LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Windows 10 käyttöjärjestelmän tietoturvaominaisuudet

Hovi, Petteri

Laurea-ammattikorkeakoulu

Windows 10 käyttöjärjestelmän tietoturvaominaisuudet

Petteri Hovi
Tietojenkäsittelyn koulutus
Opinnäytetyö
Toukokuu, 2017

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutus
Tradenomi

Petteri Hovi

Windows 10 käyttöjärjestelmän tietoturvaominaisuudet

Vuosi 2017 Sivumäärä 41

Tämän opinnäytetyön tarkoituksena on selvittää Windows 10 käyttöjärjestelmän tietoturvaan liittyviä ominaisuuksia ja kuinka niitä voitaisiin hyödyntää kohteena olevan yrityksen työasemilla. Työn toimeksiantajana toimii suuri suomalainen yritys, joka toimii kahdeksassa eri maassa ja työllistää yli 5000 henkilöä.

Tavoitteena oli tuottaa ratkaisuja sekä suosituksia, mitä Windows 10 käyttöjärjestelmän ominaisuuksia yritys voisi ottaa käyttöön parantaakseen työasemiensa tietoturvaa.

Teoreettinen viitekehys muodostuu tietoturvan tämän hetken ja tulevaisuuden uhkista sekä mahdollisuuksista. Lähteinä toimivat tietoturva-alan kirjallisuus ja internet aineistot.

Tässä tutkimuksellisessa kehittämistyössä lähestymistapana toimi tapaustutkimus, jonka tarkoituksena on tuottaa syvällistä ja yksityiskohtaista tietoa. Menetelminä toimivat dokumenttianalyysi ja ennakointi, joiden avulla hyvin laajasta aineistosta onnistui kriittisesti tarkastelemalla löytämään olennaiset lähteet sekä saamaan näkökulmia aiheeseen.

Työn tuloksena syntyi monta kehitysehdotusta, joiden avulla tietoturvallisuutta voidaan kehittää. Tärkeimmäksi tietoturvallisuutta parantavaksi tekijäksi katson kaikkien työasemien päivittämisen Windows 7 käyttöjärjestelmästä Windows 10 käyttöjärjestelmään. Tämä mahdollistaa uusien tietoturva ominaisuuksien käyttöönottamisen kaikilla yrityksen työasemilla. Toiseksi tärkeäksi kehitysehdotukseksi nostan järjestelmänvalvoja (admin) tasoisten oikeuksien poistamisen kaikilta käyttäjiltä, minkä avulla estetään tehokkaasti haittaohjelmien leviäminen.

Asiasanat:Windows, Tietoturva, Kyberturvallisuus, Työasema

Laurea University of Applied Sciences
Degree Programme in Business Information Technology
Bachelor's Thesis

Abstract

Petteri Hovi

Windows 10 operating system's information security features

Year 2017 Pages 41

The purpose of this thesis was to find out about the information security (InfoSec) features of Windows 10 operating system and how to use them on the workstations of the target company. The work is commissioned by a large Finnish company operating in eight different countries and employing over 5,000 people.

The goal was to produce solutions and recommendations on which Windows 10 operating system features could be used by the company to improve the security of its workstations.

The theoretical framework of this thesis consists of the information about the threats and opportunities on InfoSec now and in the future. The sources that were used are the information security industry literature and the internet material.

In this research development approach, the approach was a case study designed to provide in-depth and detailed information. The methods were document analysis and anticipation that enabled mass of material to be critically examined by looking at relevant sources and getting perspectives on the topic.

As a result of the work, many development proposals were created to develop information security. The most important factor that would improve InfoSec is updating all workstations from Windows 7 to Windows 10 operating system. This enables the introduction of new InfoSec features on all company workstations. Another important development suggestion would be to remove the administrator level rights from all users, effectively preventing the spread of malware.

Keywords:Windows, Information Security, InfoSec, Cyber Security, Workstation

Sisällys

1 Johdanto

Nykyajan yhteiskunnan yksi merkittävistä kulmakivistä on nopealla tahdilla kehittyvä teknologia. Tietotekniikka on kehittynyt huomattavasti niistä ajoista kun vuonna 1981 tuotiin markkinoille ensimmäinen henkilökohtainen tietokone (Personal Computer, PC). 1980-ja 1990-luvuilla palvelut olivat vielä suunniteltu hyvin rajatuille käyttäjäryhmille, esimerkiksi liittyen tiettyjen työtehtävien suorittamiseen tehdyistä teknologisista ratkaisuista on siirrytty kaikkien ihmisten käyttämiin teknologioihin ja varsinkin siirtyminen on vahvasti tapahtunut kohti laajasti vaikuttavia palveluita. 1990-luvun lopussa ja 2000-luvun alkupuolella henkilökohtaisen tietokoneen rinnalle nousi vahvasti matkapuhelin ja vähän myöhemmin älypuhelin. 2010-luvulla mukaan ovat tulleet tabletit sekä erilaiset henkilökohtaiset älylaitteet kuten älykellot. Nyt on alkanut ilmestyä paljon erilaisia verkkoon liitettäviä etänä ohjattavia laitteita ja sensoreita, joiden avulla kerätään tietoa. Näitä laitteita kutsutaan nimellä esineiden internet -laitteet (Internet of Things, IoT). Näiden kaikkien laitteiden ja internetin jatkoksi teknologinen kehitys ajaa vahvasti digitalisaation suuntaan. Rousku (2017, 6) määrittelee, että ”Yleisesti ottaen toiminnan digitalisoiminen tarkoittaa palveluiden kehittämistä käyttäjän ja toiminnan tarpeiden näkökulmasta, alati kehittyvää teknologiaa hyödyntäen.” Monet meistä voivat ajatella, että tietoturvallisuus ei koske itseä, koska ei käsittele tai hallitse mitään sellaista tietoa, jonka joku kokisi kiinnostavaksi tai tarpeelliseksi. Ajatus on väärä, koska jos käytät mitään internetin kautta tarjottavia palveluita oli se sitten töissä, kotona tai missä vaan, niin sinulla on käytössäsi laite sekä muuta tekniikka, jotka jo sellaisinaan ovat tietoturvarikollisille resurssi jota he voivat hyödyntää. Ne voidaan kaapata esimerkiksi rikollisten ylläpitämään bottiverkkoon, jonka avulla toteutetaan rikollisia toimia, laitteesi voi mahdollistaa tietämättäsi pääsyn työpaikan tietojärjestelmiin, josta saadaan taloudellisesti arvokasta tietoa tai pesukonettasi voidaan käyttää osana palvelunestohyökkäystä. Näiden syiden takia tietoturvallisuudesta on tullut alue, joka täytyy huomioida kaikessa toiminnassa. (Järvinen & Rousku 2017.)

Opinnäytetyöni tarkoituksena on tutkia, mitä uhkia kuuluu tämän ajan tietoturvallisuuteen sekä kuinka nämä uhat voivat vaikuttaa yleiseen tietoturvallisuuteen organisaatioissa. Lisäksi tutkin, miten tutkimukseni kohdeyrityksessä voidaan estää näitä uhkia Microsoft Windows 10-käyttöjärjestelmän tietoturvaominaisuuksien avulla.

Tietoturvallisuuteen liittyvien vaatimusten mukaisesti opinnäytetyön kohdeyritys pidetään nimettömänä. Kyseessä on suuri pörssissä toimiva yritys, jonka toiminta-alue on Suomi, Venäjä, Baltia, Tsekki, Slovakia ja Puola. Henkilöstöä yrityksellä on yli 5000 ja liikevaihto yli miljardi euroa.

2 Tavoite

Opinnäytetyön tavoitteena on tuottaa suosituksia ja ehdotuksia Windows 10-käyttöjärjestelmän tietoturvaan liittyvistä mahdollisuuksista, joiden avulla kohdeyrityksen olisi mahdollista parantaa tietoturvaansa tällä hetkellä ja varautua tulevaisuuteen. Tarkoituksena on opinnäytetyön tuloksien perusteella ryhtyä työssä ehdottuihin toimenpiteisiin, joiden toteutukset tullaan päättämään erikseen yrityksen resurssien ja IT strategian mukaisesti. Yrityksen IT strategiassa vuosille 2015-2018 yhtenä keskeisenä toimenpiteenä määritellään tietoturvan parantaminen.

Opinnäytteen tavoitteeseen päästään hakemalla vastaukset seuraaviin tutkimuskysymyksiin:

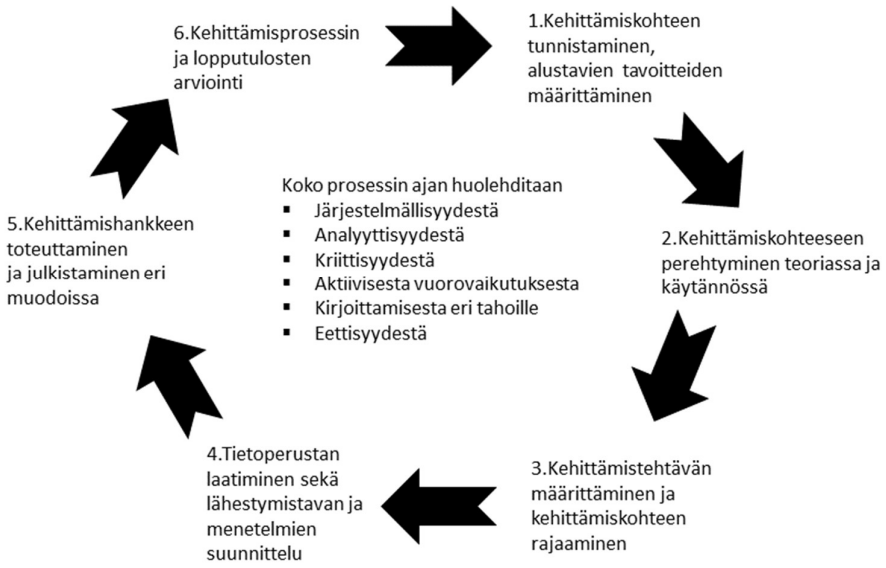
1. Mitä tietoturvaominaisuuksia löytyy Windows 10-käyttöjärjestelmästä?
2. Miten Windows 10-käyttöjärjestelmän ominaisuudet vastaavat tämän hetken ja tulevaisuuden tietoturva uhkiin?
3. Miten nämä selvitetyt tietoturvaominaisuudet voidaan hyödyntää kohdeyrityksessä?

3 Tutkimusmenelmät

Tämä opinnäytetyö on tehty käyttämällä tutkimuksellista kehittämistyötä, jossa korostuvat toiminnallisuus, parannusten hakeminen asiantiloihin sekä ideoiden ja ratkaisuiden toteutettavuuden parantaminen. Tutkimuksellista kehittämistyötä eivät ohjaa pääasiallisesti teoreettiset vaan käytännölliset tavoitteet, joihin saadaan tukea teoriasta. (Ojasalo, Moilanen ja Ritalahti 2014, 17.)

Tutkimuksellisen kehittämistyön tarkoituksena on yleensä liiketoiminnan ja työelämän kehittäminen ja muutoksen aikaansaaminen. Tutkimuksellisen kehittämistyön prosessi etenee vaiheittain. Ensimmäiseksi pitää tunnistaa kehittämiskohde sekä ymmärtää siihen liittyvät tekijät. Kohteen tunnistamisen jälkeen alkaa tiedon hakeminen, siihen liittyvää tietoa haetaan käytännöstä sekä perehtymällä eri teoreettisiin lähteisiin. Seuraavaksi tekijältä vaaditaan kriittisyyttä ja kykyä tehdä valintoja sekä yhdistellä asioita, tarkoituksena olisi löytää selvä näkökulma, jonka mukaan työssä edetään. Tietoperusta on olemassa olevaa kirjoitettua tietoa, minkä avulla työn suunnittelu ja toteuttaminen tapahtuu. Sitten kohteena olevasta organisaatiosta ja toimintaympäristöstä jo kootun tiedon avulla määritetään kehittämistehtävä ja rajataan kehittämisen kohde. Tämän jälkeen pystytään kuvaamaan työhön liittyvät prosessit sekä suunnittelemaan miten lähestyä aihetta menetelmien avulla. Seuraavaksi tulee työn toteuttaminen ja jakaminen, johon olisi tärkeää varata aikaa ja resursseja, koska tavoitteena

kehittämistyössä on tuottaa hyödyllisiä muutoksia työelämään. Viimeisenä vaiheena tulee kehittämistyön arviointi, jonka avulla on tarkoitus osoittaa kuinka työssä onnistuttiin ja sen pätevyys edellyttää tavoitteiden, panosten sekä prosessien ja aikaansaannosten tunnistamista ja kuvaamista. (Ojasalo ym. 2014.)



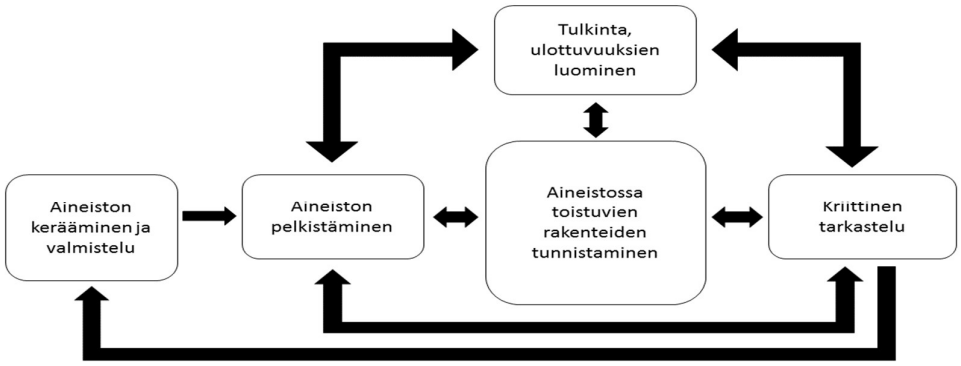
Kuvio 1: Tutkimuksellisen kehittämistyön prosessi (Ojasalo ym. 2014).

Opinnäytetyöni tarkoituksena on tuottaa kehittämisehdotuksia ja siihen sopii hyvin lähestymistavaksi tapaustutkimus, koska sen pyrkimyksenä on tuottaa syvällistä ja yksityiskohtaista tietoa tutkittavasta tapauksesta. Siinä ei ole tarkoituksena viedä muutosta eteenpäin tai kehittää mitään todellista vaan luoda ideoita tai ehdotuksia, joilla mahdollinen ongelma voidaan ratkaista. (Ojasalo ym. 2014.)

Menetelmiksi valikoituvat dokumenttianalyysi ja ennakointi. Dokumenttianalyysin avulla ilmiöille saadaan kerättyä taustatietoa sekä eri näkökulmia. Siinä pyritään saattamaan päätelmät kirjalliseen muotoon aineistoista, joita voivat olla esimerkiksi www-sivut, artikkelit, muistiot, valokuvat, puheet, raportit ja blogit. (Ojasalo ym. 2014.)

