Haaga-Helia
ammattikorkeakoulu Oy

Pilvipalveluiden tietoturvallisuus yrityskäytössä

Roope Pohjanheimo

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2020

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t) Roope Pohjanheimo	
Koulutusohjelma Tietojenkäsittelyn koulutusohjelma	
Raportin/Opinnäytetyön nimi Pilvipalveluiden tietoturvallisuus yrityskäytössä	**Sivu- ja liitesivumäärä** 38

Tämä opinnäytetyö käsittelee pilvipalveluiden tietoturvallisuutta yrityskäytössä tutkimalla pilvipalveluihin kohdistuvia riskejä sekä seikkoja, jotka vaikuttavat pilvipalveluiden tietoturvallisuuteen. Tutkimuksessa käsitellään myös Microsoftin Azure-pilvipalvelua ja sen tietoturvakäytäntöjä sekä toteutustapoja.

Tutkimus on rajattu koskemaan vain yritysten käyttämiä pilvipalveluita ja siinä keskitytään lähinnä IaaS-mallin pilvipalveluihin. Tutkimusmenetelmänä käytettiin kirjallisuuskatsausta, koska se nähtiin aiheeseen sopivimmaksi tutkimusmenetelmäksi.

Opinnäytetyössä tarkastellaan ensin isoimpia pilvipalveluihin kohdistuvia riskejä, jonka jälkeen siirrytään tutkimaan yleisesti pilvipalveluiden tietoturvallisuuteen vaikuttavia tekijöitä. Viimeisenä tutkimuksen osiona tutkitaan Microsoft Azuren infrastruktuurin tietoturvallisuutta ja tietoturvakäytäntöjä.

Pilveen liittyy riskejä, mutta ne ovat pitkälti samanlaisia, kuin perinteisessä On-premises ympäristössäkin. Pilvessä käytetään kuitenkin jaettua vastuumallia asiakkaan ja palveluntarjoajan välillä, joten riskienhallinta kuuluu kummallekin osapuolelle. Tutkimuksen yhden osa-alueen kohteena ollut pilvipalvelu Microsoft Azure toteuttaa tutkimuksen mukaan infrastruktuurinsa tietoturvaa erittäin pätevästi, eikä siinä nähty minkäänlaisia kritisoimisen kohteita.

Opinnäytetyön tuloksena on todettu, että kun pilvipalveluntarjoaja on huolellisesti valittu taustat tarkistaen, sopimukset tehty asianmukaisesti kaikesta mahdollisesta ja siirtyminen pilveen on tehty asianmukaisesti oikeanlaisia käytäntöjä ja arkkitehtuuria käyttäen, niin ei yrityksen tulisi pelätä tietojensa jakamista kolmannen osapuolen kanssa.

Asiasanat
Tietoturva, Pilvipalvelut, Microsoft Azure, Tietosuoja

Sisällys

1 Johdanto

Pilvipalveluiden suosio on kasvanut räjähdysmäisesti viimeisen kymmenen vuoden aikana ja lähes kaikilla yrityksillä onkin jo joitain pilvipalveluita käytössään. (Shein 2019) Pilvipalveluiden suosio perustuu pitkälti niiden kustannustehokkuuteen, skaalautuvuuteen ja helppokäyttöisyyteen. Suosion mukana keskustelunaiheeksi on noussut myös pilvipalveluiden tietoturva. Pilvipalveluiden tietoturva mietityttää, koska data ja sen suojaus ei ole enää vain yrityksen omissa käsissä, vaan pilvipalvelun käyttöönoton myötä myös pilvipalvelun-tarjoajalla on iso rooli datan suojelemisessa ja tietoturvan toteuttamisessa. Yrityksille pilveen siirtyminen ei siis ole mikään pieni askel, vaan todella kauan ja tarkkaan harkittu siirto. Pilvipalveluiden ympärillä pyörivän tietoturvakeskustelun myötä valitsin tämän aiheen tutkittavakseni.

Tämän opinnäytetyön tarkoituksena on selvittää, ovatko pilvipalvelut tarpeeksi turvallisia käytettäväksi yritysympäristöissä. Tämä tapahtuu tutkimalla pilvipalveluiden tietoturvallisuuteen vaikuttavia tekijöitä ja niihin kohdistuvia riskejä. Tavoitteena on poistaa pilvipalveluiden tietoturvaan liittyviä väärinkäsityksiä ja antaa lukijalle kattava kokonaiskuva pilvipalveluiden tietoturvakäytännöistä. Tutkimus on rajattu koskemaan vain yrityksille suunnattuja pilvipalveluja ja siinä keskitytään lähinnä IaaS-mallin pilvipalveluihin. Tutkimuksessa tutkitaan myös Microsoft Azuren tietoturvallisuutta ja sen tietoturvakäytäntöjä. Tämä tehdään, jotta tutkimuksesta tulisi mahdollisimman käytännönläheinen ja konkreettinen.

Tässä opinnäytetyössä tutkimuskysymyksinä toimivat seuraavat kysymykset:

- Millaisia riskejä pilvipalveluiden käyttöön liittyy?
- Millaisilla tavoilla pilvestä voidaan tehdä mahdollisimman tietoturvallinen?
- Miten Microsoft Azuren tietoturvaa toteutetaan?

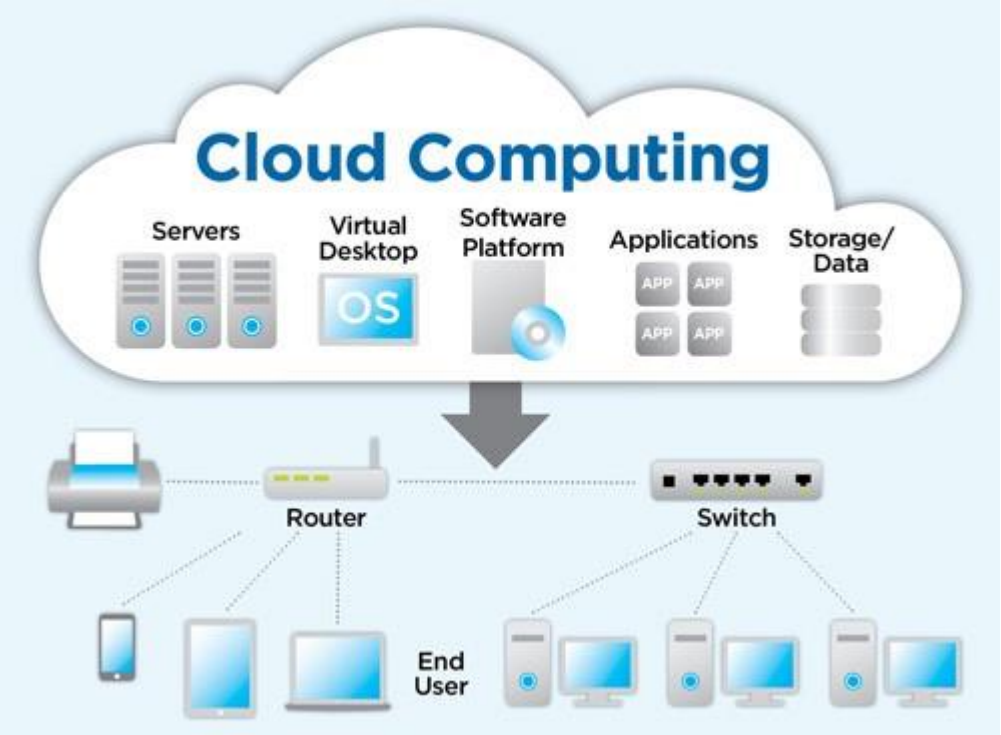
Tämä tutkimus toteutetaan kirjallisuuskatsauksena, sillä aiheesta löytyy kattavasti tietoa avoimista lähteistä ja se nähdään tähän tutkimukseen sopivimmaksi vaihtoehdoksi. Tutkimuksen 4. kappale, eli Microsoft Azuren tietoturvallisuuden tutkiminen tapahtuu tutkimalla Microsoftin tietoturvakäytäntöjä ja dokumentaatioita Azureen liittyen.

Opinnäytetyö jakaantuu neljään osaan. Ensimmäisessä kappaleessa käydään läpi pilvipalveluiden taustaa, eli mitä ne ovat ja miten niitä voidaan jaotella. Ensimmäisessä kappaleessa käsitellään myös tietoturvan määritelmää sekä tietosuojaa. Toisessa kappaleessa perehdytään pilvipalveluiden tietoturvariskeihin Cloud Security Alliancen vuonna 2019 tekemän tutkimuksen mukaan yleisellä tasolla. Kolmannessa kappaleessa tutkitaan millaisilla tavoilla ja käytännöillä pilvestä voidaan tehdä mahdollisimman turvallinen. Toisessa ja

kolmannessa kappaleessa ei siis paneuduta mihinkään yksittäiseen pilvipalveluun, vaan tutkitaan asiaa yleisesti ottaen huomioon kaikenlaiset pilvipalvelut. Viimeisessä kappaleessa tutkitaan Microsoft Azuren infrastruktuurin tietoturvaa. Kappaleen tarkoituksena on selvittää, kuinka tietoturvallinen Microsoft Azure on käytettäväksi yritysympäristössä ja mitä Microsoft tekee Azuren infrastruktuurin tietoturvallisuuden eteen.

2 Pilvipalvelut yleisesti

Pilvipalvelut tarkoittavat internetin ylitse käytettäviä tiedostoja, ohjelmistoja ja palveluita, jotka sijaitsevat palveluntarjoajan palvelimilla yrityksen omien palvelimien sijasta. Yrityksen ei siis tarvitse itse omistaa omaa datakeskusta tai rakentaa omaa infrastruktuuriaan, sillä tämä kaikki voidaan tehdä pilvipalveluiden avulla. Pilvipalvelut mahdollistavat esimerkiksi sen, että päästäkseen käsiksi haluttuihin tiedostoihin voidaan käyttää mitä tahansa laitetta, eikä vain yhtä ja samaa, jolla tiedosto on luotu. (Ranger 2018) Pilvi voidaan jakaa Front- ja Back end -osiin, jotka ovat yhdistettynä toisiinsa internetin välityksellä. Front endillä tarkoitetaan osiota, jossa palvelua käytetään ja joka on näkyvä pilvipalvelun käyttäjälle. Back endillä puolestaan tarkoitetaan tietokoneita, palvelimia ja tietovarastoja, jotka tekevät pilvipalvelun käytön mahdolliseksi. (Fastmetrics) Kuva 1. havainnollistaa pilven toimintaa.



Kuva 1. Pilven toimintaperiaate (World Informatix)

Pilvipalvelut ovat yritykselle usein erittäin kustannustehokas ratkaisu omien järjestelmien pyörittämiseen, sillä niiden veloitus skaalautuu usein käytön mukaisesti. Mitä enemmän palveluita käytetään, sitä enemmän niistä maksetaan. (Ranger 2018) Pilveen siirtyminen onkin usein yrityksille erittäin houkutteleva vaihtoehto juurikin sen veloituksen skaalautuvuuden ja käytettävyysmahdollisuuksien takia.

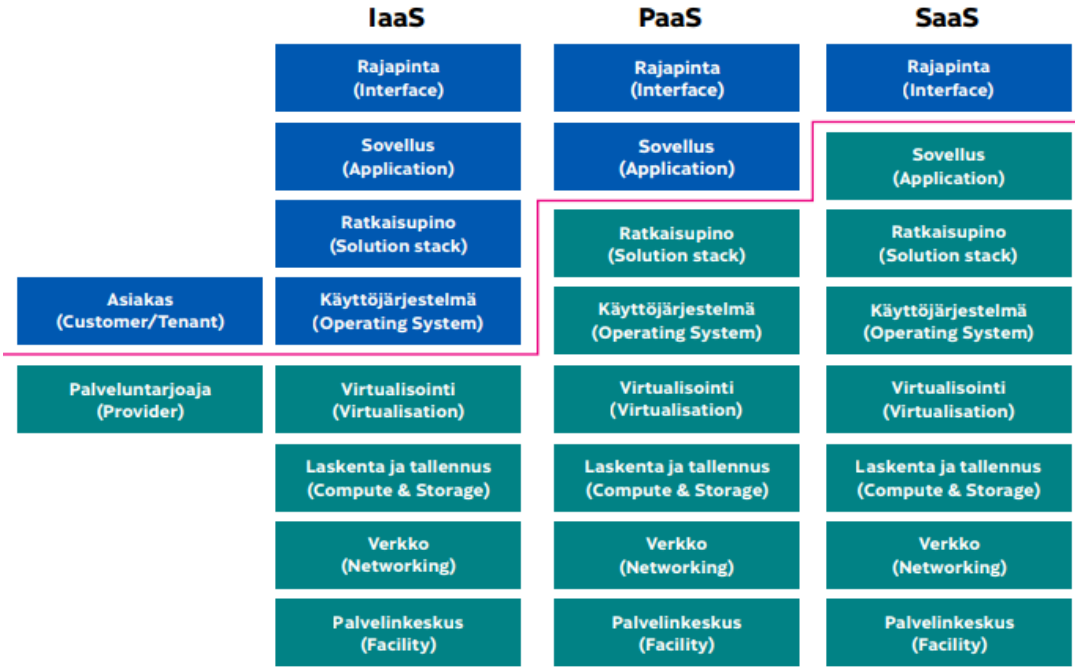
Pilvipalvelut ovat nostaneet suosiotaan huimasti viimeisen kymmenen vuoden aikana. Flexeran vuonna 2019 teettämän tutkimuksen mukaan 94% prosenttia kyselyyn vastanneista

yrityksistä käyttää pilveä jollain tavalla osana yrityksen toimintaa (Flexera 2019). Yritysten käyttämät pilvi-infrastruktuurit ovat myös kasvamassa ja ennustetaankin, että vuoden 2020 lopussa 67% yrityksistä tulee käyttämään pilvi-infrastruktuuria (Radoslav 2019). Pilven yleistyminen johtuu pääasiassa teknologioiden edistyksestä ja nopeiden internetyhteyksien yleistymisestä ympäri maailman. Yritykset ovat halunneet myös jatkuvasti investoida infrastruktuurin jatkuvaan rakentamiseen ja päivittämiseen, joka on johtanut pilvipalveluiden valtavaan suosioon. (Huntington 2019)

2.1 Pilven palvelumallit

Pilvipalvelut voidaan jakaa kolmeen eri alaluokkaan, jotka ovat Software as a Service (SaaS), Platform as a Service (PaaS) ja Infrastructure as a Service (IaaS). SaaS-mallissa yritys ei itse hallitse mitään osaa ohjelmistossa, vaan kaikkea hallinnoi palveluntarjoaja. PaaS ja IaaS -malleissa yrityksellä on hallintaoikeuksia ohjelmistoihin tai palveluihin, eikä palveluntarjoaja hallinnoi kaikkea. Kaikissa pilvipalvelumalleissa on kuitenkin aina mukana kolmas osapuoli, joka hallinnoi joitakin osia palvelusta. On-Premises on niin sanottu perinteinen hallintamalli, jossa yritys hallinnoi kaikkea ohjelmistoon tai palveluun liittyvää itse palvelimista lähtien.

