jamk

Turvallisesti pilvessä

Microsoft Office 365 pilvisovellusten pääsynhallinta ja turvallinen käyttö

Jon Sundberg

Opinnäytetyö, AMK
Toukokuu, 2022
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Sundberg, Jon

Turvallisesti pilvessä

Jyväskylä: Jyväskylän ammattikorkeakoulu. **Huhtikuu 2022**, 50 sivua.

Tekniikan ala, Tieto ja viestintätekniikan insinööri, Kyberturvallisuus

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Opinnäytetyön tarkoituksena on tutkia mitä eri vaatimuksia pääsynhallinnan, tiedon tallentamisen ja tietoturvallisen käytön toteutuksessa on otettava huomioon julkishallinnollisessa organisaatiossa. Tavoitteena on luoda opinnäytetyöstä ohjenuora turvalliseen pilvipalvelun käyttöön ja antaa kuva, mitä vaatimuksia organisaation on otettava huomioon. Tavoitteena oli myös perehdyttää käyttäjä pilvipalveluihin liittyviin uhkiin sekä pääsynhallinnan toteutuksen tärkeyteen.

Tutkielma toteutettiin perehtymillä julkisiin suosituksiin, säädöksiin ja lainsäädäntöön, haastateltiin tietoturva-alalla olevia henkilöitä sekä perehdyttiin Microsoftin tarjoamien pilvipalveluiden tietoturvakontrolleihin. Haastateltavien toimenkuvaan kuuluu pilvipalveluiden käyttöönotto ja tietoturvan ylläpito. Tutkielmassa perehdyttiin myös Microsoftin viralliseen tekniseen dokumentaatioon, mikä mahdollistaa tutkielman hyödyntämisen Microsoftin pilvipalveluiden käyttöönotossa.

Haastattelujen ja tutkinnan perusteella ilmeni, että pilvipalveluiden tietoturvan uhat on tiedostettu organisaatioissa sekä teknistä dokumentaatiota ja ohjeita löytyy runsaasti. Tosin selkeitä käytännön ohjeita tai suosituksia toteutustavoista ei löytynyt helposti. Havaintona oli, että pilvipalveluiden tietoturvan yhtenä uhkana on tietämyksen puute sekä helppous palveluna, jolloin riittäviä kontrolleja, sopimuksia tai käytäntöjä ei huomioida käyttöönotossa. Toisena havaintona oli eri tietoturvaa parantavien työkalujen suuri määrä, sekä näiden työkalujen monipuolisuus vaihtelevissa ympäristöissä.

Avainsanat (asiasanat)

Pilvipalvelut, pääsynhallinta, tietoturva, tietoturvallisuus, julkishallinto

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Sundberg, Jon

Cloud security

Jyväskylä: JAMK University of Applied Sciences, April 2022, 50 pages.

School of Technology. Degree Programme in information and communication technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The purpose of the thesis is to study what different requirements must be considered in the implementation of access control, data storage and information security in a public administration organization. The aim is to create a guideline for the safe use of the cloud service from the thesis and to give an idea of what requirements the organization must follow. The goal was also to familiarize the user with the threats related to cloud services, as well as the importance of implementing access control.

The thesis was carried out by studying public recommendations, regulations and legislation, interviewing people in the information security industry, and looked at the security controls of cloud services provided by Microsoft. The job descriptions of the interviewees include the implementation of cloud services and the maintenance of data security. The thesis also looked at Microsoft's official technical documentation, which enables the thesis to be utilized in the implementation of Microsoft's cloud services.

Based on the interviews and the investigation, it became clear that the security threats to cloud services have been recognized in the organizations, and there is a lot of technical documentation and instructions. However, clear practical instructions or recommendations on implementation methods were not easily found. It was observed that the combined threat to the information security of cloud services is the lack of knowledge and ease as a service, in which case sufficient controls, agreements or practices are not considered in the implementation. Another finding was the large number of different tools that improve security, as well as the versatility of these tools in varying environments.

Keywords/tags (subjects)

Cloud services, Access control, Information security, Public administration

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Termit ja lyhenteet

AD Active Directory on Microsoftin Azuressa oleva palvelin, johon tallentuu yrityksen henkilökunnan käyttäjätunnukset ja muita mahdollisia tietoja (Microsoft 2021b).

CA Conditional Access on Microsoftin Azuressa oleva työkalu, jolla voidaan hallita mm. organisaation pääsynhallintasääntöjä (Microsoft 2022i).

DC Domain controller palvelin, jonka kautta hallitaan käyttäjiä, laitteita, ryhmiä (Petters 2020).

GDPR General Data Protection Regulation, eli yleinen tietosuoja-asetus. Laki on luotu säätelemään henkilötietojen käsittelyä kaikissa EU-maissa. (Tietovaltuutetun toimisto n.d.)

IaaS Infrastructure as a Service pilvipalvelumallissa palveluntuottaja tarjoaa asiakkaalle palvelun siten että asiakkaan käyttöön tulee web-pohjainen liittymä, jonka kautta onnistuu palvelun hallinta. (IBM 2021).

M365 Microsoft 365 tarkoittaa Microsoftin M365 lisenssin palveluita, joihin kuuluu O365 lisenssin lisäksi kattavammat tietoturvatyökalut (Poisson, 2020).

MDC Microsoft Defender for Cloud on Microsoftin pilviympäristön hallinnan ja suojauksen työkalu (Azure n.d.).

MDE Microsoft Defender for Endpoint on Microsoftin pilvessä operoiva työasemasuojauksen hallintatyökalu (Microsoft 2022j).

MDI Microsoft Defender for Identity on Microsoftin identiteetin suojauksen pilvessä operoiva palvelu (Microsoft 2021a).

MDO Micorosft Defender for Office on Microsoftin pilvisovellusten suojaukseen luotu työkalu (Microsoft 2022j).

MFA Multi-factor authentication on kaksivaiheinen todentaminen, toiselta nimeltään 2fa. Kirjautuminen vahvistetaan jollain toisella varmenteella. (Magic Cloud 2019.)

O365 Office 365 tarkoittaa Microsoft Officen peruspalveluita, kuten Word, Excel, Powerpoint, Sharepoint, Onedrive jne (Poisson, 2020).

PaaS Platform as a Service pilvipalvelumallissa palveluntarjoaja tarjoaa alustan palvelulle, johon asiakas pystyy haluamansa palvelun siirtämään (IBM 2021).

SaaS Software as a Service pilvipalvelumallissa palveluntarjoaja vastaa koko ohjelmistosta. Asiakas toimii käyttäjänä. SaaS palvelua käytetään tyypillisesti internet selaimen kautta. (IBM 2021.)

SOC Security Operations Center eli tietoturvavalvomo, johon keskitetään organisaation tietoturvaan liittyvät herätteet. SOC:n tehtävänä on valvoa ja reagoida tietoturvauhkiin. (Microfocus 2021.)

XDR Extended detection and response tarkoittaa usean tason suojausta. Päätelaitesuojauksen lisäksi XDR suojaa, sekä valvoo verkkoliikennettä, pilviliikennettä, palvelimia ja sähköpostia. (Aarness 2022.)

1 Johdanto

Pilvipalvelut ovat tärkeä osa organisaatioiden työskentelyä ja tiedonhallintaa. Yhä useammin tietoa ja toimintaa siirretään pilveen fyysisten tallennuspaikkojen sijaan. Pilvipalveluiden käyttämisessä piilee kuitenkin riskejä ja haasteita, joten on tärkeää, että organisaatiot tietävät, mitä haluavat pilvipalvelulta ja mitä palveluita heille on saatavilla. Pilvipalveluiden käyttöönotto ja turvallinen käyttö ovat siis ajankohtaisia ja tärkeitä asioita hyvin monessa yrityksessä ja organisaatiossa. Aihe on ajankohtainen, koska pilvipalveluiden käyttö yleistyy jatkuvasti ja käytännöt ovat hyvin vanhanaikaisia. Oikein toteutettuna pilvipalveluiden käyttö on turvallista, tehokasta sekä monimuotoista.

Tämän opinnäytetyön tarkoituksena oli selvittää, mitä seikkoja julkishallinnollisten toimijoiden tulisi ottaa huomioon pilvipalveluiden käyttöönotossa, käytössä ja pääsynhallinnassa. Tutkimuksessani selvitin, mitä rajoitteita, ohjeita ja suosituksia pilvipalveluiden käyttöön on annettu valtiotasolta. Lähempään tarkasteluun otin Microsoftin O365-pilvipalvelun sisältämät pääsynhallinnan, tiedonkäsittelyn, eheyden sekä luottamuksellisuuden työkalut.

Toteutin opinnäytetyön tutustumalla viralliseen dokumentaatioon, ohjeistuksiin sekä perehtymällä tekniseen käytäntöön. Ennen keskittymistä Microsoftin O365-pilvipalveluun on tärkeää hahmottaa, mitä pilvipalvelut ylipäätään ovat ja mitä linjauksia, kontrolleja ja suosituksia niille on annettu. Tutkimuksen tavoitteena oli löytää vastaus tutkimuskysymykseen: mitä on otettava huomioon turvallisessa O365-pilvipalveluiden käyttöönotossa ja käytössä julkishallinnollisen toimijan ympäristössä. Tutkimuksessani haastatteluun valikoitui kaksi tietoturva-asiantuntijaa ja tietoturvapäällikkö julkishallinnollisessa yrityksessä. Tutkin myös tarkemmin, miten pääsynhallinnalla voidaan turvallisesti käyttää O365-pilvipalveluita sekä mitä uhkia pilvipalvelun käyttö tuo mukanaan.

Tutkimuksessa käsitellään myös sitä, miten pilvipalveluiden pääsynhallinta ja tietoturvallinen käyttö tulisi toteuttaa, jolloin tutkimusta voisi käyttää apuna pilvipalveluiden käyttöönotossa. Tavoitteena oli luoda organisaatioille selkeä muistilista siitä, mitä pilvipalveluiden käyttöönotossa ja käytössä tulisi ottaa huomioon. Muistilista löytyy liitteestä 1. Aihe koskettaa tutkijan omaa työnkuvaa tietoturva-asiantuntijana julkishallinnollisella puolella. Yhtenä vastuualueenani on pilvipalveluiden tietoturva ja pääsynhallinta, joten aiheen tutkiminen ja tämän opinnäytetyön tekeminen laajentavat ja kehittävät myös omaa osaamista sekä tietotaitoa.

Työn toimeksiantajana toimi Jyväskylän Ammattikorkeakoulun (Jamk) CYBERDI-projekti. CYBERDI-projekti toimii Jamk:n IT-instituutissa, jossa opiskellaan kyberturvallisuutta, ohjelmointia sekä tietojärjestelmien kehittämistä, ylläpitoa ja hallintaa. Jamk:n IT-instituutista valmistuu opiskelijoita AMK-insinööreiksi ja ICT-tradenomeiksi. CYBERDI-projekti tehdään yhteistyössä Poliisiammattikorkeakoulun (POLAMK) kanssa ja tavoitteena on kehittää kyberrikollisuuden havainnointia, tutkintaa ja kehittää asiantuntijoita riittävälle tasolle Euroopassa. Projektin tavoitteena on myös kasvattaa tietoisuutta kyberrikollisuudesta yritysmaailmassa, terveydenhoitopuolella sekä sosiaalisen median käytössä. Lisäksi tavoitteena on kehittää laajempaa osaamista suomalaisten ICT käyttäytymisessä (CYBERDI n.d.).

Jyväskylän ammattikorkeakoulu on 8500 opiskelijan vuonna 1994 perustettu koulu, josta valmistuu vuosittain yli 1500 opiskelijaa kahdeksalle eri alalle. Jamk:n omistaa Jyväskylän kaupunki (90 %), Äänekosken ammatillisen koulutuksen kuntayhtymä POKE (5 %) ja Jämsän kaupunki (5 %). Yhtiön toimialana on AMK:n ylläpito. Jamk:ssa on mahdollista opiskella yli 40 tutkintoa seitsemällä eri alalla ja kumppaniverkoston kautta opiskelijoita on yli 70 eri maasta. Organisaationa Jamk:lla on neljä yksikköä koulutukselle sekä erillinen hallintoyksikkö. Koulutusta tuotetaan ammatillisessa opettajakorkeakoulussa, hyvinvointi-, liiketoiminta-, ja teknologiayksiköissä Vahvuusaloiksi Jamk on määritellyt biotalouden, monialaisen koulutuksen, sovelletun kyberturvallisuuden, automaation ja robotiikan, matkailun sekä uudistuvan oppimisen. Vahvuusalat ovat tunnettuja kansainvälisellä tasolla ja jokainen vahvuusala on Keski-Suomen maakuntastrategian ja Jyväskylän kaupungin kasvusopimuksen kanssa yhteensopivia. (Jamk n.d.).

2 Tutkimusmenetelmät

2.1 Tutkimuskysymys

Tutkimuksen tavoitteena on selvittää mitä on huomioitava Microsoftin pilvipalvelun käyttöönotossa tietoturvan osalta julkishallinnollisen toimijan organisaatiossa. Tavoitteena on antaa muistilista, jota organisaatio pystyy hyödyntämään suunnitellessaan pilvipalveluiden käyttöönottoa.

Opinnäytetyön tavoitteena on antaa vastaus tutkimuskysymykseen:

- Mitä on otettava huomioon turvallisessa O365-pilvipalveluiden käyttöönotossa ja käytössä julkishallinnollisen toimijan ympäristössä?

Tämä on kysymys, jonka ympärille opinnäytetyö rakentuu. Koska kysymys on laaja, on kysymys jaettu alakysymyksiin, jotka rajaavat ja antavat suunnan pääkysymykselle.

- Miten pääsynhallinnan avulla voidaan turvallisesti käyttää O365-pilvipalveluita?
- Mitä uhkia pilvipalvelun käyttö tuo mukanaan?

