Haaga-Helia
ammattikorkeakoulu Oy

Zero Trust – tietoturvan nykymalli

Irene Kunnari

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma 2020

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)

Irene Kunnari

Koulutusohjelma

Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön nimi	**Sivu- ja liitesivumäärä**
Zero Trust – tietoturvan nykymalli	34 + 2

Tämä opinnäytetyö käsittelee vuonna 2010 kehitettyä uudenlaista tietoturvamallia, Zero Trustia. Zero Trust poikkeaa pitkään standardina olleesta, luotettavan sisäverkon suojeluun keskittyvästä tietoturvamallista, johon usein saatetaan viitata nimityksellä castle-and-moat-tietoturvamalli. Opinnäytetyön alussa esitellään yleisesti castle-and-moat-tietoturvamalli, sekä nykypäivän ympäristöihin paremmin skaalautuva Zero Trust-tietoturvamalli. Zero Trust-tietoturvamallin periaatteena on lähtökohta, jonka mukaan yksikään verkko ei ole vahvasta suojauksestaan huolimatta luotettava. Koko IT-ympäristö tulee rakentaa edellä mainitusta lähtökohdasta ja Zero Trustin mottoon ”Never Trust, Always Verify” heijastaen.

Zero Trustin pääperiaatteiksi opinnäytetyössä määritellään kolme Zero Trust-ympäristön rakentamisessa huomioon otettavaa osa-aluetta; mikrosegmentaatio, autentikointi ja pääsynvalvonta, sekä monitorointi. Nämä kolme tavoitetta luovat moniulotteisen, mutta dynaamisen, turvallisen ja helposti hallittavan IT-ympäristön, joka parhaimmillaan skaalautuu erilaisten yritysten olemassa oleviin ympäristöihin. Zero Trustia sekä siihen mahdollisesti liittyviä teknologioita ja palveluita käsitellään opinnäytetyötä varten hahmotellun kuvitteellisen esimerkkiyrityksen ympäristön kautta. Esimerkkiyrityksen Zero Trust-ympäristö ja sen esittely antaa konkreettisemman kuvan yhdenlaisesta mahdollisesta Zero Trust toteutuksesta. Konkreettisuuden lisäämiseksi, opinnäytetyössä on käytetty myös mahdollisesti kuluttajille tuttuja esimerkkejä Zero Trustia mukailevista menetelmistä. Opinnäytetyössä on myös tutkittu lyhyesti Googlen ja Gartnerin kehittämiä, omia versioitaan Zero Trust-tyyppisestä tietoturvan mallista.

Opinnäytetyö luo suomenkielisen materiaalin yksilöille ja yrityksille Zero Trustista kokonaisuutena, mistä suomenkielistä materiaalia muuten on hyvin rajoitetusti saatavilla.

Asiasanat

tietoturva, Zero Trust, BeyondCorp, tietoturvamalli

Author(s)

Irene Kunnari

Degree Programme

Degree Programme in Information Technology (Tietojenkäsittely)

Thesis title	**Number of pages and appendix pages**
Zero Trust – a new cybersecurity model	34 + 2

This thesis is about a new cybersecurity model Zero Trust, which was founded in 2010. Zero Trust is a new approach to cybersecurity compared to the traditional Castle and moat-model which concentrates on protecting the trusted private network. In the beginning of this thesis, the main differences between the Castle and moat-model and the new Zero Trust model as a more scalable solution into today's environments are explained. The main idea of Zero Trust is that no network is trusted despite its strong security. The whole IT-environment should be built based on Zero Trust motto "Never Trust, Always Verify".

In this thesis, the main principles for building Zero Trust environment are defined into three areas; micro-segmentation, authentication and access control, and monitoring. These principles together form a dynamic, secure and easily manageable IT-environment that its best scales into different, already existing environments. Technologies and services related to Zero Trust are presented from a view of an example case that is fictional 50-100 employee company. The example case gives the reader a more concrete description about Zero Trust's possible implementations. Whenever possible, the thesis also includes consumer-friendly examples of technologies supporting Zero Trust. The thesis also includes a short research about Zero Trust based models by Google and Gartner.

This thesis provides novel Finnish material for individuals and companies to explore Zero Trust and its dimensions in cybersecurity.

Keywords

cybersecurity, Zero Trust, BeyondCorp, cybersecurity model

Sisällys

1 Johdanto

Tämä opinnäytetyö käsittelee vuonna 2010 kehitettyä uudenlaista tietoturvamallia, Zero Trustia. Zero Trust poikkeaa pitkään standardina olleesta, luotettavan sisäverkon suojeluun keskittyvästä tietoturvamallista, johon usein saatetaan viitata nimityksellä castle-and-moat-tietoturvamalli. Zero Trust-tietoturvamallin periaatteena sen sijaan on lähtökohta, jonka mukaan yksikään verkko ei ole vahvasta suojauksestaan huolimatta luotettava. Lähtökohdan ajatuksena on se, että hyökkääjät onnistuvat aina pääsemään sisäverkkojen ”luotetulle” puolelle jotakin kautta. Tämän takia sisäverkkojen suojaus tulisi rakentaa siitä lähtökohdasta, että hyökkääjä on jo päässyt sisälle verkkoon. Zero Trustin tietoturvamallilla pyritään vähentämään IT-ympäristön hyökkäyspinta-alaa ja estämään hyökkääjien tehokas ja tuhoisa eteneminen sisäverkossa.

IT-ympäristöjen kehitys yhä moninaisemmiksi kokonaisuuksiksi on nopeaa nykypäivänä. Kasvavissa yrityksissä vaatimukset tietoturvalle ovat kovat, mutta tietoturvan jatkuva kehitys yrityksen mukana ei ole itsestäänselvyys. Zero Trust mallin tarkoituksena onkin mahdollistaa yritykselle dynaaminen tietoturva, jonka ylläpitäminen on helppoa myös yrityksen ympäristön muuttuessa tai kasvaessa. Etenkin nykypäivänä uudenlaisten teknologioiden lisääntyessä on tärkeää, että tietoturva skaalautuu erilaisille alustoille tehokkaasti. Zero Trustin toteuttamisen yhtenä tavoitteena tietoturvan vahvistamisen ohella on, että työmäärä yritysten IT-tiimissä vähenee ja muuttuu yksinkertaisemmaksi.

1.1 Opinnäytetyön tausta ja tavoitteet

Opinnäytetyössä on tavoiteltu kirjoitustyyliä ja lähestymistapaa aiheeseen, millä myös tietoturvaan ennalta perehtymättömien olisi mahdollisimman helppo saada aiheesta kiinni ja ymmärtää Zero Trustin kokonaisuus. Myös kuka tahansa; lukija, tietotekniikan ammattilainen tai yläkoululainen toivottavasti voisi kokea opinnäytetyöstäni lukemansa asian hyödylliseksi. Zero Trustia voi helposti heijastaa myös kuluttajan omaan tietoturvaan, ja opinnäytetyöhöni olen sisällyttänyt joitain esimerkkejä, jotka ovat mahdollisesti monelle tuttuja. Zero Trustista ei löydy juurikaan materiaalia suomeksi, jonka takia tämä opinnäytetyö on toivottavasti helpompi ymmärtää heille, jotka eivät englanninkielisestä materiaalista välttämättä kykene hahmottamaan Zero Trustin pääperiaatteita.

Henkilökohtainen oppimistavoitteeni opinnäytetyötä tehdessäni on ymmärtää Zero Trustin pääperiaatteet sekä konkreettisesti teknologioita ja menetelmiä, joita niiden

saavuttamiseen voi hyödyntää. Koen Zero Trustin oleelliseksi aiheeksi nykypäivän teknologioita ja pilvipainotteisia infrastruktuureita tietoturvan kannalta kehittäessä.

1.2 Opinnäytetyön rajaus

Tämä opinnäytetyö keskittyy Zero Trustin määrittelemiseen tietoturvan mallina sekä käsitteen tukemien teknologioiden esittelemiseen. Zero Trustin periaatteet ovat tässä työssä tutkimusteni perusteella rajattu kolmeen pääperiaatteeseen, mutta eri tahoilla voi olla eri tyyli rajata pääperiaatteita. Syvällisempi tekniikoiden kuvailu pyritään rajaamaan pois tästä opinnäytetyöstä ja keskittymään Zero Trustiin kokonaisuutena niin, että myös alaan perehtymätön voi opinnäytetyön sisällön omaksua. Ymmärryksen tueksi opinnäytetyöhön on sisällytetty liitteenä sanasto, joka sisältää opinnäytetyössä mainittuja käsitteitä.

2 Tutkimusmenetelmät

Opinnäytetyön tutkimusmenetelmänä toimii kirjallisista lähteistä saatavan tiedon yhdistely sekä muodostus kokonaisuudeksi. Tutkimuskohde, tutkimuskysymykset sekä kirjallisuuskatsaus tutkimusmenetelmänä ovat selitetty seuraavissa alikappaleissa.