Alla olevassa kuvassa on mallinnettu, kuinka dokumenttianalyysin aineiston valmistelun prosessi etenee. Aineiston keräämisellä ja valmistelulla tavoitellaan sitä, että aineisto on selkeä ja analysointi voidaan tehdä sen pohjalta. Esimerkkinä jokaiselle analysoitavalle www-sivulle ja alasivulle annetaan numero tai kirjainkoodi, johon voidaan helposti viitata myöhemmässä

vaiheessa. Tässä vaiheessa on tärkeää suunnitella hyvä arkistointitapa sekä tallentaa ja jaotella aineisto eri tiedostoiksi. Aineiston analysointia ja pelkistämistä voidaan tehdä teoriaohjaavasti, aineistolähtöisesti tai teorialähtöisesti. Esimerkkinä mitä aineistolähtöisellä sisällönanalyysillä tarkoitetaan. Sen tarkoitus on kuvata sisältöä sanallisesti ja selkeästi. Analyysin avulla aineisto pyritään järjestämään selkeään ja tiiviiseen muotoon. Sisällönanalyysiin kuuluvat: aineiston pelkistäminen, ryhmittely ja abstrahointi. Pelkistämisen avulla on tarkoitus tehdä aineisto tiiviimmäksi ja selkeämmäksi, joka tarkoittaa sitä että runsaasta ja monipuolisesta aineistosta on pyrkimyksenä rajata ja tunnistaa pieni määrä näkökulmia. Klusteroinnin eli ryhmittelyn avulla käydään alkuperäisaineisto tarkasti läpi ja sieltä etsitään samankaltaisuuksia ja eroavaisuuksia kuvaavia käsitteitä. Käsitteet, jotka tarkoittavat samaa asiaa ryhmitellään ja yhdistetään luokaksi sekä annetaan nimi, joka kuvaa sisältöä. Abstrahoinnilla tarkoitetaan oleellisen tiedon erottamista tutkimuksen kannalta ja sen perusteella muodostetaan teoreettinen käsitteistö. Näiden käsitteiden avulla tutkija muodostaa kuvauksen tutkimuskohteesta ja vertaa teoriaa sekä johtopäätöksiä koko ajan alkuperäisaineistoon muodostaessaan uutta teoriaa. (Ojasalo ym. 2014.)



Kuvio 2: Laadullisen tutkimuksen yleinen malli (Ojasalo 2014).

Toinen menetelmäni on ennakointi (foresight). Siihen kuuluvat tulevaisuutta koskevan tiedon tuottaminen, hankinta, käsittely, muokkaus, analysointi ja raportointi. Varsinkin IT-alalla muutosvauhti on niin nopeaa, että on tärkeää yrittää ennakoida, mihin kehitys on menossa. Ennakoinnin avulla pyritään hahmottamaan, mikä on mahdollista tulevaisuudessa ja miten siihen voidaan varautua. (Ojasalo ym. 2014.)

Megatrendi- ja trendianalyysi on ennakoinnin menetelmä, jota voidaan kutsua monitoroinniksi eli muutosten tarkasteluksi toimintaympäristössä ja sen avulla pyritään selvittämään prosesseja ja kehityskulkuja, silloin kun ne tapahtuvat tai heti sen jälkeen, jotain niiden aiheuttamaa on tapahtunut (Rubin 2017).

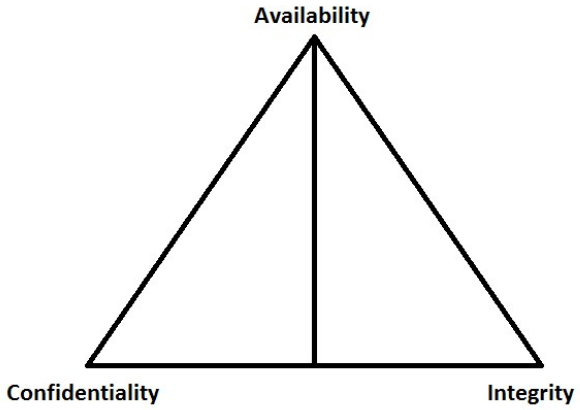
Alla olevassa taulukossa on määriteltynä megatrendien ja trendien tunnistamiseen vaikuttavia tekijöitä. Lisäksi tarkasteltavaksi olisi hyvä huomioida analyysin tilaajan tarpeet ja toiveet sekä selvittäminen kenen tavoitteita tutkimus palvelee. Esimerkiksi tietoturvallisuuden ilmiöiden näkökulmat ovat varmasti erilaiset organisaatioiden johtajien mielestä kuin vaikkapa tetharjoittelijan (työelämääntutustuja) näkökulmasta. Megatrendien ja trendien määrittämiseen vaikuttavat erilaiset tekijät sen määrittelijän omassa yhteiskunnallisessa missä listauksia ja analyysejä tehdään sekä mistä näkökulmasta niitä tarkastellaan. (Rubin 2017.)

Tekijät	**Piirteet**
Henkilökohtaiset	Tekijän omat kiinnostuksen kohteet, arvot, kognitiivinen tyyli, ilmaisukieli ja tavallisimmin käytetyt ilmaukset
Institutionaaliset	Asema, toiminnan orientaatio (kaupallinen, ei-kaupallinen, eturyhmä tms.)
Ammatilliset	Koulutus, asiakkaat, tieteentraditio, tieteellinen paradigma
Metodologiset	Lähestymistapa, menetelmät, kerätyn tiedon luonne
Kulttuuriset	Kansallisuus, rotu ja etninen tausta, uskonto, historia
Ideologiset	Poliittinen, maailmankuvallinen tietämisen tapa (länsimainen, ei-eurooppalainen, tms.)
Tutkimuksen alue/taso globaalissa järjestelmässä	Instituutio, alue, valtio, maanosa, maapallo; toiminnan alue
Analyysin alue	Tapahtumat, käytännöt, ilmiöt, käsitykset, kehityskulut
Analyysin luonne	Kriittinen, teknologialähtöinen, positivistinen tms.

Kuvio 3: Megatrendien ja trendien tunnistamiseen vaikuttavia tekijöitä (Rubin 2017).

4 Tietoturva

Tietoturvallisuutta voidaan lähteä määrittelemään kolmen käsitteen avulla: Luottamuksellisuus, eheys ja saatavuus. Nämä käsitteet muodostavat mallin, joka tunnetaan nimellä CIA-malli (confidentialy, integrity ja availability). Tämä malli on toiminut monta vuosikymmentä ytimenä tietojärjestelmien turvallisuuden suunnittelussa. Tiedon luottamuksellisuudella tarkoitetaan yksityisyyden säilymistä, eli tiedot ovat vain niiden saatavilla kenelle ne on tarkoitettu ja tietoja ei saa paljastaa ulkopuolisille. Eheydellä tarkoitetaan tilaa, jossa tiedot ovat virheettömästi ja yhtenäisesti ylläpidetty ellei valtuutettuja muutoksia ole tehty. Tiedon tallennuksessa, siirrossa ja käytössä ei ole tapahtunut muutoksia. Käytettävyys on tilanne, jossa tieto on tarvittaessa saatavilla kun sitä tarvitaan. (Panmore Institute 2017.)



Kuvio 4: CIA-malli (Saltzer & Schroeder 1975).

Edellisten käsitteiden lisäksi nykyaikaisessa tietoturvatutkimuksessa ja -käytännössä käytetään vielä ”kolmea A:ta”: assurance, authenticity, anonymity.

Varmuus (Assurance) etsii vastausta kysymykseen; voimmeko luottaa siihen, että järjestelmät sekä ihmiset toimivat kuten oletetaan? Varmuuden määritelmä on tapa, jolla luottamus on tuotettu sekä hallittu järjestelmissä. (Argiento 2013.)

Luottamuksen voidaan ajatella syntyvän seuraavistä tekijöistä. Politiikat ovat määritelmiä kuinka järjestelmien ja ihmisten tulisi toimia. Käyttöoikeudet ovat kuvauksia teoista, joita järjestelmät ja ihmiset on sallittu suorittaa. Suojaukset ovat tapoja, joilla vahvistetaan politiikat sekä käyttöoikeudet. (Argiento 2013.)

Autenttisuus (Authencity) tarkoittaa määritelmänä sitä, jonka avulla varmistetaan että järjestelmiltä sekä ihmisiltä tulevat käskyt, politiikat ja käyttöoikeudet ovat aitoja. Kiistämättömyys kuuluu osana autenttisuuteen, jolla tarkoitetaan tapaa varmistaa esimerkiksi sopimuksen aitous. Autenttisuus ja kiistämättömyys saavutetaan digitaalisella allekirjoituksella. Digitaalisilla allekirjoituksilla voidaan myös saavuttaa eheys (integrity). (Argiento 2013.)

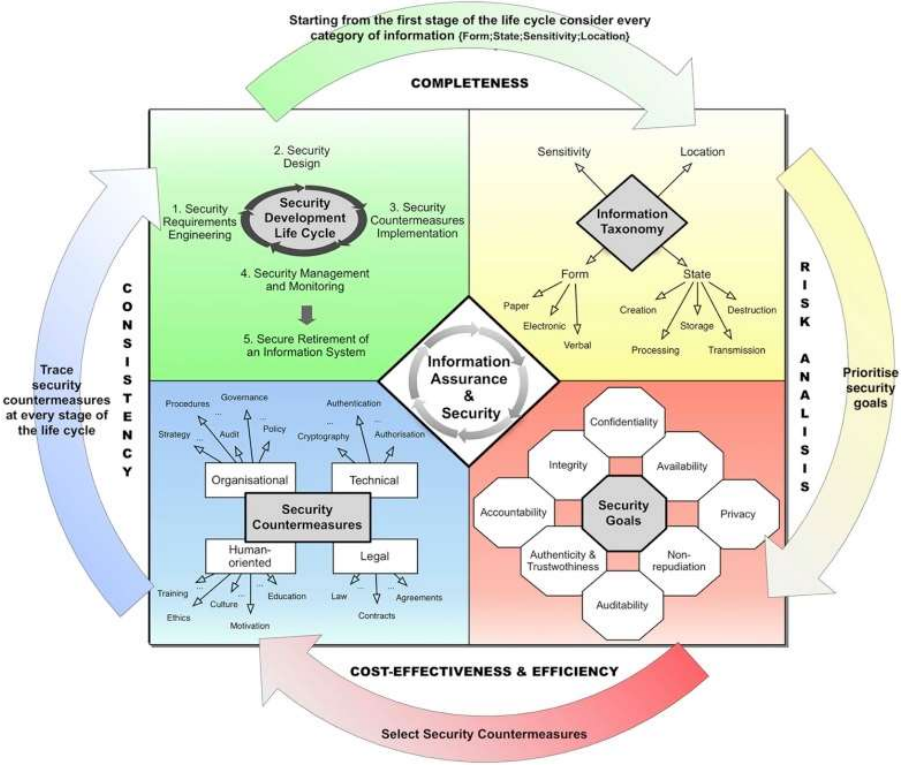
Anonymiteetti (Anonymity) tarkoittaa ihmisen identiteetin pitämistä piilotettuna. Identiteetti on vahvasti sidottuna moneen järjestelmään mitä käytämme, esimerkiksi sähköpostiin, sairauskertomuksiin ja korttiostoksiin. Anonymiteetti voidaan saavuttaa näillä tavoilla. Koostaminen (aggregation) tapahtuu yhdistelemällä tietoa useasta yksilöstä, joista julkaistaan vain keskiarvoja tai summia jolloin yksilöitä ei voida erottaa. Sekoittamalla (mixing) satunnaisesti yhdistelemällä eri jonot transaktiosta, informaatiosta ja kommunikaatiosta, josta voidaan esimerkiksi tehdä hakuja, mutta ei pystytä tunnistamaan yksilöä. Sovellustason välimuisteilla (proxies) luodaan luotettuja agentteja, jotka tekevät toimia henkilön puolesta,

jolloin sitä ei voida yhdistää yksilöön. Nimimerkeillä (pseudonyms) luodaan vale identiteetit, joita käytetään verkko kommunikaatiossa ja vain luotettu taho tietää todellisen identiteetin. (Argiento 2013.)

Tämän hetken yhtenä parhaimmista tietoturvaa selittävistä ja kuvaavista malleista voidaan pitää RMIAS-mallia (Reference Model of Information Assurance and Security), johon on kerätty yhteen paljon erillistä tietoa laajan asiantuntija joukon avulla. Se korostaa kokonaisvaltaista lähestymistapaa tietoturvaan ja mallin perusta löytyy CIA kolmiosta. (Cherdantseva & Hilton 2016.)

Mallissa on neljä eri ulottuvuutta, jotka ovat:

- Turvallisuuden kehittymisen elinkaari (Security Development Life Cycle), kuvaa informaation turvallisuuden elinkaaren.
- Informaation luokittelu (Information Taxonomy), kuvaa tavat jolla informaatiota suojataan.
- Turvallisuuden tavoitteet (Security Goals), listaa yleisesti yhteensopivat turvallisuus tavoitteet.
- Turvallisuuden vastatoimet (Security Countermeasures Dimensions), kategorioi eri vastatoimet, jotka ovat saatavilla informaation suojaamiseksi.



Kuvio 5: RMIAS-malli (Cherdantseva & Hilton 2013).

Mallin avulla organisaatiot pystyvät luomaan informaation turvallisuuteen liittyvän toimintapa dokumentin (Information Security Policy Document, ISPD). Mallissa yhden ulottovuuden elementit tulee aina yhdistää kaikkiin elementteihin ja niiden ulottuvuuksiin, jotta voidaan luoda kattava lista olosuhteista, joissa informaatio tarvitsee suojaamista. Tällä tavoin varmistutaan siitä, että toimintapa ohjeistus vastaa kaikkiin riskinä pidettäviin olosuhteisiin. (Cherdantseva & Hilton, 2016.)

4.1 Tietoturvauhkat ja trendit

Nykyään on selvää, että jokaiseen meistä kohdistuu tietoturvaan liittyvä uhka, jossa suurimpana motivaation lähteenä on rahastaminen. Vuosi 2016 voidaan nähdä kyberrikollisuuden rahastamisen tehokkuuden vuotena. Samanlainen trendi näyttäisi myös jatkuvan tulevaisuudessa. (ENISA 2016.)

Megatrendeiksi nostavat (Lehto, Limnéll, Innola, Pöyhönen, Rusi & Salminen 2017) raportissaan kiristyshaittaohjelmien kasvun, haavoittuvuuksien hyödyntämisen, laitteistoihin kohdistuvat uhkat, yrityksen sisäpiirin hyökkäyskanavana, liiketoiminnan tuhoamiseen tähtäävät hyökkäykset ja henkilötietojen varastamiseen tähtäävät hyökkäykset.

McAfeen mukaan tietoturvallisuuden suurimmat tulevaisuuden uhat ovat: teollistuva hakkerointi, alati laajeneva kyberhyökkäysala, IT markkinoiden monimutkaisuus ja hajautuneisuus liittyen tietoturvaan. Ennustuksissa nähdään tulevaisuudessa yhä laajeneva kyberhyökkäysala, hyökkääjien kehittyminen, tietovuotoihin liittyvä kustannusten nousu, tietoturvateknologioiden yhteensopivuuden puuttuminen ja kyvykkäiden tietoturvaosaajien puuttuminen.
AT&T nostaa arvioissaan tulevaisuuden viisi keskeistä aluetta, joissa voi syntyä paljon uusia mahdollisuuksia kyberhyökkääjille. Ne ovat esineiden internet, pilvipalvelut, Big Data, mobiliteetti ja BYOD (Bring Your Own Device). (Lehto ym. 2017.)

4.2 Suurimmat uhkat

ENISA on listannut top 15 uhkaa vuodelta 2016 ja mikä on niiden kehitys suunta tulevaisuudessa. Aineisto on kerätty joulukuun 2015 ja joulukuun 2016 välisenä aikana.