2.2 Tutkimusmetodologia

Kvalitatiivinen menetelmä, eli laadullinen tutkimus, valikoitui tutkimuksen metodologiaksi. Kvalitatiivinen tutkimus eroaa kvantitatiivisesta tutkimuksesta eniten aineiston hankinnan osalta. Kvantitatiivisessa tutkimuksessa pyritään matemaattisin keinoin tilastollisesti löytämään vastauksia, kun taas laadullisessa tutkimuksessa tiedon luonne on erilainen. (Grönfors 2011, 4—5.)

Laadullista tutkimusta voidaan tehdä hyvin monella eri tavalla (Tuomi & Sarajärvi 2009, 9). Tutkijan on tärkeää miettiä, minkälainen lähestymistapa sopii juuri omaan tutkimukseen. Valitsin laadullisen tutkimuksen, koska sen avulla pääsen syvällisemmin pureutumaan siihen, miten julkishallinnollisen toimijan ympäristössä pilvipalvelut on otettu käyttöön ja miten niiden tietoturvasta pidetään huolta. Laadullisen tutkimuksen ominaispiirteisiin voidaan luokitella tietynlaisen aineiston käyttö, joka tässä tutkimuksessa on haastattelu (Juhila n.d.). Laadullisen tutkimukseen kuuluu

olennaisesti myös teoria ja sen suhde tutkittavaan asiaan. Teoria antaa pohjaa tutkittavalle aiheelle. (Sarajärvi & Tuomi 2017.)

Tutkimus toteutettiin perehtymällä viralliseen dokumentaatioon, ohjeistuksiin ja teknisiin käytäntöihin, sekä haastattelemalla kolmea alalla työskentelevää henkilöä. Haastattelut toteutettiin anonyymisti ja heihin viitataan nimikkeellä Haastateltava 1, 2 ja 3.

2.3 Aineiston kerääminen

Työ aloitettiin tutkimalla pilvipalveluiden pääsynhallinnan ja tietoturvan eri toteutusmetodeja sekä millaisia kontrolleja ja suosituksia julkishallinnon toimijoille on asetettu. Keskityin erityisesti Microsoftin 365-pilvipalveluun. Tietoa kerättiin myös tutkijan työkokemuksen ja haastattelujen avulla. Haastattelu on yksi laadullisen tutkimuksen aineistonkeruumenetelmistä (Saaranen-Kauppinen & Puusniekka 2006). Haastattelun avulla saadaan tietoa juuri kyseessä olevasta asiasta. Se on hyvin yleinen tapa tehdä laadullista tutkimusta. (Hyvärinen, Suoninen & Vuori n.d.) Tässä tutkimuksessa haastatteluiden tavoitteena on syventää tiedonhankinnan kautta saatua tietoa erityisesti O365-pilvipalveluiden käyttöönotosta ja käytöstä.

Haastattelut toteutettiin teemahaastatteluna. Teemahaastattelussa tutkija määrittelee isommat teemat, joihin kysymykset liittyvät. Tämä antaa haastateltavalle tilaa kertoa vapaammin omista ajatuksistaan. (Hyvärinen ym. n.d.) Toinen tapa luokitella haastattelua on miettiä, kuinka valmiiksi jäsennelty se on (Saaranen-Kauppinen & Puusniekka 2006). Lähtökohtana on siis myös puolistrukturoitu haastattelu. Se antaa tilaa haastateltavalle, mutta myös ohjaa kysymyksillään. Tärkeää huomioitavaa verrattuna strukturoituun haastatteluun on kuitenkin se, että tutkija voi poiketa kysymyslistastaan ja elää haastattelussa mukana. Tarkkoja kysymyksiä kannattaa kuitenkin miettiä valmiiksi varsinkin asiantuntijahaastatteluissa, jotta saadaan esille faktat, joihin ollaan vastausta etsimässä. (Hyvärinen ym. n.d.)

2.3.1 Haastateltavat

Haastateltavina toimivat kaksi eri tietoturva-asiantuntijaa sekä tietoturvapäällikkö julkishallinnollisesta organisaatiosta. Haastateltavien valikoitumiseen vaikutti se, että heistä jokainen käyttää or-

ganisaatiossaan Microsoftin pilvipalveluita, sekä jokaisen työtehtävään kuuluu pilvipalveluiden tietoturvasta huolehtiminen. Haastateltavat eivät esiinny nimillä vaan heihin viitataan Haastateltava-nimikkeellä. Alla taulukko (taulukko 1), josta näkyy haastateltavien taustatekijät.

Taulukko 1 Haastateltavien taustatiedot

	Haastateltava 1	Haastateltava 2	Haastateltava 3
Titteli	Tietoturva-asiantuntija	Tietoturva-asiantuntija	Tietoturvapäällikkö
Työuran pituus/kokemus	3-vuotta	2-vuotta	10-vuotta
Microsoftin pilvipalvelut	O365-palvelut, M365 Security	O365-palvelut, M365 Security	O365-palvelut

2.4 Tutkimuseettinen tarkastelu

Aihe on lähellä tutkijaa itseään, joten täysin objektiivinen näkökulma on mahdoton toteuttaa. Kuten Grönfors (2011, 5) kertoo: ”*Kvalitatiivista tutkimusta suorittavat tutkijat tuskin voivat sanoa tutkimuksensa olevan objektiivista, koska tutkija itse on tärkein tutkimusväline.*” Koen oman asiantuntemuksen aiheesta kuitenkin syventävän tutkimusta. On kuitenkin tärkeää, että otan huomioon sen, että aihe on minulle jo ennestään tuttu.

Tutkimusta tehdessä on tärkeää ottaa huomioon tutkimuksen eettisyys. Tutkimukseen osallistuneet haastateltavat osallistuivat haastatteluun vapaaehtoisesti ja heidän tietojaan käsitellään luot-

tamuksellisesti. (Leinonen 2018.) Tutkimuksen luottamuksellisuuden vuoksi on tärkeää, ettei yksittäistä ihmistä voida tunnistaa haastattelun perusteella (Tuomi & Sarajärvi 2009, 22). Ottaen huomioon, että kyseisessä tutkimuksessa avataan pilvipalveluiden tietoturvaa ja organisaatioiden asiantuntijoiden ajatuksia siitä, on hyvin tärkeää, että tietoa käsitellään varoen ja luottamuksellisesti. Hyvään tieteelliseen käytäntöön kuuluukin se, että tutkija noudattaa huolellisuutta ja tarkkuutta työssään (Tutkimuseettinen neuvottelukunta 2012, 6).

2.5 Rajaukset

Pilvipalveluita on hyvin paljon erilaisia. Rajaan työni koskettamaan pääosin Microsoftin Office 365-palveluita julkishallinnon organisaatiossa. Työssä ei käsitellä kaikkia Microsoftin tietoturvapalveluita vaan niitä, jotka liittyvät pilvipalveluihin, pilvipalvelun tietoturvaan tai pääsynhallintaan.

3 Mikä on pilvipalvelu?

Pilvipalvelu on palvelutyyppi, jossa käyttäjä ostaa palvelun tuotettuna muualla. Pilvipalvelulla ei ole fyysistä sijaintia käyttäjällä vaan kaikki tietojenkäsittelyratkaisut toimivat verkon yli. (Ranger, S. 2022.) ”*Pilvipalveluiden avulla organisaatiosi voi ottaa nopeasti käyttöön uusia ratkaisuja ilman omia järjestelmä-, laite- tai ohjelmistoinvestointeja (VM IT n.d.).*”

Pilvipalveluiden käyttö kasvaa koko maailmassa jatkuvasti. Vuonna 2021 n. 41 % EU:n alueella toimivista yrityksistä käyttää pilvipalveluita sähköpostin sekä tiedostojen hallinnassa. Verrattuna aikaisempaan vuoteen, kasvua on ollut 5 %. Vastaavasti suomalaisista yrityksistä 75 % käyttää pilvipalveluita ja Suomi on kärkimaita pilvipalveluiden käytössä koko EU:n alueella. (Eurostat 2021.)

Kuviossa (Kuvio 1) on kuvattu maksullisten pilvipalveluiden määrän nousua viimeisten vuosien aikana. Eli kuviossa nähdään kuinka monta prosenttia suomalaisista yrityksistä käyttää pilvipalveluita vuosittain.

Kuvio 1 Maksullisten pilvipalveluiden käytön määrä suomalaisissa yrityksissä (Ficom 2021)

3.1 PiTuKri

Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) tarkoituksena on edesauttaa viranomaisten tietoturvallista pilvipalveluiden käyttöä tietojen käsittelyn yhteydessä. PiTuKri on tarkoitettu arviointikriteeristöksi pilvipalveluiden turvallisuudelle ja se on luotu Suomen kansallisten toimijoiden perspektiivistä. Kriteeristön luomisessa on otettu huomioon BSI:n pilviturvallisuuskriteeristö, CSA-pilviturvallisuusyhteisön suojausmatriisi, ISO27001[5]- ja ISO27017[6]-standardit. Lisäksi on huomioitu Katakri-kriteeristö. PiTuKri:n tavoite on toimia tukena Valtiovarainministeriön julkisen hallinnon pilvipalveluiden linjausten käyttöönotossa. (Traficom 2020b, 3.) Kriteeristön tavoitteena on saada pidettyä mahdolliset tietoihin kohdistuvat riskit mahdollisimman pienenä.

PiTuKri on jaettu 11 eri osa-alueeseen. Osa-alue 1 on erityisasemassa muihin osa-alueisiin verrattuna. Esiehdot määrittävät jatkoarvioinnin tarpeen. PiTuKri:n osa-alueet ovat:

- Osa-alue 1: Esiehdot
- Osa-alue 2: Turvallisuusjohtaminen
- Osa-alue 3: Henkilöstöturvallisuus
- Osa-alue 4: Fyysinen turvallisuus
- Osa-alue 5: Tietoliikenneturvallisuus
- Osa-alue 6: Identiteetin ja pääsyn hallinta
- Osa-alue 7: Tietojärjestelmäturvallisuus
- Osa-alue 8: Salaus
- Osa-alue 9: Käyttöturvallisuus
- Osa-alue 10: Siirrettävyys ja yhteensopivuus
- Osa-alue 11: Muutostenhallinta ja järjestelmäkehitys

Nämä osa-alueet koostuvat vaatimuskorteista. Kortteihin on määritelty teema, itse vaatimus, miten vaatimusta voidaan soveltaa, mikä on suojaustavoite sekä lisätiedot, jotka helpottavat vaatimuksen toteuttamista ja tulkintaa. (Traficom 2020b, 7.)

3.2 Katakri – tietoturvallisuuden auditointityökalu viranomaisille

Katakria käytetään yritysten turvallisuusjärjestelyjen ja viranomaisten tietojärjestelmien turvallisuuden auditointi- sekä arviointityökaluna. Katakri on luotu varmistamaan, että organisaaioiden tietoturvallisuus salassapidettävän tiedon paljastumisen ehkäisemiseksi on kunnossa ja tietovuodon riski minimoitu. Yleisesti Katakri on luotu kansainvälisten säädösten ja velvoittein vähittäisvaatimuksin. (Traficom 2020a, 5.)

Katakri on jaettu kolmeen osa-alueeseen: Turvallisuusjohtaminen, Fyysinen turvallisuus ja Tekninen tietoturva. Turvallisuusjohtaminen osa-alueessa tarkastellaan organisaation tietoturvan hallintajärjestelmää ja henkilöstön kyvykkyyttä turvallisuusluokitellun tiedon hallintaa ja suojausta varten. Fyysisen turvallisuuden osa-alueessa käsitellään turvallisuusluokiteltujen tietojen käyttöympäristön tietoturvavaatimuksia. Teknisessä osiossa käsitellään teknisen tietojenkäsittelyympäristön tietoturvaa. (Traficom 2020a, 5.)

3.3 Julkisen hallinnon pilvipalvelu-linjaukset

Valtiovarainministeriö on julkaissut julkisen hallinnon pilvipalvelulinjaukset 18.1.2019 (Valtiovarainministeriö 2019). ”*Linjaukset määrittävät, miten julkisen hallinnon organisaation omistamaa tietoa voidaan käsitellä pilvipalveluissa*.” Tavoite on olla tukena valtion, maakuntien ja kuntien päätöksenteossa uusia ICT-palveluita suunnitellessa ja hankkiessa. (Valtiovarainministeriö 2018.) Pilvipalveluiden käyttö on kasvanut erityisesti nyt koronan vuoksi. Sen takia nämä linjaukset ovat tärkeitä. (Mutta 2020.)

Mutta (2020) kertoo linjausten näkökulmista, joita ovat ohjausvaikutuksen vaikuttavuus, kustannus-hyöty-arviointi, hankinta ja sopimukset sekä tavoiteltu riskitaso uuden teknologian käyttöönotossa. Seuraavassa listassa on esitettynä julkisen hallinnon pilvipalvelulinjaukset (Valtiovarainministeriö 2018, 9—10):

1. *”Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta”*
2. *”Pilvipalveluissa on kiinnitettävä erityistä huomiota sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen”*

3. *”Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset”*
4. *”Mikäli pilvipalvelu tai pilvipalveluteknologia tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita”*
5. *”Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti sekä oleellisten sopimusehtojen muuttuessa.”*
6. *”Julkisen tiedon käsittelyä ei rajoiteta”*
7. *”Ei-julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu”*

Linjaukset on tehty hyödyntäen Norjassa, Skotlannissa ja Kanadassa käytössä olevista vastaavista linjauksista sekä linjausten luonnissa on myös huomioitu VAHTI-tietoturvaohjeistusta (Valtiovarainministeriö 2018, 11: Mutta 2020).