Kuva 2 havainnollistaa näiden eri palvelumallien hallintavastuita. Sinisellä värillä kuvatut osiot ovat yrityksen itsensä hallittavissa ja vihreällä värillä kuvattuja kohtia hallitsee palveluntarjoaja. Näistä kolmesta pilvipalvelumallista kerrotaan tarkemmin alempana.



Kuva 2. Eri pilvipalvelumallien hallintavastuut (Kyberturvallisuuskeskus 2020)

2.1.1 SaaS

SaaS, eli Software as a Service (Suom. Ohjelmisto palveluna) tarkoittaa ohjelmistoa, joka toimii internetin ylitse. SaaS-tuotteiden käyttöön tarvitaan vain verkkoyhteys ja internetselain, eikä käyttäjän tarvitse huolehtia muusta, sillä palveluntuottaja hoitaa loput. Mitään asennuksia ei siis tarvita. SaaS on erittäin kustannustehokas tapa yritykselle käyttää ohjelmistoja, sillä palveluntuottaja hoitaa kaikki ohjelmiston ylläpitoon liittyvät asiat ja ohjelmistoa voidaan käyttää milloin vain ja mistä vain. (Turner 2019)

Hyvänä esimerkkinä SaaS-ohjelmistosta toimii Salesforce, joka on yksi maailman tunnetuimmista SaaS-ohjelmistoista. Salesforce tarjoaa esimerkiksi asiakkuudenhallintajärjestelmän verkon yli, joten yritysten ei tarvitse ostaa kalliita ohjelmistolisenssejä. (Sraders 2020)

2.1.2 PaaS

PaaS, eli Platform as a Service (Suom. Alusta palveluna) tarkoittaa sovellusalustaa, jolle yritykset voivat kehittää, ajaa ja hallita omia ohjelmistoja ja järjestelmiään. Tässä mallissa sovelluskehittäjät voivat keskittyä ohjelmien kehittämiseen eikä heidän tarvitse huolehtia esimerkiksi alustan infrastruktuurista, vaan tämä tapahtuu palveluntarjoajan toimesta. Tämä nopeuttaa kehittäjien työtä ja antaa heille joustavuutta koko prosessiin. (Watts & Raza 2019)

WordPress on hyvä esimerkki PaaS-palvelusta, sillä siinä WordPress toimii vain julkaisualustana ja käyttäjän on itse huolehdittava esimerkiksi päivityksistä ja tietoturvasta (Eronen 2016).

2.1.3 IaaS

IaaS, eli Infrastructure as a Service (Suom. Infrastruktuuri palveluna) tarkoittaa palvelumallia, jossa palveluntarjoaja tarjoaa yritykselle verkon yli käytettävää palvelinkapasiteettia. Tämä malli korvaa siis perinteiset yritysten omat konesalit, sillä palvelimet sijaitsevat palveluntarjoajan tiloissa. (Telia 2018) Kuvassa 1 nähdään, että tässä mallissa palveluntarjoaja huolehtii vain palvelimista, tallennustilasta, virtualisoinnista ja tietoverkoista. Yrityksen kontolle jää siis hoidettavaksi loput.

IaaS-malli mahdollistaa yrityksille erittäin joustavan, helposti skaalautuvan ja kustannustehokkaan infrastruktuurin, jossa yrityksellä itsellään on kuitenkin täysi hallintaoikeus omaan

infrastruktuuriinsa. Yritykset voivat esimerkiksi lisätä palvelinkapasiteettia sen käytön mukaan. IaaS-malli on erittäin suosittu esimerkiksi startup-yritysten keskuudessa, sillä palvelu on erittäin helppo ottaa käyttöön ja sitä on helppo skaalata yrityksen nopeaan kasvuun. (Watts & Raza 2019)

IaaS-mallia käyttävältä yritykseltä vaaditaan kuitenkin paljon osaamista, sillä heidän vastuulleen jäävät esimerkiksi kaikki infrastruktuuria koskevat konfiguraatiot. Näihin kuuluvat esimerkiksi tietoturva ja palomuuraus. (Eronen 2016)

2.1.4 On-premises

On-premises tarkoittaa ohjelmistoa tai järjestelmiä, joita hallitaan kokonaan yrityksen omilla palvelimilla. On-premises on siis niin sanottu perinteinen hallintamuoto yritys- ja asiakasjärjestelmien käyttöön. Tässä mallissa vaaditaan tyypillisesti lisenssi kaikille ohjelman tai järjestelmän käyttäjille ja yritys on kokonaan itse vastuussa kaikesta siihen liittyvästä, kuten tietoturvallisuudesta, saatavuudesta ja hallinnoinnista. Tästä syystä On-premises-malli onkin myös usein kalliimpi ratkaisu, kuin pilviratkaisut. (Techopedia)

2.2 Pilven toimitusmallit

Pilvipalveluiden arkkitehtuureita voidaan toimittaa kolmella eri tavalla, jotka ovat yksityinen pilvi, julkinen pilvi sekä hybridipilvi. Tässä alaluvussa käsitellään näitä toimitusvaihtoehtoja ja niiden eroavaisuuksia.

2.2.1 Yksityinen pilvi

Yksityinen pilvi tarkoittaa pilvipalvelumallia, jossa pilvipalvelu on yksinomaan vain yhden yrityksen käytössä. Tässä mallissa palvelimet voivat sijaita yrityksen omissa tiloissa tai niitä voidaan hallita kolmannen osapuolen toimesta. Jos kolmas osapuoli hoitaa yksityisen pilven hallintaa, niin laskentaresurssit on eristetty, eli niitä ei jaeta muiden asiakkaiden kanssa ja ne toimitetaan asiakkaalle turvallisen yksityisen verkon ylitse. Yksityisessä pilvessä asiakkaalla on parempi hallittavuus infrastruktuuristaan ja sen avulla voidaan helposti toteuttaa yrityksen haluamia vaatimuksia. (Raza 2020)

2.2.2 Julkinen pilvi

Julkinen pilvi on pilvipalvelumalli, jossa palvelut tai järjestelmät toimitetaan internetin ylitse. Julkisessa pilvessä toimivat ohjelmat voivat vaihdella sähköpostiohjelmista kokonaiseen infrastruktuuriin. Tässä palvelumallissa palveluntarjoaja on vastuussa laskentare-

surssien, eli esimerkiksi palvelinten ja tietokantojen toiminnasta. Julkinen pilvi tarjoaa asiakkaalle korkeaa joustavuutta sekä skaalautuvuutta hyvin kustannustehokkaalla hinnoittelulla. Julkinen pilvi on palvelumalleista suosituin ja se tarjoaakin usein kaiken kokoisille yrityksille laajan valikoiman ratkaisuja heidän tarpeisiinsa. (Raza 2020)

2.2.3 Hybridipilvi

Hybridipilvi tarkoittaa ratkaisua, jossa julkinen ja yksityinen pilvi on yhdistetty toisiinsa. Yrityksen käyttämät ohjelmat ja tiedot voivat siis jakautua yksityisen ja julkisen pilven välillä niin, että ne noudattavat yrityksen määrittämiä käytäntöjä koskien turvallisuutta, suorituskykyä, skaalautuvuutta ja kustannustehokkuutta. Yritys voi ottaa julkisen pilven käyttöönsä yksityisen pilven kanssa esimerkiksi, jos se haluaa julkisesta pilvestä lisää laskentatehoja hetkellisiä verkkoliikenteen ruuhkapiikkejä varten. (Raza 2020)

2.3 Tietoturvan määritelmä

Tietoturvalla tarkoitetaan teknisiä ja hallinnollisia toimia, joilla varmistetaan tiedon luotettavuus, eheys sekä saatavuus (Confidentiality, Integrity, Availability). Näistä muodostuu niin sanottu CIA-kolmio, joka on tietoturvan ydin. Luottamuksellisuudella varmistetaan, että tietty tieto on saatavilla vain henkilöille, jotka ovat siihen oikeutettuja. Eheydellä varmistetaan, että tietoa ei voida muuttaa, paitsi jos on siihen oikeutettu. Käytettävyydellä varmistetaan, että tiedot ovat aina käytettävissä henkilöille, jotka ovat siihen oikeutettuja. (Kyberturvallisuuskeskus 2019a)

Luottamuksellisuuden todentamiseksi yrityksen täytyy siis pystyä jollakin keinolla todentamaan, kuka dataan yrittää päästä käsiksi. Todentamista voidaan harjoittaa esimerkiksi käyttäjätunnus + salasana -yhdistelmillä tai biometrisillä tunnisteilla. Tietojen salaaminen parantaa myös niiden luotettavuutta. (Fruhlinger 2020)

Eheyttä voidaan harjoittaa monilla samoilla keinoilla kuin luottamuksellisuuttakin, sillä kun hakkeri ei pääse järjestelmiin käsiksi, ei hän voi myöskään muuttaa niiden sisältämiä tietoja. Eheyttä voidaan kuitenkin harjoittaa muutamilla muillakin keinoilla. Yksi esimerkki näistä keinoista on tiivisteet. Tiivisteiden avulla voidaan varmistaa, että tieto pysyy samana koko sen elinkaaren ajan. Jos tiiviste muuttuu, niin tieto on vaarantunut. (Fruhlinger 2020)

Käytettävyyttä pyritään harjoittamaan esimerkiksi hyvillä verkkoresursseilla ja ajan tasalla olevilla varmuuskopioilla, jotta tieto olisi käytettävissä jopa pahimpien skenaarioiden aikana. Yrityksen tulisi soveltaa näitä periaatteita omaan turvallisuuspolitiikkaansa ja miettiä

mitkä tiedot ovat tärkeimpiä yrityksen toiminnan kannalta ja suojata ne. Turvallisuuspolitiikka ohjaa täten yrityksen toimia ja päätöksiä tietoturvaan liittyen ja auttaa esimerkiksi valitsemaan oikeita työkaluja tiedon suojaamiseen. (Fruhlinger 2020)

Tietoturvaa toteutetaan usein hallintamallien ja järjestelmien avulla, joita voidaan suunnitella käyttämällä erilaisia viitekehyksiä ja standardeja. ISO 27001 on yksi tunnetuimmista standardeista, joka asettaa vaatimuksia hallintajärjestelmän toiminnalle ja auttaa näin yritystä hallitsemaan tietoturvaansa. (Naden 2020) ISO 27001 tarjoaa siis ohjenuoran, jota yritys voi seurata kehittäessään tietoturvan hallintajärjestelmää. Hallintajärjestelmän viitekehys keskittyy usein riskien arviointiin sekä riskienhallintaan. (Raza 2019)

Hallintajärjestelmän tulisi kehittyä jatkuvasti ja ISO 27001:n mukaan hallintajärjestelmän implementointi seuraakin PDCA-mallia (Plan, Do, Check, Act). Tässä mallissa suunnitteluvaiheen tarkoituksena on ensin tunnistaa ongelmat ja kerätä tietoa, joiden avulla voidaan tunnistaa tietoturvariskejä. Tämän jälkeen määritellään käytännöt ja prosessit, joiden avulla voidaan käsitellä ongelmien syitä. Toteutusvaiheessa implementoidaan määritellyt käytännöt ja prosessit. Valvontavaiheessa monitoroidaan määriteltyjen käytäntöjen sekä prosessien tehokkuutta. Tässä vaiheessa tulisi myös arvioida hallintajärjestelmän tuottamia konkreettisia tuloksia. Toimintavaiheessa keskitytään jatkuvaan kehittymiseen, eli dokumentoidaan tuloksia, jaetaan tietoa ja käytetään hyväksi palautetta, jotta järjestelmästä, käytännöistä ja prosesseista saataisiin tulevaisuudessa entistä parempia. (Raza 2019)

Yritykseen kohdistuvia tietoturvariskejä voidaan arvioida samalla tavalla kuin muitakin riskejä, eli kertomalla uhkan todennäköisyys sen seurauksilla. Näin saadaan selville yritykseen kohdistuvan riskin suuruus. Todennäköisyydellä tarkoitetaan siis sitä, kuinka todennäköisesti uhka toteutuu ja seurauksilla taas tarkoittaa sitä, kuinka suuri vaikutus uhkalla on yrityksen toimintaan, jos se toteutuu. Kuvassa 3 esitetään taulukko, jonka avulla voidaan laskea riskin suuruus. Jos uhkan todennäköisyys olisi korkea ja sen seuraus olisi vakava, niin tällöin riskin suuruus olisi siis 3x2=6, eli se olisi yritykselle merkittävä tietoturvariski. (Valtiovarainministeriö 2003, 41-43)

Uhkan todennäköisyys	Uhkan seuraukset			
		Vähäinen (1)	Vakava (2)	Erittäin vakava (3)
	Alhainen (1)	Merkityksetön 1	Vähäinen 2	Kohtalainen 3
	Keskimääräinen (2)	Vähäinen 2	Kohtalainen 4	Merkittävä 6
	Korkea (3)	Kohtalainen 3	Merkittävä 6	Sietämätön 9

Kuva 3. Riskienhallintataulukko, jolla voidaan laskea riskin suuruus (Valtiovarainministeriö 2003, 43, muokattu)

