VALTIOVARAINMINISTERIÖ

Kohdistetut hyökkäykset

6/2009

VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

Kohdistetut hyökkäykset

Valtiovarainministeriön julkaisuja 6/2009 VAHTI

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

ISSN 1455-2566 (nid.)
ISBN 978-952-251-012-9 (nid.)
ISSN 1798-0860 (PDF)
ISSN 978-952-251-013-6 (PDF)

YMPÄRISTÖMERKKI
MILJÖMÄRKT
441 002
Painotuote

Edita Prima Oy
Helsinki 2009

Lyhyesti VAHTIsta

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

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

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

VAHTIn toiminnalla on parannettu valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä, kansalaistoiminnassa ja kansainvälisesti. VAHTIn toiminnan tuloksena muun muassa on aikaansaatu erittäin kattava yleinen tietoturvaohjeisto. Valtiovarainministeriön ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita. VAHTI on valmistellut, ohjannut ja toteuttanut laajan valtion tietoturvallisuuden kehitysohjelman, jossa on aikaansaatu merkittävää kehitystyötä yhteensä 26 kehityskohteessa yli 300 hankkeisiin nimetyn henkilön toimesta. VAHTI on saanut kolmena vuotena tunnustuspalkinnon esimerkillisestä toiminnasta Suomen tietoturvallisuuden parantamisessa.

VAHTIn verkkosivuilta (www.vm.fi/vahti) löytyy monipuolisesti tietoa VAHTIn toiminnasta, tuloksista, suunnitelmista ja menossa olevista hankkeista sekä voimassa olevista ja valmisteilla olevista julkaisuista.

Sisältö

1 Johdanto

Kohdistetun hyökkäyksen tavoitteena on jonkin *tietyn tiedon* kaappaaminen tai tietyn kohteen toiminnan haittaaminen. Tämän VAHTIn alaisuudessa laaditun selvityksen painopisteenä ovat tiedon luottamuksellisuutta ja eheyttä uhkaavat tietokaappaukset, koska niitä on erityisen hankala havaita ja estää käytössä olevilla torjuntamalleilla. Palvelunestohyökkäykset jätetään tässä vain kursoriselle käsittelylle. Julkisen palvelun ylikuormittamista ei yleensä ole erityisen hankala huomata.

Tietoriskien torjunnan painopiste on yhä vieläkin satunnaisesti kohteensa valitsevissa hyökkäyksissä, jotka on helppo havaita ja kohtalaisen helppo torjua. Vaikka lainsäädäntö edellyttää viranomaisen käsittelemän aineiston suojaamista ja vaikka tietoturva-asiantuntijat tunnistavat kohdistettujen hyökkäysten aiheuttaman uhan, turvallisen käyttöympäristön rakentamiseen tarvittavat resurssit on vaikea perustella johdolle niin kauan kuin konkreettinen uhka on piilossa. Tämän selvityksen tavoitteena onkin tuoda kohdistettujen hyökkäysten uhka esille, jotta organisaatioilla olisi paremmat edellytykset muokata toimintaprosessit ja järjestelmät nykyistä turvallisemmiksi.

Tavoitteena on ollut kirjoittaa mahdollisimman konkreettinen esitys. Abstraktiotaso on kuitenkin ollut pakko pitää sen verran yleisellä tasolla, ettei teksti vanhene vielä painovaiheessa. Olen pyrkinyt kirjoittamaan auki olennaisia periaatteita, jotta tieto olisi helposti sovellettavissa jatkossakin olosuhteiden muuttuessa. Hienoinen poleemisuus on tarkoituksellista. Sen tavoitteena on motivoida lukijaa kyseenalaistamaan niitä yleisiä, mutta helposti korjattavissa olevia ”löysiä” käytäntöjä, jotka tällä hetkellä vaarantavat julkishallinnossa käsiteltävän tiedon turvallisuuden.

1.1 Reunaehdot kohdistettujen hyökkäysten torjunnalle

Kohdistetun tietokaappauksen onnistumisen edellytyksenä on jokin erityinen haavoittuvuus tiedon käsittelemisen prosesseissa. Niinpä torjunnassa on olennaista tunnistaa yhtälailla oman ympäristön haavoittuvuudet kuin suojauksen kohteena oleva tieto.

Kohdistettuja hyökkäyksiä ei tehdä ennalta tunnistettavissa olevilla hyökkäystavoilla, joten niiden havaitsemisessa ei pidä luottaa automaattisiin järjes-

telmiin. Suojautumista ei myöskään pidä jättää määräyksillä työntekijän viitseliäisyyden varaan. Jos hyökkäykset todella halutaan estää, käyttöympäristö pitää rakentaa paljon nykyistä turvallisemmaksi ja sitä on ylläpidettävä jatkuvasti huolella.

1.1.1 Lainsäädännön asettamat vaatimukset

Lainsäädäntö asettaa viranomaiselle vaatimuksia sekä käsiteltävän tiedon eheyden ja luottamuksellisuuden turvaamiseksi että saatavuuden takaamiseksi.

Julkishallinnolla on velvollisuus noudattaa hyvää tiedonhallintatapaa viranomaisen asiakirjojen sisältämän tiedon käsittelyssä sekä tietojärjestelmien ylläpidossa lain viranomaisten toiminnan julkisuudesta (621/1999) (jäljempänä Julkisuuslaki) sekä Julkisuuslakia täydentävien asetusten nojalla. Henkilötietolaki (523/1999) edellyttää huolellisuutta ja tarkoitussidonnaisuutta kaiken henkilötiedon käsittelyssä ja Sähköisen viestinnän tietosuojalaki (516/2004) (SVTSL) velvoittaa pitämään viestinnän tunnistamistiedot salassa. Lisäksi viestintää välittävällä organisaatiolla on oikeus käsitellä tunnistamistietoja väärinkäytösten havaitsemiseksi vasta sen jälkeen, kun pääsy viestintäjärjestelmään on rajattu. Useilla hallinnonaloilla on lisäksi omaa velvoittavaa erityislainsäädäntöä.

1.1.2 Lainsäädännön asettamat rajoitukset

Työnantajan oikeudesta torjua tietopääomaansa kohdistuvia uhkia säädetään laissa yksityisyyden suojasta työelämässä (759/2004; jäljempänä Työelämän tietosuojalaki). Työnantajan tarjoamien viestintäpalveluiden tunnistamistietojen käsittelystä säädetään kuitenkin Sähköisen viestinnän tietosuojalaissa.

Työntekijän yksityisyyttä suojeleva työelämän tietosuojalaki rajoittaa työantajan roolissa olevan organisaation ja sille palvelua tuottavien yritysten oikeutta selvittää teknisin menetelmin verkon tapahtumia. Lailla pyritään kuitenkin hakemaan tasapainoa työnantajan oikeudelle turvata tietopääomansa sekä työntekijän oikeudelle yksityisyyteen. Yksityisyyttä voidaan kohtuullisessa määrin rajoittaa työnantajan merkittävien intressien turvaamiseksi, kunhan yksityisyyteen potentiaalisesti vaikuttavat toimenpiteet käsitellään YT-menettelyllä.

Luottamuksellisen viestinnän suoja on perusoikeus, josta ei voi luopua sopimuksella – eikä työnantajalla myöskään ole mahdollisuutta solmia sopimusta kaikkien työntekijän potentiaalisten yhteistyökumppaneiden kanssa.

Henkilöiden välisen luottamukselliseksi tarkoitetun viestinnän suojaaminen on aidosti välttämätöntä. Tietoverkossa kulkee kuitenkin myös hyökkäysliikennettä, jolla on yksinomaan rikollinen tarkoitus. Lainsäädäntö ei kaikilta osin tue tällaisen liikenteen havaitsemista. Sähköisen viestinnän tietosuoja-

direktiivi (2002/58/EY) on suunniteltu suojaamaan asiakkaan yksityisyyttä tai oikeutettuja etuja yleisesti tarjottavien viestintäpalveluiden tarjoajalta eli lähinnä teleyritykseltä. Toisin kuin muualla Euroopassa, Suomessa direktiivin kansallisesti toteuttava SVTSL on ulotettu säätelemään myös julkishallinnon, yksityisten yritysten sekä yhteisöjen työntekijöille tai jäsenille tarjoamia sähköisiä viestintäpalveluita. Tällöin SVTSL ei sääntele alkuperäisen tarkoituksen mukaisesti viestin sivullisen välittäjän ja asiakkaan suhdetta, vaan myös organisaatioita, jotka voivat olla hyökkäyksen kohteena. Laki mahdollistaa hyökkäysten *automaattisen* havainnoinnin. Ongelmana on, että kohdistettuja hyökkäyksiä ei lähtökohtaisesti ole mahdollista tunnistaa automaattisin työkaluin.

1.2 Selvityksen rakenne ja kohderyhmä

Luvussa 3 esittelen yleisellä tasolla kohdistettujen hyökkäysten toteutustapoja, jotta ymmärretään, mitä pyritään torjumaan, eli havaitsemaan ja estämään. Menestyksekäs torjunta edellyttää tunkeutujan tavoitteiden ymmärtämistä, sillä yleistä ”taikasauvaa” kohdistettujen hyökkäysten torjuntaan ei todellisuudessa ole olemassa edes teoreettisena mallina.

Luvussa 4 esittelen valmistavia toimenpiteitä, jotka ovat välttämätön edellytys onnistuneelle torjunnalle. Kohdistetun hyökkäyksen havainnointi on poikkeaman tunnistamista ja selvittämistä, joten hyökkäystä ei voi havaita tuntematta normaalitilaa. Suojautuminen puolestaan haittaa usein käytettävyyttä. Niinpä on tunnettava erityissuojattavat kohteet, jotta tiukimmat suojaukset voidaan rajata vain niihin.

Luvussa 5 käsittelen kohdistettujen tietokaappausten havaitsemista ja luvussa 6 niiltä suojautumista. Tavoitteena on keskittyä nykyisen kehitys- ja ylläpitoprosessin tyypillisiin ongelmakohtiin, jotka altistavat organisaation tietopääoman kohdistetuille tietokaappauksille.

Selvityksen näkökulma – kuten laatimisen motiivikin – on selkeästi rikostorjunnallinen. Selvitys perustuu paljolti kokemusperäiseen tietoon, mutta kaikki todellisiin tapauksiin yhdistettävissä olevat yksityiskohdat on jätetty pois, jotta selvitys voisi olla julkinen. Julkisena tämän kaltaisesta selvityksestä saadaan suurin rikostorjunnallinen hyöty.

Selvitystä varten ei ole tehty kyselytutkimusta, koska kyselystä olisi aiheutunut riski eri toimijoiden – VAHTIn ja poliisin – tiedonsaantioikeuksien sekaantumisesta. Poliisin tiedonsaantioikeudet on tarkkaan säädetty vain laissa mainittujen tehtävien hoitamista varten.

Selvityksen kohderyhmänä on tietoturvallisuuden ja järjestelmäylläpidon piirissä toimivat henkilöt. Lainsäädännön vaatimukset on yritetty avata tasolla, joka olisi mielekäs erityisesti tietoteknisesti koulutetulle henkilölle.

Tarkoitus ei ole rajata kohderyhmää vain julkishallintoon, vaikka esimerkeissä vilisevät viranomaisen aineistot. Kohdistettujen hyökkäysten uhka kos-

kee kaikkia tahoja, joilla on verkossa tavoitettavaa tietopääomaa tai toimintaa. Tietokaappauksen uhka kohdistuu aivan erityisesti tuotekehitystä tekeviin yrityksiin. Yksityisellä sektorilla on huomioitava toimintavapautta mahdollisesti rajoittavat siviilioikeudelliset sopimukset sekä tasapainoilu eri maiden ristiriitaisten lainsäädäntöpuitteiden välissä.

Kiitän Seppo Sundbergia ja Mikael Kiviniemeä kumpaakin hyvistä kehitysehdotuksista sekä Minna Mannista ja Erja Kinnusta huolella tehdystä tarkastuksesta.

Sari Kajantie

2 Johdon tiivistelmä

Viranomaisella on velvollisuus huolehtia käsittelemänsä tiedon turvallisuudesta. Julkinen tieto on pidettävä sekä yleisön saatavilla että sisällöltään oikeana, kun taas salassa pidettävä tieto on pidettävä turvassa. Viranomainen vastaa siitä, ettei viranomaistoiminta loukkaa sen enempää sivullisten kuin toimenpiteen kohteenkaan oikeusturvaa – ilman laissa erikseen määrättyä perustetta.

Tehtävä ei ole erityisen helppo, sillä nykyinen tietoturvamalli ei juurikaan tue tietoon kohdistetuilta hyökkäyksiltä suojautumista.

- Nykyiset toimistoympäristöt ovat lähtökohtaisesti haavoittuvia kohdistetuille hyökkäyksille.
- Vain osa viranomaisista on rakentanut käyttöympäristönsä tavalla, joka tarjoaa riittävät edellytykset operatiivisen tiedon turvaamiselle.
- Julkishallinnon organisaatiot maksavat huomattavia summia ohjelmistovalmistajille ja IT-integraattoreille jokseenkin kelvottomasta ohjelmistolaadusta. Niin kauan kuin asiakkaat eivät vaadi nykyistä turvallisempia toimistoympäristöjä, eivät auditoi toimitettujen järjestelmien toteutusta eivätkä ole valmiita maksamaan laadukkaista – tai edes valmiista – ohjelmistoista, ohjelmistoteollisuudella ei ole kannustinta parantaa tuotantoprosessiaan.
- Operatiivisessa tietoturvatyössä huomio kohdistetaan massahyökkäyksiin, jotka on helppo havaita ja helppo torjua. Kaikkein vahingollisimpia hyökkäyksiä ei edes yritetä havaita.
- Vika on ensisijaisesti johtamisessa. Resurssit kohdennetaan toisarvoisiin kohteisiin, koska joko tietoturvatyötä ei mitata lainkaan tai sitä mitataan väärin. Julkishallinnossa on taipumusta mitata helppoja kvantitatiivisia suureita liiemmin välittämättä kuvaavatko ne sitä ilmiötä, josta halutaan tietoa. Tietoturvatyössä mitataan usein havaittuja haittaohjelmatartuntoja, vaikka se on epäolennaista. Varsinaiset tietovarkaat jätetään tällöin toimimaan vapaasti.

- Koska käyttöympäristö ei tarjoa käsiteltävälle tiedolle riittävää turvaa, tilannetta yritetään paikata työntekijöille annetuilla määräyksillä, jotka sekä haittaavat toimintaa että kuluttavat tarpeettomasti työntekijöiden resursseja. Jos tiedon suojaamisella on organisaatiolle ylipäätään jotain merkitystä, sen ei pidä olla vain työntekijän muistamisen varassa. Ei myöskään ole erityisen todennäköistä, että organisaatioon soluttautunut tietovaras pysäytetään käyttöohjeella.

Nykyisellä tietoturvamallilla saadaan aikaan turvaton ympäristö, joka heikentää organisaation tuloksellista toimintaa.

