Tietoturvan monitorointi paikallisesti toteutettuna tai ulkoistettuna palveluna

Pyry Jokinen

2020 Laurea

Laurea-ammattikorkeakoulu

Tietoturvan monitorointi paikallisesti toteutettuna tai ulkoistettuna palveluna

Pyry Jokinen

Tietojenkäsittely

Opinnäytetyö

Joulukuu, 2020

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittely
Tradenomi (AMK)

Pyry Jokinen
Tietoturvan monitorointi paikallisesti toteutettuna tai ulkoistettuna palveluna
Vuosi 2020 Sivumäärä 24

Opinnäytetyö tulee organisaatiolle, jolla on suunnitteilla hanke tietoturvan monitoroinnin tehostamiseksi. Toimeksiantajan tehtäväksiannosta tehdään selvitys tietoturvan monitoroinnista yleisellä tasolla vertaillen monitoroinnin toteuttamista paikallisesti tai ulkoistettuna palveluna. Opinnäytetyön tarkoituksena on tuottaa hankkeessa hyödynnettävää tietoa, kun pohditaan tietoturvan monitoroinnin toteuttamistapaa. Työssä keskitytään selvittämään mahdollisia tietoturvan monitorointiratkaisuja huomioiden samalla yritysten vaihtelevat taloudelliset ja henkilöstöön liittyvät resurssit.

Työn tietoperustassa käsitellään tieto- ja kyberturvallisuuteen liittyviä teorioita ja organisaatioihin kohdistuvia tietoturvallisuuteen liittyviä velvoitteita. Lisäksi tarkastellaan, miten tietosuojavelvoitteiisin ja yrityksiä kohtaaviin tietoturvauhkiin voi vastata lokienhallinnan avulla. Tämän jälkeen perehdytään, miten lokien monitorointi on mahdollista toteuttaa organisaatioissa paikallisesti tai palveluna. Tiedon hankintaan käytettiin aiempia tutkimuksia, kirjallisuutta, sekä julkaisuja aiheesta. Lisäksi haastateltiin vapaamuotoisesti kahta toimeksiantaja-organisaation tietoturvasta vastaavaa jäsentä.

Tietoturvan toteutusta suunnitellessaan organisaation tulee tarkastella, mitkä sen riskienhallinnan tavoitteet ovat, ja mitä asiantuntemusta se tarvitsee niiden saavuttamiseksi. Lisäksi organisaation on pohdittava, mitä näistä asiantuntemuksista sen on mahdollista tai kannattavaa hankkia yritykseen, ja missä tapauksissa asiantuntemus kannattaa hankkia ulkoistettuna.

Asiasanat: tietoturva, lokienhallinta, paikallisesti, ulkoistettuna, palveluna

Laurea University of Applied Sciences **Abstract**

Degree Programme in Business Information Technology

Bachelor's Thesis

Pyry Jokinen

Monitoring of the Information Security Locally or as an Outsourced Service

Year 2020 Pages 24

This thesis was commissioned by an organization looking to enhance the monitoring of their information systems. On behalf of the client, this thesis seeks to find out information about security and log monitoring and its implementation methods locally and as a service. The goal of the research was to produce information that can be utilized, when considering whether log monitoring should be done locally or outsourced to a third party.

The knowledge base begins by reviewing the theory on information security and data protection obligations. After that was examined, how the log management can be used to address the organization's data protection obligations and to minimize information security risks. Finally, it addresses how the log monitoring can be implemented either locally or as an outsourced service. Previous research, literature and publications on the subject were used to obtain information. In addition, two information security officers of the client organization were interviewed in a free-form manner.

When planning the implementation of information security, an organization should consider what will be the risks of the management objectives and what expertise the organization will need to achieve them. In addition, the organization needs to consider, if the expertise is profitable for the company to acquire in-house, and in which cases it is more worthwhile to acquire the expertise outsourced.

Keywords: information security, monitoring, log management, outsourcing

Sisällys

1 Johdanto

Nykypäivän tietoyhteiskunnassa, jossa yritykset ja organisaatiot ovat pitkälti riippuvaisia digitaalisista palveluista ja järjestelmistä, tietoturvan merkitys kasvaa entisestään. Niin maailmanlaajuiset kuin kotimaisetkin organisaatiot joutuvat kohtaamaan kasvavan määrän tietoturvauhkia. Suomen Kyberturvallisuuskeskus kertoo vuoden 2019 vuosittaisessa katsauksessaan Suomeenkin rantautuneesta uudesta ilmiöstä nimeltä "big game hunting", jossa rikolliset kohdistavat kiristyshaittaohjelmahyökkäyksiä yrityksiin suurien lunnaiden toivossa (Tietoturvan vuosi 2019, 2020, 22).

Hyökkäykset voivat hidastaa yrityksen normaalia toimintaa, sekä aiheuttaa mittavia taloudellisia ja maineellisia tappioita. Viimeisimpänä esimerkkinä voidaan pitää psykoterapiakeskus Vastaamoon kohdistunutta tietomurtoa, jossa suuri määrä Vastaamon potilastietoja varastettiin ja niillä kiristettiin yritystä ja sen asiakkaita. (YLE, 2020.)

Viimevuosina tietomurtojen määrä Suomessa on lisääntynyt, minkä vuoksi tapahtumatietojen ja erilaisten lokien seuranta on keskeinen osa yrityksen tietoturvaa. Kyberturvallisuuskeskus toteaakin vuosikatsauksessaan, että ”hyökkäysten havainnointi ja paikallistaminen on erittäin vaikeaa, jos lokeja ei kerätä riittävästi. Esimerkiksi ohjelmistohaavoittuvuuksia hyödynnetään hyökkäyksissä lähes välittömästi, kun tieto haavoittuvuudesta on tullut julkisuuteen” (Tietoturvan vuosi 2018, 2019, 5).

Opinnäytetyössä käsitellään tietoturvallisuuden teoriaa ja tavoitteita, sekä organisaatioihin kohdistuvia tietoturvallisuusvelvoitteita tietosuojan näkökulmasta. Lisäksi käsitellään, miten organisaation on mahdollista vastata tietoturvauhkiin ja velvoitteisiin lokienhallinnan avulla. Lopussa pohditaan millaisissa tilanteissa tietoturvan monitoroinnin toteutus on kannattavaa toteuttaa paikallisesti tai ulkoistettuna.

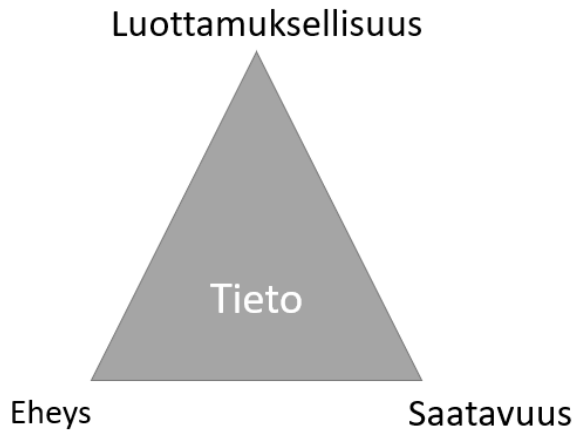
2 Tietoturva

Mitä suuremmassa määrin organisaatioiden toiminta siirtyy manuaalisista palveluista sähköistettyihin, sitä enemmän niihin kohdistuu tieto- ja kyberturvallisuusuhkia. Nykyaikana keskeinen oletus on, että yritykset pystyvät takaamaan turvalliset ja luotettavat digitaaliset palvelut. (Tietoturvapoikkeamatilanteiden hallinta, 2017, 11.)