Valtiovarainministeriön (2018, 13) mukaan on kolme eri pilvipalvelutyyppiä:

- *”Yksityinen Pilvi (Private cloud)”*
- *”Julkinen pilvi (Public cloud)”*
- *”Hybridi pilvi (Hybrid cloud)”*

Yksityinen pilvi on palvelutyyppi, jossa pilvipalvelu tuotetaan vain palvelua käyttävälle organisaatiolle. Pilvipalvelun konfigurointi suoritetaan asiakasorganisaation vaatimusten mukaisesti. Tyypillisesti palvelu, käyttö ja takuusopimukset on neuvoteltavissa ja käyttäjän vaikuttavuus sopimuksiin tyypillisesti laaja. Julkinen pilvi on pilvipalvelun tyyppi, mikä on julkisesti tarjolla ja hankittavissa. Pilvipalvelua ei käyttäjäorganisaatio voi juurikaan muokata palvelu, käyttö ja takuusopimukset on palvelutarjoajan määrittelemät. Hybridi pilvi on pilvipalvelutyyppi, missä yhdistyy yksityinen pilvi tai oma konesali julkisen pilven kanssa yhdeksi palveluksi. Hybridi pilvi tyyppisessä ratkaisussa voidaan hyödyntää julkista pilvipalvelua kapasiteetin laajentamisessa ja tieto voidaan hajauttaa eri pilvipalveluiden välillä. Tyypillisesti palvelu, käyttö ja takuusopimukset on neuvoteltavissa ja muotoiltavissa asiakasorganisaation tahtotilan mukaan. (Valtiovarainministeriö 2018, 14—15.)

Valtiovarainministeriön (2018, 13) mukaan pilvipalvelut on toteutettu kolmen eri pääpalvelumallin mukaan:

- Infrastruktuuri palvelu (IaaS)

- Ohjelmistoalusta palvelu (Paas)
- Ohjelmisto palvelu (SaaS)

Kuviossa 2 on eritelty, miten eri palvelumalleissa vastuu on jaettu toimittajan ja asiakkaan välillä. On tärkeää huomioida, että vastuu tiedon suojelemisesta kuuluu sekä asiakkaalle että palveluntarjoajalle (Harvey 2018).

IaaS	PaaS	SaaS
Tieto	Tieto	Tieto
Käyttöliittymät	Käyttöliittymät	Käyttöliittymät
Sovellukset	Sovellukset	**VASTUU SIIRTYY**
Väliohjelmisto	**VASTUU SIIRTYY**	Sovellukset
Käyttöjärjestelmät	Väliohjelmisto	Väliohjelmisto
Virtuaalilaitteet	Käyttöjärjestelmät	Käyttöjärjestelmät
Virtuaaliverkot	Virtuaalilaitteet	Virtuaalilaitteet
VASTUU SIIRTYY	Virtuaaliverkot	Virtuaaliverkot
Hypervisor	Hypervisor	Hypervisor
Prosessointi ja muisti	Prosessointi ja muisti	Prosessointi ja muisti
Tallennustila	Tallennustila	Tallennustila
Verkon käyttöliittymät	Verkon käyttöliittymät	Verkon käyttöliittymät
Datakeskukset	Datakeskukset	Datakeskukset

Kuvio 2 Pilvipalvelumallit (Harvey 2018)

3.4 Pilvipalvelun mukana tulevat uhat

Pilvipalveluita käyttöönottaessa on varauduttava uusiin uhkiin ja erilaisiin hallintakeinoihin turvallisen käytön varmistamiseksi. On arvioitava, minkälaisella toteutuksella haluaa pilviympäristön olevan, millaiset vastuut ja omistajuudet ympäristössä on. Nämä pystytään parhaassa tapauksessa sopimaan asiakkaan toiveiden mukaiseksi, jos ympäristön muokattavuus sen sallii. (Vetikko 2020a.) Myös Kyberturvallisuuskeskus (2014, 7) toteaa raportissaan ”*Palvelua käyttöönottavan organisaation voi olla järkevää sisällyttää sopimukseen mahdollinen auditointioikeus sen tarkastamiseen, että yrityksen tietoja käsitellään laaditun palvelusopimuksen mukaisesti.*” Kauppi (2019) on myös sitä mieltä, että pilvipalveluiden käyttö soveltuu julkishallinnolliseen käyttöön. On kuitenkin tärkeää huomioida lainsäädäntö ja varmistaa palvelun turvallisuus.

Alla olevassa kuviossa (Kuvio 3) nähdään, miten kyberhyökkäysten määrä on noussut maailmalla vuoden 2020 alusta vuoden 2021 loppuun. Kuviossa on laskettu mukaan kaikki kyberhyökkäykset, mutta antaa osviittaa myös pilvipalveluihin kohdistuvien uhkien määrän noususta. Kuviossa ei ole eriteltynä julkishallinnollisten toimijoiden organisaatioita, vaan diagrammi kuvaa kaikkien alojen toimijoita.

Kuvio 3 Kyberhyökkäysten määrän nousu (Check Point n.d)

Alalukuihin olen kerännyt yleisimmät uhat, joita tutkimuksen aikana nousi esiin. Uhat eivät ole vakavuus tai tärkeysjärjestyksessä, koska eri toimintaympäristöissä uhkien riskin suuruus vaihtelee. Uhat on koottu Vetikon (2020 b,c) koostaman listauksen uhista, keskittyen julkishallinnollisen toimijan ympäristöön kohdistuvista riskeistä.

3.4.1 Uhka 1: Tiedon omistajuus ja menetys

Palvelun ulkoistamisen yhteydessä on huomioitava, ettei tiedon fyysinen sijainti ole enää omassa konesalissa, vaan sijaitsee pilvessä palveluntarjoajan keskitetyssä konesalissa. Palveluntarjoajaa valitessa on huomioitava luotettavuus ja toimintamalli tiedon käytettävyyden varmistamiseksi.

Palvelun hallintamalli sovitaan sopimuksessa organisaation ja palveluntarjoajan välillä. Eri palveluntarjoajilla on mahdollisuus toteuttaa vastuumatriisi omalla tavallaan. Tärkeintä on kuitenkin vastuunjaon selkeys sopimuksen molemmilla osapuolilla. (Vetikko 2020b.) Myös Kyberturvallisuuskeskus (2014, 7) toteaa pilvipalvelun toteutuksen riippuvan pilvipalvelua tarjoavan yrityksen ominaisuuksista sekä palvelusopimuksessa määritellystä palvelutasosta.

Tietojen menettämisen riski on aina riippumatta siitä, onko kyseessä organisaation oma konesali vai pilvipalvelu. Pilvipalvelussa on kuitenkin huomioitava tietojen säilyvyys eri tavalla kuin konesalissa. ”*Pilvipalveluiden toiminta varmistetaan useimmiten varmuuskopioinnin tai palvelun kahdentamisen avulla*” toteaa Kyberturvallisuuskeskus (2014, 7). Pilvipalveluissa on mahdollisuus ottaa käyttöön esimerkiksi Data Loss Prevention (DLP) sääntö, jolla arkaluontoisen tiedon menettäminen on mahdollista estää (Vetikko 2020b).

3.4.2 Uhka 2: Käyttäjätilin menettäminen haitalliselle taholle ja käyttäjän tietojen myynti

Pilvipalvelun mahdollistama yhteistyö, etätyöskentely ja useiden uusien työkalujen käyttö vaativat myös palveluun kirjautumisen. Verkossa työskennellessä myös tietojenkalastelu kampanjat ovat kasvaneet valtavasti ja tunnusten vuotaminen on yleisempää, kuin ennen. Pilvipalveluihin pääsynhallinta on mahdollista toteuttaa turvallisemmin esimerkiksi IP-rajauksen avulla, niin että kirjautuminen on mahdollista vain organisaation omasta sisäverkosta. (Vetikko 2020b.)

Palveluntarjoajan valitsemisessa on huomioitava millaista tietoa palvelu kerää käyttäjistä ja mihin tarkoitukseen. Käyttäjien tietojen myyntiä on mahdollista rajoittaa sopimuksen avulla, jolloin organisaatiolla on jokin rajapinta käyttäjien tietojen käsittelyyn ja keräämiseen. (Vetikko 2020b.)

3.4.3 Uhka 3: Lainsäädännön rikkominen

”*Kotimaistenkin pilvipalveluiden osalta on hyvä varmistaa palvelinten sijaintimaa. Jos palvelu on osittain tai kokonaan toteutettu ulkomailla siihen saattaa kohdistua myös ulkomaisen lainsäädännön asettamia vaatimuksia.*” (Kyberturvallisuuskeskus 2014, 17.) Palveluiden siirtyessä pilveen on huomioitava lainsäädäntö, jonka noudattamatta jättämisestä voi tulla yritykselle rahallisia sanktioita. Esimerkiksi EU:n tietosuoja-asetus (GDPR) asettaa vaatimukset tietojen siirrolle EU- / ETA-

alueen ulkopuolelle. Pilvipalvelun käyttöönotossa on suositeltavaa hyödyntää tietosuoja-asiantuntijan osaamista, jotta osataan toteuttaa palvelu lain vaatimin ehdoin. (Vetikko 2020b.) On suositeltavaa käyttää niitä pilvipalveluita, joiden tietoturva sekä palveluntarjoajan turvallisuus on tarkastettu turvallisuusselvityslain puitteissa tehdyssä yritysturvallisuusselvityksessä (Lausuntopalvelu n.d., 12).

3.4.4 Uhka 4: Palvelun toimimattomuus

Pilvipalveluiden käytössä on huomioitava, että mahdolliset häiriöt palvelussa voivat estää tietoihin pääsyn ja mahdollisesti aiheuttaa jopa rahallisia menetyksiä organisaatiolle. Pilvipalvelun tarjoaja pystyy antamaan organisaatiolle Service Level Agreement (SLA) -lupauksen, mikä määrittelee palvelun saatavuuden tason ja mahdolliset korvaukset aiheutuneista kuluista. (Vetikko 2020b.)

Pilvipalvelun toimimattomuudesta on olemassa myös julkisuuteen päätynyt esimerkki. 31.8.2019 Yhdysvaltojen itärannikolla Amazonin datakeskukseen tuli sähkökatkos, sekä varageneraattoreissa oli toimintahäiriö. Seurauksena oli palveluiden toimimattomuus sekä osa asiakkaiden tiedoista hävisi peruuttamattomasti. (Kauppi 2019.) Kauppi (2019) toteaakin artikkelissa: ”*Lopulta hienoinkin pilvipalvelu pohjautuu niihin aivan samoihin tietokoneisiin mitä muutkin käyttävät, ja varmuuskopiointi myös muualle on tarpeen.*”

3.4.5 Uhka 5: Kasvava haittaohjelmien määrä

Vaikka haittaohjelmia on ollut kauan ennen pilvipalveluita, on otettava huomioon haittaohjelmien mahdollinen leviäminen pilvipalveluiden kautta. ”*Pilvipalveluntarjoajan ohjelmistojen päivityskäytännöt on myös hyvä selvittää. Yleensä etenkin suurilla pilvipalveluntarjoajilla ohjelmistopäivitysten käytännöt on hyvin järjestetty ja resursoitu. Asiakkaan tulee kuitenkin itse varmistaa, että päivitysmenettely toimii halutulla tavalla.*” (Kyberturvallisuuskeskus 2014, 12.) On siis huolehdittava etenkin vanhojen järjestelmäversioiden päivittämisestä ja pidettävä huolta tietoliikenteen salauksesta. (Vetikko 2020c.)

Pelkästään Euroopan alueella vuodesta 2020 vuoteen 2021 haittaohjelmien ja hyökkäysten määrä kohdistettuna yrityksiin on noussut peräti 68 %. Tästä terveydenhuollon alalle nousua on 71 %, mikä on toimiala huomioiden huolestuttavaa. (CheckPoint n.d.)

3.4.6 Uhka 6: Reagointiaika poikkeamien ja uhkien käsittelyyn viivästyy

Pilvipalveluiden myötä palveluiden ylläpito on ulkoistettu, joten palveluntarjoajan lokitietojen keruu on avainasemassa poikkeamien ja uhkien käsittelyyn. Lokien analysoinnin helpottamiseksi on olemassa Security Information and Event Management (SIEM) palvelu. SIEM:n yhdistäminen Security Operations Center (SOC) palveluun, saadaan kokonaisvaltainen kuva tapahtumista, jolloin organisaatioon kohdistuneen uhan käsittely on helpompaa ja nopeampaa. Lokitietojen säilyttäminen riittävän pitkän ajan on tarpeellista mahdollista rikostutkintaa tai muuta myöhempää tarvetta varten. (Vetikko 2020c.)

4 Microsoft 365-pilvipalvelun pääsynhallinta ja tietoturva

4.1 Office 365 sekä Microsoft 365

Microsoftin 365-pilvipalvelu on hyvin suosittu yritysten keskuudessa. Palveluihin kuuluvat muun muassa Teams, Sharepoint sekä Office365-palvelut. Esimerkiksi näiden kanavien kautta kulkee paljon tietoa, joten tietoturvan huomiointi on ensisijaisen tärkeää. (Microsoft 2020.)

Tässä kappaleessa käydään läpi Microsoft 365 tietoturvan parantamiseen käytettäviä metodeja ja työkaluja. Kappaleessa ei avata tarkkoja teknisiä toteutuksia vaan käydään läpi perustasolla millaisia ominaisuuksia ja työkaluja on käytössä.

