Riku Pessinen

Henkilörekistereiden tietosuojavaatimukset ja niiden toteuttaminen DLP-ratkaisuilla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

17.9.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Riku Pessinen Henkilörekistereiden tietosuojavaatimukset ja niiden toteuttaminen DLP-ratkaisuilla 63 sivua + 7 liitettä 17.9.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Development Director Markku Selin Security Consultant Sanna Partti lehtori Marko Uusitalo

Tämän Santa Monica Networks Oy:lle tehdyn insinöörityön tarkoituksena oli selvittää, millaisia vaatimuksia Euroopan komission ehdottama tietosuoja-asetus 2012/0011 sekä valtioneuvoston tietoturva-asetus 681/2010 asettavat ja miten asetusten edellyttämät vaatimukset voidaan toteuttaa.

Työssä tarkasteltiin asetusten sisältöä, jonka perusteella huomattiin, että asetukset edellyttävät huomattavia tietoturvavaatimuksia henkilörekistereiden käsittelyyn liittyen. Arkaluonteinen tieto on yksiselitteisesti suojattava, ja on estettävä sen tuhoutuminen, luvaton leviäminen, muuttaminen ja tiedonsaanti. Työssä kartoitettiin yleisimpiä tietovuotoriskejä, tietovuodon kustannuksia ja mahdollisuuksia tietovuotojen estämiseen. Tämän perusteella huomattiin, että tietovuotoja voi estää tietoja käsittelevien henkilöiden tietoturvakoulutuksella sekä teknisillä ratkaisuilla.

Työssä selvitettiin, millaisia vaatimuksia teknisiltä ratkaisuilta vaaditaan, ja todettiin, että DLP-ratkaisu on todennäköisin vaihtoehto tietovuotojen estämiseen. Tämän selvittämiseksi työssä testattiin kahden laitevalmistajan DLP-ratkaisuja: Check Pointin gateway-ratkaisua ja McAfeen endpoint-ratkaisua. Testin perusteella havaittiin, että DLP-ratkaisu soveltuu asetusten edellyttämien vaatimusten toteuttamiseen.

Työssä tarkasteltiin myös DLP-ratkaisujen markkinakehitystä sekä pohdittiin, mitä DLP-ympäristö ja sen käyttöönotto vaatii. Tällöin huomattiin, että toimivaan DLP-ympäristöön tarvitaan sekä gateway- että endpoint-ratkaisu. Lisäksi havaittiin, että DLP-ratkaisun käyttöönottoon on varattava reilusti aikaa, jotta siitä saadaan toimiva kokonaisuus.

Avainsanat	Tietosuoja-asetus 2012/0011, tietoturva-asetus 681/2010, henkilörekisteri, tietovuoto, DLP

Author(s) Title Number of Pages Date	Riku Pessinen Using DLP Solutions to Meet Security Requirements of Processing Personal Data 63 pages + 7 appendices 17 September 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Markku Selin, Development Director Sanna Partti, Security Consultant Marko Uusitalo, Senior Lecturer

The purpose of this Bachelor's thesis, carried out for Santa Monica Networks Oy, was to investigate what kind of requirements the proposal for a General Data Protection Regulation 2012/0011 by the European Commission and the Government Decree 618/2010 on Information Security in Central Government sets, and how these requirements can be met.

The study examined the contents of the regulations, and it was found that both of the regulations set remarkable security requirements regarding the processing of personal data. Personal data has to be protected against accidental or unlawful destruction, unauthorized disclosure, dissemination and unauthorized alteration. The study explores possible risks for data breaches, the costs of a data breach and means to prevent data breaches. It was found that data breaches can be prevented by instructing staff with security practices and by using technical solutions.

The requirements for technical solutions were examined, and based on the findings, DLP seemed to be the most probable solution for data breach prevention. To find evidence for this, the DLP gateway solution by Check Point and DLP endpoint solution by McAfee were tested in a lab environment. According to the tests, the DLP solution is well suited for fulfilling the security requirements set by the regulations.

The market development for DLP solutions was also examined, and the deployment of a DLP environment was discussed. It was found that a functional DLP environment requires both a gateway and an endpoint solution. It was also noticed that deploying a DLP solution takes a great deal of time and needs careful planning to make it properly functional.

Keywords	General Data Protection Regulation 2012/0011, Government Decree 681/2010, personal data, data breach, DLP

Sisällys

Lyhenteet ja määritelmät

CA	Certificate authority. Taho, joka myöntää digitaalisia varmenteita eli sertifikaatteja.
CIFS	Common Internet Filesystem. Protokolla tiedostojen jakamiseen verkossa.
CLI	Command-line interface. Komentoliittymä. Tekstipohjainen käyttöliittymä.
DLP	Data Loss/Leak Prevention. Tekniikka, joka mahdollistaa tietovuotojen havaitsemisen ja estämisen.
Debug, debuggaus	Termi, jota käytetään tietojärjestelmissä esiintyvien virheellisten toimintojen paikallistamisesta ja korjaamisesta.
FTP	File Transfer Protocol. Asiakas-palvelin-periaatteella toimiva tiedonsiirtomenetelmä.
FTPS	File Transfer Protocol Secure. TLS/SSL-salausta käyttävä laajennus FTP-protokollaan, joka mahdollistaa salatun tiedonsiirron
Henkilörekisteri	Henkilötietoja sisältävä tietojoukko.
Henkilötieto	Kaikki rekisteröityä koskevat tiedot rekisterissä.
Henkilötietojen käsittelijä	Henkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.
Heräte	Sähköpostiin, puhelimeen tai muuhun laitteeseen lähetettävä ilmoitus, kun jokin määrätty asia on tapahtunut.
HTTP	Hypertext Transfer Protocol. Selaimen ja palvelimen välinen tiedonsiirtoprotokolla.

HTTPS	Hypertext Transfer Protocol Secure. Suojatun ja salatun tiedonsiirron mahdollistava protokolla selaimen ja palvelimen välillä.
IDS	Intrusion Detection System. Järjestelmä, joka pyrkii tunnistamaan verkkoon suuntautuvat hyökkäysyritykset.
IPS	Intrusion Prevention System. Järjestelmä, joka pyrkii tunnistamaan ja estämään verkkoon suuntautuvat hyökkäysyritykset.
IRC	Internet Relay Chat. Reaaliaikaisen viestinnän mahdollistava protokolla.
Käsittely	Kaikenlainen toiminta, jota kohdistetaan henkilötietoihin automaattisesti tai manuaalisesti.
LDAP	Lightweight Directory Access Protocol. Hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla.
NFS	Network File System. Protokolla tiedostojen jakamiseen verkossa.
PDF	Portable Document Format. Sähköisessä julkaisemisessa käytettävä tiedostomuoto.
Rekisterinpitäjä	Henkilörekisteriä ylläpitävä taho, kuten yksityishenkilö, yritys, yhdistys tai viranomainen, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä.
Rekisteröity	Henkilö, joka on tunnistettu tai tunnistettavissa suoraan tai epäsuorasti henkilörekisterissä olevilla tiedoilla.
SCP	Secure copy. SSH-protokollaa käyttävä turvallinen tiedonsiirtomenetelmä.

SIEM	Security Information and Event Management. Järjestelmä, joka havainnoi tietoturvatapahtumia reaaliaikaisesti ja raportoivasti.
SMTP	Simple Mail Transfer Protocol. Protokolla sähköpostiviestien välittämiseen.
SSH	Secure Shell. Salatun tietoliikenteen mahdollistava protokolla.
SSL	Secure Sockets Layer. Salausprotokolla, joka mahdollistaa tietoliikenteen suojaamisen.
TLS	Transport Layer Security. Salausprotokolla, joka mahdollistaa tietoliikenteen suojaamisen.
USB	Universal Serial Bus. Sarjaväyläarkkitehtuuri oheislaitteiden liittämiseksi tietokoneeseen.
Valvontaviranomainen	EU-jäsenvaltioiden määrittelemä viranomainen tietosuoja-asetuksen säännösten noudattamisen valvontaan.
Vastaanottaja	Henkilö, viranomainen, virasto tai muu elin, jolle henkilötietoja luovutetaan.
VoIP	Voice over Internet Protocol. Tekniikka, joka mahdollistaa äänensiirron tietoverkossa puhelinverkon tavoin.
VPN	Virtual Private Network. Tekniikka, jolla useampia verkkoja voi yhdistää suojatusti muodostaen näennäisesti yksityisen verkon.

1 Johdanto

Kehittyvä teknologia ja tiedon siirtyminen sähköiseen muotoon yhä enemmän edellyttää myös lainsäädännöllisiä muutoksia. Luottamuksellisen tiedon siirto ja käsittely tietojärjestelmissä ja -verkoissa lisää erilaisia riskejä, jolloin on tärkeää huolehtia tietoturvasta. Nykyinen lainsäädäntö ei huomioi riittävästi tietojärjestelmien ja -verkkojen tietoturvaa. Tähän on tulossa muutos Euroopan unionin lainsäädännössä sekä kansallisella tasolla.

Tämä insinöörityö on tehty Santa Monica Networks Oy:lle, joka on turvallisiin tietoverkkoihin keskittynyt asiantuntija. Vuodesta 2005 Santa Monica Networks Oy:nä toiminut yritys pyrkii olemaan verkko- ja tietoturvateknologian suunnannäyttäjä, jonka toimintaan kuuluvat asiantuntijapalvelut, ylläpitopalvelut, koulutuspalvelut, hallinta- ja valvontapalvelut sekä määrittely- ja testauspalvelut.

Santa Monica Networks Group toimii Suomessa ja kaikissa Baltian maissa. Konsernissa on 119 työntekijää, joista 50 työskentelee Suomessa. Yrityksen liikevaihto oli vuonna 2011 noin 29,25 miljoonaa euroa. Santa Monica Networks Oy tarjoaa maailman johtavien tietoliikenne- ja tietoturvavalmistajien tuotteita, ja on sertifioitu useimpien valmistajien korkeimmalle partneritasolle.

Tämän insinöörityön tavoitteena on tutkia, minkälaisia vaatimuksia Euroopan komission tietosuoja-asetus 2012/0011 sekä valtioneuvoston tietoturva-asetus 681/2010 asettavat ja miten nämä vaatimukset ovat toteutettavissa. Tarkoituksena on selvittää, mitä asetukset käytännössä tarkoittavat ja miten niiden tietoturvaan liittyviä määräyksiä voidaan noudattaa.

Työn tilaajalla on tarve selvittää, ovatko DLP-ratkaisut käyttökelpoisia ja soveltuuko DLP tekniikkana noudattamaan asetusten tietoturvavaatimuksia. Tämän selvittämiseksi työssä selvitetään, millaisia vaatimuksia teknisiltä järjestelmiltä vaaditaan, ja testataan kahden laitevalmistajan DLP-ratkaisuja: Check Pointin sekä McAfeen.

2 EU:n tietosuoja-asetus 2012/0011

Euroopan komissio pyrkii uudistamaan henkilötietojen suojaa ja käsittelyä EU:n lainsäädäntökehyksellä, joka sisältää ehdotuksen tietosuoja-asetuksesta 2012/0011 sekä direktiivistä 2012/0010 [1, 2]. Tietosuoja-asetus pohjautuu direktiiviin, joten molemmat käsittelevät pääosin samoja asioita. Asetuksessa asiat on esitetty tiukemmin, kun taas direktiivissä ei ole käytännön sovellutuksiin otettu juuri kantaa. Asetus on sitova säädös, jota on sovellettava sellaisenaan kaikkialla EU:ssa siirtymäajan umpeuduttua. Direktiivi vastaavasti on säädös, jonka tavoitteisiin EU-maiden täytyy pyrkiä, mutta kukin EU-maa voi kansallisesti päättää, kuinka tavoitteet käytännössä toteutetaan. [3.] Tämä työ pohjautuu tietosuoja-asetuksen säädöksiin, sillä niitä joudutaan soveltamaan käytännössä sellaisenaan.

Uusi lainsäädäntökehys tulee korvaamaan nykyisen vuonna 1995 voimaantulleen direktiivin 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä [4]. Euroopan komissio on perustellut uudistusta korostetusti sillä, että teknologian kehittyessä on erityisen tärkeää huolehtia yksityisyyden suojasta. Tietoa jaetaan ja tallennetaan huomattavasti suuremmassa mittakaavassa kuin vuonna 1995, ja tätä hyödyntävät niin yksityiset yritykset kuin viranomaiset. Myös yksityiset ihmiset antavat yhä useammin henkilötietojaan eri tahojen käyttöön maailmanlaajuisesti. Euroopan unionissa on omaksuttava tiukempi asenne henkilötietojen suojaamiseen kaikilla aloilla, mukaan lukien lainvalvonta, rikoksentorjunta sekä kansainväliset suhteet. Komission mukaan Euroopan unionissa tarvitaan nykyistä kattavampi ja johdonmukaisempi ohjeistus henkilötietojen suojaa koskevan perusoikeuden toteuttamiseksi. [2, s. 1-2.]

Nykyisellä direktiivillä 95/46/EY oli kaksi tavoitetta: suojata yksilöiden tietosuojaa koskeva perusoikeus ja taata henkilötietojen vapaa liikkuvuus jäsenvaltioiden välillä. Direktiiviä on täydennetty vuoden 1995 jälkeen useilla säädöksillä, joilla on pyritty vahvistamaan tietosuojakäytäntöjä mm. poliisiyhteistyön ja rikosasioissa tehtävän oikeudellisen yhteistyön alalla, kuten puitepäätöksessä 2008/977/YOS (entinen ”kolmas pilari”). Direktiivin tavoitteet ja periaatteet ovat edelleen pätevät, mutta sen avulla ei ole pystytty mahdollistamaan henkilötietojen suojan täytäntöönpanoa kaikkialla EU-alueella eikä lieventämään riskejä henkilötietojen käsittelyssä verkkoympäristöissä. Euroopan komission mukaan EU tarvitsee vahvemman ja johdonmukaisemman tietosuojakehyksen, jotta digitaalinen tiedonkäsittely voi kehittyä ja jotta yksilöt voisivat valvoa omien tietojensa käyttöä. [2, s. 1-2.]

Verkkoympäristöissä toimiessa luottamus tekniikkaan sekä tiedon eheyteen ja luottamuksellisuuteen on hyvin tärkeää. Käyttäjän on oltava tietoinen, ettei kukaan pääse muuttamaan tai varastamaan tietoja, oli kyse sitten julkisesta verkkokaupasta tai viranomaisen sisäisestä järjestelmästä. Euroopan komissio pyrkii tietosuoja-asetuksella kehittämään luottamusta verkkoympäristöissä toimimiseen, sillä tällä hetkellä kuluttajat suhtautuvat uusiin verkkopalveluihin epäluuloisesti. Tämä uhkaa hidastaa verkkopalveluiden ja -teknologioiden kehittymistä. [2, s. 1-2.] Henkilötietojen suoja on keskeisellä sijalla myös Eurooppa 2020 -strategiassa [5].

2.1 Soveltamisala ja perusvaatimukset

Asetusta tullaan soveltamaan automatisoituun ja manuaaliseen henkilötietojen käsittelyyn, mikäli henkilötiedot muodostavat rekisterin osan tai joiden tarkoitus on muodostaa rekisterin osa. Tämä ei kuitenkaan koske henkilötietojen käsittelyä, jota suorittaa Euroopan unionin lainsäädännön ulkopuoliset tahot, unionin omat toimielimet tai laitokset, rikosten torjuntaan, tutkintaan ja selvittämiseen liittyvät viranomaiset eikä yksityinen henkilö ilman ansaitsemistarkoitusta. Alueellisesti asetusta sovelletaan, mikäli rekisterinpitäjällä tai henkilötietojen käsittelijällä on toimipaikka Euroopan unionin alueella, jossa henkilötietoja käsitellään. Asetusta sovelletaan myös niissä tapauksissa, joissa rekisteröity asuu unionin alueella ja rekisterinpitäjä tarjoaa tavaroita tai palveluita rekisteröidylle tai muutoin seuraa rekisteröidyn käyttäytymistä. [2, 2-3. artikla.]

Käytännössä asetusta voidaan soveltaa niin yritysten, yhteisöjen kuin viranomaisten henkilötietojen käsittelyyn. Asetus ei ota kantaa tässä suhteessa yrityksen tai yhteisön kokoon tai henkilöstömäärään. Edellisen perusteella myös ulkomaalaiset verkkopalvelut ovat myös asetuksen alaisia, mikäli ne tarjoavat EU-alueella asuville ihmisille palveluita. Verkkopalvelun ei siis fyysisesti tarvitsisi sijaita EU-alueella.

Asetus määrittää muutamia yleisiä perusvaatimuksia henkilötietojen käsittelyyn. Käsittelyn on oltava lainmukaista sekä rekisteröidyn kannalta asianmukaista ja läpinäkyvää. Rekisterissä olevat tiedot on kerättävä vain tiettyä tarkoitusta varten, eikä niitä saa hyödyntää muihin tarkoituksiin myöhemmin. Kerättävien tietojen pitää olla olennaisia, mikä tarkoittaa, että tietoja pitää kerätä mahdollisimman vähän ja vain sen verran kuin on tarpeellista. Ylimääräisiä tietoja ei saa kerätä: rekisterinpitäjän on pystyttävä osoittamaan, mitkä tiedot ovat tarpeellisia kyseiseen tarkoitukseen. Rekisterinpitäjän on

pidettävä huoli siitä, että rekisterin tiedot ovat täsmällisiä ja päivitettyjä ja että virheelliset tiedot oikaistaan tai poistetaan viipymättä. Rekisteriä on pidettävä vain niin kauan kuin on tarpeen, ja henkilötiedot pitää poistaa rekisteristä tämän jälkeen. [2, 5. artikla.] Poikkeuksena tästä on historiantutkimus tai tilastollinen tai tieteellinen tutkimus, joissa rekisteritietoja voidaan säilyttää erityisluvalla pidempään [2, 83. artikla]. Vastuu henkilötietojen käsittelystä kuuluu rekisterinpitäjälle, ja rekisterinpitäjän on pystyttävä osoittamaan kaikilta osin, että asetuksen säännöksiä on noudatettu. [2, 5. artikla.]

Henkilötietojen käsittely on lainmukaista ja sallittua vain seuraavissa tapauksissa, jotka mainitaan asetuksen 6. artiklassa.

- Käsittely on sallittua silloin, kuin rekisteröity on antanut oman suostumuksensa tai pyynnön henkilötietojen käsittelyyn [2, 6. artikla].
- Rekisterinpitäjällä voi myös olla lakisääteinen velvollisuus henkilötietojen käsittelyyn, kuten esimerkiksi väestörekistereissä, tai käsittely voi olla tarpeen rekisteröidyn elintärkeiden etujen suojaamiseksi, kuten esimerkiksi hätä- ja kriisitilanteissa. [2, 6. artikla.]
- Henkilötietoja saa käsitellä historiantutkimusta tai tilastollista tai tieteellistä tutkimusta varten erityisluvalla [2, 83. artikla].
- Käsittely voi myös olla tarpeen yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten, tai rekisterinpitäjällä voi olla oikeutettu etu käsittelyn toteuttamiseksi. [2, 6. artikla.]

Viimeisenä mainittu oikeutettu etu voi olla kyseenalainen tekijä; voidaanko esimerkiksi kuluttajamyyntiin suuntautuneessa yrityksessä perustella asiakasrekisterin pitoa sillä, että se on yrityksen toiminnan kannalta välttämätöntä? Rekisterinpitäjällä on kuitenkin velvollisuus pystyä perustelemaan tämä oikeutettu etu. [2, 6. artikla.]

2.2 Rekisteröidyn oikeudet

Tietosuoja-asetuksen 3. luku määrittää rekisteröidylle oikeuksia, joista merkittävimpiä ovat tiedonsaantioikeus, oikeus tietojen oikaisemiseen ja poistamiseen sekä oikeus vastustaa henkilötietojen käsittelyä. [2, 3. luku.]

Rekisteröidyllä on oikeus saada ja tarkistuttaa rekisterissä olevia tietoja. 15. artikla määrittää tiedonsaantioikeuden, jonka avulla rekisteröity voi pyytää vahvistusta siitä,

käsitteleekö rekisterinpitäjä häntä koskevia tietoja vai ei. Mikäli tietoja käsitellään, rekisterinpitäjän pitää ilmoittaa rekisteröidylle alla olevat tiedot:

- käsittelyn tarkoitus ja kyseessä olevat henkilötietojen ryhmät
- tahot joille henkilötietoja on luovutettu tai tarkoitus luovuttaa
- käsiteltävät henkilötiedot ja niiden säilytysaika
- tieto siitä, että rekisteröidyllä on oikeus tietojen oikaisemiseen tai poistamiseen, tai valituksen tekemiseen valvontaviranomaiselle ja tämän yhteystiedot
- käsittelyn merkitys ja mahdolliset seuraukset. [2, 15. artikla.]

Rekisterinpitäjän on toimitettava nämä tiedot helposti ymmärrettävässä muodossa ja selkeällä kielellä viimeistään kuukauden kuluttua pyynnön esittämisestä. Tiedot pitää toimittaa kirjallisesti, tai mikäli rekisteröity on pyytänyt tietoja sähköisesti, ne pitää toimittaa myös sähköisesti, ellei rekisteröity toisin pyydä. Mikäli rekisterinpitäjä ei suostu toimittamaan tietoja, on tämän ilmoitettava kieltäytymisen syy ja kerrottava mahdollisuudesta tehdä valitus valvontaviranomaiselle. Rekisteröidylle tämän toimenpiteen pitää olla maksutonta, paitsi jos rekisterinpitäjä voi osoittaa pyynnön olevan kohtuuton tai toistuva, jolloin rekisterinpitäjä voi pyytää asiasta maksun tai kieltäytyä. Asetus kuitenkin painottaa tässäkin asiassa vastuun asian todistamisesta olevan rekisterinpitäjällä. [2, 12. artikla.]

Tällä hetkellä esimerkiksi Kela kertoo kotisivuillaan, että he ylläpitävät useita rekistereitä henkilöistä [6]. Näiden rekisteritietojen tarkistamista voi pyytää ilmaiseksi kerran vuodessa. Tietosuoja-asetuksen valossa ei kuitenkaan liene kohtuutonta, etteikö tietojaan voisi tarkistaa useammankin kerran maksutta. Asetuksen 12. artiklassa kuitenkin määritellään, että kuukauden määräaikaa voi pidentää, jos useat rekisteröidyt käyttävät oikeuttaan samanaikaisesti [2, 12. artikla].

Mikäli henkilötietoja käsitellään sähköisesti, on rekisteröidyllä oikeus saada jäljennös näistä tiedoista, jolloin rekisteröity voi käyttää tietoja muissa tarkoituksissa uudelleen. Kun henkilötietojen käsittely perustuu suostumukseen tai sopimukseen, rekisteröidyllä on oikeus siirtää henkilötiedot toisiin järjestelmiin yleisesti käytetyssä sähköisessä muodossa. [2, 18. artikla.]

Rekisteröidyllä on oikeus vaatia virheellisten tietojen oikaisua (oikeus tietojen oikaisemiseen), kuten myös vaatia tietojen poistamista. Tämä tunnetaan käsitteenä ”oikeus tulla unohdetuksi” (engl. ”right to be forgotten”). Rekisteröity voi vaatia tietojen poistamista seuraavissa tapauksissa:

- Tietoja ei enää tarvita siinä tarkoituksessa, jota varten ne kerättiin.
- Rekisteröity peruuttaa suostumuksensa tietojen keräämiseen.
- Tietojen säilytysaika on päättynyt.
- Rekisteröity vastustaa henkilötietojen käsittelyä.
- Käsittely ei ole muista syistä asetuksen mukaisia. [2, 17. artikla.]

Rekisterinpitäjän pitää poistaa henkilötiedot viipymättä, paitsi jos niiden säilyttäminen ei ole tarpeen erikseen määrätyillä asetuksilla, kuten esimerkiksi väestörekisterissä. Rekisterinpitäjä voi myös poistamisen sijaan rajoittaa henkilötietojen käyttöä, mikäli rekisteröity kiistää tietojen paikkansapitävyyden, tietoja on säilytettävä todistelua varten, jonkun henkilön oikeuksien suojaamiseksi tai yleisen edun takia. Tällöin rekisterinpitäjällä on vastuu varmistaa tietojen säilyttämisen tarpeellisuuden. Kun tiedot on lopullisesti poistettu, rekisterinpitäjä ei saa muutoin käsitellä kyseisiä tietoja enää. [2, 17. artikla.]

Mikäli rekisterinpitäjä on luovuttanut tai julkaissut rekisteritietoja, rekisterinpitäjän on tehtävä kohtuulliset toimenpiteet näiden tietojen poistamiseksi kolmansilta osapuolilta. Käytännössä tämä tarkoittaa sitä, että rekisterinpitäjä pyytää kolmansia osapuolia poistamaan esimerkiksi henkilötietoihin liittyvät verkkodokumenttien linkit, tietojen jäljennykset ja kopiot. Rekisterinpitäjän on myös ilmoitettava henkilötietojen oikaisusta tai poistosta jokaiselle vastaanottajalle, joille tietoja on luovutettu, mikäli tämä ei osoittaudu kohtuuttomaksi. [2, 13. ja 17. artikla.]

Rekisteröidyllä on oikeus vastustaa henkilötietojen käsittelyä, mikäli niiden käsittely on perusteltu luvussa 2.1 esitetyn henkilötietojen käsittelyn lainmukaisuuden viimeisen kohdan mukaan. Käsittelyyn voi kuitenkin olla jokin perusteltu syy, joka syrjäyttää rekisteröidyn edut tai perusoikeudet. Käytännössä siis rekisteröidyllä on oikeus vastustaa henkilötietojen käsittelyä, mikäli rekisterinpitäjä on perustellut tietojen käsittelyä oikeutetun edun mukaan. Tämä vaikuttaa ristiriitaiselta, sillä rekisterinpitäjä voi kerätä henkilötietoja perusteenaan oikeutettu etu, mutta samalla rekisteröity voi tätä vastustaa. Ky-

seinen kiista päätynee siis valvontaviranomaisen päätettäväksi. Asetus ottaa kantaa myös suoramarkkinointiin; rekisteröidyllä on oikeus vastustaa maksutta suoramarkkinointiin liittyvää henkilötietojen käsittelyä. Rekisterinpitäjän on myös selkeästi ilmoitettava, että tietoja tullaan käyttämään suoramarkkinointiin. [2, 19. artikla.]

Rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, mikäli rekisteröity katsoo, ettei henkilötietojen käsittely ole asetuksen säännösten mukaisia. Asetus painottaa rekisterinpitäjää muistuttamaan aktiivisesti tästä oikeudesta rekisteröidylle. Tämän lisäksi rekisteröidyllä on oikeus oikeussuojakeinoihin rekisterinpitäjää tai henkilötietojen käsittelijää vastaan, mutta myös valvontaviranomaista vastaan. Oikeussuojakeinot tulevat tarpeellisiksi mikäli rekisteröity vaatii vahingonkorvauksia rekisterinpitäjältä tai henkilötietojen käsittelijältä, ja myös valvontaviranomaisen päätöksistä voi nostaa kanteen. [2, 73–75. artikla.]

2.3 Rekisterinpitäjän vastuu

Henkilörekisteriä kerätessä rekisterinpitäjällä on velvollisuus ilmoittaa rekisteröidylle vähintään alla olevat tiedot:

- rekisterinpitäjän, tämän mahdollisen edustajan sekä tietosuojavastaavan yhteystiedot
- henkilötietojen käsittelyn tarkoitus ja millä perustein henkilötietoja kerätään, sekä niiden säilytysaika
- rekisteröidyn tiedonsaantioikeus, oikeus tehdä valitus valvontaviranomaiselle ja viranomaisen yhteystiedot
- tieto siitä, mikäli rekisterinpitäjä aikoo siirtää tietoja kolmansille osapuolille tai kolmansiin maihin
- muut mahdolliset tietojenkäsittelyyn liittyvät tiedot. [2, 14. artikla.]

Mikäli rekisterinpitäjä kerää itse henkilötietoja, on tämän ilmoitettava rekisteröidylle onko tietojen antaminen pakollista vai vapaaehtoista. Molemmissa tapauksissa on myös ilmoitettava tietojen antamatta jättämisen mahdolliset seuraamukset. Jos henkilötietoja ei kerätä suoraan rekisteröidyltä, rekisterinpitäjän on ilmoitettava mistä tiedot ovat peräisin. Tällöin tiedot ovat ilmoitettava rekisteröidylle kohtuullisen ajan kuluttua tai viimeistään silloin, kun tietoja luovutetaan toiselle vastaanottajalle. [2, 14. artikla.]

