladattava korjaustiedosto valmistajan WWW- tai FTP-palvelimelta (File Transfer Protocol). Useimmiten sähköpostin liitetiedostona lähetetty ohjelmiston korjauspäivitykseksi väitetty tiedosto lon todellisuudessa haittaohjelma.

Viestintäviraston CERT-FI ryhmä julkaisee ajankohtaista suomenkielistä tietoa eri valmistajien ohjelmistohaavoittuvuuksista WWW-sivuillaan osoitteessa www.cert.fi CERT-FI:n varoitukset ohjelmistohaavoittuvuuksista ja muista ajankohtaisista tietoturvauhista on saatavina myös sähköpostijakeluna.

5.3 Torjuntaohjelmat, niiden päivitykset ja seuranta

Virustorjuntaohjelmistot ovat ohjelmistoja, joiden tehtävänä on suojata tietojärjestelmää haittaohjelmilta. Virustorjuntaohjelmisto tunnistaa haittaohjelmia erilaisten viruskuvaustietokannassa kuvattujen tunnisteiden perusteella, estää niiden suorittamisen ja pyrkii poistamaan ne tietojärjestelmästä. Virustorjuntaohjelmistot voidaan jakaa käyttötarkoitukseltaan kolmeen ryhmään: työasemassa, sähköpostipalvelimessa sekä Internet yhdyskäytävässä käytettäviin torjuntaohjelmistoihin.

Virustorjuntaohjelmistoilla on merkittävä rooli suojauduttaessa haittaohjelmilta, koska ohjelmistojen korjauspäivitykset ja järjestelmien turvalliset asetukset eivät välttämättä suojaa tietojärjestelmiä niiltä haittaohjelmilta, jotka hyväksikäyttävät ihmisten tietämättömyyttä tai hyväuskoisuutta. Päivitetyn virustorjuntaohjelmiston käyttö pienentää merkittävästi haittaohjelmien aiheuttamaa uhkaa.

On huomioitava, ettei pelkkä yhdyskäytävätason ja/tai postipalvelimen virustorjunta ole riittävä, vaan myös sisäverkon työasemien suojaamisesta virustorjuntaohjelmistolla tulee huolehtia. Yhdyskäytävän ja postipalvelimen torjuntaohjelmistot eivät suojaa sisäverkkoa saastuneen kannettavan laitteen tai salatun yhteyden kautta leviältä haittaohjelmilta.

Riittävän syvän, kerroksittaisen puolustuksen saavuttamiseksi tulee sisäverkko suojata sekä yhdyskäytävä- että työasematason torjunta-ohjelmistoilla. Puolustuksen syvyyden saavuttamiseksi tulee eri puolustuskerroksilla käyttää eri valmistajien torjuntaohjelmistoja.

5.3.1 Torjuntaohjelmistojen konfigurointi

Yhdyskäytävätasolle ja postipalvelimiin asennettavista torjuntaohjelmistoista tulee kytkeä pois päältä ominaisuus, joka lähettää automaattisesti tiedotteen ”viestin lä-

hettäjälle” torjuntaohjelmiston löydettyä haittaohjelman. Tästä ominaisuudesta on huomattavasti enemmän haittaa kuin hyötyä, koska nykyiset sähköpostin kautta leviävät haittaohjelmat poikkeuksetta väärentävät lähettäjätiedot ja automaattiset ilmoitukset lähetetään väärennettyihin lähdeosoitteisiin. Väärennettyihin osoitteisiin lähetetyt automaattiset ilmoitukset ovat ei-toivottua viestintää, mikä lisää postipalvelimien kuormitusta ja aiheuttaa hämmennystä ja joissakin tapauksissa jopa turhaa selvitystyötä viestin vastaanottajalle.

Työasemiin asennettavat torjuntaohjelmistot täytyy konfiguroida niin, ettei tavallisilla käyttäjillä ole mahdollisuuksia tehdä muutoksia ohjelmistojen asetuksiin tai pysäyttää ohjelmistoa. Torjuntaohjelmiston täytyy käynnistyä aina järjestelmän käynnistymisen yhteydessä ilman käyttäjän toimenpiteitä. Työasemien torjuntaohjelmistojen käyttö tulee olla keskitetysti hallittua ja valvottua, ja ylläpidon tulee suorittaa jatkuvaa torjuntaohjelmistojen käyttöön liittyvää seurantaa.

5.3.2 Torjuntaohjelmiston päivitykset

Koska virustorjuntaohjelmistot kykenevät tunnistamaan vain ne haittaohjelmat, jotka ovat kuvattuna torjuntaohjelmiston virustunnisteissa, on niiden ajantasaisena pitäminen erittäin tärkeää. Virustorjuntaohjelmistojen valmistajat tekevät päivityksiä virustunnisteisiin jopa useita kertoja päivässä, joten torjuntaohjelmiston automaattisen päivitysominaisuuden käyttö on ainoa tapa pitää ne ajantasaisena. Torjuntaohjelmiston tulee välittömästi käynnistyksen jälkeen ja muutoin riittävän usein tarkistaa virustunnisteiden ajantasaisuus.