2.1 Tutkimuskohde

Tutkimuskohteena tälle opinnäytetyölle toimii John Kindervagin vuonna 2010 kehittelemä tietoturvan ajatusmalli Zero Trust. Zero Trust on tietoturvan malli, joka keskittyy IT-ympäristöissä siihen lähtökohtaan, jonka mukaan yksikään verkko, laite, käyttäjä tai muu ei ole vahvasta suojauksestaan huolimatta luotettava. Zero Trustin motto on ”Never Trust, Always Verify” ja tämä motto heijastuu Zero Trustin päätavoitteista, jotka käsitellään syvemmin opinnäytetyön kappaleessa 4.

2.2 Tutkimuskysymykset

Lähestyn tutkimusaihettani seuraavien tutkimuskysymysten pohjalta.

1. Mikä on Zero Trust ja mitkä ovat ajatuksen keskeisimmät periaatteet?
2. Mitkä ovat oleellisimmat teknologiat Zero Trustin tukena?

Tutkimuskysymykseni tukevat tavoitettani tutkimalla selvittää Zero Trustin keskeisimmät piirteet ja koostaa tutkimuksen tuloksista yhtenäinen kattava selitys näistä piirteistä. Jatkona ensimmäiselle tutkimuskysymykselle, sisällytän myös tutkimustuloksia Zero Trustin tukena käytettävistä teknologioista ja menetelmistä. Lähestymistapana toiseen tutkimuskysymykseen käytän kuvitteellista esimerkkiyritystä. Hahmottelen sen IT-ympäristön ja esittelen tutkimusteni perusteella esimerkkipalveluita, -teknologioita ja menetelmiä, joita samantyyppinen yritys voisi Zero Trust tietoturvamallia tavoitellessaan käyttää.

2.3 Tutkimustyyppi

Tutkimus tehdään kirjallisuuskatsauksena. Lähdemateriaalia on kerätty pääsääntöisesti englanninkielisenä netistä. Myös suomenkielistä lähdemateriaalia on pyritty käyttämään löydöksien mukaan. Lähdemateriaali sisältää artikkeleita ja raportteja tietoturvasta, Zero Trustista ja näihin liittyvistä eri osa-alueista ja teknologioista. Kirjallisuuskatsauksen lisäksi laadin kuvitteellisen tapausesimerkin toisen tutkimuskysymykseni selvittämiseen, minkä avulla konkretisoin Zero Trustin edistämiseksi käytettäviä menetelmiä käytännössä.

3 Tietoturvan kehitys nykypäivään

Tietoturvan merkitys nykypäivänä on suuri. Uusien teknologioiden myötä myös tietoturvan rikkomiseksi tehtävät hyökkäykset kasvavat. Tietoturvahyökkäyksiä toteutetaan erilaisia ja niitä voidaan kohdistaa lähes mihin tahansa verkkoihin kytkettyihin laitteisiin ympäri maailmaa. Vuonna 2018 Accenturen julkaisemassa The Cost of Cybercrime-raportissa käy ilmi, että viimeisten 5 vuoden aikana onnistuneet tietoturvahyökkäykset ovat kasvaneet määrältään 67 prosenttia. Teknologian kehittyessä, myös tietoturvan täytyy pysyä kehittyvän teknologian mukana tarjoamassa suojaa hyökkäyksiä vastaan. Olemassa olevista teknologioista löydetään jatkuvasti heikkouksia, joista avautuu uusia potentiaalisia hyökkäysvektoreita. Tietoturvan toteuttaminen ja lähtökohdat siihen vaihtelevat paljon riippuen täysin käytössä olevista laitteista, palveluista ja tuotteista sekä turvattavan kohteen tyypistä. Vaikka tietoturva on laaja kokonaisuus, yleisiä tietoturvaan sovellettavia malleja on kuitenkin tietoturvan aikana ehtinyt muodostua Ennen kuin syvennytään tietoturvan eri malleihin, käsitellään tämän opinnäytetyön ymmärtämistä oleellisesti pohjustava kysymys: Mitä on tietoturva?

3.1 Tietoturvan tarkoitus

Tietoturvalla tarkoitetaan tiedon turvaamista niin, että voidaan olla varma kohteen luottamuksellisuudesta, eheydestä ja saatavuudesta (engl. Confidentiality, Integrity, Availability). Tietoturvan kohde voi olla monenlainen, esimerkiksi tietojärjestelmä, palvelu, verkkoliikenne tai joitain muita tietoja. Edellä mainitut tietoturvan kolme, yhdessä CIA-malliksi kutsuttua perustavoitetta pyrkivät siihen, että tieto on saatavilla sekä muokattavissa vain siihen oikeutetuilla henkilöillä, ja että tieto on oikeutettujen henkilöiden saatavilla aina silloin kun sille on tarve. Tietoturvalla ja sen toimivuudella on merkittävä rooli etenkin mahdollisissa häiriötilanteissa, jolloin tietoturvan perusperiaatteet saattavat olla alttiimpia hyökkäyksille. Tällaisia häiriötilanteita voi olla esimerkiksi silloin, jos ohjelmistossa ilmenee jokin vika, joka vaikuttaa sen toiminnallisuuteen heikentävällä tavalla. (Pietikäinen 2013.)

Vaikka luottamuksellisuutta, eheyttä ja saatavuutta pidetään keskeisimpinä tietoturvan tavoitteina, on näiden kolmen muodostamaa kokonaisuutta pidetty myös liian suppeana tietoturvaa kuvaillessa. Näin ollen tietoturvan tavoitteita määritellessä niihin usein lisätään myös todennus, pääsynvalvonta ja kiistämättömyys (engl. authentication, access control, non-repudiation). Nämä täydentävät tietoturvan tavoitteita varmistamalla, että esimerkiksi käyttäjä tai laite todistetusti varmistetaan oikeutetuksi ja vasta tämän perusteella pääsy sallitaan. Kiistämättömyydellä taataan, että transaktioista tai muusta liikenteestä löytyy

tarpeeksi kattavat lokitiedot, jotta tilanteen tullessa niitä voidaan käyttää todistamaan tapahtuneet toiminnot. Nämä kaikki tietoturvan tavoitteet yhdessä muodostavat kokonaisuuden, jonka tarkoituksena on pitää jokainen tavoite turvattuna erilaisia teknologioita ja menetelmiä käyttäen. (Tirronen 2003.)

3.2 Castle-and-moat – perinteinen tietoturvamalli

”Castle and moat” tarkoittaa suomeksi ”linna ja vallihauta”. Vallihauta puolustusmenetelmänä on ollut yksi linnan tärkeimpiä suojauksia silloin kun linnat olivat täysin toiminnallisia. Tätä historiallista puolustusmallia, jossa pääpaino on pitää tunkeilijat ulkopuolella vallihaudan ja muurin avulla, voidaan myös heijastaa niin kutsuttuun perinteiseen tietoturvamalliin. Tähän perinteiseen tietoturvamalliin viitatessa käytetäänkin englannin kielistä nimitystä ”castle and moat” -malli. (Mayne 2016.)

Caste and moat -mallissa linna on se, jonka ympärille suojaus rakennetaan ja johon sisäänpääsyä vartioidaan. Tietoturvamallissa linnan roolia kuvaa yleensä suojattu, yksityinen verkko. Esimerkiksi yrityksen sisäverkkoa suojataan verkon sisäänkäyntiä valvomalla, ja sisään onnistuneesti autentikoiduttua avautuu pääsy sisäverkon eri resursseihin. Yrityksen sisäverkossa olevia resursseja voi olla esimerkiksi yrityksen omilla palvelimilla ylläpidetty intranet tai esimerkiksi verkkoon liitetty printteri. Sisäverkossa pääsee liikkumaan eri resursseihin ilman valvontaa, sillä päätös verkon käyttäjän luotettavuudesta on jo tehty sisäänkäynnillä ulkoverkosta sisäverkkoon, eli siirtyessä WAN-verkosta LAN-verkkoon. Verkkoon pyrkijä voidaan esimerkiksi varmentaa salasanalla, minkä onnistuessa tulija saa pääsyn sisäverkkoon ja automaattisesti siitä sisäverkosta löytyviin resursseihin ja niiden dataan. (Sande 2019.)

Vallihaudan roolia castle and moat -tietoturvamallissa kuvaa useimmiten palomuuri (engl. firewall). Palomuurin tarkoitus on vartioida pääsyä internetistä suojeltuun LAN-verkkoon. Palomuuri voi olla erillinen laite kytkettynä internetin ja yrityksen sisäverkon yhdyskäytävän (engl. gateway) väliin. Palomuuri voi olla myös sovelluspohjainen, sisäänrakennettu ominaisuus yrityksen yhdyskäytävänä toimivassa reitittimessä. Kaikki liikenne sisäänpäin verkkoon sekä ulospäin verkosta kulkee yhdyskäytävän ja niin ollen myös palomuurin läpi. Palomuuria konfiguroimalla voidaan määritellä, minkä sääntöjen perusteella verkkoon päästetään liikennettä sisälle ja mitä sieltä päästetään ulos internettiin. Mallissa pyritään rajaamaan suojattu alue selkeästi ulkopuolesta ja keskittymään rakentamaan rajalle vahva puolustusjärjestelmä, joka hoitaa pääosan sisäverkon suojauksesta. (Barracuda.)