Kohdistetulla hyökkäyksellä aiheutetun vahingon rajaaminen edellyttää, että hyökkäys kyetään havaitsemaan mahdollisimman aikaisin. Ei pidä olettaa, että mikään automaattinen järjestelmä pystyisi tunnistamaan hiljaisesti liikkuvaa tietokaapparia. Kohdistetun hyökkäyksen havaitseminen on poikkeaman tunnistamista, mikä taas edellyttää normaalin verkkoliikenteen syvällistä tuntemista – lainsäädännön sallimissa puitteissa. Motivoituneen ja järjestelmänsä läpeensä tuntevan ylläpitohenkilöstön merkitystä ei voi liikaa korostaa. Mikään tietotekninen järjestelmä ei korvaa ylläpitäjää, jolla on hyvä tuntuma järjestelmän normaalitilaan.

Viranomaisen tiedon suojaaminen edellyttää käyttöympäristöjen perusturvallisuuden parantamista nykyisestä – ja järjestelmien rakentamista ihmiselle soveltuviksi.

Hyökkäysten torjunnasta aiheutuvan toiminnallisen haitan ja kustannusten tulee olla tasapainossa suojattavan intressin kanssa. Jos jonkin viranomaisen käsittelemän tiedon vuotamisesta aiheutuu henkeen tai terveyteen kohdistuva uhka, on aivan selvää, että viranomaisen on seurattava tiedon käyttöä ja estettävä tiedon asiaton käsittely siitäkin huolimatta, että seuranta maksaa, hankaloittaa tiedon viranomaiskäsittelyä tai työntekijät saattavat kokea seurannan yksityisyyttään loukkaavana. Samaan aikaan esimerkiksi viraston sisäistä tiedotuspalvelua ei ole syytä suojata tavalla, joka tekee sen käytöstä hankalaa.

Kohdistettujen tietokaappausten menestyksellinen torjunta lähtee siitä, että organisaatio aidosti ymmärtää omaa toimintaansa sekä omaan tietopääomaan kohdistunutta uhkaa. Kun tunnetaan mikä ja missä on erityistä suojausta edellyttävää tietoa, torjunta voidaan kohdentaa siihen lainsäädännön asettamissa puitteissa. Tällöin muun tiedon käsittelyä ei hankaloiteta kohtuuttomasti. Tavoitteena tulisi olla nykyistä turvallisemmin ja tuloksellisemmin toimiva organisaatio.

3 Kohdistettujen hyökkäysten tekotavoista

Hyötyä tavoittelevat rikolliset pyrkivät iskemään sinne, missä tavoitteeseen pääsee helpoimmin ja pienimmällä kiinnijäämisen riskillä. Kohdistetuissa hyökkäyksissä tekijät ovat kuitenkin valmiita näkemään enemmän vaivaa kuin satunnaisesti haavoittuvimpiin järjestelmiin kohdistuvissa hyökkäyksissä. Kohdistetun hyökkäyksen tekijällä on vahva motivaatio päästä käsiksi johonkin tiettyyn suojattuun tietoon.

3.1 Tietokaappaukset

Kohdistetun tietokaappauksen tavoitteena on lukea, kopioida tai muuttaa jotakin tiettyä tietoa, jolla on rikolliselle erityistä merkitystä.

Tietokaappauksen onnistumisen edellytys on selkeä haavoittuvuus tiedon käsittelemisen prosessissa. Haavoittuvuus voi olla tekninen tietoturva-aukko tai järjestelmäsuunnittelun heikkous, mutta se voi liittyä myös työntekijöiden tapaan suhtautua käsittelemäänsä tietoon. Rikolliset ovat osaamisprofiililtaan hyvin erilaisia. Tekninen ja sosiaalinen hakkerointitaito eivät useinkaan yhdisty samassa henkilössä. Tunkeutuja pyrkii luonnollisesti valitsemaan kohdejärjestelmästä tai kohdeprosessista sellaisia haavoittuvuuksia, jotka ovat tekijälle itselleen mahdollisimman käyttökelpoisia. Riittävän motivoituneella tietoa tavoittelevalla taholla voi myös olla käytössään suuri joukko asiantuntijoita, joilla on kullakin omanlaisensa erityistaidot. Omaa tietoaan suojaavan organisaation on suojauduttava kaiken laisilta relevanteilta uhilta. Rikolliselle riittää vain yksi hyödynnettävissä oleva haavoittuvuus.

Jotta tunkeutuja onnistuisi pääsemään kohdeorganisaation tietoon käsiksi tulematta havaituksi, hän pyrkii ohittamaan suojaukset ja naamioimaan yhteyden mahdollisimman harmittoman ja normaalin näköiseksi:

- Tunkeutuja käyttää liikennöintiin sellaisia protokollia, jotka kohdeorganisaatio nimenomaisesti päästää omaan verkkoonsa tai omasta verkostaan ulos. Esimerkkejä tyypillisistä ulkoa sisäänpäin sallituista liikenne-

käytännöistä ovat ulkoa tuleva sähköpostiliikenne, sisältäpäin avattujen TCP-yhteyksien[1] vastauspaketit sekä verkon ohjausliikenteeseen kuuluvat ICMP-paketit[2].

- Kohdistettujen tietokaappauksien estämisessä ei pidä luottaa liikaa palomuureihin. Hyökkäyksen aktiiviset vaiheet käynnistyvät organisaation sisäverkosta käsin, jolloin verkon ulkorajalle sijoitettu palomuuri ei juurikaan tarjoa suojaa. Palomuurin tarjoama turva liittyy lähinnä yhteyksien dokumentoimiseen, joka voi helpottaa tapahtumien selvittämistä.
- Hyökkäysvektoreina käytetään sellaisten ohjelmien haavoittuvuuksia, joille voi lähettää syötteitä ulkoa. Varsinaisten ulos tarjottujen palveluiden lisäksi tällaisia löytyy myös palveluiden asiakaspäästä, työasemilta. Tyypillisiä hyökkäyskohteita ovat toimisto-ohjelmistot, joille syöte lähetetään sähköpostitse käyttäjän avaamana dokumenttina, sekä yleisimmät WWW-selaimet apuohjelmineen, joista kaikista löytyy jatkuvasti haavoittuvuuksia.
- ”Epämääräisten” liitteiden poistaminen saapuvista sähköpostiviesteistä ei auta, sillä kohdistettuja hyökkäyksiä ei tehdä helposti epämääräisiksi tunnistettavissa olevilla liitteillä.
- Jos tunkeutumisessa ja tiedonkeruussa käytetään apuna haittaohjelmaa, tunkeutuja pitää tarkasti huolta siitä, ettei mikään markkinoilla oleva automaattinen ratkaisu kykene tunnistamaan juuri tätä haittakoodia. Edes parhaimmat heuristiseen tunnistamiseen kykenevät haitallisen liikenteen tai koodin havainnointijärjestelmät eivät lähtökohtaisesti kykene tunnistamaan kohdistettuun hyökkäykseen käytettävää pientä lataajaa, joka välttää käynnistyshetkellä tekemästä mitään epäilyttävää. Ne kun eivät esimerkiksi aiheuta heti verkkoliikennettä.
- Kohdistettuja haittaohjelmia ei yritetä lähettää ”M4ke M0neY F4ST”-roskaposteilla eikä vastaanottajaa vinkata WWW-sivulle, jolla käyntiä käyttäjä ei kehtaisi tunnustaa tietohallinnolle. Kohdistetussa hyökkäyksessä kehyskertomus on huolella laadittu järkevältä kuulostavaksi, jotta vastaanottajalla olisi aidosti perusteltu syy avata (suorittaa) haitallinen sisältö. Viestin lähettäjäksi on tyypillisesti väärennetty jokin uskottavalta näyttävä taho, kuten asiakas, palveluntuottaja tai yhteistyöviranomainen.

---

[1] Transmission Control Protocol (TCP) on luotettavan siirtoyhteyden eli virheenkorjauksen ja ruuhkanhallinnan tarjoava Internetin yhteyskäytäntö, jota käytetään kaikkien yhteydellisten liikennöintikäytäntöjen, kuten sähköpostin tai WWW-palvelun siirtoyhteyksiin.

[2] Internet Control Message Protocol (ICMP) on TCP/IP-verkon liikenteen ohjaukseen käytettävä protokolla, joka toimii koko ajan ”konepellin alla”. Käyttäjille ICMP-on tuttu pingistä, eli verkon latenssia mittaavista paketeista vastauksineen, jotka oikealta nimeltään ovat ICMP_ECHO_REQUEST ja ICMP_ECHO_ REPLY.

> Käyttäjille annettu ohjeistus ”älä avaa epämääräisten viestien liitteitä” ei auta suojaamaan käyttäjää kohdistetulta hyökkäykseltä. Haittakoodin lähettämiseen käytetty viesti ei ole epämääräinen.

Aiemmin tietokaappausten reittinä olivat erityisesti puutteellisesti suojatut palvelimet tai salaamaton verkkoliikenne, mutta palvelinpään ja liikennöinnin suojausten parantuessa tilanne on muuttunut. Kun yksinkertainen tunkeutuminen järjestelmään haavoittuvan palvelun kautta ei enää ole yhtä helppoa ja verkkoliikenteen kaappaaminenkin on käynyt hankalammaksi, rikolliset ovat joutuneet kehittämään monimutkaisempia työkaluja, joilla hyökätään nyt nimenomaan asiakaspäähän. Kohdevalinta on sinällään perusteltu: asiakaspäästä voi jatkossakin olettaa löytyvän eniten haavoittuvia kohteita. Samalla kerättävien tietotyyppien joukko on laajentunut. Siinä missä aiemmin kerättiin lähinnä luottokorttinumeroiden kaltaista palvelinpään tietokantoihin säilöttyä dataa, nyt kerätään mitä tahansa dataa asiakaspäästä. Usein kaapattava tieto on helposti tunnistettavaa, määrämuotoista ja automaattisesti prosessoitavaa dataa, kuten WWW-lomakkeille syötettävää tietoa, mutta se voi olla mitä tahansa tietoa, jota käsitellään työasemalla tai johon työaseman käyttäjän oikeuksilla päästään käsiksi.

Kun tulovirrat laajoista identiteettivarkauksista ovat kasvaneet, on käynyt kannattavaksi tuottaa haittaohjelma-aihioita myytäväksi ja vuokrattavaksi. Uuden sukupolven haittaohjelmatuotanto on tehnyt toiminnasta entistä ”teollisempaa”. Toiminta ei vaadi aivan yhtä suurta vaivannäköä kuin ennen, jos kohdeorganisaation tapa turvata tietojaan on puutteellinen.

Osin samoja työkaluja tai ainakin samaa koodia on nyt voitu ottaa käyttöön myös kohdistetuissa hyökkäyksissä. Kaikenlaisten hyötyä tavoittelevien hyökkäysten painopiste onkin selkeästi siirtynyt kohti asiakaspäässä tapahtuvaa näppäinpainallusten keruuta sekä käyttäjän tiedostojen tai yhteyksien kaappaamista. Teollistuminen on tosin myös lisännyt ilmiön näkyvyyttä. ”Käsin” tunkeutuvia yritysvakoojia on todella varsin vaikea havaita. Jos ja kun kohdistettuja hyökkäyksiä tehdään samoilla työkaluilla, joilla laajoja identiteettivarkauksiakin tehdään, todennäköisyys havaitsemiselle kasvaa.

3.2 Esimerkki: haittaohjelmalla toteutettu kohdistettu tietokaappaus

Tarkastellaan esimerkkitoteutusta, jotta ymmärretään millaisia vaiheita tyypilliseen haittaohjelmaa hyödyntävään kohdistettuun hyökkäykseen liittyy. On syytä korostaa, että kyseessä todella on vain esimerkki. Kohdistettuja tietokaappauksia voidaan yhä tehdä yhtälailla ihmisvoimin kuin haittaohjelmillakin. Haittaohjelma-avusteinen tietokaappaus vain on rikollisen näkökulmasta

tällä hetkellä ylivoimaisesti tehokkain tekotapa, sillä sen toteutuskustannukset ovat monta kertaluokkaa soluttautumista tai työntekijän suostuttelua pienemmät. Tekotapa on myös tuloksellinen, koska varsin harva organisaatio suojaa tietoaan riittävän hyvin työasemiin kohdistetuilta tietokaappauksilta.

Haittaohjelmalla työasemapäähän toteutettu hyökkäys koostuu tyypillisesti useista eri vaiheista, jotka aiheuttavat erilaisia havaittavissa olevia oireita – joskaan niiden havaitseminen ei ole aivan helppoa.

3.2.1 I - Tiedusteluvaihe

Hyökkääjä hankkii kohdeorganisaatiosta tietoa jo paljon ennen varsinaista hyökkäystä. Tiedustelu voi tapahtua yhtälailla sosiaalisilla kuin teknisilläkin menetelmillä, riippuen hyökkääjän ominaisuuksista.

Rikollinen voi kerätä avoimista lähteistä julkista tietoa esimerkiksi kohdevirastossa käynnissä olevista projekteista ja henkilökunnan yhteistyökumppaneista. Julkishallinnossa käytetyistä ohjelmistoista voi saada kohtalaisen helposti tietoa julkisten tarjouskierrosten ja vuolaan raportoinnin tähden. Sähköpostiohjelmat versioineen saa selville lähettämällä organisaation tietopalveluun kysymyksen vaikkapa organisaation alueellistamissuunnitelmista. WWW-selaimista vastaavat tiedot saa ohjaamalla organisaation työntekijöitä rikollisen hallussa olevalle sisällöltään harmittomalle sivustolle sähköpostissa kierrätettävän vitsin avulla.

Verkon aktiivilaitteet, kuten reitittimet tai kytkimet, antavat usein epäsuorasti kysyjälle tarkkaa tietoa sisäverkon topologiasta, vaikka yksittäiset työasemat tai palvelimet eivät ulkoa tulleisiin kyselyihin vastaisikaan.

3.2.2 II - Haittakoodin ujuttaminen kohdeorganisaatioon

Jotta kohteeseen toimitettava ylimääräinen koodi ei herättäisi huomiota, haittaohjelma jaetaan usein kahteen osaan; lataajaan ja varsinaiseen tietoa keräävään haittakoodiin. Ensimmäinen osa on usein pieni ja toiminnaltaan hyvin yksinkertainen lataaja, jonka ainut tehtävä on varsinaisen tietoa kaappaavan haittaohjelman hakeminen verkosta kohteeseen.

Lataaja voidaan lähettää sähköpostin liitteenä olevassa dokumentissa, jolla hyödynnetään toimisto-ohjelmiston haavoittuvuutta. Vaihtoehtoisesti kohde voidaan houkutella WWW-palveluun, josta haittaohjelma ujutetaan käyttäjän koneelle käyttäjän haavoittuvaa WWW-selainta hyväksikäyttäen.

Liitteen avaamisen eli murtokoodin suorittamisen todennäköisyyttä voidaan kasvattaa käyttämällä jotakin tunnekoukkua. Tavoitteena on tällöin saada vastaanottaja toimimaan ensin ja ajattelemaan vasta myöhemmin. Suhteellisen helposti herätettävä tunne on suuttumus tai puolustusreaktio, joita voidaan saada aikaan vaikkapa voimakkaalla kritiikillä kohdehenkilön toimintaan.