2.4 Tietosuoja

Tietosuojalla tarkoitetaan yksityisyyden suojaa, jonka tarkoituksena on turvata rekisteröidyn henkilötietojen oikea käsittely ja suojaaminen luvattomalta käytöltä. Tietosuoja on perusoikeus, joten jokaisella on oikeus henkilötietojensa suojaan. Henkilötiedolla tarkoitetaan tietoja, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Näitä tietoja ovat siis sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa joko suoraan tai välillisesti yhdistelemällä tietoja toisiinsa. Henkilötietoja ovat siis esimerkiksi henkilön nimi, osoite, henkilötunnus, puhelinnumero ja IP-osoite. Henkilötietoja voidaan kuitenkin anonymisoida, jolloin tiedoista ei voida enää tunnistaa henkilöä. Tällöin tietoihin ei enää sovelleta tietosuojasäännöksiä. Tietoturvan avulla toteutetaan tietosuojaa, eli tietoturvatoimenpiteiden avulla suojataan tietoaineistoa ja tietojärjestelmiä, joissa säilytetään henkilötietoja ja näin turvataan rekisteröidyn oikeuksien toteutuminen. (Tietosuojavaltuutetun toimisto)

2.4.1 GDPR

GDPR, eli General Data Protection Regulation on Euroopan unionin vuonna 2018 laatima yleinen tietosuoja-asetus, jossa asetetaan tarkat vaatimukset yrityksille ja organisaatioille henkilötietojen keräämistä, säilytystä ja hallinnointia varten. Tätä asetusta sovelletaan kaikkiin yrityksiin ja organisaatioihin, jotka sijaitsevat EU:ssa, riippumatta siitä missä itse henkilötietojenkäsittely tapahtuu. Asetusta sovelletaan myös niihin yrityksiin, jotka sijaitsevat EU:n ulkopuolella, mutta käsittelevät henkilötietoja, jotka liittyvät tavaroiden tai palveluiden tarjoamiseen henkilöille EU:ssa. GDPR:n perusteella yritys saa käsitellä henkilötietoja vain, jos sille on laissa määritelty peruste. (Euroopan Unioni 2020)

3 Pilven tietoturvariskit

Pilven tietoturvariskit koostuvat pitkälti samankaltaisista asioista kuin perinteisen on-premises -mallinkin riskit. Eroavaisuutena on kuteinkin se, että vastuu riskienhallinnasta kuuluu sekä palveluntarjoajalle että pilvipalvelun asiakkaalle. Asiakkaan täytyy siis ymmärtää vastuunjako sekä huolehtia, että palveluntarjoaja hoitaa oman osuutensa. (Morrow 2018) Tässä kappaleessa käsitellään viittä isointa pilveen kohdistuvaa uhkaa Cloud Security Alliancen (CSA) vuonna 2019 teettämän tutkimuksen mukaan. Tutkimukseen osallistui 241 pilven tietoturvan ammattilaista. (Cloud Security Alliance 2019, 6) CSA on maailman johtava pilvipalveluiden tietoturvallisuuteen keskittynyt organisaatio, jonka tavoitteena on varmistaa turvallinen pilviympäristö.

3.1 Tietomurrot

CSA:n teettämän tutkimuksen mukaan isoimmaksi uhkaksi pilvipalveluiden turvallisuudelle on listattu tietomurrot. Tietomurto tarkoittaa tapahtumaa, jossa asiakkaan tietoja varastetaan, käytetään tai katsotaan luvattomasti. Tietomurto käsittää siis tietoja, joita ei ole tarkoitettu julkiseen käyttöön. Tietomurron kohteeksi joutunut yritys voi menettää mainettaan ja luottamustaan asiakkaiden ja yhteistyökumppaneiden keskuudessa. Rahalliset menetykset voivat myös olla suuria. (Cloud Security Alliance 2019, 7)

Tietomurrot on listattu isoimmaksi uhaksi, koska tiedosta on tulossa kyberhyökkäyksien merkittävin kohde. Tämän takia yritysten tulisikin määrittää sen tiedon arvo liiketoiminnalle ja sen menetyksestä koituneet haitat. Yrityksen tulisi myös miettiä tarkkaan, mitä tietoja pilveen siirretään. (Cloud Security Alliance 2019, 7) Koska pilvipalveluihin voidaan päästä käsiksi mistä tahansa ja miltä laitteelta tahansa, niin ne ovat erittäin altistuvaisia tietomurroille. Tämän takia yrityksellä tulisi olla käytössään erittäin vahva identiteetin- ja pääsynhallinta.

3.2 Väärät konfiguraatiot ja puutteellinen muutosten hallinta

Toisena tietoturvauhkana CSA:n listauksessa ovat väärät konfiguraatiot ja puutteellinen muutosten hallinta. Vääränlaisia konfiguraatioita tapahtuu, kun laitteistoja asennetaan väärin, ja tämän seurauksena ne jäävät haavoittuviksi hyökkäyksille. Kun puhutaan vääränlaisista konfiguraatioista, niin tällä voidaan tarkoittaa esimerkiksi suojaamattomia tietovarastoja, liiallisia käyttöoikeuksia tai käyttäjätunnuksia, joiden oletussalasanaa ja asetuksia ei ole vaihdettu. Vääränlaiset konfiguraatiot ovat yleisin syy tietomurtojen tapahtumiseen. Oikeanlainen konfigurointi jää asiakkaan vastuulle. (Cloud Security Alliance 2019, 10)

Vääränlaiset konfiguraatiot johtuvat kuitenkin usein puutteellisesta muutosten hallinnasta. Pilviympäristöt ja niiden metodit eroavat perinteisistä tietojenkäsittelytavoista tavoilla, jotka tekevät muutoksen hallinnasta vaikeampaa. Pilviympäristössä muutos tapahtuu paljon nopeammin, kuin perinteisessä ympäristössä, jossa muutoksen saaminen tuotantoon voi kestää jopa viikkoja. Pilviympäristöissä muutosten hallinta vaatii siis erittäin ketterää ja proaktiivista lähestymistapaa, jotka tulisi ottaa käyttöön pilveen siirtyessä. (Cloud Security Alliance 2019, 10)

3.3 Pilven tietoturva-arkkitehtuurin ja strategian puuttuminen

Yrityksen tai jonkin sen palvelun siirtyessä pilveen yksi isoimmista haasteista on sopivan tietoturva-arkkitehtuurin toteutus. Yrityksen siirtyessä pilveen vanhoilla IT-käytännöillä ja tietoturva-arkkitehtuurilla ilman muutoksia, sen tietoja altistuu useille uhkille. Jaetun vastuumallin ymmärtämättömyys on myös osasyynä tähän. (Cloud Security Alliance 2019, 13)

Usein pilveen siirtyminen tehdään hätiköiden, ja turvallisuuden sijasta muutoksessa tärkeimpinä tekijöinä pidetään toiminnallisuutta sekä muutoksen nopeutta. Tämä johtaa siihen, että yrityksen tietoturva-arkkitehtuuri ja strategia jäävät puutteellisiksi ja näin ollen yritys jää haavoittuvaiseksi kyberhyökkäyksiä vastaan. Jos yritys taas ottaa käyttöön pilveen sopivan tietoturva-arkkitehtuurin ja kehittää kestävän tietoturvastrategian, niin yrityksellä on erittäin hyvät lähtökohdat toimia ja tehdä liiketoiminta-aktiviteetteja pilvessä. Kun pilveen siirtyminen tehdään huolellisesti ja tietoturva-arkkitehtuuri sekä strategia toimivat pilveen siirtymisen perustana, niin tällöin vähennetään huomattavasti riskiä joutua onnistuneiden hyökkäysten kohteeksi. (Cloud Security Alliance 2019, 13)

3.4 Puutteellinen Identiteetin- ja pääsynhallinta

Identiteetin- ja pääsynhallintajärjestelmät tarkoittavat työkaluja ja käytäntöjä, joiden avulla yritys voi hallita, monitoroida sekä turvata pääsyn järjestelmiinsä. Pilvipalvelun käyttöönotto tuo useita muutoksia perinteisiin hallintajärjestelmiin ja käytäntöihin, jotka liittyvät identiteetin- ja pääsynhallintaan. Tämän seurauksena identiteetin- ja pääsynhallinnan ongelmat muodostuvat merkittävämmiksi, kuin perinteisessä ympäristössä. Pilviympäristössä sekä asiakkaan, että palveluntarjoajan tulee hallita identiteetin- ja pääsynhallintaa vaarantamatta turvallisuutta. Tietoturvapoikkeamia voi syntyä esimerkiksi puutteellisesta pääsytietojen suojaamisesta, identiteetin- ja pääsynhallintajärjestelmien skaalautuvuuden puutteesta, kaksivaiheisen tunnistautumisen puutteesta tai heikoista salasanoista. (Cloud Security Alliance 2019, 16)

3.5 Tilin kaappaus

Tilin kaappaus on uhka, jossa hyökkääjä saa haltuunsa käyttäjätilin, jolla on laajat käyttöoikeudet. Pilvipalveluissa tällainen tili on esimerkiksi tili, jolla on järjestelmänvalvojan oikeudet pilvipalvelun hallintaan. Tilin kaappaus voi tapahtua esimerkiksi tietojenkalastelu-hyökkäykselle altistumisen johdosta. Koska pilvipalveluihin voidaan päästä käsiksi mistä tahansa ja miltä laitteelta tahansa internetin ylitse, voi hyökkääjä kaappaamillaan tunnuksilla mahdollisesti hallita yrityksen järjestelmiä. Yrityksen tulisikin pitää tilin kaappauksia todellisena uhkana ja lisätä henkilöstön tietoisuutta tällaisia hyökkäyksiä vastaan. Myös yrityksen identiteetin -ja pääsynhallintajärjestelmien tulisi olla kunnossa, jotta tämän tyyppisiä hyökkäyksiä ei tapahtuisi. Tilin kaappauksen tapahtuessa kaikki tilin sisältämät tiedot, palvelut ja sen hallinta ovat vaarassa. (Cloud Security Alliance 2019, 20)

4 Pilven tietoturvan parantaminen

Pilvipalveluiden tietoturva perustuu pitkälti luottamukseen asiakkaan ja palveluntarjoajan välillä. Asiakkaan tuleekin siis aina ensimmäiseksi perehtyä huolellisesti palveluntarjoajan taustoihin ja turvallisuuskäytäntöihin ennen palvelun käyttöönottoa. (Papolu 2018) Pilvipalvelun tietoturvan vastuualueet voidaan useimmissa tapauksissa jakaa palveluntarjoajan ja asiakkaan vastuulle kuuluviin osuuksiin kuvan 2 mukaisesti (Kyberturvallisuuskeskus 2020). Pilvipalvelun tietoturvakokonaisuus ei siis muodostu vain palveluntarjoajan tietoturvallisuuskäytännöistä, vaan asiakkaalla on myös itsellään, palvelumallin mukaan, vastuu pilven tekemisessä turvalliseksi.

Tässä kappaleessa käsitellään seikkoja, joilla pilvestä voidaan tehdä tietoturvallisempi ja läpinäkyvämpi yrityksen suuntaan.

4.1 Sopimukset

Pilvipalveluiden tietoturvan toteuttamisessa sopimukset näyttelevät todella isoa osaa. Niiden avulla voidaan varautua esimerkiksi erilaisiin uhkatilanteisiin. Yrityksen ja palveluntarjoajan kannattaakin tehdä kirjalliset sopimukset monista eri asioista, kuten tietojen sijainnista, tiedon käsittelyoikeuksista, turvallisuusvaatimuksista, jatkuvuuden varmistamisesta sekä henkilötiedoista.

Tiedon sijainnista tulisi varmistua sopimuksen avulla, koska sillä on usein iso merkitys lainsäädännön kannalta. Jos palveluntarjoajan palvelinten sijainti on muualla, kuin yrityksen kotimaassa, niin silloin palveluun ja tiedon käsittelyyn voi kohdistua sijaintimaan lainsäädännön asettamia vaatimuksia, joita todennäköisesti hyödynnettäisiin esimerkiksi riitatilanteissa. Mikäli palveluntarjoajan palvelimet sijaitsevat muualla kuin yrityksen kotimaassa, niin yrityksen kannalta tässä tilanteessa on helpointa luoda sopimus, jossa määritellään, että sovellettavaksi lainsäädännöksi asetetaan oman maan kansallinen lainsäädäntö. Myös toimivaltainen tuomioistuin tulisi riitatilanteiden varalta määritellä sopimuksessa. (Kyberturvallisuuskeskus)

Tiedon käsittelyoikeuksista kannattaa varmistua sopimuksella, sillä sen avulla voidaan varmistua siitä, että tietoon pääsevät käsiksi vain siihen valtuutetut henkilöt. Tiedon käyttöoikeudet voidaan tällaisella sopimuksella pitää vain yrityksellä tai esimerkiksi yrityksellä ja palveluntarjoajan puolelta siihen valtuutetuilla henkilöillä. (Kyberturvallisuuskeskus) Tämän sopimuksen avulla voidaan siis varmistua siitä, että tietoon ei kosketa ilman lupaa.

Turvallisuusvaatimukset kannattaa myös varmistaa sopimuksen avulla. Tässä sopimuksessa määritellään turvallisuusvaatimuksia ja tietoturvakäytäntöjä, joita palveluntarjoaja sitoutuu noudattamaan yrityksen tietojen käsittelyssä. (Kyberturvallisuuskeskus)

Jatkuvuuden varmistamisesta sekä palveluntarjoajaa koskevista häiriöistä ja uhkatilanteista tulisi myös luoda sopimus. Tällaisia poikkeustilanteita varten kannattaa tehdä sopimus, jotta varmistutaan siitä, että yrityksellä on jatkuvasti pääsy tietoihinsa palveluntarjoajan toiminnan katkeamisesta huolimatta. Sopimuksessa on tärkeää määritellä myös tietojen siirrettävyys tai niiden tuhoaminen sellaisessa tilanteessa, jossa palveluntarjoajan toiminta lakkaa kokonaan. (Kyberturvallisuuskeskus)

Tämän tyyppisten sopimusten avulla yritys pystyy varmistumaan siitä, miten ja missä heidän tietojaan säilytetään ja käsitellään. Muiden sopimusten lisäksi yrityksen kannattaa vielä määritellä erillinen palvelutasosopimus, jossa määritellään tietyt vaatimustasot palveluntarjoajalle. Jos näitä vaatimustasoja ei täytetä, niin palveluntarjoajalle seuraa sanktioita.