Tämä perinteinen ja pitkään standardina pidetty castle and moat -tietoturvamalli on erityisesti lähivuosina alkanut herättää sekä kysymyksiä että epäilyksiä liittyen mallin sopivuuteen nykypäivän ympäristöihin. Epäilyksiin vaikuttaa esimerkiksi se, että tietoturvaan panostetaan yhä enemmän taloudellisesti, mutta silti rahaa menetetään jatkuvasti erilaisten hyökkäysten seurauksena. Caste and moat -mallissa pyritään rakentamaan vahva suojaus ulko-ja sisäpuolen rajalle, ja käyttämään tätä rajaa vahvimpana tietoturvan komponenttina. Useat suurimmat ja kalleimmat tietoturvahyökkäykset ovat kuitenkin alkaneet siitä, että hyökkääjä on jo päässyt sisälle suojattuun verkkoon ja onnistunut aiheuttamaan mittavaa tuhoa puutteellisen tietoturvatason takia itse sisäverkossa. Näissä tapauksissa koko sisäverkon tietoturvasuojaus on pitkälti laskettu verkon palomuurin varaan. Palomuurin läpi päästessä kulkijaa kohdellaan automaattisesti luotettavana sisäverkossa liikkuessaan, sillä verkon sisäpuolella kulkijan identiteettiä ei enää kyseenalaisteta. (Bradley 2019.)

Tietoturvan perinteisessä mallissa yhdeksi suureksi heikkoudeksi voidaan siis käsittää internetin ja sisäverkon välillä oleva palomuuri. Palomuuri kuitenkaan ei itsessään ole heikentävä tekijä, vaan heikkoudeksi muodostuu palomuurin myöntämä luottamus sen läpäisijälle. Jos hyökkääjä onnistuu läpäisemään palomuurin, hän ansaitsee samanlaisen luottamuksen kuin verkon muut käyttäjät ja saa pääsyn verkon sisällä oleviin resursseihin. Verkon sisällä naamioitunutta hyökkääjää ei pyydetä enää uudestaan todistamaan luotettavuuttaan. Hyökkääjä käyttää siis ansaitsemaansa luottamusta hyökkäysvektorina kohteen sensitiiviseen dataan. Vuonna 2010 Forrester Researchin analyytikko John Kindervag havaitsi, että jos tämä luottamus pyrittäisiin poistamaan verkosta kokonaan, niin sitä ei olisi myöskään mahdollista käyttää hyökkäysvektorina. (Palo Alto Networks.)

3.3 Zero Trust – nykyaikaisempi lähtökohta tietoturvaan

John Kindervag kertoo itse Youtubessa ShortestPathFirst-kanavalla julkaistulla haastatteluvideolla (2019) Zero Trust mallista. Zero Trustin ensisijainen periaate on pyrkiä korjaamaan perinteisen tietoturvamallin ajatus luotetuista ja epäluotetuista verkoista. Luotetut verkot perinteisessä tietoturvan ajatusmallissa ovat suojattuja yksityisiä verkkoja, ja epäluotettavat verkot ovat julkisia verkkoja. Kindervag kertoo kuitenkin aikaisen työkokemuksensa perusteella, että penetraatiotestaajat onnistuvat aina löytämään jonkun keinon tunkeutua sisäverkkoon. Tämän takia Zero Trust mallissa aloitetaan purkamaan ajatus luotetuista ja epäluotetuista verkoista siitä lähtökohdasta, että jokaista verkkoa tulee pitää epäluotettavana. Tällöin kiinnittyy huomio verkon sisäiseen suojaukseen täysin erilaisella tavalla, verrattuna castle and moat -malliin. Jos kukaan verkossa ei ole luotettava, myöskään sisäverkon resurssit eivät tulisi olla automaattisesti verkon käyttäjien

saatavilla. Zero Trustin toteuttaminen verkkoon aloitetaan verkon sisäpuolelta kaikista kriittisimmästä verkon osasta, ja seuraavaksi edetään vahvistamaan verkon muita osia. Zero Trustin toteuttaminen ei tapahdu yhdessä yössä, eikä vanhaa tietoturvasuojaa poisteta käytöstä sen toteuttamista varten. Sen sijaan Zero Trustia lähdetään toteuttamaan vahvistamalla omaa ympäristöään Zero Trustia tukevia menetelmiä, teknologioita ja mahdollisesti palveluita käyttäen.

Zero Trustin ”kummisetänä” pidetty John Kindervag on työskennellyt Palo Alto Networks yrityksessä osastoteknologiajohtajana (engl. Field Chief Technology Officer) vuodesta 2017 lähtien. Osastoteknologiajohtajan työnkuva usein tarkoittaa yrityksen tietyn osaston teknologiajohtajaa, jossa pääsee perehtymään lähemmin osaston toimintaan verrattuna koko yrityksen teknologiajohtajaan. Vuonna 2010 Zero Trustin julkaistessaan Kindervag toimi kuitenkin Forrester Researchin varapresidenttinä sekä pääanalyytikkona Forrester Researchin turvallisuus- ja riskitiimissä. Kindervagia usein pidetään jopa maailman johtavimpana tietoturva-asiantuntijana ja hänen kehittelemäänsä Zero Trustia sovelletaan jo useissa suuryrityksissä, kuten Coca Colalla ja Googlella. (Security Roundtable; Smith 2011.)

Zero Trustin tavoitteena on suojata kohteita, esimerkiksi yrityksiä, kehittyneiltä tietoturvahyökkäyksiltä ja myös auttaa yrityksiä saavuttamaan tietoturvasertifikaattien ja säännösten mukaisen ympäristön. Zero Trust koskettaa jokaista suojattavan ympäristön osaa, niin käyttäjiä, verkkoja, tietoja, kuin laitteitakin. Zero Trust tietoturvamallia ei ole mahdollista saavuttaa puoliksi, vaan se vaatii, että jokainen ympäristön osa käydään läpi ja tarvittavat muutokset tehdään tietoturvan vahvistamiseksi. Zero Trustin saavuttamiseksi voidaan määritellä periaatteita, joita käsitellään tarkemmin seuraavassa kappaleessa 4.

4 Zero Trustin periaatteet

Zero Trust on tietoturvan viitekehys (engl. framework). Zero Trustia ei siis voi rakentaa yksittäisellä tuotteella tai palvelulla, vaan koko infrastruktuuri ja sen osat sekä niiden suojaus täytyy olla rakennettu lähtökohtana Zero Trust-ajatus. Vahvempaa tietoturvamallia kannattaa alkaa tavoittelemaan keskittymällä suojauksen parantamiseen mahdollisimman pieni osa kerrallaan, eikä pyrkiä rakentamaan Zero Trust suojausta verkkoon yhdessä päivässä.

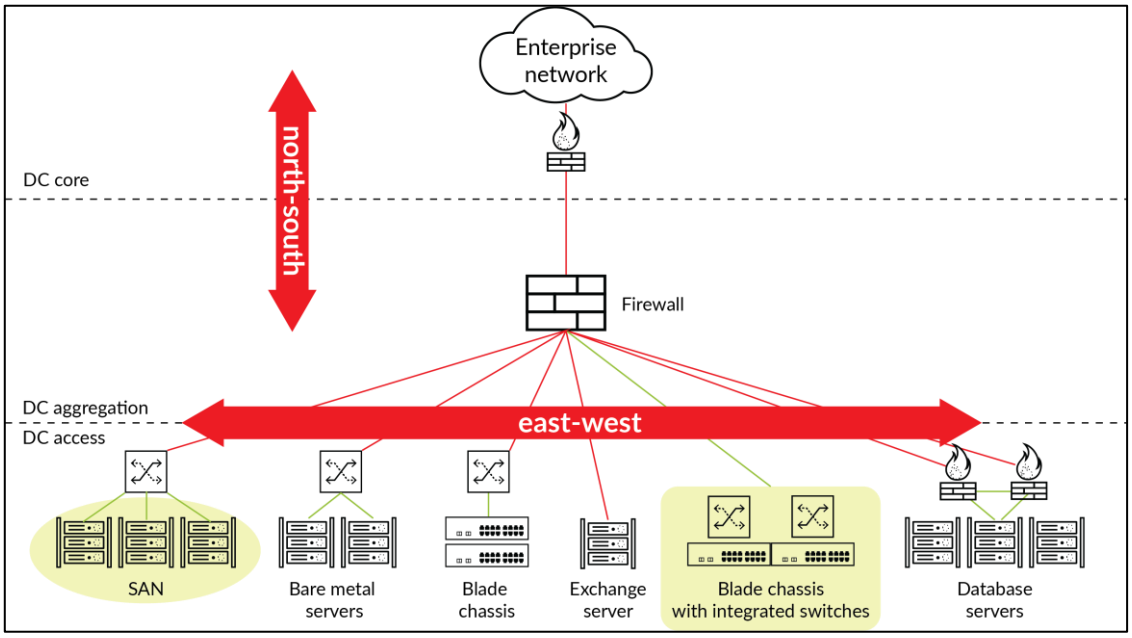
Zero Trust mallista sekä sen toteuttamismahdollisuuksista on usealla eri yrityksellä oma näkemyksensä. Mallin tarkoitus onkin skaalautua mahdollisimman monen erilaisen yrityksen infrastruktuuriin ja olla sovellettavissa kaiken kokoisiin yrityksiin ja sen käyttämiin palveluihin ja resursseihin. Zero Trust toteutuksen kokonaisuus tietoturvan vahvistamiseksi voi olla täysin erilainen riippuen tuotteista, palveluista ja teknologioista, jotka ovat suojattavan kohteen käytössä. Zero Trust malli pyritään kuitenkin määrittelemään sen saavutusta tukemien periaatteiden mukaan, mitkä myös vaihtelevat usein riippuen siitä kuka ne määrittelevät. Periaatteet voi rajata esimerkiksi kolmeen perusperiaatteeseen, mutta joillekin Zero Trust voi merkitä vaikka 10 eri periaatetta, joita seuraamalla Zero Trust saavutetaan. Kaikissa näissä periaatteissa on yleensä kuitenkin samoja ajatuksia, mutta ne saattavat olla esitettynä eri tavoilla ja erilaisina kokonaisuuksina.