Käyttäjän käynnistäessä toimisto-ohjelman lukeakseen dokumentin sisällön, haittakoodi murtautuu järjestelmään toimisto-ohjelman haavoittuvuuden kautta. Haavoittuvuudesta ja toimisto-ohjelmasta riippuen käyttäjälle voidaan näyttää tiedoston tekstisisältö, jotta käyttäjän olisi mahdollisimman hankala havaita tapahtunutta. Dokumentin lukemisen käynnistyminen voi tuntua hitaalta, mutta nykyisissä toimistoympäristöissä käyttäjä voi perustellusti pitää sitä hyvinkin normaalina.

3.2.3 III - Haittaohjelman aktivoituminen

Hyökkääjä voi asettaa lataajan odottamaan jonkin aikaa ennen aktivoitumista, jotta sähköpostiliitteen avaamisen yhteydessä käynnistyvät verkkoyhteydet eivät aiheuttaisi automaattista hälytystä. Pidempikestoinen odottaminen mahdollistaa myös sen, että lataajan toimittamiseen liittyvät tietotekniset jäljet, kuten sähköpostin tai http-välityspalvelinten (proxy) lokien tunnistamistiedot, ehtivät kadota.

Aktivoituessaan lataaja hakee varsinaisen tiedonkeruukoodin verkosta hyökkääjän määrittelemästä paikasta. Osoite voi olla kovakoodattuna lataajaan tai lataaja voi hakea voimassaolevan konfiguraatiotiedoston kontrollipalvelimestaan heti aktivoiduttuaan ennen tiedonkeruukoodin hakua. Kokonaisuuden kannalta käyttökelpoisempi tapa valitaan rikollisen hallitseman verkkoinfrastruktuurin luotettavuuden ja dynaamisuuden mukaan.

3.2.4 IV - Tiedonkeruu

Myös tiedonkeruukoodi saattaa odottaa ennen omaa aktivoitumistaan.

Aktivoiduttuaan haittaohjelma ryhtyy keräämään tietoa kohdejärjestelmästä. Haittaohjelma saa talteen näppäinpainallukset, näkee käyttäjän ruutunäkymän, voi käsitellä työaseman muistia ja tallennuslaitteita. Haittakoodilla on siten lähtökohtaisesti pääsy kaikkeen tietoon, jota työaseman haltija työasemassaan käsittelee, sekä mahdollisesti myös muualla sijaitsevaan tietoon, joihin on automaattisesti pääsy työaseman haltijan oikeuksilla.

Jos käyttäjä pääsee haittaohjelman saastuttamalla työasemalla käsiksi tai käsittelee salassa pidettävää aineistoa, haittaohjelma voi kaapata senkin ja lähettää edelleen hyökkääjälle

Tieto voidaan kerätä ennalta määrätyllä haittaohjelmaan koodatulla tavalla tai etäohjatusti siten, että rikollinen valitsee haittaohjelman löytämästä datasta kiinnostavan osan.

3.2.5 V - Tiedon lähettäminen ulos organisaatiosta

Kun haittaohjelma on kerännyt tarvittavan tietomassan, se pitää saada organisaation verkosta ulos rikollisten haltuun.

Tiedon kuljettaminen sisäverkosta ulos on usein suoraviivaisempaa kuin haittakoodin saaminen sisään, sillä nykyinen suojausmalli keskittyy lähinnä ulkoa tulevien yhteyksien rajoittamiseen. Kuljetus voidaan toteuttaa millä tahansa tiedonsiirtoprotokollalla – myös itse tarkoitusta varten toteutetulla – mihin tahansa kohdeporttiin rikollisen hallussa olevaan kohdeosoitteeseen. Jos organisaatio rajoittaa ulos päästettävän liikenteen kohdeportteja, haittaohjelma voi käyttää sallittuja portteja protokollasta riippumatta.

Tiedon kuljetuksessa voidaan käyttää myös rikoskumppania. Fyysinen läsnäolo kuitenkin kasvattaa toteutuksen paljastumisriskiä ja tietokaappauksen toteutuskustannuksia. Tällöin myös menetetään automatisoinnin tuoma skaalautuvuus.

3.3 Palvelunestohyökkäykset

Palvelunestohyökkäyksen tarkoituksena on nimensä mukaisesti estää jonkin verkkopalvelun asiallinen käyttö. Palvelunestohyökkäyksen alle mahtuu kuitenkin hyvin erilaisia ilmiöitä pelkän julkisen WWW-palvelun ruuhkauttamisesta varsinaisiin operatiivisiin järjestelmiin kohdistuviin tai kriittisen infrastruktuurin toimintaa haittaaviin hyökkäyksiin.

Julkisuudessa on esiintynyt esimerkkejä myös kiristystarkoituksessa tehdyistä palvelunestohyökkäyksistä. Ilmiön voi kuitenkin olettaa jäävän kohtalaisen marginaaliseksi, sillä teon liiketoimintalogiikka on verkkorikokseksi harvinaisen huono. Järjestäytyneen verkkorikollisuuden liiketoimintamalli perustuu poikkeuksellisen hyvään riskin ja tuoton suhteeseen alhaisilla toteutuskustannuksilla; verkossa riski jäädä kiinni on reaalimaailmaa pienempi ja tuottopotentiaali suurempi. Kiristyksessä ei päde muihin verkkorikoksiin olennaisesti kuuluva kiinnijäännin riskin pienuus, koska rikolliset joutuvat ottamaan rahaa vastaan. Palvelunestohyökkäys myös sitoo rikollisen infrastruktuurin. Samaa bot-verkkoa[3] on hankala käyttää samaan aikaan huomattavasti paremmin kassavirtaa tuottavaan toimintaan kuten identiteettivarkauksiin.

Palvelunestohyökkäys voidaan toteuttaa joko ylivoimalla tai käyttämällä jotakin kohdepalvelun ohjelmistohaavoittuvuutta, joka mahdollistaa resurssien – kuten muistin tai verkko-sockettien – varaamisen ilman aika- tai määrärajoituksia.

Hyökkäyksessä käytettävä protokolla vaikuttaa torjuntaan sekä jossain määrin lähteen jäljittämiseen. UDP[4]:lla tai ICMP:llä toteutettujen hyökkäysten läh-

[3] Bot-verkko [roBOTtiverkko, botnet, bottiverkko] on murretuista koneista muodostettu etäohjattava verkko, jota rikolliset käyttävät infrastruktuurinaan.

[4] User Datagram Protocol on kuljetuskerroksen yhteyskäytäntö, joka ei TCP:n tavoin tarjoa luotettavaa siirtoyhteyttä, joten sitä käytetään vain pakettihävikkiä sietävien sovellusten, kuten eräiden audiopalveluiden, toteuttamiseen. UDP-paketin lähettäjä voi helposti väärentää lähdeosoitteen

deosoite on käytännössä aina väärennetty, mutta sellainen liikenne on myös helppo pysäyttää saapuvan liikenteen suodatuksella. Sovellusprotokollaa, esimerkiksi http:tä, käyttävät yhteydet ovat hankalia torjua, koska haitallisia yhteyksiä on vaikea erottaa automaattisesti legitiimeistä selailuyhteyksistä – erityisesti jos yhteydet tulevat tuhansilta erillisiltä bot-verkon koneilta. TCP:n päällä toimivissa sovellusprotokollissa lähdeosoitteen väärentäminen saman reititysalueen ulkopuolelle on itsessään hankalaa, joten hyökkäys todennäköisesti tulee juuri siitä suunnasta, joka kohteena olevan palvelun lokeista löytyy. Lokijälkeä seuraamalla ei kuitenkaan löydy suoraan tekijää, vaan bot-verkon koneet, eli joukon murrettujen koneiden haltijoita. Tällöin lähdeosoitteiden paljastumisella ei ole juurikaan merkitystä: vastatoimenpiteet kohdistuvat niihin sivullisiin, joiden kone on murrettu ja kaapattu mukaan hyökkäykseen.

3.3.1 Julkisen verkkopalvelun käytön estäminen

Viranomaisen julkisen tiedotuspalvelun lamauttamisesta aiheutuva vahinko on pääsääntöisesti viestinnällinen ja imagoon kohdistuva. Siitä voi toki olla haittaa, ettei viranomaisen tieto ole helposti saatavilla, mutta tällaisesta hyökkäyksestä ei kuitenkaan aiheudu vaaraa tietojen luottamuksellisuudelle tai eheydelle. Viranomaisella on yleensä myös vaihtoehtoisia tiedotuskanavia, joita käyttäen viestintäkatkosta aiheutuvaa vahinkoa voidaan rajata.

Tällaisen hyökkäyksen motiivi on yleensä myös viestinnällinen: motiivin voi kiteyttää lausahdukseen ”mun isin auto kulkee kovempaa, ku sun isin auto!!!” Variaatioita teemasta on nähty nuorisojoukkioiden, erilaisten aatteiden ja uskontojen sekä kansakuntien välillä.

Erityisesti julkishallinnossa on kuitenkin otettava huomioon myös muut mahdolliset motiivit, kuten poikkeamankäsittelyyn osallistuvien resurssien sitominen toissijaiseen kohteeseen, epävarmuuden aiheuttaminen tai kohdeorganisaation vasteen – yhtälailla havainnointikyvyn kuin reagointitavankin – mittaaminen.

WWW-sivuston lamauttaminen on kohtuullisen helppoa, senhän täytyy näkyä ulkoverkkoon. Hyökkäyksen toteuttamisen vaikeusastetta voi kasvattaa rakentamalla järjestelmän kuormitusta kestävälle alustalle sekä lisäämällä verkkopalvelun hajautusta. Riippuu palvelun merkityksestä, onko hajautuksesta aiheutuva kustannusten kasvu perusteltua vai ei.

3.3.2 Operatiivisen järjestelmän lamauttaminen

Operatiivisiin järjestelmiin tai viranomaisen kriittiseen infrastruktuuriin kohdistuvan hyökkäyksen tavoitteena voi olla reaalielämän vahingon aiheuttaminen tai viranomaisen operatiivisen toiminnan haittaaminen. Hyökkäyksen aiheuttama uhka on vakava, sillä onnistuneella hyökkäyksellä voidaan saada aikaan jopa henkeen tai terveyteen kohdistuvaa vahinkoa. Kunnolla

suojattuun toimintoon kohdistuva palvelunestohyökkäys vaatii kuitenkin aivan eri luokan toimenpiteitä ja osaamista kuin julkisen palvelun lamauttaminen.

Operatiiviset järjestelmät eivät yleensä näy suoraan ulkoverkkoon, joten niitä ei lamauteta ylivoimalla, vaan edellä kuvatuilla ohjelmistohaavoittuvuuksilla, joita julkishallinnon ostamissa järjestelmissä kyllä yleensä riittää. Siinä missä julkisen palvelun ylikuormittaminen on hyvin helppoa, niin operatiivisen järjestelmän kuormitus edellyttää huolellista esivalmistelua, koska kuormitus voidaan tehdä lähinnä organisaation sisäverkosta käsin uloimpien suojakerrosten ohittamisen jälkeen.

Operatiiviset järjestelmät tulisikin aina sijoittaa kokonaan eri verkkoalueelle kuin julkiset tiedotuspalvelut, jotta tiedotuspalveluihin kohdistuneet hyökkäykset eivät vaikeuttaisi viranomaisen varsinaista toimintaa.

Nimenomaisesti operatiivisiin järjestelmiin tai kriittiseen infrastruktuuriin kohdistuvien palvelunestohyökkäysten torjunnassa tärkeintä on rakentaa sekä kuormaa kestäviä että vikasietoisia järjestelmiä. Tavoitteet ovat jossain määrin ristiriitaisia, sillä kuormankesto saattaa edellyttää hajautusta tai kuormanjakojärjestelmiä, jotka lisäävät olennaisesti järjestelmän monimutkaisuutta ja siten vikaherkkyyttä. Ominaisuuksien välillä tulisi siis löytää organisaation toiminnan kannalta järkevä kompromissi. Järjestelmien toteutus – eikä vain dokumentaatio – on auditoitava säännöllisesti. Testauksessa tulee käyttää riittävän suurta määrää täysin virheellistä liikennettä, jotta järjestelmän kyky sietää protokollasta poikkeavia syötteitä saadaan esille.

4 Varautuminen – havaitsemisen ja suojautumisen edellytykset

4.1 Varautumisen tavoite

Varautumisen tavoitteena on parantaa organisaation edellytyksiä havaita kohdistettuja hyökkäyksiä sekä vaikeuttaa niiden toteuttamista.

Varautuminen kohdistettujen hyökkäysten havaitsemiseen

Hyväkään kohdistettujen hyökkäyksien havainnointikyky ei estä hyökkäyksien tapahtumista. Se ei kuitenkaan edes ole havainnoinnin tarkoitus, vaan ensisijainen tavoite on *vahinkojen rajaaminen*. Mitä nopeammin hyökkäys havaitaan, sitä todennäköisemmin löydetään jokin mekanismi, jolla hyökkäyksestä aiheutuvaa haittaa voidaan vähentää.

Toinen tavoite on *todisteiden turvaaminen*. Todisteita tarvitaan yhtälailla rikosprosessiin kuin organisaatiota itseään varten. Organisaation on voitava selvittää, miksi hyökkäys onnistui ja mitä voidaan jatkossa tehdä kohdistettujen hyökkäysten vaikeuttamiseksi.

Varautuminen kohdistetuilta hyökkäyksiltä suojautumiseen

Suojautumisen tavoitteena on *vaikeuttaa* kohdistettujen hyökkäysten toteuttamista. Suojautumisen toteutuksessa on tärkeää löytää organisaation oman toiminnan kannalta järkevä tasapaino käytettävyyden ja suojan välille, suojaus kun väistämättä hankaloittaa tiedon käsittelemistä. Suojautuminen ei saa estää organisaation toiminnan kannalta välttämätöntä viestintää, sillä myös tiedon saatavuus on tietoturvallisuuden komponentti. Koska julkishallinnossa suojeltavat intressit (salassa pidettävä operatiivinen aineisto, henkilötiedot, jne.) ovat niin suuret, hienoista käytön hankaloitumista on kuitenkin voitava sietää. Mitä paremmin organisaatiossa pystytään tunnistamaan ja erottelemaan tiukkaa suojausta edellyttävät kohteet, sitä joustavammin muiden palveluiden käyttö voidaan toteuttaa.

4.2 Varautumisen menetelmistä

Kohdistetun hyökkäyksen havainnointi on poikkeaman havaitsemista ja sen syyn selvittämistä. Jotta poikkeama olisi ylipäätään mahdollista tunnistaa, organisaation on tunnettava normaalitila ja oltava valmis selvittämään havaitun poikkeaman syy. Aina syy ei suinkaan ole tahallinen hyökkäys. Taustalla voi yhtälailla olla jokin tahaton ”näppihäiriö” tai virheellinen määrittely. Koska ajatus jokaisen poikkeaman käsittelystä käsin ei ole realistinen, on tärkeää hahmottaa mitkä omassa ympäristössä ilmenevät poikkeamat ovat erityisen uhkaavia.