4.2 Identiteetin- ja pääsynhallinta

Kuten aikaisemmassa riskiosiossa mainittiin, puutteellinen identiteetin- ja pääsynhallinta muodostavat pilviympäristössä ison uhkan yritykselle. Aikaisemmin käsiteltiin identiteetin- ja pääsynhallinnan muodostamia uhkia, joten seuraavassa kappaleessa käsitellään keinoja, joilla identiteetin- ja pääsynhallinnasta voidaan tehdä turvallisempi.

4.2.1 Vähimpien käyttöoikeuksien periaate

Vähimpien käyttöoikeuksien periaatteella tarkoitetaan, että millä tahansa laiteella, prosessilla tai käyttäjällä tulisi olla pienimmät mahdolliset käyttöoikeudet tehtävän suorittamiseen. Käytännössä tällä siis tarkoitetaan sitä, että esimerkiksi ohjelmoija ei tarvitse oikeuksia yrityksen taloustietoihin tai normaali käyttäjä järjestelmänvalvojan oikeuksia, eli korkeimpia mahdollisia oikeuksia. Vähimpien käyttöoikeuksien periaatteen noudattaminen vähentää huomattavasti riskiä, että hyökkääjät saisivat haltuunsa yrityksen kriittisiä järjestelmiä tai sensitiivistä dataa vain käyttämällä hyväksi niin sanottuja normaaleja alhaisen tason käyttäjätilejä. (Lord 2018)

Vähimpien käyttöoikeuksien periaatteella voidaan myös estää mahdollisen viruksen leviäminen suoraan ympäri yritystä, sillä jos yhden työntekijän tunnukset ovat joutuneet vääriin käsiin, on hyökkääjällä tällöin käyttöoikeus vain tämän työntekijän käyttämiin järjestelmiin

tai järjestelmän osaan. Jos työntekijällä olisi käyttäjätili, jolla on järjestelmänvalvojan oikeudet, niin virus voisi levitä suoraan yrityksen kaikkiin järjestelmiin. Myöskin käyttäjillä, joilla on järjestelmänvalvojan oikeudet, tulisi olla alempien oikeuksien käyttäjätili, jota käytetään aina silloin kuin järjestelmänvalvojan oikeudet eivät ole välttämättömyys. (Lord 2018)

4.2.2 Single Sign-On & Kaksivaiheinen tunnistautuminen

Single Sign-On (SSO) on käyttäjän todennusjärjestelmä, joka mahdollistaa kirjautumisen moneen eri palveluun yksillä ja samoilla tunnuksilla, jotka ovat yleensä yrityksen domain-tunnukset. Käyttäjällä on siis mahdollisuus käyttää monia eri palveluita vain yhdellä kirjautumisella, eikä kaikkiin palveluihin tarvitse kirjautua erikseen. Pilvipalveluiden aikakaudella, kun monilla yrityksillä on käytössään lukuisia eri palveluita ja järjestelmiä, joihin kaikkiin tarvittaisiin normaalisti eri tunnukset, SSO on erittäin houkutteleva vaihtoehto. (Drinkwater 2018)

Oikein implementoituna SSO on hyväksi tuottavuudelle, IT-monitoroinnille sekä hallinnalle ja turvallisuuskontrolloinnille. Yrityksen IT-ylläpitäjät voivat SSO:n avulla helposti antaa tai poistaa käyttäjän käyttöoikeuksia eri palveluihin ja järjestelmiin. SSO:n avulla myös vähennetään heikkojen, unohdettujen ja hävinneiden salasanojen riskiä. Centrifyn teknologiajohtaja Barry Scottin mukaan isoin syy tietoturvamurtoihin on vääriin käsiin joutuneet tunnukset. Scott sanoo, että mitä enemmän tunnuksia käyttäjillä on käsiteltävinään, niin sitä huonommaksi heidän salasanansa menevät ja samoja salasanoja aletaan käyttämään monissa eri palveluissa. Tämä siis ajaa siihen, että tunnukset on helppo kaapata huonojen salasanojen vuoksi. SSO:n käyttöönotolla yritys voi välttää tämän ja käyttäjät voivat luoda itselleen yhden, erittäin vahvan salasanan. (Drinkwater 2018)

Forresterin tekemän tutkimuksen mukaan yritykset maksavat keskimäärin jopa 70 dollaria yhtä resetoitua salasanaa kohden, koska salasanan resetoimisesta aiheutuu IT-tuelle turhaa työtä ja työntekijälle menetettyä työaikaa (Lu 2019). SSO:n avulla salasanojen resetoiminen vähentyy huomattavasti, kun työntekijöillä on vain yksi salasana muistettavanaan.

Koska SSO:n myötä käyttäjillä on käytössään vain yksi tunnuspari moneen eri palveluun, niin yrityksen tulisi ehdottomasti ottaa käyttöön myös kaksivaiheinen tunnistautuminen, jotta SSO:sta saataisiin mahdollisimman turvallinen. Kaksivaiheinen tunnistautuminen tarkoittaa tunnistautumismenetelmää, jossa käyttäjän täytyy normaalin tunnusparin lisäksi todentaa itsensä jollakin muulla tavalla. Kaksivaiheisena tunnistautumisena voi toimia jo-

kin, mitä käyttäjällä on, jokin, mitä hän on tai jokin, missä hän on. Käyttäjä voi siis tunnistaa itsensä esimerkiksi matkapuhelimen avulla tai biometrisillä tunnisteilla. Sijaintitietoon perustuvaa tunnistautumista käytetään harvoin, mutta sekin on mahdollista. Käytetyin menetelmä kaksivaiheiseen tunnistautumiseen on matkapuhelimen avulla tunnistautuminen. Tämä toimii siten, että kun käyttäjä on kirjautumassa johonkin palveluun, niin käyttäjätunnusten syöttämisen jälkeen palvelu lähettää hänen matkapuhelimeensa tekstiviestin, joka sisältää numeerisen koodin, jota palvelu kysyy. Ilman tätä koodia käyttäjä ei siis pääse kirjautumaan palveluun. (Fruhlinger 2019)

Jotkin sivustot ja palvelut tarjoavat myös mobiilisovelluksiin perustuvaa kaksivaiheista tunnistautumista, jossa käyttäjän tunnistekoodit ovat koko ajan sovelluksessa ja ne vaihtuvat tietyin väliajoin. Tämä tunnistautumistapa on tekstiviestitunnistautumista turvallisempi, koska osaavat hakkerit kykenevät varastamaan käyttäjän tunnistekoodin tekstiviestiliikenteen välistä. (Murphy 2018)

Kaksivaiheinen tunnistautuminen estää siis tehokkaasti tunnusten joutumista vääriin käsiin ja yrityksen tietojen vaarantumista. Vaikka hyökkääjä olisikin jollain tavalla saanut käyttäjän tunnukset haltuunsa, niin hän ei pelkästään niiden avulla pääse kirjautumaan yrityksen palveluihin vaan hän tarvitsisi lisäksi käyttäjän matkapuhelimen, jossa on koodi kaksivaiheiseen tunnistautumiseen.

4.3 Sertifikaatit & arviointikriteeristöt

Palveluntarjoajille on olemassa erilaisia sertifikaatteja, joiden avulla he pystyvät osoittamaan luotettavuuttaan. Palveluntarjoaja voi esimerkiksi hankkia itselleen ISO 27001 sertifioinnin, joka osoittaa asiakkaille, että palveluntarjoaja haluaa noudattaa kansainvälisesti hyväksyttyjä tietosuoja- ja tietoturvastandardeja. Sertifioinnin avulla voidaan siis markkinoida omaa halukkuutta noudattaa näitä standardeja sekä säännöksiä ja se luokin usein maailmanlaajuisia liiketoimintamahdollisuuksia, sillä sertifioinnit ovat yhä yleisempiä vaatimuksia sopimuksia allekirjoitettaessa. (IT Governance 2020)

Palveluntarjoaja voi myös hankkia työntekijöilleen erilaisia sertifiointeja, joiden avulla pystytään todistamaan myös työntekijöiden osaamista sekä luomaan luotettava kuva yrityksestä asiakkaille. Erilaisten sertifiointien avulla palveluntarjoaja voi siis erottua muiden kilpailijoiden joukosta, koska heillä on jotain mikä konkreettisesti todistaa yrityksen ja sen työntekijöiden osaamista sekä luotettavuutta. (Hoelscher 2018)

Pilvipalveluiden turvallisuuden arviointiin on olemassa myös arviointikriteeristöjä, joiden avulla yritys pystyy helposti arvioimaan täyttääkö pilvipalvelu kriteeristön kriteerit ja yrityksen tarpeet. Yksi näistä arviointikriteeristöistä on Pitukri, joka tarkoittaa Kyberturvallisuuskeskuksen julkaisemaa pilvipalveluiden turvallisuuden arviointikriteeristöä ja se on tarkoitettu parantamaan pilvipalveluissa käsiteltävän tiedon turvallisuutta. Pitukri on suunniteltu käytettäväksi viranomaispalveluiden arvioinnissa, mutta sitä voidaan hyödyntää myös muiden organisaatioiden pilvipalveluiden arvioinnissa. Pitukria hyödyntämällä saadaan parempi kuva hankkeilla olevan tai jo olemassa olevan pilvipalvelun tietoturvallisuudesta. (Kyberturvallisuuskeskus 2019b)

Pitukrin laadinnassa on hyödynnetty erityisesti BSI:n, eli Saksan liittovaltion tietoturvaviraston pilviturvallisuuskriteeristöä, CSA:n suojausmatriisia, ISO 27001 ja 27017 standardeja sekä Katakri-kriteeristöä, eli viranomaisten auditointityökalua (Kyberturvallisuuskeskus 2020).

4.4 Zero Trust-malli

Zero Trust on tietoturvamalli, joka poistaa ajatuksen luottamuksesta verkkojen, ohjelmien ja datan suojaamisessa. Tässä mallissa kaikkia käyttäjiä ja laitteita pidetään epäluotettavina, ennen kuin ne todetaan luotettaviksi, jopa yrityksen sisäisiä käyttäjiä. Zero Trust toimii siis ”älä luota kehenkään, varmista aina” -periaatteella. Tätä ajatusta noudatetaan kaikkien käyttäjien, laitteiden, ohjelmien ja pakettien kohdalla riippumatta siitä mitä ne ovat tai missä ne ovat. (Kindervag & Staten 2018) Zero Trust siis poistaa luottamuksen elementit yrityksen siirtyessä pilvipalveluun. Koska luottamus on todella isossa roolissa pilvipalveluissa, niin Zero Trust on erittäin hyvä tietoturvamalli varsinkin pilvipalveluita käyttävälle yritykselle.

Zero Trust-mallin periaatteita ovat nimenomainen tarkistaminen, vähimpien oikeuksien käyttäminen, tarkka liikenteen monitorointi sekä tietomurtojen hallinta. Nimenomainen tarkistaminen tarkoittaa, että kaikki tulee aina todentaa ja hyväksyä kaikkien arvopisteiden mukaan. Arvopisteitä voivat olla esimerkiksi käyttäjätiedot, sijainti, laitteen kunto, kuormitus, ja tietojen luokitus. Vähimpien oikeuksien käyttäminen tarkoittaa käyttöoikeuksien rajoittamista siten, että käyttäjällä on pääsy vain välttämättömiin tietoihin ja resursseihin, joita hän tarvitsee. Liikennettä tulee myös Zero Trust-mallissa monitoroida jatkuvasti, jotta hyökkääjillä ei olisi helppoa pääsyä yrityksen verkkoon. (Microsoft)

Yrityksen siirtyessä Zero Trust-malliin heidän tulisi ensin selvittää minkälaisia ohjelmia ja dataa yrityksillä on, missä ne ovat, ketkä niitä käyttävät ja keillä on käyttöoikeus niihin. Tä-

män jälkeen tulisi tunnistaa yritykselle kriittisimmät tiedot, ohjelmat ja palvelut liiketoiminnan kannalta, jotta niitä osataan suojata paremmin. Kun nämä vaiheet on tehty, niin yrityksen tulisi kartoittaa kuinka yrityksen käyttämät ohjelmat toimivat. (Paloalto Networks)

5 Microsoft Azuren tietoturvallisuus

Azure on Microsoftin vuonna 2010 julkaisema julkinen IaaS-pilvipalvelu, joka mahdollistaa yrityksille infrastruktuurin pyörittämisen pilvessä. Se toimii *maksa siitä mitä käytät* -periaatteella, minkä johdosta se on usein yrityksille erittäin kustannustehokas ratkaisu. Azure mahdollistaa yrityksille satojen eri palveluiden käytön yhdellä alustalla. Azuressa voidaan pyörittää esimerkiksi yrityksen tietokantoja, tallennustiloja ja verkkosivuja. Azure tarjoaa yrityksille myös monia palveluja, kuten esimerkiksi Azure Active Directorya, joka toimii samalla tavalla kuin normaali Active Directory, mutta pilvessä. (Hoffman 2018)

Microsoft käyttää vuosittain miljardi dollaria tietoturvansa parantamiseen, joista suurin osa budjetoidaan uusiin innovaatioihin. Azuren hallituksen tietoturvajohtajan, Matthew Rathbunin mukaan pilveen siirtyminen on käännekohta, jossa täytyy muuttaa ajattelumallia kyberturvallisuudesta. Hän kertoo myös, että 90% hänen näkemästään uhkamaisemasta alkaa ihmiselementillä, eli ihmisen tekemällä virheellä, joka jotenkin vaarantaa turvallisuuden. Rathbunin mukaan ihanteellisessa tilanteessa päädytäänkin maailmaan, jossa ihmiset eivät ole ollenkaan tekemisissä Azuren tuotantoympäristön kanssa. (Patterson 2018)

Microsoftin pelkkään tietoturvaan vuosittain käyttämä rahamäärä on siis todella vakuuttava ja antaa sellaisen kuvan, että yritys välittää asiakkaidensa tietoturvasta ja haluaa kehittää sitä jatkuvasti. Suurimmalla osalla Azurea käyttävistä asiakkaista tuskin on itsellään laittaa näin paljoa rahaa tietoturvaan ja sen kehittämiseen. Tämä saa siis Azuren näyttämään erittäin houkuttelevalta vaihtoehdolta yritykselle myös tietoturvan saralta.