Tietoturvallisuudella tarkoitetaan hallinnollisia ja teknisiä toimia, joilla pyritään takaamaan, että organisaatiossa vallitsee tila, jossa tietoturvariskit ovat hallinnassa (Kyberturvallisuuden sanasto, 2018, 21). Laajasti käytetyn CIA (Confidentiality, Integrity, Availability) -mallin

mukaisesti, tietoturvan tavoitteena on varmistaa tiedon luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuudella tarkoitetaan, että tietoa käsittelevät vain ne henkilöt, joilla on siihen valtuudet. Eheydellä tarkoitetaan tiedon suojaamista luvattomilta tai tahattomilta muutoksilta. Saatavuudella varmistetaan, että tieto on käyttäjien käytettävissä tarpeen vaatiessa. (Evans, Bond, & Bement, 2004.)

CIA-mallin mukaan tietoturva on kokonaisuus, joka muodostuu tasapainosta sen osa-alueiden välillä. Esimerkiksi tiedon vahva suojaaminen heikentää tiedon saatavuutta, sillä siihen on vaikeampi päästä käsiksi. Säilyttääkseen tiedon luottamuksellisuuden, tiedot on suojattava ja salattava esimerkiksi siten, että niiden käsittely edellyttää kaksivaiheista tunnistautumista ja VPN-yhteyttä. Tiedon eheyden ja saatavuuden takaamiseksi, esimerkiksi vikasietotilanteissa, tieto voidaan varmuuskopioida, ja sitä voidaan säilyttää useassa paikassa. Varmuuskopioitu tieto tulee puolestaan suojata salaus-ja tunnisteohjelmilla, jotta tiedon luottamuksellisuus ja muuttumattomuus voidaan varmistaa tiedon varastoinnissa ja siirrossa. (Chapple & Seidl, 2020, 46.)



Kuva 1. CIA-malli

Kyberturvallisuus voidaan katsoa tietoturvallisuutta täydentäväksi, elektronisten järjestelmien osa-alueeksi. Määritelmän mukaan kyberturvallisuutta ovat ne toimenpiteet, joilla pyritään suojaamaan tietojärjestelmiä ja niissä olevaa tietoa, ohjelmistoja, laitteita, sekä tietoliikenneyhteyksiä kyberuhkilta. Kyberuhkalla tarkoitetaan mahdollisuutta sellaiseen tapahtumaan, joka negatiivisesti vaikuttaisi kybertoimintaympäristöön, eli useammasta tietojärjestelmästä muodostuvaan toimintaympäristöön. Tällaisia uhkia ovat esimerkiksi tietojenkalastelu, haittaohjelmat ja palvelunestohyökkäykset. (Kyberturvallisuuden sanasto, 2018, 24-25.)

Kyberuhkilta voidaan suojautua noudattamalla tietoturvakäytänteitä. Niiden tarkoitus on turvata ja varmistaa asianmukainen suoja organisaation tietotekniselle ympäristölle ja muille

kriittisille resursseille, kuten henkilötiedoille. Käytänteet auttavat tietoturvauhkien ja haavoittuvuuksien tunnistamisessa, sekä organisaation kohtaamien kokonaisriskien vähentämisessä. (Chapple, Stewart & Gibson, 2018.)

3 Tietosuoja-asetukset

Osa tietoturvakäytänteistä on asetusten sanelemia. Vuonna 2018 voimaan astunut GDPR (General Data Protection Regulation) eli EU:n yleinen tietosuoja-asetus velvoittaa, että kaikki yritykset, joissa käsitellään henkilötietoja, noudattavat tiettyjä käytänteitä tietojen suojaamiseksi. Henkilötiedoilla tarkoitetaan kaikkia tietoja, joiden avulla voidaan selvittää kenestä on kyse. Henkilöistä, joiden tietoja käsitellään, käytetään termiä rekisteröity. Rekisterinpitäjäksi kutsutaan tahoa, joka tekee päätöksen henkilötietojen keräyksestä ja käyttötarkoituksesta. Henkilötietojen käsittelijäksi kutsutaan sellaista, joka käsittelee henkilötietoja rekisterinpitäjän puolesta. Henkilötietojen käsittelijä ei siis tee päätöstä tietojen keräyksestä, vaan prosessoi tietoja rekisterinpitäjän antamien ohjeiden mukaan. (Euroopan unioni, 2020.)

Yrityksen kannalta on olennaista selvittää, luokitellaanko yritys rekisterinpitäjäksi vai vain henkilötietojen käsittelijäksi. Tietosuoja-asetuksessa on määritelty erilaiset velvoitteet ja vastuut yrityksen koon, tietojenkäsittelytoimien, sekä roolin mukaan. Rekisterinpitäjällä on viimekädessä vastuu henkilötietojen lainmukaisesta käsittelystä ja siitä, että sen alaiset käsittelijät noudattavat lakia. Yrityksillä voi olla eri rooli eri sopimussuhteissa tai tilanteissa, minkä vuoksi yrityksen kannattaa arvioida asemansa tapauskohtaisesti. (Hanninen & Laine, 2017, 25.)

Tietosuoja-asetuksessa on säädetty henkilötietojen käsittelyn periaatteista, joita on noudatettava aina, kun henkilötietoja käsitellään. Tietosuojaperiaatteet ovat

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys,
- käyttötarkoitussidonnaisuus,
- tietojen minimointi,
- tietojen täsmällisyys,
- tietojen säilytyksen rajoittaminen,
- tietojen eheys ja luottamuksellisuus sekä
- rekisterinpitäjän osoitusvelvollisuus.

(Hanninen & Laine, 2017, 47)

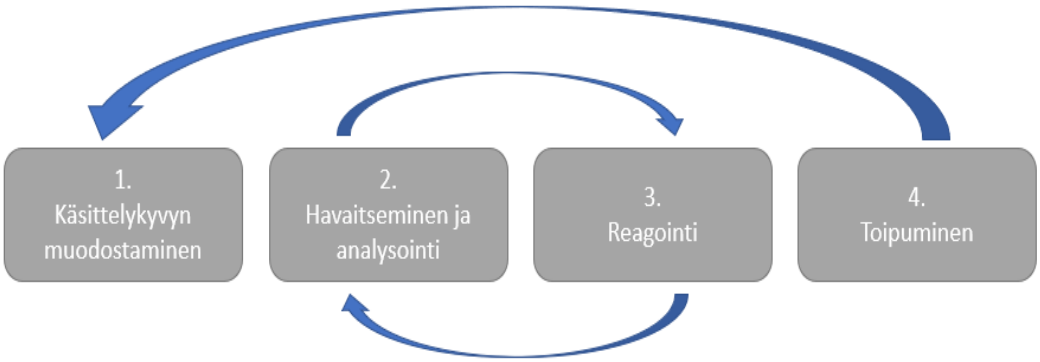
Sen lisäksi, että tietosuojaperiaatteita on noudatettava aina, kun henkilötietoja käsitellään, rekisterinpitäjän on pystyttävä osoittamaan, että se toimii tietosuojaperiaatteiden mukaisesti. Asetus velvoittaa, että organisaation on myös voitava osoittaa toteen, jos tietosuojaloukkaus on tapahtunut. Tietosuojaloukkauksella tarkoitetaan tapahtumaa, jossa henkilötietoja häviää, muuttuu tai joutuu luvattoman tarkastelun kohteeksi. (Tietosuojavaltuutetun toimisto, 2020.)