Kohdistetuilta hyökkäyksiltä suojautumisessa tärkein edellytys on se, että organisaatio ymmärtää toimintaansa. Kun tiedetään, missä suojattavaa tietoa ja helposti hyödynnettäviä haavoittuvia kohteita on, voidaan järeimmät suojaus- ja havainnointikeinot kohdistaa aiempaa tarkemmin. Näin voidaan myös minimoida muulle käytölle aiheutettava haitta.

4.2.1 Suojattavan tiedon kartoittaminen

4.2.1.1 Lainsäädännön perusteella turvaamista edellyttävä aineisto

Ensimmäinen tehtävä on tunnistaa salassa pidettävä aineisto, minkä suuri osa julkishallinnon organisaatiosta onkin jo tehnyt. Kannattaa huomata, että salassa pidettävän aineiston joukko on olennaisesti laajempi kuin turvaluokiteltava aineisto. (Tätä kirjoitettaessa vielä voimassaolevan) Julkisuusasetuksen mukaan salassa pidettäviä – mutta eivät turvaluokiteltavia – ovat JulkL 26 § 1 momentin 3), 4) ja 6) kohtien perusteella salassa pidettävät asiakirjat. Näistä kohta 6) eli kanteluasiakirjat koskevat koko julkishallintoa. Salassapitovaatimuksen voi asettaa myös muu lainsäädäntö kuin julkisuuslaki. Esimerkiksi henkilötiedot tai terveystiedot ovat myös salassa pidettäviä ja monilla aloilla on omaa erityislainsäädäntöä, joka vaikuttaa tiedon turvaamisen tarpeeseen. Lisäksi myös siviilioikeudelliset sopimukset voivat edellyttää tiedon turvaamista.

Julkishallinnossa on paljon täysin julkista aineistoa, jonka luottamuksellisuutta ei millään tavoin tarvitse suojata, mutta jonka eheänä säilymisestä on silti pidettävä tarkasti huolta. Tällaista aineistoa ovat esimerkiksi viranomaisen tiedotteet ja varoitukset.

4.2.1.2 ”Kiinnostava” aineisto

Koska kohdistetuissa tietorikoksissa tavoitellaan tiettyä tietoa, josta rikollinen voi hyötyä, organisaation tulisi säännöllisesti ajatella käsittelemäänsä aineistoa potentiaalisen rikollisen näkökulmasta: mikä on sellaista tietoa, jota kaap-

paamalla voidaan hankkia hyötyä? Hyöty ei tässä välttämättä ole vain taloudellista, vaan se voi yhtälailla olla ideologista.

Kiinnostavaa tietoa pohdittaessa kannattaa muistaa rikollisten suuri kirjo. Massiivisten identiteettivarkauksien toteuttajien näkökulmasta hyödyllistä tietoa on vain automaattisesti tunnistettava ja prosessoitava määrämuotoinen henkilötieto, kun taas yritysvakoilija voi olla valmis suuriin ponnistuksiin päästäkseen käsiksi kaikenlaiseen tutkimustietoon.

Kiinnostavaa tietoa voi olla järjestelmien pääsynvalvontadata siinä missä varsinainen substanssitietokin. Siksi selvityksessä tulisikin kuulla erilaisissa rooleissa toimivia työntekijöitä. Tiedon omistajien, käsittelijöiden ja alustajärjestelmien ylläpitäjien näkemykset kiinnostavasta datasta voivat erota suuresti toisistaan.

4.2.1.3 Missä erityistä suojaamista edellyttävää aineistoa käsitellään?

Sen jälkeen kun organisaatiolla on selkeä näkemys suojausta edellyttävästä tai muuten kiinnostavasta tiedostaan, tulisi selvittää, missä kaikkialla tällaista aineistoa todellisuudessa käsitellään. Yleensä dataa ei nimittäin löydy vain tiukasti suojatuista ja huolella ylläpidetyistä tietovarastoista, joissa sen tulisi sijaita, vaan tietoa saatetaan käsitellä missä vain minkä työntekijät sattuvat kokemaan näppäräksi. Tietoa saattaa löytyä ylläpitämättömiltä ”labrakoneilta”, kotikoneilta, puutteellisesti suojatuilta kannettavilta tai erilaisista mobiililaitteista.

Tärkeintä on, että organisaatio saa todellisen kuvan tilanteesta. Siksi selvitys kannattaa tehdä mahdollisimman vapaassa hengessä ja välttäen kovin suorasanaista palautetta huonoistakaan käytännöistä, sillä kovin ankara vastaanotto voi kannustaa pimittämään tietoa.

Tiedon kerääjän valintaan kannattaa myös kiinnittää huomiota. Edellä mainituista syistä olisi parempi, jos kerääjä ei olisi esimiesasemassa, vaan riippumaton asiantuntija. Toisaalta kerääjän tulisi olla sellaisessa asemassa, että kohteet katsovat mahdolliseksi puhua kerääjän kanssa myös salassa pidettävistä turvallisuusjärjestelyistä (JulkL 26:1, 7. kohta).

Palautteen aika on vasta sitten, kun tieto on koottu ja analysoitu. Jatkokartoitusten onnistumista voi edesauttaa se, että kriittisimmän palautteen antaja ei ole sama henkilö kuin tiedon kerääjä. Ylipäätään palautteenannossa kannattaa kiinnittää huomiota viestintätapaan. Tiedon suojaamisen näkökulmasta ensisijaisena tavoitteena ei ole syyllisten etsiminen, vaan toimintatavan muuttaminen. Syyllisten osoittelu voi haitata tavoitteen toteutumista.

4.2.2 Omien järjestelmien tunteminen.

Reaalimaailman murtovarkaat eivät tule asuntoon ensisijaisesti keskeltä seinää, vaan todennäköisimmin ovista tai ikkunoista. Tilanne on verkossa aivan sama. Niinpä organisaation tulee ensin selvittää, missä on sellaisia potenti-

aalisesti haavoittuvia kohteita, joissa haavoittuvuutta on suhteellisen helppo hyväksikäyttää. Kun ”ovet ja ikkunat” tunnetaan, ylläpidollisia toimenpiteitä tai verkkoliikenteen suodatusta voidaan keskittää erityisesti niihin.

4.2.2.1 Helpoimmin hyväksikäytettävissä olevien kohteiden kartoitus

Ensimmäisen joukon säännöllisesti seurattavia kohteita muodostavat kaikki ne komponentit, jotka käsittelevät ulkoverkosta tulevaa dataa tai jotka liikennöivät itse ulos. Tällaisia kohteita ovat esimerkiksi:

- Ohjelmistot, jotka ottavat suoraan vastaan komentoja ulkomaailmasta. Tällaisia ovat organisaation tarjoamat palvelut, kuten WWW-palvelu, auktorisoitu nimipalvelu, LDAP-hakemistopalvelu tai sähköpostipalvelu.
- Työasemien WWW-selaimet apuohjelmineen, -objekteineen ja kirjastoineen.
- Työasemien sähköpostiohjelmistot sekä toimisto-ohjelmat ja dokumenttien katseluohjelmat.
- Liikennettä ohjaavat tai suodattavat reitittimet tai palomuurit.

Teknisten komponenttien lisäksi asiakaspalvelutehtävissä toimiva henkilökunta voi avuliaisuudessaan muodostaa hyväksikäytettävissä olevan kohteen.

Ylläpitohenkilökunta puolestaan yleensä osaa olla kertomatta tietoturvallisuuteen liittyviä yksityiskohtia, mutta avoimeen kulttuuriin tottunut ylläpitohenkilöstökin voi olla provosoitavissa kertomaan yksityiskohtia esimerkiksi kumotakseen perusteettomat väitteet organisaation tiedonsuojausmenettelyjen puutteellisuudesta.

4.2.2.2 Erityisen haavoittuvien kohteiden tunnistaminen

Helposti hyväksikäytettävissä oleva kohde on siis sellainen, johon pääsee ulkopuolelta käsiksi. Erityisen haavoittuva kohde voi olla myös jokin ulkopuoliselta liikenteeltä suojattu kohde, jota on kuitenkin helppo käyttää hyväksi sisäverkosta käsin. Vastaavasti kohde voi olla myös työntekijä, joka ei toimi asiakasrajapinnassa.

Organisaation on selvitettävä selvästi haavoittuvat kohteet, joita ei ole mahdollista suojata kunnolla järjestelmän omin keinoin. Tällaisia ovat esimerkiksi järjestelmät, joissa takuuehdot tai jokin sovellus estää haavoittuvien varusohjelmien päivittämisen. Sellaisia voivat olla esimerkiksi useat fyysiset kulunvalvontajärjestelmät, mittalaitteisiin liittyvät työasemat tai jotkin yksittäistä sovellusta ajavat ulkopuolisen toimittajan ympäristöt.

4.2.3 Minkä palvelun estämällä saa aikaan uhrille haittaa – tai tekijälle huomiota?

Palvelunestohyökkäyksiin varautuakseen organisaation tulisi tunnistaa, missä on sellaisia resursseja, joiden ylikuormitus aiheuttaa ongelmia toiminnan jatkuvuudelle. Lisäksi tulisi tunnistaa ne palvelut, joiden toiminnan estämällä rikollinen voi saada viestinnällistä hyötyä tai missä on sellaisia resursseja, joiden toiminnan voi estää helposti ja näin kiinnittää ylläpidon huomion merkityksettömään kohteeseen.

4.2.3 Informaation kulun hallinta.

4.2.3.1 Sisäverkon osiointi

Organisaation verkon ulkorajalle sijoitettu rajapalomuuri ei missään olosuhteissa ole riittävä turva julkishallinnossa käsiteltävän tiedon suojaksi, vaan myös sisäverkkoon tulee rakentaa sekä liikenteen seuranta- että rajoituskykyä. Helpoimmin se voidaan toteuttaa jakamalla sisäverkko osiin millä tahansa aktiivilaitteilla, jotka mahdollistavat liikenteen rajoittamisen ja tapahtumien kirjaamisen. Verkon osiointi edesauttaa olennaisesti sekä kohdistettujen hyökkäysten havaitsemista että niiltä suojautumista.

Hyökkäysten havainnoinnin kannalta verkon osiointi on tärkeää, koska muuten mahdollisuudet seurata verkkoliikennettä ovat hyvin rajalliset. Kyse ei ole vain teknisistä, vaan myös normiston asettamista rajoituksista. Lainsäädäntö estää välitettävän viestintäliikenteen järjestelmällisen seuraamisen (tarkemmin luvussa 5.1). Siksi kaikki sellaiset viestintäpalvelut, joiden käytön seuranta on lainsäädännössä voimakkaasti rajoitettu, on syytä erotella sellaisista palveluista, joiden käytön seuranta on lainsäädännön puitteissa a) mahdollista ja b) käsiteltävän tiedon suojan kannalta tarpeellista.

Osiointi on tärkeää myös suojautumisen kannalta. Tietokaappaajalle aiheutettu pienikin lisähankaluus on omiaan parantamaan tiedon suojaa. Toisaalta tiedon luottamuksellisuuden ja eheyden suojaaminen usein käytännössä hankaloittaa tiedon käyttöä, mikä heikentää sen saatavuutta, aiheuttaa käyttäjille vaivaa ja organisaatiolle kustannuksia. Viisaasti toteutetulla verkon osioinnilla voidaan vähentää käyttäjille aiheutuvaa hankaluutta ja vaivaa, koska tällöin tiukempia tietoturvamenettelyitä ei tarvitse kohdistaa kaikkeen käyttöön vaan ainoastaan erityistä turvaamista edellyttävän tiedon käyttöön. Verkon osioinnilla voidaan jakaa erilaista suojaustasoa edellyttävät – ja erilaista haittaa aiheuttavat – toiminnot erilleen.

Käsiteltävälle tiedolle potentiaalisen uhan aiheuttavat komponentit tulisi eristää omiin verkkoihinsa. Tällaisia ovat:

- Ulos näkyvät palvelimet. Erityisesti tiedottamiseen liittyvät palvelimet tulisi sijoittaa verkkoteknisesti kokonaan eri paikkaan kuin sisäverkon palvelut, sillä ulos tarjottavat palvelut ovat alttiita palvelunestohyökkäyksille, joilta ei voi suojautua (viranomaisen käytettävissä olevin resurssein) kuin rajatusti. Jos palvelut sijoitetaan myös eri yhteyden päähän kuin sisäverkosta ulos kuljetettava liikenne, mahdollinen palvelunestohyökkäys ei juuri vaikuta organisaation muuhun toimintaan.
- Eri osastojen tai yksiköiden tuotantotyöasemaverkot. Jos verkot on eroteltu toisistaan, yhdessä verkossa aiheutunut poikkeamatilanne ei haittaa muiden osastojen toimintaa.
- Verkot, joihin henkilökunta tai vierailijat voivat kytkeä kannettavan tietokoneen.

Erillisiin verkkoihin tulisi sijoittaa myös erityistä suojaa tarvitsevat järjestelmät sekä järjestelmät, joiden liikenteen tarkkailulle lainsäädäntö asettaa erilaiset vaatimukset.

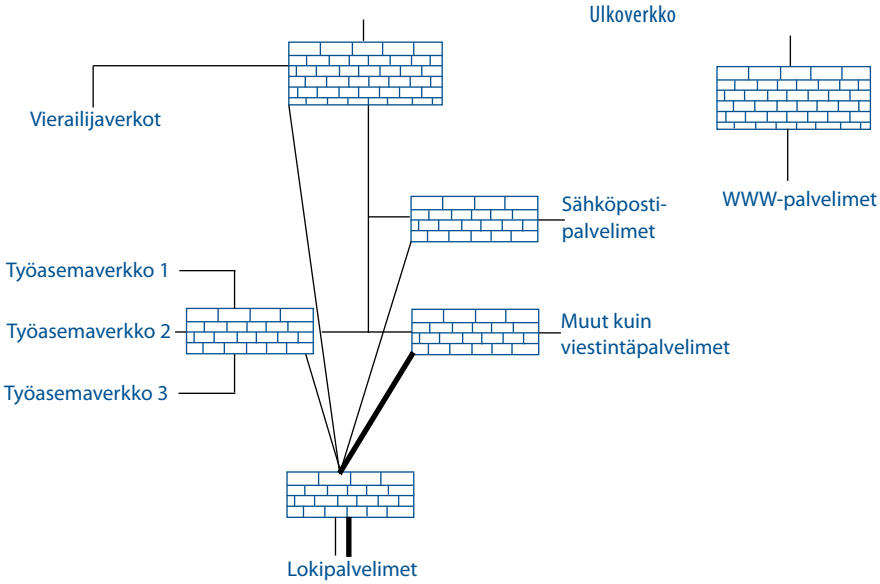
Tällaisia ovat:

- Viestintäpalvelimet, kuten ne postipalvelimet, joilta käyttäjät lukevat sähköpostinsa. Viestintäpalvelimilla organisaatio tarjoaa käyttäjilleen viestintäpalvelua välittäjän roolissa (ns. yhteisötilaajana), eikä organisaatio voi seurata liikennettä kuin hyvin rajoitetusti (ks. luku 5.1).
- Muut palvelimet ja järjestelmät, kuten
  - sisäiset tiedosto-, tietokanta-, todennuspalvelimet
  - järjestelmät, joita ei sopimus- tai sovellusteknisistä syistä ole mahdollista päivittää
  - lokijärjestelmät, jotka keräävät organisaation tietojärjestelmien lokit.