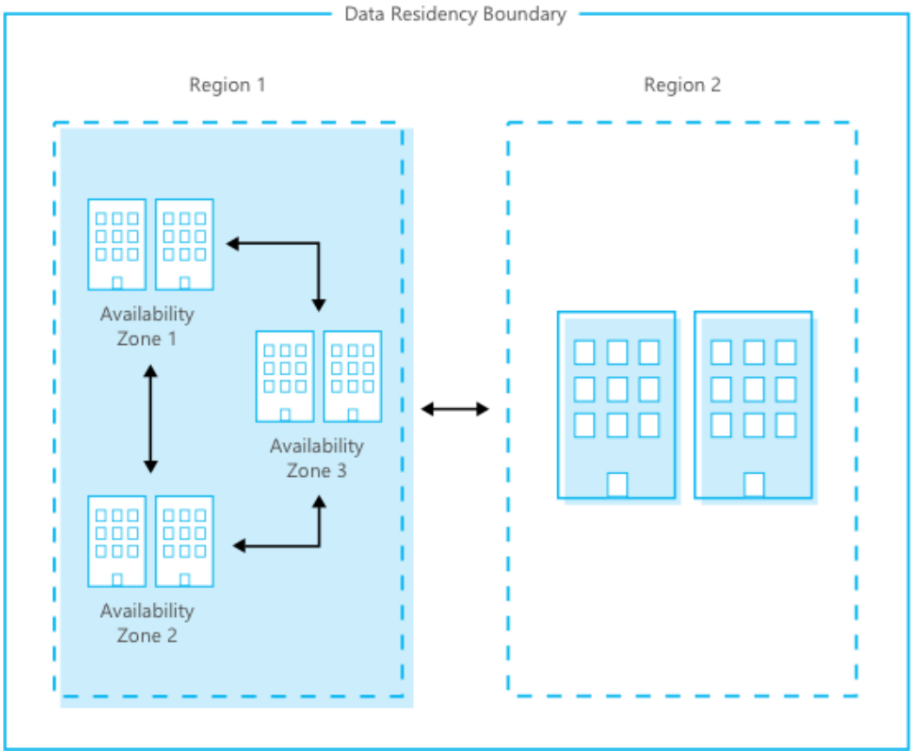
Tässä kappaleessa tutkitaan Microsoft Azuren infrastruktuurin tietoturvan tasoa sekä tietoturvakäytäntöjä. Tutkimus tapahtuu läpi käymällä läpi Microsoftin dokumentaatiota Azuren tietoturvakäytännöistä. Tutkimuksessa paneudutaan nimenomaan siihen, kuinka turvallinen Azure on valmiina IaaS-alustana, eli miten sen infrastruktuurin tietoturvaa hoidetaan ja mitä sen eteen on tehty. Tutkimuksessa ei siis tuoda esille tarkkoja tapoja, joilla käyttäjä voi itse tehdä Azuresta tietoturvallisemman, mutta käsitellään kuitenkin muutamia tärkeimpiä mahdollisuuksia, joita Microsoft käyttäjilleen antaa.

5.1 Datakeskukset ja niiden turvallisuus

Azure koostuu globaalisti hajautetuista datakeskuksista, joita sijaitsee 52:lla eri alueella. Nämä alueet on jaettu maantieteellisesti ja tämän avulla varmistetaan datan sijainti, suvereniteetti ja se, että alueen lainsäädäntöä ja vaatimuksia noudatetaan datan käsittelyssä. Tämän avulla mahdollistetaan Azuren käyttö myös niille asiakkaille, joilla on tiedon sijaintiin ja sen säilyttämiseen liittyviä tarkkoja määräyksiä. Nämä maantieteelliset sijainnit ovat

sietokykyisiä kestämään kokonaisia alueellisia vikoja, sillä vian sattuessa datakeskus yhdistetään sille tarkoitettuun erilliseen suuren kapasiteetin verkkoinfrastruktuuriin. (Baldwin & Kess 2019a)

Alueiden sisällä datakeskukset jaetaan moniin eri sijainteihin, joita kutsutaan saatavuusalueiksi. Jokainen saatavuusalue koostuu yhdestä tai useammasta datakeskuksesta, jotka ovat kaikki varustettu itsenäisillä virtalähteillä, jäähdytyksellä ja verkolla. Näiden saatavuusalueiden avulla pystytään pitämään tietojen saatavuus korkeana ja mahdollistetaan pieniviiveinen tietojen replikaatio. Näin ollen yritys voi siis ajaa Azuressa liiketoiminnalle kriittisiäkin ohjelmia. (Baldwin & Kess 2019a) Kuvassa 4. havainnollistetaan näiden datakeskusten ja alueiden hajautusta ja yhdistämistä toisiinsa.



Kuva 4. Azuren datakeskukset ja alueet jaetaan ja yhdistetään toisiinsa kuvan mukaisesti (Baldwin & Kess 2019a)

Microsoft suunnittelee, rakentaa ja operoi datakeskuksia tavoilla, jotka mahdollistavat niiden tiukan valvonnan ja kontrolloinnin. Microsoft käyttää kerroksellista lähestymistapaa suojatessaan datakeskuksien fyysistä turvallisuutta. Kun Microsoftin datakeskuksessa halutaan vierailla, päästäkseen itse palvelimiin käsiksi tulee vierailijan käydä läpi viisivaiheinen turvallisuusselvitys. Ensimmäiseksi vierailijan tulee etukäteen kysyä pääsyä datakeskukseen ja kertoa hyvä syy, miksi hänen tulisi päästä sisään. Hyväksyttävä syy päästä sisään datakeskukseen voi olla esimerkiksi auditointi. Tämän jälkeen hakemus joko hyväk-

sytään tai hylätään Microsoftin työntekijöiden toimesta. Jos hakemus hyväksytään, on vierailijalla pääsy vain tiettyyn, häntä koskevaan alueeseen datakeskuksessa ja tietyksi aikaa. Vierailijan saapuessa datakeskukselle, hänen tulee mennä sisään tarkoin vartioidusta ovesta, jota valvotaan kameroin. Datakeskusta ympäröivät myös korkeat raudasta tehdyt aidat. Datakeskuksen sisääntuloaula on täynnä vartijoita, jotka on tarkkaan valittu tehtävään ja heille on teetetty turvallisuusselvitykset. Vierailijan tullessa sisään hänen tulee tunnistautua kaksivaiheisella tunnistuksella sisään päästäkseen. Kaksivaiheisena tunnistautumisena toimii Microsoftilla biometrinen tunniste, eli esimerkiksi sormenjälki. Tämän jälkeen on vuorossa Datakeskustasolle saapuminen, jossa vierailijaa odottaa koko vartalon tarkistus metalliesineiden varalta. Tämä tehdään, jotta pystytään varmistumaan siitä, että mitään luvatonta dataa ei tuoda datakeskukseen tai poistu sieltä. Vierailijan lähtiessä hänen tulee kävellä uudelleen metallintunnistimen läpi. (Baldwin & Kess 2019a)

Microsoft arvioi datakeskustensa fyysistä turvallisuutta määräajoin, jotta se vastaa Azuren turvallisuusvaatimuksia. Datakeskuksessa työskentelevällä henkilöstöllä ei ole pääsyä Azure-järjestelmiin, eikä heillä ole fyysistä pääsyä Azure-huoneisiin. Koko Azuren infrastruktuuri suunnitellaan siten, että se vastaa kansainvälisiä ja monia aloja koskevia vaatimuksia, standardeja ja säännöksiä, kuten ISO 27001, HIPAA, FedRAMP ja SOC. (Baldwin & Kess 2019a)

5.2 Azuren tietokanta

Suojellakseen asiakasdataa ja tarjotakseen vahvoja turvallisuusominaisuuksia, Azuren tietokannalla on omat turvallisuuskyvykkyytensä. Azuren tietokanta tukee ainoastaan TDS protokollaa, joka vaatii, että tietokantaan voidaan käyttää vain oletusportin, eli TCP/1433:n ylitse. Azuren tietokanta sisältää myös oman palomuurin, joka estää oletuksena kaiken liikenteen tietokantaan. Tietokannan yhdyskäytävässä on myös palvelunestohyökkäyksiltä suojaava DosGuard, joka seuraa aktiivisesti hylättyjä kirjautumisia IP-osoitteista ja osaa tällä tavoin estää kirjautumisyrityksiä, mikäli ne tulevat jatkuvasti samasta IP-osoitteesta. (Lanfear 2020)

5.3 Azuren tuotantoympäristön hallinta, operointi ja monitorointi

Azuren parissa työskentelee jopa 3500 Microsoftin omaa tietoturva-asiantuntijaa, jotka pitävät huolen asiakkaidensa tietoturvasta monitoroimalla ympäri vuoden 24/7 Azurea kohtaavia uhkia. Microsoft käyttää toiminnassaan myös niin sanottuja blue- ja red team harjoitteita, joiden avulla järjestelmistä pystytään löytämään mahdollisia haavoittuvuuksia. Punainen tiimi yrittää hyökätä järjestelmään, kuten oikeat hakkerit ja sininen tiimi yrittää

puolestaan puolustaa hyökkäyksiä. Jokaisen harjoituksen jälkeen tiimit käyvät läpi, mitä he ovat oppineet ja löydökset kootaan yhteen. (Ben-Menahem, 2018)

Azuren tuotantoympäristöä hallitaan, operoidaan ja monitoroidaan monien eri järjestelmien ja ohjelmien monitorointityökalujen avulla. Jos ympäristössä havaitaan tietoturvapoikkeama, niin reagointiprosessi aloitetaan heti ja Azuren niin sanottu incident response-tiimi alkaa töihin ongelman ratkaisemiseksi. (Baldwin & Kess 2019b)

Azuren järjestelmäympäristö koostuu kahdesta verkosta, jotka ovat Azuren tuotantoympäristö, eli Azure network ja Microsoftin corporate network, eli corpnet. Corpnetiä käyttävät Azuren tukihenkilöt ja se tukee Microsoftin sisäisä toimintoja sekä sisältää pääsyn sisäisiin sovelluksiin, joita käytetään Azuren asiakastukeen. Corpnet on sekä fyysisesti että loogisesti erotettu Azuren tuotantoverkosta ja Azuren tukihenkilöt pääsevät käsiksi siihen Azuren työasemia käyttäen. (Baldwin & Kess 2019b)

Palvelinten käyttöjärjestelmille, tietokannoille ja verkkolaitteille suoritetaan haavoittuvuusskannauksia vähintään neljä kertaa vuodessa. Näitä skannauksia suoritetaan puolueettoman toimijan toimesta, jotta voidaan aidosti varmistua järjestelmien turvallisuudesta. Azuren järjestelmiä myös päivitetään jatkuvasti sisäänrakennetun käyttöönottojärjestelmän kautta, jotta järjestelmät pystytään suojaamaan mahdollisimman hyvin tunnetuilta haavoittuvuuksilta. Azure hyödyntää myös Microsoft Security Response Centerin resursseja tietoturvapoikkeamien havainnoinnissa. (Baldwin 2019)

Azure myös arvioi ja päivittää laitteistojen, ohjelmistojen ja verkkolaitteiden konfiguraatioasetuksia vuosittain. Muutoksia kehitetään, testataan ja hyväksytään kehitysympäristössä ennen kuin ne ajetaan Azuren tuotantoympäristöön. (Baldwin 2019)

5.4 Asiakastietojen suojaus

Microsoft tarjoaa asiakkailleen vahvan datan suojan oletusarvoisesti sekä myös vaihtoehtoisesti asiakkaan toimesta. Asiakkaiden dataa suojellaan esimerkiksi datan segregaatiolla, eli erottelulla ja datan salauksella. Microsoft ei luonnollisesti monitoroi tai tarkkaile asiakkaan dataa, eikä tiedä millaista dataa asiakas Azureen tallentaa. Microsoftin operaatio- ja tukihenkilöillä ei myöskään ole oletusarvoisesti pääsyä asiakasdataan. Jos nämä henkilöt tarvitsevat pääsyä dataan, niin hyväksytys tapahtuu aina johdon toimesta. Dataan pääsyä hallitaan tarkasti ja käynnit merkitään lokikirjaan sekä henkilöille myönnetään aina mahdollisimman pienet oikeudet tehtävän suorittamiseen. Asiakkaiden virtuaalikoneilla ei myöskään ole Microsoftin omia normaaleja- tai järjestelmänvalvojakäyttäjiä. (Sherer, Baldwin & Kess 2020)

Datan erottelu on tärkeää, sillä Azure on usean asiakkaan palvelu ja monien asiakkaiden dataa säilötään samoilla fyysisillä laitteilla. Azure käyttää loogista eristystä erottaakseen asiakkaiden datat toisistaan. Erottelu tarjoaa siis usean asiakkaan palvelun laajuuden ja taloudelliset hyödyt, samalla estäen asiakkaita pääsemästä käsiksi toistensa dataan. (Sherer ym. 2020)

Azure tarjoaa asiakkailleen laajan skaalan erilaisia datan salausmahdollisuuksia, antaen asiakkaalleen joustavuuden valita ratkaisun, joka tukee parhaiten yrityksen tarpeita. Asiakasyritys on siis itse vastuussa siitä, että datan salaus Azuressa hoidetaan yrityksen käytäntöjen mukaisesti. Azuressa on Key Vault-niminen sovellus, jonka avulla asiakasyritys voi helposti kontrolloida avaimia, joita käytetään salaamaan dataa. Asiakas voi myös ottaa salauksen käyttöön omien virtuaalikoneidensa sekä loppukäyttäjien koneiden välillä. Sisään- tai ulosmenevä liikenne voidaan siis salata. Azure käyttää tähän TLS 1.2 tai uudempaa protokollaa 2048-bittisillä RSA/SHA256 salausavaimilla CESG/NCSC:n (National Cyber Security Centre) suositusten mukaisesti. (Sherer ym. 2020)

Microsoftin mukaan salauksien käyttöönotto on tehty asiakkaille erittäin helpoksi, mutta se jää kuitenkin asiakkaan vastuulle. Tässä tulee hyvin esiin pilvipalvelun jaettu vastuumalli. Asiakkaan tulee aina ymmärtää, mikä on heidän vastuullaan ja mikä palveluntarjoajan vastuulla, jotta tämän kaltaiset asiat saadaan hoidettua asianmukaisesti.