Seuraavissa kappaleissa esittelen tarkemmin kolme Zero Trustin oleellista periaatetta; mikrosegmentointi, pääsynvalvonta ja monitorointi. Mikrosegmentaatiossa oleellisinta on määritellä yksityiskohtaisesti yrityksen koko IT-ympäristö ja erotella samanlaiset osat omiin kokonaisuuksiinsa. Mikrosegmentoitu ympäristö tukee kustomoidun ja dynaamisen pääsynvalvonnan toteuttamisen jokaiseen ympäristön tarkasti määriteltyihin resurssiin, jolloin voidaan rajata pääsy resursseihin noudattamalla minimioikeuksien periaatetta (engl. principle of least privilege). Jotta edellä kuvailtua ympäristöä voidaan ylläpitää ja kehittää tehokkaasti ja luotettavasti, täytyy suorittaa jatkuvaa monitorointia ja lokin keräämistä. Seuraavissa kappaleissa esittelen tarkemmin edellä kuvaillut periaatteet ja niihin liittyviä tekniikoita sekä menetelmiä.

4.1 Mikrosegmentaatio

Perinteistä segmentointia on tehty verkoissa jo pitkään, millä on muun muassa keskitytty käyttäjän ja palvelimen välisen liikenteen suodattamiseen ja suojaamiseen. Tätä liikennettä kutsutaan pohjoinen-etelä suuntaiseksi liikenteeksi (kuvio 1), kun liikenne

kulkee sisäverkon resurssin, ja ulkoverkossa olevan käyttäjän välillä. Segmentoinnin avulla tavoitellaan myös parantamaan verkon suorituskykyä sekä sen hallintaa. Mikrosegmentoinnin tavoitteet Zero Trustissa sen sijaan ovat täysin eri lähtökohdista suunniteltu, kuin perinteisen segmentoinnin tavoitteet. Mikrosegmentoinnilla tarkoitetaan segmentoinnin tapaan datan erottelua toisistaan omiksi erillisiksi kokonaisuuksiksi, mutta erona perinteiseen segmentointiin, mikrosegmentoinnin tavoitteena on keskittyä paljon yksityiskohtaisemmin yhä tarkemmin rajatumpien osien riskien ja turvallisuuden hallintaan. Mikrosegmentoinnilla halutaan ehkäistä hyökkääjien mahdollisuuksia liikkua verkossa lateraalisesti eri resurssien välillä, mikäli hyökkääjä on jo onnistunut saamaan itsensä verkon sisälle. Lateraalista liikkumistapaa voidaan kuvailla myös länsi-itä suuntaiseksi liikkumiseksi (kuvio 1), jolloin liikenne kulkee verkon sisällä eri resurssien, esimerkiksi palvelimien välillä. Kuten castle and moat mallin heikkouksia tutkittaessa kävi ilmi, suojauksen puuttuminen lateraalisesti leviäviä hyökkäyksiä kohtaan on mahdollistanut suuren osan vakavimmista ja laajimmista tietoturvahyökkäyksistä. ICT-alan tutkimus- ja konsultointiyritys Gartnerin blogikirjoittaja Beadle myös huomioi tämän vuonna 2018 kirjoittamassaan blogikirjoituksessaan, jossa hän listasi mikrosegmentoinnin yhdeksi tärkeimmistä projekteista, mikä tietoturvajohtajien kannattaisi toteuttaa edistääkseen yrityksensä tietoturvaa. Lateraalisessa liikkumistavassa hyökkääjät pääsevät liikkumaan verkon eri resurssien välillä käyttämällä hyödyksi luottamusta, jonka he ansaitsevat päästessään sisään verkkoon. (Friedman 2017; Palo Alto Networks.)



Kuvio 1. Verkon liikenteen eri suuntia havainnollistettuna (Palo Alto Networks)

Mikrosegmentointi sekä sitä kautta myös muut tässä opinnäytetyössä määritellyistä Zero Trustin periaatteista lähtevät siitä, että määritellään mitä sekä minkälaisia resursseja ympäristössä on. Ei ole itsestäänselvyys, että jokainen yritys tietäisi, tai että heillä olisi

edes tarpeeksi kattavaa ja helposti saatavilla olevaa näkyvyyttä määritelläkseen jokaisen verkon tai ympäristön laitteen ja resurssin. Tietoturva-ammattilaisten mukaan juuri näkyvyyden puuttuminen verkossa on yksi suurimpia esteitä, joka hankaloittaa ammattilaisten pyrkimystä aloittaa työskentely kohti mikrosegmentoitua ympäristöä. Mikrosegmentoinnin tarkoituksena on jakaa yrityksen ympäristön ja verkon resurssit eroteltuihin kokonaisuuksiin niin, että samanlaiset resurssit kuuluvat omaan osaansa. Samanlaisilla resursseilla tarkoitetaan esimerkiksi sellaisia kohteita, joilla on keskenään samanlainen käyttötarkoitus. Kuviossa 1 olevat palvelimet ovat eroteltuna toisistaan niin, että käyttäjä ei pääse suoraan liikkumaan eri tehtäviin liittyvien palvelimien välillä. Tämän tavoitteen takia on oleellista, että resurssit ja niiden toiminta tunnetaan perinpohjaisesti ennen kuin mikrosegmentointia aletaan tehdä ja suojausta rakentaa eroteltujen osien ympärille. Etenkin on kriittistä tietää, mitä yhteyksiä verkon resurssit tarvitsevat keskenään ja miten nämä eri resurssit kommunikoivat verkon ulkopuolelle. (Bednarz 2019; Chickowski 2019.)

Mikrosegmentoinnissa pyritään verkkokerroksien OSI-mallin (kuvio 2) kerroksen 7, eli sovelluskerroksen tasolla toteutettavien mikrosegmenttien suojaukseen. Perinteisessä segmentoinnissa keskitytään kuljetuskerrokseen 4, jossa oleellisimpina suojauksina toimivat liikenteen suodattaminen esimerkiksi palomuurien avulla, sekä porttien hallinnointi. Nykypäivän hyökkäysmenetelmät ovat kuitenkin jo niin kehittyneitä, että resurssien suojaaminen pelkän kuljetuskerroksen tasolla ei estä hyökkääjiä pääsemästä läpi suojattavaan kohteeseen. Zero Trustissa halutaan keskittyä jokaisen OSI-mallin verkkokerroksen turvaamiseen erikseen. Tuomalla suojaus sovelluskerrokseen asti, pystytään suojaamaan tehokkaammin ja turvallisemmin pienempiä kokonaisuuksia, jotka voivat kuulua esimerkiksi fyysisiin palvelimiin, virtuaalikoneisiin ja pilvipalveluihin. Mikrosegmentaation avulla suojauksesta voidaan rakentaa dynaaminen osa ympäristöä, joka mahdollistaa myös sen nopean kehityksen yrityksen muun kehitystahdin mukana. (Givati 2018.)

Kuvio 2. Verkon OSI-malli (Vahtera 2018)

Mikrosegmentoinnin vahvuutena osana Zero Trustia on se, että se mahdollistaa yksityiskohtaisesti muodostetun suojauksen rakentamisen eri mikrosegmenttien ympärille. Ennen suojauksen rakentamista tulee kuitenkin analysoida ja perehtyä suojattavan sisällön liikennöintiin sisäverkossa sekä ulkoverkossa. Jos mikrosegmentointia lähtee toteuttamaan liian suppealla tiedolla suojattavien resurssien vaatimuksista, voi se johtaa esimerkiksi yllättäviin katkoksiin resurssien saatavuudessa. Tilanne on hyvin mahdollinen, jos vahingossa puutteellisen analyysin takia suojauksella estetään jotkin tarvittavat yhteydet. Resurssien analysoiminen voi olla haaste yritykselle, mikäli aiemmin tässä luvussa yleiseksi todettu näkyvyyden puuttuminen verkon tietoihin on olemassa oleva ongelma. (Chickowski 2019.)