Nämä ovat sellaisia palveluita, joihin kohdistuvassa liikenteessä organisaatio on selkeästi osapuolena ja voi siten käsitellä tunnistamistietoja myös sisältöön kohdistuvien väärinkäytösten selvittämiseksi.

Kuvassa on hahmoteltu kohteita, jotka tulisi vähintään erotella verkkoteknisesti toisistaan:

Karkea hahmotelma verkkotopologiasta



Kun viestintäpalvelimet on eroteltu muista palvelimista ja muut palvelimet on eroteltu työasemaverkoista, viranomaisen asiakirjoja sisältäviä palvelimia yhdistävien verkkojen liikenteeseen voidaan kohdistaa olennaisesti tarkempaa seurantaa ja liikennerajoituksia kuin mitä muutoin olisi lainsäädännön puitteissa mahdollista.

4.2.3.2 Verkkoliikenteen salaaminen

Osa julkishallinnon organisaatioista on jo reagoinut ipv4-protokollan heikkouksiin5, mutta loppujenkin olisi syytä turvata sisäverkon liikenne salaamalla hyötykuorma ja edesauttamalla yhteyden osapuolten tunnistamista.

Verkkoliikenteen salaamisen tarkoitus ei ole vain hankaloittaa tiedon kaappaamista verkosta, vaan yhtä tärkeää on se, että hyötykuorman salaaminen edesauttaa organisaation omia mahdollisuuksia seurata liikennettä. Kun verkkoliikenne on salattua, sitä on lainsäädännön puitteissa helpompi seurata, koska viestinnän sisältö ei voi vahingossakaan paljastua ylläpitäjälle. Organisaation

[5] Liikennöinnin osapuolia ei varmisteta ja sisältö kuljetetaan selväkielisenä, koska ipv4 kehitettiin ympäristöön, jossa muihin verkon liikennöijiin saattoi luottaa. Protokolla ei ole huono. Ainoastaan täysin väärässä käytössä.

omiin palvelimiin kohdistuvien yhteyksien pakettien seuranta on mahdollista kun organisaatio on yhteydessä osapuolena, eikä substanssisisältö voi joutua seurannassa vääriin käsiin. Salaus ei kuitenkaan poista velvollisuutta seurannan huolelliseen harkintaan. Kannattaa muistaa, että joissakin protokollissa – lähinnä pikaviestintä- tai vertaisverkkoprotokollissa – viestinnän osapuolten tunnistamistiedot paljastuvat suoraan paketin otsikkotiedoista, joten kaiken liikenteen geneeristä seuraamista liikenteen salaaminen ei mahdollista.

Salaus myös estää tiedonkaappaajaa hankkimasta (sisältö)tietoa verkkoliikennettä kuuntelemalla, jolloin saadaan poistettua yksi suhteellisen helppo keino tiedonkaappaajan valikoimasta.

Ylläpidon niin sanotut hyvät käytännöt kehottavat välttämään verkkoliikenteen salaamista, koska se estää haitallisen sisällön automaattisen seulomisen hyökkäyksenhavainnointijärjestelmillä. Kohdistettujen hyökkäysten osalta niiden havainnointikyky on kuitenkin ylipäätään niin pieni, että edut voittavat selkeästi haitan.

4.2.3.3 Ylläpitäjien keskinäisen kommunikaation turvaaminen

Usein organisaatiolla on jo paljon kohdistettujenkin hyökkäysten havainnointia edesauttavaa tietoa, mutta se on väärässä paikassa. Siitä voi tulla toimintaa ohjaavaa informaatiota vasta, kun eri paikoissa sijaitsevat tiedon palaset saadaan yhdistettyä. Tyypillisesti verkon ja sen eri palveluiden ylläpitovastuut on jaettu eri ryhmille. Rajapalomuurin lokista voidaan nähdä erikoinen lähdeosoite, mutta vasta kohdepalvelimen loki kertoo, mitä yhteydellä tapahtuu. Poikkeaman syyn selvittäminen edellyttää näiden tietojen yhdistämistä.

Jokaisella verkon koneella – testilaitteillakin – tulisi olla vastuullinen ylläpitäjä, joka seuraa järjestelmän toimintaa. Vastuullisen ylläpitäjän on myös oltava tietoinen vastuustaan – myös ulkoistettujen palveluiden osalta. Erityisesti erilaisten rajapintojen vastuut on selvitettävä ja kommunikoitava selkeästi kaikille osapuolille.

Organisaatiolla tulisi olla ennalta määritelty prosessi tietojen luontevaan vaihtamiseen. Keinona voisi olla organisaation tietoturvavastuullisten ja ylläpitäjien ja muodostama CSIRT (Computer Security Incident Response Team[6]), jonka sisällä tietoja voisi vaihtaa mahdollisimman vapaasti tietoturvallisuuden ylläpitämiseksi.

Organisaation tietoturvavastaavien, lakimiesten ja teknisen henkilökunnan kannattaa avata kommunikaatioyhteys ajoissa. Väistämättä kestää aikaa, ennen kuin kieli saadaan hiottua samaksi. Sen jälkeen erilaisten tarkastelunäkökulmien yhdistäminen on aidosti hedelmällistä. Toimintaa poikkeamatilanteissa voidaan harjoitella ”sotaharjoituksissa”. Havaintojen analysoinnin lisäksi

[6] Tunnettiin aiemmin yleisesti lyhenteellä CERT ennen kuin CERT/CC teki CERT®-termistä rekisteröidyn tavaramerkin. Nyttemmin käytössä on yleensä jokin variaatio ”Incident Response Team”-teemasta.

opitaan toimimaan normaalista poikkeavassa olosuhteessa. Poikkeamatilanneviestinnästä ja ”sotaharjoituksista” kerrotaan tarkemmin VAHTI-ohjeessa : Tietoturvapoikkeamatilanteiden hallinta (3/2005).

4.2.3.4 Käyttäjäkoulutus

Organisaation työntekijöille tulisi jakaa tietoa kohdistettujen tietokaappausten riskeistä, yhtä lailla teknisistä kuin puhuttamalla toteutetuista.

Tiedottamisessa tulee kuitenkin huomioida kohderyhmän tarpeet. Joillekin henkilöstöryhmille toimii parhaiten kategorinen tietojenluovutuskielto, kun taas toiset ryhmät on saatava ymmärtämään kiellon perusteet. Erilaisten asiantuntijaryhmien tulee sisäistää, mikä todella on salassa pidettävää aineistoa sekä millä perusteella ja millä edellytyksillä sitä voi luovuttaa esimerkiksi muille viranomaisille.

Erilaiset käyttöä hankaloittavat suojausmekanismit on myös tärkeää perustella henkilökunnalle selkeästi. Käytön kohtuuton hankaloittaminen ajaa parhaat työntekijät käyttämään huomattavan määrän energiaa suojausten kiertämiseen – urheilumielessä, jos ei muuten – kun taas perusteltuun rajoitukseen mukaudutaan helposti. Myös käyttörajoituksista tulee tiedottaa tavalla, joka on kullekin eri kohdejoukolle mielekäs. Osa käyttäjistä tarvitsee yksinkertaiset toimintaohjeet, osa taas tarvitsee perustelut, joiden avulla voi sekä ymmärtää käyttörajoituksen tarpeen että soveltaa käyttötapaa uusiinkin ympäristöihin. Perusteiden selvittäminen erilaisille asiantuntijatehtävissä toimiville henkilöille on ylipäätään hyödyllinen harjoitus. Jos ei rajoitusta voi perustella tavalla, joka kuulostaa asiantuntijan korviin järkevältä, rajoitusta ei todennäköisesti ole toteutettu järkevästi.

Kannattaa huomata, että käyttäjäkoulutuksen vaikuttavuus on rajallinen kohdistettujen tietokaappausten torjunnassa. Käyttäjillä ei ole yleisissä toimistoympäristössä juuri minkäänlaisia mahdollisuuksia havaita tietoa keräävän haittaohjelman toimintaa. Käyttäjäkoulutuksella ei myöskään torjuta organisaatioon soluttautunutta tietokaappaajaa, joka käyttää omia – työtehtäviään varten saamiaan – käyttöoikeuksia tiedon kokoamiseen.

5 Kohdistettujen tietokaappauksien havaitsemisesta

Kohdistetun hyökkäyksen tekijän tavoitteena on liikkua tietojärjestelmissä kenenkään havaitsematta. Koska hyökkääjä mukailee käyttäjäkunnan normaaleja yhteyskäytäntöjä, hyökkäyssormenjälkien tunnistamiseen perustuva automaattinen järjestelmä ei lähtökohtaisesti pysty havaitsemaan tällaista liikennöijää. Kohdistetun hyökkäyksen havaitseminen ei ylipäätään ole mahdollista ilman, että organisaatio tuntee syvällisesti normaalin verkkoliikenteensä – eikä se silloinkaan ole helppoa.

5.1 Havainnointi verkossa - lainsäädännön asettamat rajoitukset

Suomessa lainsäädäntö asettaa varsin tiukkoja rajoituksia kohdistettujen hyökkäysten havainnointimenetelmiin.

Kaikilla organisaatiolla on lähtökohtaisesti oikeus suojautua hyökkäyksillä aiheutetuilta vahingoilta. Viranomaisilla on oikeuden lisäksi myös velvollisuus käsitellä viranomaisen tietoaineistoa hyvän tiedonhallintatavan mukaisesti (JulkL 18 §, henkilötiedon osalta henkilötietolaki, etc.), mikä käytännössä edellyttää kykyä havaita aineistoon kohdistuva oikeudeton käsittely.

Hyökkäysten havainnointi ei kuitenkaan saa loukata perustuslaissa taattua luottamukselliseksi tarkoitetun viestinnän suojaa (Sähköisen viestinnän tietosuojalaki (SVTSL)) eikä myöskään kohtuuttomasti työntekijöiden yksityisyyttä (Työelämän tietosuojalaki).

Viestinnän tunnistamistietojen käsittelyä rajaa viestintäverkossa sähköisen viestinnän tietosuojalaki, jonka mukaan:

- Viestinnän *osapuoli* saa käsitellä tunnistamistietoja haluamallaan tavalla (8 §) – ei siis viestinnän välittäjä, vaan viestinnän lähde tai kohde.

  Viestintäpalvelua työntekijöilleen tarjoava työnantaja ei ole viestinnän osapuoli, vaan ulkopuolinen välittäjä. Työnantaja on yhteyden osapuolena vain, jos kyseessä on jo tunnistamistietojen perusteella selkeästi työnantajalle eikä yksittäiselle työntekijälle tarkoitettu viesti. Tällainen on *esimer-*

kiksi http-GET-pyyntö viraston WWW-palvelimelle viraston tiedotteisiin tai sähköposti osoitteeseen kirjaamo@virasto.fi.

- Viestin *välittäjällä* ei lähtökohtaisesti ole oikeutta käsitellä tunnistamistietoja, muuta kuin SVTSL:ssä erikseen mainituissa tarkoituksissa.

Suurin osa käsittelyn mahdollistavista perusteista koskee vain teleyrityksiä, jotka tarjoavat maksullisia palveluita asiakkailleen[7].

Yhteisötilaajia käsittelyoikeuksista koskevat konkreettisesti 9 § (”Tunnistamistietojen käsittely palvelujen toteuttamiseksi ja käyttämiseksi”), 12 § (Käsittely teknistä kehittämistä varten) ja 14 § (Käsittely teknisen vian tai virheen havaitsemiseksi).

Päivitysversiossa 125/2009 pykälät 13 a - 13 j tarkentavat, kuinka tunnistamistietoja saa käsitellä 9 § toteuttamiseksi. Aiemmasta poiketen näyttäisi siltä, että ulkoakaan tulevan liikenteen lähdeosoitetta ei enää voi käyttää vahingollisen yhteyden hakukriteerinä – ainakaan ilman raskasta manuaalisen käsittelyn menettelyä. Niinpä organisaatio ei voi selvittää automaattisesti, mihin kaikkiin oman verkon koneisiin jostakin vahingollisesta lähdeosoitteesta on liikennöity. Esimerkiksi kohdeosoitetta tai protokollaa voi kuitenkin käyttää kriteerinä.

9 § mahdollistaa tunnistamistietojen käsittelyn nimenomaan viestintäpalvelun tietoturvallisuudesta huolehtimiseksi, joten viranomaistyönantaja ei saa käsitellä sähköpostijärjestelmän tunnistamistietoja huolehtiakseen oman tietopääomansa suojaamisesta. Lain uusin versio ei tuo tältä osin uutta. Se kylläkin mahdollistaa toimenpiteet epäiltäessä yrityssalaisuuden luovuttamista *ulkopuoliselle*, mutta EI viranomaistiedon vuotajan selvittämistä. Työnantaja ei siten saa selvittää sähköpostilokeista, kuka työntekijöistä on lähettänyt omasta työsähköpostiliittymästään salassa pidettävää viranomaistietoa ulos8 eikä myöskään luovuttaa tietoa esitutkintaviranomaiselle.

SVTSL:n 20 § sallii eräät muut toimenpiteet tietoturvan toteuttamiseksi, mutta niistä ei juuri ole hyötyä kohdistettujen hyökkäyksien tor-

---

[7] Sähköisen viestinnän tietosuojalain paikoitellen haastava sovellettavuus on hyvinkin ymmärrettävää, kun muistaa laajan soveltamisalan. Lain lähtökohtana oleva sähköisen viestinnän tietosuojadirektiivi (2002/58/EY) on laadittu säätelemään teleyritysten toimintaa suhteessa asiakkaisiin. Suomessa direktiivin toteuttava laki on kuitenkin ulotettu koskemaan myös julkishallintoa, yhteisöjä sekä ja yksityisiä yrityksiä suhteessa käyttäjiin. Tällöin laista aivan väistämättä tulee varsin monimutkainen eikä kaikilta osin aivan direktiivin hengen mukainen.

[8] Jos organisaatio lähtee tarkastelemaan seurannan edellytyksiä väärinkäytön kautta (13 d §), vaikkapa kieltämällä salassa pidettävän tiedon lähettämisen viestintäverkon välityksellä organisaation ulkopuolelle, tulkintaan on syytä kysyä kanta Viestintävirastosta. Rajanvedon tekee viimekädessä tuomioistuin. Määräys on myös muotoiltava siten, ettei se hankaloita viranomaisyhteistyötä. Samalla on myös muistettava, että viestintää on SVTSL:n mukaan kaikki yleiseen viestintäverkkoon kytketyn verkon tietoliikenne.

junnassa, sillä pykälä mahdollistaa päätöksenteon lähinnä automaattisilla hyökkäyksenhavainnointijärjestelmillä vahingollisen sisällön tai liikenteen estämiseksi. Jos kuitenkin on selkeästi pääteltävissä, että viesti sisältää tunnistamatonta haittakoodia, pykälä sallii jopa (haitallisen) sisällön manuaalisen käsittelyn.