Microsoft auttaa myös asiakkaitaan varmistamaan, että data on turvassa kyberhyökkäyksien varalta tai fyysisten datakeskusta koskevien vaurioiden varalta. Tämä tarkoittaa siis käytännössä datan replikointia toiseen paikkaan. Asiakkaalla on mahdollisuus valita kolmesta eri replikointivaihtoehdosta, jotka ovat paikallisesti talletettu varastointi, alueellisesti talletettu varastointi sekä maantieteellisesti talletettu varastointi. (Sherer ym. 2020)

Paikallisesti tallennetussa varastoinnissa ylläpidetään kolmea kopiota asiakkaan datasta. Se on replikoitu kolme kertaa yhdessä datakeskuksessa, yhdellä alueella. Kaikki tieto on siis samassa paikassa, mutta ei yhdellä laitteella. Tämä siis suojelee asiakkaan dataa normaaleilta laitteistovioilta, mutta ei esimerkiksi koko datakeskuksen vioilta. (Sherer ym. 2020)

Alueellisesti tallennetussa varastoinnissa tallennetaan myöskin kolme kopiota asiakkaan datasta, mutta ne ovat jaettu kahden tai kolmen eri datakeskuksen kanssa, joten data on paremmin turvassa mahdollisilta datakeskusvaurioilta. Datan replikointi tapahtuu yhden tai mahdollisesti kahden eri alueen välillä. (Sherer ym. 2020)

Maantieteellisesti tallennettu varastointi on oletusarvoisesti käytössä asiakkaan ottaessa käyttöön Azuren tallennustilan. Tämä replikointimuoto mahdollistaa sen, että asiakkaan datasta tehdään kuusi kopiota ja se replikoidaan kolme kertaa ensisijaisesti valitun alueen sisällä. Tämän lisäksi data replikoidaan kolmesti toissijaisen alueen sisällä, joka sijaitsee satojen kilometrien päässä ensisijaisesti alueesta. Tämä replikointimuoto suojelee asiakkaan dataa parhaimmalla mahdollisella tavalla. Vaikka asiakkaan käyttämä ensisijainen alue tuhoutuisi tai vioittuisi kokonaan, olisi data silti saatavilla toissijaiselta alueelta. (Sherer ym. 2020)

5.5 Azuren saatavuus & luottamuksellisuus

Microsoft lupaa palvelulleen korkean saatavuuden, luotettavuuden, tehokkuuden sekä skaalautuvuuden, jotka saavutetaan virtualisointiteknologian avulla saatavalla laajalla redundanssilla. Microsoftin datakeskuksissa on katkeamattomia virtalähteitä, joilla varmistetaan jatkuva sähkönsyöttö lyhyiden virtakatkosten varalta. Tämän lisäksi datakeskuksissa on myös generaattoreita, jotka tuottavat sähköä pidempien katkosten tai huoltokatkojen varalle. Datakeskuksissa on myös polttoaineella toimivia generaattoreita, joita käytetään luonnonkatastrofin sattuessa. Microsoft monitoroi Azuren tuotantoympäristöä vuoden jokaisena päivänä 24/7 hätätilanteiden ja katkoksien varalta. Asiakkaan pääsy Azuren tietokantaan varmistetaan yhdyskäytävän kautta, jossa tietokanta on jatkuvasti saatavilla. Aktiivisten tietokantojen terveyttä ja tilaa monitoroidaan myös viiden minuutin välein tehtävillä tarkastuksilla. (Baldwin & Kess 2019c)

Kuten aiemmin kerrottiin, Azuressa asiakkaan tiedot myös replikoidaan moneen eri paikkaan ja katastrofin sattuessa tiedot saadaan palautettua toisesta sijainnista, tai liikenne kiertämään toisen sijainnin kautta. Tällä tavalla palvelu saadaan pidettyä jatkuvasti saatavilla.

Microsoftin lupauksista huolimatta Azuressa on ollut muutamia merkittäviä käyttökatkoksia, joista viimeisin on tapahtunut toukokuussa 2019. Azure koki vuosina 2018-2019 kolme isompaa käyttökatkosta, joista kaksi johtui jäähdytysjärjestelmän ongelmista ja yksi DNS-migraation ongelmista. (Fadilpašić 2018; Krazit 2018; Pietschmann 2019) Vuoden 2018 syyskuussa tapahtuneessa katkoksessa jotkin Azuren palvelut olivat alhaalla jopa yli 24 tuntia ennen kuin ne saatiin palautettua toimintaan (Krazit 2018). Näistä katkoksista huolimatta Azuren ydinpalvelut olivat kuitenkin ylhäällä 99,995 % heinäkuun 2018 ja heinäkuun 2019 välillä. (Evans 2019)

Microsoft joutui ison tietomurron kohteeksi myös joulukuussa 2019, kun sen tietokannasta onnistuttiin saamaan 250 miljoonaa asiakasrekisteriä. Tietokanta sisälsi Microsoftin asiakastuen analytiikkadataa, joka oli kuitenkin anonymisoitua. Tietojen joukossa oli esimerkiksi sähköpostiosoitteita, IP-osoitteita sekä tietoja tukitapauksista. Microsoftin mukaan suurin osa rekistereistä ei kuitenkaan sisältänyt henkilötietoja ja sen mukaan henkilökohtaiset tiedot myös poistetaan tukitapauksista automatisoiduilla työkaluilla proseduurien mukaisesti, kun ne viedään tietokantaan. Jotkin sähköpostiosoitteet olivat kuitenkin päätyneet tietokantaan siinä muodossa, että niistä pystyi lukemaan asiakkaiden nimiä. Microsoftin mukaan tämä tietomurto johtui virheellisesti konfiguroiduista Azuren turvallisuussäännöistä. (Cimpanu 2020) Tässä tapauksessa Azuren luottamuksellisuus siis vaarantui, kun tietoihin pääsivät käsiksi myös sellaiset henkilöt, joilla ei ollut siihen lupaa.

5.6 Azuren sertifikaatit ja säännösten noudattaminen

Azure omistaa laajan skaalan erilaisia sertifiointeja ja se noudattaa monia kansallisia sekä alueellisia lainsäädäntöjä ja säännöksiä, kuten GDPR:ää. Tämän ansiosta Azuren käyttö on mahdollista sellaisillekin asiakkaille, joille näiden noudattaminen on tärkeää. Azurelle on myönnetty esimerkiksi ISO 27001 sertifiointi, joka osoittaa, että Microsoft käyttää maailmanlaajuisesti tunnettuja prosesseja ja parhaita käytäntöjä infrastruktuurinsa hallintaan (Baumgartner, Borys, & Mazzoli 2020).

Muita mainitsemisen arvoisia Azurelle myönnettyjä sertifikaatteja tai todistuksia ovat CSA STAR-sertifikaatti, FedRAMP-valtuutus sekä SOC-todistukset. (Microsoft) CSA STAR (Security, Trust & Assurance Registry) -sertifikaatti on ilmainen, julkisesti saatavilla oleva rekisteri, johon pilvipalveluntarjoajat voivat julkaista CSA-arviointejaan. Azure on saanut tämän sertifikaatin, koska sillä on ISO 27001 sertifiointi ja se noudattaa CSA:n suojausmatriisissa määriteltyjä kriteereitä. (Baumgartner & Mazzoli 2020a)

FedRAMP on valtuutus, jonka avulla Yhdysvaltojen hallitukset ja virastot voivat halutessaan käyttää Azurea. Sen avulla taataan, että Azure on tarpeeksi turvallinen käytettäväksi valtiollisella tasolla. (Baumgartner & Mazzoli 2020b)

SOC (Service Organization Controls) on valvontastandardi, joka turvaa pilvessä tallennettujen ja käsiteltyjen tietojen luottamuksellisuuden ja yksityisyyden. SOC-todistusten avulla pystytään siis osoittamaan asiakkaalle, että heidän tietojaan käsitellään luottamuksellisesti ja yksityisyys säilytetään. (Baumgartner, Borys, Cole & Mazzoli 2020)

Azure on sitoutunut noudattamaan myös eri aloihin liittyviä säännöksiä, kuten HIPAA (Health Insurance Portability and Accountability Act), joka on Yhdysvaltojen terveydenhuoltolaki, jossa asetetaan vaatimukset yksilöitävissä olevien terveystietojen käytölle, julkistamiselle sekä suojaamiselle. (Baumgartner, Cole & Mazzoli 2020) Tämä siis tarkoittaa käytännössä sitä, että Yhdysvaltojen terveydenhuoltoalan organisaatiot voivat halutessaan käyttää Microsoftin ja Azuren tarjoamia palveluita toiminnassaan.

Azuren palveluvalikoimaan on tulossa Compliance Manager lisäys, joka auttaa asiakasta hallitsemaan määräysten ja säännösten noudattamista jaetun vastuumallin puitteissa. Compliance Managerin avulla asiakas voi yhdistää säännöksiä, jotka Microsoft on toimittanut auditoijille sekä säätäjille palvelustaan omaan yritykseensä sopiviksi. Palvelu on kuitenkin vasta julkisessa testausvaiheessa, joten se ei ole vielä täysin valmis. (Vukos-Walker ym. 2020)

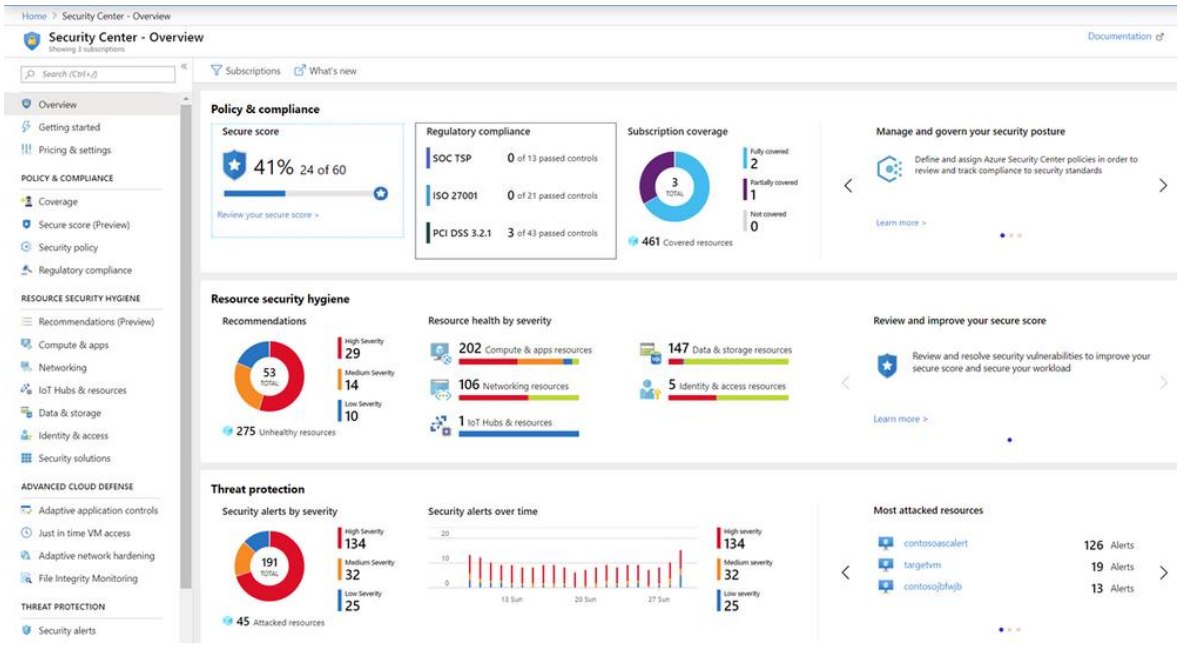
5.7 Asiakkaan määriteltävät tietoturvatoimet

Vaikka Azuren infrastruktuurin suojaus olisi muutoin kunnossa, asiakkaan täytyy silti tehdä itse lisätoimia, jotta Azuren käyttö olisi varmasti tietoturvallista. Tämän takia Azure tarjoaakin asiakkailleen paljon erilaisia suojauskeinoja, joilla pyritään varmistamaan palvelun luotettavuus, eheys ja saatavuus. Asiakas voi siis ottaa näitä palveluita itse käyttöön Azuren hallintaportaalista, eikä näiden käyttöönotto riipu Microsoftista. Tässä kappaleessa käydään läpi lyhyesti muutamia tärkeimpiä suojaustyökaluja, joita asiakas voi itse ottaa käyttöön.