Kun mikrosegmentin sisällä olevien resurssien käyttötarkoitus sekä liikennöiminen on saatu analysoitua huolellisesti, voidaan tämän segmentin suojaus rakentaa ottaen huomioon vain tarvittavat ominaisuudet. Tällöin voidaan rajoittaa kaikki muu, mitä ei tarvita toiminnallisuuteen. Edellä kuvailtua toimintatapaa kutsutaan minimioikeuksien periaatteeksi (engl. principle of least privilege), joka tarkoittaa, että käyttäjällä, laitteella, ohjelmalla tai millään muullakaan verkon kanssa kommunikoivalla tekniikalla tulee olla vain ne minimioikeudet, jotka tämä tarvitsee suorittamaan tehtäväänsä. Minimioikeuksista voidaan käyttää myös nimitystä vähimmäisoikeudet. Mikrosegmentointia toteuttamaan lähtiessä verkon analyysin perusteella, tulee suojausta lähteä parantamaan niistä osista, jotka sisältävät kaikista sensitiivisintä dataa tai ovat muuten yrityksen kriittisimpiä resursseja. Aloittaessa lähdetään lisäämään tietoturvakerroksia sisäverkkoon, eikä olemassa olevia suojauksia vähennetä tai poisteta sitä varten. (Bednarz 2019.)

Mikrosegmentoinnin tärkeyttä ei saa unohtaa myöskään niiden verkkolaitteiden kohdalla, joita ei ensisijaisesti pidettäisi ympäristön tietoturvariskeinä. Esimerkiksi monen yrityksen verkossa liitettynä oleva printteri voi tarjota potentiaalisia hyökkäysvektoreita hyökkääjille. Myös muut IoT-laitteet, kuten esimerkiksi kamerat, tarjoavat potentiaalisia väyliä edetä eteenpäin yrityksen verkossa. Myös mahdollisissa yrityksen käyttämissä pilvipalveluissa tulee tehdä mikrosegmentoinnin eteen tutkimusta palvelun tarjoamista mahdollisuuksista rajata käyttäjien pääsyä erilaisiin datakokonaisuuksiin. Mikrosegmentaatio edistää Zero Trustia silloin, kun se tehdään huolella eikä mitään ympäristön osia jätetä analysoimatta. Mikrosegmentaation valmistelu auttaa yritystä saavuttamaan näkyvyyttä ympäristöönsä, ja sen toteutus mahdollistaa yritykselle edistyneet tavat suojata eri segmentit vahvalla autentikoinnilla ja pääsynvalvonnalla.

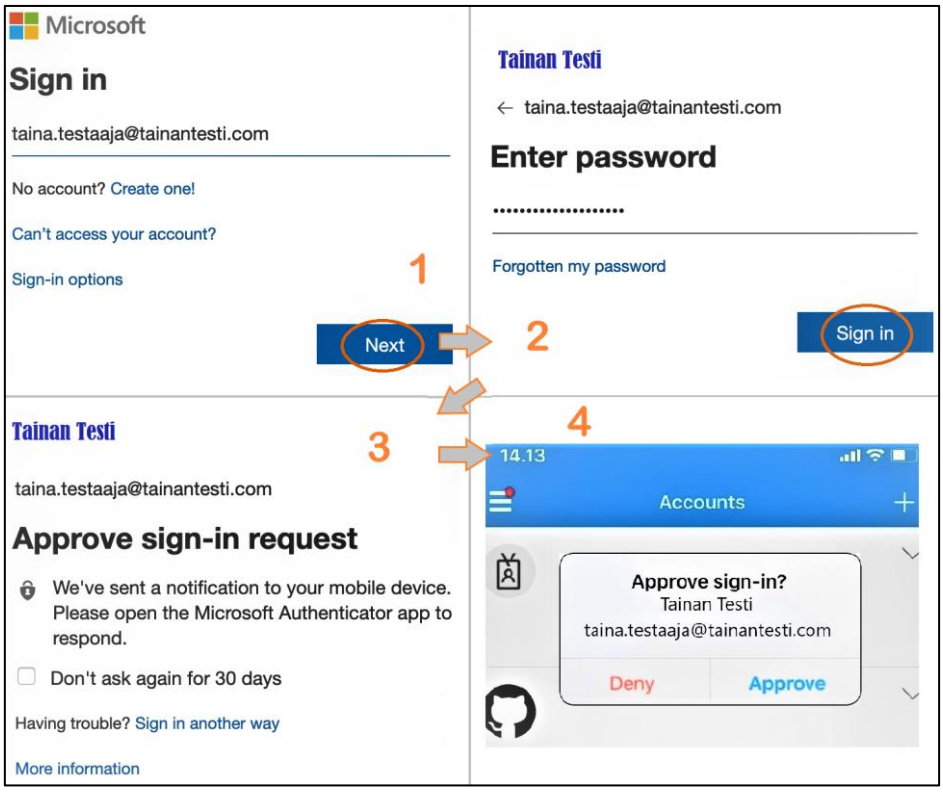
4.2 Autentikointi ja pääsynvalvonta

Zero Trustin keskeisimpiä periaatteita on pyrkiä kohti Zero Trustin mottoa ”Never trust, always verify” (suom. Älä ikinä luota, varmista aina). Tämä tarkoittaa sitä, että yhteenkään käyttäjään, laitteeseen, verkkoon tai muuhun ei ensisijaisesti luoteta, vaan esimerkiksi käyttäjän täytyy aina uudestaan todistaa olevansa oikeutettu halutessaan päästä tiettyihin palveluihin tai resursseihin. Verkon sisältä tuleviin pyyntöihin ei luoteta sen enempää kuin ulkopuolelta tuleviin pyyntöihin, eikä käyttäjälle anneta pääsyä vain sen takia, että se on samassa yksityisessä verkossa. Zero Trustin mukaan myöskään perinteistä käyttäjä-salasanayhdistelmäistä autentikointia ei enää pidetä riittävänä, vaan käyttäjät siirretään käyttämään vahvempia autentikointiprosesseja. (Chow 2017.)

Vahvemman autentikaatioprosessin toteuttaminen edellyttää, että käyttäjän identiteetin todennus voidaan tehdä useampaan erilaiseen varmennukseen pohjautuen, käyttäjätunnuksen ja vahvan salasanan lisäksi. Identiteetin autentikoimisella halutaan varmistua siitä, että henkilö, joka yrittää päästä sisään palveluun tai muuhun resurssiin on juuri se, kuka hän väittää olevansa. Kirjautumiseen voidaan lisätä eri vaiheita, jotka oletetaan olevan saatavilla vain tällä kyseisellä käyttäjällä, ja joihin käsiksi pääseminen on hankalaa ulkopuolisille. Kirjautuminen voidaan myös hyväksyä tai hylätä sen perusteella, miltä laitteelta käyttäjä yrittää kirjautua. Kuluttajienkin keskuudessa yleistynyt teknologia kirjautumisprosessin vahvistamiseksi on monivaiheinen todennus (engl. Multi-Factor Authentication), jossa voidaan käyttää esimerkiksi mobiiliapplikaatioon saapuvaa koodia tai ilmoitusta salasanan lisäksi (kuvio 3). Monivaiheisen todennuksen osana voi toimia myös biometrinen tunnistautuminen, kuten sormenjälki, tai SMS-viestiin tai toiseen sähköpostiin saapuva varmennusviesti. Guida (2019) on kuitenkin vertaillut artikkelissaan eri tapoja ja todennut SMS-viestit, sekä toisen sähköpostiosoitteen heikoimmiksi ja helpoiten hyökkääjien saavutettavissa oleviksi menetelmiksi monivaiheisen todennuksen osana. Tapaus voi olla esimerkiksi se, että hyökkääjä on jo onnistunut kaappaamaan toisen sähköpostitilin ja onnistuu sitä kautta pääsemään käsiksi myös sinne saapuvaan monivaiheisen todennuksen varmistuskoodiin. Monivaiheisesta todennuksesta kirjoitetaan ja puhutaan usein myös lyhenteellä MFA, joka tulee sen englanninkielisestä nimestä. (Trulioo 2018; Atlassian.)