Sisäverkon järjestelmien torjuntaohjelmistojen virustunnisteiden päivittäminen tulee järjestää keskitetysti sisäverkon palvelimelta, mikä mahdollistaa torjuntaohjelmistojen päivittymisen keskitetyn valvonnan. Ylläpidon tulee jatkuvasti seurata, että torjuntaohjelmistojen virustunnisteet päivittyvät tarvittavin väliajoin.

Erityistä huomiota on kiinnitettävä kannettavien tietokoneiden ja muiden mobiililaitteiden torjuntaohjelmistojen virustunnisteiden päivittymiseen. Virustunnisteiden päivittäminen pitää määrittää kannettavissa laitteissa niin, että tunnisteet päivittyvät aina laitteen ollessa kytkeytyneenä Internetiin. Kannettavan laitteen ollessa sisäverkon ulkopuolella kytkeytyneenä Internetiin päivitykset haetaan suoraan torjuntaohjelmiston valmistajan palvelimelta.

Kauan sisäverkosta poissa olleiden kannettavien tietokoneiden viruskuvausten ja ohjelmistojen päivitystilanne sekä muu tietoturvatilanne tulee tarkistaa ennen niiden kytkemistä sisäverkkoon. Tarkistaminen voidaan tehdä manuaalisesti organisaation ylläpidon toimenpiteenä. Tarkistaminen voidaan suorittaa sisäverkkoon kytkeytyville kannettaville tietokoneille myös automaattisesti teknisillä menetelmillä. Tällöin sisäverkkoon kytkeytyville kannettaville laitteille sallitaan yhteydenotto ainoastaan järjes-

telmän tietoturvan tarkistavaan palvelimeen, ja vasta tarkistustoimenpiteen jälkeen sallitaan kirjautuminen lähiverkkoon.

5.4 Organisaation verkon suojaaminen

Nopeasti muuttuvilta ja yhä useammin yksittäisiä suojakerroksia läpäiseviltä haittaohjelmilta suojauduttaessa tulee organisaation sisäverkon puolustuksen kerroksellisuuteen kiinnittää erityistä huomiota. Puolustuksen kerroksellisuudella voidaan varautua yksittäisen puolustuskerroksen pettämiseen. Seuraavissa luvuissa kuvatun lisäksi löytyy linjauksia Valtiohallinnon tietoturvallisuuden johtoryhmän VAHTI ohjeista 2/2001 ja 1/2003.

5.4.1 Verkon ulkorajojen suojaaminen

Verkkopalomuuri on merkittävin yksittäinen laite suojattaessa sisäverkkoa avoimesta verkosta tulevilta uhilta, haittaohjelmista erityisesti verkkomadoilta. Siksi palomuuria tulee hallita ja konfiguroida erityisen huolellisesti ja asiantuntemuksella. Sisään tulevan liikenteen lisäksi palomuurilla suojataan sisäverkkoa suodattamalla myös ulospäin menevää liikennettä. Palomuurin säännöissä tulee kiinnittää erityistä huomiota siihen, mitä liikennettä sallitaan sisäverkosta ulospäin - esimerkiksi vertaisverkkoohjelmistojen käyttö lisää merkittävästi organisaation haittaohjelmariskiä.

Organisaation ulkopuolelta tulevasta liikenteestä voidaan ennen palomuuria olevalla reitittimellä suodattaa tarpeeton liikenne, joka kohdistuu yleisimpien haittaohjelmien käyttämiin kohdeportteihin. Näin saadaan lisää kerroksellisuutta sisäverkon suojaamiseen.

Sisäverkon ja ulkoverkon välinen http- ja ftp-liikenne tulee ohjata yhdyskäytävään asennetun virustorjuntaohjelmiston läpi. Yksi tehokas keino suojautua selaimen välityksellä tarttuvilta haittaohjelmilta on rajoittaa käyttäjien pääsyä epäilyttäville WWW-sivustoille, joiden kautta tapahtuva haittaohjelman tartuntariski on korkea. Tällaisia WWW-sivustoja ovat esimerkiksi aikuisviihdepalvelusivustot.

Toisaalta organisaation kannattaa harkita koko Internetin käytön estämistä työntekijöiden henkilökohtaisista työasemista huomioiden siinä käsiteltävän tiedon kriittisyys organisaatiolle; WWW-sivujen selailu voidaan järjestää käyttämällä erillisiä vain WWW-sivujen selailuun tarkoitettuja työasemia, jotka eivät ole samassa sisäverkossa muiden työasemien kanssa. Tällaisia yhteiskäyttöön tarkoitettuja Internet-koneita voidaan sijoittaa esimerkiksi organisaation kahvihuoneeseen.