Lain uusimmassa versiossa 20 §:n automaattisen käsittelyn kriteeriksi on lisätty myös maksuvälinepetoksen valmistelu (RL 37:11). Kannattaa huomata, että pykälä ei salli minkään muun Phishingin[9], esimerkiksi henkilötietojen kalastelun, automaattista pysäyttämistä. Pykälän soveltaminen ylipäätään edellyttää rikostunnusmerkistön punnintaa, joka ei yleensä ole aivan suoraviivaista edes rutiinia hankkineelle esitutkintaviranomaiselle.

Asiaa on hankala ilmaista täsmällisesti kuulostamatta komiteamietinnöltä, joten konkretisoidaan vielä esimerkillä, jossa verrataan henkilötietoa sisältävän rekisterin ja sähköpostin käytön seurantaa:

Viranomaisen rekisterin tai tunnistuspalvelun omistaja on tietokanta- tai autentikointiyhteydessä osapuoli ja siten saa käsitellä tunnistamistietoja haluamallaan tavalla (Sähköisen viestinnän tietosuojalaki). Viestinnän osapuolena organisaatio voi käsitellä lokitietoja myös työnantajaroolissa, kunhan käsittelytapa on esitelty YT-menettely mukaisesti (Työelämän tietosuojalaki). Esimerkiksi Väestötietojärjestelmässä käsitellään salassa pidettävää henkilötietoa, jonka joutuminen vääriin käsiin loukkaa rekisteröidyn yksityisyyttä. Tällöin yhteyksien seuranta on selkeästi perusteltua.

Kun samainen organisaatio on viestinnässä vain teknisen välittäjän roolissa vaikkapa sähköpostipalvelun ylläpitäjänä, organisaatio saa käsitellä tunnistamistietoja kylläkin viestintäjärjestelmän turvallisuutta uhkaavien tietoturvapoikkeamien selvittämiseksi, mutta ei työnantajaroolissa työntekijöiden työpanoksen tai muun vastaavan seurantaan. Organisaation toiminnan tai työntekijöiden käsittelemien henkilötietojen suojaaminen tietoliikennettä seuraamalla ei ole mahdollista, vaikka suojattava intressi olisi kuinka suuri. Jos organisaatio lähtee toteuttamaan seurantaa väärinkäytön perusteella (13 d §), tulkintaan on syytä kysyä kanta Viestintävirastosta ja Tietosuojavaltuutetulta.

[9] Tietojen ”kalastaminen” suurilta käyttäjäjoukoilta kysymällä niitä sähköpostitse johonkin peitetarinaan vetoamalla. Phishingissä käytetään siten hyväksi ohjelmistohaavoittuvuuden sijaan inhimillistä ”haavoittuvuutta” eli hyväuskoisuutta.

Jonkin yksittäisen menetelmän laillisuuden arvioinnissa kannattaa muistaa, ettei lakiteksti ole RFC[10], jossa syntaksi aina voittaa semanttisen merkityksen. Kun mietitään, onko jokin haluttu toimenpide laillinen, kannattaa aina miettiä, mikä on a) toimenpiteen tavoite ja b) mikä on toimenpiteen mahdollisesti estävän lain tarkoitus. Mikä on se intressi, jota lailla pyritään suojelemaan ja loukkaako toimenpide intressiä? Jos loukkaa, onko toimenpiteeseen silti jokin laista löytyvä erityinen oikeutus?

Kun ymmärretään sekä oman toiminnan että lain varsinainen tarkoitus, on helpompi hakea lain tarkoittama tasapaino ristiriidassa oleville oikeuksille. Tällöin on usein mahdollista löytää jokin kompromissi, jonka avulla voidaan toteuttaa edes rajattu osa tavoitellusta toimenpiteestä. Verkon osiointi (ks. Luku Varautuminen; 4.2.3 Informaation kulun hallinta) on esimerkki tällaisesta tasapainoilusta. Välitettävän viestinnän täydellinen seuranta ei yksinkertaisesti ole mahdollista, mutta kun osiointi on tehty riittävän tarkasti, kuhunkin verkko-osioon voidaan kohdistaa osion liikenteen tyypille sopivaa seurantaa. Jos voidaan olla varmoja, että tietyn verkko-osion seurannalla EI voi paljastua sellaista luottamukselliseksi tarkoitettua viestintää, jossa organisaatio ei olisi osapuolena, silloin – ja vain silloin – liikennettä voidaan seurata tarkasti. Seuranta tulee toteuttaa työelämän tietosuojalain mukaisesti huolellisuutta ja tarkoitussidonnaisuutta noudattaen sekä huomioiden velvoite YT-menettelyyn.

Kun mietitään, voiko jotakin verkkoliikenteen seurantakeinoa käyttää:

1. Ensin tulee kysyä: *”Voiko seurannalla paljastua luottamuksellisen viestinnän sisältöä tai tietoa osapuolista?”*
   Luottamukselliseksi tarkoitettua viestintää voi olla sähköpostin lisäksi missä tahansa muussa viestintään käytetyssä protokollassa, kuten irc, http[s] tai pikaviestintäprotokollat. Myöskään julkiseksi tarkoitetussa viestinnässä välittäjä ei saa käsitellä tunnistamistietoja muuten kuin laissa sallittuja tarkoituksia varten.

2. Jos viestintää voi paljastua, voidaan edelleen kysyä: *”Onko viestintä sellaista, jossa oma organisaatio ei ole selkeästi osapuoli?”*
   Palvelun omistaja on osapuolena esimerkiksi kirjautumisyhteydessä, tietokantayhteyksissä tai organisaatio-osoitteisiin lähetetyissä sähköposteissa.

3. Jos organisaatio on osapuolena, tulisi vielä kysyä: *”Käsitelläänkö viestinnässä sellaista viranomaisen tietoa, joka on suojattava ja jonka suojaaminen perustellusti edellyttää liikenteen seurantaa?”*

[10] Internet Engineering Task Forcessa käsiteltävä Internetin liikennöintikäytäntöjä ehdottava, määrittelevä tai standardoiva Request for Comments -dokumentti. <URL: http://www.ietf.org/rfc.html> Teknistaustaisille tietoturva-asiantuntijoille RFC:t ovat joskus kokolailla lainsäädäntöä tutumpi elementti.

Esimerkiksi salassa pidettävän aineiston käsittelyssä selkeästi tarvitaan erityistä suojaa.

Julkisen vallan käyttö on aina sopeutettava täsmällisesti vallitsevaan lainsäädäntöön – lakia taivuttamatta. Jos lain edellyttämä toiminta ei ole kohtuullista tai oikeudenmukaista, viranomaisen tehtävä on nostaa lainsäädännön epäkohdat esille, jotta eduskunta voi hallituksen esityksestä muuttaa reaalielämässä huonosti toimivaa normistoa. Toiminta on siitä huolimatta toteutettava lain edellyttämällä tavalla.

5.2 Huomioita havaitsemisen menetelmistä

5.2.1 Havainnointi verkossa

5.2.1.1 Normaalitilan selvittäminen

Havainnointiprosessin ensimmäisenä tehtävänä on oppia tuntemaan normaalitilanne, jotta ainakin joissain olosuhteissa pystytään tunnistamaan sellaisia poikkeamatilanteita, joiden taustalla saattaa olla kohdistettu hyökkäys. Mahdollisesti havaittavissa oleva toiminto on esimerkiksi tiedon kuljettaminen organisaation verkosta ulos tai tiedon järjestelmällinen kokoaminen niistä sisäverkon kohteista, joihin kaapatulla työasemalla tai työaseman käyttäjällä on pääsyoikeus. Jotta ongelmakenttä ei kävisi turhan tylsäksi, poikkeamien tunnistaminen ei luonnollisesti auta havaitsemaan sellaista tietoa uloskuljettavaa yhteyttä, joka otetaan normaaleilla protokollilla normaaleilta näyttäviin kohteisiin.

Normaaliin liikenteeseen perehtyminen luonnollisesti kuluttaa ylläpitoresursseja, mutta sen jälkeen kun ylläpidolla on edes karkea käsitys verkossa normaalisti näkyvästä liikenteestä, aikaa ei kulu harmittoman, mutta poikkeavalta näyttävän liikenteen syyn selvittämiseen. Tyypillisiä esimerkkejä oudolta näyttävää liikennettä aiheuttavista laitteista ovat verkkotulostimet, videovalvontajärjestelmät ja eräät kulunvalvontajärjestelmät.

Merkittävä osa poikkeamista aiheutuu erilaisista käyttäjän tai ylläpidon tekemistä tahattomista virheistä. Jotta ylläpito ei joutuisi reagoimaan koko voimalla jokaiseen poikkeamaan, sen tulisi vähitellen oppia tunnistamaan myös millaisia virheitä käyttäjät tyypillisesti tekevät.

Sitten (ja vasta sitten!) kun ylläpito aidosti ymmärtää automaattisten tunnistamisjärjestelmien rajoitukset, niitä kannattaa ehdottomasti käyttää apuna. Niistä on paljon hyötyä suuren lokimassan jäsentämisessä ja tunnettujen hyökkäystapojen seulomisessa. Tunnistettavissa olevien poikkeamien määrä on kasvanut huomattavasti sekä laskentatehon että algoritmien kehittymisen myötä. Silti IDS ei lähtökohtaisesti pysty havaitsemaan kuin sen osan poikkeamista, joka käyttäytyy ennalta havainnointikriteeriksi valitulla tavalla. Edes oppiviin

järjestelmiin ei saa luottaa liikaa – nehän oppivat vasta tapahtuman jälkeen. Johtopäätösten merkityksen arviointi tulisi myös aina jättää ihmisen käsiin. Mikään havainnointikeino ei voi korvata sitoutuneen ja järjestelmän läpikotaisin tuntevan ylläpitäjän intuitiota.

5.2.1.2 Käyttökelpoisia apuvälineitä

Verkon tilanteen hahmottamista auttavat liikennemäärätilastoista tehdyt visualisoinnit ja erityisesti Flow-tieto[11], jota reitittimet myös pystyvät tuottamaan suhteellisen kivuttomasti. Siitä voidaan helposti havainnoida poikkeamia, kuten vaikkapa nimipalvelukyselyt omasta verkosta ulkopuolisiin nimipalvelimiin. Haittakoodi usein käyttää – bot-verkon hallinnan helpottamiseksi – rikollisen bot-verkossa ylläpitämää omaa nimipalvelua.

Vaikka pääsyvalvontaa suorittaviin laitteisiin kuten palomuureihin ei tule luottaa liikaa verkon suojaamisessa, ne ovat erinomaisia apuvälineitä yhteyksien havaitsemisessa ja dokumentoinnissa. Lokit tulisi kuitenkin ohjata turvalliseen lokipalvelimeen, jotta tunkeutujan olisi mahdollisimman hankala muuttaa lokeja. Verkkolaitteet tuottavat lokia täsmälleen sillä protokollatasolla, jolla ne liikennettä käsittelevät. Verkkokerroksella toimiva pääsyvalvontasuodatin ei siten näe liikenteen kohdeporttia. Kohdistettujen hyökkäysten havainnoinnin kannalta on olennaista kirjata lokiin nimenomaan onnistuneet yhteydet, eikä vain torjuttuja yhteyksiä (torjuttujen yhteyksien kirjaus on lähinnä palomuurivalmistajan markkinointiviestintää).

Nykyisin havaitsemisen painopiste tuntuu vielä olevan ulkoa sisään avattavissa yhteyksissä. Kohdistettujen hyökkäyksien havaitsemisen kannalta olennaista on kuitenkin tunnistaa omasta verkosta ulos avatut yhteydet, sillä ne ovat niitä harvoja tietokaappauksen vaiheita, jotka saattavat olla helpostikin havaittavissa.

Hunajapurkit (a honeypot[12]) ovat vahva, joskin ylläpidolta taitoa ja sitoutumista vaativa työkalu satunnaisesti kohdistuvien hyökkäysten havainnointiin. Niistä saatavan tiedon informaatioarvo on kuitenkin pienempi tarkasti kohdistetuissa hyökkäyksissä. Hunajapurkki ei luonnollisesti näe sellaista liikennettä, joka on lähetetty jollekin tarkasti rajatulle vastaanottajalle.

---

[11] IETF:n IPFIX-työryhmä Ciscon Netflow 9:n pohjalta määrittelemä avoin Flow-protokolla

[12] Honeypot on haavoittuvalta työasemalta tai ohjelmistolta näyttävä kokonaisuus, jonka avulla voidaan havainnoida hyökkäyksen tarkkaa tapahtumankulkua: mitä muutoksia haittaohjelma järjestelmässä tekee, mitä tietoa se kerää ja minne se liikennöi. Passiivinen honeypot pystyy havaitsemaan vain satunnaisesti kohdistuvia hyökkäyksiä, jotka sattuvat osumaan honeypotiin.

5.2.2 Havainnointi tietojärjestelmissä

Tietojärjestelmissä tulisi seurata kriittisten komponenttien muutoksia ja selvittää kunkin muutoksen syy. Vaikka kohdistetut hyökkäykset onkin suunnattu pääasiassa työasemiin, tulee seurannan kohdistua kaikkiin laitteisiin, joilla, joiden kautta tai joiden tarjoamin oikeuksin on mahdollista käsitellä suojattavaksi tarkoitettua tietoa.

Työasemissa kriittisiä komponentteja ovat ulkopäin tulevia yhteyksiä hyväksyvät ohjelmistot; sähköpostiohjelmistot, WWW-selaimet apuohjelmineen sekä toimisto-ohjelmistot, kaikki kirjastoineen. Palvelimissa kriittisiä kohteita ovat erityisoikeuksin suoritettavat ohjelmat kirjastoineen, verkkopalveluohjelmistot määrittelytiedostoineen, kaikki pääsyvalvontatiedot, autentikointijärjestelmät sekä muut komponentit, joita käytetään käsittelyoikeuksien vaihtamiseen. Havaintoja kannattaa tehdä sekä järjestelmän sisällä vertaamalla tarkistussummia että kartoittamalla ulkoa käsin järjestelmän tarjoamia palveluita – tarkastettavasta järjestelmästä riippumattomilla työkaluilla. Näin saadaan selville, mitä palveluita järjestelmä todellisuudessa tarjoaa ulos, eikä vain mitä olisi tietoturvapolitiikan perusteella tarkoitus tarjota.

Tunkeutujan lisäämät palvelut sen enempää kuin muutkaan komponentit eivät ole näkyvissä järjestelmän omin työkaluin, jos tunkeutuja on lisännyt kernel-tason ”suodattimen” (rootkit[13]) tai vaihtanut järjestelmän tilaa selvittävät ohjelmat sellaisiksi, jotka toimivat muuten oikein, mutteivät näytä tunkeutujan lisäämiä prosesseja tai tiedostoja. Jos tunkeutuja on muuttanut vain työkaluja tai kirjastoja, järjestelmän tilasta saa kuitenkin oikeaa tietoa käyttämällä omia staattisesti linkattuja työkaluja (kirjoitussuojatulta medialta).

Kriittisten palvelinkomponenttien seurannasta aiheutuvaa vaivaa voi pienentää olennaisesti pitämällä päällä vain toiminnan kannalta välttämättömät verkkopalvelut ja poistamalla erityisoikeudet antavat suid- ja sgid-bitit tarpeettomista kohteista. Tarpeellisten palveluiden selvittäminen on luonnollisesti resursseja vaativa urakka, mutta se helpottaa seurantaa jatkossa suuresti.