Tietosuojaloukkauksen tapahtuessa, rekisterinpitäjän on tehtävä siitä ilmoitus valvontaviranomaiselle, paitsi tilanteissa, joissa loukkauksen ei katsota aiheuttavan todennäköistä riskiä rekisteröidyn tiedoille, kuten palvelunestohyökkäyksissä. Rekisterinpitäjä on velvoitettu ilmoittamaan tietoturvaloukkauksesta myös rekisteröidylle, jos loukkauksen katsotaan saattaneen rekisteröidyn henkilötiedot vaaraan, esimerkiksi tilanteessa jossa tallennetut maksutiedot ovat vuotaneet ulkopuolisten haltuun. (Hanninen & Laine, 2017, 109.)

Ilmoitus loukkauksesta on tehtävä 72 tunnin kuluessa siitä, kun loukkaus on havaittu. Ilmoituksen myöhästyessä yrityksen on sisäisen dokumentaation avulla pystyttävä osoittamaan, että tietosuoja-asetuksia on noudatettu ja ilmoituksen viivästymiseen on ollut hyvä syy, tai riskeerata sanktiot ja maineriski. Ilmoitus voidaan jättää tekemättä tietyin syin, mutta tällöinkin rekisterinpitäjän on voitava osoittaa, että ilmoitusta ei ollut tarpeen tehdä, eikä henkilötietoja vaarantunut loukkauksessa. Tietoturvaloukkausten todennäköisien seurauksien arviointi on mahdotonta, ilman riittävää tietoa. Yrityksen tietoturvaprosessien ja tietojärjestelmien dokumentaation on siis oltava kattavaa, jotta osoitus- ja ilmoitusvelvollisuus täyttyy. (Hanninen & Laine, 2017, 109-113.)

4 Tietoturvapoikkeamien havaitseminen

Täyttääkseen osoitus- ja ilmoitusvelvollisuuden asettamat tavoitteet, yrityksellä on oltava ajantasainen tietoturvapoikkeamien ja lokienhallinnan prosessi. Tietoturvapoikkeamaksi katsotaan muutos tai poikkeama datassa tai tietojärjestelmän normaalissa toiminnassa. Poikkeamat voivat vaarantaa tiedon luottamuksellisuuden, eheyden tai saatavuuden tilaa, joten niiden havaitseminen ja dokumentointi on oleellista tietoturvallisuuden ylläpitämiseksi.



Kuva 2. Tietoturvapoikkeamien hallintaprosessi (mukaillen Tietoturvapoikkeamatilanteiden hallinta, 2017, 13.)

Ohessa on esitetty Suomen hallituksen, erityisesti julkishallinnon palveluita tuottaville yrityksille kohdistettu tietoturvapoikkeamien hallintaprosessin malli. Mallin tavoitteena on varautuminen häiriötilanteisiin, häiriötilanteiden seurausten minimointi ja häiriötilanteiden muodostumisen estäminen.

Hallintaprosessin ensimmäinen osa käsittää erilaiset varautumistoimenpiteet ja hallinnolliset menettelyt, joiden avulla poikkeamatilanteissa voidaan toimia. Olennaista varautumisessa on tietojärjestelmien riittävä dokumentaatio, tilannekuvan muodostaminen ja havainnointikyvyn kehittäminen. Toinen vaihe käsittää normaalista toiminnasta poikkeavien tapahtumien havaitsemisen ja analysoinnin. Tavoitteena on selvittää mitä on tapahtunut ja miksi. Analysoinnin lopputulemana saadaan tietää, onko kyseessä toimenpiteitä vaativa tietoturvapoikkeama vai tavallinen häiriötilanne. Kolmas vaihe käsittää poikkeamatilanteisiin reagoinnin ja reagoinnissa käytettävät toimenpiteet. Käynnistettävät toimenpiteet vaihtelevat poikkeustilanteen analysoinnin lopputuleman mukaan. Toipumisvaiheessa toiminta palautetaan asteittain takaisin normaalitilaan. Tapahtunut tilanne dokumentoidaan ja siitä luodaan tarvittavat raportit, joita käytetään edelleen havainnekyvyn ja varautumisen kehittämiseen, vastaavia tapahtumia varten. (Tietoturvapoikkeamatilanteiden hallinta, 2017, 14.)

Edellä kuvattu malli antaa yleiskuvan siitä, millaisia yritysten tietoturvapoikkeamien käsittelyprosessien keskeiset piirteet ovat. Käsittelyprosessiin vaikuttavia tekijöitä ovat yrityksen toimiala, koko ja organisaatiorakenne. Organisaatiorakenteeseen vaikuttavat esimerkiksi yhteistyöyritykset tai palveluiden ulkoistaminen. Erilaisissa kokoonpanoissa vastuut ja velvollisuudet jakautuvat eri tavoin selvitykseen osallistuvien osapuolien kesken. Olennaisinta on, että tietoturvapoikkeamien hallintakyky on riittävää yrityksen toiminnan ja siihen kohdistuvien vaatimusten ja riskien kanssa (Tietoturvapoikkeamatilanteiden hallinta, 2017, 14).

5 Lokienhallinta

Lokitiedolla tarkoitetaan aikajärjestyksessä ilmoitettua tietoa, johon on kirjattu ylös tapahtumia ja niiden aiheuttajia tietojärjestelmissä, verkoissa ja muissa toimintaympäristöissä. Lokitietoja käytetään hyödyksi tapahtumien dokumentointiin, vianetsintään sekä tietoturvapoikkeamien havaitsemiseen. (Lokien keräys ja käyttö, 2016, 2.)

Lokien keräämisen tavoitteena on

- Tehostaa tietosuojan ja -turvallisuuden valvontaa varmistamalla tietojen käytön jäljitettävyys,
- helpottaa häiriöiden ja virhetilanteiden havaitsemista ja selvittelyä,
- parantaa yksilön suojaa varmistamalla tapahtumien kiistämättömyys,
- mahdollistaa väärinkäytösten havaitseminen ja selvittäminen ja
- ennaltaehkäistä osaltaan väärinkäytöksiä.

(Tietoturvapoikkeamatilanteiden hallinta, 2017, 28.)