5.4.2 Sisäverkon sisäiset suojautumismenetelmät

Sisäverkossa suojauskerrosten rakentaminen on ongelmallisempaa kuin verkon rajalla. Verkon rajoilla olevat torjuntamenetelmät eivät suojaa sisäverkkoa, jos haittaohjelma pääsee esimerkiksi kannettavan tietokoneen mukana sisäverkkoon. Sisäverkon järjestelmien suojaamisessa on tärkeintä, että järjestelmät ovat turvallisesti konfiguroitu (luku 5.1), järjestelmien ohjelmistopäivityksistä on huolehdittu (luku 5.2) ja että työasemissa käytetään ajantasaista virustorjuntaohjelmistoa (5.3) ja mahdollisuuksien mukaan käytetään eri toimittajien torjuntaohjelmistoja verkon rajalla ja työasemissa.

On mahdollista, ettei sisäverkon järjestelmiä ole ennätetty päivittää tai ne ovat muusta syystä päivittämättä, kun uusi nopeasti leviävä mato pääsee sisäverkkoon. On myös mahdollista, että sisäverkkoon pääsee uusi nopeasti leviävä mato, joka hyväksikäyttää entuudestaan tuntematonta haavoittuvuutta. Tällaisiin uhkiin voidaan varautua rakentamalla erillinen suojauskerros sisäverkkoon järjestelmäkohtaisesti, joko järjestelmän omalla palomuurilla, tai erikseen hankittavalla ohjelmistopohjaisella palomuurilla. Sisäverkon työasemakohtaisen palomuuriratkaisujen tulee olla keskitetysti hallittuja ja valvottuja.

Sisäverkon rakenteellisilla ratkaisuilla on merkittävä rooli minimoitaessa vahinkoja ja varauduttaessa toiminnan jatkuvuuteen haittaohjelmista, erityisesti verkkomadoista, aiheutuvan riskin toteutuessa.

> Madon leviämistä sisäverkossa voidaan ehkäistä jakamalla sisäverkko pienempiin segmentteihin ja suodattamalla osien välistä verkkoliikennettä palomuurilla tai muulla pakettisuodattimella. Vähintäänkin organisaation sisäverkon kriittiset palvelimet, testi- ja tuotantojärjestelmät sekä työasemat tulee erottaa omiin verkkosegmentteihinsä osana tietoturva-arkkitehtuuria.

5.5 Työskentely organisaation ulkopuolella

Kun päätelaite sijaitsee organisaation verkon ulkopuolella, ei siihen voida teknisesti ulottaa samaa keskitettyä valvontaa ja hallintaa kuin sisäverkkoon kytkettyyn laitteeseen. Tällöin se muodostaa helpomman kohteen haittaohjelmalle. Jos laitetta ei organisaation ulkopuolella liitetä Internettiin ovat tartuntamahdollisuudet pienemmät. Tarvittaessa on tietoliikenneyhteys aina järjestettävä organisaation tietoverkon kautta.

Salattu yhteys mahdollistaa haittaohjelman pääsyn organisaation palomuurien ja suojausten läpi huomaamatta. Vaara on suuri kun käsitellään salattua sähköpostia.

Riskiä voidaan hallita sallimalla yhteys vain organisaation etätyöasemilta eteisverkkoon, johon myös luotetut kumppanit voidaan päästää.

VPN-yhteyden (Virtual Private Network) avulla haittaohjelmat voivat päästä gateway-tason torjuntaohjelmiston läpi. Vaikka ulkoapäin sisäverkkoon otetun VPN-yhteyden salaus puretaan sisäverkon rajalla olevassa palomuurissa tai VPN-laitteessa, haittaohjelmaa ei ehkä havaita gateway-tason torjunta-ohjelmistolla, koska

– gateway-tason torjuntaohjelmisto voi olla sijoitettu ulommas kuin salauksen purkava laite, jolloin VPN-liikenne menee salattuna gateway-tason tarkastusohjelmiston läpi,
– mikäli gateway-tason torjuntaohjelmistolla tarkastetaan vain sähköposti ja HTTP-liikenne, eri portteja käyttävä mato voi päästä sisäverkkoon VPN-yhteden kautta.

Edellä kuvatun mukaisesti VPN-yhteys on reitti sellaisille verkkomadolle, jonka käyttämä portti suodatetaan palomuurissa. Salattuja yhteyksiä voidaan muodostaa myös työasemalta ulospäin. Esimerkiksi SSL- (Secure Socket Layer), SSH- (Secure Shell) tai HTTPS-yhteyksillä liikenne menee työasemalle asti salattuna.

Virustunnisteet on päivitettävä kuitenkin Internetin kautta palvelua tarjoavan yrityksen sivuilta organisaation palvelimille, jota kautta myös etäyhteydellä olevat työasemat saavat yhteyden Internettiin.

Kannettavissa työasemissa on oltava myös turvalliset menettelyt, kuinka Bluetooth ja WLAN palveluita käytetään jos niiden käyttö on sallittua.

Kaikkien ratkaisujen on perustuttava etukäteen laadittuun uhka-analyysiin. Uhkia ovat mm. keskitetyn valvonnan puute, virustunnisteiden päivityksien ajantasaisuus ja muut tietoturvaan liittyvät käytännöt, esimerkiksi käyttöjärjestelmien turva-aukkojen päivitys.