5.2.3 Käyttäjien tekemät havainnot

Jos kohdistettu hyökkäys aiheuttaa mitään havaittavissa olevia piirteitä, oireina on tyypillisesti jokin hyvin pieni normaalista poikkeava ilmiö, kuten ylimääräinen salasanakysely tai dokumentinlukuohjelman ylimääräinen vilahdus ruudulla.

Teknisen havainnoinnin lisäksi organisaatiolla tulisi olla vaivaton ja helppokäyttöinen valmis prosessi käyttäjien tekemien havaintojen kirjaamiseen ja

[13] rootkit on kernel-tasolla toimiva yleensä haittaohjelman mukana tuleva komponentti, jonka tarkoituksena on peittää haittaohjelman olemassaolo käyttäjältä ja käyttäjän oikeuksin toimivilta sovelluksilta. Rootkitit peittävät yhtälailla prosesseja, tiedostoja kuin avattuja verkkoyhteyksiäkin.

käsittelyyn. Vaivattomuus on olennaista, sillä ei voi olettaa, että kiireiset käyttäjät kuluttaisivat kohtuuttomasti aikaa ilmiön kuvailemiseen ja laajoihin kyselylomakkeisiin vastailemiseen. Ainut tapa saada systemaattisesti tietoa on tarjota mahdollisuus sen lähettämiseen helposti.

Yhtälailla tärkeää on muistaa antaa palautetta poikkeamasta ilmoittaneelle käyttäjälle. Käyttäjälle tulisi antaa tieto siitä, mihin toimenpiteisiin ilmoituksen johdosta on ryhdytty ja mistä poikkeamassa oli kyse, jos se vain on julkisuuslain puitteissa mahdollista. Käyttäjät ovat kyllä valmiita näkemään hiukan vaivaakin, jos kokevat, että havaintojen ilmoittamisella on merkitystä.

6 Kohdistetuilta tietokaappauksilta suojautumisesta

Suurin osa organisaatioiden suojaustoimenpiteistä suunnataan satunnaisesti uhrinsa valitseviin hyökkäyksiin, jotka on helppo havaita ja kohtuullisen helppo torjua. Niiltäkin suojautuminen on toki perusteltua: satunnaisilla hyökkäyksillä aiheutettu vahinko on kasvanut aiemmasta, kun järjestäytyneesti toimivat rikollisryhmät ovat ryhtyneet kaappaamaan helposti rahaksi muutettavaa määrämuotoista tietoa, kuten luottokorttinumeroita, asiointitunnuksia tai sähköpostiosoitteita. Tilanne on silti ongelmallinen. Kun huomion saavat lähinnä hälyä aiheuttavat hyökkäykset, hiljaisesti toteutettuja tietokaappauksia ei havaita juuri lainkaan eikä niiltä suojauduta riittävästi.

Kohdistetuilta hyökkäyksiltä on mahdollista suojautua vain parantamalla käyttöympäristöjen perusturvallisuutta nykyisestä ja rakentamalla järjestelmät olennaisesti nykyistä käyttäjäystävällisemmiksi. Kohdistetulta hyökkäykseltä suojautuminen edellyttää heikkouksien minimointia sellaisissa kohteissa, joissa heikkouden hyväksikäyttö voi aiheuttaa vahinkoa. Tilanteeseen voi vaikuttaa joko vähentämällä haavoittuvuuksia tai rajaamalla vahinkoa, jota yksittäisen haavoittuvuuden hyväksikäytöllä voidaan saada aikaan.

Suojauksella aiheutetun vaivan ja kustannusten täytyy olla tasapainossa hyödyn kanssa. Sen jälkeen kun tiedetään (4.2.2), mikä on erityisesti suojaamista edellyttävää aineistoa, missä sitä käsitellään ja missä on haavoittuvia sekä hyväksikäytettävissä olevia kohteita, suojautumisjärjestelyt voidaan suunnitella kunkin kohteen edellyttämällä tavalla. Tällöin käsiteltävää tietoa voidaan suojata aiempaa tehokkaammin ilman, että viestintää ja muuta käyttöä hankaloitetaan tarpeettomasti. Viestintäyhteyksien katkaiseminen tai viestinnän vaikeuttaminen perusteettomasti ei ole kohtuullinen ratkaisu. Myös tiedon saatavuus on tietoturvallisuuden komponentti – puhumattakaan sen merkityksestä organisaation toimintakyvylle tai imagolle.

6.1 Käyttöympäristösuunnittelu

Kuten varautumisen yhteydessä todettiin, helpoimmin hyväksikäytettäviä komponentteja ovat ulkoa syötteitä tai suoritettavaa koodia saavat ohjelmistot

aina palvelinohjelmistoista työasemien WWW-selaimiin ja toimisto-ohjelmistoihin. Paikallisesti rikollinen voi käyttää hyväkseen haavoittuvia todentamiseen liittyviä komponentteja sekä ohjelmistoja, joiden suorituksen ajaksi nostetaan suoritusoikeuksia[14]. Hyväksikäytettävien komponenttien väärinkäyttöä voidaan hankaloittaa lukuisilla eri keinoilla, joista tässä eräitä keskeisimpiä.

6.1.1 Ohjelmistovalinnat

Tietoturvallisuus ei ole vain pakollinen termi, joka tulee muistaa mainita räätälöityjen ohjelmistojen vaatimuksissa, vaan se tulisi huomioida paljon nykyistä paremmin myös peruskäyttöympäristön ohjelmistovalinnoissa. Tällä hetkellä kaikkein haavoittuvin komponentti on yleensä työasema ohjelmistoineen.

Julkishallinnossakin tunnutaan hyväksyttävän, että pelkkä sähköpostitse tulleen dokumentin sisällön selvittäminen saa vaarantaa salassa pidettävän tiedon luottamuksellisuuden, koska sähköpostitse saapuvaa suoritettavaa koodia ei pääsääntöisesti edes yritetä eristää viraston tietopääomasta. Viranomaisten ei pitäisi sietää tilannetta, joka ei todellisuudessa ole mitenkään sisäsyntyisesti tietotekniikkaan kuuluva, vaan liittyy yleisimpiin ohjelmistoihin ja toteutuksiin. Ohjelmistoteollisuudella ei ole kannustinta parantaa tuotantoprosessia, ellei turvallisuus ala näkyä valintakriteerinä myös peruskäyttöympäristön hankinnoissa.

Toimistoympäristön ohjelmistovalinnoissa kannattaa huomioida ohjelmiston toimittajan ylläpitoprosessi ja ohjelmiston turvallisuushistoria. Hyvä historia ei ole tae tulevasta menestyksestä, mutta huono historia antaa todennäköisiä viitteitä yhtä surkeaan jatkoon. Palvelinohjelmien valinnassa tulisi nykyistä enemmän painottaa vikasietoisuutta ja skaalautuvuutta.

6.1.2 Suoritusympäristön rajaus

Suurin osa nykyisin yleisesti käytettävistä toimistoympäristöistä ovat haavoittuvia kohdistetuille hyökkäyksille. Haavoittuvuuksien hyväksikäyttöä ei tällöin voi kategorisesti estää. Hyväksikäytöllä aiheutetun vahingon määrää voi kuitenkin pienentää olennaisesti rajaamalla haitallisen koodin toimintaympäristöä. Rajatun ympäristön voi toteuttaa monella eri tavoin; keveimmillään yksinkertaisin käyttöoikeusrajauksin, tehokkaimmillaan suorittamalla ulkoa tuleva koodi eristetyssä ympäristössä.

[14] Esimerkkinä unix-taustaisten järjestelmien suid tai sgid-suoritusoikeuksin varustetut ohjelmat.

6.1.2.1 Käyttöoikeuksista yleisesti

Tietoa keräävä haittaohjelma toimii niillä oikeuksilla, jotka se on käynnistyessään saanut. Yleisesti haittaohjelma toimii samoin oikeuksin kuin millä haittaohjelman hyväksikäyttämää haavoittuvaa ohjelmaa ajanut prosessi sattui toimimaan haittaohjelman tunkeutumishetkellä. Haittaohjelma pystyy keräämään talteen kaiken sen tiedon, johon pääsee käsiksi samoin oikeuksin. Esimerkiksi monet kertakirjautumisjärjestelmät laajentavat suuresti myös haittaohjelman tavoitettavissa olevan tiedon määrää.

Käyttöympäristö tulee aina rakentaa siten, että järjestelmiä käytetään rajatuilla tavallisen käyttäjän oikeuksilla. Vain toiminnon todella sitä vaatiessa voidaan käyttää erilaisia pääkäyttäjän oikeuksia tai rajattuja erioikeuksia. Kertakirjausjärjestelmien osalta organisaation tulee etsiä käytettävyyden ja riskin välille järkevä tasapaino. Julkishallinnossa on paljon järjestelmiä, joihin käyttäjiä voidaan hyvin päästää kertakirjausjärjestelmällä. Salassa pidettävää tietoa sisältävät järjestelmät eivät kuulu niihin.

6.1.2.2 Epäluotettavan koodin suorittaminen rajoitetussa ympäristössä

Tietokaappauksen riskiä voi pienentää olennaisesti suorittamalla epäluotettavaksi katsottava koodi rajatussa ympäristössä, jossa se ei voi päästä suoraan suojattavaan tietoon käsiksi.

Epäluotettavuuden kriteerit luonnollisesti vaihtelevat organisaation käsittelemän tiedon suojaustarpeiden mukaan. Yksinkertaisimmillaan epäluotettavaksi koodiksi voidaan katsoa mikä tahansa sähköpostitse saapuva tai selaimen hakema suoritettava koodi.

Sähköpostiasiakkaita tai selaimia voi ajaa esimerkiksi erillisessä palvelimessa (mikä tahansa edusta-unix[15], citrix). Paikallisten toimistodokumenttien käsittely puolestaan tehdään joko käyttäjien työasemilla tai edelleen toisessa edustakoneessa, jolloin viestinnän edustakoneella yksittäisen käyttäjän oikeuksin toimiva haittaohjelma ei voi aivan yhtä helposti tavoittaa suojattavaa aineistoa. Käyttäjien työasemilta ei tällöin myöskään tarvitse olla lainkaan yhteyksiä suoraan ulos, jolloin niille jotakin muuta reittiä päätyvä haittaohjelma ei voi toimittaa keräämäänsä materiaalia aivan yhtä helposti verkosta ulos.

Vaihtoehtoinen malli on hoitaa viestintä omassa työasemassa ja dokumenttien käsittely erillisessä dokumenttivarastossa. Suoja ei ole aivan yhtä hyvä kuin ensimmäisessä mallissa, sillä tässä tapauksessa käyttäjä liikennöi käsittelemään suojattua tietoa haavoittuvan laitteen kautta. Esimerkiksi näytönkuvia (screen dump) ja näppäinpainalluksia keräävä haittaohjelma pystyy yhä tavoittamaan käyttäjän näkemän ja kirjoittaman tiedon ja haittaohjelman tai käsin toimi-

[15] ”unix” kattaa tässä kaikki unixin kaltaiset käyttöjärjestelmät UNIXeista linuxeihin ja Mac OS X:ään.

van tunkeutujan voi olla mahdollista hyödyntää käyttäjän antamaa autentikointitietoa ja murtautua käyttäjän perässä dokumenttivarastoon. Suoja on silti parempi kuin nykyisessä mallissa, jossa kaikki dokumentit ovat suoraan haittaohjelman saatavilla.

Kaikkein keveimmillään ulkoa tullutta koodia voi ajaa virtuaalikoneessa tai eri käyttäjätunnuksella, jonka ympäristö voi olla rajoitettu (chrooted, sandboxed). Menettely on helppo toteuttaa, mutta suoja luonnollisesti on rajallinen, sillä virtuaalikoneesta voi olla mahdollista murtautua ulos.

Riippuu luonnollisesti organisaatiosta, missä kohtaa saavutetaan järkevä tasapaino kustannus-, suorituskyky- ja turvallisuuskriteereille.

6.1.2.3 Eräitä muita rajauskeinoja

Haitallisen koodin aiheuttaman uhan pienentämiseen voidaan hakea erilaisia luovuutta osoittavia vahingonrajauskeinoja yksittäisten komponenttienkin osalta, kunhan tunnistetaan, hyväksytään ja viestitään käyttäjille suojauskeinosta mahdollisesti aiheutuvat sivuvaikutukset.

Toimisto-ohjelmien haavoittuvuuksien vaikutuksia voidaan rajata avaamalla epäluotettavat dokumentit toimistosovellusten sijaan esiprosessoreilla, jotka muuttavat dokumentin tekstimuotoon, esimerkiksi XML:ksi. Ylipäätään organisaatioiden kannattaisi ottaa käytännöksi sisällön siirtäminen sähköpostitse aina tekstinä: joko raakatekstinä, jollakin tekstimuotoisella rakenteisella kuvauskielellä tai rtf:nä. Omalle käyttäjäkunnalle annettu ohje ei kuitenkaan riitä suojaukseksi, sillä se ei estä eikä juuri edes vähennä ulkopuolelta tulevien binäärimuotoisten dokumenttien määrää.

6.1.3 Salassa pidettävän tiedon siirto ja säilyttäminen

Varautumisen yhteydessä tuotiin esiin verkkoliikenteen salaus ja osapuolten varmentaminen. Salassa pidettävä tieto tulee salakirjoittaa kaikenlaisen muunkin kuljetuksen ajaksi. Vaatimus koskee yhtälailla siirrettäviä talletusvälineitä kuin kannettavien tietokoneiden sisältämää salassa pidettävää tietoa riippumatta siitä, onko tieto tiedostossa, poistettuna tiedostojärjestelmän näkyviltä vai muistista sivutettuna levylle. Kannettavissa kannattaa siten suosia ratkaisuja, joissa koko levy tai levyosio – eikä vain tiedostojärjestelmä – salataan.

Paikallaan ja päällä pysyvissä palvelimissa on hiukan vapaammat kädet hakea kompromissia toiminnallisuuden ja turvallisuuden välillä. Tiedon salaus on palvelimissa tarpeen, jos ylläpito on ulkoistettu tai palvelinten levyihin pääsee helposti käsiksi. Tällöin saattaa kuitenkin riittää tietokannassa olevan operatiivisen tiedon salaaminen.

6.2 Ylläpitoprosessi

Käyttöympäristön rakentaminen kerran turvalliseksi ei luonnollisestikaan riitä. Aika rapauttaa järjestelmän kuin järjestelmän, ellei sitä ylläpidetä jatkuvasti. Käyttöjärjestelmätoimittajan julkaisemien turvallisuuspäivitysten asentamisen lisäksi ajan tasalla on pidettävä vähintään kaikki ulkoa syötteitä saavat ohjelmat, ohjelmat, joilla käsitellään turvattavaa tietoa sekä pääsynvalvontaan liittyvät ja erityisoikeuksin suoritettavat ohjelmat kirjastoineen. Pelkästään ulkoa syötteitä saavien ohjelmistojen päivittäminen ei siis riitä, vaan myös vain sisäverkkoon näkyviä kriittisiä komponentteja on ylläpidettävä. Tietorikollinen ei ole vain ”tuolla ulkona”, vaan ylläpitoprosessin lähtökohdaksi tulisi ottaa se, että tavoitteellinen tietorikollinen on ennen pitkää sisäverkossa.