Tietokoneet, puhelimet, reitittimet, palomuurit, sekä muut laitteet ja ohjelmistot kirjaavat jatkuvasti erilaisia käyttölokeja, tapahtumalokeja, viestintälokeja, virhelokeja ja pääsynvalvontalokeja. Ilman lokitietoja mahdollisten virheiden havaitseminen ja selvittäminen olisi mahdotonta. Käänteisesti lokien avulla voidaan myös nähdä milloin järjestelmät toimivat oikein, ja siten ylläpitää niin sanottua lähtötilannetta eli vertailukohtaa, jota vastaan poikkeamat havaitaan. Tietoturvan näkökulmasta lokienhallinta on hyvin keskeistä. Viestintälokeista voidaan havaita tietoliikenteessä esiintyvät poikkeamat. Pääsynvalvontalokeista voidaan jäljittää järjestelmään kohdistunut luvaton käyttö, ja muutoslokista nähdä mitä luvaton käyttäjä teki järjestelmässä. (Lokien keräys ja käyttö, 2016, 2.)

Poikkeamien havaitsemisen ja selvittämisen kannalta, lokitietoja on kerättävä oleellisista tietojärjestelmistä. Lokitiedot voivat sisältää henkilötietoja, jonka vuoksi lokienhallinnassa on huomioitava tietosuojalainsäädännön asettamat velvoitteet. Minimointiperiaatteen mukaan lokitettujen henkilötietojen on oltava perusteltua ja suhteutettu niiden käyttötarkoitukseen (Kyberturvallisuuskeskus, 2020a). Lokienhallintaa suunnitellessa arvioidaan, millä tarkkuudella lokitiedot otetaan talteen, jotta tietoturvapoikkeamat voidaan parhaiten todentaa. Jos lokitus on säädetty liian raskaaksi, hyödyllistä tietoa on vaikea löytää kaiken datan keskeltä.

Hyvistä lokitiedoista tulisi selvitä ainakin seuraavat tiedot:

- Aikaleima – Tapahtuman ajankohta
- Tapahtuma ja tekijä – Mitä tehtiin ja kuka teki
- Käyttöoikeudet – Millä valtuuksilla ja käyttöoikeuksilla tapahtuma tehtiin tai yritettiin tehdä
- Lähde – Mistä lähteestä tapahtuma tehtiin
- Kohde – Mihin tietoon tai järjestelmään tapahtuma kohdistui
- Tapahtuman tila – Onnistuiko tapahtuma

(Kyberturvallisuuskeskus, 2020a.)

Kaikkien käytössä olevien tietojärjestelmien tulisi dokumentoida lokitiedot omista tapahtumistaan. Lokitiedoissa tulisi näkyä sekä järjestelmän käyttäjien toimenpiteet, että automaattiset tapahtumat. Myös itse lokitietojen tarkastelusta ja käsittelystä tulisi kirjata erilliset lokitiedot. (Lokien keräys ja käyttö, 2016, 4). Lokitietojen säilytysaika ja turvallinen tallennus on varmistettava, sillä osa tietoturvapoikkeamista voi paljastua vasta pitkän ajan kuluttua (Tietoturvapoikkeamatilanteiden hallinta, 2017, 30). Hyvin suunniteltu lokijärjestelmä on muista järjestelmistä erillinen, varmuuskopioitu, ja sen eheys on varmistettu siten, että tietoja ei voi jälkikäteen enää muokata. Jos lokitiedot ovat tallennettuna vain yhteen sijaintiin, lokitietoihin pyrkivä luvaton käyttäjä voi onnistuessaan päästä muokkaamaan tai poistamaan kaikki lokitiedot (Lokien keräys ja käyttö, 2016, 4).

Tietoturvapoikkeamia selvittäessä on olennaista, että lokitiedoissa näkyvät ajankohdat ovat luotettavia. Tästä syystä organisaation tulisi säätää kaikki järjestelmät käyttämään samaa aikalähdettä, jotta tapahtumien vertailu tapahtuisi loogisesti.
(Tietoturvapoikkeamatilanteiden hallinta, 2017, 30.)

6 Tietoturvan monitorointi organisaatiossa

Monitoroinnin voidaan siis todeta olevan keskeinen osa organisaation tietoturvallisuutta, minkä avulla ehkäistään ja puolustaudutaan uhkilta ja vastataan tietoturvavaatimuksiin. Monitorointi antaa organisaatioille kyvyn tunnistaa ja analysoida tapahtumia sen tietoverkossa, ohjelmistossa ja laitteissa. Se on jatkuva toimenpide, jonka keskiössä on siihen käytettävät järjestelmät ja niistä vastaava henkilöstö. Teknologian avulla saavutetaan tietoturvapoikkeamien havaitsemiseen vaadittu lokien valvonta, tapahtumien analysointi ja poikkeamista ilmoittaminen. Tietoturvaan koulutettu henkilökunta puolestaan valvoo järjestelmiä ja reagoi niiden tuottamaan informaatioon.

Organisaation tietoturvasta voi vastata organisaation tarpeiden ja resurssien mukaisesti tietohallinnon henkilöstöä, jotka hoitavat sivutoimisesti myös tietoturvaa, tai erikseen tietoturvaan keskitetty henkilöstö. Security Operations Center (SOC) eli tietoturvavalvomo, vastaa keskitetysti organisaation kyberturvallisuudesta. SOC voi olla organisaation itsensä ylläpitämä eli paikallinen, tai kolmannelta osapuolelta ostettu palvelu. Valvomosta käsin suoritetaan organisaation tietoturvan valvonta, poikkeamien havainta ja uhkien seuranta (LogPoint, 2020).

7 Lokien monitorointijärjestelmät

Useimpien organisaatioiden tietoverkkoihin on liittyneenä valtava määrä erilaisia laitteita ja ohjelmistoja. Jokaisen laitteen lokitiedostojen yksittäinen tarkistaminen olisi epäkäytännöllistä ja resursseja hukkaava prosessi. Lokienmonitorointijärjestelmät toimivat keskitettyinä lokienkäsittelyohjelmina, jotka keräävät, säilövät ja analysoivat tapahtumatietoja eri lähteistä. Järjestelmiä käytetään manuaalisen lokien auditoinnin apuna, erityisesti rutiininomaisten tehtävien automatisoimiseen (Chapple, Stewart & Gibson, 2018, 688). Keskitetyissä lokienhallintaohjelmissa on myös usein mahdollisuus tietoliikenteen reaaliaikaiseen seurantaan ja poikkeamista hälyttämiseen. Lokienhallintajärjestelmän toimintaa on kuvattu oheisessa kuvassa.

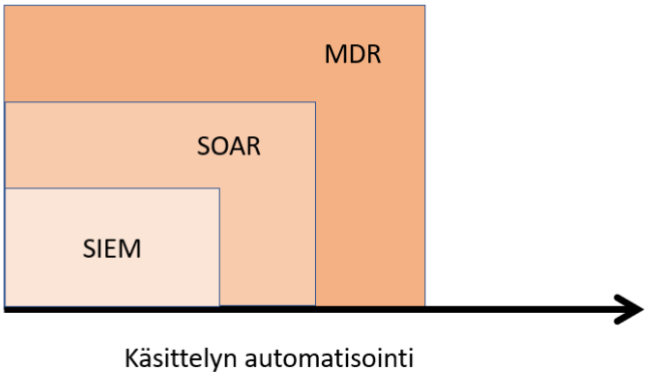
Kuva 3. Keskitetty lokienhallintajärjestelmä (mukaillen Nixu, 2014.)