5.7.1 Azure Security Center

Azure Security Center (ASC) on yhtenäinen infrastruktuurin turvallisuuden hallintajärjestelmä, joka vahvistaa datakeskusten turvallisuutta ja tarjoaa edistyksellistä suojaa tietoturvauhkia vastaan pilvessä. ASC:n avulla voidaan arvioida omaa IT-ympäristöä ja ymmärtää näin ympäristön turvallisuustilannetta. Se arvioi myös ympäristössä pyöriviä työmääriä ja antaa niiden mukaan ylläpitäjälle suosituksia tavoista, joilla voidaan ehkäistä uhkia sekä erillisiä turvallisuushälytyksiä sen havaitessa tietoturvapoikkeamia. ASC on myös natiivisti integroitu Azureen, joten sen käyttöönotto on helppoa sekä nopeaa ja se tarjoaa automaattista suojaa Azuren palveluissa. ASC on mahdollista ottaa käyttöön myös Azuren ulkopuolisissa palveluissa ja laitteissa asentamalla niihin lokianalyysiagentti, joka lähettää lokitiedot ASC:hen. Tämän avulla koko yrityksen ympäristöä voidaan siis seurata ASC:n avulla, vaikka yrityksessä olisikin myös On-premises -laitteita. (Lanfear ym. 2020)

ASC monitoroi jatkuvasti uusia laitteita ja palveluita, joita lisätään yrityksen ympäristöön ja arvioi, ovatko ne konfiguroitu oikein parhaiden käytäntöjen mukaisesti. Jos laitteita ei ole konfiguroitu oikein, niin ne liputetaan ja ylläpitäjä saa listauksen suositelluista toimenpiteistä, joita laitteille tulisi tehdä. Tämän lisäksi ylläpitäjälle annetaan ohjeita, kuinka näitä toimenpiteitä tulisi tehdä. Tämän kaltaisen monitoroinnin ansiosta ASC osaa muodostaa yrityksen ympäristöstä turvallisuuspisteytyksen, jonka avulla voidaan helposti nähdä, kuinka turvallinen ympäristö todella on. Ylläpitäjä näkee turvallisuuspisteytyksen alla suosituksia ja niiden vaikutuksia pisteytykseen. Näiden suositusten avulla ylläpitäjällä on helppo työ vähentää mahdollista hyökkäyspinta-alaa ja tehdä yrityksen ympäristöstä entistä turvallisempi. ASC:n uhkiensuojaus sisältää myös analyysityökalun, jonka avulla voidaan ymmärtää paremmin yritykseen kohdistuneen hyökkäyksen kokonaiskuvaa. Tämän työkalun avulla voidaan esimerkiksi selvittää mistä hyökkäys oli lähtöisin ja millaisia vaikutuksia sillä oli järjestelmiin. (Lanfear ym. 2020) Kuvassa 5. nähdään Azure Security Centerin hallintaportaalin päänäkymä, jossa annetaan yrityksen IT-ylläpitäjille paljon dataa yrityksen IT-ympäristöstä. Päänäkymässä voidaan nähdä esimerkiksi ympäristön turvallisuuspisteytys sekä ympäristöä koskevat turvallisuushälytykset.



Kuva 5. Azure Security Centerin hallintaportaalin päänäkymä (Elyashar 2019)

5.7.2 Azure Sentinel

Azuren Sentinel on pilvinatiivi ja skaalautuva SIEM (Security Information Event Management) ja SOAR (Security Orchestration Automated Response) -järjestelmä, joka on verrattain uusi lisäys Azuren palveluvalikoimaan. Sentinel otetiin yleiseen käyttöön syyskuussa 2019 (Bieringer 2019). SIEM-järjestelmällä tarkoitetaan siis järjestelmää, joka kerää ja yh-

distelee yrityksen IT-ympäristöstä lokitietoja ja näiden avulla identifioi ja analysoi mahdollisia ympäristöä kohtaavia uhkia. SOAR taas tarkoittaa järjestelmää, jonka avulla voidaan automatisoida incident response -tehtäviä. SOAR integroi kaikki yrityksen tietoturvajärjestelmät, työkalut ja ohjelmat toisiinsa ja näin ollen mahdollistaa automatisoinnin. (Kirtley 2020)

Sentinel voi siis päällisin puolin vaikuttaa hyvin samanlaiselta järjestelmältä, kuin Azure Security Center, koska molemmat keräävät lokitietoja ja näiden avulla analysoivat järjestelmiä. Sentinel kuitenkin keskittyy enemmän ongelmien tutkimiseen sekä niiden ratkaisemiseen, kun taas Security Center kerää dataa ja havaitsee ongelmia. Security Center toimii siis myös yhtenä Sentinelin datanlähteenä, jonka avulla se voi havaita paremmin yritystä uhkaavia hyökkäyksiä. (Yoon 2020)

5.7.3 Azure Active Directory

Azure Active Directory (Azure AD) on Microsoftin pilvipohjainen identiteetin- ja pääsynhallintajärjestelmä, jonka avulla käyttäjät voivat kirjautua sekä yrityksen toimialueen ulkoisiin palveluihin, kuten Azure portaaliin ja myös toimialueen sisäisiin palveluihin, kuten yrityksen intranetiin. IT-ylläpitäjät voivat siis Azure AD:n avulla kontrolloida käyttäjien pääsyä palveluihin ja järjestelmiin sekä suojata identiteettejä ja käyttäjätunnuksia yrityksen käytäntöjen mukaisesti. (Ross ym. 2020)

Azure AD on siis pohjimmiltaan samanlainen palvelu, kuin Microsoftin vanhempi versio Active Directorystä, jota käytetään On-premises -ympäristöissä. Pilvessä toimiva Azure AD tekee kuitenkin monista asioista helpompaa, koska sillä voidaan hallita myös web-pohjaisia palveluita ja käyttäjät, ryhmät sekä käyttöoikeudet linkittyvät automaattisesti niihin. Azure AD käyttää myös täysin eri protokollia, kuin perinteinen Active Directory, joka toimi Kerberos ja NTLM -protokollien avulla. Azure AD käyttää toimiakseen SAML, OAuth, WS-Federation sekä OpenID Connect -protokollia ja se tukee myös SSO:ta sekä kaksivaiheista tunnistautumista, joka tekee palveluihin kirjautumisesta huomattavasti turvallisempaa. (Ng 2020)

Lisäksi Azure AD antaa yritysten IT-ylläpitäjille tietoa heidän toimialueensa tilien turvallisuudesta turvallisuuspisteytyksen avulla. Tämän pisteytyksen avulla tileistä on helppo tehdä entistä turvallisempia. Pisteytys muodostuu vertaamalla tilien asetuksia Microsoftin parhaisiin käytäntöihin. Toimintaperiaate on siis sama kuin Azuren Security Centerissä, eli käyttäjälle annetaan suosituksia, joita hän voi tehdä, jotta tilistä saadaan turvallisempi. (Flores ym. 2020)

6 Pohdinta

Lähes jokainen meistä käyttää tietämättään jotakin pilvipalvelua päivittäin. Ne eivät siis ole enää mikään uusi ja ihmeellinen asia, vaan jokapäiväinen normi. Sama koskee yrityskäyttöä, lähes jokaisessa yrityksessä on käytössä jokin pilvipalvelu, ja monessa yrityksessä koko infrastruktuuri on pilvessä. Pilvipalvelut tekevät käytettävyydestä erittäin helppoa, koska tietoon voidaan päästä käsiksi miltä laitteelta tahansa ja mistä tahansa. Samalla menetämme kuitenkin otetta omista tiedoistamme, ja emme enää välttämättä tiedosta, kenelle tietojamme jaamme. Tutkimus kuitenkin osoittaa, että kun pilvipalveluntarjoaja on huolellisesti valittu taustat tarkistaen, sopimukset tehty asianmukaisesti kaikesta mahdollisesta ja siirtyminen pilveen on tehty asianmukaisesti oikeanlaisia käytäntöjä ja arkkitehtuuria käyttäen, niin ei yrityksen tulisi pelätä tietojensa jakamista kolmannen osapuolen kanssa. Tutkimuksen kohteena ollut pilvipalvelu, Microsoft Azure sitoutuu noudattamaan erittäin tarkkoja säännöksiä, määräyksiä ja lakeja, jotka koskevat asiakkaan dataa. Tämän lisäksi Azuren työntekijöillä ei lähtökohtaisesti ole pääsyä dataan. Uskon ja toivon, että ainakin markkinoilla olevat muut isot pilvipalveluntarjoajat pyrkivät samaan tavoitteeseen ja kunnioittavat asiakkaidensa yksityisyyttä.

Pilven tietoturvariskit koostuvat pitkälti samoista asioista, kuin perinteisen On-premises -mallinkin riskit. Pilvessä noudatetaan kuitenkin jaettua vastuumallia asiakkaan ja palveluntarjoajan välillä, joten pilvessä riskienhallinta kuuluu kummallekin osapuolelle. Pilvessä riskit usein myös korostuvat verrattuna perinteiseen On-premises -ympäristöön. Suurimpia pilveen kohdistuvia tietoturvariskejä CSA:n vuoden 2019 tutkimuksen mukaan olivat siis tietomurrot, väärät konfiguraatiot ja puutteellinen muutosten hallinta, pilven tietoturva-arkkitehtuurin ja strategian puuttuminen, puutteellinen identiteetin- ja pääsynhallinta sekä tilin kaappaus.

Yleisellä tasolla pilvipalveluiden tietoturvallisuus perustuu pitkälti luottamukseen asiakkaan ja palveluntarjoajan välillä. Pilvipalveluiden tietoturvasta voidaan varmistua mahdollisimman hyvin sopimusten avulla, jotka ovat todella isossa osassa pilven tietoturvan toteuttamisessa. Sopimusten avulla asiakas varmistuu ja saa lupauksen siitä, miten hänen tietoaan pilvessä käsitellään. Sopimusten lisäksi asiakkaan kannattaa arvioida arviointikriteeristöjen avulla, täyttääkö pilvipalveluntarjoaja asiakkaan tarpeet ja kriteerit turvallisuuden suhteen. Asiakkaan kannattaa myös kiinnittää huomiota palveluntarjoajan sertifiointeihin, koska niiden avulla palveluntarjoaja voi osoittaa asiakkailleen omaa luotettavuuttaan sekä halukkuuttaan noudattaa kansainvälisiä standardeja ja/tai säännöksiä. Näiden lisäksi asiakkaan tulisi pitää huolta identiteetin- ja pääsynhallintansa riittävyydestä pilvessä sekä

mahdollisesti ottaa myös käyttöön Zero Trust-suojausmalli, joka poistaa ajatuksen luottamuksesta käsiteltäessä tietoturvaa.

Microsoft Azuren tietoturvan tutkimista olisi voinut jatkaa todella kauan, sillä tietoturvaan liittyy todella paljon osa-alueita, jotka muodostuvat yhdeksi kokonaisuudeksi ja Microsoftin dokumentaatioista ja muistakin lähteistä löytyi todella paljon mielenkiintoista tietoa, joita ei tässä tutkimuksessa ole mainittu. Aihe rajattiin tämän takia koskemaan Azuren infrastruktuurin tietoturvaa, koska se on usein yrityksille tuntemattomampi puoli pilvipalveluista, eikä usein tiedetä mitä palveluntarjoajan päässä todella tapahtuu ja miten asiakkaan dataa todella suojataan. Microsoftin tietoturvan toteutusmetodeista koskien Azuren infrastruktuuria, saatiin selkeä kuva ja opittiin ymmärtämään, miten Azurea suojataan.

Microsoft Azuren tietoturvataso osoittautui tutkimuksen perusteella todella positiiviseksi yllätykseksi ja Microsoft vaikuttaakin suojaavan Azuren infrastruktuuria todella hyvin sekä aktiivisesti. Koska Azure on Iaas-palvelumallin pilvipalvelu, jää asiakkaan vastuulle kuitenkin merkittävä rooli yrityksen infrastruktuurin suojaamisesta. Tutkimusta tehdessäni kävi selväksi, että Microsoft antaa asiakkailleen todella paljon hyviä neuvoja, kuinka yrityksen pilvi-infrastruktuurista voidaan tehdä Azuressa turvallinen. Azuren eri palveluissa ohjeistetaan kaikissa paljon asiakasta esimerkiksi pisteytyksien avulla, joista puhuttiin luvussa 5.7. Eli vaikka yritys joutuukin tekemään määrityksiä itse, jotta palvelusta saadaan turvallinen, niin hänen ei tarvitse miettiä miten palvelusta tehdään turvallinen, koska siihen tarjotaan jatkuvasti ohjeita.

Tutkimus muistuttaa myös siitä, että isot pilvipalveluntarjoajat pystyvät tarjoamaan asiakkailleen tietoturvaa, johon heillä ei omilla resursseillaan todennäköisesti olisi varaa. Eli vaikka asiakas joutuu pilvessä luottamaan kolmannen osapuolen toimintaan, niin saa hän myös todella kattavan tietoturvapaketin käyttöönsä, mikäli palveluntarjoaja on valittu huolellisesti.

6.1 Tutkimuksen luotettavuus ja jatkokehitysideat

Tutkimuksen luotettavuutta on pyritty todistamaan ajankohtaisilla lähteillä, jotka ovat alan ammattilaisten kirjoittamia. Tutkimuksen vanhimmat lähteet ovat vuodelta 2018 lukuun ottamatta riskien arviointiin liittyvää ohjeistusta, joka oli vuodelta 2003. Suurin osa lähteistä on vuosilta 2019-2020 ja ovat siis erittäin uusia ja ajankohtaisia. Lähteistä ei tutkimuksen aikana ollutkaan pulaa, sillä aiheesta löytyi erittäin kattavasti ajankohtaista tietoa avoimista lähteistä. Ajankohtaiset lähteet ovat tämän tutkimuksen kannata oleellisia, koska pilvimaailmassa asiat muuttuvat nopeasti, joten vasta muutaman vuoden vanhatkin tiedot voivat olla jo vanhentuneita. Tutkimuksen toteutustapa, eli kirjallisuuskatsaus osoittautui

myös mielestäni oikeaksi tutkimusmenetelmäksi tähän tutkimukseen. En missään vaiheessa kokenut, että esimerkiksi haastattelu tai kyselytutkimus olisi ollut tarpeellinen osana tutkimusta, vaikkakin niillä olisi voinutkin saada eri näkökulmaa asiaan.

Tätä tutkimusta voidaan hyödyntää esimerkiksi tilanteissa, joissa halutaan tietää enemmän ajankohtaisista pilveen kohdistuvista riskeistä tai tilanteissa, joissa tutkitaan pilvipalvelun turvallisuuteen vaikuttavia tekijöitä. Tutkimuksen jatkokehittämiskohteena voisi toimia esimerkiksi vertailu suurten pilvipalveluntarjoajien, eli Microsoft Azuren, Amazon Web Servicesin sekä Google Cloudin tietoturvan välillä. Tässä voitaisiin tutkia miten nämä yritykset toteuttavat tietoturvaansa ja eroavatko nämä toteutustavat sekä tietoturvallisuuden tasot merkittävästi toisistaan.

6.2 Oma oppiminen opinnäytetyöprosessin aikana

Opinnäytetyön tiukasta aikataulusta huolimatta opinnäytetyöprosessi sujui mielestäni hyvin ilman suurempia vaikeuksia. Aihe ja tutkimusmenetelmät osoittautuivat mielestäni itselleni oikeiksi ratkaisuiksi ja ne tekivät kirjoittamisesta helpompaa. Opinnäytetyötä olisi jälkikäteen ajateltuna voinut rajata hieman enemmän esimerkiksi koskemaan vain Microsoft Azuren tietoturvallisuutta. Azuresta löytyi niin paljon tietoa, että siitä olisi hyvin voinut tehdä kokonaan itsenäisen työn. Eniten vaikeuksia työn aikana tuottikin hieman liian suuri laajuus ja tämän seurauksena oli vaikeaa päättää, mistä aiheista tulisi kirjoittaa.