Opinnäytetyössä käytetään kahta saman tyyppistä lyhennettä O365 sekä M365. Lyhenteillä tarkoitetaan Office 365 lisenssin sekä Microsoft 365 lisenssin palveluita, joissa sisällöiltään on jonkin verran eroa. Osa entisistä O365 lisenssityypeistä vaihtoi nimensä Microsoft 365 lisenssiksi. Office 365 termi sisältää perinteisen Officen tuotteet kuten Word, Outlook, Excel, Onedrive, Onenote jne. O365 paketti ei kuitenkaan sisällä kaikkia samoja tietoturvaratkaisuja mitä M365 lisenssi sisältää. (Poisson 2020.) M365 sisältää O365 sisällön lisäksi Windows 10 pro sekä MS Security tuotteet, jolloin pääsee käsiksi laajempaan osaan Microsoftin tarjoamia tietoturvapaketteja. Käytännössä M365 lisenssi on tarkoitettu niille organisaatioille, jotka haluavat kerralla kattavan ratkaisun Officen palveluita päivittäisestä työskentelystä, laajoihin tietoturvatyökaluihin. M365 lisenssin tuomien työkalujen avulla on mahdollista korvata esimerkiksi joitakin ulkoistettuja sähköpostisuodatuksen palveluita ja saada näkyvyys postiliikenteen suojauksesta samaan hallintaympäristöön. (Perus 2020.) Lisenssien hinnoitteluun ei tässä opinnäytetyössä oteta kantaa, vaan käsitellään pelkkinä tuotteina.

Alapuolella olevasta kuviosta (Kuvio 4) näkee, mitä eroa näillä lisensseillä on ja millaisia palveluita lisenssillä saa. Tarkempaa tietoa lisenssien eroista kannattaa selvittää oman organisaation tietoturva-asiantuntijalta tai vastaavasti palveluntarjoajan asiantuntijalta.

	Office 365	Microsoft 365
Office-sovellukset	x	x
Sähköposti ja kalenteri	x	x
Kokoustyökalut	x	x
Laite- ja sovellushallinta	osittain	x
Verkostoituminen	x	x
Tiedostojen hallinta	x	x
Automaatiotyökalut	x	x
Identiteetin- ja pääsynhallinta	osittain	x
Uhilta suojautuminen		x
Tiedon suojaaminen	osittain	osittain
Tietoturvahallinta		x
Vaatimusten mukaisuuden hallinta	x	x

Kuvio 4 Office 365 ja Microsoft 365 eroavaisuudet (Microsoft n.d. a.)

4.2 Todentamisen vaihtoehdot

Microsoftin pilvipalvelun pääsynhallinta voidaan toteuttaa usealla eri metodilla. Microsoft (2021) käyttää seuraavia vaihtoehtoja:

- Windows Hello for Business
- Microsoft Authenticator app
- FIDO2 Security key
- OATH software tokens
- Tekstiviestivarmennus
- Puheluvarmennus
- Salasana

4.2.1 Multi-factor Authentication (MFA)

Kaksivaiheinen todentaminen, eli MFA (Multi-factor Authentication) on metodi, jolla käyttäjä vahvistaa oman kirjautumisensa haluttuun järjestelmään (Hernández 2020). Kuten Jokinen (2021) toteaa salasanat ovat usein hyvin heikkoja ja vahvatkin salasanat voidaan murtaa. Tietojenkalastelu-hyökkäyksiä tapahtuu jatkuvasti. Tämän vuoksi monivaiheista tunnistautumista suositellaan kaikille. (Arstila 2019.) ”*Monivaiheinen tunnistautuminen toisin sanoen tekee käyttäjätilistä turvallisemman ja vähemmän alttiin hyökkäyksille*” toteaa Magic Cloud (2019) artikkelissaan. Usein tietojenkalastelu ja tietomurrot on kohdistettu yrityksen ylimpään johtoon sekä työntekijöihin. Käyttäjätunnuksia kalastellaan useimmiten huijausviesteillä ja -sivuilla. (Kyberturvallisuuskeskus 2018.) Jokinen (2021) painottaa: ”*Monivaiheisella tunnistautumisella vaikeutetaan merkittävästi ulkopuolisten pääsyä yrityksen järjestelmiin, jos käyttäjätunnus ja salasana joutuisivat vääriin käsiin.*” Kaksivaiheisen todentamisen vuoksi menetettyjen tunnusten käyttö on haitalliselle taholle hyvin hankalaa tai jopa mahdotonta. Oikein määriteltynä MFA saadaan toteutettua niin ettei ulkopuolisilla ole teknisistä mahdollista käyttää menetettyjä tunnuksia ollenkaan. (Kyberturvallisuuskeskus 2019, 22.)

Teknisesti MFA toimii siten, että järjestelmään on määritelty kirjautumisen vahvistus jollain halutulla tavalla. Näitä tapoja on mm. tekstiviestivahvistus, puheluvahvistus, mobiiliapplikaation käyttö tai erillinen laite, jossa vaihtuva koodi. (Microsoft 2021b.) Kirjautuminen tulee siis vahvistaa mobiililaitteella (Jokinen 2021). Autentikointimetodit käsitellään myöhemmin tämän työn luvuissa 4.1.3 – 4.1.8.

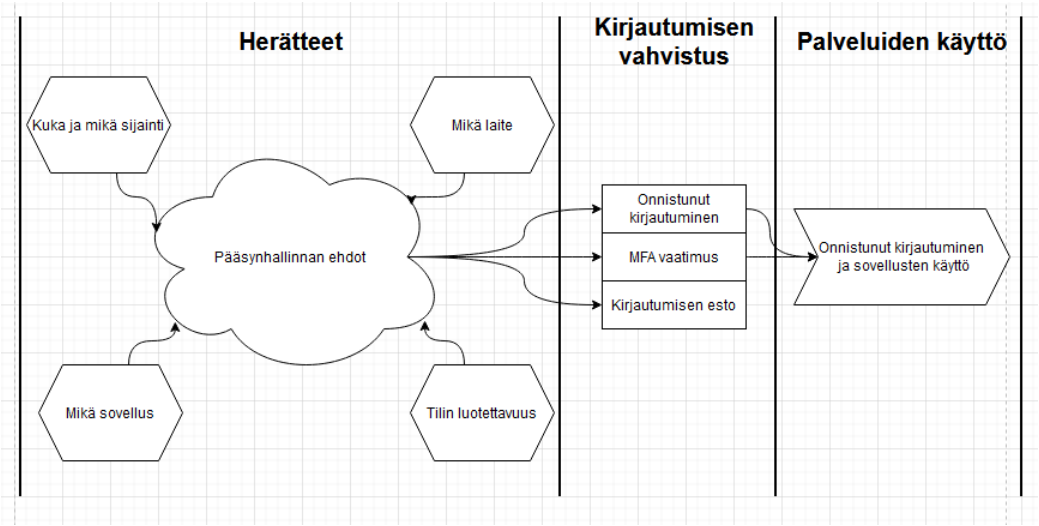
MFA:n tärkeys nousi haastatteluissa esiin pääsynhallinnan osalta. Jokainen haastateltava oli yhtä mieltä siitä, ettei ilman kaksivaiheista tunnistautumista ole turvallista käyttää pilvipalveluita muualta kuin luotetuista sijainneista.

4.2.2 Conditional Access

Conditional Access (CA) on Azure Active Directory (Azure AD) ympäristössä oleva identiteetin ja pääsynhallinta työkalu. CA toimii sääntöjen avulla, joilla luodaan organisaatiolle halutut ehdot sille, miten autentikointi tapahtuu. CA säännöt määritellään organisaation tahtotilan mukaan reagoi-

maan kirjautumisen herätteisiin ja sääntöjen toteutuessa kirjautuminen palveluun onnistuu. Säännöt perustuvat Azure AD tietoihin käyttäjästä ja määritellään roolipohjaiseksi, käyttäjäryhmälle tai kaikille lisensoiduille käyttäjille. Sääntöihin on mahdollista tehdä tarkka määrittely esimerkiksi siihen mistä sijainnista kirjautuminen on mahdollista tai kokonaan estetty, millaisella laitteella kirjautuminen onnistuu ja monella muulla ehdolla. (Microsoft 2022a.)

(Kuvio 5) kuvaa CA:n toimintaperiaatetta. CA-sääntö saa herätteet käyttäjän tiedoista, mistä miltä laitteelta, mihin sovellukseen jne. ja toimii ennalta määrätyn toimintamallin mukaan. Kirjautuminen joko onnistuu ehtojen täyttyessä tai estetään kokonaan. Kaikesta toiminnasta jää lokitieto Azureen.



Kuvio 5 Azure Active Directory Conditionall Access arkkitehtuuri (Microsoft 2022i.)

4.2.3 Windows Hello For Business

Windows Hello on toteutettu biometrisella tunnistautumisella, joko kasvojentunnistus tai sormenjälki. Käyttäjä voi määritellä PIN koodin korvaamaan biometrisen tunnistamisen, jos tunnistuksessa on ongelma. Biometrisen tunnistautumisen tiedot säilytetään kyseisellä laitteella, eikä tietoa siirretä koskaan palvelimille tai muihin ulkoisiin sijainteihin. Microsoft suosittelee Windows Hello:n toissijaisena todentamisena MFA Authenticator sovellusta. (Microsoft 2022d.)

4.2.4 FIDO2 security keys

FIDO (Fast Identity Online) on fyysinen autentikointi metodi, jonka avulla käyttäjä pystyy kirjautumaan palveluun ilman salasanaa. Käytännössä FIDO2 avulla kirjautuminen tapahtuu seuraavanlaisesti:

Käyttäjä kytkee FIDO2 laitteen työasemaansa, jonka työasema tunnistaa. Windows lähettää varmennuspyynnön käyttäjän mobiililaitteeseen (Microsoft authenticator), jonka käyttäjä hyväksyy. Windows vahvistaa kirjatumistiedot ja päästää käyttäjän sisään. (Microsoft 2022e.)

4.2.5 OATH Software tokens

OATH hardware tokens todentamisessa käytetään jatkuvasti päivittyvää koodiavainta. Varmennuksessa käytettävä koodi vaihtuu 30-60 sekunnin käyttäjän valitsemassa sovelluksessa (esimerkiksi Microsoft Authenticator). (Microsoft 2022f.)

4.2.6 Tekstiviestivarmennus

Tekstiviestivarmennuksessa käyttäjä kirjautuu palveluun käyttäjätunnus-salasana paria käyttäen, jonka jälkeen Microsoft vahvistaa kirjautumisen lähettämällä kuusinumeroisen koodin tekstiviestillä ennalta määritettyyn puhelinnumeroon. Käyttäjä syöttää numerokoodin kirjautumisikkunaan, jonka jälkeen autentikointi on suoritettu. (Microsoft 2022g.)

4.2.7 Puheluvarmennus

Puheluvarmennuksessa käyttäjä kirjautuu palveluun käyttäjätunnus-salasana paria käyttäen, jonka jälkeen hänelle tulee saapuva automaattinen puhelu ennalta määritettyyn puhelinnumeroon, jossa pyydetään painamaan tiettyä näppäintä. Tämän jälkeen autentikointi on suoritettu onnistuneesti ja käyttäjä pääsee kirjautumaan palveluun. (Microsoft 2022h.)

4.2.8 Salasana

Käyttäjätunnus-salasana pari on näistä kirjautumismetodeista heikoin ja helpointen murrettavissa. Perinteistä ”*single factor authentication*” metodia ei suosita käytettäväksi ainoana autentikointi tapana missään ympäristössä. (Microsoft 2021b.)

4.3 Tiedon säilytys pilvipalveluissa

4.3.1 Tiedon sijainti

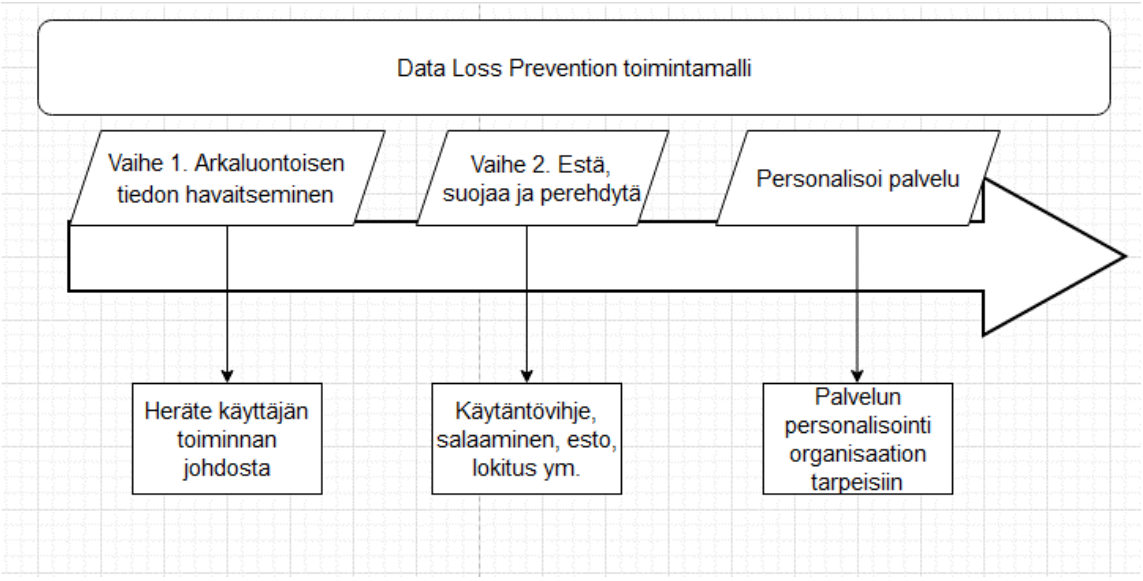
Microsoftin pilvipalveluissa tieto säilytetään palveluntarjoajan datakeskuksissa, jotka sijaitsevat EU:n alueella. Yrityksen on mahdollista pyytää tiedon tarkempi sijainti näin halutessaan. Tiedon fyysinen sijainti voi aiheuttaa riskejä esimerkiksi alueen lainsäädännön muodossa. Sijaintia koskevien riskien sekä vaatimusten arvioinnissa on kannattavaa huomioida EU:n asetus tietojen siirrosta. (Traficom 2020b, 13.)