Laitteen perusteella autentikoitaessa halutaan identiteetin lisäksi varmistaa, että käyttäjä pääsee kirjautumaan palveluihin vain tunnetulta laitteelta, jonka tietoturvataso voidaan varmistaa. Tämän mahdollistamiseksi laite tulee olla liitettynä yrityksen laitehallintajärjestelmään (engl. Mobile Device Management). Laitehallintajärjestelmän avulla yritys voi monitoroida ja hallinnoida liitettyjen mobiililaitteidensa ja tietokoneidensa

tietoturvatasoa. Laitteille voidaan määrittää käytettävän laitehallintajärjestelmän mukaan useita tietoturvavaatimuksia, joita laitteen tulee noudattaa ollakseen hyväksytty. Laite voidaan päästää kirjautumaan resursseihin esimerkiksi sen perusteella, onko käyttäjän laitteen tietoturva vaatimusten tasolla vai ei, tai ylipäätänsäkään edes liitettynä osaksi yrityksen laitehallintajärjestelmää. Järjestelmän avulla voidaan käyttäjille toteuttaa myös vähimmäisoikeus-periaatetta rajoittamalla tiettyjen laitteiden pääsyä eri palveluihin. Vähimmäisoikeudet käyttäjille sallimalla, yrityksen käyttäjät pääsevät kirjautumaan laitteillaan vain niihin palveluihin ja resursseihin, joita he tarvitsevat työnsä tekemiseen. Laitehallintajärjestelmän avulla voidaan varmistaa, ettei käyttäjä pääse kirjautumaan esimerkiksi omalta henkilökohtaiselta tietokoneeltaan tai puhelimeltaan yrityksen kriittisiin palveluihin. (Atlassian; Continuum Product Team 2019.)



Kuvio 3. Monivaiheinen todennus, jossa käytetään lisänä Microsoft Authenticator mobiiliapplikaatioon saapuvaa ilmoitusta

Laitehallintajärjestelmän tukena toimii järjestelmä, joka sisältää käyttäjät sekä käyttäjäryhmät. Markkinoilla on ratkaisuja, jotka tukevat käyttäjä- sekä laitehallintaa samalla alustalla. Esimerkkinä tällaisesta palvelusta on Microsoft Azure, joka tarjoaa useita eri palveluja IT-infrastruktuurin hallinnan alustaksi tai tueksi. Samaa palvelua käyttäessä integraatio ja dynaamisuus on luotettavampaa, mutta monet järjestelmät ovat integroitavissa toisiinsa ja yhä useampiin erilaisiin resursseihin. Järjestelmän käyttäjäryhmät tulisi rakentaa niin, että Zero Trustin kannalta on myös tarpeellista, että käyttäjät ovat rajattu ryhmiin arvioiden käyttäjien tarvitsemaa pääsyä, esimerkiksi tiimiä tai

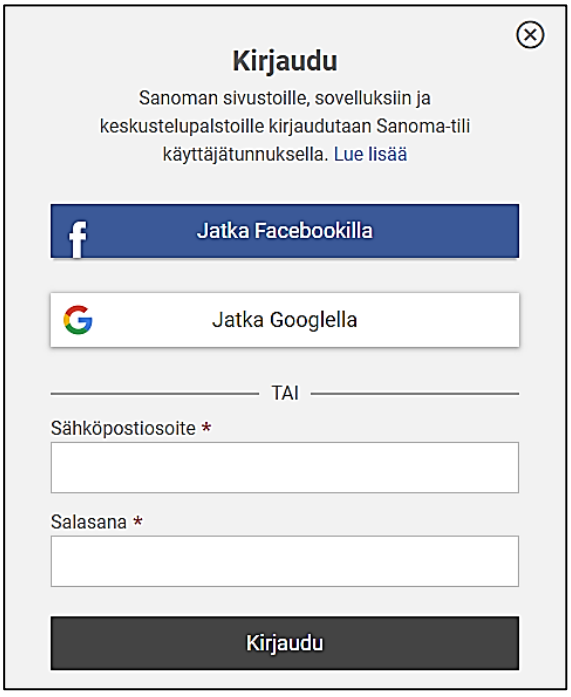
positiota yrityksessä. Jos yrityksellä on käyttäjäryhmiä, voidaan näitä ryhmiä käyttää myös rajoittamaan pääsyä eri palveluihin tai resursseihin. Yksittäisten käyttäjien rajoittaminen varsinkin mikrosegmentoidussa ympäristössä olisi työlästä, sillä mikrosegmentaatio tarjoaa pääsyn rajoituksille useita eri kohtia. Käyttäjäryhmien käyttäminen pääsynvalvonnassa on myös paljon skaalautuvampaa, jos sitä sovelletaan dynaamiseen ympäristöön. Käyttäjällä tai laitteella ei tule olla mitään muita oikeuksia kuin ainoastaan ne, joita tarvitsee tarkoitetussa toiminnassa.

Mikrosegmentoitu ympäristö sekä järjestelmä, johon on liitettynä yrityksen laitteet sekä käyttäjät, mahdollistavat yritykselle lähtökohdan rakentaa ja ylläpitää dynaamista pääsynvalvontaa (engl. access control) yrityksen palveluihin ja resursseihin. Pääsynvalvonta mahdollistaa käyttäjien pääsyn rajoittamisen palveluihin, joita he eivät tarvitse työnsä tekemiseen. Myös eri palveluissa pääsynvalvontaa tehdään niiden sisällä, ja varmistetaan etteivät käyttäjät pääse sellaisiin palvelun osiin, jotka eivät ole tarkoitettu heille. Tarkasti rajoitetun pääsynvalvonnan etuna on hallinnointiin kuluvan työmäärän vähentymisen lisäksi se, että jos käyttäjätili onnistutaan kaappaamaan, efekti ei ole yhtä suuri kuin se voisi olla, jos käyttäjälle ei olisi rajoitettu mitään palveluita. Zero Trustia tavoitellessa käyttäjien tulee aina autentikoitua uudestaan, kun käyttäjä yrittää päästä palveluun tai muuhun resurssiin. (Cloudlfare.)

Käyttäjien pääsyä arvioidaan sen perusteella, mitä he tarvitsevat työnsä tekemiseen. Käyttäjän pääsyn voi määritellä hänen roolinsa perusteella, jota kutsutaan rooliperustaiseksi pääsynvalvonnaksi (engl. Role-Based Access Control, RBAC). Yrityksessä voi olla useita eri rooleja, ja ne voidaan määritellä joko henkilön position mukaan tai tiimin mukaan. Henkilön positio voi olla esimerkiksi ylläpitäjä tai käyttäjä. Näiden kahta voidaan vielä tarkentaa esimerkiksi osaston tai tiimin perusteella. Käyttäjäryhmien käyttäminen hyödyksi rooliperustaisessa pääsynvalvonnassa helpottaa ylläpitäjien työtä, mikäli uusi työntekijä saapuu yritykseen tai olemassa oleva työntekijä vaihtaa työtehtävää yrityksen sisällä. Rooliperustainen pääsynvalvonta tarjoaa myös loogisen määrittelyn käyttäjän oikeuksista ja yrityksen on näin helpompaa sekä skaalautuvampaa toimia ja mahdollisesti todistaa tietoturvatasoaan ulkopuolisille auditoijille. (Covington 2019; Zhang 2019.)

Rooliperustaisesta pääsynvalvonnasta on myös kehitelty vielä useampia attribuutteja huomioon ottavia tekniikoita (engl. Attribute-Based Access Control, ABAC), jotka arvioivat käyttäjän roolin lisäksi myös esimerkiksi päivämäärää, kellonaikaa, käyttäjän lokaatiota ja datan tyyppiä, mihin käyttäjä haluaa päästä. Mikäli käyttäjä täyttää kaikki attribuuttien vaatimukset, vasta sen perusteella hänelle myönnetään pääsy. (Covington 2019.)

Keskitetyt käyttäjähallintajärjestelmät mahdollistavat yritykselle kertakirjautumisen käyttämisen. Kertakirjautuminen (engl. Single-Sign On, SSO) on "pääsynvalvonnan toteutustapa, jossa käyttäjä pääsee yhdellä tunnistautumisella kaikkiin saman pääsynvalvonnan piirissä oleviin palveluihin ja resursseihin käyttövaltuuksiensa puitteissa" (VAHTI 8/2008, 49). Kertakirjautumisen ydin on siis siinä, että käyttäjä tarvitsee vain yhden tunnuksen kirjautuakseen yrityksen kaikkiin resursseihin, myös yrityksen käytössä oleviin kolmannen osapuolen tarjoamiin palveluihin. Kertakirjautuminen tukee dynaamista ympäristöä, sillä sen avulla voidaan päivittää käyttäjän tietoja käyttämällä vain yhtä palvelua, joka tarjoaa kertakirjautumisen yritykselle. Esimerkiksi Microsoftin ja Googlen tunnukset tarjoavat yrityksille mahdollisuuden konfiguroida yrityksen muut resurssit hyväksymään kirjautumisen näitä tilejä käyttämällä sekä synkronoimaan käyttäjätiedot kertakirjautumisen tarjoavalta palvelulta. Tämän mahdollistamiseksi kuitenkin myös palvelussa täytyy olla mahdollisuus ulkoistaa kirjautuminen toiselle osapuolelle, kuten mainituille Microsoftille tai Googlelle. Monelle kuluttajalle tuttu tapa kertakirjautumisen tarjoavasta palvelusta on Facebook, jolla pystyy tänä päivänä kirjautumaan usealle eri web-sivustolle, joka ei välttämättä liity muuten Facebookiin. Esimerkiksi Helsingin Sanomien sähköinen kirjasto, Sanoma, hyväksyy Googlen ja Facebookin ulkoisina identiteetintarjoajina kirjautumisprosessissa (kuvio 4). Jos kertakirjautuminen on käytössä palveluihin, niin yrityksen ei tarvitse hallinnoida käyttäjätilien lisäämistä ja poistamista palveluista erikseen, vaan hallinnointi suoritetaan kertakirjautumisen tarjoavasta palvelusta. Rooliperustaisen pääsynvalvonnan avulla voidaan automaattisesti antaa tietyille käyttäjäryhmille oikeuksia eri palveluihin, jotka kertakirjautumisen avulla voidaan synkronoida kohdepalveluun. Kestävät säännöt rakentamalla ylläpitäjien työmäärä ei kasva, vaikka käytössä olisikin useita erillisiä palveluita useilla eri käyttäjäoikeustasoilla. (Kuparinen 2018.)