Samaa henkilörekisteriä voi käyttää myös useammat tahot, jolloin rekisterinpitäjiä on useampia. Tällöin rekisterinpitäjien pitää yhdessä määrittää käsittelyn tarkoitus, edellytys ja keinot, ja päättää kunkin rekisterinpitäjän vastuualueet erityisesti niiden toimenpiteiden osalta, joiden avulla rekisteröidyt voivat käyttää oikeuksiaan. Mikäli rekisterinpitäjä ei ole sijoittunut EU-alueelle, on tämän nimettävä edustaja unionin aluetta varten. Tämä ei kuitenkaan koske alle 250 työntekijän yrityksiä, viranomaisia, julkishallintoa tai rekisterinpitäjää, joka tarjoaa vain satunnaisesti palveluita unionin alueelle tai jos rekisterinpitäjä on sitoutunut sellaiseen kolmanteen maahan, jonka tietosuoja on Euroopan komission mukaan riittävä. [2, 24–25. artikla.]

Asetus määrittää rekisterinpitäjän noudattamaan oletusarvoista tietosuojaa. Rekisterinpitäjällä on velvollisuus toteuttaa asianmukaisin keinoin ja tekniikoin henkilörekisterin toteutus, jotta se vastaisi asetuksessa määrättyjä säädöksiä tietoturvallisuudesta ja rekisteröidyn oikeuksien suojaamisesta. Rekisterinpitäjän pitää huolehtia, että henkilötietojen käsittely koskee vain niitä henkilötietoja, jotka ovat välttämättömiä kyseiseen käsittelyyn. Henkilötietoja ei saa erikseen kerätä tai säilyttää suurempia määriä, ja henkilörekisteriä on ylläpidettävä vain niin kauan kuin on rekisterin tarkoituksen kannalta välttämätöntä. [2, 23. artikla.] Rekisterinpitäjällä ja henkilötietojen käsittelijällä on myös salassapitovelvollisuus, mikäli käsiteltävät henkilötiedot ovat salassa pidettäviä [2, 84. artikla].

Rekisterinpitäjän on ylläpidettävä henkilörekisteriin liittyviä asiakirjoja, joista täytyy käydä ilmi henkilörekisterin tietoja. Asetus määrää seuraava tiedot pakollisiksi:

- rekisterinpitäjän, tämän mahdollisen edustajan, henkilötietojen käsittelijän sekä mahdollisen tietosuojavastaavan yhteystiedot
- henkilötietojen käsittelyn tarkoitukset, kuvaukset rekisteröityjen ryhmistä ja niihin liittyvistä tietoryhmistä
- tarvittaessa henkilötietojen vastaanottajat sekä tiedot henkilötietojen siirrosta kolmansiin maihin
- tietoryhmien poistamisen määräajoista sekä kuvaus henkilörekisterin tietosuojasta. [2, 28. artikla.]

Asiakirjojen ylläpito ei koske yrityksiä tai organisaatioita, joissa on alle 250 työntekijää ja jotka käsittelevät henkilötietoja ainoastaan pääasiallisen toimintansa aputoimintona. Muissa tapauksissa rekisterinpitäjän, tämän mahdollisen edustajan tai henkilötietojen käsittelijän on pyydettäessä esitettävä asiakirjat valvontaviranomaiselle. [2, 28–29. ar-

tikla.] Rekisterinpitäjän ja henkilötietojen käsittelijän on muutoinkin tehtävä yhteistyötä valvontaviranomaisen kanssa: valvontaviranomaisella tulee olla pääsy kaikkien henkilötietojen lisäksi myös itse laitteistoihin ja tiloihin, joissa henkilötietoja käsitellään, mikäli voidaan epäillä mahdollisia rikkeitä tässä asetuksessa esitettyihin vaatimuksiin [2, 53. artikla]. Rekisterinpitäjän tai henkilötietojen käsittelijän on vastattava valvontaviranomaisen vaateisiin kohtuullisen ajan kuluessa [2, 28–29. artikla].

2.4 Henkilötietojen käsittelijä

Jos rekisterinpitäjä ei itse käsittele henkilötietoja, on tämän nimettävä henkilötietojen käsittelijä. Henkilötietojen käsittelijän vastuulla on käsitellä henkilötietoja asetuksen säännösten mukaisesti ja varmistaa rekisteröidyn oikeuksien suojelu. Henkilötietojen käsittelijän on toimittava rekisterinpitäjän ohjeiden mukaan ja otettava palvelukseensa vain sellaista henkilöstöä, joka on sitoutunut noudattamaan salassapitovelvollisuutta. Rekisterinpitäjän ja henkilötietojen käsittelijän on laadittava erillinen sopimus henkilötietojen käsittelystä. Käsittelyn päätyttyä henkilötietojen käsittelijä ei saa käsitellä kyseisiä tietoja enää, ja tämän on luovutettava kaikki käsittelyn aineisto rekisterinpitäjälle. [2, 26. artikla.]

Jos henkilötietojen käsittelijä käsittelee muita kuin rekisterinpitäjän määräämiä henkilötietoja, käsittelijää pidetään kyseisen käsittelyn osalta rekisterinpitäjänä. Henkilötietojen käsittelijän on toteutettava asetuksessa vaadittavat tietoturvallisuuteen liittyvät määräykset omissa tiloissaan ja järjestelmissään. [2, 26. artikla.]

2.5 Tietoturvallisuuteen liittyvät säädökset

Asetuksen tietoturvaa käsittelevä osuus määrittää rekisterinpitäjän ja henkilötietojen käsittelijän vastaamaan perusteellisesti henkilörekisterin sekä käsittelyn tietoturvasta. Henkilötiedot ovat suojattava asianmukaisilla turvallisuusmenetelmillä huomioon ottaen uusin tekniikka ja toimenpiteiden toteuttamiskustannukset. Henkilötiedot ovat yksikäsitteisesti suojattava seuraavilta mahdollisilta tapauksilta:

- vahingossa tapahtuvalta tai laittomalta tuhoamiselta
- vahingossa tapahtuvalta häviämiseltä

- lainvastaiselta käsittelyltä
- henkilötietojen luvaton luovutus, levittäminen, muuttaminen ja tiedonsaanti on estettävä. [2, 30. artikla.]

Asetus jättää komissiolle mahdollisuuden täytäntöönpanosäädöksiin, joilla edellä olevia voidaan vielä vahvistaa, painottaen henkilötietojen luvatonta luovuttamista, lukemista, jäljentämistä, muuttamista, poistamista sekä siirtämistä. Käytännössä siis rekisterinpitäjän ja henkilötietojen käsittelijän on varmistuttava siitä, ettei henkilötietoja tuhoudu tai häviä tahattomasti tai tahallisesti, ja etteivät ulkopuoliset tahot pääse henkilötietoihin käsiksi. Tämän voi mahdollistaa tietojärjestelmien luotettavuudella ja eheydellä, mutta henkilötietojen parissa työskentelevällä henkilöstöllä on tietosuojan kannalta myös merkittävä rooli. [2, 30. artikla.]

2.6 Valvontaviranomainen

Asetus määrittää jäsenvaltiot valvomaan tämän asetuksen noudattamista perustamalla valvontaviranomaisen roolin. Tätä varten yhden tai useamman jäsenmaakohtaisen viranomaisen on seurattava ja valvottava asetuksen soveltamista ja tehtävä yhteistyötä muiden valvontaviranomaisten kanssa. Jäsenmaiden on ilmoitettava valitsemastaan valvontaviranomaisesta Euroopan komissiolle viimeistään asetuksen voimaantulopäivänä. [2, 46. artikla.]

Valvontaviranomainen toimii riippumattomana tahona valvoen ja ohjeistaen tämän asetuksen säädöksiä. Valvontaviranomainen ei saa pyytää ohjeistusta tehtäviensä hoitoon miltään taholta, minkä perusteella valvontaviranomainen on ylin päättävä elin. Valvontaviranomaisen jäsenistön valitsee jäsenvaltion parlamentti tai hallitus, ja jäsenillä on oltava yleisesti tunnistettu kokemus henkilötietojen suojaa koskevista tehtävistä. Asetus ei ota kantaa valvontaviranomaisen jäsenmäärään, kunhan jäsenvaltio määrittää valvontaviranomaiselle riittävät resurssit tehtävien tehokkaaseen suorittamiseen. Oletettavaa on, että valvontaviranomaiseksi ei riitä missään EU-valtiossa yksi henkilö. [2, 47–48. artikla.]

Valvontaviranomaisen päätehtäviin kuuluu tutkia rekisteröityjen tekemiä valituksia rekisterinpitäjistä ja ratkaista riitatilanteita näiden välillä. Asetus painottaa valvontaviranomaisen roolia rekisteröidyn edun ajajaksi ja yksilön oikeuksia ja vapauksia suojele-

vaksi tahoksi; valvontaviranomaisen on edistettävä ja tiedotettava henkilötietojen käsittelyyn liittyvistä riskeistä ja oikeuksista kansalaisille. Asetus määrää valvontaviranomaiselle useita valtuuksia rekisterinpitäjiä ja henkilötietojen käsittelijöitä kohtaan, mutta ei yhtäkään rekisteröityä kohtaan. [2, 52–53. artikla.]

Valvontaviranomaisen jäsenten toimikausi on oltava vähintään neljä vuotta. Jäsenvaltio saa itsenäisesti päättää toimikauden pituudesta ja siitä, voivatko jäsenet suorittaa useampia toimikausia. Asetus antaa jäsenvaltioille vapauden päättää valvontaviranomaisen käytännön asioista, kuten jäseniltä vaadittavasta pätevyydestä ja tarkemmista tehtävistä. Valvontaviranomaisen jäsenillä ja muulla henkilöstöllä on myös elinikäinen salassapitovelvollisuus kaikkiin luottamuksellisiin tietoihin liittyen, joita nämä ovat käsitelleet tehtävissään. Asetus kieltää valvontaviranomaisten jäseniltä kaiken muun samanaikaisen ammattitoiminnan ohella myös sellaisen toiminnan, joka ei sovellu yhteen valvontaviranomaisen tehtävien kanssa. Jäsenen voi erottaa, mikäli tämä ei täytä enää tehtävien asettamia vaatimuksia tai jos jäsen on syyllistynyt vakavaan virheeseen. [2, 48–50. artikla.]

Asetus määrää myös, että pitää perustaa Euroopan tietosuojaneuvosto, johon täytyy kuulua yksi valvontaviranomaisen johtaja kustakin jäsenvaltiosta sekä Euroopan tietosuojavaltuutettu. Tämä tietosuojaneuvosto vastaa tietosuojakäytäntöjen kehittämisestä ja antaa Euroopan komissiolle neuvoja tietosuoja-asetuksen mahdollisesta muuttamisesta. Tietosuojaneuvosto tarkastelee tämän asetuksen suositusten ja käytäntöjen soveltamisesta ja edistää valvontaviranomaisen toimia kussakin jäsenvaltiossa. Tietosuojaneuvosto ei kuitenkaan ole valvontaviranomaisia valvova taho, joskin asetus määrittää tietosuojaneuvoston antamaan lausuntoja valvontaviranomaisten päätösluonnoksista liittyen eri jäsenvaltioiden valvontaviranomaisten yhteistyöhön. [2, 64. ja 66. artikla.]

2.7 Rikkeiden seuraamukset ja sanktiot

Asetus määrittää rekisterinpitäjälle vastuut ja seuraamukset henkilötietojen käsittelyyn liittyvistä rikkeistä. Yksittäinen rekisteröity voi vaatia myös vahingonkorvauksia, mikäli tälle on aiheutunut vahinkoa tämän asetuksen säännösten noudattamatta jättämisestä. Rekisterinpitäjä ja henkilötietojen käsittelijä voidaan vapauttaa tästä vastuusta vain, jos kyseiset tahot voivat osoittaa, etteivät ole vastuussa rikkeen tai vahingon aiheuttanees-

ta tapahtumasta. Asetus kuitenkin toisaalta määrittää oletusarvoisen tietosuojan josta rekisterinpitäjä sekä henkilötietojen käsittelijä vastaavat, joten tämän soveltaminen jäänee tapauskohtaiseksi. [2, 77. artikla.]

Valvontaviranomaisella on valtuus määrätä hallinnollisia seuraamuksia ja sanktioita tämän asetuksen noudattamatta jättämisestä rekisterinpitäjälle tai tämän nimittämälle edustajalle. Näiden seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Rangaistukset ovat lähinnä sakkorangaistuksia, joissa sakon määrään vaikuttaa sääntöjen rikkomisen luonne, vakavuus ja kesto, tahallisuus tai tuottamuksellisuus, kyseisen tahon aiemmat rikkomukset, tekniset ja organisatoriset toimenpiteet ja menettelyt sekä valvontaviranomaisen kanssa käyty yhteistyö asian korjaamiseksi. [2, 79. artikla.]

Mikäli kyseessä on ensimmäinen ja tahaton rikkomus, valvontaviranomainen voi antaa asiasta kirjallisen varoituksen tai jättää seuraamus määräämättä, jos kyseisen rikkeen tekee yksityinen henkilö ilman ansaitsemistarkoitusta tai jos kyseessä on yritys tai järjestö, jolla on alle 250 työntekijää ja joka käsittelee henkilötietoja ainoastaan pääasiallisen toimintansa aputoimintona. [2, 79. artikla.]

Valvontaviranomaisen on määrättävä sakkoa enintään 250 000 euroa tai enintään 0,5 prosenttia yrityksen maailmanlaajuisesta liikevaihdosta seuraavissa tapauksissa:

- rekisterinpitäjä ei menettele oikein mikäli rekisteröity pyytää henkilötietojen tarkistusta, tai ei toimita viipymättä tai vaaditussa muodossa rekisteröidyn pyytämiä tietoja (tiedonsaantioikeus)
- rekisterinpitäjä perii henkilötietojen tarkastuksesta tai rekisteröityjen pyyntöihin vastaamisesta maksun. [2, 79. artikla.]

Valvontaviranomaisen on määrättävä sakkoa enintään 500 000 euroa tai enintään 1 prosentti yrityksen maailmanlaajuisesta liikevaihdosta seuraavissa tapauksissa:

- rekisterinpitäjä ei anna rekisteröidylle tämän pyytämiä tietoja tai antaa puutteellisia tietoja, tai jos tiedot eivät ole riittävän selkeässä muodossa
- rekisterinpitäjä ei oikaise vääriä henkilötietoja (oikeus tietojen oikaisemiseen), eikä ilmoita oikaistuista tiedoista vastaanottajille joille tietoja on luovutettu
- rekisterinpitäjä ei noudata rekisteröidyn oikeutta tulla unohdetuksi ja poistaa henkilötiedot tai ei toteuta kaikkia tähän liittyviä toimenpiteitä

- rekisterinpitäjä ei toimita henkilötietojen jäljennöstä sähköisessä muodossa tai estää rekisteröityä siirtämästä henkilötietoja toiseen järjestelmään
- rekisterinpitäjä ei määritä yhteisten rekisterinpitäjien vastuualueita riittävästi tai lainkaan
- rekisterinpitäjä ei säilytä ollenkaan tai riittävässä määrin asetuksessa määrättyjä asiakirjoja
- rekisterinpitäjä ei noudata sananvapauteen, historiantutkimukseen, tilastollisiin tai tieteellisiin tutkimuksiin määrättyjä sääntöjä [2, 79. artikla.]

Muista vakavimmista rikkeistä valvontaviranomaisen on määrättävä sakkoa enintään 1 000 000 euroa tai enintään 2 prosenttia yrityksen maailmanlaajuisesta liikevaihdosta. Tällaisia rikkeitä ovat muun muassa henkilötietojen käsittely ilman riittävää oikeusperustaa tai jos rekisterinpitäjä ei noudata asetuksessa määrättyjä tietoturvavaatimuksia. [2, 79. artikla.]

2.8 Voimaantulo

Tietoturva-asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu Euroopan unionin virallisessa lehdessä. Asetusta sovelletaan kahden vuoden kuluttua edellä mainitusta päivämäärästä. [2, 91. artikla.] Tämän työn tekohetkellä direktiiviä ei ole vielä otettu käsittelyyn, mutta tietosuoja-asetus on käsitelty Euroopan komission toimesta 6.6.2013 [7]. Tällä hetkellä asetus odottaa komission päätöstä, ja oletettavasti päätös tehdään kuluvan vuoden aikana.

Tämä tarkoittaisi sitä, että asetusta olisi noudatettava vuonna 2015 tai 2016. Viivästykset ovat myös mahdollisia, mikäli asetuksen sisältöä joudutaan tarkastelemaan tai muuttamaan.

3 Valtioneuvoston tietoturva-asetus 681/2010

Valtioneuvoston asetuksella 681/2010 tietoturvallisuudesta valtionhallinnossa on tarkoitus luoda asianmukaiset puitteet sähköisen asianhallinnan ja sähköisten palvelujen kehittämiselle. Asetuksessa säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevia yleisiä tietoturvallisuusvaatimuksia sekä asiakirjojen luokittelua ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista vaatimuksista. Asetusta

sovelletaan myös toisen maan viranomaiselta tai kansainväliseltä toimielimeltä saadun asiakirjan käsittelyyn. Yhtenäisillä menettelyillä mahdollistetaan tietoaineistojen turvallinen käsittely viranomaisten ja viranomaistietoa käsittelevien osapuolten kanssa. [8; 9, s. 13.]

Asetus määrää hieman samanlaisia tietoturvavaatimuksia kuin EU:n tietosuoja-asetus 2012/0011, joskaan ei niin ehdottomin säännöksin. Asetus painottuu enemmän asiakirjojen suojaustasoihin ja suojattujen asiakirjojen käsittelyyn, ja määrää pakolliseksi myös tietoturvan perustason toteuttamisen. [8.]

3.1 Tietoturvan perustason toteuttaminen

Asetus määrää valtionhallinnon viranomaiselle toteutettavaksi perustason tietoturvan, johon lukeutuu myös tietoturvariskien kartoitus. Viranomaisen on huolehdittava siitä, että sen käytössä on riittävä osaaminen ja välineistö tietoturvallisuuden varmistamiseen. Tietoturvallisuuteen liittyvät tehtävät ja vastuut ovat myös määritettävä. Hyvä tiedonhallintatapa edellyttää asiakirjojen ja tietoaineistojen saatavuutta ja käytettävyyttä. Tähän kuuluu myös rekisteritietojen ja asiakirjojen salassapitorakenteesta huolehtiminen. Asiakirjojen käsittelyyn on myös määrättävä tehtävät ja vastuu. Asiakirjoja on valvottava ja hallittava pääsynhallinnalla siten, että vain tarpeelliset henkilöt pääsevät niihin käsiksi. [8; 9, s. 35–36.]

Henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville on annettava riittävä ohjeistus ja koulutus asianmukaisesta käsittelystä. Henkilöstön luotettavuus on varmistettava tarvittaessa esimerkiksi turvallisuusselvitysmenettelyn kautta. Myös tilat, joissa salassa pidettäviä tietoja tai henkilörekistereitä käsitellään, tulee olla asianmukaisesti suojattuja ja valvottuja. [8; 9, s. 36.]

Asetus vaatii suojaamaan tiedot tarpeellisilla toimenpiteillä, ja tietojärjestelmissä tulee toteuttaa asianmukainen käytön hallinta ja valvonta sekä huolehtia riittävistä turvallisuusjärjestelyistä. Lisäksi on estettävä tietojen luvaton tai asiaton muuttaminen tai käsittely. [8.]

Perustason tietoturvan toteuttaminen asettaa hieman samanlaisen vaatimuksen tietoturvalle kuten EU:n tietosuoja-asetus (vrt. luku 2.5). Suojattujen asiakirjojen ja henkilö-

tietojen luvaton ja asiaton käyttö sekä tuhoutuminen on estettävä asianmukaisilla turvallisuusjärjestelyillä.

3.2 Asiakirjojen luokittelu

Asetus määrittää ohjeistuksen salassa pidettävien asiakirjojen luokittelulle. Viranomainen voi kuitenkin itse päättää, luokitteleeko tämä asiakirjoja vai ei. Asiakirjat voi luokitella seuraaviin luokkiin:

- Suojaustaso 1: Asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle.
- Suojaustaso 2: Asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle.
- Suojaustaso 3: Asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle.
- Suojaustaso 4: Asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle. [8, 9. artikla.]

Asiakirjat ja niihin sisältyvät tiedot voidaan luokitella sen mukaan, minkälaisia tietoturvaan liittyviä vaatimuksia niiden käsittelyssä on tarpeen noudattaa. Luokittelu voidaan kohdistaa myös vain sellaisiin asiakirjoihin tai käsittelyvaiheisiin, joissa tarvitaan erityistoimenpiteitä suojattavan edun vuoksi. Suojattaviin asiakirjoihin on myös sisällytettävä turvallisuusluokitusmerkintä, josta käy ilmi asiakirjan suojaustaso. Turvallisuusluokitusmerkinnät ovat

- ”ERITTÄIN SALAINEN” (suojaustaso 1)
- ”SALAINEN” (suojaustaso 2)
- ”LUOTTAMUKSELLINEN” (suojaustaso 3)
- ”KÄYTTÖ RAJOITETTU” (suojaustaso 4). [8, 11. artikla.]

Turvallisuusluokitusmerkinnät on merkittävä tarvittaessa myös ruotsiksi tai englanniksi. Tällöin merkinnät ovat ”YTTERST HEMLIG” tai ”TOP SECRET” (suojaustaso 1),

”HEMLIG” tai ”SECRET” (suojaustaso 2), ”KONFIDENTIELL” tai ”CONFIDENTIAL” (suojaustaso 3) ja ”BEGRÄNSAD TILLGÅNG” tai ”RESTRICTED” (suojaustaso 4). [8, 11–12 artikla.]

3.3 Luokitellun asiakirjan käsittelyä koskevat vaatimukset

Suojaustasoihin 1-3 kuuluviin asiakirjoihin on annettava käyttöoikeus vain niille, joilla on työtehtäviensä vuoksi tarpeen saada tietoja asiakirjasta tai muutoin käsitellä sitä. Sama koskee myös suojaustason 4 asiakirjaa, mikäli siihen kuuluu arkaluonteisia henkilötietoja tai biometrisia tunnistetietoja. Suojaustasoihin 1 ja 2 kuuluvat asiakirjat on säilytettävä kassakaapissa tai muussa vastaavassa lukittavassa kaapissa. Lisäksi niiden henkilöiden on oltava tunnistettavissa, joilla on pääsyoikeus tiloihin, joissa käsitellään tai säilytetään asiakirjoja. Luokiteltuja asiakirjoja ei saa säilyttää tai käsitellä muualla kuin viranomaisen toimitiloissa, ellei tätä ole erikseen sallittu. [8, 13–14. artikla.]

Suojaustasoihin 1 ja 2 kuuluva asiakirja voidaan tallentaa sähköisesti laitteelle, mikäli laite ei ole kytketty tietoverkkoon tai tietoverkko on sellainen, joka on erityisvalvottu eikä siihen ole yhteyttä muista tietoverkoista. Suojaustasoon 2 kuuluva asiakirja voidaan tallentaa tietoverkkoon liitetylle laitteelle, jos verkon käyttö on rajoitettu ja jos asiakirja tallennetaan vahvasti suojattuna. Suojaustasoon 3 kuuluva asiakirja voidaan tallentaa tietoverkkoon liitetylle laitteelle, jos verkon käyttö on rajoitettu ja asiakirja tallennetaan salattuna tai muutoin suojattuna. Edellinen koskee myös suojaustasoon 4 kuuluvaa asiakirjaa, mikäli siihen liittyy arkaluontoisia henkilötietoja tai biometrisia tunnistetietoja. Vastaavanlaisissa tietoverkoissa asiakirjojen siirtäminen on myös sallittu. [8, 16. artikla.]

Suojaustasoon 1 kuuluvaa asiakirjaa ei saa kopioida ilman sen laatineen viranomaisen lupaa. Lisäksi suojaustasojen 1 ja 2 asiakirjojen kopiot on luetteloitava. Mikäli asiakirjoja välitetään eteenpäin, on ne pakattava asianmukaisesti ja toimitettava henkilökohtaisesti tai muulla viranomaisen hyväksymällä tavalla vastaanottajalle. Myös asiakirjojen käsittely on kirjattava tietojärjestelmään tai muuhun lokiin. Tarpeettomaksi käyneet suojaustasojen 1 ja 2 asiakirjojen kopiot tulee hävittää, jollei niitä palauteta asiakirjan laatineelle viranomaiselle. [8, 17–21. artikla.]

3.4 Voimaantulo

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnosta on tullut voimaan 1. lokakuuta 2010. Siirtymäsäännöksissä mainitaan, että viranomaisen tietojenkäsittely on saatettava vastaamaan tietoturvallisuuden perustasoa kolmen vuoden kuluessa asetuksen voimaantulosta, eli 1. lokakuuta 2013 mennessä. Luokiteltujen asiakirjojen käsittely on saatettava vastaamaan asetuksen säädöksiä viiden vuoden kuluessa siitä, kun viranomainen on päättänyt luokitella asiakirjansa. Toimitiloja koskevat vaatimukset on toteutettava viiden vuoden kuluessa asetuksen voimaantulosta, eli 1. lokakuuta 2015 mennessä. [8, 22–23 artikla.]

4 Tietoturvan toteuttaminen käytännössä

Luvuissa 2 ja 3 esitetyt asetukset vaativat, että arkaluonteista tietoa ei saa kadota tai vuotaa väärille tahoille tietojärjestelmissä ja -verkoissa. Euroopan komission ehdotus tietosuoja-asetuksesta 2012/0011 edellyttää, että henkilörekisterin tietoja ei saa luvattomasti muuttaa tai käsitellä, eikä tietoja saa hävitä tai tuhoutua. Valtioneuvoston asetuksen 681/2010 edellyttämä tietoturvan perustason toteuttaminen vaatii myös salattujen tietojen suojaamista ja tietojen luvattoman tai asiattoman muuttamisen tai käsittelyn estämistä. Asetusten tietoturvavaatimukset edellyttävät niin teknisiä järjestelmiä kuin myös henkilöstön ohjeistamista. Ennen teknisten järjestelmien käyttöönottoa on syytä tunnistaa ja suunnitella mahdolliset tietoturvariskit ja määrittää, miten näitä voidaan ehkäistä.

4.1 Miten tietoa vuotaa

Tietovuoto tarkoittaa, että hallussa oleva tieto pääsee tavalla tai toisella väärälle taholle. Tämä tieto voi olla niin fyysistä kuin elektronista, ja tietoa voi myös kadota tai tuhoutua tarkoituksettomasti. Nykyaikana yhä useammin arkaluontoinen tieto siirretään elektronisesti tietojärjestelmiä ja -verkkoja hyödyntäen. Siirrettävää tietoa voi olla esimerkiksi rahaliikenne, henkilötiedot sekä yrityssalaisuudet. Tällöin on luonnollista olettaa, että tätä tietoa tavoittelevat myös ulkopuoliset tahot. Tiedon, tietojärjestelmien ja -verkkojen suojaaminen on avainasemassa turvallisen tiedonsiirron varmistamiseksi.

Tietovuodot ja niiden estäminen ovat nykyaikana merkittävä osa tietoturvallisuutta. Tietoturvayhtiö Symantecin Internet Security Threat -raportin mukaan vuonna 2012 varastettiin 12 miljoonaa identiteettiä kuukaudessa koko vuoden keskiarvona [10, s. 18].

Kuva 1. Vuoden 2012 aikana varastetut identiteetit Symantecin raportin mukaan [10, s. 18].

Tässä työssä käsitellään tietojärjestelmissä ja -verkoissa tapahtuvia tietovuotoja. Tietovuodon aiheuttaja voi olla joko ulkoinen tai sisäinen, ja se voi tapahtua joko tahallisesti tai tahattomasti. Ulkoisilla tekijöillä tarkoitetaan tässä esimerkiksi ulkoisia hyökkäyksiä tietojärjestelmiä tai -verkkoja kohtaan. Näitä voivat olla esimerkiksi palvelunestohyökkäykset, murtautumisyritykset, haittaohjelmien levittäminen sekä verkon liikenteen seuraaminen ulkoapäin, joiden vaikutuksesta tietoa päätyy ulkopuolisille tahoille. Ulkoisia hyökkäyksiä pystytään havaitsemaan ja estämään esimerkiksi palomuurien ja erilaisten tunkeilijoiden havaitsemis- ja estojärjestelmien (IDS/IPS, Intrusion Detection/Prevention System) avulla. Julkisissa verkoissa on suositeltavaa suojata tieto esimerkiksi kryptauksella ja käyttää suojattuja yhteysmenetelmiä. Tällöin ulkopuolinen taho ei välttämättä voi hyödyntää tietoa vaikka pääsisikin siihen käsiksi.