Otettaessa työasemasta suora etäyhteys Internetin palveluihin esimerkiksi web-posteihin ohitetaan organisaation suojaukset ja altistutaan haittaohjelmille. Ratkaisuna tähän on sallittava vain suljettu etäyhteys tai soittosarja organisaation verkon palveluihin, joiden kautta tarvittaessa voidaan kytkeytyä Internettiin.

6. TOIMINNAN KEHITTÄMINEN JA KOULUTUS

6.1 Kehittämissuunnitelma

Haittaohjelmien torjunnan edellytys on, että organisaatiossa on määritelty järjestelmänhallinnasta ja tietoturvallisuuden valvonnan kehittämisestä vastaava organisaation osa. Tämän lisäksi tulee kiinnittää huomiota valittavaan työasema-arkkitehtuuriin, jolla on vaikutusta haittaohjelmien torjuntaan ja niiltä suojautumiseen.

Mikäli esimerkiksi yhteistyökumppanin suunnittelema järjestelmä tai sen osa poikkeaa oleellisesti olemassa olevasta ohjeistuksesta, suunnitelmalle on saatava järjestelmänhallinnasta ja tietoturvallisuuden valvonnasta vastaavan organisaation hyväksyminen osana normaalia ohjelmisto-, käyttö- ja tietoliikenneturvallisuuden kehittämistä.

Kehittämissuunnitelmien vuosittaisissa tarkasteluissa on arvioitava seuraavien asiakirjojen ajantasaisuus ja muutostarpeet:

- Tietoturvallisuuden hallinnan prosessikuvaukset
- Tietoturvallisuussuunnitelma
- Yleiset valvonta- ja hallintaohjeet

Vuosittaisessa tarkastelussa tulee selvittää vastuuhenkilöiltä mistä he saavat tarvittavia lisäohjeita, kuinka he seuraavat tietoteknisten järjestelmien kehitystä ja kuka vastaa tietojärjestelmien tai –verkkojen ylläpitoon, käyttöön ja tietoturvallisuuteen liittyviin kysymyksiin.

6.2 Koulutus

Tukiorganisaation teknisen henkilöstön on osattava käytössä olevien turvallisuustuotteiden oikea käyttö ja heille on annettava siihen tarvittava koulutus. Samoin heille on annettava riittävä koulutus käyttöjärjestelmien hallitsemisesta sekä tietoverkon turvallisuuteen vaikuttavista tekijöistä ja verkon aktiivilaitteiden ja selainten turvallisista asetuksista.

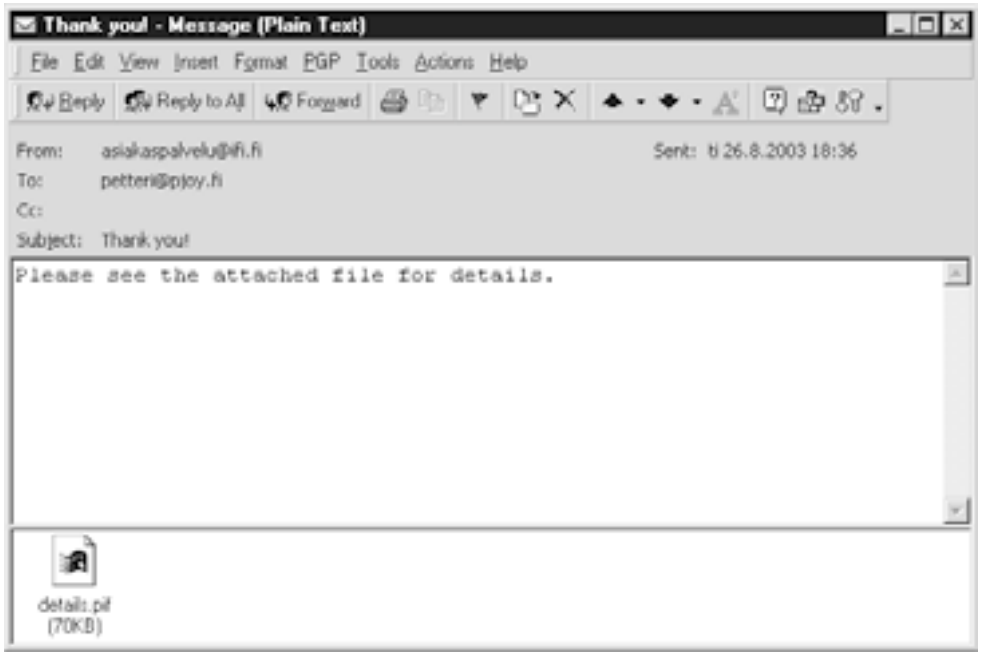
Loppukäyttäjille on opastettava varoitukset, joita haittaohjelmien havain-nointiin liittyy sekä kuinka heidän tulee toimia erilaisissa tilanteissa. Loppukäyttäjiä on valistettava eri keinoin Internetin ja sähköpostin mahdollisuuksista ja vaaroista myönteiseen sävyyn siten, että he hallitsevat surffausennakoinnin ja ovat harkitsevaisia tiedon haussa avoimista tietolähteistä. Tietoturvakoulutus on osa uuden henkilön

perehdyttämis-koulutusta. Koulutuksessa voidaan hyödyntää VAHTI-ohjetta 5/2003 ”Käyttäjän tietoturvaohje”:

Varsinkin sähköpostin käytön osalta on käyttäjille selvästi kerrottava miksi vain organisaation omaa sähköpostia saa käyttää sekä työnantajan mahdollisuus estää muiden sähköpostipalveluiden käyttö.