4.3.2 Menetyksen esto (DLP)

Data Loss Prevention työkalu on luotu estämään arkaluontoisen tiedon päätyminen sellaisille tahoille, joille tiedon ei haluta päätyvän. Myös (Vetikko 2020b.) toteaa artikkelissaan: ”*Datan päätymisen oikeudettomasti ulkopuolisen käsiin yritys voi estää tietojen salaamisella, tietojen automatisoidulla poistamisella tallennusmedioilta ja tietovuotojen havaitsemiseen käytetyillä ohjelmistoilla (Data Loss Prevention, DLP), joita myös pilvipalveluihin on tarjolla.*” Organisaation on itse mahdollista määritellä miten DLP säännöt reagoivat arkaluontoiseen tietoon. Tiedon siirto voidaan estää, voidaan kytkeä hälytykset päälle tai voidaan antaa käyttäjille käytäntövihje ennen lähetystä. (Brook 2020.)

DLP säännön määrittely vaatii usean eri vaiheen. Täytyy määritellä, missä sijainnissa olevaa tietoa halutaan suojata, ketä käyttäjäryhmiä sääntö koskee, minkälaiseen tietoon sääntö tarttuu ja millä tarkkuudella. Sääntö voidaan konfiguroida havaitsemaan esimerkiksi henkilötunnuksia, jolloin kaikista henkilötunnuksista tai henkilötunnusta muistuttavista merkkijonoista aktivoituu säännölle määrätty prosessi. (Brook 2020.)

Alla olevassa (Kuvio 6) on kuvattu DLP:n toimintaperiaate. Sääntö havaitsee arkaluontoista tietoa sisältävän kohteen, suorittaa sääntöön määritellyn toimenpiteen ja tarvittaessa antaa käyttäjälle käytäntövihjeen. DLP personoidaan organisaation käytönmukaiseksi käyttäjäkokemuksen parantamiseksi ja turhien hälytysten minimoimiseksi.



Kuvio 6 DLP Delivery Roadmap (Microsoft 2015)

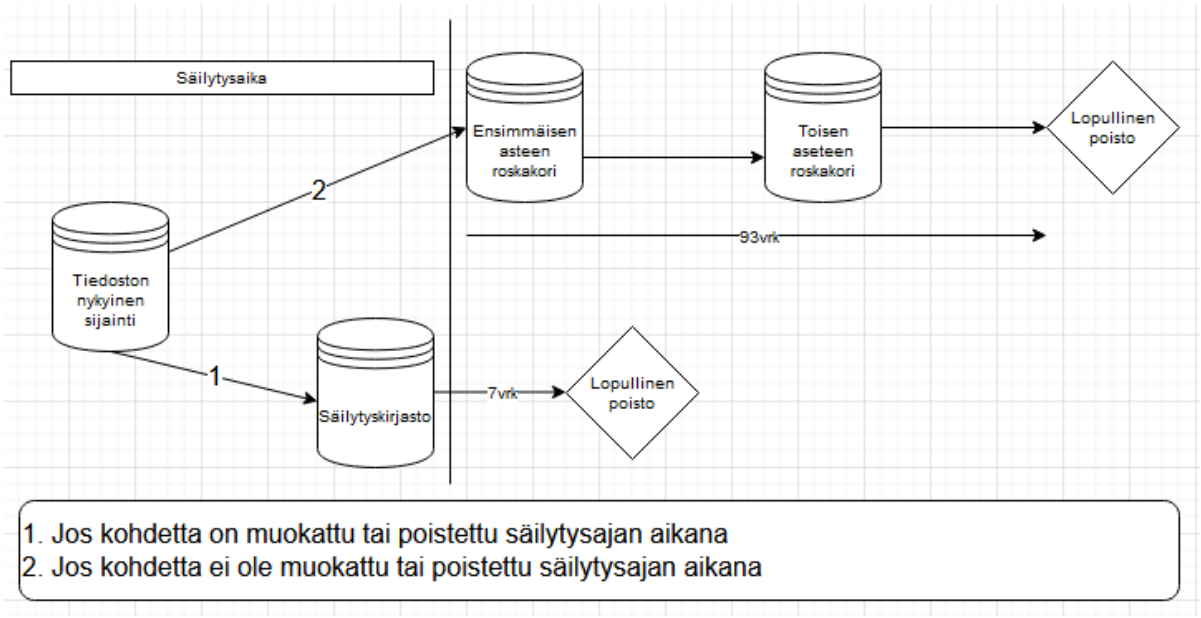
4.3.3 Säilytyskäytännöt (Retention policies)

Säilytyskäytäntöjen avulla organisaatio pystyy varmistamaan, ettei tahattomasti tai tarkoituksenmukaisesti poistettu tieto poistu kokonaan ennen kuin tietty säilytysaika on täyttynyt. Säilytyskäytännön määrittelyssä organisaation tietohallinnon on päätettävä mitä palvelua käytäntö koskee, miten pitkäksi aikaa säilytys luodaan ja mitä tapahtuu, kun säilytysaika on täyttynyt. (Microsoft 2022b.)

Säilytyskäytännön piirissä oleva tieto säilyy siinä sijainnissa, missä se on alun perin ollut, käyttäjä ei vain kykene enää näkemään tuota tietoa tai palauttamaan sitä itse. Palautus tapahtuu aina ylläpitäjän toimesta. (Microsoft 2022b.)

Dokumenttien säilytyskäytäntö on mahdollista määritellä alkamaan luontihetkestä tai viimeisestä muokkauksesta. Jos säilytyskäytäntö määritellään alkamaan luontihetkestä, säilytettään dokumentista 500 viimeisintä versiota, joiden säilytysaika loppuu samana hetkenä. Jos säilytyskäytäntö on määritelty alkamaan muokkaushetkestä, säilytetään dokumentista jokaisesta muokatusta versiosta oma kopio, joiden säilytysaika loppuu, kun muokkauksesta on kulunut käytäntöön määritetty aika. (Microsoft 2022c.)

Seuraavassa (Kuvio 7) on kuvattu, miten säilytyskäytännöstä poisto toimii käytännössä. Organisaatio määrittelee säilytysajan, sekä toimintamallin, mitä tapahtuu säilytysajan täytyttyä. Säilytysajassa on huomioitava lain tuomat rajoitteet. Säilytysajan täytyttyä lopullisen poiston jälkeen, tietojen palautus ei ole enää mahdollista.



Kuvio 7 Säilytyskäytäntö (RecordPoint 2019)

Kuten haastatteluissakin, että aiemmin mainittu tiedon säilyvyys on tärkeä osa pilvipalveluiden turvallisuutta, on DLP säännöillä määriteltävä säilytyskäytäntö siihen hyvä ratkaisu.

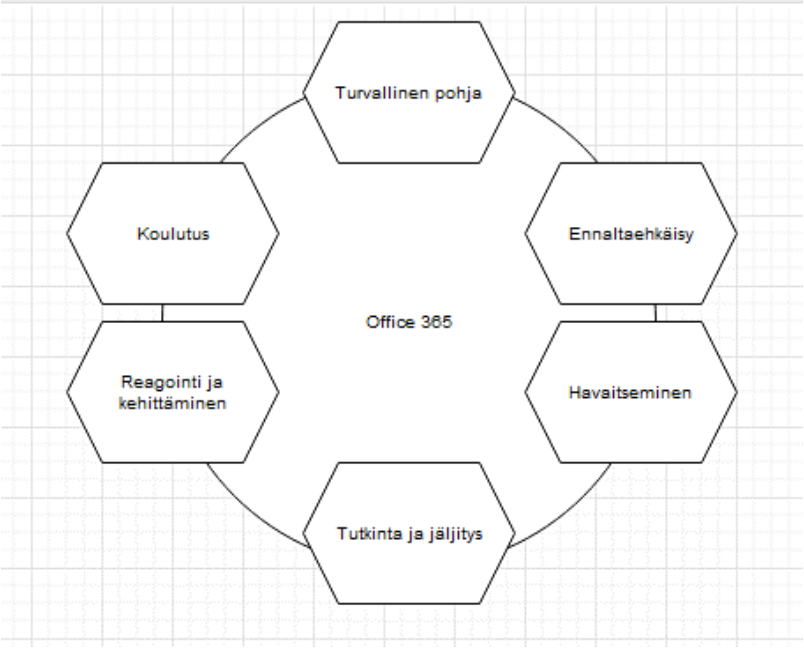
4.4 Microsoftin pilvipalvelun tietoturvatyökalut

Tässä kappaleessa käsitellään pilvisovelluksille tarkoitettua Microsoftin Defender for Office (MDO), työasemien pilvipohjaista suojausta Defender for Endpoint (MDE) ja pilven dataliikenteen ja organisaation identiteetin suojaustyökalua Defender for Identity (MDI) pintapuolisesti. Näiden pilvityökalujen avulla voidaan suojata pilvipalveluiden lisäksi fyysisiä kohteita, kuten työasemia ja palvelimia. Identiteetin suojauksella tarkoitetaan Domain Controllerien (DC) seurantaa poikkeavuuksien ja hyökkäysten varalta. (Microsoft 2022j.) Fyysisten laitteiden, kuten työasemien, palvelimien tai muiden verkkolaitteiden suojaukseen ei oteta kantaa tässä opinnäytetyössä, vaikka kyseisillä tuotteilla näiden suojaus onkin mahdollista.

4.4.1 Defender for Office (MDO)

MDO työkalun avulla pystytään tunnistamaan, ennaltaehkäisemään, tutkimaan ja korjaamaan O365 palveluihin kohdistuvia uhkia, haittaohjelmia, kalasteluja ja muita mahdollisia ongelmia. Kyseisiä palveluita on esimerkiksi Word, Excel, Powerpoint, Outlook, OneDrive, Teams ja Sharepoint. MDO toimii pilvessä suojaten käyttäjätilit, toisin kuin perinteisemmän haittaohjelmasuojaukset, eikä ole riippuvainen työasemalle asennetusta sovelluksesta. (Microsoft 2022j.)

Alla olevassa kuviossa (Kuvio 8) näkyy MDO:n toimintamalli. Office palveluiden ympärille on rakennettu teknisten työkalujen lisäksi perehdyttämiseen liittyvät työkalut. MDO:n keskeisenä toiminnallisuutena on kokonaisvaltainen suojaus. Toiminta perustuu mm. sähköpostin suodatukseen, ennen kuin sähköposti päätyy työasemalle, pilvitallennustiloihin tallennettujen tiedostojen analysointiin sekä tietoturvauhkien tutkintaan ja jäljittämiseen koko ympäristössä (Microsoft 2022j.)



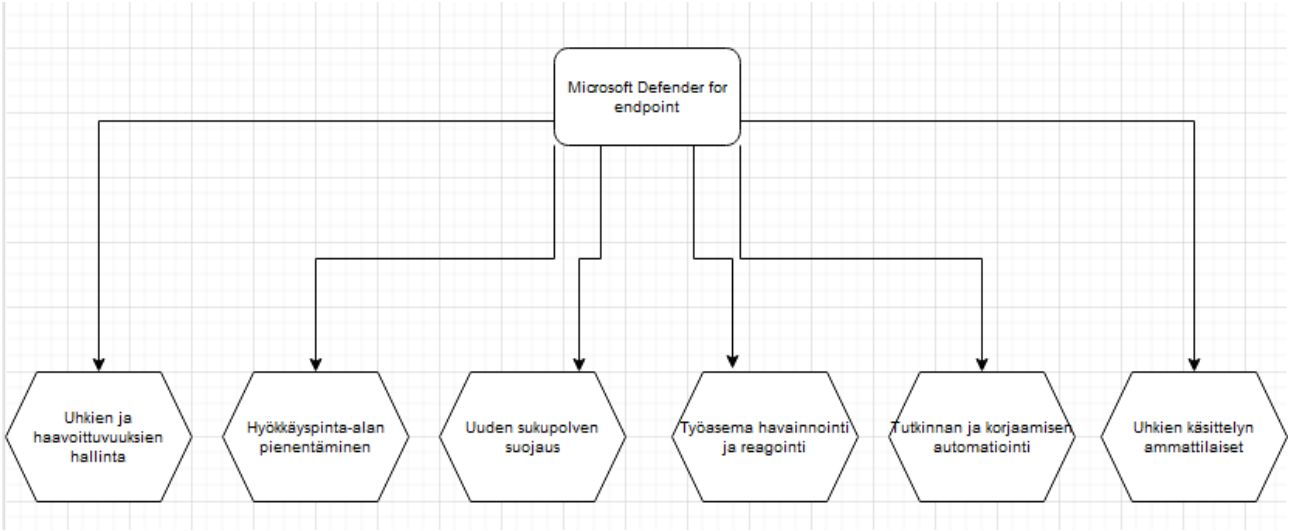
Kuvio 8 Defender for Office (Microsoft n.d. b)

Haastatteluissakin ilmeni suuren osan pilvipalveluihin kohdistuvista kalasteluista, sekä haitallisesta sisällöstä kohdistuu sähköpostiliikenteeseen sekä jaettuihin tiedostoihin. Sen vuoksi MDO:n tuoma laaja suojaus ja jäljitys on tehokas työkalu näiden torjumiseen koko organisaatiossa.

4.4.2 Defender for Endpoint (MDE)

MDE on työaseman suojaus, joka toimii perinteisen Microsoft Defender (työasemasuojaus) kanssa. Perinteisen suojauksen lisäksi MDE on liitettynä pilveen, jolloin reaaliaikainen suojaus, analysointi ja tutkinta on mahdollista. Teknisesti MDE eroaa työaseman Microsoft Defender virustorjunnasta siten, että työasemalle asennetaan käyttäytymistä valvova sensori, mikä kerää tietoa käyttöjärjestelmästä ja lähettää tiedon pilveen analysoitavaksi. (Microsoft 2022j.)