Tietojärjestelmissä ja -verkoissa tietoa voi myös kadota tiedonsiirrossa tai laitteiston fyysisten komponenttien hajoamisen kautta. Tätä voidaan ehkäistä muun muassa tietojärjestelmien luotettavuudella ja redundanttisuudella.

Sisäinen tietovuoto on vastaavasti tietyn tietojärjestelmän, -verkon tai organisaation sisältäpäin tapahtuva tietoturvarike. Tämä voi olla esimerkiksi tiedon tahallista tuhoamista, huolimatonta käsittelyä, tahallista vuotamista sekä haittaohjelmien päästämistä järjestelmiin. Sisäinen tietovuoto on pääsääntöisesti käyttäjälähtöistä, joskin esimerkiksi käytetyissä ohjelmistoissa ja järjestelmissä esiintyvät haavoittuvuudet voidaan myös luokitella sisäisiksi uhiksi.

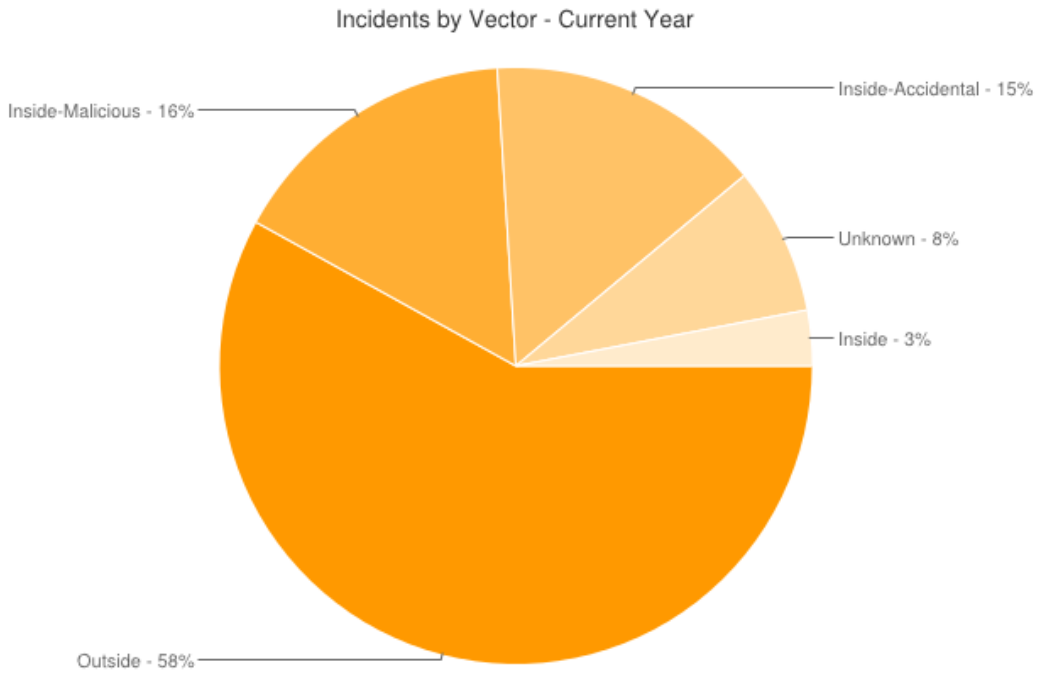
Ulkoiset hyökkäykset ovat nykyaikana huomioitu lähes jokaisen tahon tietoturvakäytänteissä. Tässä työssä tutustutaan sisäisiin tietovuotoihin, joista tarkastellaan yleisimpiä sisäisten tietovuotojen ilmenemistapoja ja miten niitä voidaan estää. [11, s. 5-6.] Luvuissa 2 ja 3 esitetyt asetukset edellyttävät sisäisten tietovuotojen ja tiedon häviämisen estämistä.

4.1.1 Sisäiset tietovuodot

Sisäisiä tietovuotoja voi tapahtua niin tahallisesti kuin tahattomasti. Tahallinen tietovuoto on tietoinen teko, yleensä jonkin henkilön tai henkilöryhmän aiheuttama, ja siihen on yleensä jokin painava motiivi. Tahallinen tietovuoto voi olla esimerkiksi arkaluontoisten tietojen toimittamista kilpailevalle taholle tai sabotointia tietojen tahallisella muuttamisella tai tuhoamisella. Yleisimpiä syitä tahalliseen tietovuotoon ovat taloudellisen edun tavoittelu ja esimerkiksi irtisanotun henkilön katkeruus entistä työnantajaansa kohtaan. [11, s. 7.]

Tahaton tietovuoto tapahtuu vahingossa ilman, että tietovuodon aiheuttaja on tarkoittanut tai ymmärtänyt tätä. Yleensä vahinko tapahtuu joko tietämättömyydestä käytössä olevia tietojärjestelmiä kohtaan tai huolimattomuuden takia. Tällaisia tapahtumia voivat olla muiden muassa arkaluontoisen tiedon siirto salaamattomana tai ulkopuolisten tahojen pääsyn mahdollistaminen tietojärjestelmiin. Tahaton tietovuoto voi aiheutua myös huolimattomalla työvälineiden käsittelyllä, kuten esimerkiksi tärkeiden tiedostojen poistamisella vahingossa ilman varmuuskopiointia tai jopa tietokoneen hukkaamisella, jolloin joku muu voi päästä tietoihin käsiksi. Myös käyttäjän henkilökohtaisen tietoturvan laiminlyönti on sisäinen tietovuotoriski.

Sisäiset tietovuodot muodostavat merkittävän osan tietovuodoista. Esimerkiksi Open Security Foundationin ylläpitämän DataLossDB-tietokannan mukaan sisäiset tietovuodot, niin tahalliset kuin tahattomat, muodostavat noin kolmasosan kaikista tietovuodoista vuonna 2013 työn tekohetkeen mennessä. [12.]



Kuva 2. Vuonna 2013 tapahtuneiden tietovuotojen jakauma [12].

DataLossDB:n kuvassa kuvataan tahallisia sisäisiä hyökkäyksiä Inside-Malicious -termillä ja tahattomia sisäisiä tietovuotoja Inside-Accidental -termillä [12]. Tietoturvayhtiö Symantec on havainnoinut vastaavasti sisäisten tietovuotojen merkittävän osuuden omassa raportissaan, joka myös tarkkailee kuluvan vuoden tietovuotojen ilmentymiä [13, s. 11].

Kuva 3. Symantecin tilasto tämän vuoden tietovuotojen syistä [13, s. 11].

Symantecin mukaan vahingossa tapahtuvat sisäiset tahattomat tietovuodot (engl. ”Accidentally Made Public”) ovat selkeästi tahallisia tietovuotoja (engl. ”Insider Theft”) yleisimpiä. Vahingossa julkaistut ja lähetetyt arkaluontoiset tiedot muodostivat suuremman osan tietovuodoista kuin esimerkiksi ulkopuoliset hyökkäykset [23, s. 11]. Samaa on havainnut myös tietoturvayhtiö Check Point. Tämän vuoden tietoturvaraportissaan Check Point kertoo, että esimerkiksi 28 %:ssa tutkituista organisaatioista sisäisesti tarkoitettu sähköposti on vahingossa lähetetty ulkoiselle taholle [14, s. 31]. Raportista ilmenee myös alla olevat osuudet tietovuodoista. Prosenttiosuus kuvaa organisaatioita, joista on lähetetty organisaation ulkopuolelle seuraavia tietoja:

- 29 % - luottokorttitietoja
- 24 % - lähdekoodia sisältäviä tiedostoja
- 14 % - salasanalla suojattuja tiedostoja
- 13 % - palkkatietoja
- 7 % - luottamukselliseksi merkittyjä sähköposteja
- 6 % - yrityksen sisäisiä tietoja
- 3 % - pankkitilien tunnistetietoja. [14, s. 32.]

Check Pointin tietoturvaraportti antaa myös useita esimerkkejä käytännössä tapahtuneista tahattomista tietovuodoista. Esimerkiksi Texasin A&M-yliopisto lähetti huhtikuussa 2012 sähköpostin vahingossa täysin väärälle henkilölle. Sähköpostin liitetiedosto sisälsi yliopiston tuhansien entisten opiskelijoiden henkilötietoja. Lokakuussa 2012 japanilaisen sanomalehden Yomiuri Shimbun toimittaja lähetti tutkimustuloksiaan vahingossa kollegan sijaan useille median edustajille. Tämä päätyi toimittajan irtisanomiseen. [14, s. 31.]

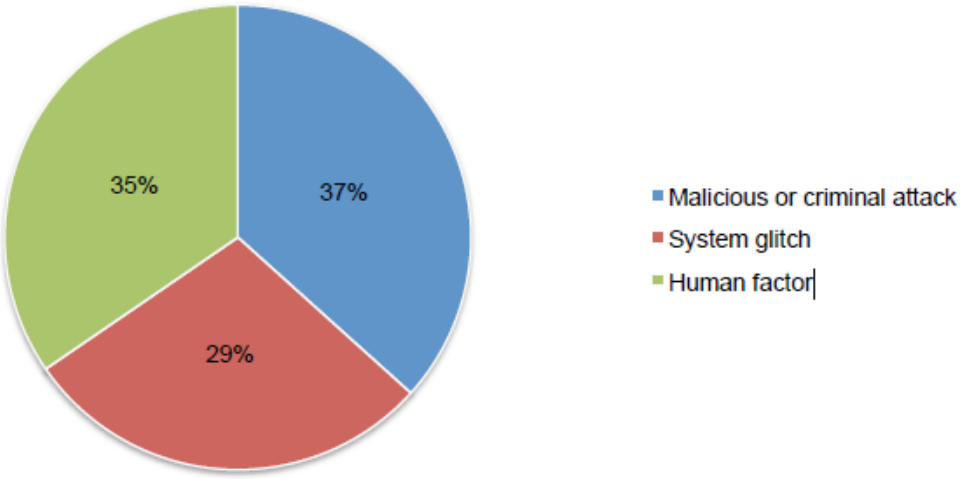
4.1.2 Tietovuodon kustannukset

Suomesta ei ole saatavilla tilastoa tietovuotojen kustannuksista, mutta esimerkiksi tutkimusyritys Ponemon Institute on tutkinut Symantecin avustuksella tietovuotojen kustannuksia suurimmissa maissa kuluvana vuotena. Tutkimus kattaa yhdeksän maata, joista Euroopan maita ovat Englanti, Ranska, Saksa sekä Italia. [15.] Tietovuodon kustannukset koostuvat kokonaisuudessaan seuraavista osista:

- Tietovuodon havaitseminen – Toimenpiteet, joilla havaitaan tietovuoto tapahtuneeksi.
- Eskalointi – Vaadittavat ilmoitukset tietovuodosta organisaatiossa määrätyille henkilöille.
- Ilmoitus ulkopuolisille tahoille – Ilmoittaminen tietovuodosta asiakkaille, yksityishenkilöille tai muille tahoille, joiden rekisteritietoja tietovuoto koskee.
- Tietovuodon jälkeiset toimenpiteet – Mahdolliset jälkitoimenpiteet, joilla tietovuodon vaikutus jäisi mahdollisimman alhaiseksi. [15, s. 20.]

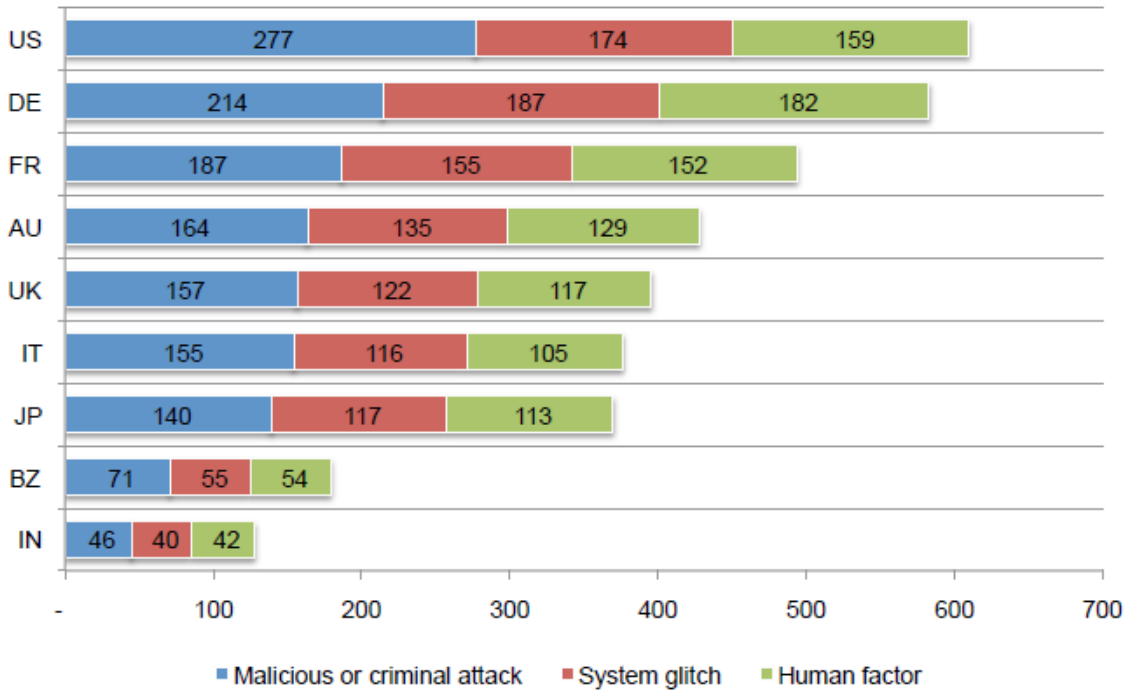
Edellisten toimenpiteiden lisäksi tietovuodolla saattaa olla myös epäsuoria kustannusvaikutuksia. Asiakas- ja kumppanuussuhteet saattavat kärsiä, varsinkin niiden osalta, joita tietovuoto on koskenut. Myös uusien suhteiden solmiminen saattaa tuottaa vaikeuksia, sillä julkisuudessa ollut tietovuoto on merkittävä negatiivinen tekijä. [15, s. 20.]

Ponemon Instituten tutkimus jakaa tietovuotojen juurisyyt kolmeen alueeseen; tahallisiin hyökkäyksiin (engl. ”Malicious or criminal attack”), järjestelmien tahattomiin häiriöihin (engl. ”System glitch”) sekä käyttäjälähtöisiin tietovuotoihin (engl. ”Human factor”). [15, s. 7.] Tutkimuksessa esiintyneet tietovuodot jakautuivat näihin juurisyihin kuvan 4 mukaisesti.



Kuva 4. Ponemon Instituten tutkimuksen tietovuotojen juurisyiden jakauma [15, s. 7].

Tahallisilla hyökkäyksillä tarkoitetaan tässä ulkopuolisia sekä sisäisiä hyökkääjiä, mutta myös huolimattomia käyttäjiä, jotka esimerkiksi päästävät vahingossa hyökkääjän haittaohjelmia järjestelmiin. [15, s. 7.] Kuvassa 5 on näkyvillä tietovuotojen kokonaiskustannukset tutkituissa maissa asukasta kohden Yhdysvaltain dollareina.



Kuva 5. Tietovuotojen kokonaiskustannukset tutkituissa maissa eri juurisyiden mukaan [15, s. 8].

Tuloksista on nähtävillä, että tahallisten hyökkäysten seuraukset ovat muita kalliimpia. Tähän kuitenkin lukeutuvat tahalliset ulkoiset ja sisäiset hyökkäykset, kuin myös käyttäjän huolimattomuudesta aiheutunut ulkoinen hyökkäys. Järjestelmähäiriöt sekä käyttäjälähtöiset tietovuodot voidaan kuitenkin luokitella sisäisiksi tietovuodoiksi. Tässä käyttäjälähtöisellä tietovuodolla tarkoitetaan vahingossa tapahtunutta tahatonta tietovuotoa. Kokonaisuudessaan käyttäjälähtöisten, käyttäjän huolimattomuudesta johtuneiden sekä tahalliset tietovuotojen estäminen toisi merkittäviä säästöjä kokonaisuuteen.

Tutkimuksessa huomattiin eräiden toimenpiteiden vähentävän tietovuotojen kokonaiskustannuksia. Näitä olivat ulkopuolisten konsulttien käyttäminen, tietoturvajohtajan nimittäminen, toimintasuunnitelma tietovuodon sattuessa sekä olemassa oleva tietoturvapolitiikka. Kustannukset olivat myös suoraan verrannollisia tietovuodon kokoon ja vaikutusalaan. [15, s. 9.]

Luvussa 2 käsitelty Euroopan komission ehdotus tietosuoja-asetuksesta 2012/0011 määrää myös sanktioita henkilörekistereihin kohdistuvista tietovuodoista, jotka saattavat olla jopa 1 000 000 euroa tai 2 % yrityksen maailmanlaajuisesta liikevaihdosta.

Mahdollisesti myös kansallinen oikeuslaitos tai muu taho voi määrätä sakkorangaistuksen tapahtuneesta tietovuodosta. Esimerkiksi vuonna 2012 Stoke-on-Trentin kaupunginvaltuuston jäsen lähetti vahingossa arkaluonteista tietoa sähköpostitse väärälle vastaanottajalle. Kaupunginvaltuusto sai tapauksesta 120 000 punnan sakon. [14, s. 30.]

4.2 Yleisimpiä tietovuotoriskejä

Tietovuoto voi aiheutua useilla eri tavoilla. Seuraavassa on käsitelty yleisimpiä tietovuodon mahdollistavia asioita, jotka voivat olla joko tahallisia tai tahattomia. Useissa tietovuodoissa vahinko voi tapahtua sisäisesti ulkoisen tekijän kautta. Tällainen on esimerkiksi onnistunut ulkoinen hyökkäys, jonka avulla päästään sisäisiin tietoihin käsiksi.

4.2.1 Sähköposti

Kenties yleisimmin käytetty tietovuodon mahdollistava viestintäväline on sähköposti. Käyttäjä voi lähettää arkaluonteista tietoa joko sähköpostin tekstikentässä tai liitetie-

dostona. Liitetiedosto voi olla myös salattu, pakattu tai liitetty muihin tiedostoihin, jolloin sen alkuperä ja tarkoitus on hankalampi selvittää. Arkaluonteisesta tiedosta voi myös ottaa esimerkiksi kuvaruutukaappauksia ja liittää ne sähköpostiin kuvina. Sähköpostitse voi myös vahingossa lähettää arkaluonteista tietoa, esimerkiksi henkilötietoja tai jopa vääränlaisen liitetiedoston, tai lähettää sähköpostin täysin väärälle vastaanottajalle tai vastaanottajaryhmälle. [11, s. 11–12.] Sähköpostin lieveilmiöinä ovat erilaiset huijausviestit ja muu roskapostitus, joiden välityksellä voi levitä helposti myös haittaohjelmia käyttäjän huolimattomuuden seurauksena. Nykyään useimmat rikolliset ja huijarit kohdentavat resurssejaan sosiaalisen median sivustoille sähköpostin sijaan. [10, s. 31.]

Yleensä yrityksillä ja organisaatioilla on käytössään jokin määrätty sähköpostiohjelma, mutta sähköpostin kautta voi lähettää tietoa myös Web-pohjaisilla sähköpostipalveluilla (engl. ”Web Mail”). Tällaiset palvelut käyttävät yleensä suojattua verkkoyhteyttä (HTTPS, Hypertext Transfer Protocol Secure), jolloin käyttäjän ja palvelun välistä liikennettä on hankalampi valvoa. [11, s. 11–12.]

4.2.2 Pikaviestimet

Monet yritykset ja organisaatiot sallivat henkilöstönsä käyttää ja asentaa käytössään oleville työasemilleen omia ohjelmia. Monet yritykset myös hyödyntävät pikaviestimiä sisäisessä viestinnässään. Pikaviestimien kautta voi lähettää myös tiedostoja, jolloin niiden käytössä on samanlaisia riskejä kuin sähköpostissakin. Pikaviestimiä on äärimmäisen monia, jotka lisäksi käyttävät yleensä omia protokolliaan. Nämä voivat olla täten joko salattuja tai salaamattomia. Yleisimpiä käytössä olevia pikaviestimiä ovat muun muassa Skype, IRC (Internet Relay Chat) sekä yrityskäyttöön suunnattu Microsoft Lync. Useimmilla pikaviestimillä voi lähettää myös ääntä ja kuvaa, jolloin ne voivat toimia eräänlaisina VoIP-puhelimina (Voice Over Internet Protocol). Pikaviestimet ovat myös etenevissä määrin suosittuja kohteita haittaohjelmille. [11, s. 9.]

4.2.3 Vertaisverkot ja välityspalvelimet

Peer-to-Peer (P2P) eli vertaisverkko-ohjelmat ovat mahdollinen tapa jakaa tietoa suurille käyttäjämäärille. Vertaisverkossa voi kuka hyvänsä jakaa mitä tahansa, jolloin sen avulla leviävät myös haittaohjelmat ja muu laiton sisältö. Vertaisverkon avulla on helppo jakaa suuria tiedostoja jopa anonyymisti, jolloin se on otollinen alusta tahallisiin tie-

tovuotoihin. Check Pointin tietoturvaraportin mukaan 61 % tutkituista organisaatioista käytti erilaisia vertaisverkko-ohjelmia. Raportissa annetaan esimerkkejä vertaisverkoissa tapahtuneista tietovuodoista, kuten esimerkiksi EPN Inc -yrityksestä, joka altisti tuhansien ihmisten henkilötietoja saataville vertaisverkkoon vuonna 2012. Suosituin vertaisverkko-ohjelma on tällä hetkellä BitTorrent. [14, s. 20–21.]

Myös erilaiset anonymiteetin tarjoavat julkiset välityspalvelimet (engl. ”Proxy”, ”Anonymous Proxy”) mahdollistavat käyttäjien haitallisen toiminnan peittämisen. Välityspalvelimien toimintaperiaatteena on peittää sitä käyttävien asiakasohjelmien identiteettitiedot, jolloin asiakasohjelmien jäljittäminen on mahdotonta. Tällöin myös käytössä olevat tietoturvasäännöt ovat ohitettavissa, sillä niitä valvotaan yleensä käyttäjien identiteettitietojen perusteella. Tunnettuja välityspalvelimia käyttäviä ohjelmia ovat esimerkiksi Tor ja Hamachi. [14, s. 22.]

4.2.4 Verkkosivustot ja -palvelut

Tietoa voi vuotaa myös verkkosivustojen ja -sovellusten kautta. Näitä ovat muun muassa kotisivut, verkkokaupat, erilaiset verkkotietokannat ja sosiaalisen median sivustot. Niiden kautta voidaan vahingossa sekä tahallisesti julkaista arkaluonteista tietoa. Riski syntyy myös silloin, kun käyttäjille annetaan vahingossa liikaa oikeuksia verkkopalveluihin, jolloin nämä saattavat nähdä arkaluonteisia tietoja palvelusta. Myös henkilöstön omat henkilökohtaiset verkkojulkaisut tai sosiaalisen median julkaisut voivat käsitellä näitä tietoja. [11, s. 13.]

Verkkopalveluissa lisääntyneet haittaohjelmat ja huijausyritykset ovat myös sisäinen tietovuotoriski, joskin itse vahinko tapahtuu ulkoisen tekijän kautta. Haittaohjelma leviää yleisimmin käyttäjän huolimattomuuden tai käytössä olevien sovellusten tietoturva-aukkojen takia. Viime aikoina esimerkiksi yleisesti käytössä olevissa Adoben Flash- ja Oraclen Java -ohjelmistoissa sekä Adoben PDF-tiedostomuodossa (Portable Document Format) on ollut tietoturva-aukkoja. [10, s. 26.]

Haittaohjelmat saattavat etsiä tietokoneelta mahdollisia salaisia asiakirjoja, pyrkiä pääsemään käytössä oleviin tietokantoihin tai vahingoittaa järjestelmiä. [11, s. 13.] Verkkosivujen haavoittuvuudet ovat myös riskitekijä käyttäjälle; tällöin rikollinen voi esimerkiksi laittaa omaa sisältöään tunnetulle verkkosivulle ja näin varastaa tietoa tai aiheuttaa

muuta haittaa käyttäjille. Symantecin tilastojen mukaan verkkosivuihin kohdistuneet hyökkäykset ovat kasvaneet liki kolmasosan viime vuosien aikana [10, s. 26].

Lisäksi erilaiset tiedostonjakopalvelut, kuten Dropbox ja Windows Live Office, antavat käyttäjille mahdollisuuden ladata ja jakaa tiedostoja palvelussa. Tällöin arkaluontoiset tiedostot saattavat päästä vääriin käsiin, vaikka niiden näkyvyys olisi määritelty tietyille käyttäjille. Tiedostonjakopalveluissa on olemassa myös riski tiedon katoamiseen. [14, s. 24.]

4.2.5 FTP

FTP eli File Transfer Protocol on yleisimmin käytetty tiedonsiirtomenetelmä, jossa tietoa voidaan siirtää palvelimen ja asiakasohjelman välillä. FTP-palvelinohjelmistoja on vapaasti saatavilla, jolloin suurienkin tiedostojen siirto on helposti mahdollista. Mahdollinen tietovuotoriski ilmenee siinä, että FTP:n kautta siirretään arkaluontoista tietoa salaamattomana julkisen verkon yli tai jos sitä käytetään tarkoituksella siirtämään arkaluontoista tietoa muualle. FTPS (FTP Secure) salaa FTP-liikenteen, jolloin tiedonsiirto on turvallisempaa. Myös muita vastaavia tiedonsiirtomenetelmiä on olemassa, kuten esimerkiksi salattua SSH-protokollaa (Secure Shell) käyttävä Secure copy (SCP). Tiedonsiirtomenetelmät ovat yleensä enemmän käytössä tahallisissa tietovuodoissa. [11, s. 14.]

4.2.6 Ulkoiset tallennusvälineet

Ulkoiset tallennusvälineet ovat helppo tapa siirtää ja kopioida tiedostoja. USB-muisti tai muistikortti sopii lähes jokaiseen laitteeseen. Nämä ovat myös pienen kokonsa vuoksi helposti kuljetettavissa ja piilotettavissa. Tämän vuoksi nämä ovat lisäksi helposti varastettavissa tai kadotettavissa. [11, s. 16.]

Edellisten lisäksi mahdollisia tallennusvälineitä ovat ulkoiset kiintolevyt, CD/DVD-asemat sekä erilaiset musiikki- ja videotoistimet. Lisäksi USB-liitännän sijaan voidaan käyttää esimerkiksi langatonta Bluetooth-tiedonsiirtotekniikkaa. Tämän avulla tiedostoja voi helposti ja huomaamattomasti kopioida kahden päätelaitteen välillä. [11, s. 16.] Ulkoisia tallennusvälineitä käytettäessä on hyvä käyttää yrityksen tai organisaation omia

välineitä, sillä käyttäjien henkilökohtaiset tallennusvälineet voivat altistaa tuotantoverkon haittaohjelmille.

4.2.7 Mobiililaitteet

Mobiililaitteet, kuten puhelimet ja tabletit, voivat myös mahdollistaa tietovuotoja. Yrityksen tai organisaation mobiililaitteet saattavat altistua haittaohjelmille tai ulkoisiin hyökkäyksiin, mikäli niitä käytetään esimerkiksi julkisissa verkoissa. Lisäksi arkaluonteista tietoa sisältävä mobiililaite on helpompi varastaa kuin esimerkiksi tietokone, ja usein niissä olevia tietoja ei pystytä salaamaan [10, s. 37]. Usein myös käyttäjät eivät ole mobiililaitteiden tietoturvasta riittävän tietoisia, ja saattavat tehdä mobiililaitteilla asioita, jotka uhkaavat tietoturvaa. Ylläpidon on myös hankala hallita mobiililaitteita kokonaisvaltaisesti ja varmistaa, onko kyse oikeasta käyttäjästä sekä käyttäjäoikeuksista. [10, s. 37].

Käyttäjien henkilökohtaiset mobiililaitteet voivat myös muodostaa tietoturvauhkia, jos niitä käytetään yrityksen tai organisaation omassa verkossa. Henkilöstön omat mobiililaitteet voivat altistaa tuotantoverkon haittaohjelmille tai jopa urkinnalle. Mobiililaitteille suunnatut haittaohjelmat ja haavoittuvuudet ovat lisääntyneet viime vuosien aikana runsaasti. Symantecin raportin mukaan Android-käyttöjärjestelmälle oli eniten tunnettuja uhkia, siinä missä Applen iOS-käyttöjärjestelmästä dokumentoitiin eniten haavoittuvuuksia (kuva 6). [10, s. 35.]