Vuosittaisessa tietoturvallisuuden täydennyskoulutuksen suunnitelmassa on huolehdittava, että henkilöstö saa riittävän tiedon organisaation kaikista tietoturvaohjeista, tietää mitä tuotteita on käytössä, mitkä ovat suojautumisen perusperiaatteet sekä tietää keihin pitää ottaa yhteyttä epäillystä haittaohjelmatartunnasta.

Social Engineering, uteliaisuuden hyväksikäyttöön liittyvä koulutus on oltava osa henkilöstön täydennyskoulutusta siten, että henkilöstö tunnistaa nämä tilanteet ja huomioi niiden uhat myös Internetin ja sähköpostin käytössä.



Kuvassa on viruksen SoBigF saastuttama sähköpostiviesti. Tyypilliset tunnusmerkit ovat pif muodossa oleva liitetiedosto, tuntematon lähettäjä ja englanninkielinen saate, joka kehottaa liitteen avaamiseen.

Vaikka etätyö on sallittu vain työnantajan laitteilla, organisaation on varauduttava tukemaan työntekijöitään myös heidän kotityöasemiensa haittaohjelmatorjunnassa.

On tärkeää huomata, ettei henkilöstöltä voida vaatia tietoturvallisuustoimen-piteiden osaamista ellei sillä ole käytettävissä koulutuksen lisäksi vahvistettuja, hyväksyttyjä tietoturvallisuusohjeita.

7. LIITTEET

Liite 1. Toiminta haittaohjelmatapauksessa

Liite 2. Selaimen asetukset

Liite 3. Käyttäjän pikaopas

Liite 4. Sisäisten ja ulkoisten velvoitteiden luettelo (lakiliite)

Liite 5. VM:n tietoturvaohjeita ja -julkaisuja: (www.vm.fi/vahti)

Toiminta haittaohjelmatapauksessa	**Toimija 1**	**Toimija 2**	**Johto**	**O K ?**
Selvittää, mitä tapahtui ja missä?		x	T	
Selvittää, miten laajasti vaikuttaa toimintaan?	T	x	x	
Määrittää, miten pitkäaikainen vaikutus tapahtumalla on toimintaan?	T	x	x	
Päättää tarvittavien toimenpiteiden käynnistämisestä.			T	
Johtaa toimenpiteitä reagoitaessa tietoturvaloukkausepäilytapaukseen.	T	x	x	
Kokoaa järjestelmien käytettävyysraportin, vaikutusanalyysin, korjausehdotukset, määrittää korjaustoimenpiteet jne….	x	T		
Raportoi ylemmälle johtoportaalle			T	
Kokoaa ja johtaa tarvittaessa reagointiin vaadittavaa nopean toiminnan ryhmän.	T			
Päättää raportointi- ja tilannekatsausten ajankohdat.			T	
Tiedottaa valvontaorganisaatiolle, sisäisille yhteistyökumppaneille, viranomaisille, ym….		T	x	
Ohjaa ja valvoo järjestelmähallintatyökaluilla toteutettavia operaatioita.	T			
Kokoaa ja arvioi vahinkojen ja menetysten määrän ja laadun, sekä kartoittaa tiedostetut uhat ja riskit.		T		
❑ Tietoliikennelaitteet / -verkot	T	x		
❑ Palvelimet / järjestelmäsovellukset	x	T		
❑ Tietoaineisto / -kannat	x	T		
Vastaa tietojen pelastamisesta ja palauttamisesta.		T		
Aloittaa järjestelmien toipumissuunnitelmien toteuttamisen.	T			
Vastaa yhteistoiminnasta seuraavien tahojen kanssa: x1, x2…			T	

Toiminta haittaohjelmatapauksessa	**Toimija 1**	**Toimija 2**	**Johto**	**OK?**
Vastaa prosessinohjausjärjestelmään laadittavista tapahtumailmoituksista ja –raporteista.		T		
Vastaa järjestelmien palauttamisesta, jatkotoimenpiteistä, tapauksessa havaittujen järjestelmien tietoturva-aukkojen korjauksista ym…			T	

X:llä merkitty tehtävään osallistuvat, T:llä merkitty toteutuksesta vastaava organisaation osa tai tekijät. Taulukko on esimerkki ja kussakin organisaatiossa on erikseen määritettävä tarvittavat vastuut ja tekijät välittömien järjestelmällisten torjunta toimenpiteiden käynnistämiseksi.