7.1 SIEM

SIEM (Security Information and Event Management) on termi, jota käytetään ohjelmistoista, joissa yhdistyy kahden erillisen ohjelmiston toiminnallisuus: Security Event Management (SEM) ja Security Information Management (SIM). SIEM-ohjelmistojen avulla pystytään yhdistelemään tapahtumia ja tietoja eri lähteistä. Siten voidaan esimerkiksi nähdä kirjautuminen palomuurin lokista, sekä tarkistaa Windowsin tapahtumalokista, mitä tiedostoja kirjautumisen aikana on muokattu. SIEM-ohjelmistot pystyvät esittämään lokien tapahtumat graafisina näkyminä, mitkä auttavat tilannekohtaisen havainnointikyvyn muodostamisessa. (Nathans, 2014, 13 ja Dulaney & Easttom, 2017, 83.)

SIEM-ohjelmistojen suurimpia vahvuuksia on juurikin mahdollisuus korrelaatioon, eli tietojen yhdistelyyn useammasta lähteestä, jolloin saadaan useista pienemmistä tapahtumista koostettu suurempi tilannekuva. Esimerkkitapauksena korrelaation hyödyistä voidaan pitää seuraavaa kuvitteellista skenaariota: Työntekijän kulkukortti skannautuu aamulla tämän saapuessa töihin. Työntekijän ollessa toimistolla, tämän VPN tunnuksilla pyritään kirjautumaan organisaation verkkoon toimiston sisäverkon ulkopuolisesta IP-osoitteesta. Molemmat tapaukset ovat erillään harmittomia, mutta yhdessä herättävät epäilyksen, ovatko työntekijän tunnukset tai kulkukortti vaarantuneet. (Vacca, 2013, 20.)

Kohdistamattomat lokienmonitorointijärjestelmät voivat aiheettomilla ilmoituksilla heikentää työnkulun tehokkuutta. Hälytyksiä voi kohdistaa lisäämällä SIEM-ohjelmistoon käyttötapauksia. Käyttötapaukset ovat yhdistelmä sääntöjä, sääntöjen välisiä suhteita ja ennalta määritettyjä toimia, joiden mukaan SIEM käsittelee ja tuottaa ilmoituksia. Organisaation omaan ympäristöön kustomoidut hälytykset parantavat kykyä tunnistaa oikeat uhat virheilmoituksista. (Kumar, 2020.)



Kuva 4. Lokitietojen käsittelyn automatisointi

7.2 SOAR

SOAR (Security Orchestration, Automation and Response) on ohjelmistokokonaisuus, joka muistuttaa toiminnallisuudeltaan SIEM-ohjelmistoja siinä, että molempien periaatteena on sisäistää ja analysoida dataa organisaation tietojärjestelmistä ja ulkoisista lähteistä. Suurimpana erona SIEM-järjestelmiin, SOAR-järjestelmät pyrkivät automatisoimaan tietoturvapoikkeamiin reagoinnin, kun taas SIEM-järjestelmät pyrkivät automatisoimaan niiden havainnoinnin. SOAR-järjestelmä tutkii ja kategorisoi tietoturvapoikkeamia ennalta määritettyjen asetusten, sekä koneoppimisen eli aiempien vastaavien tapahtumien perusteella. Järjestelmä pyrkii ratkaisemaan tapauksen itse, tai muussa tapauksessa lähettää sen edelleen tietoturva-asiantuntijalle tarkempaa tarkastelua varten. SOAR-ohjelmistoja käytetään yleisesti osana SOC-ympäristöä yhdessä SIEM:in kanssa työnkulun helpottamiseksi. (Miller, 2019 ja Watts, 2020.)

7.3 MDR

MDR (Managed Detection and Response) on yritysten ja organisaatioiden tietoliikenteen ulkoistamiseen suunnatuista palveluista käytettävä termi. Security-as-a-Service (SaaS) on suunnattu erityisesti organisaatioille, joilla ei ole omia resursseja toteuttaa monitorointia. MDR-ratkaisuissa asiakkaat käyttävät palveluntarjoajan ohjelmistoja omassa toimintaympäristössään. Siten palveluntarjoaja saa tarvittavan datan tietoturvan monitorointiin. (Miller, 2020.)

Tyypillisessä tapauksessa MDR-palvelun tarjoajalla on vuorokauden ympäri toimivia tietoturvavalvomoita, joille asiakas voi ulkoistaa organisaationsa tietoturvan monitoroinnin. SOC:stä käsin palveluntarjoajan tietoturva-asiantuntijoista koostuva tiimi valvoo etänä yrityksen tietojärjestelmiä, käyttäen SIEM- ja SOAR ohjelmistoja tietoliikenteen valvontaan. MDR-palvelut erikoistuvat etenkin normaalista poikkeavien tapahtumien havainnointiin ja tietoturvatapahtumien tutkintaan. (Zhang, 2020.)

8 Haavoittuvuustiedot

Verkossa toimivat rikolliset hyödyntävät uusia haavoittuvuuksia lähes välittömästi niiden tultua julki. Yritysten onkin pystyttävä päivittämään tietojärjestelmiään ja sovelluksiaan lähes reaaliaikaisesti suojautuakseen uusilta haavoittuvuuksilta. (Tietoturvan vuosi 2019, 2020, 6.).

Tietoturvapoikkeamien hallinnoimisessa, aktiivinen viestintä on keskeinen osa havainnointikyvyn kehittämistä. Kyberturvallisuuskeskus kehottaakin kaikkia yrityksiä aktiiviseen tiedonvaihtoon, jolloin kollektiivinen tietoturvallisuuden tilannekuva paranee, kun organisaatiot jakavat tietoa keskenään. (Kyberturvallisuus ja yrityksen hallituksen vastuu, 2020, 18.)

Eri organisaatioiden keskenään jakama haavoittuvuustieto on perusedellytys, kun pyritään nopeuttamaan selvitystyötä, tai ehkäisemään ja pysäyttämään tietoturvauhkien leviäminen organisaatioiden välillä. Kattavan tilannekuvan perusteella on mahdollista kohdistaa tietoturvatoimenpiteet niihin kohteisiin, joissa tietoturvauhkat ovat todennäköisimpiä. (Tietoturvapoikkeamatilanteiden hallinta, 2017, 21.)

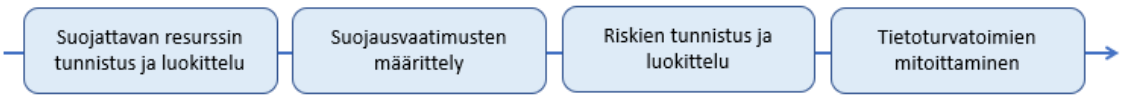
SIEM-ohjelmistoihin on mahdollista yhdistää syötteitä, joiden kautta ohjelmisto saa ajantasaista tietoa uusista tietoturvahaavoittuvuuksista ja uhkista. Esimerkiksi Suomessa, kyberturvallisuuskeskus ylläpitää toimialakohtaisia tiedonjakoon keskittyviä ISAC (Information Sharing and Analysis Centre)-tiedonvaihtoryhmiä. (Kyberturvallisuuskeskus, 2020b.)