Platform	Documented Vulnerabilities
Apple iOS	387
Android	13
BlackBerry	13
Nokia	0
LG Electronics	0
Windows Mobile	2

Device Type	Number of Threats
Android malware	103
Symbian malware	3
Windows Mobile malware	1
iOS malware	1

Kuva 6. Vuonna 2012 havaitut mobiilikäyttöjärjestelmien tietoturvauhat ja haavoittuvuudet [10, s. 35].

Lisäksi mobiililaitteilla on helppo tallentaa tietoa tai ottaa jopa valokuvia tai videota, jotka voi lähettää suoraan laitteelta eteenpäin [11, s. 17].

4.2.8 Etäyhteydet

Erilaiset etäyhteydet ja etätyöpöydät ovat varsinkin yrityskäytössä tärkeitä, mutta niissä on myös potentiaalinen tietovuotoriski. Mikäli niiden käyttöä ei valvota, väärinkäytöksiä voi esiintyä. Sama koskee myös erilaisia VPN-ratkaisuja (Virtual Private Network), jossa asiakasohjelma ottaa salatun VPN-yhteyden organisaation verkkoon. Tietovuotoriski voi syntyä silloin, kun jokin ulkopuolinen taho pääsee käyttäjän tunnuksiin käsiksi tai jos käyttäjä tahallaan käyttää etäyhteyttä tahalliseen tietovuotoon.

Myös etäyhteysohjelmissa saattaa olla tietoturva-aukkoja. Esimerkiksi Microsoftin etätyöpöytäyhteyttä hyödynnettiin Nitro-nimeä käyttäneessä hyökkäyksessä vuonna 2011. [14, s. 24.]

4.2.9 Social Engineering – käyttäjän vastuu

Social Engineering -termillä kuvataan psykologista käyttäjän manipulointia, joka keskittyy nykyaikaisiin viestintävälineisiin. Hyökkääjä pyrkii vaikuttamaan käyttäjään psykolo-

gisia keinoja käyttäen, ja saamaan käyttäjältä haluamiaan tietoja tai pääsyoikeuksia järjestelmiin. Tätä kutsutaan myös tietojen kalasteluksi (engl. ”phishing”). Nykyään tyypillinen huijausyritys on harmittoman näköinen huijaussivustolle johtava linkki, joka leviää sähköpostin tai sosiaalisen median välityksellä. Yleistä on myös luotettavana henkilönä esiintyminen, esimerkiksi ylläpitohenkilönä tai ulkopuolisena konsulttina. Huijaus- ja kalasteluyrityksiä tapahtuu usein myös puhelimitse. Sosiaalisessa mediassa huijausyritykset kasvoivat 123 % vuonna 2012. [10, s. 51.]

Henkilöstön valveutuneisuus on kriittinen osa tietovuotojen ehkäisemisessä. Edistyneet huijaussivustot voivat käyttää jopa varmennettua ja luotettavaa SSL-sertifikaattia, jolloin kokeneempikin käyttäjä voi luulla sivua turvalliseksi. [10, s. 51.] Suomessa asiaa helpottaa toistaiseksi se, että käyttäjämanipulointia tehdään harvoin suomeksi – ja sekin kohtuullisen ontuvasti.

Myös henkilöstön huolimattomuus avaa tietovuotoriskin: mikäli esimerkiksi mobiililaitetta tai tietokonetta käytetään ilman vahvaa salasanaa tai jos nämä jätetään suojaamatta, kun itse ei ole paikalla, voi kuka hyvänsä päästä niissä oleviin tietoihin käsiksi. Lisäksi yhteiskäyttöiset tunnukset järjestelmiin lisäävät tietovuotoriskiä, sillä tällöin ei voida tietää, kuka yksittäinen käyttäjä on kyseessä, jolloin riski väärinkäyttöihin kasvaa.

Edellä esitettyjen tietovuotoriskien lisäksi sähköisen tiedon voi myös muuttaa fyysiseksi tiedoksi. Sähköiset dokumentit voi tulostaa, jolloin on mahdollista kuljettaa salaista tietoa kohtuullisen huomaamatta. Tiedosta voi esimerkiksi myös ottaa valokuvia kameralla. [11, s. 17.] Myös fyysiset dokumentit on suojattava asianmukaisella tavalla tietovuotojen ehkäisemiseksi.

4.3 Tietosuojan mahdollistaminen

4.3.1 Tietoturvakäytännöt

Yrityksen, yhteisön tai viranomaisen on otettava huomioon luvussa 4.2 esitellyt tietovuotoriskit jo senkin takia, että ne ovat haitallisia ja kalliita toiminnalle. Lisäksi luvuissa 2 ja 3 esitetyt asetukset vaativat estämään ulkoiset ja sisäiset tietovuodot sekä tiedon häviämisen henkilörekistereiden käsittelyyn liittyen. Tietovuotojen mahdollisuuksia on tutkittava tarkasti ja mietittävä minkälaiset käytännöt olisivat kokonaisuuden kannalta

järkeviä. Oleellista on määrittää arkaluonteinen tieto, jota ei saa päästää organisaation ulkopuolelle. Esimerkiksi tiukasti suojellussa ympäristössä henkilöt eivät saisi tuoda mitään laitteita työpaikalle ja heidän toimintansa olisi tarkkaan kontrolloitua.

Tietoturvakäytänteisiin on muun muassa sovittava, miten henkilöstö saa käyttää sähköpostia ja Internetiä, ja saako omia ohjelmia asentaa työkoneille. Check Pointin tutkimuksen mukaan erilaiset verkkosovellukset olivat useille organisaatioille tärkeitä toiminnan kannalta, mutta vastaavasti näiden käyttö voi olla tietovuotoriski. [14, s. 36.]

Omien laitteiden tuominen ja kytkeminen organisaation verkkoon on myös päätettävä: tätä varten on suositeltavaa käyttää ainakin erillistä vierailijaverkkoa. Verkkoliikenteen sallimisesta ja valvonnasta on oltava selkeä yksiselitteinen ohjeistus. Pääsyoikeuksien ja tunnusten hallinta on myös suuressa roolissa: käyttäjän pitäisi päästä vain niihin tiedostoihin ja järjestelmiin, jotka ovat edellytyksenä työtehtävien hoitamiseen. Tämä koskee myös etäkäyttöä esimerkiksi VPN-yhteyden avulla. Haittaohjelmien pääsy järjestelmiin on estettävä niin henkilöstön koulutuksella kuin haittaohjelmien torjuntaan tarkoitetuilla ohjelmistoilla. Ylläpitohenkilöstön on oltava valveutuneita käytettävissä olevista ohjelmistoista ja laitteista, ja seurattava niiden tietoturva-aukkoja.

Mahdolliset pilvipalvelut ja muut ulkoiset toimijat tuovat myös haasteita tietoturvaan. Asiakas ei voi olla varma, kuka pääsee näkemään tietoja esimerkiksi ongelmanratkaisutilanteissa. Lisäksi onnistunut hyökkäys palveluntarjoajaa vastaan tarkoittaa usein sitä, että kaikkien asiakkaiden tiedot ovat vaarassa. Pilvipalveluita ja ulkoisia toimijoita käytettäessä on kartoitettava tarkkaan mahdolliset riskit, ja suojattava omat tietonsa mahdollisimman hyvin. [10, s. 39.] Tietosuoja-asetus 2012/0011 velvoittaa EU:n ulkopuoliset palveluntarjoajat noudattamaan asetuksen säädöksiä, mikäli ne tarjoavat palveluitaan EU:n alueella. On mahdollista, että EU:n ulkopuoliset palveluntarjoajat eivät tarjoa enää palveluita EU-alueelle asetuksen voimaantulon jälkeen.

Käytössä olevat tekniset ratkaisut ovat mitoitettava resurssien kannalta siten, että niissä on riittävästi kapasiteettia. Tarpeellisia tietoturvalaitteita ovat ainakin palomuuri, IDS/IPS-laite sekä tietovuotoja estävä ja havaitseva laite, joita käsitellään luvussa 4.4. Organisaation ja verkon koosta riippuen edellä mainitut ratkaisut voivat olla joko samassa laitteessa tai erillisinä. Lisäksi työasemiin ja palvelimiin on tarpeen asentaa paikalliset palomuurit sekä virusten ja haittaohjelmien torjuntaan tarkoitetut ohjelmistot. Myös mobiililaitteille on olemassa erilaisia haittaohjelmien torjuntaan tarkoitettuja rat-

kaisuja. Käytössä olevat tekniset ratkaisut eivät kuitenkaan saa estää tai viivästyttää työntekoa.

Tietoturvakäytänteisiin on suotuisaa määrittää, mitä saa ja mitä ei saa tehdä, jotta väärinkäytöksistä voisi tulla rangaistuksenalaisia ja täten väärinkäyttäjästä korvausvelvollinen. Henkilöstöä on ohjeistettava käytössä olevista tietoturvakäytänteistä, ja koulutettava käytänteissä esitettyjen vaatimusten täyttämisestä. Tietoturvakäytänteisiin on myös määriteltävä ohjeistus siitä, miten toimia tilanteissa, joissa tietovuoto on jo tapahtunut. Tietoturvakäytänteet voi ilmaista tietoturvapolitiikassa tai niistä voi tehdä erillisen ohjeistuksen. Oleellista on, että tietoturvakäytänteet ovat toimivia, jolloin ne eivät haittaa kohtuuttomasti käyttäjien normaalia toimintaa.

4.3.2 Tietosuojavastaava

Euroopan komission ehdotus tietosuoja-asetuksesta 2012/0011 määrittää pakolliseksi tietosuojavastaavan nimittämisen, mikäli tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin, yritys, jossa on vähintään 250 työntekijää tai jos henkilötietojen käsittelytoimet vaativat luonteensa, laajuutensa ja/tai tarkoituksensa vuoksi rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. Tietosuojavastaavan voi halutessaan nimittää myös muutkin kuin edellä luetellut tahot. [2, 35. artikla.]

Tietosuojavastaavan tehtäviin kuuluu seurata ja valvoa asetuksen noudattamista ja toimeenpanoa erityisesti tietosuojaan liittyvissä asioissa. Tietosuojavastaava neuvoo rekisterinpitäjää ja henkilötietojen käsittelijää näiden velvollisuuksista ja henkilötietojen asianmukaisesta käsittelystä. Tietosuojavastaava toimii yhteyspisteenä valvontaviranomaisen kanssa, ja tämän tehtävän on seurata henkilötietojen käsittelyyn osallistuvan henkilöstön osaamista ja koulutusta. [2, 37. artikla.]

Tietosuojavastaavaksi nimitettävällä henkilöllä on oltava riittävä ammattipätevyys ja erityisesti tietosuojalainsäädäntöä ja alan käytänteitä koskeva erityisasiantuntemus. Erityisasiantuntemuksen taso määräytyy henkilötietojen käsittelyn edellyttämän suojan perusteella. Tietosuojavastaava on valittava vähintään kahdeksi vuodeksi kerrallaan; enimmäismäärää ei ole säädetty. Saman henkilön voi nimittää tehtävään uudelleen useamman kerran. Rekisterinpitäjällä tai henkilötietojen käsittelijällä on velvollisuus erottaa tietosuojavastaava, mikäli tämä ei täytä enää tehtävää edellyttäviä vaatimuksia. [2, 35. artikla.]

Käytännössä tietosuojavastaavaksi voidaan nimittää esimerkiksi tietoturvapäällikkö tai muu tietoturvasta vastaava johtava henkilö. Yleensä käytännön tietoturvan toteuttamiseen on syytä varata enemmän resursseja kuin vain yksi henkilö.

4.3.3 Henkilöstön koulutus

Tietosuojan kannalta teknisillä ratkaisuilla pystytään estämään vahinkoja, mutta suurin rooli tietovuodoissa ja tietoturvan toteutumisessa on henkilöstöllä. Oli kyse sitten yrityksestä, yhdistyksestä tai viranomaisesta, henkilöstön tietoturvakoulutus on avainasemassa tietovuotojen ehkäisemisessä.

Koulutuksen pitää olla sellaista, että se on helposti ymmärrettävissä kaikille henkilöille organisaatiossa työtehtävästä riippumatta. Koulutuksen on herätettävä käyttäjät ajattelemaan tietoturvaan liittyviä asioita omissa tehtävissään. Henkilöstöä on ohjeistettava käytössä olevasta ja tulevasta lainsäädännöstä sekä tiedottaa julkishallinnon tietoturvallisuutta ohjeistavista tahoista, kuten Viestintävirastosta ja Tietosuojavaltuutetun toimistosta. [16, s. 14, 30.]

Tietojen käytön mahdollistaminen ja turvaaminen ovat tietoturvallisuuden tärkeimpiä vaatimuksia. Henkilöstön ohjeistuksen lähtökohtana tulee olla tietoisuus siitä, mitä tietoja organisaatiossa täytyy suojata ja miksi. Käyttäjille tulee ohjeistaa kunkin tiedon tai tietoryhmän suojaustarpeista ja mahdollisista salassapitovaatimuksista. [16, s. 17.] Henkilöstöä tulisi ohjeistaa niin järjestelmien ja ohjelmien turvalliseen käyttöön liittyen kuin myös laitteiden fyysiseen turvallisuuteen. Henkilöstöä on ohjeistettava käytössä olevista teknisistä ratkaisuista ja kertoa, miten ne mahdollisesti seuraavat käyttäjän toimia. Oleellista on painottaa, että tekniset ratkaisut ovat mahdollisesti haavoittuvaisia hyökkäyksille ja haittaohjelmille, jolloin käyttäjän toimilla on suuri merkitys vahinkojen estämisessä. [14, s. 37.]

Henkilöstöä on hyvä ohjeistaa myös Social Engineering -termistä ja kertoa, että erilaiset huijaukset ja tietojen kalasteluyritykset ovat arkipäivää niin verkossa kuin puhelimitse toteutettuna. Myös haittaohjelmien riskeistä ja leviämistavoista on tarpeen ohjeistaa käyttäjiä. [10, s. 52.]

Tärkeää on myös kertoa toimintasuunnitelmista, mikäli tietoturvarike tai tietovuoto on tapahtunut kaikista varotoimenpiteistä huolimatta. Lisäksi käyttäjiä voi ohjeistaa toimintatavoista, mikäli nämä itse havaitsevat tietoturvarikkeen tai tietovuodon.

4.4 Tekniset ratkaisut tietovuotojen valvontaan

Jotta teknisillä ratkaisuilla voidaan toteuttaa luvuissa 2 ja 3 esitettyjen asetusten vaatimuksia, niiden täytyy pystyä havaitsemaan arkaluontoinen tieto ja estämään sen luvaton käyttö ja tuhoutuminen. Teknisten ratkaisujen täytyy havaita ja estää sekä sisäiset että ulkoiset tietovuodot.

Tietovuotojen ja tietoturvarikkeiden havainnointiin on tällä hetkellä olemassa kaksi vakiintunutta tekniikkaa; SIEM eli Security Information And Event Management sekä DLP eli Data Loss/Leak Prevention.

SIEM-ratkaisut perustuvat reaaliaikaiseen tietoturvapoikkeamien monitorointiin (SEM, Security Event Management) sekä tietoturvapoikkeamien lokitietojen hallintaan (SIM, Security Information Management). SEM on suunnattu havaitsemaan tietoturvauhat reaaliaikaisesti ja ilmoittamaan niistä ylläpitohenkilöstölle, joka voi tällöin tehdä tarpeelliset toimenpiteet uhan ehkäisemiseksi. SIM on vastaavasti tarkoitettu pidemmällä aikavälillä esiintyneiden tietoturvauhkien tarkkailemiseen, kuten esimerkiksi raportointia ja analysointia varten tai tietoturvan kehittämiseen aikaisempien tapahtumien perusteella. Tämänhetkiset SIEM-ratkaisut hyödyntävät sekä SEM:n että SIM:n ominaisuuksia, joskin näissä käsitteissä saattaa olla eroja eri laitevalmistajien keskuudessa. [17, s. 3.]

SIEM-ratkaisuilla voidaan siis reaaliaikaisesti havaita tietoturvauhkia ja -poikkeamia, mutta näihin reagoiminen jää ylläpitohenkilöstön tehtäväksi. Näin ollen SIEM:n avulla ei pystyttäisi noudattamaan luvuissa 2 ja 3 esitettyjen asetusten vaatimaa henkilörekistereiden tietojen suojaa, sillä SIEM-ratkaisut eivät voi estää tietovuotoja reaaliajassa.

DLP-ratkaisut ovat kehitetty juuri arkaluonteisen tiedon tarkkailuun ja sen levittämisen ja tuhoutumisen estämiseen. Tällä hetkellä markkinoilla olevat DLP-ratkaisut voidaan jakaa verkkoliikennettä tarkkaileviin gateway-ratkaisuihin sekä työasemia valvoviin endpoint-ratkaisuihin. Myös mobiililaitteille on olemassa alustavia ratkaisuja [18]. DLP-

ratkaisujen avulla voidaan tarkkailla esimerkiksi sähköpostia, tiedostonsiirtoa, tiedostopalvelimia sekä työasemiin liitettäviä lisälaitteita. DLP-ratkaisut havaitsevat arkaluontoisen tiedon ennalta määrättyjen sääntöjen perusteella, ja voivat tehdä tiedolle määrättyjä toimenpiteitä – ääritapauksessa estämään tiedon käytön ja siirron kokonaan. [19.]

DLP-ratkaisuilla voidaan estää arkaluontoisen tiedon leviäminen organisaation ulkopuolelle sekä yhtä lailla eri osastoille organisaatiossa. Esimerkiksi henkilöstön tietoja käsittelevältä osastolta voidaan estää kyseisten tietojen leviäminen muille osastoille. DLP-ratkaisujen avulla voidaan käyttäjille tuoda reaaliaikaista tietoa mahdollisen tietovuodon sattuessa, jolloin käyttäjä osaa välttää tekemäänsä toimenpidettä jatkossa. DLP-ratkaisut ilmoittavat havaituista tietovuototapahtumista ylläpidolle reaaliaikaisesti sekä tallentavat lokiin tapahtumia pidemmällä aikavälillä, jolloin DLP-ratkaisut toimivat myös eräänlaisena SIEM-ratkaisuna. [14, s. 35.]

DLP-ratkaisu on teknisistä ratkaisuista todennäköisin vaihtoehto, jolla voitaisiin täyttää luvussa 2 ja 3 esitettyjen asetusten vaatimukset tietovuotojen estämiseen. Tämän selvittämiseksi luvussa 5 on testattu kahden laitevalmistajan DLP-ratkaisuja; Check Pointin gateway-ratkaisua sekä McAfeen endpoint-ratkaisua.

4.5 Valvonnan laillisuus

Tällä hetkellä voimassa olevaa Sähköisen viestinnän tietosuojalakia 516/2004 on sittemmin täydennetty hallituksen esityksellä HE 48/2008 vuonna 2009. Tämän perusteella on muodostettu asetus 125/2009, joka on tällä hetkellä voimassa oleva laki. Asetus antaa yhteisötilaajalle, joka tässä tapauksessa voi olla esimerkiksi Internet-yhteyden tilaava yritys tai organisaatio, oikeuden käsitellä sähköisen viestinnän tunnistetietoja. Tunnistetieto tarkoittaa tässä esimerkiksi sähköpostiviestin tietoja, kuten lähettäjää ja vastaanottajaa, mutta ei itse viestin sisältöä. Yhteisötilaajalla on oikeus käsitellä tunnistetietoja, mikäli tämän tietoverkossa havaitaan väärinkäyttötapauksia. Asetus määrää yhteisötilaajan määrittämään etukäteen, miten tämän tietoverkkoa saa käyttää, millaisiin kohdeosoitteisiin viestintää ei saa harjoittaa ja miten yrityssalaisuuksia saa siirtää tietoverkossa. [20.]

Asetuksen 125/2009 perusteella olisi siis perusteltua valvoa viestinnän tunnistetietoja tietovuotojen ehkäisemiseksi ja estämiseksi, mutta itse viestin sisältöä ei saa manuaa-

lisesti tutkia. Asetuksen 20. artiklassa määritellään, että tietoturvan toteuttamiseksi viestin automaattinen sisällöllinen analyysi on sallittua, joten esimerkiksi viestin sisältöä tarkkailevalle DLP-ratkaisulle ei ole estettä. [20.]

Asetus tulee kuitenkin muuttumaan lähivuosina Liikenne- ja viestintäministeriön valmisteleman tietoyhteiskuntakaaren LVM059:00/2011 toimesta, joka tulee käsittämään uuden Sähköisen viestinnän tietosuojalain [23]. Tällä hetkellä ei ole tarkempaa tietoa, miten tietoyhteiskuntakaari tulee muuttamaan aikaisempaa asetusta, mutta luvussa 2 esitetyn Euroopan komission tietosuoja-asetuksen nojalla henkilötietojen suojaamisen keinot on otettava myös kansallisessa lainsäädännössä huomioon.

4.6 Tietovuodosta ilmoittaminen

Mikäli tietovuoto tapahtuu kaikista varotoimenpiteistä ja teknisistä ratkaisuista huolimatta, EU:n tietosuoja-asetus määrää rekisterinpitäjän ilmoittamaan asiasta sekä valvontaviranomaiselle että rekisteröidyille, joita asia koskee. [2, 31–32. artikla.]

Rekisterinpitäjän on ilmoitettava tietovuodosta valvontaviranomaiselle 24 tunnin sisällä sen huomaamisesta mahdollisuuksien mukaan [2, 31. artikla]. Mikäli rekisterinpitäjä ei tee ilmoitusta tässä ajassa, tämän on tehtävä perusteellinen selvitys asiasta ja tälle voidaan määrätä sakkoa enintään 1 000 000 euroa tai 2 prosenttia yrityksen maailmanlaajuisesta liikevaihdosta [2, 79. artikla]. Valvontaviranomaiselle tehtävään ilmoitukseen täytyy sisältyä vähintään kuvaus tapahtuneesta, keihin rekisteröityihin tapaus vaikuttaa, ilmoitettava tietosuojavastaavan tiedot, kuvattava mitä seurauksia tapahtumasta voi olla sekä esitettävä toimenpiteitä, joilla voidaan lievittää tietovuodon haittavaikutuksia ja joita rekisterinpitäjä on jo toteuttanut. [2, 31. artikla.]

Kun rekisterinpitäjä on ilmoittanut tietovuodosta valvontaviranomaiselle, täytyy myös kaikille asiaa koskeville rekisteröidyille ilmoittaa asiasta ilman aiheetonta viivytystä. Rekisteröidyille ei kuitenkaan tarvitse ilmoittaa, jos rekisterinpitäjä on osoittanut valvontaviranomaiselle noudattaneensa asianmukaisia teknisiä suojatoimenpiteitä tietovuodon sattuessa. Teknisillä suojatoimenpiteillä tarkoitetaan tietojen muuttamista sellaiseen muotoon, etteivät tiedot ole ymmärrettävissä sellaisille tahoille, joilla ei ole lupaa päästä tietoihin. [2, 32. artikla.]

Kaikki mahdolliset henkilötietoja koskevat tietovuodot ja suoritetut toimenpiteet on dokumentoitava, jolloin valvontaviranomainen voi tarkistaa, onko tapauksessa noudatettu asetuksen säännöksiä. [2, 31. artikla.]

5 DLP-ratkaisut

DLP-ratkaisuja tarjoavia laitevalmistajia on tällä hetkellä useita. Tutkimusyritys Gartner listaa vuoden 2013 Magic Quadrant for Content-Aware DLP -raportissaan Symantecin, Websensen, RSA:n, McAfeen, Verdasysin sekä CA Technologiesin alan johtaviksi laitevalmistajiksi (kuva 7). [19.]

Kuva 7. Gartnerin Magic Quadrant for Content-Aware DLP -raportin tulokset tammikuulta 2013 [19].

Muista tunnetuista laitevalmistajista myös Check Point ja Cisco tarjoavat DLP-ratkaisuja [22, 26]. Tässä työssä testataan McAfeen endpoint-ratkaisua sekä Check Pointin gateway-ratkaisua. McAfee on eräs alan johtajista, jolla on suuri valikoima erilaisia tietoturvaratkaisuja. McAfee on menestynyt erityisesti työasematuotteissa, joten tässä työssä testataan työasemia tarkkailevaa McAfeen DLP Endpoint -ohjelmistoa. Check Point on tunnettu pitkäaikaisena johtavana palomuurilaitteiden valmistajana.

Tässä työssä testataan Check Pointin Software Blade -arkkitehtuuriin perustuvaa DLP-ratkaisua. [27, 28.]

Kyseessä ei ole DLP-ratkaisujen vertailu, joten Check Pointin gateway-ratkaisua käsitellään myös yleisesti gateway-tyyppisenä ratkaisuna, ja McAfeen endpoint-ratkaisua käsitellään myös yleisesti endpoint-ratkaisuna. Molemmista ratkaisuista voidaan suurin piirtein olettaa, miten muutkin markkinoilla olevat ratkaisut toimivat.

5.1 Arkaluonteisen tiedon luokittelu

DLP-ratkaisuja käytettäessä on oleellista määrittää ja luokitella, mikä on arkaluonteista tietoa. Tämä voi olla hyvin suuri prosessi, ja se määrittää koko DLP-ympäristön toimivuuden. Ilman oikein luokiteltua tietoa DLP-ratkaisu on käytännössä turha, sillä tällöin ei voida muodostaa oikeanlaisia sääntöjä eikä politiikkaa. Arkaluonteista tietoa voi olla esimerkiksi yrityksen liikesalaisuudet, henkilötiedot, asiakastiedot, maksutiedot sekä tietokannat. Arkaluonteinen tieto voi olla mitä hyvänsä ja missä muodossa tahansa; se voi olla päivittäisessä käytössä, säilöttynä tai jatkuvassa tiedonsiirrossa.

DLP-ratkaisuja testattaessa otettiin huomioon luvuissa 2 ja 3 esitettyjen asetusten vaatimukset henkilörekistereiden tietosuojaan. Tätä varten luotiin kuviteltu henkilörekisteri, johon sisältyi seuraavia tietoja:

- Henkilön nimi, esim. Matti Virtanen
- Henkilötunnus, esim. 100180-1675
- Tunnistenumero rekisterissä (työntekijänumero), esim. 100012
- Katuosoite, esim. Esimerkkikuja 1
- Postinumero, esim. 10101
- Kaupunki, esim. Helsinki
- Puhelinnumero, esim. 0401234567
- IBAN-tilinumero, esim. FI4250001510000023.

Kuvitellun henkilörekisterin tiedot määriteltiin arkaluonteisiksi tiedoiksi. Henkilörekisterin tiedot ovat arkaluonteisia, esiintyivät ne sitten yksinään tai kokonaisena tiedostona.

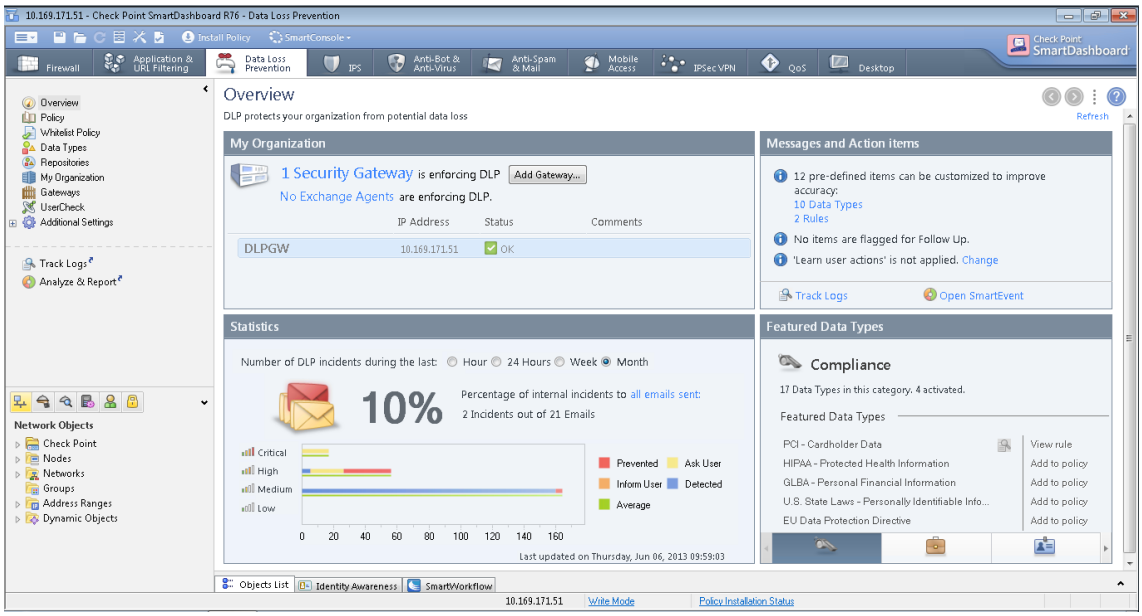
Testirekisteri tallennettiin kolmeen eri tiedostomuotoon; tekstitiedostoksi (.txt), Microsoft Word -dokumentiksi (.docx) sekä PDF-tiedostoksi, jotka määriteltiin suojattaviksi tiedostoiksi.