	Uhkat 2016	Trendi
1	Haittaohjelmat	↑
2	Verkossa tapahtuvat hyökkäykset	↑
3	Verkkosovellus ja –palvelu hyökkäykset	↑
4	Palvelunestohyökkäykset	↑
5	Bottiverkot	↑
6	Tietojen kalastukset	→
7	Roskapostit	↓
8	Kiristyshaittaohjelmat	→
9	Sisäpiirin uhkat	→
10	Fyysinen manipulaatio, vahingoittaminen, varkaus ja katoaminen	↑
11	Exploit kits	↑
12	Tietomurrot	↑
13	Henkilötietovarkaudet	↓
14	Informaation vuodot	↑
15	Kybervakoilu	↓

Kuvio 6: TOP 15 Kyberturvallisuus uhat 2016 (ENISA 2016).

Tietotekniikan termitalkoot (2005) määrittelevät, että haittaohjelmat aiheuttavat koneen käyttäjän kannalta ei toivottuja tapahtumia tietojärjestelmässä tai sen osassa. Haittaohjelmia ovat esimerkiksi virukset, madot ja troijanhevoset sekä näiden yhdistelmät.

Haittaohjelmat ovat jo toisen vuoden putkeen suurin tietoturvallisuus uhka. Haittaohjelmien kokonaislukumäärä on jo ylittänyt selvästi 600 miljoonan rajan. Vuonna 2016 mobiili haittaohjelmien kasvu on ollut merkittävää. Kasvu vuodesta 2015 on ollut noin 150 prosenttia. (McAfee 2016.)

Haittaohjelmien kaksi tärkeintä kiinnostuksen kohdetta ovat olleet tietojen varastaminen ja kiristysohjelmat. Hyvin laaja kiristysohjelmien lisääntyminen on kiinnittänyt myös monien eri toimijoiden huomion, jotka toimivat uhkien kanssa. (FBI 2016; AO Kaspersky LAB 2016.)

Verkossa tapahtuvat hyökkäykset käyttävät verkkokomponentteja hyökkäys alustana. Verkkokomponenteilla tarkoitetaan verkkoinfrastruktuuria, kuten verkko-palvelimet, verkkoselainten sisällön hallinta järjestelmät (CMS) ja verkkoselainten laajennukset. CMS järjestelmien vääränlainen käyttö (asennus, konfigurointi ja ylläpito) näyttää olevan lähteenä hyvin suurelle osalle verkkohyökkäyksiä. (Sucuri Inc. 2016.)

Selainten haavoittuvuuksia pyritään myös käyttämään hyökkäyksien kohteena laajamittaisesti. Vuonna 2016 suurin osa hyökkäyksistä kohdistui Internet Explorer-selaimeen, toisena oli Chrome-selain ja tämän jälkeen Safari- sekä Mozilla-selain. (Symantec Corporation 2016.)

Verkkosovellus ja -palvelu hyökkäyksistä löytyy tiettyjä päällekäisyyksiä verrattuna kohtaan ”Verkossa tapahtuvat hyökkäykset”. Joitakin hyökkäyksiä verkkosovelluksia ja -palveluita kohtaan voidaan tehdä hyödyntämällä verkkoinfrastruktuurin haavoittuvuuksia. Hyökkäykset verkkosovelluksia ja -palveluita kohtaan ovat lisääntyneet vuonna 2016 noin 15 prosentilla verrattuna vuoteen 2015. Uhkaa voidaan pitää suurimpana organisaatioita kohtaan. (CyberEdge Group 2016; WhiteHat Security 2016.)

Suurin osa tietomurroista johtuu verkkosovelluksista vaikka kokonaismäärältään suurin osa hyökkäyksistä eivät kohdistu niihin (Verizon Enterprise 2016).

Tietotekniikan termitalkoot (2014) määrittelevät, että palvelunestohyökkäykset ovat verkkohyökkäys, jossa pyritään lamaannuttamaan jokin palvelu tai tietojärjestelmä. Palvelunestohyökkäys voi esimerkiksi lamaannuttaa sähköpostin suurella määrällä sähköpostiviestejä taikka palvelimen tai reitittimen liian suurella määrällä palvelupyyntöjä.

Vuonna 2016 palvelunestohyökkäykset ovat lisääntyneet jokaisella eri järjestelmien ja sektorien osa-alueella (Akamai Technologies 2016).

Palvelunestohyökkäyksien päätarkoitus on ollut kiristäminen, palveluiden ja infrastruktuurin alasajo ja lopuksi tietomurto (Metropolitan.fi 2016).

Vuonna 2016 tapahtuneet suuret palvelunesto hyökkäykset ovat saaneet monet huolestumaan siitä, että ne voivat aiheuttaa uhan koko internetille (Ars Technica 2016).

Bottiverkot määritellään tietotekniikan termitalkoiden (2008) mukaan, että ne ovat kaapatuista tietokoneista muodostuva verkko, jota sen haltija käyttää huomaamattomasti haitallisiin tai laittomiin tarkoituksiin. Bottiverkkoa voidaan käyttää esimerkiksi hajautettuihin palvelunestohyökkäyksiin, roskapostien lähettämiseen, käyttäjätietojen keräämiseen vakoiluohjelmien avulla tai verkkourkintaan. Bottiverkon haltija voi käyttää verkkoa itse tai myydä sen käyttöoikeuksia esimerkiksi roskapostittajille. Bottiverkkoon kuuluvat tietokoneet ovat yhteydessä komentopalvelimeen, jonka kautta niiden toimintaa ohjataan. Botti-sana on lyhennetty muoto sanasta robotti.

Ottaen huomioon bottiverkkojen luonteen ne ovat pääasiallinen työkalu, joita on käytetty moninaisiin hyökkäyksiin vuonna 2016. Suurin nousu tapahtui IoT bottiverkoissa, varsinkin palvelunestohyökkäyksiin käytettyinä. Kuten mobiilialustat olivat muutama vuosi sitten, näyttäisi siltä että IoT on seuraava alusta jolle tietoturva uhat siirtyvät. Kuten suurimmalle osalle tietoturvauhkista on tyypillistä rahastaminen myös bottiverkkojen tärkein ajuri. (Mimoso 2016.)

Bottiverkkoja voidaan myös käyttää tiettyjen kohde ryhmien uhkaamiseen. Esimerkkinä tästä voidaan käyttää Jaku bottiverkkoa, joka iski moniin kansainvälisiin organisaatioiden työntekijöihin vuosina 2015-2016. Uhrien kokonaismäärä on arvioitu olevan noin 19000 henkilöä. (Settle, Dey, Griffin & Toro 2016.)

Tietojen kalastukset ovat käyttäjän manipuloinnin muoto, jossa pyritään sähköpostin tai verkkosivun välityksellä saamaan luottamuksellista tietoa. Verkkourkinta voi tapahtua esimerkiksi niin, että käyttäjältä pyydetään pankin nimissä sähköpostitse luottokortin numero ja tunnusluku. (Tietotekniikan termitalkoot 2012.)

Vaikka lukumääräisesti tietojen kalastelu yritykset eivät ole kasvaneet, niin laadukkuus ja käyttötavat kohdistaa uhka oikeaan uhriin ovat parantuneet. Sosiaalisesta mediasta löytyvää tietoa hyväksikäytetään ja tietojenkalastelu on myös hyvin suuressa roolissa kiristysohjelmien käytössä. Huomattavaa on myös, että tietojenkalastelu on saavuttanut johtaja tason ja näiden johdosta yritykset ovat kärsineet mainittavia tappioita. (Europol 2016; Fadilpasic 2016; KrebsonSecurity 2016.)

Käyttäjiltä mitattuna kuinka he pärjäävät tietojenkalastelu viestien kanssa, 30 prosenttia viesteistä on avattu keskimäärin, 12 prosenttia ovat avanneet tai klikanneet liitettyä tiedostoa/linkkiä ja ovat näin aiheuttaneet tartunnan järjestelmään. Molemmat numerot ovat suurempia kuin aiempina vuosina, vaikka voisi ajatella että ne olisivat pienentyneet koska käyttäjät ovat tulleet varovaisimmiksi. Selityksenä voi toimia tietojen kalastelijoiden suurempi tehokuus ja keinot, jonka avulla pystytään huijaamaan käyttäjiä. (Verizon 2016.)

Roskapostit ovat vastaanottajan kannalta ei-toivottu keskustelupalsta- tai sähköpostiviesti, joka usein lähetetään mainostarkoituksessa suurelle vastaanottajajoukolle yhdellä kertaa. Roskapostia saatetaan lähettää myös häirintätarkoituksessa. (Tietotekniikan termitalkoot 2010.)

Rospostien määrä on ollut jatkuvassa laskusuhdanteessa vuodesta 2013 alkaen vähentyen 85 prosentista 55 prosenttiin sähköpostien kokonaismäärässä laskettuna. Vaikka kokonaismäärä on ollut laskussa, niin roskaposti silti kukoistaa hyökkäyksien alkuunpanijana, monesti esimer-

kiksi tietojenkalastelu viestit lähetetään roskapostina ja ne ovat ensimmäiset askeleet onnistuneille hyökkäyksille. Laatu ja tehokkuus on selvästi parantunut roskapostien osalta ja ne ovat edelleen useimmin käytetty menetelmä tietoturva rikollisten parissa tavoittaa uhrit. (Kaspersky Lab 2016; Lang 2016; Symantec 2016.)

Kiristyshaittaohjelmat ovat haittaohjelmia, jotka salaavat tietokoneella olevia tietoja ja vaatiivat käyttäjältä lunnaita salauksen purkamisesta. Kiristysohjelma voi tulla tietokoneeseen esimerkiksi sähköpostin liitetiedostona. Kun käyttäjä avaa liitetiedoston, kiristysohjelma latautuu koneelle, minkä jälkeen ohjelma esimerkiksi muuntaa joitakin tiedostoja salakirjoitettuun muotoon. Näitä tiedostoja ei voi avata ilman oikeaa salauksenpurkuavainta. Kiristysohjelman tekijä lupaa toimittaa avaimen lunnaita vastaan. (Tietotekniikan termitalkoot 2016.)

Kaikista tietoturva uhkista vuonna 2016 kiristysohjelmat ovat lisänneet kasvuaan kaikissa kategorioissa: kampanjojen lukumäärässä, uhrien lukumäärässä, lunnaiden maksamisessa keskimäärin, edistyksellisten tartuttamis tapojen käytössä, vahinkojen syvyydessä ja kyberrikollisten liikevaihdon lisäämisessä. Vuonna 2016 odotetaan että kiristämisellä ja lunnailla saatu liikevaihto saavuttaa yhden biljoonan dollarin rajan. Kuten monissa kyberrikollisuuden toimissa, kryptovaluutat ovat johtaneet tähän kehitykseen tarjoamalla lähes anonyymit tavat rahastaa lunnailla. (Cheung 2016; Wolff 2016.)

Kiristysohjelma perheiden määrä on lisääntynyt vuoteen 2015 verrattuna 46 kappaleella. Niiden toimintatavoissa ja moninaisuudessa on tapahtunut selkeä parannus. Päätoimintatapaan liittyvät parannukset aiheuttavat kokonaisvaltaista vahinkoa tiedostoille mukaanlukien varmuuskopiot; lisää kohdistettua vahinkoa tietyille tiedosto tyypeille (esimerkiksi tietokanta tiedostot, verotukseen liittyvät tiedostot, verkkosivut); hyväksikäyttää käyttäjien haavoittuvuuksia lisätäkseen tartuntojen määrää; salaukset tartutetuille koneille enemmän huomaamattomia. (Trendmicro 2016; Spring 2016.)

Sisäpiiristä tuleva uhka on monissa tutkimuksissa osoitettu, että sen kautta tuleva vaara on hyvin todennäköinen. Tiedetään esimerkiksi että tahattomasti aiheutettu uhka käsittää merkittävän osan rekisteröidyistä tapauksista, noin 50-60 prosenttia. Huolimattomuus on toinen syy, jonka seurauksena sisäpiiriläiset aiheuttavat uhkia. Vaikka ne eivät olisi tahallisesti aiheutettuja, niin niiden aiheuttavat vuodot ovat vaikeasti havaittavia. (Crowd Research Partners 2016.)

Viisi eniten tunnistettua tapausta ovat: käyttöoikeuksien väärinkäyttö (noin 60 prosenttia), tiedon huono käsittely (noin 13 prosenttia), ei hyväksyttyjen laitteiden käyttö (noin 10 pro-

senttia) ja sopimattomien ohjelmien käyttö (noin 10 prosenttia). Suurimpana motiivina on rahallisen edun tavoittelu noin 50 prosentissa varmistetuissa sisäpiiri tapauksissa, vakoileminen on toisena noin 30 prosentin osuudella. (Virtru 2016.)

Fyysistä manipulaatiota, vahingoittamista, varkautta tai katoamista pidetään yhtenä pääsyynä tietomurroissa. Kokonaismäärältään tieto murroista ja tiedon vuotamisesta noin 40 prosenttia johtuu laitteiden häviämisestä, kuten kannettavat tietokoneet ja usb-tikut. (McAfee 2016.)

Exploit kits on verkossa toimiva sivusto, minkä tavoitteena on saastuttaa sivustolla vierailija haittaohjelmalla. Sitä voidaan nimittää siis haittaohjelmanjakelualustaksi. (Viestintävirasto 2015.)

Exploit kittien päätarkoituksena on havaitsemisen välttäminen. Yksi kuuluisa exploit kit on Angler ja sen toimintavoista on tehty tarkkaa tutkimusta. On väitetty, että sen kehittäjät ovat matkineet toimintapoja muista jo olemassa olevista työkaluista, kuten muista exploit kiteistä. On myös esitetty, että Angler olisi tuottanut tekijöilleen yli 60 miljoonaa dollaria. (Talos 2015.)

Tietomurrot ovat tunkeutumista suojattuun tietojärjestelmään tai suojatussa tietojärjestelmässä olevan tiedon oikeudetonta tarkastelua (Tietotekniikan termitalkoot 2009).

Tietomurrot ovat kasvaneet vuonna 2016 noin 25 prosenttia korkeammaksi, kuin vuonna 2015. On hyvä myös tiedostaa, että tietomurtoja yleensä tehdään sen vuoksi, että voidaan tehdä lisää murtoja. Tämä johtuu siitä, että suurin osa murretuista tiedoista käsittää yleensä käyttäjätunnuksia. Yli 20 prosenttia murroista on tehty käyttämällä varastettuja käyttäjätietoja. Murron teon ja sen havaitsemisen välinen aika on selvästi lisääntynyt myös vuonna 2016, se osoittaa hyökkäysten tehokkuutta, että noin 90 prosenttia rikkomuksista tapahtuu sekuntien ja minuuttien sisällä kun taas murtojen havaitseminen samassa ajassa tapahtuu vain 25 prosentissa tapauksia. (Verizon 2016.)

Henkilötietovarkaudet ovat toisen ihmisen henkilötietojen tai muiden luottamuksellisten tietojen luvaton haltuunotto ja käyttäminen taloudellisen tai muun hyödyn saamiseksi. Henkilötietovarkaus voidaan tehdä esimerkiksi ottamalla selville toisen ihmisen henkilötunnus tai luottokortin numero ja käyttämällä niitä ostosten tekemiseen verkkokaupoissa. Henkilötietovarkaat voivat poimia luottamuksellisia tietoja esimerkiksi roskiin heitetyistä papereista, tietokannoista tai pankkiautomaatteihin ujutetuista lukulaitteista. (Tietotekniikan termitalkoot 2013.)