9 Tietoturvan toteuttaminen organisaatiossa

Aiemmin tietoturva nähtiin osittain omana kokonaisuutenaan, erillisenä organisaation muusta toiminnasta. Nykyään tunnistetaan, että tietoturvan tulisi olla osa organisaation normaalia toimintaa, sisällytettynä jo suunnitteluvaiheessa sen prosesseihin (Rousku, 2017). Periaatteena voidaan pitää, että organisaation tietoturvan tulisi olla linjassa organisaation omien tavoitteiden, sekä organisaation toimialan asettamien vaatimusten kanssa.

Tietoturvalinjaukset määritellään yleensä osana organisaation tietoturvallisuuden tavoitetilaa. Tietoturvan perimmäisenä tavoitteena on keskeisten toimintojen jatkuvuuden turvaaminen ja toiminnan kannalta oleellisten tietojen suojaaminen. Toimet, joilla organisaatio pyrkii kohti asettamaansa tavoitetilaa, määritellään usein organisaation tietoturvapolitiikassa (Pirinen, 2016). Tietoturvapolitiikka on organisaation sidosryhmille jaettavaksi tarkoitettu dokumentti, johon sisältyvät organisaation tietoturvaan ja tietosuojaan liittyvät määräykset ja toimintatavat.

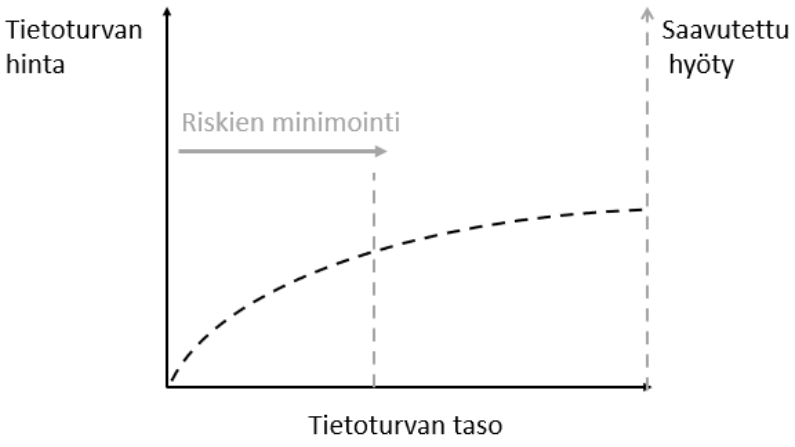
Ennen kuin organisaatio voi suunnitella tietoturvaansa, sen on ensin tunnistettava mitä suojattavia resursseja ja tietoja sillä on, sekä millaista suojausta ne vaativat. Kaikki tieto ei ole saman arvoista. Tietoturvan tason määrittämiseksi tulisi myös selvittää organisaation resursseihin kohdistuvat riskit. Ilman riskien arviointia, on mahdotonta kohdistaa tietoturvaa oikein, tai suunnitella kustannustehokasta tietoturvaa. (Chapple, Stewart & Gibson, 2018, 160 ja Mattsson, 2019.)



Kuva 5. Riskienhallinnan prosessi (mukaillen Mattsson, 2019.)

Tietoturvasta aiheutuvien kustannusten summa voidaan jakaa riskien torjunnasta syntyvien, sekä toteutuneiden eli realisoituneiden riskien liiketoimintavaikutusten perusteella. Tietoturvaan sijoittamista suunnitellessa on arvioitava, kuinka arvokasta suojattava tieto on, sekä millaiset taloudelliset- ja maineelliset tappiot suojausten epäonnistuessa syntyy. Riskienhallinnan avulla pyritään löytämään optimaalinen piste, missä riskien minimoinnin ja realisoituneiden riskien aiheuttamien kustannusten välillä vallitsee tasapaino. (Ranta, 2020.)

Kustannuksia suunnitellessa on hyvä huomata, että tietoturvasta saavutettu hyöty ei ole suoraan verrannollinen suhteessa siihen sijoitetun pääoman kanssa. Tätä suhdetta on kuvannut muun muassa Böhme, laajasti sitatoidussa tutkimuksessaan ”Security Metrics and Security Investment Models” (2010). Julkaisussa vertaillaan aiempien tutkimusten datan perusteella tietoturvaan sijoitettujen kustannusten suhdetta siitä saavutettuihin hyötyihin, jota on havainnollistettu oheisessa taulukossa.



Kuva 6. Kustannustehokkuus tietoturvassa (mukaillen Böhme, 2010.)

10 Toimintojen ulkoistaminen

Ulkoistettujen tietoturvapalvelujen kysyntä kasvaa Suomessa, sillä tarvittavan tietoturva-asiantuntemuksen löytäminen voi osoittautua haasteelliseksi. Vuoden 2020 Digibarometrin mukaan, jopa 60 % suomen kyberturvallisuusalan yrityksistä kokee pulaa kyberturvallisuuden osaajista (Mattila, Mäkäräinen, Pajarinen, Seppälä, Ali-Yrkkö, Tervo & Elias, 2020, 12). FISC:n eli Suomen kyberturva-alan edunvalvontajärjestön keväällä 2020 tuottaman tutkimuksen perusteella, Suomessa on tällä hetkellä pula osaavista kyberturva-alan ammattilaisista. Sopivaa osaamista on vaikea löytää, ja tarvittavan osaamisen omaavista käydään suurta kilpailua. Tilanteessa, jossa asiantuntemusta voi olla vaikea palkata organisaation sisälle, asiantuntemus voidaan päättää ostaa ulkoistettuna.

Lähtökohtaisesti organisaation tulisi selvittää, millaista tieto- ja kyberturvallisuuden asiantuntemusta se tarvitsee onnistuakseen riskienhallinnan tavoitteissaan. Lisäksi on selvitettävä, millaista asiantuntemusta sillä jo on. Vasta tämän jälkeen voidaan selvittää, mitä tarvittavista asiantuntemuksista on mahdollista hankkia organisaatioon sisäiseksi, ja mikä ulkoistettuna. (Kyberturvallisuus ja yrityksen hallituksen vastuu, 2020, 26.)

Palveluiden ulkoistamiseen liittyy paljon tarkkaa suunnittelua ja selvitystyötä. Vaatimusten määrittely on kriittistä, kun harkitaan palveluiden ostamista tai ulkoistamista. Muussa tapauksessa ulkoistaja voi olettaa saavansa palveluita joista ei ole sovittu, tai toimittaja voi veloittaa palveluista joita asiakas ei ole tilannut. (Ranta, 2020.) Vaatimusten määrittelyllä vältytään myös tilanteilta, missä asiakas olettaa tietoturvan olevan kunnossa, koska se on ulkoistettu. Poikkeustilanteen tapahtuessa, palvelun toimittaja voi kuitenkin kuitenkin välttyä sille kuuluvasta vastuusta, jos sopimuksessa ei ole määritelty millaista tietoturvaa siltä on edellytetty. Asettamalla tarkat vaatimukset ja ehdot palveluille hankintavaiheessa, voidaan palveluntarjoajia vertailla kilpailutuksen näkökulmasta paremmin. Siten voidaan myös välttyä lisäkustannuksilta, jos jokin toiminnallisuus onkin otettava käyttöön jälkikäteen. Toimintojen ulkoistamisessa on huomioitava, että kokonaisvastuu säilyy aina organisaatiolla, vaikka toimittaja olisikin vastuussa tuottamistaan palveluista (Tietoturvallisuudella tuloksia, 2007, 51).