Arkaluonteista tietoa määritellessä yleisesti ottaen on helpompi tarkastella tietoja, jotka voidaan ilmaista esimerkiksi säännöllisten lausekkeiden avulla. Tällaiset tiedot ovat yleensä tietyn pituisia, ja ne sisältävät kirjain- ja numerosarjoja. Tällainen tieto on helppo analysoida automaattisesti. Esimerkkirekisterissä tällaisia tietoja ovat henkilötunnus, postinumero, puhelinnumero sekä IBAN-tilinumero. Nimen ja osoitteen tunnistamisessa ainoana keinona on verrata niitä olemassa olevaan tietokantaan, joka sisältää samanlaisia tai lähes samanlaisia tietoja. Arkaluonteinen tieto voitaisiin määrittää myös tiedoston ominaisuuksien perusteella, kuten tiedostopäätteen, -nimen tai tiedoston koon mukaan.

Asetusten perusteella tietovuoto on tapahtunut, jos yhdenkin rekisteröidyn henkilötiedot joutuvat väärille tahoille tai tuhoutuvat vahingossa. Tämä asettaa teknisille ratkaisulle tietynlaisen ongelman: ei voida tietää, milloin esimerkiksi omat osoitetiedot lähetetään tarkoituksella ja milloin tietovuoto on aiheellinen. Usein myös yhteystiedot löytyvät esimerkiksi sähköpostin allekirjoituksesta. Ylläpitohenkilöstön on määriteltävä tietyt rajat, joiden mukaan tekniset järjestelmät reagoivat mahdollisiin tietovuotoihin.

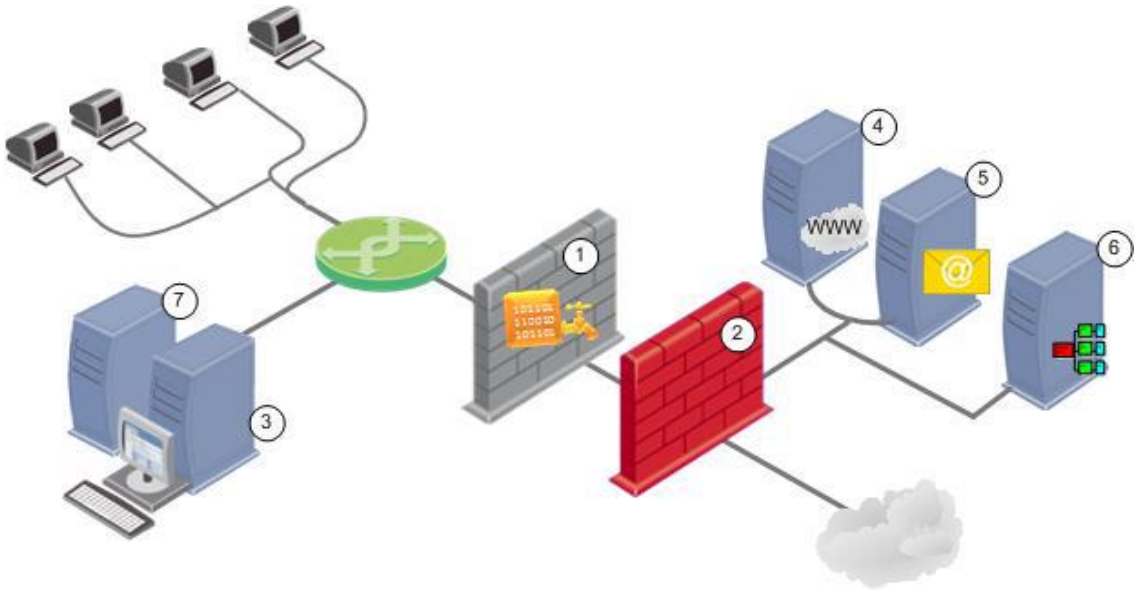
5.2 Check Point DLP Network Gateway

Check Pointin DLP Software Blade -ratkaisu on verkkoliikennettä tarkkaileva järjestelmä, joka estää tai sallii tiedonsiirron ennalta määrättyjen sääntöjen mukaan. Software Blade -arkkitehtuuriin perustuva DLP-ratkaisu voidaan lisätä mihin tahansa Check Pointin Security Gateway -laitteeseen. Laitetta voidaan hallita Check Pointin SmartDashboard -hallintapaneelilla sekä salatun SSH-yhteyden avulla. Samassa laitteessa voi toimia DLP:n lisäksi muitakin palveluita, kuten esimerkiksi palomuuri tai IDS/IPS-ratkaisu. Laitteet voidaan myös kahdentaa klusteriksi vikasietoisuuden lisäämiseksi. [22, s. 10.] Tässä työssä käytetään Security Gateway -laitteelle lisättyä DLP Software Blade -ratkaisua nimityksellä DLP Gateway.



Kuva 8. Check Pointin SmartDashboard-hallintapaneelin DLP-ratkaisun etusivu.

Mikäli samassa laitteessa toimii DLP:n lisäksi muitakin tietoturvapalveluita, laite kannattaa sijoittaa suoraan verkon reunalle toimimaan yhdyskäytävänä muihin verkkoihin. Check Point suosittelee kuvan 9 mukaisesti, että DLP Gateway (1) toimisi itsenäisenä laitteena, jolloin se sijoitettaisiin palomuurin ja muiden tietoturvalaitteiden (2) taakse. [22, s. 10.]



Kuva 9. Check Pointin DLP Gatewayn sijoittaminen verkkoon [22, s. 11].

DLP Gatewayta hallitaan SmartDashboardin ja useampia laitteita käytettäessä keskitetysti myös Check Pointin Security Management Serverin (3) avulla. DLP Gateway voi käyttää Active Directory- tai LDAP-tietokantaa (Lightweight Directory Access Protocol) (6) käyttäjien tunnistamiseen, tai vaihtoehtoisesti käyttäjät voidaan lisätä suoraan laitteen sisäiseen tietokantaan. Kaikki käyttäjälähtöinen liikenne määritellään kulkemaan DLP Gatewayn kautta. DLP Gateway tarkkailee esimerkiksi sisäiselle HTTP-proxylle (4) tai sähköpostipalvelimelle (5) menevän liikenteen ohella myös suoraan muihin verkkoihin lähtevän liikenteen. DLP Gatewayn havaitsemat tapahtumat voidaan tallentaa lokeihin SmartView Trackerille (7) tarkastelua varten. [22, s. 11.]

DLP Gateway voidaan sijoittaa myös yksittäisten työasemaverkkojen tai sisäisten palvelimien eteen. Sijoituspaikka riippuu lähinnä halutusta käyttötarkoituksesta ja käyttäjämääristä. Mikäli käyttäjämäärät ovat korkeita, kannattaa hankkia useampia laitteita ja jaotella laitteiden sijoittelua. [22, s. 11.] Tällöin laitteet kannatta konfiguroida siltaavaan tilaan (”bridge mode”), jolloin ne ovat näkymättömiä verkkotasolla eivätkä osallistu reititykseen. Tämä on myös Check Pointin suosittelema käyttötapa. [22, s. 20.]

5.2.1 Ominaisuudet

DLP Gateway pystyy tarkkailemaan salaamatonta (HTTP) sekä salattua (HTTPS) verkkoliikennettä, salaamatonta tiedonsiirtoa (FTP) sekä salaamatonta sähköpostiliikennettä (SMTP, Simple Mail Transfer Protocol). Kun DLP Gateway havaitsee ennalta määrättyihin sääntöihin osuvaa liikennettä, laite luo uuden tapahtuman (”incident”) ja määrää sääntöjen perusteella sille tehtävät toimenpiteet. [22, s. 13.] DLP Gatewayssa säännölle voi asettaa seuraavat toimenpiteet:

- Detect: Tapahtumasta luodaan loki SmartView Trackeriin, ja liikenne päästetään läpi. Tieto tallennetaan tarkastelua varten. Tämä on suositeltavin toimenpide kun DLP Gateway otetaan käyttöön.
- Inform User: Muutoin sama kuin detect-tila, mutta käyttäjää tiedotetaan tapahtumasta.
- Ask User: Käyttäjältä kysytään varmistus siitä, päästetäänkö kyseinen tieto läpi. Tapahtumasta tehdään loki ja tieto tallennetaan samoin kuin detect-tilassa.
- Prevent: Tiedon läpipääsy estetään. Tapahtumasta luodaan loki ja tieto tallennetaan tarkastelua varten. [22, s. 77.]

Säännöissä verrataan tapahtumaa ennalta määrättyjen tietotyyppien (”data types”) perusteella. Mikäli tapahtuman tieto ja tietotyyppi ovat samoja, tehdään säännöissä asetetut toimenpiteet. Kun tapahtuma on käsitelty, voi DLP Gateway lähettää tiedon tapauksesta ylläpidolle, tiedon omistajalle sekä käyttäjälle, mikäli näin on erikseen määritelty. [22, s. 13.] Lähetettävä tieto on kokonaan muokattavissa, oli kyse sitten näytettävästä Internet-sivusta tai sähköpostista. Sähköpostiherätteitä voi muokata SmartDashboardissa alustavasti tai tarkemmin itse tiedostoja tekstipohjaisen käyttöliittymän (CLI, Command Line Interface) kautta [22, s. 142].

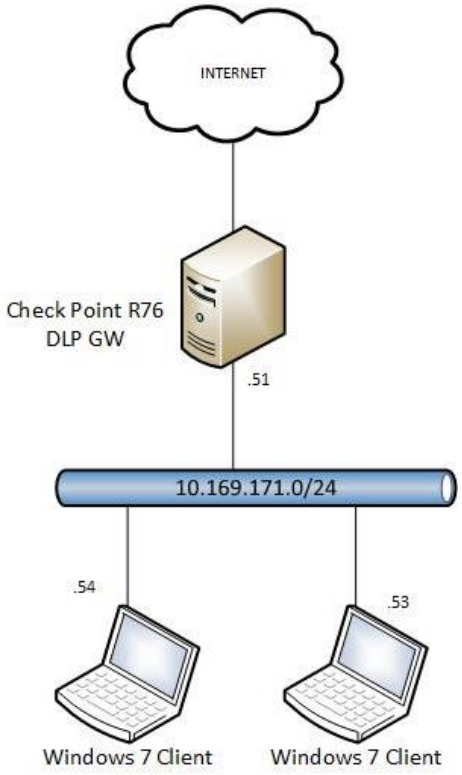
Valmiina olevia tietotyyppejä on useita, ja myös suomalaisista tietotyypeistä ennalta löytyvät esimerkiksi henkilötunnus, Y-tunnus, BAN- ja IBAN-tilinumerot, ALV-tunnus sekä Check Pointin mukaan yleisimpiä henkilöiden nimiä. Tietotyyppejä voi luoda helposti itse, ja ne voivat olla hyvinkin monimutkaisia. Tietotyypit voivat koostua muun muassa yksittäisistä avainsanoista (”keywords”) tai avainsanalistoista (”dictionary”), säännöllisiä lausekkeita (”regular expressions”) sisältävistä malleista, kuvien tai asiakirjojen malleista sekä tiedoston ominaisuuksista, kuten nimestä, koosta tai tyypistä. Monimutkaisempia malleja ja tietotyyppejä voi tehdä itse erillisen Check Pointin laitteissa käytettävän CPcode-skriptikielen avulla. [22, luku 8.].

DLP Gatewayssa on myös ns. whitelist-ominaisuus, jossa määritellyt tiedot päästetään läpi ilman tarkkailua. Aiemmin kuvattujen protokollien tarkkailun ohella DLP Gateway pystyy tarkkailemaan ja merkitsemään myös ulkoisilla tiedostopalvelimilla sijaitsevia tiedostoja. DLP Gateway tukee tiedostopalvelimia, jotka käyttävät NFS (Network File System) tai CIFS (Common Internet Filesystem) -protokollia. [17, s. 105.] Tiedostot voidaan merkitä sormenjäljellä (”fingerprint”) tai vesileimalla (”watermark”), jolloin DLP Gateway havaitsee tiedoston, mikäli sitä yritetään siirtää tämän ohi. Sormenjäljellä voi merkitä kaikkia tiedostoja, vesileima on käytössä vain Microsoft Officen docx-, pptx- ja xlsx-tiedostotyypeillä. [22, s. 106, 123.]

Check Pointin DLP-ratkaisuun kuuluu myös työasemiin asennettava User Check -ohjelma, joka kommunikoi DLP Gatewayn kanssa. User Checkin kautta käyttäjälle välitetään tietoa, mikäli DLP Gateway on havainnut käyttäjää koskevan tietovuodon. Käyttäjä voi ohjelman kautta kuitata tiedon lähettämisen, mikäli kyseinen sääntö on asetettu Ask User -tilaan. Ilman User Checkia DLP Gateway lähettää tietoa käyttäjälle sen protokollan kautta, jossa tietovuoto on havaittu.

5.2.2 Testiympäristö

Testiympäristö koostui kahdesta Windows 7 -käyttöjärjestelmää käyttävästä työasemasta sekä DLP Gatewaysta. Työasemien liikenne määriteltiin kulkemaan DLP Gatewayn kautta. DLP:n lisäksi käytössä oli palomuuri, joka salli kaiken liikenteen kaikkialle eikä näin vaikuttanut verkon toimintaan. Kuvassa 10 on esillä tämän testiympäristön topologia.

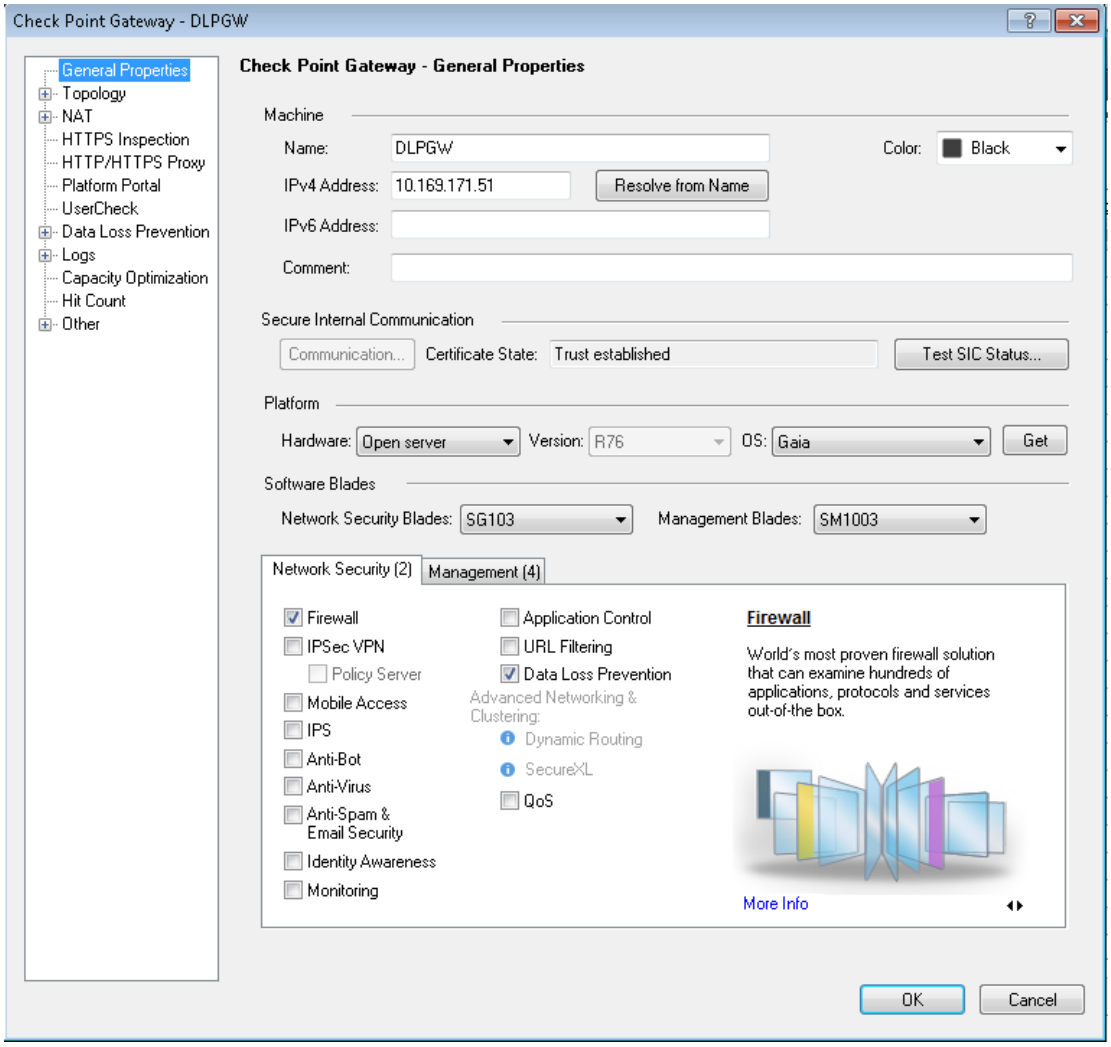


Kuva 10. Check Point -testiympäristön topologia.

Tarkoituksena oli selvittää, miten DLP Gatewayn avulla pystytään estämään luvussa 4.2 käsiteltyjä tietovuotoriskejä laitteen ominaisuuksien mukaan. Pääpaino oli tutkia laitteen perustoiminnallisuutta sekä erilaisten tietotyyppien ja sääntöjen käyttöä ja luomista.

Perusasetuksista laite määriteltiin käyttämään ilmaista Googlen nimipalvelinta sekä Gmail-sähköpostia herätteiden lähettämistä varten. Lisäksi laitteelle pitää asettaa sisäinen organisaatio, jonka perusteella laite määrittää, mikä tiedonsiirto on sisäverkoista

ulospäin. Organisaatioon voidaan määritellä verkkotunnuksia, verkkoja, käyttäjiä sekä VPN-liikennettä. Oletuksena laite määrittää kaikki sisäiset verkot, käyttäjät sekä VPN-liikenteen organisaatioon. Organisaation avulla voidaan määritellä tarkemmin, mitä kaikkea DLP Gatewayn halutaan tarkkailevan. Muutoin laite on valmis käyttöön sellaisenaan. DLP Gatewayna käytettiin virtualisoitua Open server Gaia R76-versiota (kuva 11). DLP Gateway sekä työasemat virtualisoitiin VMwaren avulla.

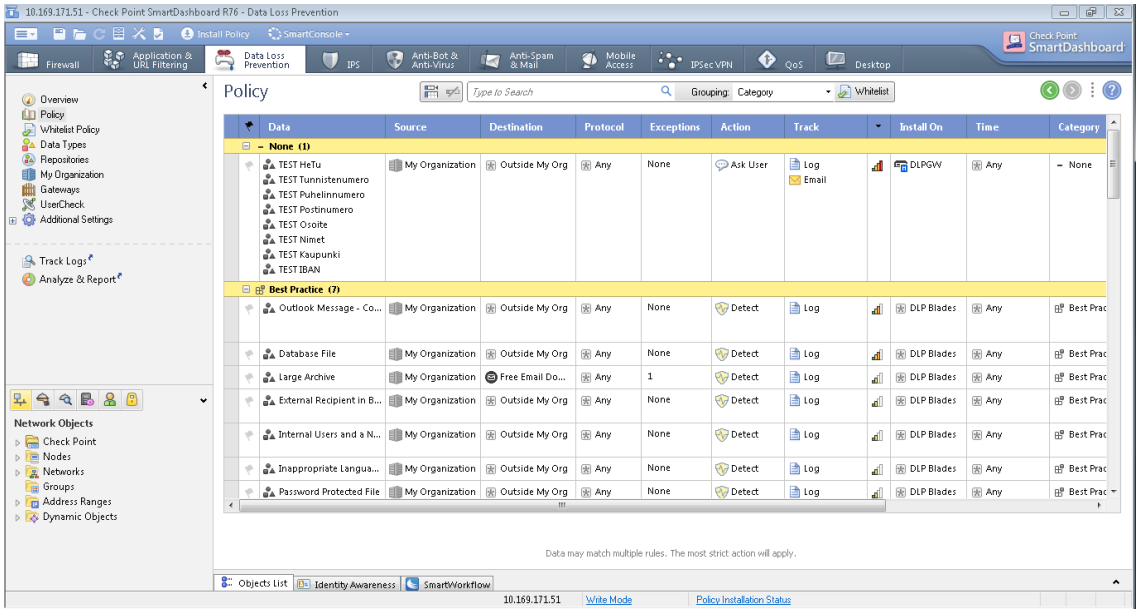


Kuva 11. DLP Gatewayn laitetiedot.

Toimintaa testattiin aluksi yksinkertaisen avainsanan sisältävällä säännöllä, jotta saatiin varmuus toiminnasta eri protokollilla. Tämän jälkeen luotiin tarvittavat tietotyypit ja säännöt, jotka kattavat luvussa 5.1 esitellyn kuvitellun henkilörekisterin. Liitteessä 1 on kerrottu tarkemmin tietotyyppien luomisesta.

Tietotyyppeihin laitettiin osumarajaksi (”threshold”) 2. Tällöin DLP Gateway ei reagoi esimerkiksi sähköpostin allekirjoituksiin, sillä tietotyypin määrittelemän tiedon pitää esiintyä vähintään kaksi kertaa. Tietotyypeistä luotiin yksinkertainen sääntö, joka tarkkailee kaikkea ulospäin suuntautuvaa liikennettä DLP Gatewaylla. Tietotyypeistä voidaan koota myös erillinen tietotyyppiryhmä, jota voidaan käyttää säännöissä yksittäisten tietotyyppien sijaan.

Kuvassa 12 on esillä DLP Gatewayn sääntönäkymä, jossa ylimpänä on tässä testauksessa käytetty sääntö. Oletuksena DLP Gatewayssa on käytössä useita yleismaailmallisia sääntöjä, jotka reagoivat esimerkiksi tietokantatiedostoihin sekä taulukkolaskentaohjelmien tiedostoihin.

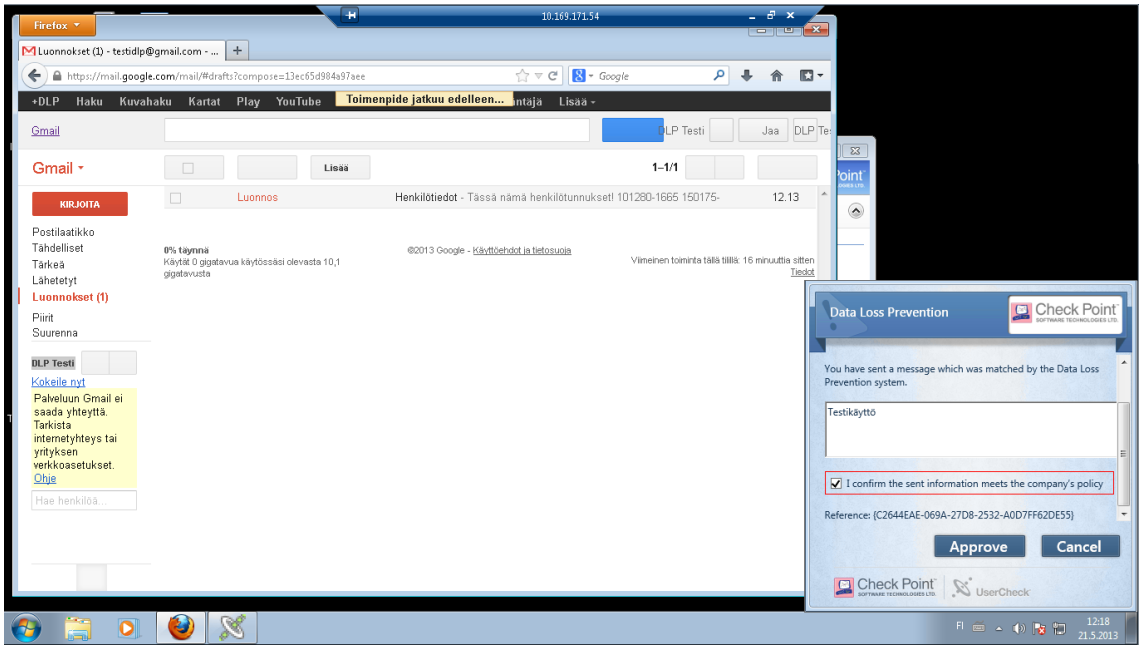


Kuva 12. DLP Gatewayn sääntönäkymä.

5.2.3 Testin tulokset

DLP Gateway havaitsee arkaluontoisen tiedon määrätyn laisesti. Laitteella on kattava loki, josta laitteen havaitsemat tapahtumat käyvät yksityiskohtaisesti ilmi. Laite voi myös reaaliaikaisesti ilmoittaa ylläpidolle, tiedon omistajalle sekä käyttäjälle havaitusta tietovuodosta. DLP Gatewaylla on kattava debug-toiminnallisuus vianetsimisen helpottamiseksi.

Ongelmaksi muodostuvat kuitenkin salatut protokollat. HTTPS-tarkkailu toimii riittävän hyvin ilman ongelmia, mutta esimerkiksi SSL/TLS-salausta käyttävää sähköpostia tai FTPS-/SCP-tiedonsiirtomenetelmiä ei pystytä tarkkailemaan. Lisäksi DLP Gateway ei kommunikoinut toimivasti työaseman kanssa ilman User Check -ohjelmistoa. User Check on siis asennettava työasemiin, jotta käyttäjälle välittyy viesti tietovuodosta. Kuvassa 13 User Check pyytää käyttäjältä lupaa viestin lähettämiseen Googlen Gmail-palvelussa.



Kuva 13. User Check -ohjelmisto pyytää käyttäjältä lupaa Gmail-viestin lähettämiseen.

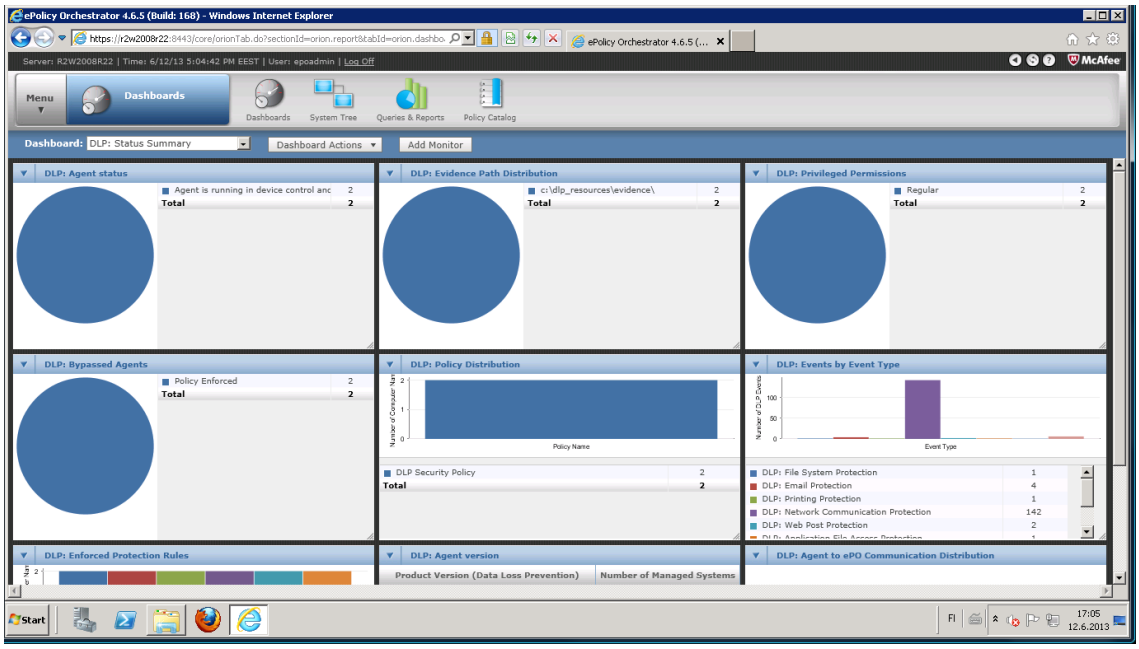
Tarkempi kuvaus DLP Gatewayn havaituista toiminnoista on esillä liitteessä 2.