Informaation vuodot ovat uhkia, jotka kohdistuvat siihen, että hyväksikäytetään komponenttien konfigurointi heikkouksia, ohjelmointivirheitä sekä käyttäjien tapaa toimia. Informaatio vuoto voi tapahtua millä tahansa komponenttien tasolla, laitteistosta ohjelmistoihin ja palveluihin. SSL/TLS protokollaa vastaan tehdyt hyökkäykset ovat hyvin yleisiä, joilla yritetään saada informaatiota. Monesti kohdistettu vanhempia selaimia kohtaan, joissa SSL/TLS salaukset ovat heikommalla tasolla. (Böck 2016.)

Kybervakoilun tarkoituksena on ottaa luvattomasti haltuun salaista informaatiota, järjestelmiä, tieto- ja viestintäverkkoja saavuttaakseen poliittista, sotilaallista tai taloudellista etua. Kohteena yleensä valtio, armeija tai yritys. Tunnettuja tapauksia on hyvin vähän ja todennäköisesti ne edustavat vain pyramidin huippua. Vakoilua on hyvin hankala havaita ja jos on onnistuttu sen havaitsemisessa, niin analysoiminen on hyvin vaikeaa sekä kallista. (National Cyber Security Centre Netherlands 2016.)

4.3 Mahdollisuudet tulevaisuudessa

Voidaan myös nähdä tapahtuvan paljon kehitystä positiiviseen suuntaan. Monet organisaatiot sekä tietoturvallisuuteen erikoistuneet yhtiöt ovat syventäneet yhteistyötään ja tämän avulla on syntynyt monia toimintaa tehostavia tapoja, järjestelmiä ja prosesseja, jotka edesauttavat tietoturvarikollisuuden ja -uhkien torjumisessa. Tietoturvallisuuden ja haavoittuvuuksien tutkimiseen panostetaan paljon sekä suuret tietoturvayritykset ovat vahvasti keskittyneet myös tutkimukseen ja kehitykseen. (Lehto ym. 2017.)

Tietoturvarikollisuuden torjumiseksi tulevaisuudessa voidaan ajatella, että IT:n, tietoturvallisuuden ja liiketoiminnan on syvennettävä yhteistyötään vahvasti sekä hakea uusia toimintapoja kuinka toimia. Siihen vaaditaan avoimuutta organisaatioissa, aktiivista tietojen jakoa tietoturvauhkista, tapahtuneista hyökkäyksistä sekä täysin uusista uhkista. Tietoturvauhkien estämiseksi AT&T on raportissaan löytänyt viisi toimintatapaa: kulttuuri, tietoturva osana liiketoimintaa, työkalut ja sovellukset, kumppanuudet sekä rahoitus. Ensimmäiseksi tietoturvallisuus täytyy sisältyä organisaation kulttuuriin. Tietoturvallisuutta parannetaan, käytetään sekä arvostetaan kaikkialla organisaatiossa. Koulutusta pitää olla riittävästi saatavilla, jotta tietoisuus tietoturvallisuuden uhkista tulee osaksi työntekijöiden kulttuuria. Tavoitteet liiketoiminnassa pitää olla samassa linjassa tietoturvallisuuden tavoitteiden kanssa. Tietoturvallisuus on aina yhtenä osana teknologia- sekä liiketoimintapäätöksissä. Kolmanneksi, organisaatioilla täytyy olla ajan tasalla olevat palvelut sekä ratkaisut tietoturvahyökkäyksien torjumiseksi sekä organisaatioiden keskeisten varojen suojaamisessa. Tärkeää olisi säännöllisesti auditoida luotettavan kumppanin toimesta koko organisaation tietoturvallisuus taso esimerkiksi erilaiset testihyökkäykset sekä toimintatapojen testit. Neljänneksi, on pohdittava ja valittava hyvin huolella sekä perustellusti kumppanit tietoturvallisuuden osalta. Mitkä kumppanit ovat niitä

joiden kanssa voidaan tietoturvallisuutta kehittää kokonaisuutena, strategisena kumppanuutena ja minkälaisia muita kumppaneita pitäisi olla. Viidenneksi, rahoitus tulee turvata, siinä on otettava huomioon riskit, käytettävät tietoturvallisuusratkaisut, käytettävissä olevat tietolähteet sekä turvattava tiedot. (Lehto ym. 2017.)

4.4 SWOT-analyysi tietoturvallisuuden tilanteesta

SWOT on lyhenne sanoista strenghts (vahvuudet), weaknesses (heikkoudet), opportunities (mahdollisuudet) ja threats (uhat). Sen avulla voidaan analysoida esimerkiksi organisaatioiden toimintakykyä ja toimintaympäristöä kokonaisuutena. Analyysin pohjalta on mahdollista tehdä päätelmiä kuinka hyväksikäytetään vahvuuksia, kuinka heikkoudet muutetaan vahvuuksiksi, kuinka mahdollisuuksia voidaan hyödyntää tulevaisuudessa ja kuinka uhkilta voidaan välttyä. Lehto ym. (2017) mainitsevat raportissaan kuinka SWOT-analyysin teemat ovat johdettu Suomen kyberturvallisuusstrategian strategisten linjausten kohdan kolme yritystoimintaa käsittelevästä kokonaisuudesta. Suomesta valittiin 16 organisaatiota seitsemältä eri toimialalta, kriittisten infrastruktuurin yrityksistä sekä niille kyberturvallisuustuotteita ja -palveluja toimittavista yrityksistä.

”Kyberturvallisuudella tarkoitetaan tilannetta, jossa kybertoimintaympäristöön voidaan luottaa ja sen toiminta turvataan. Kybertoimintaympäristö on sähköisessä muodossa olevan tiedon (datan) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva kokonaisuus. Tällaisia ovat muun muassa vedenjakelujärjestelmät, liikennevalojen ohjausjärjestelmät, ydinlaitosten tuotantojärjestelmät tai vaikkapa tietoliikenteen runkoverkon valvontajärjestelmät. Näin ollen kyberuhat uhkaavat yleensä suoraan digitaalista maailmaa, mutta niillä on välillisiä tai välittömiä vaikutuksia fyysiseen maailmaan.” (Hyvärinen 2014.)

SWOT-analyysi on jaettu sisäisiin ja ulkoisiin tekijöihin. Vahvuudet ja heikkoudet ovat sisäisiä tekijöitä, esimerkiksi vahvuutena voidaan pitää, että organisaatiolla on hyvä ja luotettava maine ympäristön haasteista huolimatta ja heikkoutena taas voi olla esimerkiksi organisaation puutteet ymmärtää oman toimintansa haasteet toimintaympäristössä. Mahdollisuudet ja uhat ovat ulkoisia tekijöitä. Mahdollisuudeksi voidaan esimerkiksi luokitella organisaation mahdollisuudet olla vaikuttamassa luottamusta lisääviin toimenpiteisiin ulkoisten kumppanien avulla ja uhaksi voidaan katsoa esimerkiksi, että organisaatio ei kykene havaitsemaan ulkopuolelta tulevia tietomurtoja. (Lehto ym. 2017.)

	Vahvuudet – Positiivisten tekijöiden vaikutus kyberturvallisuuden luottamusta lisääviin toimenpiteisiin	Heikkoudet – Negatiivisten tekijöiden vaikutus kyberturvallisuutta lisääviin toimenpiteisiin
SISÄISET	**Johtaminen:** - kyberturvallisuus huomioitu strategisena tavoitteena, politiikka usein julkaistu - tärkeimmät uhat tunnistettu, riskiperusteinen, osana kokonaisturvallisuutta ja liiketoimintaa - toimenpiteitä priorisoitu **Tilannekuva:** - uhkatiedot saadaan usein toimintaverkostosta ja kumppaneilta suoraan - Kyberturvallisuuskeskuksen tiedotteet - joissakin yrityksissä 24/7 valvonta **Henkilöstön osaaminen:** - IT-henkilöstöllä hyvää osaamista - muulle henkilöstölle annetaan usein koulutusta verkossa - osaamisen todentaminen mm. terveydenhuollossa - web-seminaarit, infokanava tiedon jakelukanavina **Tuotteet ja palvelut:** - parhaat tuotteet käytössä - palveluissa hyvä osaaminen - ulkoistettuna ostopalveluna, osin hajautettu riskiperusteisesti - työasemat usein omana palveluna, mikä sopii "tavanomaisiin" uhkiin **Sidosryhmät:** - ulkoistuksissa parhaat kumppanit - toimialayhteistyö; mm. energiayhtiö ERVA-alue - PPP-yhteistyö, mm. HVK-poolit - kansainvälinen yhteistyö - yrityksissä usein hyvä maine sidos ryhmien piirissä **Asiantuntijapalvelut:** - erilaiset auditointikäytänteet käytössä - ongelmatilanteiden selvittämisessä käytetään alan asiantuntijoita - ISO 27000, KATAKRI, HUOVI - parhaat käytänteet käytössä - tutkimusohjelmat, joissa osa yrityksistä mukana **Jatkuvuuden varmistaminen:** - harjoitustoimintaa, suunnitteluharjoituksia sekä HVK:n ja JAMK:n järjestämiä harjoituksia - varautumissuunnitelmia laadittu	**Johtaminen:** - politiikan jalkautus läpi organisaation usein haastavaa - vaativimmat uhkakuvat tunnistamatta - toiminta reagoivaa - henkilöstön roolitus usein haastavaa, informaatioturvallisuudesta vastaavan (CISO) edustus puuttuu johtoryhmästä - kuntataustaisten yritysten henkilö-resursoinnin puutteet **Tilannekuva:** - yleistilanne muodostettava hajallaan olevista tiedoista - toimintaverkoston tilannekuvan muodostaminen vaikeaa - ei reaaliaikaista tilannekuvaa IT varannoista eikä automaatiosta (ICS) **Henkilöstön osaaminen:** - koko henkilöstön kouluttaminen haastavaa - kansallisesti syväosaaminen harvojen käsissä, laajat häiriöt haastavia hoitaa - kuntataustaisissa yrityksissä osaaminen harvojen käsissä (resursointi) - IT/ICS-kokonaisuuden osaaminen **Tuotteet ja palvelut:** - kumppanuusverkoston toiminnan auditointi haastavaa - puutteellinen näkymä palvelujen suojaukseen (mm. pilvipalvelut) - yrityskeskittymät kriittisessä infrastruktuurissa - kattavan tunnistautumisen puute **Sidosryhmät:** - osalla toimialoista toimialayhteistyö-mahdollisuuden puute - liiketoiminnan ja kansallisen huoltovarmuuden yhteensovittaminen (resursointivastuu) **Asiantuntijapalvelut:** - auditoinnin kattavuus läpi koko toiminnan ja ohjelmistojen toimintaan/palveluun puutteellista - koulutuspalvelujen saatavuudessa haasteita - PPP-yhteydenpito voi olla haastavaa häiriötilanteissa - yritysten omaehtoinen tutkimustoiminta on vähentynyt
ULKOISET	**MAHDOLLISUUDET – Lista mahdollisuuksista, jotka lisäävät kyberluottamusta**	**UHKAT – Lista uhkatekijöistä, jotka vaikuttavat kyberluottamukseen**
	Edistyksellisen tekniikan hankinta: - mahdollisuus investoida uuteen tekniikkaan: erityisesti isoissa yrityksissä **Uudet yhteistyötahot:** - PPP-toiminnasta kilpailuetua - yhtenäisen tilannekuvan muodostaminen - nykyistä laajemman toimialayhteistyön mahdollisuudet **Uudet kehitysmahdollisuudet:** - tiedustelulaki ja sen muodostamat toimintaedellytykset - koulutuksen jatkokehittäminen - benchmarking-toiminta - auditointitoiminnan kehittäminen - hallittu regulaatio (toimintojen harmonisointi)	**Toimintaympäristön analysointi:** - tuntemattomat uhkatekijät ja tietomurrot - uudet liiketoimintamallit; edellyttävät uusien tekniikoiden käyttöönottoa (esim. IOT, robotiikka), joiden mukanaan tuomaa uhkakuvaa ei tunneta riittävästi **Kyberuhkien analysointi:** - haasteena teollisuusvakoilu ja valtiollisten toimijoiden kyvykkyys - terrorismi; kyberfyysinen vaikuttaminen sähköverkkoon, vesihuoltoon ja terveydenhuollon järjestelmiin sekä lääkevalmistukseen ja biopankkiin - pysyykö ohjelmistokehitys uhkien mukana; vanhentunutta suojaustekniikka käytössä - henkilöstöriskit, sisäpiiriläiset - avainhenkilöstöön kohdistuvat uhat - kyberuhat keskittyneisiin palveluihin **Toimintaverkoston analysointi:** - ei näkymää verkostoon ja sen riippuvuussuhteisiin - toimintaverkoston pullonkaulat; kriittisessä infrastruktuurissa samoja yrityksiä merkittävässä asemassa - resurssikapeikot laajojen häiriöiden tilanteessa - osaamisen katoaminen ulkoistetuissa palveluissa; ylikansallinen yhtiö, saneeraukset taloudellisista syistä, joista seuraa osaamisen katoaminen

Kuvio 7: SWOT-analyysi (Lehto ym. 2017).

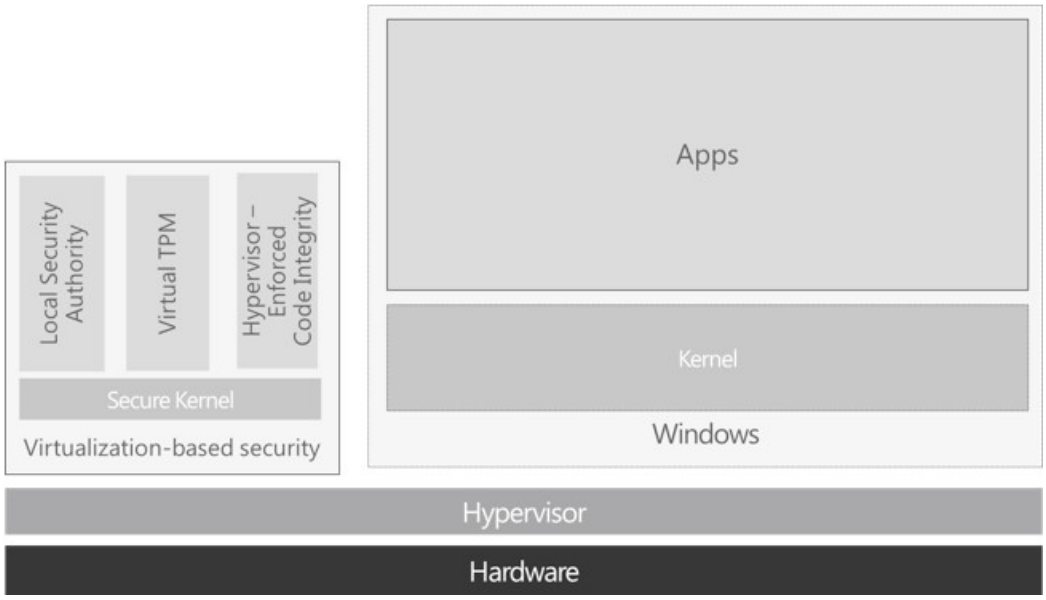
5 Windows 10 käyttöjärjestelmän tietoturvaan liittyvät ominaisuudet

Microsoft on tehnyt monia parannuksia turvallisuuteen Windows 10 käyttöjärjestelmässä. Ne voidaan luokitella seuraaviin kategorioihin; uhkan vastustaminen, informaation suojaus ja identiteetin suojaus. Käyn seuraavaksi läpi mitkä ominaisuudet kuuluvat edellä mainittuihin kategorioihin.