Esimerkki Internet Explorer -selaimen suojausasetuksista. Ajankohtaista lisätietoa on saataville verkko-osoitteessa: http://www.niscc.gov.uk

INTERNET-VYÖHYKE	
ActiveX-komponentit ja plugin-laajennukset	
ActiveX-valmistelu- ja komentosarjakomponentteja ei merkitä turvalliseksi	Poista käytöstä
Komentosarjan ActiveX-komponentit on merkitty turvalliseksi	Poista käytöstä
Lataa allekirjoitetut ActiveX-komponentit	Poista käytöstä
Lataa allekirjoittamattomat ActiveX-komponentit	Poista käytöstä
Suorita ActiveX-komponentit ja –plugin-laajennukset	Poista käytöstä
Komentosarjat	
Hyväksy liittäminen komentosarjan avulla	Poista käytöstä
Salli aktiiviset komentosarjat	Poista käytöstä
Suorita Java-ohjelmat	Poista käytöstä
Käyttäjän tunnistaminen	
Kirjautuminen	Kysy käyttäjänimi ja salasana
Lataaminen	
Lataa fontit	Poista käytöstä
Tiedostojen lataaminen	Poista käytöstä
Microsoft VM	
Java-käyttöoikeudet	Poista käytöstä
Muut	
Eri toimialueiden alikehysten käyttäminen	Poista käytöstä
Käynnistä ohjelmat ja tiedostot IFRAME:ssa	Poista käytöstä
Käyttäjätietojen säilyvyys	Poista käytöstä
Lähetä salaamattoman lomakkeen tiedot	Poista käytöstä
Näytä yhdistelmäsisältö	Poista käytöstä

Ohjelmistokanavan käyttöoikeudet	Suuri suojaus
Ota META-päivitys käyttöön	Poista käytöstä
Tietolähteiden käyttäminen eri toimialueilla	Poista käytöstä
Työpöydän kohteiden asentaminen	Poista käytöstä
Vedä ja pudota tai kopioi ja liitä tiedostoja	Poista käytöstä
Älä pyydä valitsemaan asiakassertifikaattia, kun sertifikaattia ei ole tai	Poista käytöstä
PAIKALLINEN LÄHIVERKKO -VYÖHYKE	
ActiveX-komponentit ja plugin-laajennukset	
ActiveX-valmistelu- ja komentosarjakomponentteja ei merkitä turvalliseksi	Ota käyttöön
Komentosarjan ActiveX-komponentit on merkitty turvalliseksi	Ota käyttöön
Lataa allekirjoitetut ActiveX-komponentit	Ota käyttöön
Lataa allekirjoittamattomat ActiveX-komponentit	Poista käytöstä
Suorita ActiveX-komponentit ja –plugin-laajennukset	Kysy vahvistus
Komentosarjat	
Hyväksy liittäminen komentosarjan avulla	Ota käyttöön
Salli aktiiviset komentosarjat	Ota käyttöön
Suorita Java-ohjelmat	Ota käyttöön
Scriptien suoritus	Poista käytöstä
Käyttäjän tunnistaminen	
Kirjautuminen	Kirjaudu automaattisesti käyttäen nykyistä…
Lataaminen	
Lataa fontit	Kysy vahvistus
Tiedostojen lataaminen	Ota käyttöön
Microsoft VM	
Java-käyttöoikeudet	Normaali suojaus

Muut	
Eri toimialueiden alikehysten käyttäminen	Ota käyttöön
Käynnistä ohjelmat ja tiedostot IFRAME:ssa	Ota käyttöön
Käyttäjätietojen säilyvyys	Ota käyttöön
Lähetä salaamattoman lomakkeen tiedot	Ota käyttöön
Näytä yhdistelmäsisältö	Ota käyttöön
Ohjelmistokanavan käyttöoikeudet	Normaali suojaus
Ota META-päivitys käyttöön	Ota käyttöön
Tietolähteiden käyttäminen eri toimialueilla	Poista käytöstä
Työpöydän kohteiden asentaminen	Kysy vahvistus
Vedä ja pudota tai kopioi ja liitä tiedostoja	Ota käyttöön
Älä pyydä valitsemaan asiakassertifikaattia, kun sertifikaattia ei ole tai ...	Poista käytöstä
LUOTETUT SIVUSTOT -VYÖHYKE	
ActiveX-komponentit ja plugin-laajennukset	
ActiveX-valmistelu- ja komentosarjakomponentteja ei merkitä turvalliseksi	Poista käytöstä
Komentosarjan ActiveX-komponentit on merkitty turvalliseksi	Ota käyttöön
Lataa allekirjoitetut ActiveX-komponentit	Poista käytöstä
Lataa allekirjoittamattomat ActiveX-komponentit	Poista käytöstä
Suorita ActiveX-komponentit ja –plugin-laajennukset	Kysy vahvistus
Komentosarjat	
Hyväksy liittäminen komentosarjan avulla	Poista käytöstä
Salli aktiiviset komentosarjat	Ota käyttöön
Suorita Java-ohjelmat	Poista käytöstä
Käyttäjän tunnistaminen	
Kirjautuminen	Kysy käyttäjänimi ja salasana