Kaikkien osapuolten on oltava selvillä, kuinka velvollisuudet ja vastuut jakautuvat riskien toteutuessa. Organisaatioilla voi olla jo entuudestaan sopimuksia yhteistyöyritysten tai toisten palveluntarjoajien kanssa. Voimassa olevat sopimukset on tarkistettava päällekkäisyyksien tai ristiriitojen varalta aina, kun toimiympäristöön tehdään muutoksia. Sopimuksia tehdessä on myös tärkeää huomioida muut sidosryhmät. Sopimuksissa tulee täsmentää, kenellä on ilmoitusvelvollisuus yhteistöorganisaatioille ja asiakkaille mahdollisen tietoturvatapauksen sattuessa. Palvelun toimittajan on myös vahvistettava, että se pystyy toimimaan yrityksenja

mahdollisesti muiden sidosryhmien tietoturvapolitiikassa määriteltyjen tapojen mukaisesti. (Tietoturvapoikkeamatilanteiden hallinta, 2017, 30.)

11 Yhteenveto

Lähtökohtaisesti tulisi olla selvillä, mihin tietoturvalla pyritään. Hyvä tietoturva voi toimialasta riippuen olla organisaatiolle merkittävä kilpailutekijä. Toisille organisaatioille riittää, että tietoturva täyttää lakien asettamat tietoturvavaatimukset (Mattsson, 2019). Tietoturvan tavoitteet on siis huomioitava, kun pohditaan toteutetaanko tietoturvan monitorointi itse, vai ostetaanko se osittain tai kokonaan palveluna kolmannelta osapuolelta.

Tietoturvan monitorointi paikallisesti voidaan toteuttaa implementoimalla SIEM/SOAR-järjestelmä osaksi organisaation muuta tietoturvaa. Monitorointijärjestelmän lisääminen sellaisenaan ei kuitenkaan riitä, sillä ohjelmisto on ensin integroitava organisaation ympäristöön hyötyjen maksimoimiseksi. F-Securen Hyvärinen (2018) toteaakin blogissaan, että järjestelmän käyttöönotossa menee tyypillisesti yli vuosi, ennen kuin se on saatu kunnolla sisällytettyä osaksi tietojärjestelmiä. Hyvärinen korostaa myös, että ohjelmiston ylläpitoon vaaditaan riittävästi henkilöstöresursseja, tai ohjelmisto ei tuota tarpeeksi hyötyä. Kyseessä ei ole autonominen järjestelmä, vaan tietoturvasta vastaavan henkilöstön avuksi tarkoitettu työkalu, joka tarvitsee asiantuntevaa henkilöstöä käsittelemään sen tulostetta. Hyvin implementoidulla ja ympäristöön integroidulla järjestelmällä on kuitenkin mahdollisuus saada aikaan säästöjä prosessien automatisoinnin parantaessa tehokkuutta. Mahdollisia säästöjä syntyy myös vältyttäessä realisoituneiden kyberuhkien maineellisilta ja taloudellisilta seurauksilta.

Muita paikallisesti toteutetun tietoturvan etuja on se, että organisaation sisäisellä tiimillä on läheinen tuntemus organisaatiosta ja sen toiminnasta. Sisäinen tietoturva pystyy siten reagoimaan nopeammin ja muokkaamaan työtänsä organisaation linjojen mukaiseksi. Tietoturvapoikkeaman sattuessa kommunikointi ja toiminta on nopeampaa, varsinkin jos tietoturvasta vastaava henkilöstö sijaitsee samoissa tiloissa ja pääsee tutkimaan tilannetta paikan päällä. Toisena merkittävänä etuna voidaan pitää sitä, että tieto pysyy organisaation sisällä. Mitä pienemmässä ympyrässä tietoa käsitellään, sitä pienempi riski on tietovuodoille.

Sisäisesti toteutetun tietoturvan haasteena voidaan pitää sitä, saadaanko käytettävissä olevilla resursseilla toteutettua tavoitteita ja vaatimuksia vastaava tietoturvan taso? Tietoturvan kustannuserinä voidaan pitää vähintäänkin asiantuntemuksen palkkausta ja ylläpitoa, työntekijöiden koulutusta, ohjelmistojen ja laitteiden hankintaa ja päivitystä, sekä muita tietoturvasta aiheutuvia jatkuvia kustannuksia. Tietoturvan ulkoistaminen voi olla kannattavaa yrityksille, joilla on käytössään rajalliset resurssit. Siten olemassa olevia IT-

resursseja voidaan vapauttaa organisaation muun toiminnan kannalta olennaisempien prosessien kehitykseen. Tietoturva on jatkuvasti kehittyvä ala, mistä johtuen yrityksenkin tietoturvallisuus on jatkuvan muutoksen alla. Tietoturvan ylläpitämiseen ei riitä yksinään laite- ja ohjelmistohankinnat, vaan on lisäksi pysyttävä ajan tasalla tietoturvan uhkatiedoista ja tilannekuvasta. Vaikka yritys haluaisi huolehtia tietoturvastaan itse, yrityksellä ei välttämättä ole aikaa tai riittävästi omia resursseja tietoturvan ylläpitämiseen.

Ulkoistetut palvelut eivät aina vastaa mukautuvuudeltaan itse toteutettua. Kääntöpuolena suurin osa kyberturvallisuusalan palveluntarjoajien valmiista palveluista on kehitetty tietosuoja-asetukset ja vaatimukset huomioiden, vastaamaan tietoturvan tasoltaan asiakkaiden vaihtelevia tarpeita. Niin kutsutuissa Security-as-a-service (SaaS) tuotteissa, palvelun toimittaja vastaa toimittamansa palvelun ylläpidosta. Tällöin tietoturvan toteuttamiseen vaadittavien resurssien eli asiantuntemuksen palkkauksen ja koulutuksen, laitteiden ja ohjelmistojen, uhkatiedon ja tilannekuvan järjestämisestä vastaa palveluntarjoaja. (Ranta, 2020.)

Vaikka toimittaja on vastuussa toimittamastaan palvelusta, asiakkaalle jää aina maineriski ja vastuu omista tiedoistaan. Kuten aiemmin osoitettiin, rekisterinpitäjällä on viimekädessä vastuu henkilötietojen lainmukaisesta käsittelystä ja siitä, että sen alaiset käsittelijät noudattavat lakia (Hanninen & Laine, 2017, 25). Tässä suhteessa tietoturvapalvelun ostaja on rekisterinpitäjä, ja palvelun toimittaja henkilötietojen käsittelijä.

On varmistettava, että tietoturvaa ulkoistettaessa varotaan tilannetta, jossa itse organisaatioon ei jää riittävästi tietoturvan asiantuntemusta. Koska organisaatio on viimekädessä aina vastuussa, sen sisällä on oltava riittävästi asiantuntemusta suunnittelemaan ja ylläpitämään organisaation tietoturvan tasoa ja vastuiden toteutumista. Lisäksi organisaation tulee pystyä arvioimaan, saadaanko ulkoistetuista palveluista rahoille vastinetta ja toteutuuko sopimuksissa määritellyt vaatimukset. Niin sanotut rutiinitehtävät, kuten lokien hallinta ja poikkeamien havaitseminen voidaan ulkoistaa, mutta tietoturvan kokonaiskuvan on pysyttävä organisaation sisällä. (Kemppainen, 2005.)