Alla olevassa kuvoissa (Kuvio 10) on esitetty MDE:n toimintamalli. Kyseessä on työasemasuojaus, jonka uhkien käsittely, tutkinta ja ennaltaehkäisy toimii pilvihallinnan kautta. Kuviosta 10 näkee myös minkä tyyppisiä työkaluja MDE sisältää. Käytännössä työasemalle asennettu sensori heräteistä saatuja tietoja pilveen analysoitavaksi, jossa havaintoja käsitellään viimeisimpien haavoittuvuus ja uhkatietojen perusteella. MDE on XDR (Extended Detection and Response) tyyppinen suojaus, mikä tarkoittaa laajennettua suojausta työasemalta pilveen. (Microsoft 2022k.)



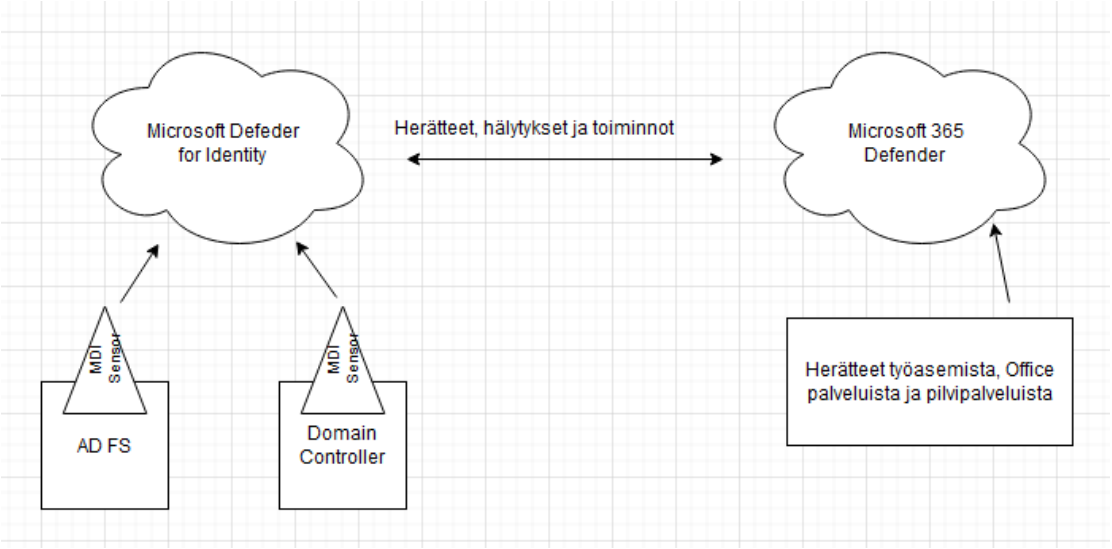
Kuvio 9 Defender for Endpoint (Microsoft n.d. c)

MDE nousi haastatteluissa esille kokonaisuuden hallinnassa, koska osa pilvipalveluihin kohdistuvista hyökkäyksistä ja uhista suunnataan erilaisten saastuneiden tiedostojen sekä ohjelmistojen kautta. MDE:n avulla pystytään suodattamaan entistä kattavammin päätelaitteille kohdistuvia uhkia.

4.4.3 Defender for Identity (MDI)

MDI on ATP (Advanced Threat Protection) tyyppinen pilvipohjainen suojaus, jonka avulla organisaatiolla on mahdollisuus havaita, tunnistaa ja tutkia kehittyneitä hyökkäyksiä, joihin perinteiset virustorjunnat eivät reagoi ajoissa. MDI mahdollistaa identiteettivarkauksien ja haitallisten käyttäjien automaattisen havaitsemisen toimintatapojen muuttuessa, sekä tunnistaa normaalista poikkeavat tapahtumat ja toimintamallit. Identiteetillä tarkoitetaan organisaation tilien ja ympäristön identiteettiä, minkä hyväksikäyttö halutaan estää. MDI luo hyökkäyksestä aikajanan, minkä avulla on helppo havaita tapahtumat, kohteet ja hyökkäyksen toimintamallin. (Microsoft 2021a.)

(Kuvio 11) kuvaa MDI:n toimintaa. MDI kerää tietoa eri herätteistä ja valvoo organisaatiossa identiteettien luotettavuutta sekä toimintoja. MDI saa tietonsa työasemille ja palvelimille asennetuista sensoreista, sekä AD:lta ja DC:ltä saamistaan herätteistä, kuten poikkeavasta käyttäjätilin käytöksestä kirjautumisyrityksissä sekä tilin ryhmien muutoksista.



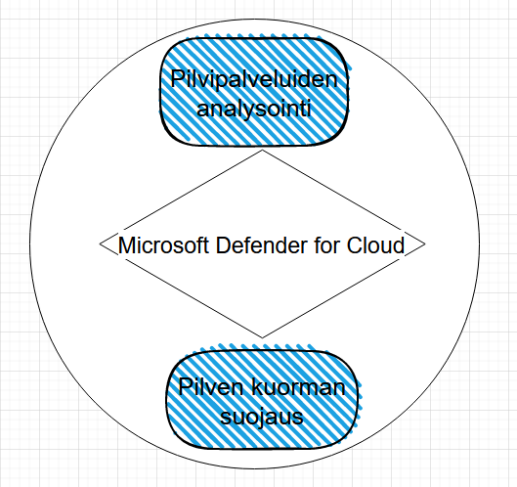
Kuvio 10 Defender for identity arkkitehtuuri (Microsoft 2021a)

MDI:n tärkeys nousi tutkimuksessa esille haastatteluissa, sekä selvitystyössä. Näissä mainittiin pääsynhallinnan tärkeys, sekä tunnusten kalasteluyritykset. MDI:n avulla pystytään valvomaan poikkeavaa käytöstä, jolloin varastettujen tunnusten hyväksikäyttö saadaan jäljitettyä mahdollisimman nopeasti.

4.4.4 Defender for Cloud (MDC)

Defender For Cloud (MDC) on luotu pilviympäristöjen tietoturvan hallintaan ja suojaukseen. MDC:n tehtävänä on havaita heikkoja kohtia organisaation pilvipalveluiden ja hybridiympäristöjen konfiguraatioissa ja auttaa korjaamaan ongelmakohdat yhden hallintapaneelin avulla. (Azure n.d.)

Alla olevassa (Kuvio 12) on esitetty MDC:n perusrakenne. MDC:n tehtävänä on analysoida pilvipalveluiden toimintaa ja poikkeavuuksia sekä seurata pilvipalveluiden kuormaa ja suojata sen toimintaa. Automatisoidun seurannan tuottama havainto aiheuttaa herätteen ylläpitäjälle, sekä tarvittaessa automaattisesti aloittaa suojaustoimenpiteet.



Kuvio 11 Defender for Cloud toiminta (Diogenes 2021)

5 Tutkimustulokset

5.1 Julkishallinnollisen organisaation tietoturva pilvipalveluissa

Tässä luvussa kerron haastattelujeni pohjalta, miten pilvipalveluiden tietoturva pitäisi huomioida käyttöönotossa ja päivittäisessä käytössä organisaatiossa. Jokaisen haastateltavan organisaatiossa oli käytössä Microsoftin pilvipalveluita. Haastateltavan 1 ja 2 organisaatiossa on käytössä O365-palvelut sekä M365 Security-palveluita. Haastateltavan 3 organisaatiossa on käytössä O365-palvelut. Haastateltava 3 kertoi, että myös heidän organisaatioonsa oli harkinnassa ottaa käyttöön M365 Security-palveluita.

Jokainen haastateltava koki tietoturvan huomioimisen ensiarvoisen tärkeäksi pilvipalveluiden käytössä. Haastateltavat kokivat aiheen ajankohtaiseksi ja haastateltava 2 sanoikin, että hänen mielestään tietoturvallisuutta pilvipalveluissa pitäisi nostaa yhä enemmän keskusteluun yleisesti mediassakin. Haastatteluista nousi selkeästi esille neljä teemaa, joiden alle pilvipalveluiden tietoturvallinen käyttö voidaan jäsentää. Näitä ovat käyttöönotto, pääsynhallinta, yleinen tietoturva sekä uhkatilanteet.

Pilvipalvelut ovat tärkeitä organisaatioille. Ne mahdollistavat monipuolisen yhteistyön tekemisen sekä sijainnista riippumattoman tiedonhallinnan. Pilvipalveluissa, kuten muissakin it-palveluissa, tietoturvan huomiointi on äärimmäisen tärkeää. Tekninen toteutus on tärkeä toteuttaa organisaation vaatimusten mukaisesti, mutta missään tilanteessa ei saa unohtaa käyttäjien perehdyttämisen tärkeyttä tietoturvallisen ympäristön toiminnassa. Tietoturvatyökalujen avulla mahdollistetaan ennaltaehkäisy, uhkien seuranta ja tutkinta. Täytyy kuitenkin tiedostaa sosiaalisen hakkeroinnin riskit yritysmaailmassa, kuten yksityiselämässäkin. Haastatteluissakin nousee useasti esille, miten pääsynhallinnan kontrollien tärkeys yhdessä käyttäjien perehdytyksen kanssa vahvistavat tietoturvaa organisaatiossa.

Haastattelujen, sekä tutkimuksen pohjalta kokosin (Liite 1) muistilistan, mitä voidaan hyödyntää pilvipalveluiden käyttöönotossa. Listasta nousee esiin perusasiat, joita seuraamalla saadaan pohja kuntoon.

5.1.1 Käyttöönotto

Jokaisella haastateltavalla nousi ensimmäisenä esille käyttöönoton suunnittelun ja toteutuksen tärkeys. Haastateltavat 1 ja 2 olivat samaa mieltä siitä, ettei käyttöönottoa tulisi toteuttaa ilman kunnollista ymmärtämistä ympäristöstä, käyttötapauksista, tarpeesta ja vaatimuksista. Haastateltava 3 puolestaan nosti esille käyttöönotossa tärkeäksi huomioida toiminnan jatkuvuus ja tiedon saatavuuden varmistaminen käyttöönottoprojektin aikana. Haastateltava 3 myös painotti asiantuntijoiden ammattitaidon ja palveluiden hallinnan olevan tärkeitä sujuvan käyttöönoton onnistumiseksi haastavassakin ympäristössä.

Haastateltava 3 kertoi O365 pilvipalveluiden käyttöönoton haasteeksi sen, ettei heidän päivittäinen toimintansa keskeydy missään vaiheessa, vaan käyttäjiä on aktiivisena vuoden jokaisena tuntina. Käyttöönoton oli toteuduttava ilman käyttökatkoksia ja tämän vuoksi toteutettiin useammassa eri osassa ja pienemmille käyttäjäryhmille kerrallaan. Käyttöönotto oli sujunut ilman teknisiä ongelmia ja lisännyt organisaatiossa monipuolisuutta etätyöskentelyyn.

5.1.2 Pääsynhallinta

Pääsynhallinnan osalta kaikki haastateltavat olivat yhtä mieltä siitä, ettei ilman modernia autentikointia sekä Conditional Access säännöillä luotuja rajauksia ole syytä lähteä käyttämään pilvipalveluita organisaatiossaan. Haastateltava 2 nosti esille, miten jatkuvasti muuttuvan maailman tilanteeseen voidaan reagoida pääsynhallintasääntöjä muokkaamalla ja näin saadaan suojattua organisaation käyttäjätilejä entistä paremmin. Haastateltava 1 nosti huomioksi, miten monella organisaatiolla ei ole huomioitu vieraskäyttäjien pääsynhallintaa ollenkaan ja tahtotila tuntuu olevan siihen suuntaan, ettei ymmärretä myös vierastilien hyväksikäytön mahdollisuuksia väärissä käsissä.

Haastateltava 2 nosti esille mitä MFA:n käyttöönotossa kannattaa huomioida: ”*MFA ratkaisun pohja on hyvä rakentaa, niin että jokaiselle käyttäjälle tulee kaksivaiheinen todentaminen käyttöön ja vain poikkeustilanteet toteutetaan eri tavalla. Tämä siksi, ettei esimerkiksi uusien tunnusten luonnissa MFA pakotus ole tunnustenluonnin prosessin varassa, vaan automaattisesti koskee kaikkia käyttäjätunnuksia ympäristössä. Jos ympäristöstä löytyy esimerkiksi hallintatunnuksia, joilla MFA:ta ei voida käyttää, voidaan näitä varten tehdä poikkeukset sääntöön.*”

5.1.3 Tietoturva

Tietoturvakontrollien osalta kaikki Haastateltavat olivat samaa mieltä tiedon säilytyksen, saatavuuden ja tiedon menetyksen eston osalta. Haastateltavat 1 ja 2 molemmat nostivat esiin tärkeyden ymmärtää tietoturvakontrollien kokonaisuus ja kattavuus sujuvassa käytössä mahdollisten uhkatilanteiden selvittämisessä. Molemmat Haastateltavat 1 ja 2 olivat työssään tulleet tilanteeseen, jossa mahdollisen tietovuodon selvityksessä on käytetty apuna säilytyskäytäntöä.

Haastateltavat 1 ja 2 mainitsivat organisaatioissaan olevan käytössä Microsoftin tietoturvapalveluista myös laajemmat suojaustyökalut Defender for Indentity (MDI), Defender for Office (MDO), Defender for Cloud (MDC) ja Defender for Endpoint (MDE). Molemmat mainitsivat näiden työkalujen kasvattavan tietoturvauhkiin reagoimista, jäljitystä, käsittelyä ja ennaltaehkäisyä. Haastateltava 3 kertoi että samat palvelut ovat parhaillaan suunnitelmissa myös hänen organisaatioonsa, muttei päätöstä ole vielä tehty.

Jokainen haastateltava oli samaa mieltä, siitä miten ensiarvoisen tärkeää on huolehtia pilvipalveluiden tietoturvasta ja käyttäjien perehdyttämisestä turvallisen käytön takaamiseksi.

5.1.4 Uhkatilanteet

Haastateltavat eivät avanneet yksityiskohtaisesti omien organisaatioidensa kokemia uhkia, mutta pystyivät kertomaan pintapuolisesti minkä tyyppisiä tilanteita on havaittu viimevuosien aikana. Uhkien käsittely toteutuu organisaation omalla toimintamallilla. Tässä kappaleessa ei oteta kantaa uhkan käsittelyyn organisaation sisällä, vaan tarkoituksena on tuoda esille, millaisia uhkia haastateltavien organisaatioissa on ilmentynyt.