Lataaminen	
Lataa fontit	Kysy vahvistus
Tiedostojen lataaminen	Ota käyttöön
Microsoft VM	
Java-käyttöoikeudet	Suuri suojaus
Muut	
Eri toimialueiden alikehysten käyttäminen	Poista käytöstä
Käynnistä ohjelmat ja tiedostot IFRAME:ssa	Poista käytöstä
Käyttäjätietojen säilyvyys	Ota käyttöön
Lähetä salaamattoman lomakkeen tiedot	Kysy vahvistus
Näytä yhdistelmäsisältö	Ota käyttöön
Ohjelmistokanavan käyttöoikeudet	Suuri suojaus
Ota META-päivitys käyttöön	Ota käyttöön
Tietolähteiden käyttäminen eri toimialueilla	Poista käytöstä
Työpöydän kohteiden asentaminen	Kysy vahvistus
Vedä ja pudota tai kopioi ja liitä tiedostoja	Ota käyttöön
Älä pyydä valitsemaan asiakassertifikaattia, kun sertifikaattia ei ole tai ...	Poista käytöstä

Liite 3. Käyttäjän pikaopas

Organisaatiosi tietoverkossa ja tietojärjestelmissä on toteutettu perustoimen-piteet haittaohjelmien tunnistamiseksi ja poistamiseksi. Pidä itsesi tietoisena noudatettavista menettelyistä ja annetuista ohjeista sekä noudata niitä.

Seuraavassa huoneentaulussa on kuvattu perusasiat haittaohjelman välttämiseksi ja toimenpiteet mahdollisen tartunnan yhteydessä.

Muista

1. Tunne organisaatiosi tietotekniset palvelut ja toimintaohjeet
2. Tutustu organisaatiosi haittaohjelmista annettuun ohjeistukseen
3. Varmistu, että käytössäsi olevassa työasemassa on toimiva virustorjuntaohjelmisto
4. Ole harkitsevainen, jos saat tuntemattomasta osoitteesta sähköpostia

Seuraaviin havaintoihin voi syynä olla haittaohjelma

1. Ylimääräiset toiminnot (äänet, käynnistymiset, oudot viestit näytöllä)
2. Levytilan yllättävä loppuminen
3. Laitteen toiminnan hidastuminen tai estyminen
4. Tiedostojen katoaminen tai niiden muuttuminen

Kun epäilet tartuntaa, toimi seuraavasti

1. Irrota työasema verkosta (tässä voi olla organisaatiokohtaisia eroja)
2. Tarkista, mitä tietoa näytöllä on
3. Raportoi välittömästi asiasta tietohallintoa (mikrotuki)

Kun työasemassa on haittaohjelma, toimi seuraavasti

1. Tarkista, mitä torjuntaohjelma ilmoittaa näytöllä
2. Raportoi välittömästi asiasta tietohallintoa (mikrotuki)
3. Kirjaa kaikki tekemäsi toimenpiteet
4. Poista haittaohjelma mikäli torjuntaohjelma tarjoaa siihen mahdollisuuden
5. Noudata torjuntaohjelman ohjeita
6. Varmistu toimenpiteen onnistumisesta
7. Tarkasta työaseman levyt (tai pyydä mikrotuki apuun)

Muista

1. Käytä työasemassa vain tietohallinnon asentamia ohjelmia
2. Varmistu, että työasemassa on automaattitoiminto, joka tarkastaa tietovälineen ennen sen käyttöä.
3. Käytä tietojen tallennuksessa organisaatiosi hyväksymiä tiedostomuotoja, esimerkiksi .rtf, .pdf, .doc, .jpg, xls ja .ppt.

4. Varmistu ennen liitetiedoston lähettämistä, että vastaanottajan säännöt sallivat tiedostomuodon käytön.
5. Paraskaan torjuntaohjelma ei tarjoa täydellistä suojaa kaikkia uusimpia haittaohjelmia vastaan.

Liite 4. Sisäisten ja ulkoisten velvoitteiden luettelo

Toiminnan ohjausta koskevat

- valtioneuvoston ohjesääntö (262/2003)

VM ohjaa valtionhallinnon tietoturvallisuutta (17 §)