5.1 Uhkan vastustaminen

Windows 10 pystyy käyttämään virtualisoimisen teknologiaa eristääkseen ydin käyttöjärjestelmän palvelut tätä menetelmää kutsutaan termillä virtuaalinen turvallisuus (Virtualization-based security VBS). Tämän avulla turvallisuuteen lisätään yksi kerros lisää ja voidaan varmistaa, että vaikka kernel toiminnot olisivat vaarantuneet, niin mikään uhka ei pysty manipuloimaan palveluita. Windows 10 voi käyttää prosessorien mukana tulevaa toisen-asteen osoitteen käännös (SLAT) teknologiaa ja virtuaalisia laajennuksia, kuten Intelin VT-x ja AMD-V.

Tähän VBS ympäristöön kuuluvat seuraavat palvelut. Hypervisor Code Integrity (HVCI) palvelulla määritetään onko suorittava koodi kernel tilassa kunnolla suunniteltu ja luotettava. Se tarjoaa suojan nollapäivä (Zero Day) ja haavoittuvuuksia vastaan hyödyntämällä suojeluun liittyviä valmiuksia varmistamalla, että kaikki ohjelmistot, jotka käynnistyvät kernel tilassa, mukaan lukien ajurit, jotka turvallisesti varaavat muistia toimivat kuten ne on tarkoitettu. Kernel tilan koodin eheys on konfiguroitavissa, joka mahdollistaa sen, että organisaatiot voivat muokata ennen käyttöjärjestelmän käynnistymistä ajettavaa tarkistus koodia. Local Security Authority (LSA) palvelu Windows 10:ssä hallitsee autentikointi operaatioita, mukaan lukien NT LAN Manager (NTLM) ja Kerberos mekanismeja. Credential Guard ominaisuus erottaa osan tästä palvelusta ja auttaa lieventämään pass-the-hash ja pass-the-ticket tekniikoita suojaamalla toimialueen käyttäjätietoja. Lisäksi sisäänkirjautumisen käyttäjätiedot tallennetaan Credential Manageriin.



Kuvio 8: VBS Arkkitehtuuri (Microsoft 2016).

Microsoft Device Guard on ominaisuus, joka yhdistää järjestelmän luotettavuus sekä kovennus ominaisuudet hyväksikäyttämällä uusia VBS vaihtoehtoja suojellakseen järjestelmän ydintä. Device Guard yhdistää jo olemassa olevia ominaisuuksia, kuten UEFI Secure Boot ja yhdistää ne uuteen HVCI palveluun sekä konfiguroitavaan koodin luotettavuuteen. (Lich, Keller & Hall 2017.)

Perusvaatimukset mitkä tietokoneen tulee täyttää, että Device Guard voidaan ottaa käyttöön:

- 64-bittinen prosessori joka tukee VT-x tai AMD-V ja SLAT
- UEFI firmware versio 2.3.1.c tai korkeampi sekä UEFI Secure Boot (Microsoft 2017).
- UEFI firmwaren pitää tukea turvallista fimwaren päivitys prosessia (Microsoft 2017).

- HVCI yhteensopivat ajurit (Microsoft 2016; Baxter 2015).
- Windows 10 Enterprise, Windows 10 Education, Windows Server 2016, or Windows 10 IoT Enterprise.

Lisäturvallisuuden saavuttamiseksi alla olevat vaatimukset tulee täyttyä (Windows 10 versio 1507 ja Windows Server 2016, Technical Preview 4):

- Käynnistys konfiguraation ja hallinnan turvallisuus
    - BIOS salasana tai vahva autentikointi pitää olla tuettuna.
    - BIOS konfiguroinnissa, BIOS autentikointi pitää olla asetettuna.
    - BIOS vaihtoehto sallituille käynnistyville laitteille pitää olla tuettuna.
    - BIOS vaihtoehdot liittyen turvallisuuteen ja käynnistykseen pitää olla suojattuna niin että toisesta käyttöjärjestelmästä ei ole mahdollista vaikuttaa niihin.

Nämä ominaisuudet ovat tuettuna alkaen Windows 10 versio 1607 ja Windows Server 2016:

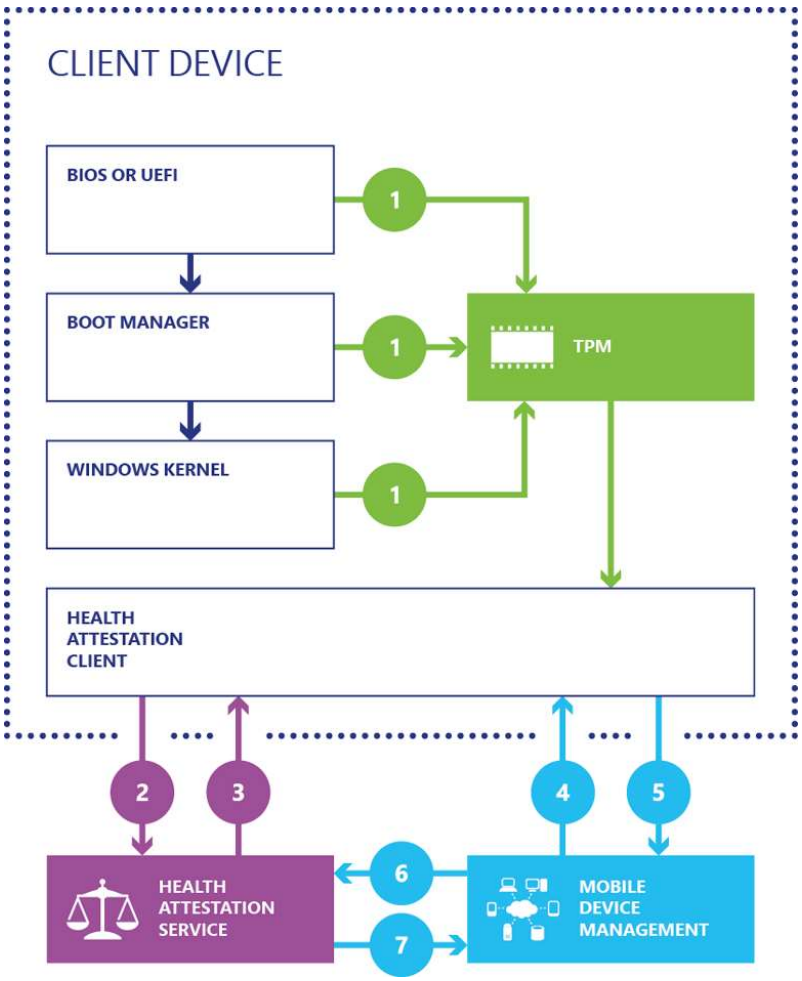
- Hardware Rooted Trust Platform Secure Boot
    - Käynnistyksen eheys (Platform Secure Boot) pitää olla tuettuna.
    - The Hardware Security Test Interface (HSTI) 1.1.a pitää olla toteutettuna (Microsoft 2017).
- Firmware päivitys Windows päivitysten kautta.
- Käynnistys konfiguraation ja hallinnan turvallisuus
    - Vaadittavat BIOS valmiudet: Laitteen valmistajan kyky lisätä ISV, OEM tai Yritys sertifikaatti Secure Boot tietokantaan laitteen valmistuksessa.
    - Vaadittavat konfiguroinnit: Microsoft UEFI CA sertifikaatti pitää poistaa Secure Boot tietokannasta. Tuki kolmannen osapuolen UEFI moduuleille on sallittu.

Nämä ominaisuudet ovat tuettuna alkaen (Windows 10 versio 1703):

- VBS:n käyttöönoton mahdollisuus NX suojauksessa UEFI:n ajonaikasissa palveluissa.
- Firmware tuki SMM suojaukselle (Microsoft 2016).

(Lich ym. 2017.)

Mitattava käynnistys ja etätodennus ovat ominaisuuksia, joilla voidaan havaita ennen käyttöjärjestelmän käynnistystä tapahtuvaa järjestelmän muokkausta tai tartuntaa kuten haittaohjelmia (bootkit ja rootkit). Windows 10 käyttää laitteen TPM moduulia ja mitattavaa käynnistystä (Windows Measured Boot) ominaisuutta analysoidakseen käynnistyksen eheyttä. Nämä tiedot Windows 10 kerää ja ne voidaan lähettää pilvipalveluun, jonka kautta voidaan analysoida laitteiden tilaa. (Microsoft 2017.)

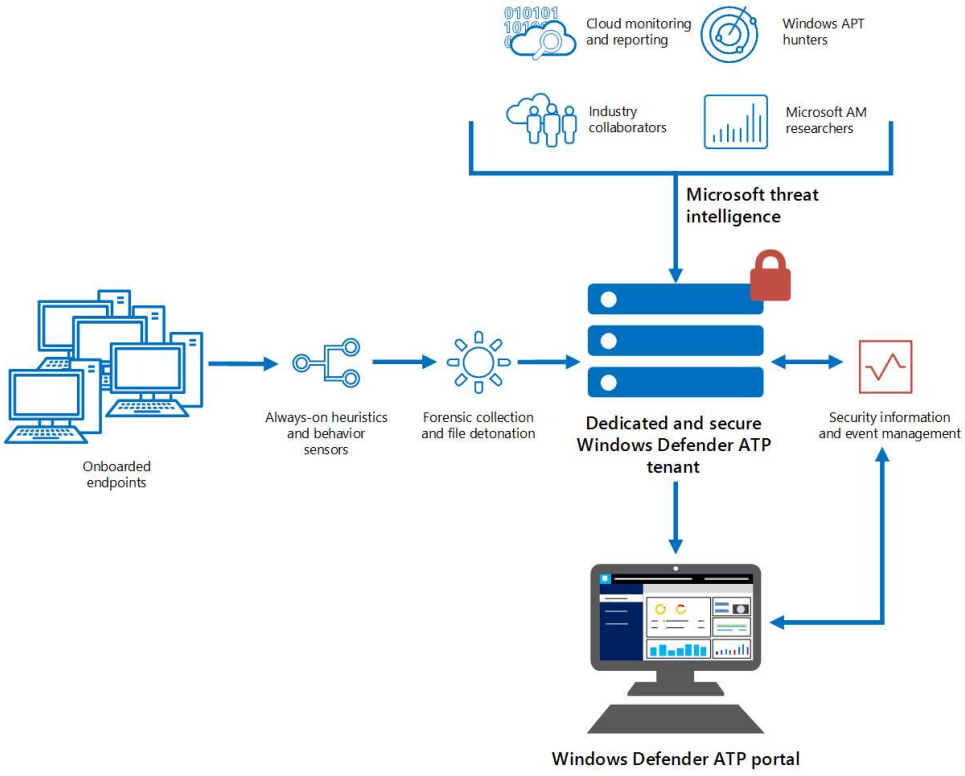


Kuvio 9: Mitattava käynnistys ja etätodennus (Microsoft 2017).

Windows Defender on käyttöjärjestelmään sisäänrakennettu haittaohjelmien tunnistus (Antimalware) ohjelma. Sen tärkeimmät uudet ominaisuudet ovat:

- Early Launch Antimalware (ELAM) yhteensopivuus. Kun Secure Boot on varmistanut, että ladattava käyttöjärjestelmä on luotettava, ELAM voi käynnistää antimalware ohjelman.
- Paikallinen konteksti havainnoille ja keskitetty tunnistus tieto. Windows Defender lisää kontekstin havaituille uhkille. Tässä tiedossa on mukana uhkan lähde sekä historia tieto siitä miten haittaohjelma liikkunut läpi järjestelmän. Tämä raportti voidaan lähettää suoraan pilvipalveluun, jonka avulla voidaan vähentää uhkia nopeammin.
- User Account Control (UAC) integrointi. Windows Defender automaattisesti skannaa mahdollisen uhkan aina kun UAC pyyntö tehdään, minkä avulla voidaan estää käyttäjiä antamasta haittaohjelmien suorittaa korotettuja käyttöoikeuksia.

Windows Defender Advanced Threat Protection (Windows Defender ATP) on turvallisuus palvelu, jonka avulla voidaan havaita, tutkia ja vastata uhkiin. Windows Defender ATP käyttää seuraavia Windows 10:n sisäänrakennettuja ominaisuuksia sekä pilvipalveluita. Windowsin sisäänrakennetut sensorit, jotka keräävät ja prosessoivat käyttäytymiseen liittyviä signaaleja käyttöjärjestelmässä ja lähettää nämä tiedot yksityiseen sekä eristettyyn pilvipalveluun. Pilvessä tapahtuva turvallisuus analytiikka, jossa hyödynnetään big-dataa, koneoppimista ja Microsoftin omista palveluista keräämää tietoa. Älykkään toiminnan hyödyntäminen, johon osallistuvat Microsoftin turvallisuus tiimit (Microsoft hunters) sekä kumppanien hyödyntäminen uhkien tunnistamisessa. (Microsoft 2017.)



Kuvio 10: Windows Defender ATP (Microsoft 2017).

Vaatimukset Windows ATP:n käyttöönotolle:

- Windows 10 versio 1607
- Internet yhteys Windows Defender ATP päätepisteille (Microsoft 2017).
- Minne Windows Defender ATP:n tiedot tallentuvat, joko Eurooppalaiseen tai Yhdysvaltalaiseen tietokeskukseen (Microsoft 2017).
- Windows Defenderin allekirjoitus päivitykset ovat määritettyinä (Microsoft 2017).
- Windows Defender Early Launch Antimalware (ELAM) ajuri on sallittuna (Microsoft 2017).

Microsoft Edge on Windows 10 käyttöjärjestelmän uusi internet selain, joka on tarkoitettu korvaamaan Internet Explorer. Se toimii oletus selaimena Windows 10:ssä. Sen mukana tuomat turvallisuus ominaisuudet ovat seuraavat: natiivi tuki Windows Hello biometriikalle, jonka avulla voidaan suojautua esimerkiksi tietojen kalastelu yrityksiltä, jotta käyttäjät eivät kirjoittaisi selväkielisiä salasanojaan verkkosivustoille (W3C 2017). SmartScreen palvelun avulla voidaan suojautua tietojen kalastelu yrityksiltä suorittamalla maineeseen perustuvia tarkistuksia ja estämällä sivustoja, joiden ajatellaan olevan vahingollisia. Sen avulla voidaan myös suojautua drive-by hyökkäyksiltä sekä estää huijausyritykset, joilla saadaan käyttäjät asentamaan haitallisia sovelluksia. Maineeseen perustuva sertifikaattien tarkistaminen, jonka avulla voidaan estää sivustoja, jotka ovat hankkineet tai väärentäneet sertifikaattinsa (Microsoft MSDN 2017). Uusi renderöinti moottori nimeltään Microsoft EdgeHTML, joka on keskittynyt moderneihin standardeihin. Tuki W3C Content Security Policy (CSP) standardille ja HTTP Strict Transport Security (HSTS) turvallisuus ominaisuus (IETF-standardiin yhteensopiva).