Kuvio 4. Sanoman tarjoamat kirjautumisvaihtoehdot (Sanoma.fi)

Kertakirjautumisen toteuttamisessa saadaan huomattavasti parannettua yrityksen tietoturvaa, sillä vahva tunnistautumisprosessi määritellään kertakirjautumisen palveluun ja tämä on ainoa, jota käyttäjän tarvitsee käyttää, vaikka yrityksellä olisi useita erilaisia palveluita. Jokainen erillinen tunnus ja salasana ovat hyökkäysvektoreita, joita voidaan hyödyntää pahaenteisissä aikeissa. Kertakirjautuminen on nykyään haluttu ja suosittu teknologia, jolla yritysten on helppo rahastaa tuotteistaan lisäkuluja. Palvelut voivat itse päättää, tarjoavatko he asiakkailleen mahdollisuutta konfiguroida kertakirjautumista vai ei. Mikäli he päättävät tehdä siitä mahdollisuuden, se useimmiten sisältyy jonkin tietyn asiakastason ominaisuuksiin, mikä useimmiten on se kaikista kallein vaihtoehto. Kertakirjautumisen lisähinnoittelu vähentää sen imagoa tietoturvaelementtinä, mutta on ennemminkin käsitelty luksuselementtinä. Jos palvelut markkinoivat itseään tietoturvallisena yrityksenä, heidän tulisi sisällyttää myös tietoturvaa tarjoava kertakirjautuminen automaattisesti palveluihinsa. Kertakirjautumista tarjoavista yrityksistä on tehty Wall of Shame-sivusto (https://sso.tax/), jossa listataan palveluita, joissa kertakirjautumisesta täytyy maksaa huomattavasti enemmän kuin peruslisenssistä. Sivulla käy ilmi, että peruslisenssin ja kertakirjautumisen sisältävän lisenssin hintaero voi olla jopa 6300 %. (robchahin 2018.)

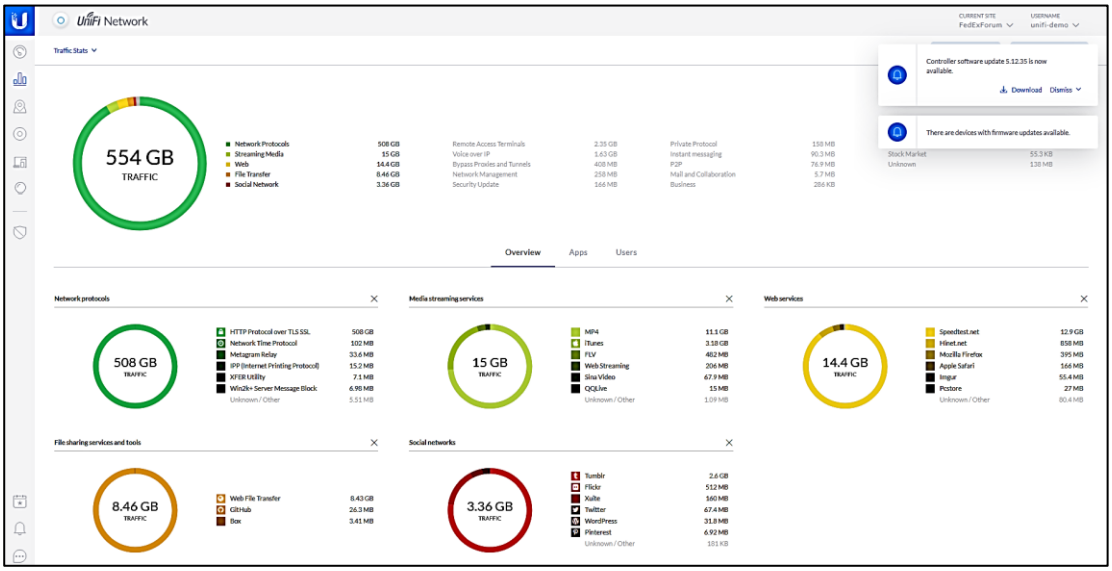
Mikrosegmentaatio ja moniulotteinen pääsynvalvonta muodostavat kompleksin ympäristön, mutta mikäli ne ovat tarkasti suunniteltu ja skaalautuvasti toteutettu, ne palvelevat yrityksen tietoturvaa ollen kustannustehokas ja helppo hallita. Silti ympäristöä täytyy kuitenkin ylläpitää ja sen yhteyksiä seurata. Seuraavassa kappaleessa käsitellään monitorointia Zero Trustin osana, mikä viimeistelee tässä opinnäytetyössä kuvaillut Zero Trustin perusperiaatteet.

4.3 Monitorointi

Monitoroinnilla tarkoitetaan Zero Trustin yhteydessä IT-ympäristön tietoturvamonitorointia, joka sisältää datan keräämistä yrityksen koko ympäristöstä, sekä sen jatkuvaa analysointia. Nykyaikaisessa ympäristössä laitteet ja palvelut ovat alttiimpia tietoturvahyökkäyksille kuin aikaisemmin, sillä nykypäivänä pilvipalvelujen käyttö on yleisempää ja työlaitteita kuljetetaan mukana useissa eri paikoissa, johtaen siihen, että myös palveluihin kirjaudutaan vaihtuvista eri sijainneista. Tämän takia Zero Trust-mallissa monitoroinnin keskiössä tulisi olla laitteet sekä palvelut, sillä näiden välillä kaikista kriittisin liikenne liikkuu. Zero Trust-mallissa laitteiden monitorointi tulisi tapahtua laitteeseen asennetun ohjelman kautta, jolloin laitetta voidaan monitoroida sijainnista riippumatta, kunhan se on yhteydessä verkkoon. (National Cyber Security Centre 2019.)

Vaikka kaikkia verkkoja tulee Zero Trust-mallissa pitää epäluotettavina, niiden monitorointi sekä analysointi tarjoaa silti yritykselle paljon etuja. Verkkoliikenteen analysointi voi tapahtua automaattisesti, ja kuten myös Zero Trustin muissakin osa-alueissa, kaikki poikkeava liikenne yrityksen ympäristössä tulisi tutkia tarkemmin, jotta mahdollisiin vika- tai häiriötilanteisiin voidaan reagoida nopeasti. Verkon monitorointiin on kehitetty palveluita, ja nykypäivänä monen yrityksen tietoturvapolitiikkaan sisältyy turvatietojen- ja tapahtumien hallintajärjestelmä eli SIEM (engl. Security Information and Event Manager). SIEM kerää tietoja useasta eri järjestelmästä yhtäaikaisesti ja puolustaa yritystä erilaisilta tietoturvauhilta analysoimalla automatisoidusti liikennettä reaaliaikaisesti. Poikkeustilanteissa tehokas SIEM-järjestelmä reagoi nopeasti lähettämällä hälytyksen yrityksen vastaaville, jotka voivat tutkia hälytyksen syytä tarkemmin. SIEM toimii yrityksen apuna myös ilmoitusvelvollisuuksissa, jotka kohdistuvat yrityksiin esimerkiksi GDPR-tietosuoja-asetuksen kautta, mikä velvoittaa yritystä tarkkailemaan ja säilyttämään lokia käyttäjien pääsystä järjestelmiin, jotka sisältävät henkilötietoja. Myös tietoturvasertifikaatit, kuten ISO27001 voivat velvoittaa sertifikaatin hakijan, sekä haltijan, valvomaan ja tilanteen vaatiessa jäljittämään liikennettä. Jäljittävyyden takaamiseksi SIEM usein sisältää myös keskitetyn lokienhallinnan, joka järjestää tapahtumat loogiseen järjestykseen. Lokitiedoista voi mahdollisesti saada muunnettua hyödyllisiä ja kustomoituja raportteja, jota yritys voi käyttää tilanteen kartoittamiseen tietyltä aikaväliltä. (Kaita.)