Tietoaineistoa koskevat

- perustuslain perusoikeussäännökset (731/1999)
  - yksityiselämän suoja (10 §)
  - sananvapaus ja julkisuus (12 §)
- laki viranomaisen toiminnan julkisuudesta (621/1999)
  - julkisuusperiaate (1 §)
  - velvoite hyvään tiedonhallintatapaan (3 §)
  - tiedonsaanti salassa pidettävästä asiakirjasta (10 §)
  - viranomaisen velvollisuudet edistää tiedonsaantia ja hyvää tiedonhallintatapaa (17 §)
  - hyvä tiedonhallintatapa (18 §)
  - salassapitovelvoitteet (22 §-25 §)
  - asiakirjasalaisuus (22 §)
  - vaitiolovelvollisuus ja hyväksikäyttökielto (23 §)
  - salassa pidettävät viranomaisen asiakirjat (24 §)
  - salassapidosta poikkeaminen ja sen lakkaaminen (26 §–32 §)
- asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
  - selvitykset hyvän tiedonhallintatavan toteuttamiseksi (1 §)
  - erityissuojattavan tietoaineiston luokitus (2 §)
  - erityissuojattavaa tietoaineistoa koskevat yleiset tietoturvallisuustoimenpiteet (3 §)
  - ohjeet, valvonta ja seuranta (4 §)
  - selosteet tietojärjestelmistä (8 §)
- asetus valtionhallinnon tietohallinnosta (155/1988 ja muutos 1401/1992)
  - tietojärjestelmät taloudellisia, turvattuja, toiminnallisesti yhteensopivia sekä tietosuojan vaatimukset täyttäviä (1 §)
  - valtionhallinnon tietojenkäsittelyn ja tietohallinnon ohjaus ja yhteensovittaminen (2 §)
  - velvoite pyytää merkittävästä tahi useaa virastoa tai laitosta koskevasta tietotekniikan soveltamiseen liittyvästä hankkeesta valtiovarainministeriön lausunto (3 §)
  - tietojenkäsittelyä ja tietohallintoa koskeva kehittämissuunnitelma (3 §)

- arkistolaki (831/1994)
  - käytettävyys ja säilyminen, tarpeettoman aineiston hävittäminen (7 §)
  - turvaaminen tuhoutumiselta, vahingoittamiselta ja asiattomalta käytöltä (12 §)
- laki valtion talousarviosta annetun lain muuttamisesta (217/2000)
  - velvollisuus hoitaa sisäinen valvonta (24 §)
- asetus valtion talousarviosta (1243/1992)ja sen muutos (263/2000)
  - taloushallinnon järjestelmien tietoturvallisuusmääräykset taloussäännössä (26 §)
  - riskeihin nähden asianmukainen sisäinen valvonta (69 §, 69a §)
  - sisäinen tarkastus (70 §)
  - koneellisin menetelmin pidetty kirjanpito ja sen menetelmäkuvaus (47 §)
- henkilötietolaki (523/1999)
  - tarkoituksena toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia (1 §)
  - tietoturvallisuus ja tietojen säilytys (32-35 §)
- laki yksityisyyden suojasta työelämässä (477/2001)

Tietoaineistoa ja tietotekniikkaa koskevat

- laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)
  - televiestinnän turvallisuus (4 §)
  - teleyrityksen tietoturvallisuusvelvoitteet (6 §)
  - teleoperaattorien vaitiolovelvollisuus (7 §)
  - rajoitukset suoramarkkinoinnille (21 §)
- edellisen lain nojalla annettu asetus (723/1999)
- viestintämarkkinalaki (393/2003)
- laki rikoslain muuttamisesta (769/1990)
  - luvaton käyttö (28. luku 7 § – 9 §)
  - vahingonteko (35. luku 1 § - 3 §)
  - laki rikoslain muuttamisesta (578/1995)
  - viestintäsalaisuuden loukkaus (38. luku 3 §)
  - tietomurto (38. luku 8 §)
  - virkasalaisuuden rikkominen (40. luku 5a §)
- laki rikoslain muuttamisesta (951/1999)
  - vaaran aiheuttaminen tietojenkäsittelylle (34. luku 9a §)
- laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- laki sähköisistä allekirjoituksista (14/2003)
- valtion virkamieslaki (750/1994)
  - virkasuhteen päättäminen, purkuperusteet, kirjallinen varoitus (7 luku)
- laki sähköisen viestinnän tietosuojasta (125/2003)

Poikkeusolojen valmiutta koskevat

- valmiuslaki 22.7.1991/1080
- laki huoltovarmuuden turvaamisesta (18.12.1992/1390)
- valtioneuvoston päätös huoltovarmuuden tavoitteista (8.5.2002/350)
- laki Puolustustaloudellisesta suunnittelukunnasta (20.5.1960/238)

Valmisteilla olevat säädökset

- työelämän tietosuojalainsäädännön täydentämishanke (HE 162/2003)

VM:n tietoturvaohjeita ja -julkaisuja: (www.vm.fi/vahti)

- Haittaohjelmista 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
- 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
- Tunnistaminen valtionhallinnon verkkopalvelimissa, VM 6/01/2003
- 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
- Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000
- Tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM 19.1.2000
- Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, VAHTI 2/1999
- Suositus toimitilaturvallisuudesta, VM 31.12.1998

VAHTI

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

3/2004

HAITTAOHJELMILTA SUOJAUTUMISEN YLEISOHJE

ISBN 951-804-443-0
ISSN 1455-2566