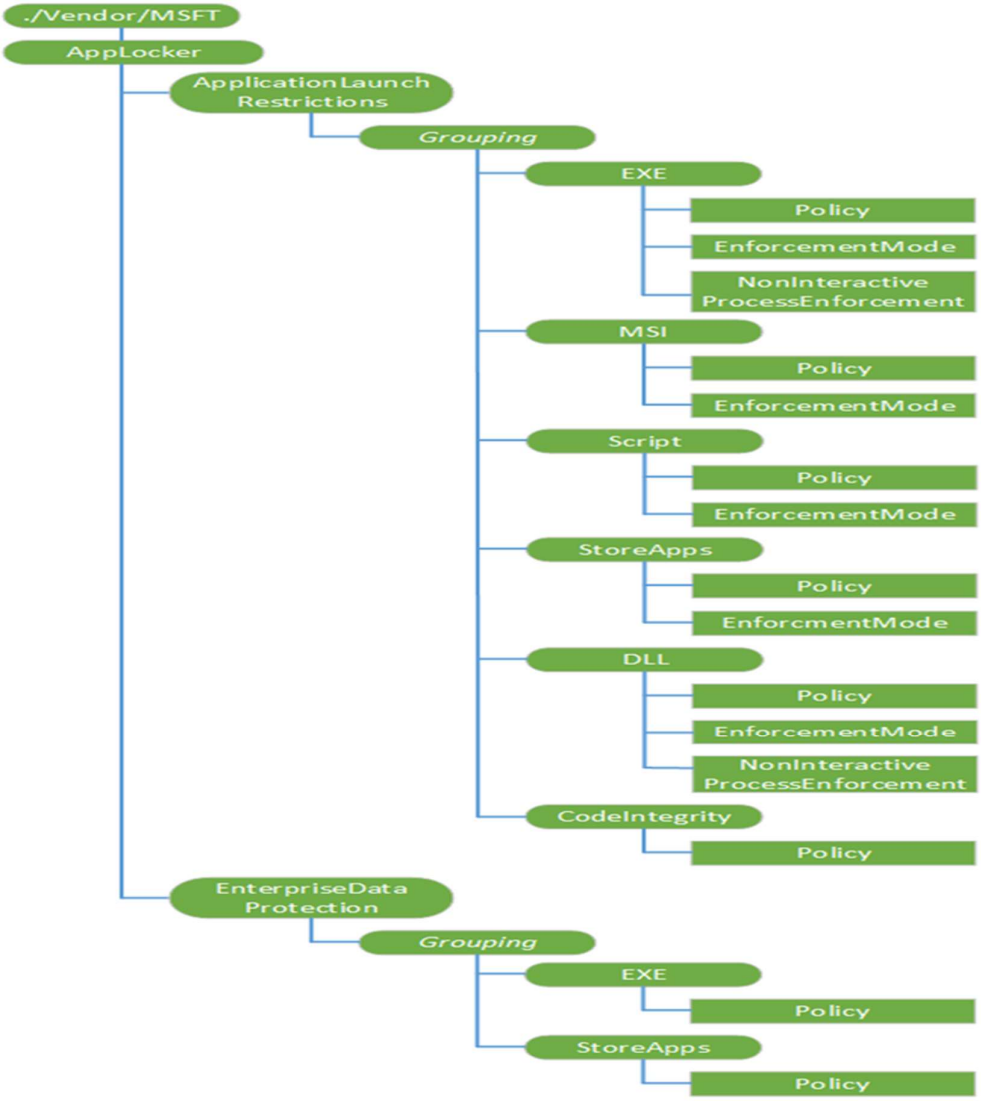
Kaikki verkkoon liittyvä sisältö ajetaan erillisessä applikaatio siilossa hiekkalaatikossa. Edge ei tue kolmannen osapuolen binääri laajennuksia, jolloin mitään sisältöä ei tarvitse ajaa siilojen ulkopuolella, jonka avulla varmistetaan turvallisuus. Koko Microsoft Edgen suunnittelu on tehty eri tavalla kuin aiemmin, se on kuin universaali Windows applikaatio. Jos käyttöjärjestelmä on 64-bittinen, myös Microsoft Edge on. Tämän avulla vahvistetaan Windows Address Space Layout Randomization (ASLR) ominaisuutta, joka satunnaistaa muistin sijoittelua selaimen prosesseissa, tehden vaikeammaksi kohdistaa hyökkäyksiä tiettyihin muistin kohtiin. Selaimesta löytyy täydellinen HTML5 tuki. Siitä on poistettu hyökkäyksiin käytettäviä alustoja sekä tuki on poistettu kokonaan seuraavilta komponenteilta ja koodikieliltä VBScript, Jscript, VML, Browser Helper Object, Toolbars ja ActiveX. Sisältöön liittyvät prosessit tukevat koodin eheyttä ja kuvien lataus estoja. Vain allekirjoitetut kuvat voidaan ladata Edgessä. Muistin korruptoitumisen lieventäminen Memory Garbage Collector (MemGC) ja Control Flow Guardin avulla.

Microsoft Edge on pärjännyt hyvin verkkoselainten turvallisuutta vertailevissa testeissä. Edge onnistui saamaan 91.4 prosenttia kiinni tietojenkalastelu yrityksistä ja 99 prosenttia sosiaalisesti suunnitelluista haittaohjelmista (SEM). Vertailussa mukana olivat Chrome ja Firefox, jotka saivat seuraavat lukemat. Chrome esti 82.4 prosenttia tietojenkalastelu yrityksistä ja 85.8 prosenttia sosiaalisesti suunnitelluista haittaohjelmista (SEM). Firefox onnistui estämään 81.4 prosenttia tietojenkalastelu yrityksistä ja 78.3 prosenttia SEM näytteistä. (NSS Labs 2017.)

AppLocker mahdollistaa applikaatioiden kontrollointia ja toiminnan hallitsemista, sääntöjen ja politiikoiden avulla. Sen avulla voidaan kontrolloida seuraavan tyyppisiä applikaatioita:

suoritettavat tiedostot (.exe ja .com), scriptit (.js, .ps1, .vbs, .cmd ja .bat), Windows asennus tiedostot (.mst, .msi ja .msp), DLL tiedostot (.dll ja .ocx) ja pakatut applikaatiot (appx). Sääntöjen määritys perustuen tiedoston attribuutteihin, jotka ovat johdettu digitaalisesta allekirjoituksesta, sisältäen julkaisijan, tuotteen nimen, tiedoston nimen ja tiedoston version. Asettaa säännön ryhmälle tai yksittäiselle käyttäjälle. Luoda poikkeuksia sääntöihin esimerkiksi sääntö joka sallii kaikki Windows prosessien ajon paitsi komentorivin (cmd.exe). Pelkkään auditointi tarkoitukseen ajettava tila, jonka avulla voidaan ymmärtää politiikan vaikutukset ennen sen pakottamista. Tuonti ja vienti säännöt, jotka vaikuttavat koko politiikkaan. Windows Powershellin avulla voidaan tehostaa sääntöjen luontia ja hallitsemista. (Microsoft Technet 2017.)

AppLocker CSP eli konfigurointi palvelu, jonka avulla voidaan määrittää mitkä applikaatiot ovat sallittuja tai eivät ole. Seuraavassa kuvassa on kuvattuna puu mallin avulla, kuinka palvelu toimii. Ensimmäiseksi ./Vendor/MSFT/AppLocker määrittää juuri solmun AppLocker CSP:lle, seuraavaksi ApplicationLaunchRestrictions määrittää rajoitukset applikaatioille, tämän jälkeen Grouping määrittää dynaamiset solmut. Nämä solmut sisältävät GUID nimeämisen, joka voi olla mitä tahansa. Sitten EXE, MSI, Script, StoreApps, DLL ja CodeIntegrity määrittävät rajoitukset käynnistää suoritettavia applikaatioita, Windows asennus tiedostoja, Microsoft Kaupan applikaatioita, DLL tiedostoja ja koodin luotettavuutta. Lopuksi Policy määrittää politiikan, jota käytetään kun käynnistetään suoritettavia tiedostoja, Windows asennus tiedostoja, scriptejä, Microsoft kaupan applikaatioita ja DLL tiedostoja. (Microsoft MSDN 2017.)



Kuvio 11: AppLocker CSP (Microsoft 2017).

5.2 Informaation suojaus

Windows Information Protection (WIP) on ominaisuus, joka voi auttaa estämään tiedon häviämisen. Se voidaan määrittää esimerkiksi salaamaan ja suojaamaan tiedostot automaattisesti sen perusteella mistä sisältö on hankittu (esimerkiksi verkkojako tai Sharepoint sivusto). Vaatimuksena WIP:n käyttöönotolle on Windows 10 versio 1607 ja Microsoft Intune tai System Center Configuration Manager (SCCM) tai kolmannen osapuolen mobile device management (MDM) ratkaisu.

WIP:n käytön mahdollisuudet ovat; erottelu yksityisen ja yrityksen tiedon välillä, ilman että käyttäjien tarvitsee vaihtaa ympäristöä tai applikaatiota esimerkiksi jos käyttäjä kopioi yrityksen tiedostoja usb-tikulle, niin ne ovat automaattisesti salattuja ja yksityiset tiedostot eivät. Tiedon suojaus yritys applikaatioille ilman, että tarvitsee päivittää applikaatioita esimerkiksi jos on asetettu kopioimisen ja liittämisen esto yritys applikaatioista yksityisiin, niin käyttäjä ei pysty kopioimaan tai liittämään tietoa niiden välillä. Vain hyväksytyt applikaatiot voivat saada pääsyn yrityksen tietoihin sekä mahdollisuus pyyhkiä tyhjäksi yritys tiedot ilman vaikutusta henkilöhtäisiin tietoihin. Myös auditointi raporttien käyttö on mahdollista. (Microsoft 2017.)

WIP politiikat, joiden mukaisesti suojaus ja hallinta asetetaan. Politiikat ovat seuraavat: Block, joka estää tiedon jakamisen kokonaan esimerkiksi yrityksen ulkopuoliselle henkilölle. Override, joka varoittaa käyttäjää jos toiminta vaikuttaa turvattomalta. Käyttäjän on mahdollista itse päättää haluaako jakaa tiedon. Auditointi lokiin jää jälki näistä toimenpiteistä. Silent, joka kerää loki tietoa sopimattomasta tiedon jakamisesta, ilman että estää mitään tai josta käyttäjä olisi saanut tiedon override tilassa. Ei sallitut teot, kuten applikaatiot jotka yrittävät päästä käsiksi WIP-suojattuun tietoon, ovat edelleen estetty.

Bitlocker on Microsoftin salaus ratkaisu, joka on ollut käytössä jo vuodesta 2004. Windows 10:n mukana on tullut uusia ominaisuuksia siihen, joita ovat seuraavat:

Automaattinen aseman salaus, oletuksena päällä puhtaissa Windows 10 asennuksissa, jos laite on läpäissyt vaatimus Windows Hardware Certification Kit testin (Microsoft 2017).

Microsoft BitLocker Administration (MBAM) parannuksia itsepalvelu portaaliin yksinkertaistamalla palautus pyyntöjä (Microsoft 2017).

Single Sign On (SSO) PIN-koodin käyttöä ei tarvitse enää suojaukseen, koska TPM hallitsee avaimia (Lich 2017).

Vain käytetyn tilan suojaus, jossa on mahdollista ottaa käyttöön salaus vain niissä kovalevyn osissa, jotka ovat käytössä. Tämän avulla salaukseen menevä aika vähentyy selvästi. (Microsoft 2017.)

5.3 Identiteetin suojaus

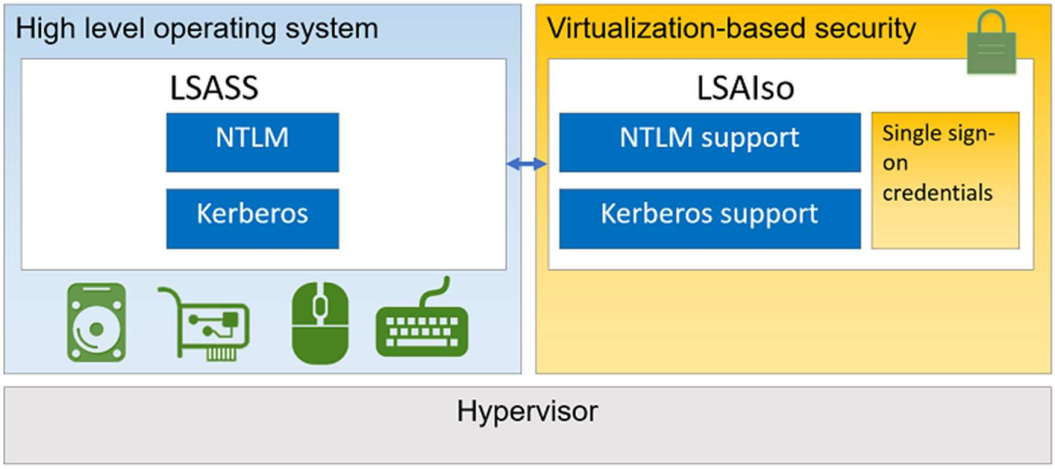
Windows Hello for Business mahdollistaa salasanojen korvauksen vahvalla kahden tekijän autentikoinnilla. Se sisältää käyttäjäntiedot, joka on sidottu laitteeseen ja käyttää biometriikkaa tai pin-koodia. Sen avulla pyritään luomaan käyttäjille turvallinen ja helppo kirjautua

laitteelle. Vahvat salasanat voivat olla monesti vaikeita muistaa ja sen takia samoja salasanoja käytetään monessa eri paikassa. Salasanat ovat myös monen hyökkäyksen kohteena esimerkiksi tietojenkalastelu yritykset. (Microsoft 2017.)

Biometrinen sisäänkirjautuminen on mahdollista tehdä kahdella tavalla, kasvojen- tai sormenjälkientunnistuksella erikseen määritetyillä laitteilla, jotka vastaavat Microsoftin vaatimuksia (Microsoft 2017).

Biometrinen tunnistautuminen voi olla käyttäjälle helpompi ja nopeampi tapa tunnistautua laitteelle tai eri palveluihin, mutta on olemassa tutkimuksia jotka kiistävät sen turvallisuuden verrattuna salasanojen käyttöön. Perusongelmana on se, että salasanan voi aina helposti vaihtaa vaikka se olisi varastettu, mutta biometristä tunnistetta taas ei voi. (Siddique, Akhtar & Kim 2017.)

Credential Guard käyttää virtuaalisaatioon perustuvaa suojaa eristääkseen salaisuudet, joihin vain luottamukselliset järjestelmän ohjelmistot voivat päästä käsiksi. Sen avulla pyritään estämään käyttäjätietoon liittyvät hyökkäykset kuten Pass-the-hash ja Pass-the-ticket. Seuraavat ominaisuudet tulevat käyttöön Credential Guardin mukana. NTLM autentikointi protokolla, Kerberos ja Credential Manager hyväksikäyttäjät alustan turvallisuus ominaisuuksia, mukaan lukien Secure Boot ja virtualisaatio suojatakseen käyttäjätietoja. NTLM ja Kerberos käyttäjätiedot kulkevat suojatussa virtuaalisessa ympäristössä, joka on eristetty käyttöjärjestelmästä.



Kuvio 12: Credential guard toiminta (Microsoft 2017).

Vaatimukset laitteelta käyttöönottoa varten:

- Tuki virtualisaatioon perustuvaan turvallisuuteen (VT-x, AMD-V ja SLAT)
- UEFI Secure Boot
- TPM 1.2 tai 2.0

- Mahdollisuus UEFI:n lukitsemiseen

(Microsoft 2017.)