Haastateltava 3 kertoi organisaation yleisimmän ja näkyvimmän uhkatilanteen olevan tietojenkalastelua useimmiten sähköpostin välityksellä. On ollut tunnettua toimitusjohtaja huijausta, jossa toimitusjohtajan nimissä on pyydetty tietoa tai rahansiirtoa. Myös aidon näköisiä salasanan vaihto lomakkeita sekä virheilmoituksia, joiden tavoitteena on saada käyttäjä syöttämään käyttäjätunnuksensa ja salasanansa hyökkääjien luomalle valesivustolle. Vastaavia tilanteita myös muiden haastateltavien organisaatioissa oli ollut viime vuosien aikana.

Haastateltava 1 totesi myös haavoittuvuuksien hyväksikäytön olevan yleistynyt viime aikoina ja nostikin esiin järjestelmien käyttöjärjestelmien pitämisen ajan tasalla sekä verkkoympäristöjen toteuttamisen siten, ettei palvelimille olisi helppoa pääsyä julkiverkosta.

Aiempien havaintojen lisäksi haastateltava 2 mainitsi uhkatilanteiksi vanhojen tietojen sekä tiedon puutteellisuuden tuomat haasteet ylläpidossa. Puutteellisten tietojen vuoksi on yksittäisen asiantuntijan lähes mahdotonta tietää sovituista toimintamalleista, minkä tyyppistä tietoa järjestelmässä käsitellään tai minkälainen pääsynhallintaprosessi palveluun on. Tällöin on mahdollista, että järjestelmään mahdollistuu pääsy sinne kuulumattomalle henkilölle tai taholle, jolloin tietovuodon toteutuminen on mahdollinen.

6 Yhteenveto

Opinnäytetyön tutkimuskysymyksenä oli ”*Mitä on otettava huomioon turvallisessa O365-pilvipalveluiden käyttöönotossa ja käytössä julkishallinnollisen toimijan ympäristössä?*” sekä alakysymyksinä: ”*Miten pääsynhallinnan avulla voidaan turvallisesti käyttää O365-palveluita?*” ja ”*Mitä uhkia pilvipalvelun käyttö tuo mukanaan?*”

Haastateltavat nostivat esiin muutaman eri uhkatilateen heidän organisaatioistaan, joista osan nostaa esiin myös (Vetikko 2020b) artikkelissaan mainiten: ”*Pilvipalveluiden määrän lisääntyessä myös eri palveluihin käytetyt kirjautumistiedot lisääntyvät jokaisen palvelun vaatiessa oman käyttäjätunnus-salasana-yhdistelmän. Tämä kuormittaa palveluiden käyttäjiä ja ylläpitäjiä useiden eri käyttäjätunnus-salasana-yhdistelmien muistamisessa ja ylläpitämisessä.*”

Olen koonnut opinnäytetyöni, teorian ja haastatteluiden pohjalta muistilistan organisaatioille, jossa käy ilmi, mitä kaikkea tulisi huomioida pilvipalveluiden käyttöönotossa sekä turvallisessa käytössä. Tämä muistilista ei sisällä kaikkia pilvipalvelun tietoturvakontrolleja ja työkaluja, vaan antaa kuvan siitä mitä on syytä huomioida käyttöönoton ja käytön yhteydessä. Käyttöönotossa on silti syytä huomioida oman organisaationsa tarpeet ja vaatimukset. Tämän vuoksi jokainen organisaatio määrittelee itse omat kontrollinsa, mutta on tärkeää huomioida lain vaatimat rajoitteet pilvipalveluille.

Huomioitavia kohtia pilvipalveluiden käytössä:

1. Tiedon säilytysaika
2. Tiedon menettämisen esto
3. Pilvipalveluiden vieraskäyttö
4. Pilvipalveluiden jakamiskäytännöt
5. Pääsynhallinta pilvipalveluihin
6. Tiedon maantieteellinen sijainti

Koska pilvipalveluissa tietoa ei ole kannattavaa säilyttää ikuisesti, on suositeltavaa määritellä, kuinka kauan pilvipalveluissa halutaan säilyttää tietoa. Yritys voi määritellä kauanko tieto halutaan säilyttää pilvipalveluissa. Säilytyskäytännöissä tulee huomioida mahdolliset lakien ja asetusten muodostamat vaatimukset ja rajaukset, sekä tietyntyyppiselle tiedolle lain määräämä säilytysaika.

Kun määritelty säilytysaika on päättynyt ja tiedon lopullinen poisto on suoritettu, ei tietoa enää pystytä palauttamaan.

Tiedon menettämisen eston avulla voidaan määritellä, minkälaista tietoa ei haluta vahingossa tai tahallisesti lähetettävän organisaation sisällä tai ulkopuolelle. Tiedon menettämisen eston avulla pystytään perehdyttämään käyttäjiä, estämään tietovuotoa sekä valvomaan arkaluontoisen tiedon käsittelyä organisaatiossa. Tämän ominaisuuden avulla voidaan myös määritellä automaattinen toimintamalli arkaluontoista tietoa käsitellessä.

Organisaatioilla on usein jopa tuhansia vierastilejä, joilla osalla pääsy voi olla hyvinkin arkaluontoiseen dataan. Näin ollen on tärkeää määritellä, miten tiedonjakaminen on mahdollista pilvipalveluissa. Yritys voi määritellä mihin tietoihin ja ympäristöihin vieraskäyttäjillä on mahdollisuus päästä sekä miten vieraskäyttäjien on mahdollista käyttää tietoja. Myös vieraskäyttäjien pääsynhallinta on syytä toteuttaa riittävällä tasolla tiedon suojaamiseksi.

Pilvipalveluiden jakamiskäytäntöjen avulla määritellään, miten tietoja on mahdollista jakaa pilvipalveluista ja millaisin ehdoin. Pilvipalveluista jakamisesta jää myös lokiin merkintä, jolloin mahdollisen tietovuodon selvittämisessä on mahdollisuus hyödyntää tätä tietoa. Jakamiskäytäntöjen tärkeys on tietovuotojen ennaltaehkäisyssä. Jos jakamista ei rajoiteta tai jakamisen ehtoja määritellä, syntyy riski, että materiaalia on jaettu organisaation ulkopuolelle tai muulle taholle, minne tiedon ei haluta päätyvän.

Pääsynhallinta on tärkeä toteuttaa organisaatiolle riittävällä tasolla, jotta mahdollisilta kalasteluyrityksiltä tai tunnusten menettämiseltä vältyttäisiin. Pääsynhallintasääntöjen avulla on mahdollista suojata käyttäjätilit aiempaa paremmin. Pääsynhallinnalla tarkoitetaan tässä yhteydessä käyttäjätilin kirjautumisvaatimuksia organisaation järjestelmään, eli mistä sijainnista kirjautuminen on mahdollista ilman kaksivaiheista todennusta, millä metodilla kaksivaiheinen todennus voidaan vahvistaa vai onko sijainteja mistä kirjautuminen on kokonaan estetty.

On tiedettävä jo käyttöönottoa suunnitellessa, minkälaista tietoa haluaa pilvipalveluissa käsiteltävän ja säilytettävän. Näissä on myös hyvä huomioida tiedon omistajuus, tiedon sijainti ja lain määräämät rajoitteet ja ohjeistukset. Näiden määrittelyssä on suositeltavaa hyödyntää tietosuoja-asiantuntijan ammattitaitoa ja perehtyä arkaluontoisen tiedon käsittelyä koskevaan lainsäädäntöön.

Yli kolmen vuoden työkokemus tietoturva-asiantuntijana isolla julkishallinnollisella toimijalla ja keskittyminen pääosin SOC toimintaan, pilvipalveluiden käyttöönottoon ja tietoturvallisuuteen on antanut seuraavanlaiset näkemykset yhdessä tämän opinnäytetyön kanssa.

Nykytilanne suomalaisissa organisaatoissa on hyvin hajanainen ja tieto pilvipalveluiden tietoturvasta on vajanaista. Osalla organisaatioista pilvipalveluiden tietoturvasta on huolehdittu riittävällä tasolla ja tilannekuvan muuttuessa myös kehitetään tietoturvaa. Joillain organisaatioilla ei ole käytännössä ollenkaan huomioitu tietoturvaa, pääsynhallintaa, tiedon menettämistä tai muita pilvipalveluissa olevia riskejä. Tällaiset organisaatiot ovat jämähtäneet aikaan, jolloin työasemalla oleva virustorjunta ja verkkoa suojaava palomuuri ovat riittävät suojaamaan yrityksen kaikkea tietoteknistä toimintaa. Maailma kuitenkin muuttuu jatkuvasti enemmän pilven suuntaan, jolloin tietoturva on huomioitava myös muutenkin, kun pelkkien haittaohjelmien tai DDOS hyökkäysten osalta.

Tietoturvan taso ja tietoturvaan käytettävät kulut kasvavat usein samaan tahtiin, mikä saattaa aiheuttaa joissain organisaatioissa haluttomuutta tietoturvan kehittämiseen kulujen nousun vuoksi. On kuitenkin tärkeää nykypäivän verkkokulttuurissa haavoittuvuuksien, tietomurtojen, haittaohjelmien ym. ongelmien ennaltaehkäiseminen tulee halvemmaksi kuin toiminnan eheyttäminen tilanteen eskaloituessa.

Organisaatiot, joissa käsitellään paljon henkilötietoa, ovat kauttaaltaan kiinnostuneempia tietoturvasta, tietosuojasta ja nykytilanteesta. Tällaisten toimijoiden tietohallinnot ovatkin halukkaimpia kehittämään tietoturvaa pysyäkseen askeleen edellä perinteisiä uhkia. Monella organisaatiolla heräsi mielenkiinto omien tietojen sijainnista ja käsittelystä Vastaamon tietomurron noustessa uutisotsikoihin. Vastaamon tietomurron jälkeen pilvipalveluiden tietoturvan kehittäminen ja tietoturvatyökaluihin panostaminen muuttui selkeästi. Vaikka pilvipalvelussa oleva tieto ei sijaitse asiakkaan

omissa tiloissa, tai välttämättä koko Suomessa, luo tietynlaisen ehkä jopa vähän vääristynee kuvan riittävästä tietoturvasta sopimuksiin nojaten.

Perehtyessä opinnäytetyön aiheeseen, havaitsin että lähes kaikki pilvipalveluiden tietoturvaan liittyvät artikkelit, kirjallisuus, verkkojulkaisut jne. keskittyivät tekniseen toteutukseen, eikä lainkaan käyttäjien perehdyttämiseen pilvipalveluissa piilevien uhkien osalta. Varsinaisia selkeitä ohjenuoria tai parhaita toimintamalleja pilvipalveluiden konfigurointiin ei ollut helposti löydettävissä, vaan suositukset olivat lähinnä yleisiä teknisiä ohjeita yksittäisten ominaisuuksien käyttöönottoon. Toivon että tästä opinnäytetyöstä on apua saada peruskäsitys pilvipalveluiden uhista, mitä on otettava huomioon ja minkälaisia resursseja on syytä varata käyttöönottoprojektia varten.

Käyttäjillä on kuitenkin suurin vastuu omien tunnusten hallinnasta, siitä minkälaista tietoa palveluun tallentaa ja miten hyödyntää pilvipalveluiden mahdollisuuksia. Perehtymätön käyttäjä lankeaa huomattavasti helpommin laadukkaasti tehtyyn kalasteluviestiin menettäen tunnuksensa, kuin työntekijä, joka tiedostaa verkossa ja pilvipalveluissa piilevät riskit.

Näkisin yhtenä jatkotutkimusaiheena pilvipalvelut käyttäjän näkökulmasta ja miten käyttäjät kokevat organisaatioiden panostavat perehdytykseen sekä kouluttamiseen. Toisena aiheena näkisin pilvipalvelut tietosuojan näkökulmasta ja lain määräämät rajoitteet pilvipalveluille, jossa perehdyttäisiin lainsäädäntöön tarkemmin. Kolmantena aiheena näkisin vertailun pilvipalvelut vastaan omat palvelimet työympäristö, eli vertailuna hyödyt, haitat, suorituskyky, vikasietoisuus, kulurakenne, kapasiteetti ja turvallisuus.