Testin perusteella voidaan sanoa, että DLP Gateway soveltuu verkkoliikennettä tarkkailevaksi DLP-ratkaisuksi, koskien verkkoliikennettä, salaamatonta tiedonsiirtoa sekä salaamatonta sähköpostiliikennettä. Sillä voidaan estää luvussa 4.2 esitettyjä tietovuotoriskejä laitteen ominaisuuksien mukaisesti.

Eräs ratkaisu salattujen protokollien tarkkailemisesta aiheutuneeseen ongelmaan voisi olla erilaisten sisäverkossa sijaitsevien välityspalvelimien käyttö. Työasemat käyttäisivät välityspalvelimia päästäkseen ulkoisiin verkkoihin, jolloin työasemien ja välityspalvelimien välinen liikenne voisi olla salaamatonta. Tällöin DLP Gateway voisi tutkia välityspalvelimille menevän ja tulevan liikenteen. Tämä edellyttää, että sisäverkko olisi muutoin turvallinen, eikä ulkopuolisilla tahoilla olisi pääsyä verkkoon.

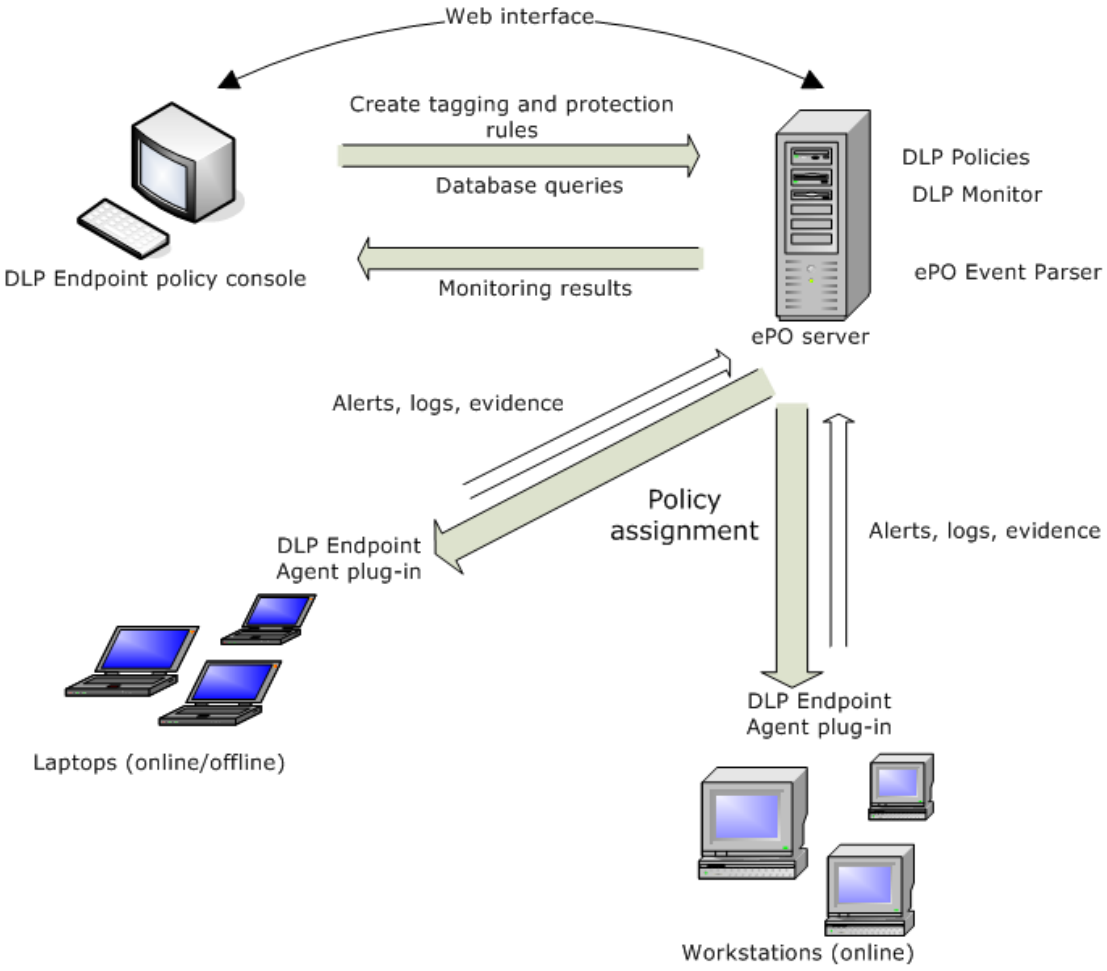
5.3 McAfee DLP Endpoint

McAfeen DLP Endpoint on työasemia ja palvelimia valvova ohjelmistokokonaisuus, joka voidaan asentaa osaksi tietoturvaratkaisuja keskitettyyn McAfeen ePolicy Orchestrator (ePO) -hallintaohjelmistoon (kuva 14). Internet-selaimella käytettävä ePO-hallintaohjelmisto on asennettava erilliselle palvelimelle. Tässä työssä käytetään tällaista palvelinta nimityksellä ePO-palvelin. McAfeen DLP Endpoint on saatavilla kahdella eri lisenssillä; toinen on suppeampi Device Control -lisenssi, joka tarkkailee lähinnä työasemiin liitettäviä ulkoisia laitteita, ja toinen on täysin lisensoitu DLP Endpoint. Device Control on oletuksena päällä uudessa asennuksessa, ja täysin lisensoituun versioon kuuluu myös Device Control. [23, s. 7.] Tässä työssä on käytetty täysin lisensoitua DLP Endpoint -ohjelmistoa.



Kuva 14. McAfee ePO:n DLP Dashboard. Näkyvillä olevat tilastot ovat vapaasti muokattavissa.

Kuvassa 15 on havainnollistettu McAfee DLP Endpointin toimintaa. Ylläpito suorittaa hallinnollisia toimenpiteitä ePO-palvelimelle, kuten esimerkiksi sääntöjen ja politiikan käyttöönottoja sekä tarkkailevat ePO-palvelimen havaitsemia tapahtumia ja lokitietoja. Työasemat kommunikoivat ePO-palvelimen kanssa McAfee Agentin välityksellä, joka on työasemiin asennettava ohjelmisto. McAfee Agentit saavat säännöt ja politiikan tietoonsa ePO-palvelimelta. Vastaavasti McAfee Agentit lähettävät ePO-palvelimelle tietoa työaseman tapahtumista.



Kuva 15. McAfee DLP Endpointin toimintakaavio [23, s. 13].

McAfee Agentit tarkastavat käytössä olevat säännöt ja politiikan paikallisesti työasemalla, jolloin toiminta tietovuodon sattuessa on viiveetöntä. Oletuksena Agentti ja ePO-palvelin kommunikoivat keskenään tunnin välein, jolloin ePO-palvelin lähettää Agentille politiikan ja vastaavasti Agentti lähettää ePO-palvelimelle mahdolliset lokitiedot ja tapahtumat.

5.3.1 Ominaisuudet

McAfeen DLP Endpoint tarkkailee työasemien tapahtumia ja määrittää tietovuototapahtumat ennalta asetetun politiikan mukaan. Politiikka muodostuu erilaisista säännöistä. Sääntöjä on karkeasti jaoteltuna kahdenlaisia; Classification- ja Tagging-säännöt luokittelevat, mikä on arkaluonteista tietoa.

- Classification Rules – Vertaa havaittua sisältöä ennalta määrättyihin avainsanoihin (”keywords”), avainsanalistoihin (”dictionary”), säännöllisiin lausekkeisiin tai tiedoston ominaisuuksiin. Näiden sääntöjen tuotoksena on erillisiä sisältöä merkitseviä kategorioita (”Content Categories”), joita voidaan käyttää Protection- ja Discovery-säännöissä.

- Tagging Rules – Tiedostoja voidaan merkitä (”tag”) joko käsin tai automaattisella järjestelmäskannauksella. Tiedostoja merkitään joko tietyn ohjelman (”Application Specific”) tai sijainnin (”Location Specific”) perusteella mikäli se sisältää määriteltyjä avainsanoja, avainsanalistoja tai säännöllisiä lausekkeita. Merkittyjä tiedostoja voidaan käyttää Protection- ja Discovery-säännöissä. [23, s. 11.]

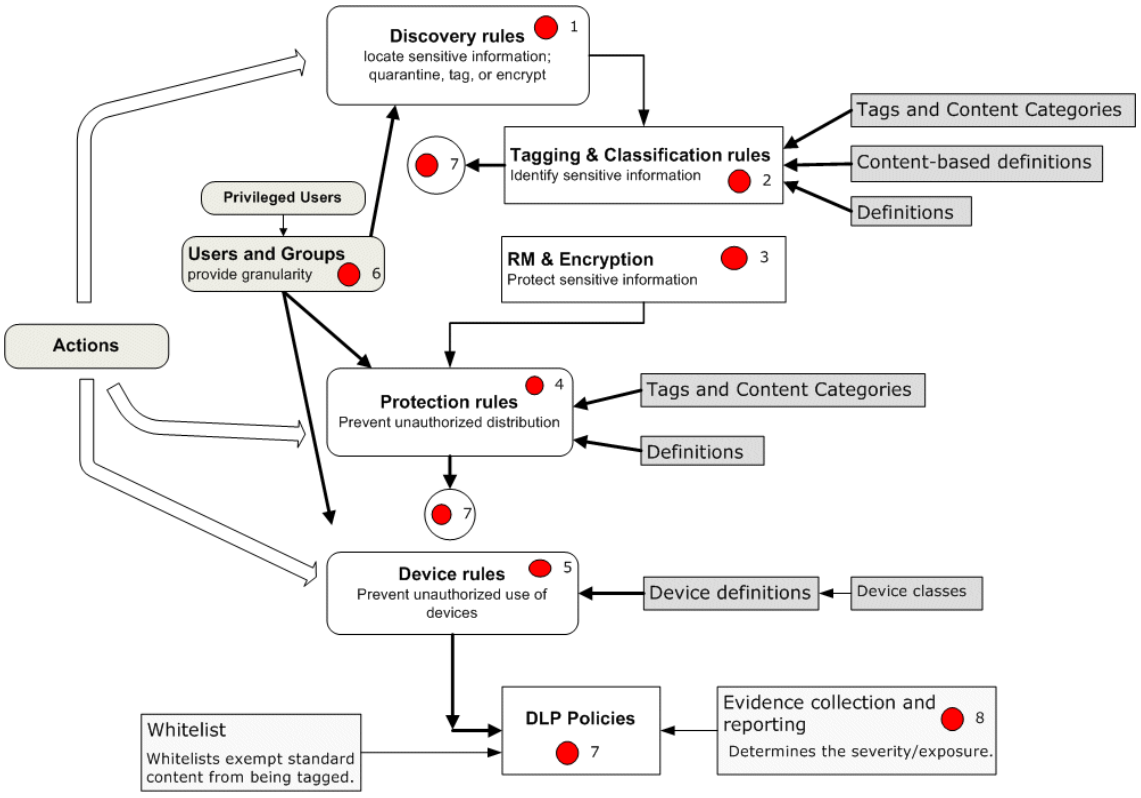
Varsinaiset toimenpiteet tehdään arkaluontoisen tiedon perusteella seuraavissa säännöissä:

- Protection Rules – Tagging- ja Content Classification -sääntöjen merkitsemän sisällön varsinaiset toimenpiteet määritellään Protection-säännöissä. Mahdollisia toimenpiteitä ovat tiedon esto (”Block”), tiedon tarkkailu (”Monitor”), käyttäjälle tiedottaminen (”Notify user”), selvityksen vaatiminen käyttäjältä (”Request justification”), tietovuodon aiheuttaneen tiedon tallennus (”Store evidence”) sekä tiedon salaus (”Encrypt”). Mahdolliset käytettävät toimenpiteet riippuvat sääntötyypistä.

- Device Rules – Ulkoisten laitteiden (esimerkiksi USB-, Bluetooth- ja Wi-Fi -laitteet) valvontaan liittyvät säännöt.

- Discovery Rules – McAfeen DLP Discover crawler voi skannata työaseman tai tiedostopalvelimen mahdollisten arkaluontoisten tietojen varalta, ja tehdä näille vaadittavia toimenpiteitä, kuten esimerkiksi tiedoston merkitsemisen (”tag”) tai karanteeniin sijoittamisen (”quarantine”). [23, s. 11.]

Sääntöjä voidaan jaotella eri käyttäjille ja käyttäjäryhmille (”User Assignment Groups”). Käyttäjiksi voidaan määritellä paikalliset käyttäjät (”local users”) tai käyttäjät ulkoisesta tietokannasta LDAP-protokollan avulla. Sääntöjä voidaan ohittaa ns. whitelist -ominaisuuden avulla, jossa määritellyt tiedostot, sisällöt ja ulkoiset laitteet eivät aiheuta toimenpiteitä. [23, s. 11–12.] Kuvassa 16 on havainnollistettu eri sääntöjen toiminnan kulkua.



Kuva 16. McAfee DLP Endpointin sääntöjen toimintakaavio [23, s. 10].

Käytössä olevia politiikkoja voi määrittää useampia, ja niitä voi jaotella eri työasemille. Politiikka asennetaan aina tiettyyn työasemaryhmään (”Computer Assignment Group”). Työasemaryhmä kumoaa käytössä olevat mahdolliset käyttäjäryhmäkohtaiset säännöt, joten kyseisiä työasemia käyttävät käyttäjät noudattavat työasemaryhmän sääntöjä. Jos kuitenkin käyttäjäryhmäkohtaisissa säännöissä on sääntöjä, joita ei löydy työasemaryhmän säännöistä, käyttäjäryhmäkohtaiset säännöt säilyvät näiltä osin. [23, s. 85–86.]

Classification- ja Tagging-sääntöjen avulla voidaan siis määrittää, mikä on arkaluontoista tietoa, ja näitä voidaan hyödyntää Protection- ja Discovery-säännöissä. Erilaisia Protection-sääntöjä on yhteensä 10:

- Application File Access Protection Rule – Tarkkailee ja rajoittaa tiedostojen käyttöä tiettyjen ohjelmien tai tiedoston ominaisuuksien perusteella.
- Clipboard Protection Rule – Tarkkailee ja rajoittaa leikepöydän käyttöä.
- Email Protection Rule – Tarkkailee ja estää sähköpostitse lähetettyä tietoa.

- File System Protection Rule – Suojaa tiedostoja tiedostopalvelimilla tai massamuistilaitteilla. Tiedostojen käyttöä ei voi estää, mutta käyttäjää voidaan tiedottaa tapahtumasta.
- Network Communication Protection Rule – Tarkkailee ja rajoittaa sisään- ja ulospäin kulkevaa verkkoliikennettä.
- PDF/Image Writer Protection Rule – Rajoittaa ohjelmallisten PDF- ja kuvatulostimien toimintaa.
- Printing Protection Rule – Tarkkailee ja rajoittaa tiedostojen tulostamista fyysisellä tulostimella.
- Removable Storage Protection Rule – Tarkkailee ja rajoittaa ulkoisille tallennusvälineille tallennettavaa tietoa.
- Screen Capture Protection Rule – Estää kuvaruutukaappauksien ottamisen havaitun sisällön perusteella.
- Web Post Protection Rule – Tarkkailee ja rajoittaa verkkosivuille lähetettävää tietoa. Toimii Internet Explorer 6 ja sitä uudemmilla selaimilla sekä Firefox 3.6, 4.0 ja 5.0 -selaimilla. Toimii verkkosivuilla, jotka käyttävät AJAX- tai Flash-teknologiaa. Product Guiden mukaan näihin kuuluvat Microsoft Outlook Web Access, Gmail, Google Docs, Yahoo sekä Hotmail. [23, s. 91–100.]

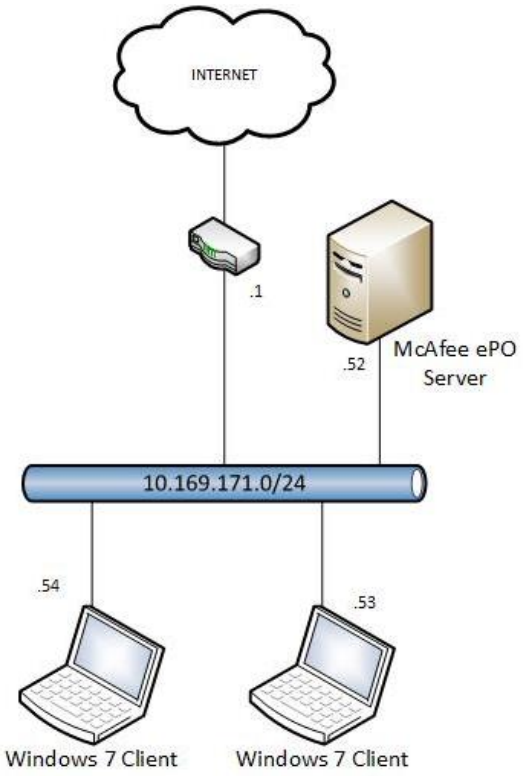
Discovery-sääntöjen avulla voidaan paikallistaa työasemilla sijaitsevat arkaluonteiset tiedot. McAfee DLP Discover crawler voi skannata järjestelmän joko erityisesti sähköpostitiedostoja etsien (”Email Storage Discovery Rule”) tai yleisesti levyjärjestelmää koskien (”File System Discovery Rule”). Järjestelmäskannauksessa voidaan etsiä arkaluontoista tietoa joko merkittyjen tiedostojen (”tags”), sisällön (”content categories”) tai tiedoston ominaisuuksien (”document properties”) mukaan. [23, s. 60–62.]

Työasemaan liitettäviä ulkoisia laitteita voidaan hallita ja valvoa erillisten Device-sääntöjen avulla. Yleisesti käytössä olevia ulkoisia laitteita ovat muun muassa älypuhelimet, muistitikut ja -kortit sekä erilaiset musiikki- ja videotoistimet. DLP Endpoint tunnistaa oletuksena yleisimmät Plug and Play -laitteet. Muutoin laitteita voi yksilöidä ja luokitella erilaisten parametrien avulla, kuten laitteen sarjanumerolla tai valmistajan koodilla. Sääntötyypit on jaoteltu Plug and Play -laitteisiin (”Plug and Play Device Rule”), ulkoisiin tallennusvälineisiin (”Removable Storage Device Rule”) sekä ulkoisissa tallennusvälineissä olevien tiedostojen käyttöä valvoviin sääntöihin (”Removable Storage File Access Device Rule”). Plug and Play -sääntöjen sekä ulkoisia tallennusvälineitä koskevien sääntöjen toiminto voi olla laitteen esto (”Block”) tai tarkkailu (”Monitor”) ja käyttäjää voidaan tiedottaa tietovuototapahtumasta. Ulkoisissa tallennusvälineissä ole-

vien tiedostojen käyttöä valvovat säännöt asettavat kyseiset tiedostot lukutilaan (”read only”), jolloin tiedostoihin ei voi tallentaa mitään eikä niitä voi poistaa. Oletuksena DLP Endpoint estää yleisimpiä suoritettavia ohjelmia. DLP Endpoint havaitsee myös pakattujen tiedostojen sisällä olevia suoritettavia ohjelmia. [23, s. 17–25.]

5.3.2 Testiympäristö

Testiympäristö koostui ePO-palvelimesta sekä kahdesta työasemasta. ePO-hallintaohjelmisto asennettiin Windows Server 2008 R2 -käyttöjärjestelmää käyttävään palvelimeen. Tietokantana toimi Microsoft SQL 2005. EPO:n versio oli 4.6.5.168 ja DLP-lisäosan 9.2.200.23. Työasemat käyttivät Windows 7 -käyttöjärjestelmää. Virtualisointialustana toimi VMware. Kuvassa 17 on esillä testiympäristön topologia.



Kuva 17. McAfee-testiympäristön topologia.

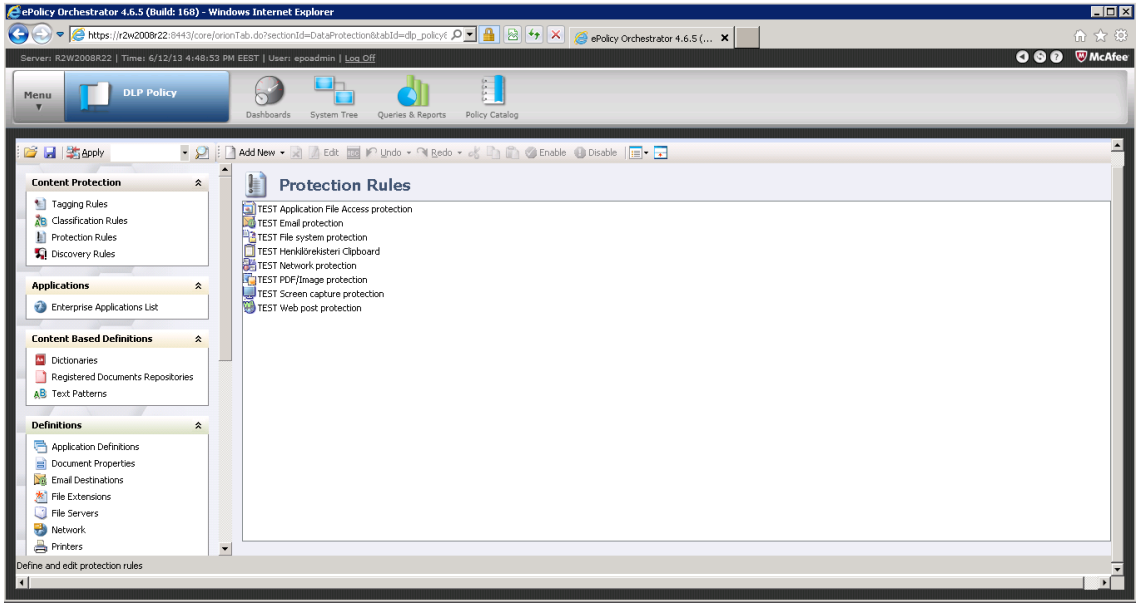
Työasemissa käytetyn McAfee Agentin versio oli 4.6.0.1694 ja DLP Monitorin 9.2.200.60.

Tarkoituksena oli selvittää, miten McAfeen DLP Endpoint -ratkaisu soveltuu luvussa 4.2 esiteltyihin tietovuotoriskien estämiseen. Virtualisoinnin takia ulkoisia laitteita koskevat

Device-säännöt jäivät testaamatta tässä toteutuksessa. Samaisesta syystä myös Protection-sääntöjen alla olevaa ulkoisia tallennusvälineitä koskevaa sääntöä (”Removable Storage Protection Rule”) ja fyysisiä tulostimia koskevaa sääntöä (”Printing Protection Rule”) ei testattu.

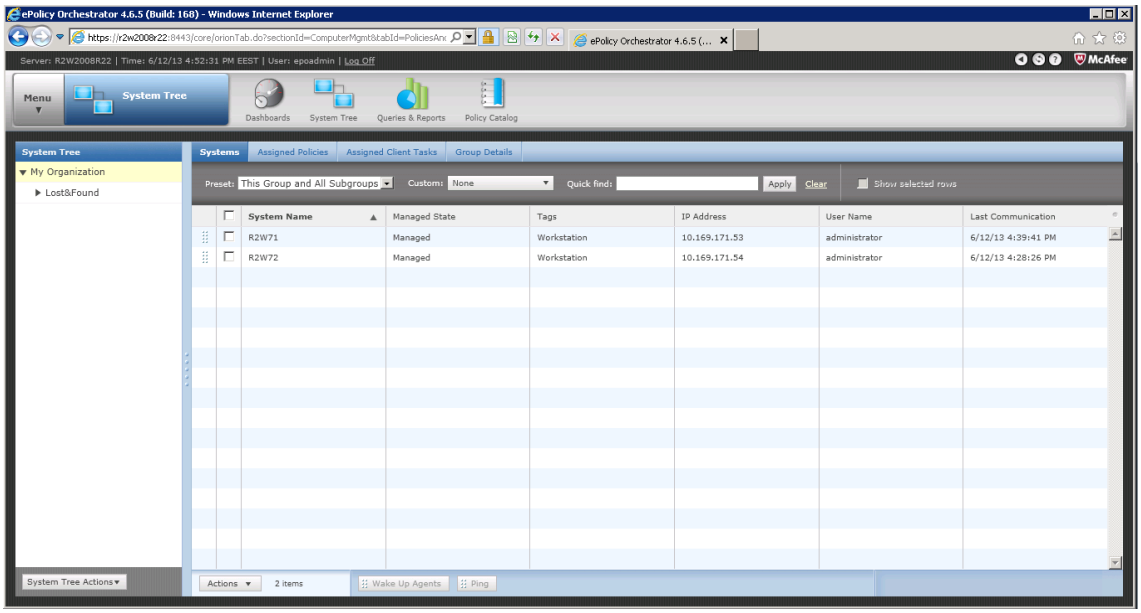
Toimintaa testattiin aluksi yksinkertaisen avainsanan sisältävillä Tagging- ja Content Classification -säännöillä, joiden perusteella voitiin luoda erilaisia Protection-sääntöjä. Kaikki mahdolliset Protection-säännöt saatiin toimimaan moitteetta tässä ympäristössä. Myös DLP Endpoint Discovery crawler toimi ongelmitta. Tämän jälkeen luotiin tarvittavat avainsanalistat ja säännölliset lausekkeet liitteen 4 mukaisesti.

Avainsanalistoista ja säännöllisistä lausekkeista muodostettiin Tagging- ja Content Classification -säännöt, joiden perusteella arkaluontoinen tieto voidaan määrittää Protection-säännöissä. Tämän jälkeen niistä muodostettiin kaikki mahdolliset Protection-säännöt kuvan 18 mukaisesti.



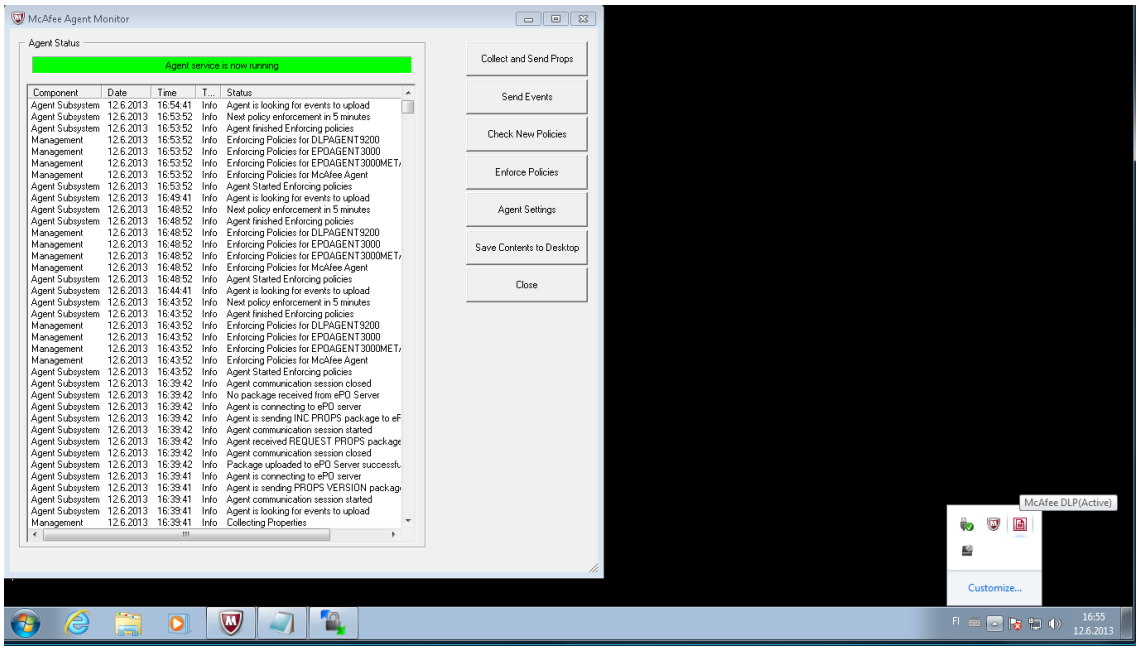
Kuva 18. Testissä käytetyt DLP Endpointin Protection-säännöt.

EPO-palvelimeen liitettyjä työasemia hallitaan ePO:ssa System Tree -sivulla (kuva 19). Sivulla voi esimerkiksi lisätä uusia työasemia, asentaa McAfee Agent ja muut tarvittavat palvelut työasemiin, muuttaa Agentin konfigurointia ja asettaa työasemille noudatettava politiikka sekä kerätä työasemien viimeisimmät tapahtumat ja lähettää politiikka Wake Up Agents -toiminnon avulla.



Kuva 19. EPO-palvelimen System Tree -sivu.