Etäyhteyksien suojaaminen Credential Guardin avulla tuli mahdolliseksi Windows 1607 versiossa. Sen avulla voidaan suojautua että järjestelmänvalvojan tunnukset eivät pääse leviämään verkon yli tai esimerkiksi Service Deskin työntekijöiden ottaessa etäyhteyden saastuneelle työasemalle tunnukset pysyvät suojattuna.

6 Tilanne kohde yrityksessä

Kohde yrityksen yleinen tietoturvallisuus on hyvällä tasolla eikä mainittavia tietomurtoja ole päässyt aiemmin tapahtumaan.

Tämän hetken tilanne yrityksen työasemien tietoturvallisuudessa on myös monipuolisesti hyödynnetty eri suojaus tapoja. Määrällisesti yrityksellä on käytössään noin 3300 työasemaa, johon kuuluvat kannettavat- sekä pöytätietokoneet. Käyttöjärjestelminä toimivat Windows 7 ja 10 (versiot 1511 ja 1607). Niiden osuus jakautuu työasemilla noin 2300 kappaletta Windows 7 ja noin 1000 kappaletta Windows 10 työasemia. Kaikki uudet työasemat toimitetaan Windows 10 käyttöjärjestelmällä sekä tarpeen vaatiessa vanhempien koneiden käyttöjärjestelmän uudelleen asennukset tehdään aina Windows 10:een. Esimerkiksi voidaan mainita tilanne, jossa Windows 7 käyttöjärjestelmä on hidastunut niin paljon, että se tarvitsee täydellisen uudelleen asennuksen, jolloin ennalta hyväksytyt ja vaatimukset täyttävät Lenovon mallisarjat voidaan päivittää Windows 10 käyttöjärjestelmään.

Kaikki työasemat ovat salattuja jo esiasennus vaiheessa BitLockerin avulla. Admin tasoisten käyttäjätunnusten käyttö on melko vähäistä ja siihen on olemassa erillinen lomake, jolla käyttäjä sitoutuu noudattamaan tiettyjä yrityksen määrittelemiä käytäntöjä. Ryhmäkäytännöillä (Group policy) on määritelty kaikille työasemille erilliset tietoturva vaatimukset, esimerkiksi salasanojen vähimmäisvaatimukset (pituus, monimutkaisuus, vaihtoväli).

Joka kuukausi tapahtuvat tietoturva päivitykset käyttöjärjestelmään, Microsoft Officeen ja tiettyihin kolmannen osapuolen ohjelmistoihin, jotka ovat Java, Adobe flashplayer ja Adobe Reader.

Kaikille työasemille on asennettuna Symantec EndPoint Protection, huolehtimaan verkkoliikenteestä ja haittaohjelmista.

Windows 10 työasemilla on käytössä UEFI Secure Boot suojausmekanismi, jonka avulla voidaan estää hyökkääjiä käynnistämästä esimerkiksi haitallisia ohjelmia työaseman käynnistymisen aikana.

7 Kehitysehdotukset

Tietoturvauhkien kehittyessä jatkuvasti kiihtyvällä tahdilla esimerkiksi AV-Test Instuten mukaan he rekisteröivät uusia haittaohjelmia yli 390 000 joka päivä, myös uhkiin varautumisen tulee muuttua. Jo Windows 10 käyttöjärjestelmän ydin on rakennettu paljon suojatummaksi ja turvallisemmaksi kuin sen edeltäjät, jonka pohjana on virtuaalisuuten pohjautuva suunnittelu, joka mahdollistaa suojausmetodit kuten Device- ja Credential Guard.

Ensimmäiseksi kohde yrityksessä tulisi aloittaa suunnitelmat miten kaikki jäljellä olevat työasemat voidaan päivittää Windows 10 käyttöjärjestelmään, jonka avulla luodaan pohja sille miten tietoturvallisuutta voidaan lähteä tehostamaan. Tämän kaltaiset projektit ovat hyvin työläitä sekä vievät paljon aikaa, tämän vuoksi suunnittelu on tärkeää aloittaa ajoissa. Tämän hetken strategiana on ollut työasemien elinkaaren mukaisesti toimittaa vain uudet koneet Windows 10 käyttöjärjestelmällä, mutta tämä voi osoittautua liian hitaaksi malliksi tietoturvallisuutta ajatellen tai liian kalliiksi, jos kaikki vanhat työasemat vaihdettaisiin uusiin. Windows 7 käyttöjärjestelmälle Microsoft on luvannut toimittaa korjaus- ja tietoturvapäivityksiä vuoteen 2020 asti, mutta uusien ominaisuuksien päivittyminen tulee keskittymään Windows 10:iin.

Yksi hyvin tärkeä ominaisuus, joka tuli monessa yhteydessä vastaan tehdessäni tätä selvitystä on järjestelmänvalvojan (admin) oikeuksien poisto käyttäjiltä. Monet haittaohjelmat eivät pääse tekemään tuhojaan ja leviämään ilman, että käyttäjällä tarpeeksi oikeuksia suorittaa haitallista koodia. Avecto painottaa raportissaan, että 94 prosenttia vuonna 2016 Microsoftin kriittiseksi luokittelemaa haavoittuvuutta olisi estettävissä pelkästään poistamalla käyttäjiltä admin oikeudet työasemilta. 66 prosenttia kaikista Microsoftin vuonna 2016 havaitsemista haavoittuvuuksista voitaisiin estää poistamalla admin oikeudet.

Käyttöönotto admin oikeuksien poistamiseksi voi olla työläs, mutta se on perusteltavissa käyttäjille ja monissa tapauksissa on mahdollista, että kaikki tarpeet mitkä ovat johtaneet siihen, että käyttäjä tarvitsee admin oikeuksia on ratkaistavissa jo etukäteen analysoimalla ja suunnittelemalla. Esimerkiksi käyttäjä tarvitsee sellaista ohjelmaa, joka tarvitsee oikeudet kirjoittaa johonkin tiettyyn rekisterin haaraan, johon normaalilla käyttäjällä ei ole oikeuksia ja ratkaisuksi tähän ongelmaan käyttäjälle on annettu admin oikeudet vaikka voitaisiin pelkästään myöntää oikeus käyttää sitä tiettyä rekisterin haaraa, jolloin admin oikeuksia ei tarvitsisi myöntää ollenkaan käyttäjälle.

Credential Guardin käyttöönoton avulla yrityksessä voidaan tehokkaasti suojautua esimerkiksi Pass the hash hyökkäyksiltä, joissa hyökkääjät pyrkivät esimerkiksi kaappaamaan ensin yhden työaseman kirjautumistiedot, jonka avulla yritetään päästä käsiksi ja valtaamaan koko orgaanisaation tietoinfrastruktuuri. Credential Guardin käyttöönottaminen on melko yksinkertaista esimerkiksi group policyn avulla, mutta siinä on tiettyjä rajoituksia kuten ohjelmat, jotka tarvitsevat kirjautumiseen kerberos DES salauksen tai NTLMv1 eivät toimi jos Credential Guard otetaan käyttöön, joten huolellinen testaus on tarpeellinen jos käyttöönottoa suunnitellaan.

AppLocker ominaisuudella on mahdollista kontrolloida ohjelmia ja tiedostoja, joita käyttäjät voivat ajaa. Sen avulla on mahdollista toteuttaa vain hyväksyttyjen ohjelmien salliminen (white listing) joka mahdollistaa sen etteivät ei sallitut ohjelmat pääse käynnistymään työasemilla. Vaatii aluksi paljon työtä tunnistaa ja listata kaikki ohjelmat jotka voidaan sallia, mutta tähän on olemassa hyviä käytäntöjä joiden avulla käyttöönotto helpottuu. AppLockerin toiminta tietoturvallisena ratkaisuna perustuu vahvasti sille olettamukselle, että käyttäjillä ei ole admin oikeuksia. Esimerkiksi moni voi ajatella, että yrityksessä on monia satoja ohjelmia ja niiden aliohjelmia, jotka tulisi kaikki listata ja sallia erikseen, mutta ei tarvitse jos pyrkii hahmottamaan ohjelmat säiliöissä eikä erillisinä omina ohjelminaan. Tiedät esimerkiksi etukäteen luottavasi C:\Program Files ja C:\Windows hakemistoista ajettaviin sovelluksiin, jolloin voit listata säännöksi ne ja tarvitsee tunnistaa vain ne ohjelmat, jotka toimivat noiden hakemistojen ulkopuolella. Kun käyttäjällä ei ole admin oikeuksia, niin edellä mainittuihin hakemistoihin ei myöskään pysty lisäämään mitään jälkikäteen, jolloin ne ovat turvallisia hakemistoja suorittaa ohjelmia. AppLocker toimii proaktiivisena tapana suojautua haitallisilta ohjelmilta. (Laiho 2014.)

Windows Hello for Business tulee tarpeeseen, kun yrityksessä otetaan lähiaikoina käyttöön Microsoft Surface Pro 4 tablet laitteet, joita tarvitsee käyttää työskentelyyn olosuhteissa missä salasanan kirjoittaminen voi olla hyvinkin hankalaa ja silloin biometrinen tunnistauminen (sormenjälki, kasvon tunnistus) on kätevin sekä turvallisin tapa hoitaa kirjautuminen laitteelle.

Windows Information Protection (WIP), joka mahdollistaa tiedon suojaamisen ja estää sen mahdollisen väärinkäytön. Kuten jo aiemmin työssä mainittiin, että sisäpiiristä tuleva uhka yrityksille on tänä päivänä hyvin todennäköinen. WIP:n avulla Windows 10 pyrkii estämään tämän uhan aiheuttaman mahdollisen haitan. Mahdollisia rajoitteita mitä tulee ottaa huomioon ennen WIP käyttöönoton suunnittelemista ovat esimerkiksi kohde yrityksessä käytössä olevat uudelleen ohjatut kansiot (folder redirection) ominaisuus, joka mahdollistaa varmuuskopioinnin palvelimille automaattisesti sekä tiedostojen offline käytön. Folder redirection ei ole tuettuna WIP:n käytännön kautta ja sitä ei voi käyttää niiden tiedostojen suojaamiseen, mutta

esimerkiksi kohde yrityksessä jo käytössä oleva OneDrive For Business on tuettu ratkaisu tai toinen mahdollinen ratkaisu on Work Folders, joka on korvannut folder redirection toiminnallisuuden.

Windows Defender on parantanut eri testeissä tasaisesti tuloksiaan, esimerkiksi AV-Testin tekemässä testissä, jossa pyrittiin testaamaan tuotetta realistisesti ja haastamaan sitä erilaisilla todellisen maailman uhkilla. Vuonna 2016 aikajaksolla maalis-ja huhtikuu tehdyillä testeillä Windows Defender tunnisti 88.9 prosenttia maaliskuussa ja 88 prosenttia huhtikuussa 0-päivä haavoittuvuuksista, kun kaikkien testattujen tuotteiden keskiarvo oli 97 prosenttia. Kun sama testi suoritettiin vuoden 2016 marras- ja joulukuun aikana tulokset olivat selvästi parantuneet, 0-päivä haavoittuvuuksista tunnistettiin marraskuussa 97.9 prosenttia ja joulukuussa 100 prosenttia. (AV-TEST 2017.)

Tämä testi jo antaa suuntaa sille, että Microsoft on selvästi alkanut vahvasti panostamaan Windows Defenderin kehittämiseen. Tulevaisuus myös näyttää positiiviseltä Defenderin kehittämisen osalta, koska Microsoft hyötyy selvästi siitä, että sillä on käytössään yli biljoonan loppu käyttäjän laitteen telemetria tiedot, joiden avulla he pystyvät keräämään eri haittaohjelmista näytteitä ja tämän avulla kehittämään entistä tehokkaampi Defender (Gartner 2017). Windows Defender Advanced Threat Protection (ATP) tarjoaa suojauksen, joka perustuu suojauksen murtumisen jälkeiseen tilaan ja sen avulla hyökkäyksien havaitseminen ja tutkiminen tulee nopeammaksi sekä tehokkaammaksi ja mahdollistaa myös pitkäjänteisten kehittyneiden uhkien tunnistamisen työasemilla sekä verkossa. Windows Defender ATP:n avulla esimerkiksi ransomwarelta suojautuminen olisi tehokkaampaa, esimerkiksi jos haitake yrittäisi poistaa käyttöjärjestelmän palautuspistettä tai tiedostojen varmuuskopioita, niin se aiheuttaisi automaattisesti hälytyksen jolloin järjestelmänvalvoja pystyy reagoimaan tilanteeseen. Tällä hetkellä Microsoftin kilpailijoilla ei ole tarjota saman tyyppistä palvelua, joka vastaisi samoihin haasteisiin kuin Defender ATP.

BIOS/UEFI salasanan käyttöönotto olisi suositeltava toimenpide, jotta mahdolliset väärinkäytöt voidaan estää yksinkertaisesti sen avulla. Esimerkiksi suojauskeinona käytetty Secure Boot on helppo käydä käydä laittamasta pois päältä, jos BIOS:a tai UEFI:a ei ole erikseen suojattu salasanalla. Sinne voi päästä sisään kuka tahansa, kenellä on fyysinen pääsy työasemalle. Kohde yrityksessä on käytössä Lenovon työasemat, joihin voidaan luoda keskitetysti ja hallitusti salasanojen pakotettu käyttö BIOS:ssa ja UEFI:ssa käyttämällä Windows Management Instrumentation (WMI) työkalua. (Lenovo 2016.)

Kehitysehdotuksista rajautuu pois Microsoft Device Guardin käyttöönotto, koska sen ylläpitäminen olisi hyvin hankalaa ja aikaa vievää. Kohde yrityksessä ei ole tällä hetkellä näköpiirissä, niin suuren riski tason omaavaa työasemaa, joka vaatisi Device Guard tasoisen suojauksen.

8 Yhteenveto

Opinnäytetyön aiheena oli tutkia mitä uhkia voidaan tunnistaa tämän hetken toimintaympäristössä ja kuinka ne voivat vaikuttaa organisaatioon. Tavoitteeksi työlle oli asettu, että siinä tuotetaan ehdotuksia sekä suosituksia kuinka yritys voi kehittää sekä parantaa tietoturvaansa Windows 10-käyttöjärjestelmän avulla.

Mielestäni onnistuin esittelemään ja käymään monipuolisesti läpi mitä tietoturvallisuus on ja kuvaamaan tämän hetken uhkat sekä mahdollisuudet mitä yrityksen näkökulmasta on oleellista huomioida. Tähän tulokseen pääsin määrittelemällä ja selittämällä mitä tietoturva on CIA-mallin (confidentialy, integrity ja availability), kolme a:n (assurance, authenticity, anonymity) sekä RMIAS-mallin (Reference Model of Information Assurance and Security) avulla. Mitkä ovat ne viisitoista tietoturva uhkaa vuonna 2016, jotka ENISA on raportissaan löytänyt ja lisäksi megatrendeiksi nostavat (Lehto ym. 2017) raportissaan kiristyshaittaohjelmien kasvun, haavoittuvuuksien hyödyntämisen, laitteistoihin kohdistuvat uhkat, yrityksen sisäpiirin hyökkäyskanavana, liiketoiminnan tuhoamiseen tähtäävät hyökkäykset ja henkilötietojen varastamiseen tähtäävät hyökkäykset. Tulevaisuuden mahdollisuuksista tietoturvan osalta voidaan myös nähdä tapahtuvan paljon positiivisia tapahtumia yhtenä esimerkkinä monet yritykset ja tietoturvayhtiöt ovat syventäneet yhteistyötään, jonka seurauksena on syntynyt monia toimintaa tehostavia prosesseja, joiden avulla tietoturvaa on parannettu. SWOT-analyysissä (Lehto ym. 2017) toivat esille mitä ovat vahvuudet, heikkoudet, uhkat ja mahdollisuudet Suomessa toimivalla yrityksellä tietoturvan osalta.