Lähteet

Aarness, A 2022. WHAT IS XDR?. Verkkojulkaisu: https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/. Viitattu 26.4.2022

Arstila, A. 2019. Kuusi askelta onnistuneeseen MFA-käyttöönottoon. Verkkojulkaisu https://sulava.com/tietoturva/kuusi-askelta-onnistuneeseen-mfa-kayttoonottoon/. Viitattu 22.3.2022

Azure. N.d. Microsoft Defender For Cloud. Verkkojulkaisu: https://azure.microsoft.com/en-us/services/defender-for-cloud/#overview. Viitattu 25.4.2022

Brook, C. 2020. What is Office 365 Data Loss Prevention? A Definition of Office 365 DLP, Benefits, and more. Verkkojulkaisu: https://digitalguardian.com/blog/what-office-365-data-loss-prevention-definition-office-365-dlp-benefits-and-more. Viitattu 23.4.2022

CheckPoint. N.d. Check Point Research: Cyber Attacks Increased 50 % Year over Year. Verkkojulkaisu: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/. Viitattu 25.4.2022

CYBERDI. N.d. Verkkojulkaisu https://jyvsectec.fi/2018/10/cyberdi/. Viitattu 23.4.2022

Diogenes, Y. 2021. A New name for multi-cloud security: Microsoft Defender for Cloud. Verkkojulkaisu: https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/a-new-name-for-multi-cloud-security-microsoft-defender-for-cloud/ba-p/2943020. Viitattu 25.4.2022

Euroopan parlamentin ja neuvoston asetus 2016/679. 2016. Euroopan parlamentin tietosuoja-asetus. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri= CELEX:32016R0679&from=EN #d1e40-1-1. Viitattu 22.2.2022

Eurostat 2021. Cloud computing – statistics on the use by enterprises. Verkkojulkaisu: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Use_of_cloud_computing:_highlights. Viitattu 23.4.2022

Ficom 2021. The use of cloud computing in Finland and around the world. Verkkojulkaisu: https://www.ficom.fi/news/the-use-of-cloud-computing-in-finland-and-around-the-world/. Viitattu 24.4.2022

Grönfors, M. 2011. Laadullisen tutkimuksen kenttätyömenetelmät. Verkkojulkaisu: https://books.google.fi/books?hl=fi&lr=&id=F3oaCwAAQBAJ&oi=fnd&pg=PA1 &dq=kvalitatiivinen+tutkimus&ots=Yh-oWmDuuX&sig=3uPrJNWIXSO2_8A8ZuC9Jdu2LM0&redir_esc=y#v=onepage&q=kvalitatiivinen%20tutkimus&f=false. Viitattu 23.4.2022

Harvey, S. 2018. Who´s responsible for cloud security? Verkkojulkaisu: https://kirkpatrickprice.com/blog/whos-responsible-cloud-security/. Viitattu 24.4.2022

Hernández, L. 2020. Kaksivaiheinen tunnistautuminen suojaa käyttäjätilejäsi. Verkkojulkaisu: https://blog.f-secure.com/fi/kaksivaiheinen-tunnistautuminen/. Viitattu 22.3.2022

Hyvärinen, M., Suoninen, E. & Vuori, J. N.d. Haastattelut. Teoksessa Vuori, J. (toim.) Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. Verkkojulkaisu: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-aineistot/haastattelut/. Viitattu 23.4.2022

IBM 2021. IaaS vs. PaaS vs. SaaS. Verkkojulkaisu: https://www.ibm.com/cloud/learn/iaas-paas-saas. Viitattu 25.4.2022

Jamk. N.d. Jamk. Verkkojulkaisu: https://www.jamk.fi/fi/jamk. Viitattu 23.4.2022

Jokinen, S. 2021. 5 syytä, miksi teillä pitäisi olla kaksivaiheinen tunnistautuminen käytössä. Verkkojulkaisu: https://materiaalit.triuvare.fi/artikkelit/miksi-teilla-pitaisi-olla-kaksivaiheinen-tunnistautuminen-kaytossa. Viitattu 22.3.2022

Juhila, K. N.d. Laadullisen tutkimuksen ominaispiirteet. Teoksessa Vuori, J. (toim.) Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. Verkkojulkaisu: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/mita-on-laadullinen-tutkimus/laadullisen-tutkimuksen-ominaispiirteet/. Viitattu 1.3.2022

Kauppi, J. 2019. Pilven tietoturva, hyödyt ja haitat. Verkkojulkaisu: https://www.leijonasecurity.fi/2019/09/18/pilven-tietoturva-hyodyt-ja-haitat/. Viitattu 25.4.2022

Kyberturvallisuuskeskus 2014. Pilvipalveluiden turvallisuus. Verkkojulkaisu: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf. Viitattu 24.4.2022

Kyberturvallisuuskeskus 2018. Office 365 -sähköpostin tietojenkalastelu ja tietomurrot erittäin yleisiä – havaitse, suojaudu, tiedota! Verkkojulkaisu: https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota. Viitattu 22.3.2022

Kyberturvallisuuskeskus 2019. Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta. Verkkojulkaisu: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Suojautuminen%20Microsoft%20Office%20365%20-tunnusten%20kalastelulta%20ja%20tietomurroilta%20web.pdf. Viitattu 22.3.2022

Lausuntopalvelu N.d. Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa. Verkkojulkaisu: https://www.lausuntopalvelu.fi/SV/Proposal/DownloadProposalAttachment?attachmentId=16635. Viitattu 27.4.2022

Leinonen, R. 2018. Tutkimuksen eettisyys. Verkkojulkaisu: https://spoken.fi/tutkimuksen-eettisyys/. Viitattu 23.4.2022

Magic Cloud 2019. Mikä on MFA ja miksi se tulisi ottaa käyttöön? Verkkojulkaisu: https://magiccloud.fi/mika-on-mfa-ja-miksi-se-tulisi-ottaa-kayttoon/. Viitattu 22.3.2022

Microfocus 2021. What is a Security Operations Center (SOC)? Verkkojulkaisu: https://www.microfocus.com/en-us/what-is/security-operations-center. Viitattu 26.4.2022

Microsoft 2015. Evolving Data Loss Prevention in SharePoint Online/OneDrive for Business and Office applications. Verkkojulkaisu: https://www.microsoft.com/en-us/microsoft-365/blog/2015/04/21/evolving-data-loss-prevention-in-sharepoint-onlineonedrive-for-business-and-office-applications/. Viitattu 18.1.2022

Microsoft 2020. Onko pilvitoimistosi ajan hermolla? Verkkojulkaisu: https://www.inmicsnebula.fi/fi/blogi/onko-pilvitoimistosi-ajan-hermolla. Viitattu 23.4.2022

Microsoft 2021a. Microsoft Defender for Identity architecture. Verkkojulkaisu: https://docs.microsoft.com/en-us/defender-for-identity/architecture. Viitattu 24.4.2022

Microsoft 2021b. What authentication and verification methods are available in Azure Active Directory? Verkkojulkaisu: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods. Viitattu 14.3.2022

Microsoft 2022a. What is Conditional Access?. Verkkojulkaisu: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview. Viitattu 23.4.2022.

Microsoft 2022b. Create and configure retention policies. Verkkojulkaisu: https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide. Viitattu 24.4.2022

Microsoft 2022c. Learn about retention for SharePoint and OneDrive. Verkkojulkaisu: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide. Viitattu 24.4.2022

Microsoft 2022d. Windows Hello for Business Overview. Verkkojulkaisu: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview. Viitattu 15.3.2022

Microsoft 2022e. Enable passwordless security key sign-in. Verkkojulkaisu: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key. Viitattu 15.4.2022

Microsoft 2022f. Authentication methods in Azure Active Directory – OATH tokens. Verkkojulkaisu: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-oath-tokens. Viitattu 20.3.2022

Microsoft 2022g. Configure and enable users for SMS-based authentication using Azure Active Directory. Verkkojulkaisu: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-sms-signin. Viitattu 8.3.2022

Microsoft 2022h. Authentication methods in Azure Active Directory – phone options. Verkkojulkaisu: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-phone-options. Viitattu 23.3.2022

Microsoft 2022i. Plan a Conditional Access deployment. Verkkojulkaisu: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access. Viitattu 20.3.2022

Microsoft 2022j. Microsoft 365 Defender. Verkkojulkaisu: https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide. Viitattu 25.4.2022

Microsoft 2022k. Protect your endpoints with Defender for Cloud's integrated EDR solution: Microsoft Defender for Endpoint. Verkkojulkaisu: https://docs.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint?tabs=windows. Viitattu 25.4.2022

Microsoft. N.d. a. Compare Office 365 to Microsoft 365. Verkkojulkaisu: https://www.microsoft.com/en-us/microsoft-365/enterprise/compare-microsoft-365-and-office-365. Viitattu 24.4.2022

Microsoft. N.d. b. Integroitu uhilta suojautuminen koko Office 365:lle. Verkkojulkaisu: https://www.microsoft.com/fi-fi/security/business/threat-protection/office-365-defender. Viitattu 24.2.2022

Microsoft. N.d. c. Complete endpoint security. Verkkojulkaisu: https://www.microsoft.com/en-us/security/business/threat-protection/endpoint-defender. Viitattu 22.4.2022

Mutta, J. 2020. Julkinen hallinto ja julkipilvi. Verkkojulkaisu: https://onrego.fi/julkinen-hallinto-ja-julkipilvi/. Viitattu 29.3.2022

Perus, M. 2020. Office 365 vs Microsoft 365 – vertailimme palveluja. Verkkoblogi: https://blogi.valtti.com/office-365-vs.-microsoft-365. Viitattu 24.4.2022

Petters, J. 2020. What is a Domain Controller, When is it Needed + Set Up. Verkkojulkaisu: https://www.varonis.com/blog/domain-controller. Viitattu 26.4.2022

Poisson, L. 2020. Office 365 vs Microsoft 365: Name Changes Explained. Verkkojulkaisu: https://www.lakesidesoftware.com/office-365-vs-microsoft-365-name-changes-explained/. Viitattu 24.4.2022

Ranger, S. 2022. What is cloud computing? Everything you need to know about the cloud explained. Verkkojulkaisu: https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/. Viitattu 10.3.2022

RecordPoint 2019. How Retention Works in Office 365. Verkkojulkaisu: https://www.sharepointeurope.com/how-retention-works-in-office-365/. Viitattu 24.3.2022

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. Aineiston hankinta. KvaliMOTV - Menetelmäopetuksen tietovaranto. Verkkojulkaisu: https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6.html. Viitattu 23.4.2022

Sarajärvi, A. & Tuomi, J. 2017. Laadullinen tutkimus ja sisällönanalyysi: Uudistettu laitos. Verkkojulkaisu: https://books.google.fi/books?hl=fi&lr=&id=h_VDDwAAQ-BAJ&oi=fnd&pg=PT3&dq=laadullinen+tutkimus+ja+sis%C3%A4ll%C3%B6nanalyysi&ots=fFtMS-SKWH&sig=0dsGHBPdCuHcqCGF79zHkKLoWuo&redir_esc=y#v=onepage&q=laadullinen%20tutkimus%20ja%20sis%C3%A4ll%C3%B6nanalyysi&f=false Viitattu 23.4.2022

Tietosuojavaltuutetun toimisto N.d. Usein kysyttyä EU:n tietosuoja-asetuksesta. Verkkojulkaisu: https://tietosuoja.fi/gdpr. Viitattu 26.4.2022

Traficom 2020a. Katakri 2020. Verkkojulkaisu: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246. Viitattu 7.3.2022

Traficom 2020b. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKRI). Verkkojulkaisu: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf. Viitattu 11.3.2022.

Tuomi, J. & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. Jyväskylä: Gummerus kirjapaino Oy

Tutkimuseettinen neuvottelukunta 2012. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Verkkojulkaisu: https://tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf. Viitattu 23.4.2022

Valtiovarainministeriö 2018. Julkisen hallinnon pilvipalvelulinjaukset. Valtiovarainministeriön julkaisu 35/2018. Verkkojulkaisu: http://urn.fi/URN:ISBN:978-952-251-982-5. Viitattu 15.2.2022

Valtiovarainministeriö 2019. Linjaukset julkisen hallinnon pilvipalveluista julkaistu. Verkkojulkaisu: https://vm.fi/-/linjaukset-julkisen-hallinnon-pilvipalveluista-julkaistu. Viitattu 15.2.2022

Vetikko, P. 2020a. Perinteisen tietoturvan hallintakeinot pätevät myös pilvessä, osa 1. Verkkojulkaisu: https://www.insta.fi/nakemyksia/perinteiset-tietoturvan-hallintakeinot-p%C3%A4tev%C3%A4t-my%C3%B6s-pilvess%C3%A4. Viitattu 23.4.2022

Vetikko, P. 2020b. Pilvipalveluiden Top 10 -tietoturvariskit (OWASP-luonnos) ja niihin varautumien, osa 2. Verkkojulkaisu: https://www.insta.fi/nakemyksia/pilvipalveluiden-top-10-tietoturvariskit-owasp-luonnos-ja-niihin-varautuminen. Viitattu 23.4.2022

Vetikko, P. 2020c. Pilvipalveluiden Top 10 -tietoturvariskit (OWASP-luonnos) ja niihin varautuminen, osa 3. Verkkojulkaisu: https://www.insta.fi/nakemyksia/pilvipalveluiden-top-10-tietoturvariskit-owasp-luonnos-ja-niihin-varautuminen-1. Viitattu 23.4.2022

VM IT. N.d. Kapasiteettipalvelut. Verkkojulkaisu: https://www.vmit.fi/palvelut/kapasiteetti. Viitattu 24.4.2022

Liitteet

Liite 1. Huomioi nämä pilvipalvelun käyttöönotossa!

1. Tiedon säilytysaika
    - Kuinka kauan pilvipalveluissa halutaan säilyttää tietoa? Yritys voi määritellä kauanko tieto halutaan säilyttää pilvipalveluissa. Tässä tulee huomioida mahdolliset lakien ja asetusten muodostamat vaatimukset ja rajaukset.

2. Tiedon menettämisen esto
    - Miten halutaan varmistaa tiedonsäilyvyys? On tärkeää, että tietoa ei voida tahallisesti tai tahattomasti poistaa pilvipalveluista. Tietojen palauttaminen on mahdollista halutun ajan puitteissa.

3. Pilvipalveluiden vieraskäyttö
    - Miten tiedonjakaminen on mahdollista pilvipalveluissa? Yritys voi määritellä mihin tietoihin ja ympäristöihin vierailla käyttäjillä on mahdollista päästä sekä miten vieraskäyttäjien on mahdollista käyttää tietoja.

4. Pilvipalveluiden jakamiskäytännöt
    - Miten tiedon jakaminen on mahdollista pilvipalveluissa ja pilvipalveluista? Yritys voi määritellä miten tietoja voidaan jakaa ja mihin sekä kuka voi jakaa ja kenelle.

5. Pääsynhallinta pilvipalveluihin
    - Yritys voi määritellä millä ehdoilla pilvipalveluihin pääsee ja minkälaista varmennusta käytetään.

6. Tiedon sijainti
    - Yrityksen on tärkeä miettiä, mitä tietoa halutaan säilyttää ja käsitellä pilvipalveluissa vai halutaanko tiettyjä asioita säilyttää fyysisessä sijainnissa.