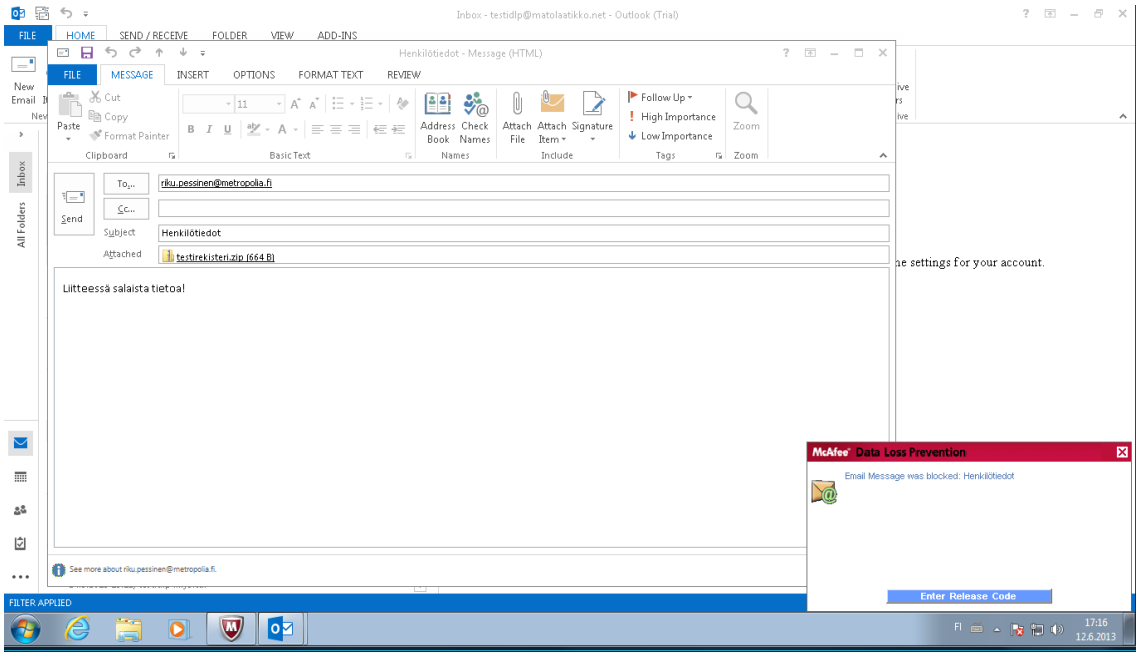
Myös työasemalla käyttäjä voi McAfee Agentin kautta lähettää ePO-palvelimelle mahdollisia tapahtumia ja pyytää uutta politiikkaa (kuva 20).



Kuva 20. Työasemalle asennettava McAfee Agent. Tehtäväpalkissa näkyy myös DLP-ohjelmisto.

5.3.3 Testin tulokset

Testattu McAfeen DLP Endpoint soveltuu työasemalla paikallisesti tapahtuvien tapahtumien havainnointiin. Se pystyy tarkkailemaan itse työaseman paikallisten tiedostojen lisäksi onnistuneesti muun muassa salattua sähköpostiliikennettä, leikepöydän käyttöä ja kuvaruutukaappauksien ottamista. Myös arkaluonteista tietoa etsivä DLP Endpoint Discovery crawler löysi ja merkitsi työasemalla olleet arkaluonteiset tiedostot. Vaikka ulkoisten laitteiden käyttöä koskevia sääntöjä ei pystytty testissä testaamaan, ei ole mitään epäilystä olettaa, etteivätkö nekin toimisi riittävän hyvin.



Kuva 21. McAfee Agent ilmoittaa käyttäjän tietovuotorikkeestä oikeaan alakulmaan avautuvalla ikkunalla.

Ongelmana endpoint-tyylisessä ratkaisussa on se, että sillä ei ole universaalia tukea eri protokollille, vaan eri ohjelmistoille erikseen. Esimerkiksi McAfeen DLP Endpoint tukee sähköpostiohjelmista vain Microsoft Outlookia ja Lotus Notesia. Tällöin organisaatiossa joutuu käyttämään tiettyjä ohjelmistoja täydellisen suojan saamiseksi. Testattu McAfeen DLP Endpoint ei myöskään pystytyt riittävällä tasolla tarkkailemaan työaseman verkkoliikennettä; esimerkiksi tiedonsiirto jäi täysin huomioimatta. Myös Internet-selaimia tarkkailevan säännön pitäisi kattaa kaiken salaamattoman sekä salatun liikenteen, jotta se olisi käyttökelpoinen.

DLP Endpontissa on kattava loki sen havaitsemista tapahtumista. Lisäksi ePO:n DLP Dashboardin etusivulta näkee hyvin viimeaikaiset tapahtumat. EPO:ssa on myös tuki sähköpostiherätteiden lähettämiseen, mutta tämä ei ainakaan testiympäristössä toiminut. Vianselvitystä varten sekä ePO-palvelimelta että työasemalla olevasta McAfee Agentista löytyy prosessien lokitiedostot sekä debug-ominaisuudet.

Tarkempi kuvaus DLP Endpointin havaituista toiminnoista on esillä liitteessä 6. Testissä havaittiin myös DLP Endpointin käyttöönottoon liittyen liitteessä 4 mainitut asiat.

Testin perusteella voidaan sanoa, että DLP Endpoint soveltuu työasemalla paikallisesti tapahtuvien tapahtumien havainnointiin. Se pystyy estämään luvussa 4.2 esitettyjä tietovuotoriskejä toimivasti. Verkkoliikenteen tarkkailemiseen se ei ole riittävän soveltuva, sillä se ei voi tarkkailla Internet-selaimen liikennettä tai tiedonsiirtoa riittävän hyvin.

Endpoint-ratkaisu voisi mahdollistaa myös salattuja verkkoprotokollia käyttävien ohjelmien tarkkailun, kuten esimerkiksi salattujen tiedonsiirtomenetelmien ja pikaviestimien tarkkailun. Tämä kuitenkin edellyttäisi joko valmistajan suoraa tukea kyseisille ohjelmille, tai mahdollisuuden käyttäjälle muokata ohjelmien ja protokollien tarkkailua.

6 DLP toteutettavana palveluna

6.1 DLP:n soveltuvuus tietoturvavaatimuksiin

DLP-ratkaisut soveltuvat toteuttamaan luvussa 2 esitetyn tietosuoja-asetuksen 2012/0011 tietoturvavaatimuksia. DLP-ratkaisu pystyy estämään henkilötietojen vahingossa tapahtuvaa tai laitonta tuhoamista sekä häviämistä, oli kyse sitten yksittäisellä työasemalla tai tiedostopalvelimella olevasta tiedosta. Tieto voidaan myös salata endpoint-ratkaisulla, jolloin sen luvaton tiedonsaanti on estettävissä [23, s. 14]. Tietoa voi hävitä myös tiedonsiirrossa, johon DLP-ratkaisu ei voi vaikuttaa.

Henkilötietojen luvatonta käsittelyä voidaan estää endpoint-ratkaisun käyttäjäoikeusvalvonnalla, joka määrittää, keillä on pääsy haluttuihin tiedostoihin [23, s. 53]. Tietojen luvatonta käsittelyä voidaan estää myös verkkotasolla gateway-ratkaisulla, jolloin määritetään, mihin kohdeosoitteisiin yksittäisen käyttäjän tai verkon on sallittua päästä. Luvattomaan käsittelyyn sisältyvät asetuksessa määrätyt luvaton muuttaminen ja tiedon-

saanti sekä lainvastainen käsittely niiltä osin, kuin se teknisillä ratkaisuilla on mahdollista.

Henkilötietojen luvatonta luovutusta ja levittämistä voidaan estää sekä gateway- että endpoint-ratkaisuilla. Gateway-ratkaisulla voidaan estää verkon yli tapahtuvaa levittämistä. Endpoint-ratkaisulla voidaan estää muun muassa tiedon kopiointia, tulostamista sekä ulkoisiin laitteisiin siirtämistä.

Valtioneuvoston tietoturva-asetus 681/2010 vaatii, että salassa pidettävän tiedon luvaton muuttaminen sekä käsittely estetään ja että tietoihin pääsevät käsiksi vain niitä tarvitsevat henkilöt. Myös tietoturva-asetus 681/2010 edellyttää tietovuotojen ja tiedon tuhoutumisen estämistä sekä käyttöoikeusvalvontaa, jotka ovat toteutettavissa DLP-ratkaisuilla edellä kuvatuin tavoin.

DLP on kehittynein teknisistä ratkaisuista, joilla voidaan estää tietovuotoja asetusten vaatimilla tavoilla. SIEM-ratkaisut eivät estä tietovuotoja, kuten luvussa 4.4 on todettu. Myös yleisimmät tietoturvalaitteet, kuten palomuurit ja IDS/IPS-laitteet, eivät tietovuotojen estämiseen pysty.

6.2 DLP-ratkaisujen markkinakehitys

Tutkimusyritys Gartnerin mukaan DLP-ratkaisujen markkinaosuus on kasvanut vakaasti viimeisen seitsemän vuoden ajan. Vuonna 2012 DLP-ratkaisujen arvo maailmanlaajuisesti oli 535 miljoonaa dollaria. Gartner arvioi tämän kasvavan vuonna 2013 670 miljoonaan dollariin. [19.]

Tietosuoja-asetuksen 2012/0011 voimaantullessa DLP-ratkaisujen määrä oletettavasti kasvaa Euroopan unionin alueella. Viime vuosien aikana DLP-ratkaisujen määrä on lisääntynyt erityisesti Ranskassa, Saksassa ja Sveitsissä [19]. DLP-ratkaisujen käyttöä edistää useissa maissa myös kansallinen lainsäädäntö, joka vaatii estämään tietovuotoja, kuten esimerkiksi Espanjassa [30].

Suomesta ei ole saatavilla tilastoa tai tutkimusta käytössä olevista DLP-ratkaisuista. Tällä hetkellä laitevalmistajia lukuun ottamatta mikään taho ei julkisesti markkinoi tai myy DLP-ratkaisuja tai -palveluita Suomessa. Lainsäädännön muuttuessa myös Suo-

messa on otettava DLP-ratkaisut huomioon todennäköisimpänä teknisenä ratkaisuna tietovuotojen estämiseen.

6.3 DLP-ympäristö

Tietovuotojen estämisestä on organisaatioille muutakin hyötyä kuin pelkästään lainsäädännön noudattaminen. DLP-ratkaisujen avulla voidaan suojata yleispätevästi mitä hyvänsä tietoja tietovuodoilta ja tuhoutumiselta, kuten arkaluonteisia luottokortti- tai maksutietoja. Verizonin Data Breach Investigations -raportin mukaan viime vuonna 66 % tietovuodoista huomattiin vasta yli kuukauden päästä tapahtuneesta, ja 69 %:ssa tapahtuneista tietovuodoista ulkoinen taho ilmoitti organisaatiolle tietovuodosta. [29, s. 52–53.] DLP-ratkaisun avulla organisaatio on itse tietoinen mahdollisista tietovuotorikkeistä.

Lisäksi DLP-ratkaisut soveltuvat muun muassa sopimattoman kielenkäytön estämiseen verkossa, sopimattomien verkkosivujen ja kohdeosoitteiden estämiseen sekä työasemissa tarpeettomien ohjelmien asentamisen estämiseen. DLP-ratkaisun avulla saadaan selville, millaista tietoa organisaation verkossa liikkuu. Tällöin tarpeettomaan tai toiminnan kannalta haitalliseen tiedonsiirtoon voidaan puuttua, jolloin voidaan säästää verkon resursseja ja kehittää organisaation toimintaa tehokkaammaksi.

Kokonaisvaltaiseen ja toimivaan DLP-ratkaisuun pitää kuulua vähintään sekä gateway- että endpoint-ratkaisu. Infrastruktuuri pitää muodostaa siten, että DLP voi havainnoida koko verkon ja kaikkien työasemien toimintaa. Myös kannettavat tietokoneet on syytä ottaa endpoint-ratkaisun piiriin. Vaikka kannettavia tietokoneita käytettäisiin muuallakin kuin DLP:n sisäisessä verkossa, ainakin McAfeen DLP Endpoint noudattaa viimeisintä saatua politiikkaa, vaikka tällä ei olisi yhteyttä ePO-palvelimeen.

Lisäksi mahdolliset mobiililaitteet on syytä ottaa huomioon. Gateway-ratkaisu pystyy tarkkailemaan niidenkin verkkoliikennettä, mikäli mobiililaitteita käytetään sisäisessä verkossa, mutta alustavia DLP-ratkaisuja mobiililaitteille on myös olemassa. Esimerkiksi tietoturvayhtiö Symantec tarjoaa Applen iOS-käyttöjärjestelmää käyttäviin laitteisiin DLP for Mobile -ratkaisua [21]. Mobiililaitteiden tietovuotouhat ovat minimoitava henkilöstön tietoturvakoulutuksella ennen kuin mobiililaitteiden DLP-ratkaisut ovat yleistyneet.

Gateway-ratkaisuun voidaan liittää DLP:n lisäksi myös muita tietoturvaominaisuuksia. Mikäli verkko ja käyttäjämäärä ovat suuria, on suositeltavaa käyttää erillisiä laitteita. Turvallisessa ympäristössä DLP:n ja palomuurin lisäksi on suositeltavaa käyttää ainakin IDS/IPS-toimintoja, sekä virusten ja haittaohjelmien torjuntaan erikoistuneita ohjelmistoja.

Ennen DLP-ratkaisun käyttöönottoa on syytä määritellä, mitä arkaluonteista tietoa halutaan suojata. Luvuissa 2 ja 3 esitettyjen asetusten valossa ainakin henkilörekistereiden tiedot on suojattava. Arkaluonteisen tiedon määrittäminen on resursseja vaativa prosessi. Oleellista on määrittää tärkeimmät tiedot ensin, jotta kokonaisuus pysyy hallittavana.

Kun DLP-ratkaisu on otettu käyttöön, on syytä tarkastella verkon liikennettä ja tapahtumia riittävän pitkällä aikavälillä ennen lopullisen politiikan käyttöönottoa. Käytännössä DLP-ratkaisu tallentaa havaitsemansa tietovuodot, mutta ei estä niitä. Ylläpidon tehtävänä on tarkastella näitä tapahtumia ja muodostaa käytettävä politiikka havaittujen tapahtumien perusteella. Tämän tarkkailuajanjakson pituus riippuu verkon koosta ja käyttäjämäärästä, joten aikavaade voi olla mitä tahansa puolesta vuodesta useisiin vuosiin. Tämä vaatii myös huomattavasti resursseja ylläpidolta.

7 Yhteenveto

Tämän työn tarkoituksena oli selvittää, millaisia vaatimuksia Euroopan komission ehdottama tietosuoja-asetus 2012/0011 sekä valtioneuvoston tietoturva-asetus 681/2010 asettavat, ja miten asetusten edellyttämät asiat voidaan toteuttaa. Tietosuoja-asetus 2012/0011 koskee liki kaikkia EU-alueella toimivia tahoja, sillä henkilörekistereitä löytyy yrityksiltä, yhteisöiltä, organisaatioilta sekä viranomaisilta. Asetus 681/2010 koskee valtionhallinnon viranomaisia, ja sitä on noudatettava 1. lokakuuta 2013 mennessä.

Asetusten tietoturvaan liittyvät vaatimukset edellyttävät, että arkaluonteinen tieto on suojattava ja estettävä sen tuhoutuminen, luvaton leviäminen, muuttaminen ja tiedonsaanti. Työssä tarkasteltiin yleisimpiä tietovuotoriskejä ja mahdollisuuksia niiden estämiseen. Tietovuotoja voi estää tietoja käsittelevien henkilöiden tietoturvakoulutuksella ja teknisillä ratkaisuilla.

Tietoturvan laiminlyönti voi johtaa sakkoihin, joka voi olla enintään 1 000 000 euroa tai 2 prosenttia yrityksen maailmanlaajuisesta liikevaihdosta. Myös kansallinen oikeuslaitos voi puuttua tietovuotoihin. Sakon lisäksi tietovuoto on merkittävä kustannustekijä negatiivisen julkisuuden ohella.

Tietovuotojen ja tiedon tuhoutumisen estämiseen kehittynein tekninen ratkaisu on DLP (Data Loss/Leak Prevention). Vain DLP-ratkaisut pystyvät estämään tiedon luvattoman levittämisen, tuhoamisen, muuttamisen sekä tiedonsaannin. Tässä työssä huomattiin, että toimivaan DLP-ympäristöön vaaditaan verkkoliikennettä tarkkaileva gateway-ratkaisu sekä työasemia tarkkaileva endpoint-ratkaisu.

Testatuissa Check Pointin ja McAfeen DLP-ratkaisuissa oli muutamia asioita, jotka pitäisi selvittää ennen käyttöönottoa. Ratkaisujen tarjoamia ominaisuuksia pitäisi tutkia syvemmin. Lisäksi saman laitevalmistajan gateway- ja endpoint-ratkaisua pitäisi testata yhdessä, jotta saataisiin varmuus DLP-ratkaisun täydellisestä toimivuudesta.

DLP-ratkaisun käyttöönottoon on varattava riittävästi aikaa. Suojattava arkaluonteinen tieto on määriteltävä ja luokiteltava. DLP-ratkaisua on koekäytettävä verkossa riittävän pitkään, jotta siihen saadaan toimiva politiikka. DLP-ratkaisun käyttöönotossa on syytä käyttää apuna ulkopuolisia asiantuntijatahoja prosessin nopeuttamiseksi ja turhien kustannusten karsimiseksi.

DLP-ratkaisu on otettava koekäyttöön mahdollisimman pian, jotta siitä saadaan tietovuotoja estävä kokonaisuus ennen asetusten voimaantuloa. DLP-ratkaisu yhdessä henkilöstön tietoturvakoulutuksen kanssa on paras mahdollinen keino estää tietovuotoja.

Lähteet

1 Ehdotus EU-direktiivistä 2012/0010. Euroopan komissio. 2012. Verkkodokumentti. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:FI:PDF>. Luettu 22.4.2013.

2 Ehdotus Euroopan tietoturva-asetuksesta 2012/0011. Euroopan komissio. 2012. Verkkodokumentti. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FI:PDF>. Luettu 22.4.2013.

3 EUROPA-sivusto. Euroopan unioni. Verkkodokumentti. <http://europa.eu/about-eu/basic-information/decision-making/legal-acts/index_fi.htm>. Luettu 22.4.2013.

4 Euroopan Parlamentin ja Neuvoston direktiivi 95/46/EY. Euroopan yhteisöjen virallinen lehti. 1995. Verkkodokumentti. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:FI:PDF>. Luettu 22.4.2013.

5 Eurooppa 2020-sivusto. Euroopan komissio. Verkkodokumentti. <http://ec.europa.eu/europe2020/index_fi.htm>. Luettu 23.4.2013.

6 Asiakastietojen rekisterit. Kela. Verkkodokumentti. <http://www.kela.fi/in/internet/suomi.nsf/NET/020703124759EH>. Luettu 23.4.2013.

7 Legislative Observatory. European Parliament. Verkkodokumentti. <http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011%28COD%29&l=en>. Luettu 26.6.2013

8 Valtioneuvoston asetus 681/2010. Finlex. 2010. Verkkodokumentti. <http://www.finlex.fi/fi/laki/alkup/2010/20100681> Luettu 26.4.2013.

9 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Valtiovarainministeriö. 2010. Verkkodokumentti. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101028Ohjeti/02_Ohje_tietotuvallisuudesta_valtionhallinnossa.pdf>. Luettu 26.4.2013.

10 Internet Security Threat Report 2013. Symantec Corporation. 2013. Verkkodokumentti. <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf>. Luettu 17.6.2013.

11 Gordon, Peter. 2007. Data Leakage – Threats and Mitigation. SANS Institute. Verkkodokumentti. <http://www.sans.org/reading_room/whitepapers/awareness/data-leakage-threats-mitigation_1931>. Luettu 28.4.2013.

12 DataLossDB. Open Security Foundation. 2013. Verkkodokumentti. <http://datalossdb.org/>. Luettu 28.4.2013.

13 Symantec Intelligent Report, May 2013. Symantec Corporation. 2013. Verkko-dokumentti. <http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_05-2013.en-us.pdf>. Luettu 18.6.2013.

14 Check Point 2013 Security Report. Check Point. 2013. Verkkodokumentti. <http://sc1.checkpoint.com/documents/security-report/>. Luettu 17.6.2013.

15 2013 Cost of Data Breach Study: Global Analysis. Ponemon Institute LLC. 2013. Verkkodokumentti. <https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf>. Luettu 18.6.2013.

16 Opas julkishallinnon tietoturvakoulutuksen järjestämisestä. Valtiovarainministeriö. 2003. Verkkodokumentti. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53763/53760_fi.pdf>. Luettu 29.4.2013.

17 A Practical Guide to Next-Generation SIEM. Sensage. 2012. Verkkodokumentti. <http://www.sensage.com/sites/default/files/sens_gd_next-gen_siem_03ol.pdf>. Luettu 26.6.2013.

18 Symantec Data Loss Prevention for Mobile. Symantec. 2012. Verkkodokumentti. <http://static1.symanteccontent.com/content/en/us/enterprise/fact_sheets/b-dlp_for_mobile_DS_21213700-1.en-us.pdf>. Luettu 26.6.2013.

19 Magic Quadrant for Content-Aware Data Loss Prevention. Gartner. 2013. Verk-kodokumentti. <http://www.gartner.com/technology/reprints.do?id=1-1DX8RZB&ct=130204&st=sg>. Luettu 26.6.2013.

20 Laki sähköisen viestinnän tietosuojalain muuttamisesta. Finlex. 2009. Verkko-dokumentti. <http://www.finlex.fi/fi/laki/alkup/2009/20090125>. Luettu 20.6.2013.

21 Laki- ja säädösvalmistelu: Tietoyhteiskuntakaari LVM059:00/2011. Liikenne- ja viestintäministeriö. 2012. Verkkodokumentti. <http://www.lvm.fi/web/fi/lakihankkeet_viestinta/-/mahti/asia/58526>. Luettu 20.6.2013.

22 Data Loss Prevention R76 Administration Guide. 2013. Check Point. Verkkodokumentti. <http://downloads.checkpoint.com/dc/download.htm?ID=22912>. Luettu 10.5.2013.

23 McAfee Data Loss Prevention 9.2 Software Product Guide. 2011. McAfee. Verkkodokumenti. <https://kb.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23613/en_US/dlp_920_pg_endpt-epo46_en-us.pdf>. Luettu 4.6.2013.

24 McAfee Data Loss Prevention 9.2 Software Installation Guide. 2011. McAfee. Verkkodokumentti. <https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23610/en_US/dlp_920_ig_endpt-epo46_en-us.pdf>. Luettu 4.6.2013.

25 Technical Articles, KB77803. McAfee. 2013. Verkkodokumentti. <http://kb.mcafee.com/agent/index?page=content&id=KB77803&actp=RSS>. Luettu 6.6.2013.

26 Cisco Data Loss Prevention. Cisco. Verkkodokumentti. <http://www.cisco.com/en/US/prod/vpndevc/ps10128/ps10154/dlp_overview.html>. Luettu 2.8.2013.

27 McAfeen verkkosivusto. McAfee. Verkkodokumentti. <http://www.mcafee.com/us/>. Luettu 2.8.2013.

28 Check Pointin verkkosivusto. Check Point. Verkkodokumentti. <http://www.checkpoint.com/>. Luettu 2.8.2013.

29 2013 Data Breach Investigations Report. Verizon. 2013. Verkkodokumentti. <http://www.verizonenterprise.com/DBIR/2013/>. Luettu 3.8.2013.

30 Royal Decree 1720/2007. Agencia Española de Protección de Datos. 2008. Verkkodokumentti. <http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/reglamentolopd_en.pdf>. Luettu 3.8.2013.

Check Point DLP Gatewayssa käytetyt tietotyypit

Henkilön nimi, katuosoite ja kaupunki lisättiin jokainen omaan avainsanalistaan. Avainsanalista koostuu avainsanoista tai ilmaisuista, joista jokainen on omalla rivillään tekstitiedostossa. Tekstitiedosto pitää olla UTF-8 -muodossa. Mikäli käytetään muita kuin englanninkielisiä sanoja tai ilmauksia, Check Point suosittelee tiedostomuodoksi doc-tiedostoa. [22, s. 110.] Avainsanalistan voi määrittää myös tarkkailemaan jokaisella rivillä esiintyviä sanoja missä järjestyksessä tahansa; esimerkiksi mikäli avainsanalistassa on nimi ”Matti Meikäläinen”, DLP Gateway havaitsee oletuksena vain ”Matti Meikäläinen” -nimen, ei ”Meikäläinen Matti” -nimeä. [22, s. 165.] Pidempien ilmaisujen kanssa tämä tosin saattaa aiheuttaa virhetulkintoja.

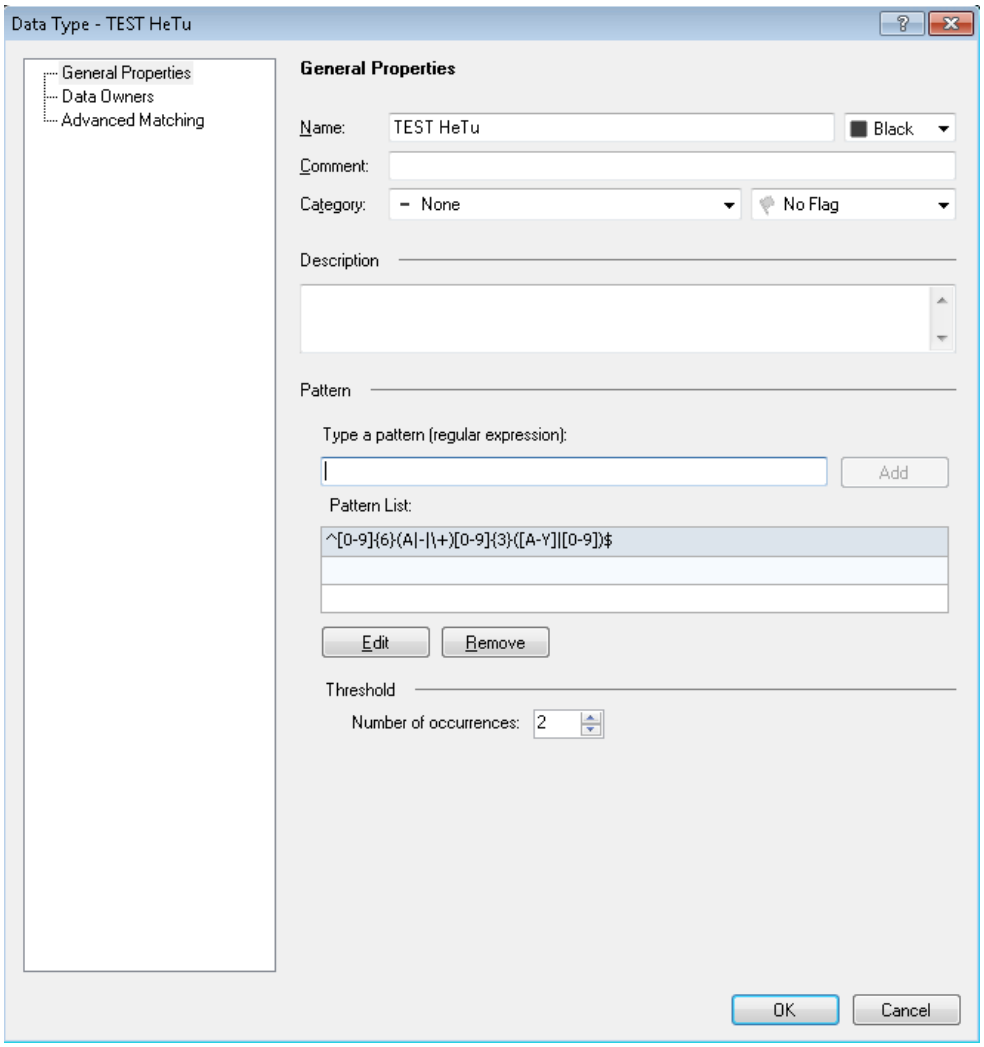
Henkilötunnus, tunnistenumero, postinumero, puhelinnumero sekä IBAN-tilinumero ovat kaikki tietyn pituisia merkkijonoja, joten niitä voidaan käsitellä säännöllisten lausekkeiden avulla. Rekisterissä esiintyvät tiedot voidaan laittaa myös avainsanalistoihin, mutta yleispäteviä säännöllisiä lausekkeita voi käyttää muissakin säännöissä. Säännölliset lausekkeet muodostettiin alla olevasti:

- Henkilötunnus: ^[0-9]{6}(A|-|\+)[0-9]{3}([A-Y]|[0-9])$
- Tunnistenumero (6 numeroa, ensimmäinen numero aina 1): ^1[0-9]{5}$
- Postinumero (5 numeroa): ^[0-9]{5}$
- Puhelinnumero (10 numeroa; ensimmäisen kolmen numeron jälkeen voi olla tyhjä väli tai väliviiva, tai kaikki numerot voivat olla kirjoitettu yhteen): ^([0-9]{3}(|-)[0-9]{7})|([0-9]{10})$
- Suomalainen IBAN-tilinumero: ^FI[0-9]{16}$

Kuvassa 1 on esimerkki henkilötunnusta tarkkailevasta tietotyypistä ja sen mahdollisista asetuksista. ”Data Owners” -sivulla voidaan määritellä erikseen tiedon omistaja, jolle lähetetään notifikaatti kun tietovuoto on havaittu. ”Advanced Matching” -sivulla voidaan tälle tietotyypille luoda edistyneempiä ominaisuuksia CPCode-skriptikielen avulla.