Opinnäytetyöprosessin aikana sain kuitenkin erittäin paljon uutta tietoa tästä aiheesta sekä opin ymmärtämään pilvipalveluiden toimintaa ja tietoturvallisuutta syvemmällä tasolla. Prosessi opetti minulle myös tieteellistä kirjoittamista uudella tavalla ja se oli kokonaisuudessaan mielenkiintoinen ja opettavainen.

Lähteet

Baldwin, M. 2019. Azure infrastructure monitoring. Luettavissa: https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-monitoring. Luettu: 29.4.2020.

Baldwin, M. & Kess, B. 2019a. Azure facilities, premises, and physical security. Luettavissa: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security. Luettu: 28.4.2020.

Baldwin, M. & Kess, B. 2019b. Management and operation of the Azure production network. Luettavissa: https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-operations. Luettu: 29.4.2020.

Baldwin, M. & Kess, B. 2019c. Azure infrastructure availability. Luettavissa: https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability. Luettu: 13.5.2020.

Baumgartner, P., Borys, A. & Mazzoli, R .2020. ISO/IEC 27001:2013 Information Security Management Standards. Luettavissa: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-iso-27001?view=o365-worldwide. Luettu: 14.5.2020.

Baumgartner, P. & Mazzoli, R. 2020a. Cloud Security Alliance (CSA) STAR certification. Luettavissa: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-csa-star-certification?view=o365-worldwide. Luettu: 14.5.2020.

Baumgartner, P. & Mazzoli, R. 2020b. Federal Risk and Authorization Management Program (FedRAMP).Luettavissa: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-fedramp?view=o365-worldwide. Luettu: 14.5.2020.

Baumgartner,P., Borys, A., Cole, L & Mazzoli, R. 2020. Service Organization Controls (SOC). Luettavissa: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc?view=o365-worldwide. Luettu: 14.5.2020.

Baumgartner, P., Cole, L. & Mazzoli, R. 2020. Health Insurance Portability and Accountability (HIPAA) & HITECH Acts. Luettavissa: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-hipaa-hitech?view=o365-worldwide. Luettu: 14.5.2020.

Ben-Menahem, A. 2018. 3 reasons why Azure's infrastructure is secure. Luettavissa: https://azure.microsoft.com/en-us/blog/3-reasons-why-azure-s-infrastructure-is-secure/. Luettu: 29.4.2020.

Bieringer, J. 2019. Azure Sentinel SIEM is now Generally Available. Luettavissa: https://www.boldbi.com/blog/azure-sentinel-siem-generally-available. Luettu: 7.5.2020.

Cimpanu, C. 2020. Microsoft discloses security breach of customer support database. ZDNet. Luettavissa: https://www.zdnet.com/article/microsoft-discloses-security-breach-of-customer-support-database/. Luettu: 14.5.2020.

Cloud Security Alliance 2019. Top Threats to Cloud Computing, The Egregious 11. Luettavissa: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/. Luettu: 22.4.2020.

Drinkwater, D. 2018. What is single sign-on? How SSO improves security and the user experience. CSO. Luettavissa: https://www.csoonline.com/article/2115776/what-is-single-sign-on-how-sso-improves-security-and-the-user-experience.html. Luettu: 5.5.2020.

Elyashar, G. 2019. Ignite 2019 releases for Azure Security Center and Azure platform security. Luettavissa: https://techcommunity.microsoft.com/t5/azure-security-center/ignite-2019-releases-for-azure-security-center-and-azure/ba-p/975570. Luettu: 17.5.2020.

Eronen, H. 2019. IaaS, PaaS, SaaS? Mikä pilvipalvelu sopii yrityksellesi. Planeetta. Luettavissa: https://www.planeetta.fi/2016/03/15/iaas-paas-saas-mika-pilvipalvelu-sopii-yrityksellesi/. Luettu 11.3.2020.

Euroopan Unioni 2020. Yleinen tietosuoja-asetus. Luettavissa: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm. Luettu: 7.4.2020.

Evans, B. 2019. After 3 Cloud Failures in 12 Months, Microsoft Fortifies Azure Reliability. Luettavissa: https://cloudwars.co/microsoft/azure-cloud-failures-microsoft-reliability/. Luettu: 17.5.2020.

Fadilpašić, S. 2018. Microsoft Azure suffers major outage. Luettavissa: https://www.itproportal.com/news/microsoft-azure-suffers-major-outage/. Luettu: 17.5.2020.

Fastmetrics. What Is Cloud Computing & How Does It Work? Luettavissa: https://www.fastmetrics.com/blog/tech/what-is-cloud-computing/. Luettu: 5.5.2020.

Flexera 2019. State of The Cloud Report. Luettavissa: https://resources.flexera.com/web/media/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf. Luettu: 11.3.2020.

Flores, J., Vilcinskas, M., Cai, S., Sharkey, K., Schonning, N., Ross, E. & Bahall, D. 2020. What is the identity secure score in Azure Active Directory? Luettavissa: https://docs.microsoft.com/en-gb/azure/active-directory/fundamentals/identity-secure-score. Luettu: 7.5.2020.

Fruhlinger, J. 2020. What is information security? Definition, principles, and jobs. CSO. Luettavissa: https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html. Luettu 1.4.2020.

Fruhlinger, J. 2019. 2fa explained: How to enable it and how it works. CSO. Luettavissa: https://www.csoonline.com/article/3239144/2fa-explained-how-to-enable-it-and-how-it-works.html. Luettu: 5.5.2020.

Hoelscher, P. 5 Benefits of Paying for an Employee's Professional Certification. Luettavissa: https://resources.infosecinstitute.com/5-benefits-of-paying-for-an-employees-professional-certification/. Luettu: 14.5.2020.

Hoffman, C. 2018. What Is Microsoft Azure, Anyway? How-To Geek. Luettavissa: https://www.howtogeek.com/337961/what-is-microsoft-azure/. Luettu 2.4.2020.

Huntington, S. 2019. How Does Cloud Computing Work? Luettavissa: https://cloudacademy.com/blog/how-does-cloud-computing-work/. Luettu: 12.3.2020.

Imke, S. 2019. How to Develop a Risk Matrix. Luettavissa: https://www.business2community.com/strategy/how-to-develop-a-risk-matrix-02234010. Luettu: 5.5.2020.

IT Governance 2020. Information Security and ISO 27001. Luettavissa: https://www.itgovernance.co.uk/green-papers/information-security-and-iso-27001-an-introduction. Luettu: 14.5.2020.

Kindervag, J & Staten, J. Why a Zero-Trust Approach Can Make the Cloud More Secure. Security Roundtable. Luettavissa: https://www.securityroundtable.org/zero-trust-approach-can-make-cloud-secure/. Luettu: 8.4.2020.

Kirtley, E. 2020. What is SIEM? What is SOAR? How are they different? Luettavissa: https://swimlane.com/blog/siem-soar/. Luettu: 7.5.2020.

Krazit, T. 2018. Microsoft releases details on last week's big Azure outage, during which servers were damaged but no data was lost. GeekWire. Luettavissa: https://www.geekwire.com/2018/microsoft-releases-details-last-weeks-big-azure-outage-servers-damaged-no-data-lost/. Luettu: 17.5.2020.

Kyberturvallisuuskeskus. Pilvipalveluiden turvallisuus. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf. Luettu: 7.4.2020.

Kyberturvallisuuskeskus 2019a. Tietoturva. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva. Luettu: 24.3.2020

Kyberturvallisuuskeskus 2019b. Tunnetko jo PiTuKrin? Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-jo-pitukrin. Luettu: 24.3.2020.

Kyberturvallisuuskeskus 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf. Luettu: 24.3.2020.

Lanfear, T. 2020. Azure SQL Database security features. Luettavissa: https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-sql. Luettu 29.4.2020.

Lanfear, T., Agiewich, R., Diogenes, Y., Pasic, A., Nevil, T., Cai, S., Haber, M., Sebolt, M., Koke, J., Burrs, R., Baldwin, M., Grootenboer, E., Coulter, D. & Lin, C. 2020. What is Azure Security Center? Luettavissa: https://docs.microsoft.com/en-gb/azure/security-center/security-center-intro. Luettu: 7.5.2020.

Lord, N. 2018. What is the Principle of Least Privilege (POLP)? A Best Practice for Information Security and Compliance. Luettavissa: https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance. Luettu: 5.5.2020.

Lu, D. 2019. How Much Are Password Resets Costing Your Company? Okta. Luettavissa: https://www.okta.com/blog/2019/08/how-much-are-password-resets-costing-your-company/. Luettu: 5.5.2020.

Microsoft. Anna etätyöntekijöille heidän tarvitsemansa tietoturva Zero Trust -suojauksen avulla. Luettavissa: https://www.microsoft.com/fi-fi/security/business/zero-trust Luettu: 8.4.2020.

Morrow, T. 2018. 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud. Luettavissa: https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html. Luettu 21.4.2020.

Murphy, D. 2018. Two-Step Text Authentication Isn't Enough to Keep Your Accounts Secure. Lifehacker. Luettavissa: https://lifehacker.com/two-factor-authentication-isnt-enough-to-keep-your-acco-1827867557. Luettu: 5.5.2020.

Naden, C. 2020. Guidance For Information Security Management Systems Auditors Just Updated. Luettavissa: https://www.iso.org/news/ref2477.html. Luettu: 13.5.2020.

Ng, C. 2020. Active Directory: Difference Between Windows and Azure AD. Luettavissa: https://www.varonis.com/blog/windows-vs-azure-active-directory/. Luettu: 7.5.2020.

Paloalto Networks. What Is Zero Trust for the Cloud? Luettavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-for-the-cloud. Luettu: 8.4.2020.

Papolu, R. 2018. How To Secure Your Data In The Cloud. Forbes. Luettavissa: https://www.forbes.com/sites/forbestechcouncil/2018/10/11/how-to-secure-your-data-in-the-cloud/#aba6013507c4. Luettu: 24.3.2020.

Patterson, D. 2018. Why Microsoft spends over $1 billion on cybersecurity each year. TechRepublic. Luettavissa: https://www.techrepublic.com/article/why-microsoft-spends-over-1-billion-on-cybersecurity-each-year/. Luettu: 2.5.2020.

Pietschmann, C. 2019. May 2, 2019: Major Azure Outage Due to DNS Migration Issue. Luettavissa: https://build5nines.com/may-2-2019-major-azure-outage-due-dns-migration-issue/. Luettu: 17.5.2020.

Radoslav, C. 2019. Cloud Computing Statistics 2020. Luettavissa: https://techjury.net/stats-about/cloud-computing. Luettu: 11.3.2020.

Ranger, S. 2018. What is cloud computing? Everything you need to know about the cloud, explained. ZDNet. Luettavissa: https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/. Luettu: 11.3.2020.

Raza, M. 2019. Introduction to Information Security Management Systems (ISMS). Luettavissa: https://www.bmc.com/blogs/introduction-to-information-security-management-systems-isms/. Luettu: 13.5.2020.

Raza, M. 2020. Public vs Private vs Hybrid Cloud Differences. Luettavissa: https://www.bmc.com/blogs/public-private-hybrid-cloud/. Luettu: 15.5.2020.

Ross, E., Flores, J., Murray, D., De Guzman, C., Mathers, B., Garg, M., Cai, S., Agiewich, R., Sanders, T., Turscak, M., Bahall, D., Love, C. & Kess, B. 2020. What is Azure Active Directory? Luettavissa: https://docs.microsoft.com/en-gb/azure/active-directory/fundamentals/active-directory-whatis. Luettu: 7.5.2020.

Shein, E. 2019. The most important cloud advances of the decade. TechRepublic. Luettavissa: https://www.techrepublic.com/article/the-most-important-cloud-advances-of-the-decade/. Luettu 17.5.2020.

Sherer, T., Baldwin, M. & Kess, B. 2020. Azure customer data protection. Luettavissa: https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data. Luettu: 28.4.2020.

Sraders, A. 2020. What is Salesforce and What Does It Do in 2020? Luettavissa: https://www.thestreet.com/technology/what-is-salesforce-14796378. Luettu: 11.3.2020.

Techopedia. On-Premises Software. Luettavissa: https://www.techopedia.com/definition/26714/on-premises-software. Luettu: 13.5.2020.

Telia 2018. Pilven monet kasvot – IaaS, PaaS ja SaaS. Luettavissa: https://www.inmicsnebula.fi/fi/blogi/pilven-monet-kasvot-iaas-paas-ja-saas?language_content_entity=fi. Luettu: 12.3.2020.

Tietosuojavaltuutetun toimisto. Tietosuoja turvaa oikeutesi henkilötietoja käsiteltäessä. Luettavissa: https://tietosuoja.fi/tietosuoja. Luettu: 13.5.2020.

Turner, B. 2019. What is SaaS? Everything you need to know. TechRadar. Luettavissa: https://www.techradar.com/news/what-is-saas. Luettu: 11.3.2020.

Valtiovarainministeriö. 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10229. Luettu: 17.5.2020.

Vukos-Walker, C., Raya, T., Sehgal, W., Halfin, D., Mazzoli, R., Smith, S., Baskaran, R., Borys, A., Willie, S., Byrd, D. & Baumgartner, P. 2020. Microsoft Compliance Manager (preview). Luettavissa: https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-overview?view=o365-worldwide. Luettu: 13.5.2020.

Watts, S. & Raza, M. 2019. SaaS vs PaaS vs IaaS: What's The Difference and How To Choose. BMC. Luettavissa: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/. Luettu: 11.3.2020.

World Informatix. Cloud Computing Security. Luettavissa: https://worldinformatixcs.com/cloud-computing-security/. Luettu: 5.5.2020.

Yoon, J. 2020. What is the difference between Azure Security Center and Azure Sentinel? Medium. Luettavissa: https://medium.com/the-cloud-builders-guild/what-is-the-difference-between-azure-security-center-and-azure-sentinel-9d91eb801cd2. Luettu: 7.5.2020.