Toimeksiannossa oli määritelty, että Windows 10 käyttöjärjestelmän tietoturvaan liittyvät ominaisuudet tulisi selvittää. Ominaisuuksien löytäminen oli helppoa, mutta niiden kokoaminen ja oleellisten tietojen poimiminen hyvin laajasta aineistosta oli melko hankalaa. Oman haasteensa toi myös se seikka, että monia käyttöjärjestelmän tietoturva ominaisuuksia kehitetään ja päivitetään nopealla tahdilla, joten piti olla tarkkana siinä mitkä osat aineistosta asetti tärkeiksi ja seurasi niiden mahdollista päivittymistä.

Työn tuloksena sain aikaiseksi monta kehityskohdetta ja ehdotusta, jotka ovat konkreettisiä ja niiden käyttöönottaminen olisi mahdollista tulevaisuudessa yrityksessä. Osa ehdotuksista ja ratkaisuista olisi melko nopeaa ja helppoa ottaa käyttöön ilman suuria projekteja, mutta osa niistä vaatii selvästi suuremman panostuksen sekä ajallisesti että rahallisestikin. Näillä keskeisillä käytännön toimilla tietoturvallisuutta voidaan mielestäni saattaa entistä paremmalle tasolle yrityksessä ja toivon, että ratkaisuja hyödynnytetään tulevaisuudessa IT strategian mukaisesti.

Lähteet

Painetut lähteet:

Argiento, R. 2013. Introduction to Computer Security. Boston: Pearson.
Järvinen, P & Rousku, K. 2017. Työpaikan tietoturvaopas – tunnista uhat, hallitse riskit. Helsinki: Alma Talent.
Ojasalo, K., Moilanen, T & Ritalahti J. 2014. Kehittämistyön Menetelmät: Uudenlaista Osaamista Liiketoimintaan. 3., uudistettu painos. Helsinki: Sanoma Pro.

Sähköiset lähteet:

Akamai Technologies. 2016. State of the Internet / Security: Q2 2016 Report on DDoS & Web App Attack Trends. Viitattu 11.3.2017. https://content.akamai.com/PG6852-q2-2016-soti-security.html
AO Kaspersky Lab. 2016. KSN REPORT: RANSOMWARE IN 2014-2016. Viitattu 3.3.2017. https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf
AT&T. 2015. Decoding the Adversary AT&T Cybersecurity Insights | Volume 1. Viitattu 20.4.2017. https://www.business.att.com/cybersecurity/archives/v1/
AV-TEST. 2017. The best antivirus software for Windows Client Business User. Viitattu 17.4.2017. https://www.av-test.org/en/antivirus/business-windows-client/windows-10/
Avecto. 2016. 2016 Microsoft Vulnerabilities Report. Viitattu 17.4.2017. http://learn.avecto.com/microsoft-vulnerabilities-report-2016
Baxter J. 2015. Driver compatibility with Device Guard in Windows 10. Viitattu 15.3.2015. https://blogs.msdn.microsoft.com/windows_hardware_certification/2015/05/22/driver-compatibility-with-device-guard-in-windows-10/
Böck H. 2016. SWEET32, HEIST/TIME, PAC and WPAD leak HTTPS URLs. Viitattu 11.3.2017. https://www.feistyduck.com/bulletproof-tls-newsletter/issue_19_sweet32_heist_time_pac_and_wpad.html
Cherdantseva, Rana, Ivins & Hilton. 2016. A Multifaceted Evaluation of the Reference Model of Information
Assurance & Security. Viitattu 1.4.2017. http://rmias.cardiff.ac.uk/RMIAS_Evaluation.pdf
Cheung K. 2016. Ransomware 2016, Billion Dollar Business Nightmare. Viitattu 4.3.2017. https://www.echoworx.com/protect-sensitive-information/ransomware-2016-billion-dollar-business-nightmare/
Crowd Research Partners. 2016. Insider threat report 2016. Viitattu 6.3.2017. http://crowdresearchpartners.com/wp-content/uploads/2016/09/Insider-Threat-Report-2016.pdf
CyberEdge Group. 2016. 2016 Cyberthreat Defense Report. Viitattu 4.3.2017.

https://webroot-cms-cdn.s3.amazonaws.com/4814/5954/2435/2016_cyberedge_group_cyberthreat_defense_report.pdf

Europol. 2016. THE INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2016. Viitattu 23.3.2017. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

Fadilpasic S. 2016. Social media still an important tool for phishing. Viitattu 23.3.2017. http://www.itproportal.com/news/social-media-still-an-important-tool-for-phishing/

Federal Bureau of Investigation(FBI). 2016. Incidents of Ransomware on the Rise Protect Yourself and Your Organization. Viitattu 3.3.2017. https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

Gartner. 2017. Magic Quadrant for Endpoint Protection Platforms. Viitattu 17.4.2017. https://www.gartner.com/doc/reprints?id=1-3SOV1H2&ct=170203&st=sb

Goodin D. 2016. Why the silencing of KrebsOnSecurity opens a troubling chapter for the 'Net. Viitattu 11.3.2017. https://arstechnica.com/security/2016/09/why-the-silencing-of-krebsonsecurity-opens-a-troubling-chapter-for-the-net/

Gudkova D, Vergelis M, Demidova N & Shcherbakova T. 2016. SPAM AND PHISHING IN Q2 2016. Viitattu 14.4.2017. https://kasperskycontenthub.com/securelist/files/2016/08/Spam-report_Q2-2016_final_ENG.pdf

Hyvärinen P. 2014. Kyberturvallisuutta vai tietoturvallisuutta?. Viitattu 30.4.2017. https://coreblog.fi/2014/10/14/kyberturvallisuutta-vai-tietoturvallisuutta/

IEBlog. 2014. Certificate reputation, a novel approach for protecting users from fraudulent certificates. Viitattu 25.3.2017. https://blogs.msdn.microsoft.com/ie/2014/03/10/certificate-reputation-a-novel-approach-for-protecting-users-from-fraudulent-certificates/

KrebsonSecurity. 2016. FBI: $2.3 Billion Lost to CEO Email Scams. Viitattu 23.3.2017. https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/

Laiho S. 2014. Proactive Security Beats Reactive Security (as seen on the Windows IT Pro Insider). Viitattu 17.4.2017. http://blog.win-fu.com/2014/08/proactive-security-beats-reactive.html

Lang E. 2016. CVE-2016-4803 dotCMS - email header injection vulnerability (Full Disclosure). Viitattu 14.4.2017. https://security.elarlang.eu/cve-2016-4803-dotcms-email-header-injection-vulnerability-full-disclosure.html

Lehto M, Limnéll J, Innola E, Pöyhönen J, Rusi T, Salminen M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Viitattu 20.4.2017. http://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0

Lenovo. 2016. Lenovo BIOS Setup using WMI Deployment Guide. Viitattu 17.4.2017. https://download.lenovo.com/pccbbs/mobiles_pdf/skl_deploy_01.pdf

Lich B. 2017. BitLocker Countermeasures. Viitattu 14.4.2017. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/bitlocker-countermeasures

Lich B, Keller J & Hall J. 2017. Introduction to Device Guard: virtualization-based security and code integrity policies. Viitattu 15.3.2017. https://technet.microsoft.com/itpro/windows/keep-secure/introduction-to-device-guard-virtualization-based-security-and-code-integrity-policies

McAfee. 2016. McAfee Labs Threats Report. Viitattu 3.3.2017. https://www.mcafee.com/ca/resources/reports/rp-quarterly-threats-dec-2016.pdf

Metropolitan.fi. 2016. DDoS attack halts heating in Finland amidst winter. Viitattu 11.3.2017. http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter

Microsoft. 2017. Windows Hello for Business. Viitattu 14.4.2017. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/hello-identity-verification

Microsoft. 2017. Windows Hello biometric requirements. Viitattu 14.4.2017. https://msdn.microsoft.com/fi-fi/windows/hardware/commercialize/design/device-experiences/biometric-requirements

Microsoft. 2017. Windows Hello face authentication. Viitattu 14.4.2017. https://msdn.microsoft.com/fi-fi/windows/hardware/commercialize/design/device-experiences/windows-hello-face-authentication

Microsoft. 2017. Protect derived domain credentials with Credential Guard. Viitattu 14.4.2017. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/credential-guard

Microsoft. 2017. Hardware Compatibility Specification for Systems for Windows 10, version 1607. Viitattu 15.3.2017. https://msdn.microsoft.com/windows/hardware/commercialize/design/compatibility/systems#system-fundamentals-firmware-uefisecureboot

Microsoft. 2016. Hardware Compatibility Specification for Filter for Windows 10, version 1607. Viitattu 15.3.2017. https://msdn.microsoft.com/windows/hardware/commercialize/design/compatibility/filter

Microsoft. 2017. Hardware Security Testability Specification. Viitattu 14.4.2017. https://msdn.microsoft.com/en-us/library/windows/hardware/mt712332.aspx

Microsoft. 2016. Windows SMM Security Mitigations Table. Viitattu 14.4.2017. http://download.microsoft.com/download/1/8/A/18A21244-EB67-4538-BAA2-1A54E0E490B6/WSMT.docx

Microsoft. 2017. Windows Defender Advanced Threat Protection. Viitattu 14.4.2017. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-defender-advanced-threat-protection

Microsoft. 2017. Configure endpoint proxy and Internet connectivity settings. Viitattu 14.4.2017. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/configure-proxy-internet-windows-defender-advanced-threat-protection

Microsoft. 2017. Windows Defender ATP data storage and privacy. Viitattu 14.4.2017. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/data-storage-privacy-windows-defender-advanced-threat-protection
Microsoft. 2017. Windows Defender Antivirus in Windows 10. Viitattu 14.4.2017. https://technet.microsoft.com/itpro/windows/keep-secure/windows-defender-antivirus-in-windows-10
Microsoft. 2017. Minimum requirements for Windows Defender ATP. Viitattu 14.4.2017. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/minimum-requirements-windows-defender-advanced-threat-protection
Microsoft. 2017. Windows Hardware Certification Kit. Viitattu 14.4.2017. https://msdn.microsoft.com/en-us/windows/compatibility/windows-hardware-certification-kit
Microsoft. 2017. Microsoft BitLocker Administration and Monitoring. Viitattu 14.4.2017. https://technet.microsoft.com/en-us/windows/hh826072.aspx
Microsoft. 2017. Protect your enterprise data using Windows Information Protection (WIP). Viitattu 14.4.2017. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/protect-enterprise-data-using-wip
Microsoft MSDN. 2016. AppLocker CSP. Viitattu 25.3.2017. https://msdn.microsoft.com/en-us/windows/hardware/commercialize/customize/mdm/applocker-csp
Microsoft Technet. 2017. AppLocker. Viitattu 25.3.2017. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/applocker-overview
Mimoso M. 2016. IOT BOTNETS ARE THE NEW NORMAL OF DDOS ATTACKS. Viitattu 1.4.2017. https://threatpost.com/iot-botnets-are-the-new-normal-of-ddos-attacks/121093/
National Cyber Security Centre Netherlands. 2016. Cyber Security Assessment Netherlands 2016. Viitattu 12.3.2017. https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html

NSS Labs. 2016. Web Browser Security Comparative Report - SEM Protection. Viitattu 25.3.2017. http://research.nsslabs.com/reportaction/free-114/Marketing
NSS Labs. 2016. Web Browser Security Comparative Report: Phishing Protection. Viitattu 25.3.2017. http://research.nsslabs.com/reportaction/free-113/Marketing
NSS Labs. 2016. Browser Security Comparative Analysis Report - Socially Engineered Malware Edition 7. Viitattu 25.3.2017. http://research.nsslabs.com/reportaction/report-28/Marketing
Panmore Institute. 2016. The CIA Triad: Confidentiality, Integrity, Availability. Viitattu 26.3.2017.http://panmore.com/the-cia-triad-confidentiality-integrity-availability
Rubin A. 2017. Trendianalyysi tulevaisuudentutkimuksen menetelmänä. Viitattu 11.4.2017. https://tulevaisuus.fi/menetelmat/toimintaympariston-muutosten-tarkastelu/trendianalyysi-tulevaisuudentutkimuksen-menetelmana/
Saltzer J.H ja Schroeder M.D. 1975. “The protection of information in computer systems” Proceedings of the IEEE. Viitattu 1.4.2017. http://ieeexplore.ieee.org/document/1451869/
Settle A, Dey B, Griffin N & Toro A. 2016. Analysis of a botnet campaign. Viitattu 23.3.2017.

https://www.forcepoint.com/sites/default/files/resources/files/report_jaku_analysis_of_botnet_campaign_en_0.pdf

Siddique K, Akhtar Z & Kim Y. 2017. Biometrics vs passwords: a modern version of the tortoise and the hare. Computer Fraud & Security. Viitattu 25.3.2017. http://www.sciencedirect.com/science/article/pii/S1361372317300076

Spring T. 2016. NECURS BOTNET IS BACK, UPDATED WITH SMARTER LOCKY VARIANT. Viitattu 4.3.2017. https://threatpost.com/necurs-botnet-is-back-updated-with-smarter-locky-variant/118883/

Sucuri Inc. 2016. WEBSITE HACKED TREND REPORT 2016 - Q1. Viitattu 3.3.2017. https://sucuri.net/website-security/Reports/Sucuri-Website-Hacked-Report-2016Q1.pdf

Symantec Corporation. 2016. Internet Security Threat Report. Viitattu 4.3.2017. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_9562&om_sem_kw=elq_14669249&om_ext_cid=biz_email_elq_

Talos. 2015. THREAT SPOTLIGHT: CISCO TALOS THWARTS ACCESS TO MASSIVE INTERNATIONAL EXPLOIT KIT GENERATING $60M ANNUALLY FROM RANSOMWARE ALONE. Viitattu 11.3.2017. http://www.talosintelligence.com/angler-exposed/

The European Union Agency for Network and Information Security (ENISA). 2017. ENISA Threat Landscape Report 2016 - 15 Top Cyber-Threats and Trends. Viitattu 3.3.2017. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport

Trendmicro. 2016. The Reign of Ransomware. Viitattu 4.3.2017. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/rpt-the-reign-of-ransomware.pdf

Verizon Enterprise. 2016. 2016 Data Breach Investigations Report. Viitattu 4.3.2017. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Viestintävirasto. 2016. Exploit kit - tehokas haittaohjelmien levittäjä. Viitattu 11.3.2017. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/03/ttn201503061108.html

Virtru Blog. 2016. Insider Threat Detection in Government Cyber Security. Viitattu 4.3.2017. https://www.virtru.com/blog/insider-threat-detection/

W3C. 2016. Web Authentication: An API for accessing Scoped Credentials. Viitattu 25.3.2017. https://w3c.github.io/webauthn/

WhiteHat Security. 2016. Web Applications Security Statistics Report. Viitattu 4.3.2017. https://www.whitehatsec.com/info/website-stats-report-2016-wp/

Wolff J. 2016. The New Economics of Cybercrime. Viitattu 5.3.2017. https://www.theatlantic.com/business/archive/2016/06/ransomware-new-economics-cybercrime/485888/

Kuviot