Säännöllisen lausekkeen tai muiden tietotyyppien toiminnallisuutta ei voi testata miten-kään etukäteen SmartDashboardissa. Tietotyypin oikean toiminnallisuuden saaminen kuntoon voi edellyttää jopa debug-viestien tarkkailua. DLP Gatewayn debuggauksesta löytyy lisätietoa liitteestä 3. Check Point suosittelee tietotyypin testaamista testikäyttä-

jän avulla, ja tarkkailemalla lokitietoja SmartView Trackerilla tai SmartEventin avulla [22, s. 119]. Tämä ei kuitenkaan auta mikäli tiedosta ei jää minkäänlaista lokitietoa.



Kuva 1. HeTu-nimisen säännöllisen lausekkeen ominaisuuksia.

Check Point DLP Gatewayn protokollien tarkkailun toimivuus

HTTP-protokollan tarkkailu on oletuksena päällä DLP Gatewayssa ja se toimi normaalisti alusta alkaen. Oletuksena Check Point tarkkailee HTTP-protokollaa porteissa 80 ja 8080, mutta portteja voi halutessaan lisätä tai muuttaa. [22, s. 134.] DLP Gateway havaitsi oletetusti käytettyjä sääntöjä vastaavan HTTP-liikenteen. Toimintaa kokeiltiin lähettämällä rekisteritietoja HTTP-protokollalla portissa 80 määrätylle palvelimelle sekä julkisille sivustoille. Mikäli User Check ei ollut käytössä ja sääntö oli laitettu Ask User -tilaan, DLP Gateway ei ilmeisesti lähettänyt tietoja eteenpäin palvelimelle ja sivu latautui aina hyväksymisen jälkeen uudelleen. User Checkin kanssa vastaavaa ongelmaa ei ollut. Ongelma luultavasti selviäisi tutkimalla DLP Gatewayn debug-tietoja.

DLP Gateway voi tarkkailla myös salattua HTTPS-protokollaa. DLP Gateway voi tarkkailla kahdella tavalla HTTPS-liikennettä: joko sisäiseen suuntaan (”Inbound HTTPS Inspection”), esimerkiksi sisäisten palvelimien suojaamiseksi tarkkailemalla muista verkoista tulevaa liikennettä, tai ulkoiseen suuntaan (”Outbound HTTPS Inspection”) tarkkailemalla sisäverkosta ulospäin liikkuvaa liikennettä. Tässä testiympäristössä kokeiltiin vain sisäverkosta ulospäin esiintyvää HTTPS-liikennettä.

DLP Gateway toimii välityspisteenä työaseman ja palvelimen välillä. Kun DLP Gateway havaitsee HTTPS-liikennettä, se keskeyttää liikenteen ja muodostaa HTTPS-yhteyden varsinaisen palvelimen kanssa. Tämän jälkeen DLP Gateway muodostaa HTTPS-yhteyden työaseman kanssa, josta HTTPS-liikenne alun perin lähti. Tällöin DLP Gateway voi purkaa työasemalta lähtevän liikenteen salauksen, tutkia sen, ja salata liikenteen uudelleen palvelimelle lähetettäessä. [22, s. 34.] Työasema ei tosin voi olla varma palvelimen luotettavuudesta, sillä se saa sertifikaatin DLP Gatewaylta.

HTTPS-tarkkailua varten DLP Gatewaylle pitää luoda CA-sertifikaatti (Certificate Authority) tai vastaavasti käyttää jo olemassa olevaa sertifikaattia. Sertifikaatti pitää myös jakaa eteenpäin työasemille. Ohje HTTPS-tarkkailun käyttöönottoon löytyy Check Pointin Data Loss Prevention R76 Administration Guidesta sivulta 34 alkaen. [22, s. 34.] Testiympäristössä käytettiin self-signed -sertifikaattia, jolloin työaseman selaimesta jouduttiin erikseen hyväksymään turvallisuuspoikkeukset HTTPS-sivuille mentäessä. Käytännössä HTTPS-tarkkailu toimi hyvin. Toimintaa kokeiltiin muun muassa HTTPS-yhteyttä käyttävillä Web Mail -sähköposteilla ja tiedostonjakopalveluissa.

Ilman User Check -ohjelmistoa HTTPS-protokollaa käytettäessä esiintyi samanlainen ongelma kuin HTTP-protokollalla. Käyttäjälle ei tullut minkäänlaista tietoa tietovuodosta, vaikka sääntöä kokeiltiin kaikilla mahdollisilla tiloilla. Ask User -tilassa liikenne katkaistiin, sillä käyttäjältä ei voinut tulla kuittausta hyväksymisestä DLP Gatewaylle.

DLP Gateway pystyy tarkkailemaan salaamattomalla SMTP-protokollalla lähetettyjä sähköposteja. Testiympäristössä kokeiltiin portteja 25 ja 26. Huomioitavaa on, että DLP Gatewaylle pitää lisätä käyttäjä sillä sähköpostiosoitteella, jota halutaan tarkkailla. DLP Gateway ei siis automaattisesti tarkista kaikkia lähetettyjä sähköposteja, vaan vain niitä, joiden osoitteet ovat erikseen määritelty. Testiympäristössä tämä aiheutti aluksi epäselvyyttä, kun käyttäjää ei oltu erikseen lisätty. Asia selvisi kuitenkin tarkemmin debug-tietoja tarkastellessa.

Muutoin SMTP-protokollan tarkkailun kanssa ei havaittu ongelmia. DLP Gateway lähetti sähköpostin takaisin vahvistusta varten mikäli sääntö oli Ask User -tilassa, ja myös Inform User- ja Prevent -tiloissa DLP Gateway tiedotti käyttäjää sähköpostitse. Toimintaa testattiin Mozillan Thunderbird -sähköpostiohjelman versiolla 17.0.6 sekä telnet-yhteyden kautta suoraan SMTP-palvelimelle komentoja antaen. DLP Gatewaylla on myös erityistuki Microsoftin Exchange -sähköpostipalvelinohjelmistoille, jonka avulla DLP Gateway pystyy myös tarkastelemaan TLS-suojauksella lähetettyjä sähköposteja. Tämän käyttöönotto vaatii pääsyn Exchange -palvelimelle, joten sitä ei tässä testiympäristössä testattu. Lisätietoa asiasta ja asennusohjeet löytyvät Check Pointin Data Loss Prevention R76 Administrator Guidesta sivulta 28 alkaen. [22, s. 28.]

DLP Gateway voi tarkkailla myös tiedonsiirtoa salaamattomalla FTP-protokollalla. Laite havaitsi ja keskeytti tiedonsiirron, mikäli FTP:n kautta siirrettävät tiedostot sisälsivät sääntöihin osuvia tietoja. Sekä sähköpostitse että FTP-tiedonsiirrossa DLP Gateway pystyi tarkkailemaan yleisimpien tekstitiedostojen ja -dokumenttien ohella myös pakattuja tiedostoja. Check Pointin Data Loss Prevention R76 Administration Guiden mukaan DLP Gateway voi tarkkailla seuraavia pakattuja tiedostoja:

- zip
- zip-exe
- gzip
- rar

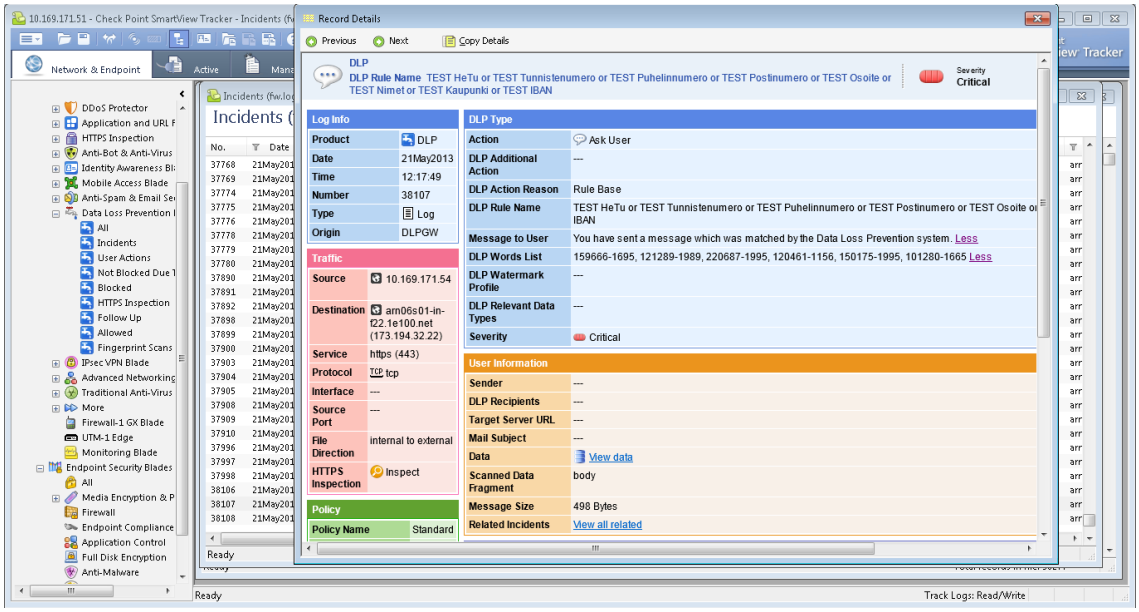
- tar
- jar
- 7z. [22, s. 81.]

Administration Guidessa ei ole mainittu, mitä tekstitiedostoja ja -dokumentteja DLP Gateway pystyy oletuksena tarkkailemaan. Testiympäristössä kokeiltiin txt-, rtf-, pdf- ja doc -tiedostoja.

FTP-protokollan tarkkailussa huomattiin debug-tietoja tarkastellessa, että DLP Gateway ei osaa käsitellä user@domain.com -muotoista käyttäjätunnusta. DLP Gateway lähetti palvelimelle vain käyttäjänimen user, jolloin se ei vastannut palvelimen tietokannassa olevaa käyttäjää.

Check Point DLP Gatewayn loki ja vianselvitys

DLP Gatewayn keräämiä lokitietoja voi tarkastella SmartView Trackerin avulla. Sääntö kerää lokitietoja vain jos tämä on erikseen laitettu päälle. Tapahtuneesta tietovuodosta käy kattavasti ilmi tietoja, kuten esimerkiksi mihin sääntöön lähetetty tieto on osunut ja mitä tietoja se on alun perin sisältänyt. Vastaavasti lokiin voi kerätä tapahtumia, jotka eivät ole osuneet mihinkään sääntöön. Kuvassa 1 näkyy lokitieto HTTPS-protokollalla lähetetyllä henkilötietoja sisältäneeltä Googlen Gmail -viestistä.



Kuva 1. SmartView Trackerin lokitieto HTTPS-protokollalla lähetetystä Gmail-viestistä.

Lokitiedosta voi myös katsoa alkuperäisen viestin, jonka perusteella DLP Gateway on huomannut tietovuodon. Tämä ei kuitenkaan ole nykyisen lainsäädännön mukaan laillista (ks. luku 4.5, s. 33).

Mikäli halutaan tarkempaa vianselvitystä tai tietoa siitä, miksi jokin lähetetty tieto ei osu mihinkään sääntöön, voidaan tarkastella DLP Gatewayn debug-tietoja. Tällöin laitteeseen on kirjauduttava CLI:n kautta. CLI:ssä debug-tilan saa päälle fw debug -komennolla. DLP Gateway käyttää eri prosesseja eri protokollille, jolloin myös jokaiseen haluttuun prosessiin on laitettava debug erikseen päälle. Seuraavat prosessit ovat perusvianselvityksen kannalta oleellisia:

- fwdlp – DLP-prosessi

- in.emaild.smtp – SMTP-protokollaa tarkkaileva prosessi
- aftpd – FTP-protokollaa tarkkaileva prosessi
- dlpu – HTTP/HTTPS -protokollaa tarkkaileva prosessi.

Laitteen tallentamat debug-tiedot löytyvät elg-tiedostoista kansiosta $FWDIR/log/. Esimerkiksi fwdlp-prosessin debugin saa päälle fw debug fwdlp on TDERROR_ALL_ALL=5 -komennolla, ja pois päältä vastaavasti fw debug fwdlp off -komennolla. Debugtiedot löytyvät tässä tapauksessa siis tiedostosta $FWDIR/log/fwdlp.elg.

Mikäli protokollien toimivuudessa on ongelmia, kannattaa kunkin protokollan prosessia debugata. Fwdlp-prosessista vastaavasti löytyy DLP:n tekemät päätökset ymmärrettävällä kielellä. Esimerkiksi fwdlp:n debug-tiedoista voi löytyä syy jos jokin lähetetty tieto ei osu mihinkään sääntöön. Alla on esimerkki fwdlp:n debug-viesteistä, kun lähetettyä sähköpostia verrataan sääntöihin ”Finland Personal Identity Code” ja ”Finland Personal Names”.

```
[fwdlp 23509 1927423696]@DLPGW[15 May 18:29:17] dlpe_rule_is_matched: Rule
name: 'Finland Personal Identity Code or Finland Personal Names
[fwdlp 23509 1927423696]@DLPGW[15 May 18:29:17] dlpe_timerange_is_active_now
[fwdlp 23509 1927423696]@DLPGW[15 May 18:29:17] dlpe_timerange_is_active_now
:: Time range 'Any' is 'Any' timerange - rule is active
[fwdlp 23509 1927423696]@DLPGW[15 May 18:29:17] dlpe_rule_target_is_match
[fwdlp 23509 1927423696]@DLPGW[15 May 18:29:17] dlpe_policy_target_is_match::
Called
[fwdlp 23509 1927423696]@DLPGW[15 May 18:29:17] dlpe_message_target_get_type:
Message target type is '0'
[fwdlp 23509 1927423696]@DLPGW[15 May 18:29:17]
dlpe_policy_target_my_org_match_mail
[fwdlp 23509 1927423696]@DLPGW[15 May 18:29:17]
dlpe_message_target_get_is_mail_internal
[fwdlp 23509 1927423696]@DLPGW[15 May 18:29:17]
dlpe_policy_target_my_org_match_mail:: Mail is NOT internal, return FALSE.
Don't need to check IP.
[fwdlp 23509 1927423696]@DLPGW[15 May 18:29:17] dlpe_rule_is_matched :: source
NOT matched rule: ({7EFA42A0-D43E-467E-831C-B39BD9A4B717})'Finland Personal
Identity Code or Finland Personal Names'
```

Esimerkki 1. Esimerkki fwdlp-prosessin debugviesteistä.

Tässä tapauksessa tietotyyppejä ei verrata sen tarkemmin, kun sähköpostin lähettäjä ei ole määritelty sisäiseksi käyttäjäksi DLP Gatewaylla (”Mail is NOT internal, return FALSE”). Fwdlp-prosessi palauttaa tämän jälkeen protokollaa tarkkailevalle prosessille tiedon siitä, ettei sähköpostissa ollut mitään sääntöihin osuvaa tietoa (”source NOT matched rule”).

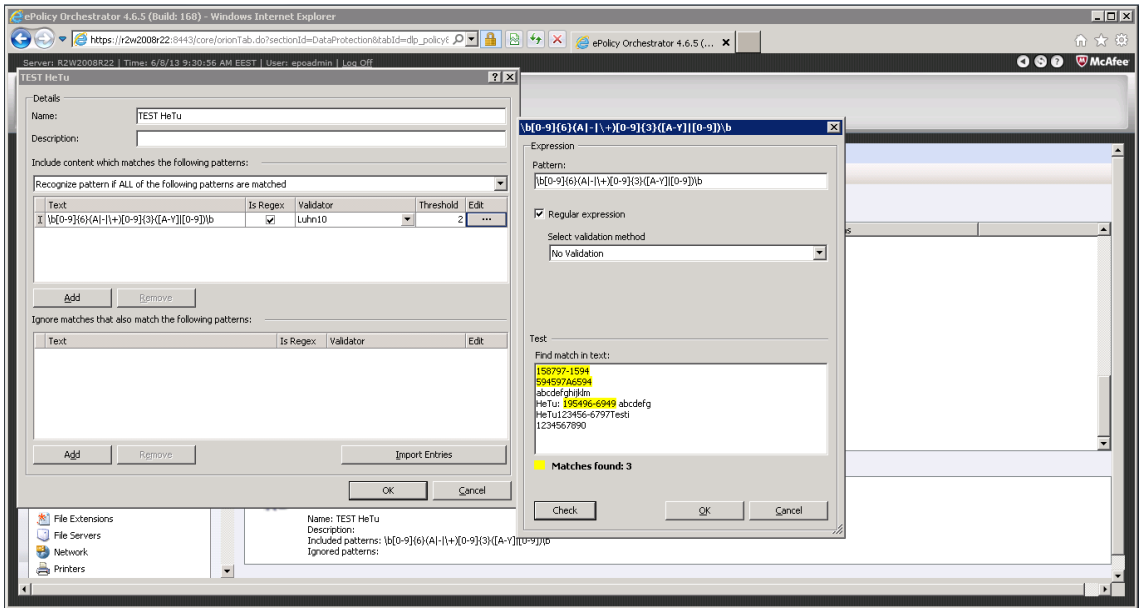
McAfee DLP Endpointin asennuksessa huomioitavaa

EPO-palvelimelle täytyy asentaa varsinaisen DLP Endpoint -ohjelmiston lisäksi myös erillinen McAfee DLP Windows Communication Foundation (WCF) -palvelu, joka toimii rajapintana ePO:n ja DLP Endpointin välillä. [24, s. 16.] DLP Endpoint vaatii työasemiin myös erillisen DLP Monitor-ohjelmiston, joka asentuu McAfee Agentin kautta automaattisesti. DLP Monitor on varsinainen DLP-prosessi.

Testiympäristön käyttöönotossa huomattiin, että ePO-palvelimen sekä työasemien piti olla samassa Windows-toimialueessa (engl. ”Windows Domain”). Tästä ei ollut mainintaa McAfeen DLP 9.2 Software Installation Guidessa [24]. Täten ePO-palvelimesta tehtiin myös Domain Controller, toimialueen ollessa ”DLP”.

McAfee DLP Endpointissa käytetyt tietotyypit

McAfee DLP Endpointissa käyteyt tietotyypit muodostettiin samalla tavalla kuin Check Pointin DLP Gatewaylle liitteessä 1. Erona Check Pointin ratkaisuun, DLP Endpointissa säännöllisen lausekkeen alku ja loppu pitää merkitä \b -merkinnällä. Avainsanalistaa ei voi myöskään tuoda suoraan ulkoisesta tiedostosta, joskin sen sisällön voi kopioida ePO:n DLP-hallintaan. Säännöllisten lausekkeiden testaaminen onnistuu suoraan niiden teon jälkeen, kuten kuvassa 1 on havainnollistettu henkilötunnusta koskevan säännöllisen lausekkeen avulla.



Kuva 1. McAfee DLP Endpointin säännöllisiä lausekkeita voi testata etukäteen.

McAfee DLP Endpointin sääntöjen toimivuus

Application File Access -sääntö tarkkailee määriteltyjen ohjelmien ja tiedostojen käyttöä. Sen avulla voidaan esimerkiksi tarkastella, mitä dokumentteja työasemalla tallennetaan. Tiedoston tallennusta ei voida estää, mutta tieto tapahtumasta voidaan tallentaa ja myös käyttäjää voidaan ilmoittaa tästä. Tästä tehtiin sääntö, joka tarkkailee Microsoft Wordilla ja Notepadilla tallennettuja tiedostoja. Tiedostojen sisältöä voidaan verrata joko Tagging- tai Content Classification -sääntöjen perusteella. Toiminnassa ei havaittu ongelmia.

Leikepöytää tarkkaileva Clipboard-sääntö voidaan laittaa estämään leikepöydän käytön joko eri ohjelmien välillä tai saman ohjelman eri dokumenttien välillä. Tiedotus käyttäjälle tapahtuu siten, että alkuperäinen sääntöön osunut tieto korvataan liitettäessä ilmoituksella, jossa kerrotaan, ettei kyseistä tietoa saa kopioida. Arkaluonteista tietoa voi kategorisoida Tagging- tai Content Classification -sääntöjen perusteella.

Sähköpostia tarkkaileva Email Protection -sääntö toimii ilmeisesti vain Microsoft Outlookilla sekä Lotus Notesilla [23, s. 93]. Toimintaa testattiin sekä Mozilla Thunderbirdin versiolla 17.0.6 että Microsoft Outlookin versiolla 2013, ja sääntö toimi vain jälkimmäisessä. Sääntö kuitenkin havaitsi sekä tekstikentässä että liitetiedostona lähetettyä arkaluonteista tietoa. Sääntö osaa myös avata yleisimmät pakatut tiedostot ja tutkia niiden sisällön. Sääntöä kokeiltiin lähettämällä sekä salaamatonta että SSL/TLS-salattua sähköpostia. File System Protection -säännössä käytettiin tiedostopalvelimena ePO-palvelimella olevaa jaettua kansiota. Sääntö esti arkaluontoisen tiedon tallentamisen palvelimelle sekä tiedostojen tuhoamisen, mutta ei tiedostojen kopiointia työasemalle. Molemmissa säännöissä tietoa voidaan kategorisoida Tagging- ja Content Classification -sääntöjen perusteella.

Yleisesti verkkoliikennettä tarkkaileva Network Communication Protection -sääntö voi käyttää vain Tagging-säännöllä merkittyjä tiedostoja. Käytännössä tämä tarkoittaa sitä, että sääntö huomaa tiedostonsiirron mutta ei esimerkiksi Internet-sivulle ja sähköpostin tai pikaviestimien kautta lähetettyä tekstiä. Sääntö havaitsi HTTP-protokollalla ja sähköpostitse lähetettyjä tiedostoja, mutta ei esimerkiksi FTP-tiedonsiirtoa. Sääntö huomasi myös HTTPS-protokollaa käyttävän Gmail-sähköpostin liitetiedoston.

PDF/Image Writer Protection -sääntö ei luokittele tiedon sisältöä mitenkään, vaan sen voi laittaa estämään tai tarkkailemaan ohjelmallisten tulostimien käyttöä. Säännön toimintaa kokeiltiin ilmaisella PDFCreator-ohjelmalla. Kuvaruutukaappauksia koskeva Screen Capture Protection -sääntö tarkkailee Tagging-sääntöjen merkitsemiä tiedosto- ja ja voi estää niistä otetut kuvaruutukaappaukset.

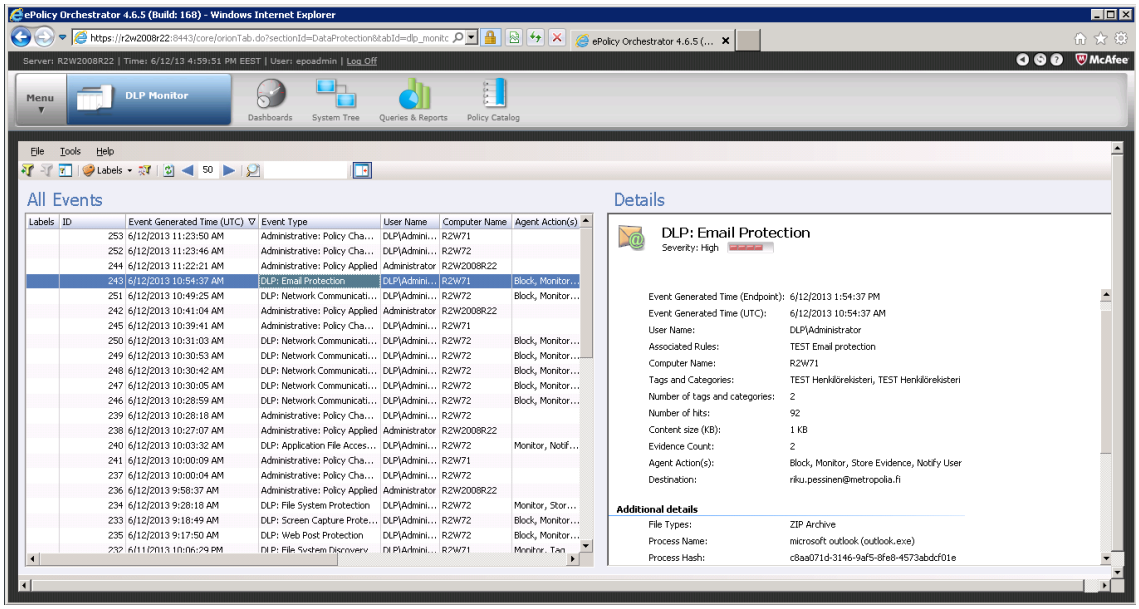
Verkkosivuille tallennettavaa tietoa tarkkaileva Web Post Protection -sääntöä kokeiltiin Internet Explorer 10 ja Mozilla Firefox 5.0 -selaimilla. Vaikka säännön pitäisi toimia McAfeen mukaan Internet Explorerin versiosta 6 lähtien, se ei kuitenkaan versiossa 10 toiminut. Mozilla Firefoxin 5.0 -versioissa sääntö toimi moitteetta niissä palveluissa kuin sen pitikin (ks. s. 50).

Myös Discovery-säännön toimivuutta kokeiltiin. Tämän käyttöönottamiseksi ePO-palvelimelta pitää muuttaa myös McAfee Agentin yleisistä asetuksista (”Global Agent configuration”) Discovery-välilehdellä järjestelmäskannaukselle jokin tietty ajankohta. DLP Endpoint Discovery crawler löysi ja merkitsi työsemilla olleet arkaluontoista tietoa sisältävät tiedostot.

Tässä testiympäristössä ePO-palvelimella ollut uusin politiikka ei asentunut työasemille Wake Up Agents -toiminnon avulla suoraan, vaan työasemalta piti Agentista erikseen pyytää uutta politiikkaa Check New Policies- ja Enforce Policies -toimintojen avulla.

McAfee DLP Endpointin loki ja vianselvitys

EPO-palvelimen ja McAfee Agenttien havaitsemia lokitietoja voi tarkastella ePO:ssa erillisellä DLP Monitor -ohjelmalla, jonka avulla saa selville DLP:n havaitsemat tietovuototapahtumat ja mahdolliset ePO-palvelimen viestit, kuten politiikkamuutokset. Tietovuototapahtumista käy selkeästi ilmi, mistä säännöstä tämä on johtunut ja mitä tietoja tähän on liittynyt. Kuvassa 1 on esimerkki Email Protection -säännön luomasta lokimerkinnästä.



Kuva 1. DLP Monitorin lokitieto Email Protection -säännön havaitsemasta tapahtumasta.

Tarkempaa vianselvitystä varten sekä ePO-palvelimesta että työasemien McAfee Agenteista on mahdollista tarkastella debug-tietoja. EPO-palvelimen debug-tiedostot sijaitsevat asennuskansiossa /Server/Logs/ -kansion alta. Mahdolliset HTTP-palvelimen virheet löytyvät /Apache2/Logs/ -kansion alta.

McAfee Agentin vianselvitystä varten pitää debug-tason lokitus ottaa käyttöön ePO-palvelimella McAfee Agentin yleisistä asetuksista (”Global Agent configuration”). Tämän jälkeen tarvittavat debug-tiedostot löytyvät työaseman C:\Program Data\McAfee\DLP\Temp\ -kansiosta. Täältä löytyvät mm. eri ohjelmien tarkkailun debug-tiedot (Internet Explorer, Mozilla Firefox, Microsoft Outlook, Lotus Notes) sekä itse Agentin toimintaan liittyvät tiedot. Tarkemmat ohjeet debug-tiedostoista ja debugin käyttöönotosta löytyy McAfeen teknisestä artikkelista KB77803. [25.]