Lähteet

Painetut

Ensimmäinen painettu lähde

Sähköiset

Böhme, R., 2010. Security Metrics and Security Investment Models. International Computer Science Institute, Berkeley, California, USA. Viitattu 21.12.2020. https://informationsecurity.uibk.ac.at/pdfs/Boehme2010_SecurityInvestment-IWSEC.pdf

Chapple, M., & Seidl, D., 2020, 46. CompTIA CySA+ Study Guide Exam CS0-002, John Wiley & Sons, Incorporated, Newark.

Chapple, M., Stewart, JM., & Gibson, D., 2018. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide: Certified Information Systems Security Professional: Official Study Guide, John Wiley & Sons, Incorporated, Newark.

Dulaney, E., & Easttom, C., 2017, 83. CompTIA Security+ Study Guide: Exam SY0-501, John Wiley & Sons, Incorporated, Newark.

Euroopan unioni, 2020. Euroopan unionin virallinen verkkosivusto. Yleinen tietosuoja-asetus. Viitattu 14.12.2020. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Evans, D., Bond, P., & Bement, A., 2004. Standards for Security Categorization of Federal Information and Information Systems. National Institute of Standards and Technology, Computer Security Resource Center. https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

Hanninen, M. & Laine, E. 2017. Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset. Kauppakamari. ISBN 978-952-246-483-5.

Hyvärinen, N., 2018. SIEM, EDR or MDR – What is the Right Solution for You? Viitattu 21.12.2020. https://blog.f-secure.com/siem-edr-mdr-right-solution/

Kemppainen, K., 2005. ” Tietoturvan ulkoistus tehtävä harkiten” Viitattu 21.12.2020. https://www.is.fi/digitoday/tietoturva/art-2000001446684.html

Kumar, A., 2020. A Quick Guide to Effective SIEM USE Cases. Viitattu 20.12.2020. https://securityintelligence.com/posts/quick-guide-to-siem-use-cases/

Kyberturvallisuuden sanasto, 2018. Turvallisuuskomitea. Sanastokeskus TSK ry. Huoltovarmuuskeskus. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Kyberturvallisuus ja yrityksen hallituksen vastuu, 2020. Traficomin julkaisuja 2/2020. Traficom Liikenne- ja Viestintävirasto. Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Kyberturvallisuuskeskus, 2020a. Näin keräät ja käytät lokitietoja. Viitattu 21.12.2020. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

Kyberturvallisuuskeskus, 2020b. ISAC tiedonvaihtoryhmät. Viitattu 10.12.2020. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat - Kyberturvallisuuskeskus 2020,

LogPoint, 2020. What is a Security Operations Center (SOC)? Viitattu 21.12.2020. https://www.logpoint.com/en/blog/security-operations-center/

Lokien keräys ja käyttö, 2016. Ohje lokitietojen tallentamiseen ja hyödyntämiseen. Ohje 4/2016. Viestintävirasto. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lokitusohje.pdf

Mattila, Juri – Mäkäräinen, Kalle – Pajarinen, Mika – Seppälä, Timo –Ali-Yrkkö, Jyrki – Tervo, Elias, 2020, 12. Digibarometri 2020: Kyberturvan tilannekuva Suomessa Helsinki: Taloustieto Oy.

Mattsson, J., 2019. Kustannustehokas tietoturva lähtee suojaamisvaatimusten ja riskien tuntemisesta. Viitattu 21.12.2020. https://www.arter.fi/kustannustehokas-tietoturva-lahtee-suojaamisvaatimusten-ja-riskien-tuntemisesta/

Miller, J., 2019. MDR vs. SIEM vs. SOAR Acronyms Explained. Viitattu 21.12.2020. https://www.bitlyft.com/mdr-vs-siem-vs-soar-acronyms-explained/

Nathans, D., 2014, 13. Designing and Building Security Operations Center, Elsevier Science & Technology Books, Rockland, MA.

Nixu, 2014. Tekninen näkökulma: Lokienhallinta vai SIEM? Nixu Oy. 2014 – Julkinen – SIEM seminaari 2014 diaesitys. Viitattu 21.12.2020. https://www.slideshare.net/NixuOy/tekninen-nkkulma-lokienhallinta-vai-siem

Pirinen, A., 2016. Organisaation tietoturvallisuus – lyhyt oppimäärä. Viitattu 21.12.2020. http://www.sytyke.org/tietoturva/organisaation-tietoturvallisuus-lyhyt-oppimaara/

Ranta, J., 2020. Tietoturva ohjelmistokehityksessä – Asiakkaiden tahtotilan ymmärtäminen. Viitattu 21.12.2020. https://www.2ns.fi/tietoturva-ohjelmistokehityksessa-asiakkaiden-tahtotilan-ymmartaminen/

Rousku, K., 2017. Sähköisen asioinnin tietoturvallisuus -ohje. Valtiovarainministeriön julkaisuja 25/2017. Valtiovarainministeriö. Vahti. Julkisen hallinnon ICT. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80012/VM_25_2017.pdf

Tietosuojavaltuutetun toimisto, 2020. Osoitusvelvollisuus. Viitattu 21.12.2020. https://tietosuoja.fi/osoitusvelvollisuus

Tietoturvallisuudella tuloksia, 2007, 51. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. 3/2007. Valtiovarainministeriö. Vahti.

Tietoturvan vuosi 2018, 2019, 5. Traficom. Kyberturvallisuuskeskus. Viitattu 21.12.2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvan_vuosi_%2018_aukeamat.pdf

Tietoturvan vuosi 2019, 2020, 22. Kyberturvallisuuskeskuksen vuosikatsaus. Traficomin julkaisuja 5/2020. Liikenne- ja viestintävirasto. Kyberturvallisuuskeskus. Viitattu 21.12.2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_tietoturvanvuosi_2019_WEB_aukeamittain.pdf

Tietoturvapoikkeamatilanteiden hallinta, 2017. Valtiovarainministeriön julkaisuja 8/2017. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. Valtiovarainministeriö. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79258/VM_8_2017.pdf

Vacca, JR., 2013, 20. Network and System Security, Elsevier Science & Technology Books, Rockland, MA.

Watts, S., 2020. What Is Security Orchestration, Automation, and Response (SOAR)? Viitattu 21.12.2020. https://www.bmc.com/blogs/soar-security-orchestration-automation-response/

YLE, 2020. Yle seurasi Vastaamon tietomurtoa: Näin kiristäjä ilmestyi Tor-verkon foorumille, poliisi pyytää harkintaa asiaan liittyvien yksityiskohtien julkaisemisessa. Viitattu 4.12.2020. https://yle.fi/uutiset/3-11612399

Zhang, E., 2020. What is Managed Detection and Response? Definition, Benefits, How to Choose a Vendor, and More. Viitattu 21.12.2020. https://digitalguardian.com/blog/what-managed-detection-and-response-definition-benefits-how-choose-vendor-and-more

Julkaisemattomat

Ensimmäinen julkaisematon lähde