Jos turvallisuuspäivitystä ei ole mahdollista asentaa vaikkapa kolmannen osapuolen tarjoaman sovelluksen takia, sovellusta ajava järjestelmä on syytä erottaa verkkoteknisesti ja kohdentaa järjestelmään liikenteen seurantaa lainsäädännön sallimissa puitteissa (luku 5.1).

Huolellinen päivitysprosessikaan ei vielä riitä, vaan järjestelmien todellinen tila tulee tarkastaa jatkuvasti. Kannattaa kuitenkin huomata, että omien järjestelmien auditoinnilla on erilainen tavoite kuin siviilioikeudellisten sopimusten (kuten PCI) ehtojen täyttämiseksi toteutetuilla auditoinnilla. Oman organisaation järjestelmäauditoinnin ainut tarkoitus on selvittää suojauksen todellinen tila. Niinpä toteutus voi olla paljon kevyempi ja keskittyä ainoastaan omassa ympäristössä olennaisiin kysymyksiin. Palvelua ei tarvitse hankkia riippumattomalta sertifioidulta taholta, jos omassa organisaatiossa on sopivaa osaamista.

Jos auditointi saadaan viestitettyä ylläpitäjille osana ylläpitoprosessia, eikä heidän työnsä tarkastamisena, tarkastuksista voidaan hyvin tehdä ryhmätyöprojekteja, joissa ylläpito on keskeisesti mukana. Sovellusten sisäisen turvallisuustilanteen tutkiminen vaatii aidosti osaamista, jota organisaatiossa ei yleensä ole muualla kuin ylläpidossa.

Ensimmäinen auditointikierros, jossa auditointi suunnitellaan, on väistämättä kohtuullisen raskas operaatio. Monet päätöksenteon tueksi (vuolaasti) tietoa tarjoavat skannerit vaativat perehtymistä, jotta olennaiset varoitukset voidaan erottaa epäolennaisista. Jatkossa tehtävä kuitenkin helpottuu, sillä mekaaninen tiedonkeruu voidaan hyvin automatisoida. Päätöksenteko ja tulkinta kannattaa kuitenkin jättää ihmisen tehtäväksi.

Palvelunestohyökkäykselle alttiit julkiset palvelut, verkon aktiivilaitteet ja erilaiset kuormanjakojärjestelmät tulisi ennen käyttöönottoa ja suurempien muutosten jälkeen testata riittävällä kuormalla ja virheellisillä syötteillä.

Auditointitarve koskee mitä suurimmassa määrin myös ulkoistettuja palveluita. Missään nimessä ei riitä, että auditointi tehdään vain dokumentaatioon, sillä se kertoo vain hurskaan tavoitetilan ja sopimusoikeudelliset lähtökohdat, ei todellista teknistä tilannetta. Asiakkaan oikeus toistuvaan tarkastamiseen

on lisättävä ulkoistussopimuksiin jo sopimusneuvottelujen yhteydessä, kuten myös huolellisempaan ylläpitoprosessiin kannustava sopimussakkomenettely.

6.3 Verkkotekniset suojausmenetelmät

Organisaatio voi parantaa käsittelemänsä tiedon turvallisuutta myös verkkoteknisin järjestelyin. Menetelmiä on hyvin eritasoisia. Jokaisen organisaation kannattaisi toteuttaa vähintään luvussa 4.2.3 esille tuotu sisäverkon osiointi, joka on kustannustehokas keino parantaa verkon hallittavuutta.

Yksinkertaisilla kriteereillä päätöksiä tekeviin automaatteihin ei pidä luottaa liikaa. Kuten havainnoinnin yhteydessä tuli esille, hyökkäyksiä tunnistavien automaattien (IDS) tekemiin johtopäätöksiin tulee suhtautua varauksellisesti. Tämä pätee vielä enemmän varsinaisiin hyökkäystentorjuntajärjestelmiin (IPS). Jos torjuttava hyökkäys on lähetetty väärennetyillä lähdeosoitteilla, IPS voi estää täysin viattoman sivullisen liikennöinnin omaan organisaatioon. IPS voi siten estää liikenteen esimerkiksi yhteistyöviranomaiselta tai ulkoistettujen palveluiden tarjoajalta, jolla ei todellisuudessa ole mitään tekemistä hyökkäyksen kanssa. IPS on helppo keino aiheuttaa itselle ”palvelunestohyökkäys”, jos sen antaa estää liikennöintiä ulkoverkosta sisäverkkoon mekaanisin kriteerein.

6.3.1 Operatiivisen verkon ja viestintäverkon fyysinen erottaminen

Ylivoimaisesti paras turvallisuus operatiivisten järjestelmien sisältämälle tiedolle saadaan, jos järjestelmät yksinkertaisesti erotetaan fyysisesti julkiseen verkkoon yhteydessä olevasta viestintäverkosta. Tässä kannattaa kuitenkin huomata, että kahden verkon erottaminen palomuurilla ei ole verkkojen fyysistä erottamista. Riittävän motivoitunut tekijä tulee palomuurista läpi. Fyysisestä erottamisesta väistämättä aiheutuu kustannuksia, sillä se edellyttää kahden erillisen aktiivi(verkko)laitekannan ylläpitoa ja kahdennettua työasemakantaa. Erottaminen on kuitenkin perusteltua, kun suojattava intressi on riittävän suuri.

Julkisten verkkojen palvelut, kuten käyttöjärjestelmäpäivitysjakelut tai julkisiin sulkulistapalveluihin perustuvat varmennepalvelut eivät toimi eristetyssä verkossa. Tällöin operatiiviseen verkkoon tulee rakentaa oma päivitys- sekä tunnistus- ja allekirjoitusinfrastruktuuri. Tällöin myös suojaustason I ja II tietoa voidaan käsitellä kunnolla ylläpidetyissä ympäristöissä. Julkiseen verkkoon liitetyissä verkoissahan niitä ei (perustellusti) saa käsitellä lainkaan.

Kun operatiivinen verkko on eroteltu fyysisesti viestintäverkosta, viestintäpalveluita voidaan tarjota nykyisellä turvallisuusparadigmalla, koska tällöin järjestelmän sisäsyntyinen haavoittuvuus ei enää aiheuta olennaista uhkaa.

6.3.2 Sisäverkon looginen osioiminen ja osioiden pääsyvalvonta

Kun fyysinen erottaminen ei ole kustannussyistä tai suojaustarpeen näkökulmasta realistista, sisäverkko on vähintään osioitava. Työantajalla on työelämän tietosuojalain puitteissa oikeus kohdistaa liikenteeseen tarpeellisia rajoituksia ja sähköisen viestinnän tietosuojalain mukaisesti oikeus rajoittaa viestintäverkkojen turvallisuutta uhkaavaa liikennettä. Työelämän tietosuojalaki edellyttää YT-menettelyä rajoitusten käsittelemiseksi.

Palomuurien tarjoamaan suojaan ei pidä luottaa sokeasti. Jos ja kun palomuuri sallii minkäänlaisia yhteyksiä, myös rikollinen voi kuljettaa yhteytensä palomuurin läpi. Palomuureissakin on ollut paljon ohjelmistohaavoittuvuuksia, joita hyödyntäen liikennettä saadaan kulkemaan sellaiseen kohteeseen, johon palomuurin asetustensa perusteella periaatteessa pitäisi estää yhteydet. Vaikka palomuuri ei mitenkään ole läpäisemätön, osioiden välisellä pääsyvalvonnalla voidaan kuitenkin kasvattaa tietokaappausten vaikeusastetta.

Pääsyvalvonnalla saadaan esimerkiksi rajoitettua eri osastojen tuotantotyöasemaverkkojen välistä suoraa levyjakoliikennettä tai estettyä suorat yhteydet työasemaverkoista ulos. Erityisen hyödyllistä olisi estää suorat DNS-kyselyt työasemaverkoista muualle kuin omaan tai palveluntarjoajan DNS-palveluun, sillä rikolliset käyttävät tietokaappauksissa omaa verkkopalveluinfrastruktuuriaan tietoa ulos kuljettavan liikenteen ohjaamiseen. Työelämän tietosuojalaki sekä sähköisen viestinnän tietosuojalaki mahdollistavat liikennerajoitukset myös osapuolten perusteella, kunhan rajoitus todella on perusteltu esimerkiksi tietoturvallisuuden ylläpitämiseksi. Rajoitus voi tällöin koskea vaikkapa sellaisia yksittäisiä osoitteita tai autonomisia reititysalueita (AS[16]), joita tietoturvayhteisön tietojen perusteella tunnetusti käytetään kaapatun tiedon tallentamiseen.

Sisäverkon eri osien välillä voidaan pitää myös sellaisia sovelluskerroksen palomuureja, jotka verkon ulkorajalla olisivat alttiita väärinkäytölle. Monimutkaisina kokonaisuuksina sovellustason palomuureissa on todennäköisesti enemmän haavoittuvuuksia kuin kuljetus- tai verkkokerroksen suodattajissa. Tilatietoa ylläpitävät palomuurit ovat myös alttiimpia resursseja kuluttaville palvelunestohyökkäyksille. Sovellustason suodatus yksittäisten sisäverkon olioiden välillä on myös paljon kustannustehokkaampaa kuin suodatus ulkoa tulevalle liikenteelle.

Koska julkiseen palveluun kohdistuvan tehokkaan palvelunestohyökkäyksen toteuttaminen on kohtalaisen helppoa, organisaation on pidettävä huolta siitä, että kriittiset palvelut sijaitsevat verkkoteknisesti mahdollisimman kaukana julkisista WWW-palveluista, mahdollisesti jopa kokonaan toisen palveluntarjoajan verkossa.

[16] AS, Autonomous System (RFC 1930) on internet-verkon reititysalueen yksikkö.

6.4 Tiedon suojaaminen omilta käyttäjiltä

Viranomaisen tiedon väärinkäyttäjä ei välttämättä ole vain ”tuolla ulkona”, vaan tiedon kaappaaja tai vuotaja voi yhtälailla olla oma työntekijä. Viranomaistieto on siksi suojattava myös omien käyttäjien oikeudettomalta käytöltä ja sisäverkosta tulevilta kaappausyrityksiltä. Varautumisen yhteydessä esitelty verkon osittaminen mahdollistaa myös omien käyttäjien tekemien toimenpiteiden (perustellun) seurannan.

Nykyinen tietoturvaparadigma korostaa voimakkaasti ohjeiden ja määräysten merkitystä tiedon turvaamisessa. Lähtökohta on sikäli ymmärrettävä, että nykyisen käytännön mukaisesti suunnitellut ja toteutetut toimistoympäristöt eivät turvaamiseen kykene. Malli on silti väärä. Ei ole erityisen todennäköistä että organisaatioon työntekijäksi soluttautunut tai rikollisryhmän organisaation sisältä värväämä työntekijä jättäisi tehtävänsä toteuttamatta käyttösääntöjen takia. Ei myöskään ole todennäköistä, että ylityöllistetty kiireinen työntekijä pysähtyisi miettimään, voiko sähköpostitse tullutta lisätietolinkkiä klikata, jos on odotettavissa, että linkin takaa löytyvä tieto nopeuttaa ja helpottaa työtä. Todennäköisesti kaikkein sitoutuneimmat ja motivoituneimmat työntekijät ovat juuri niitä, jotka varmimmin klikkaavat järkevällä peitetarinalla lähetetyt sähköpostiliitteet auki.

Fyysisen turvallisuuden toteuttamisessa ihmisen ominaisuudet huomioidaan hyvin. Ovien lukitusta ei jätetä ihmisen muistamisen varaan, vaan ovet lukittuvat automaattisesti. Sama lähtökohta tulisi ottaa tietoturvaratkaisujen kehittämiseen. Jos tiedon suojaamisella on organisaatiolle ylipäätään jotain merkitystä, organisaation on rakennettava tiedon käsittelemiseen tarkoitetut järjestelmät ihmiselle sopiviksi. Ihminen on luonteeltaan utelias, eikä epäintuitiivisten mekaanisten sääntöjen muistaminen ole ihmiselle erityisen ominaista.

Voimassa olevat VAHTI-julkaisut

VAHTI 6/2009 Kohdistetut hyökkäykset
VAHTI 5/2009 Effective Information Security
VAHTI 4/2009 Information Security Instructions for Personnel
VAHTI 3/2009 Lokiohje
VAHTI 2/2009 ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin, yleisohje
VAHTI 1/2009 VAHTIn toimintakertomus vuodelta 2008
VAHTI 9/2008 Hankkeen tietoturvaohje
VAHTI 8/2008 Valtionhallinnon tietoturvasanasto
VAHTI 7/2008 Informationssäkerhetsanvisningar för personalen
VAHTI 6/2008 Tietoturvallisuus on asenne - Selvitys julkishallinnon tietoturvakoulutustarpeista
VAHTI 5/2008 Valtion ympärivuorokautisen tietoturvavalvonnan hankeesitys
VAHTI 4/2008 Valtionhallinnon tietoturva-arviointipoolin toimintaraportti
VAHTI 3/2008 Salauskäytäntöjä koskeva tietoturvaohje
VAHTI 2/2008 Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 1/2008 Toimintakertomus 2007
VAHTI 3/2007 Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 2/2007 Älypuhelinten tietoturvallisuus
VAHTI 1/2007 Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006 Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006 Tietoturvakouluttajan opas
VAHTI 10/2006 Henkilöstön tietoturvaohje
VAHTI 9/2006 Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 8/2006 Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 7/2006 Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 6/2006 Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006 Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 4/2006 Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä

VAHTI 3/2006	Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 2/2006	Electronic-mail Handling Instruction for State Government
VAHTI 1/2006	VAHTIn toimintakertomus vuodelta 2005
VAHTI 3/2005	Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005	Information Security and Management by Results
VAHTI 5/2004	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004	Datasäkerhet och resultatstyrning
VAHTI 3/2004	Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004	Tietoturvallisuus ja tulosohjaus
VAHTI 1/2004	Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006
VAHTI 7/2003	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 5/2003	Datasäkerhetsanvisning för användaren
VAHTI 5/2003	User´s Information Security Instruction
VAHTI 3/2003	Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003	Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003	Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 4/2002	Arkaluonteisten kansainvälisten aineistojen käsittelyohje
VAHTI 3/2002	Etätyön tietoturvaohje
VAHTI 1/2002	Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 6/2001	Tietotekniikkahankintojen tietoturvallisuustarkistuslista
VAHTI 4/2001	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 2/2001	Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 3/2000	Tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 2/2000	Valtion tietoaineistojen käsittelyn tietoturvaohje

Ohjeisto löytyy VAHTIn Internet-sivuilta http://www.vm.fi/vahti. Ohjeita saa tilattua laatikoittain edullisesti painotalo Editasta. Yllämainittujen julkaisujen lisäksi VAHTIn toiminnasta kertovia raportteja löytyy VAHTIn verkkosivuilta.

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

6/2009
VAHTI
marraskuu 2009

ISSN 1455-7606 (nid.)
ISBN 978-952-251- 012-9 (nid.)
ISSN 1798-0860 (pdf)
ISBN 978-952-251-013-6 (pdf)