Verkon monitorointi lisää näkyvyyttä verkkoon ja helpottaa yritystä hahmottamaan ympäristöään kokonaisuudessaan. Jotkin verkkolaitteiden valmistajat tarjoavat suoraan tuotteiden mukana kattavan ohjelman verkon hallintaan ja liikenteen seurantaan. Esimerkiksi Ubiquiti on yritys, joka tarjoaa verkkolaitteita, jotka ovat yhdistettävissä Ubiquitin omaan kontrollointiohjelmistoon (kuvio 5). Verkon monitoroinnin merkitys lisääntyy, Zero Trust-ympäristöissäkin, samaan aikaan, kun IoT-laitteiden määrä yrityksissä kasvaa. Jotkin IoT-laitteet voivat olla kriittinen osa yrityksen tietoturvapolitiikkaa, kuten kamerat. Tällöin painoarvo niiden monitorointiin kasvaa, vaikka ne olisivatkin suojattu vahvoin menetelmin. Jokainen verkkoon kytketty laite on uusi potentiaalinen hyökkäysvektori. Kun verkkoon kytkettyjen laitteiden määrä lisääntyy, myös analysoitavan liikenteen monitorointi käy monimutkaisemmaksi ja työläämmäksi. Tämän takia on hyödyllistä, että yrityksen verkon analysointia tekevällä henkilöstöllä on käytössään tehokas ohjelma tai palvelu, joka tukee heidän työtään. Samalla vähenee henkilöstön tarve ymmärtää jokaista teknistä yksityiskohtaa yhtä tarkasti ja heillä jää enemmän aikaa keskittyä sen sijaan tutkimiseen, kun järjestelmä hoitaa suurimmaksi osaksi poikkeustilanteiden hälytykset. (Blesa 2019; Ubiquiti.)



Kuvio 5. Ubiquitin Unifi Controller-demosivulla voi testata hallintasovelluksen käyttöliittymää (Ubiquiti Unifi Controller Demo)

Kuten ensimmäisessä kappaleessa jo kerrottiinkin, Zero Trustissa monitoroinnin pääkohteena ovat yrityksen laitteet sekä palvelut, vaikka verkon monitorointi voi olla oleellinen osa niitä. Laitteita hallinnoidaan laitehallintajärjestelmän kautta, jonka tulisi ilmoittaa aina, jos jokin laite ei vastaa sille asetettuja vaatimuksia. Jos pääsynvalvonnan säännöt ovat konfiguroitu onnistuneesti, niin tällöin kyseinen käyttäjä, jonka laite ei ole vaatimusten mukainen, ei pääse myöskään kirjautumaan palveluihin, joiden ehtoina ovat hyväksytty laitteen tietoturvataso. Ilmoituksesta yrityksen ylläpitäjä voi alkaa tutkimaan asiaa mahdollisimman nopeasti ja korjata ongelman ilman, että siitä aiheutuu pitkäksi ajaksi haittaa käyttäjälle. On myös erittäin tärkeää, että laitteiden käyttöjärjestelmäpäivitykset pysyvät ajan tasalla, sillä ne voivat sisältää erittäin kriittisiä päivityksiä tietoturvan osalta. Esimerkiksi Microsoftin tammikuussa 2020 julkaisemat tietoturvapäivitykset Windows-käyttöjärjestelmän versioille sisälsivät 49 korjausta, joista 8 oli luokiteltu vakaviksi kriittisiksi korjauspäivityksiksi (Soare 2020). (National Cyber Security Centre 2019.)

Palveluiden monitorointi sisältää myös laitehallinnan tavoin päivitysten ajankohtaisuuden seuraamista. Myös nykypäivän ympäristössä, jossa myös palvelut ovat liitettynä toisiinsa jollain tapaa, tulee seurata myös niiden välisiä yhteyksiä. Niissä palveluissa, jossa kertakirjautumista ei ole mahdollista toteuttaa, tulee vahva autentikointi olla jollain muulla tavoin saavutettavissa ja sen toteutuminen tulee varmistaa pakottamalla sääntö kaikille käyttäjille. Palveluiden käyttöä tulee myös yleisesti valvoa poikkeavuuksien varalta, sillä poikkeavuudet normaalissa käytössä voivat olla seurauksia haitallisesta toiminnasta palvelussa. Markkinoilla on tarjolla järjestelmä, joka keskittyy applikaatioiden hallintaan, mikä monitoroi esimerkiksi sovelluksien käyttöastetta ja mistä voi testata miltä näyttää

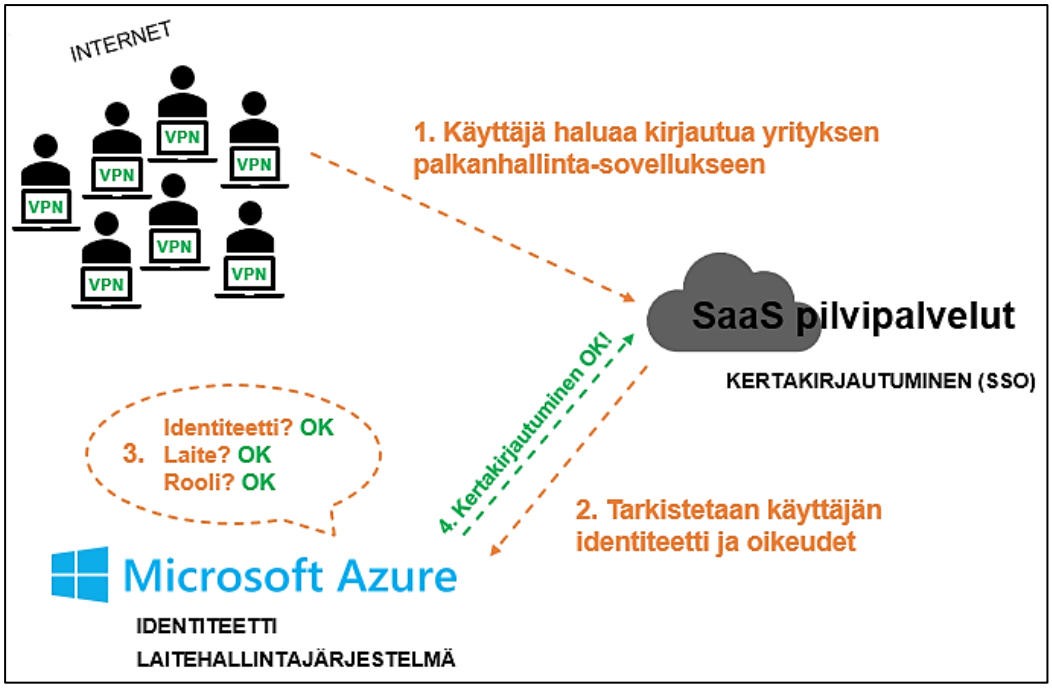
tavallisen käyttäjän käyttäjäkokemus ja pääsy yhdistettyihin sovelluksiin. Kyseinen ratkaisu skaalautuu yrityksen itse kehittämille, sekä kolmannen osapuolen tarjoamille, yrityksen käytössä oleville sovelluksille. Järjestelmään on myös mahdollisuus yhdistää koko yrityksen verkko, jolloin ylläpitäjän on helppo nopeasti tarkistaa onko vika itse sovelluksessa, yrityksen omissa yhteyksissä vai ehkä käyttäjässä. Tällöin mahdolliset sovelluksen hidastelut tai muut ongelmat käytössä voidaan selvittää tehokkaasti ja poissulkea nopeasti huolet tietoturvahyökkäysten uhasta. (AppNeta; Armstrong; National Cyber Security Centre 2019.)

Zero Trust keskittyy rakentamaan tietoturvaa analysoimalla sitä, miten data verkossa liikkuu. Tällöin opitaan miltä normaali liikenne verkossa näyttää, mikä on hyödyksi silloin, jos verkossa esiintyy haitallista liikennettä, joka todennäköisesti poikkeaa normaalista liikenteestä. Näin voidaan parantaa myös tulevaisuudessa verkon suojausta, kun opitaan koko ajan enemmän järjestelmistä sekä käyttäjistä ja niiden tuottamasta liikenteestä. Ennakoivat toimet verkon suojaukseen edistää ympäristöä kohti mukautuvaa tietoturvaa (engl. adaptive security). Mukautuva tietoturva on jatkuva prosessi, joka koostuu potentiaalisten hyökkäysten ehkäisystä, tunnistamisesta, niihin vastaamisesta, sekä mahdollisesti epäilyttävien, mutta uudenlaisten toimien raportoinnista. Mukautuvan tietoturvan toteuttaminen yrityksessä lisää tietoturvatasoa ja Zero Trustia analysoimalla kaikkea ja panostamalla ennaltaehkäisyyn. (Xenonstack 2019.)

5 Palvelut ja teknologiat Zero Trustin tukena

Zero Trust on ollut 2010 vuosikymmenen aikana paljon puhuttu aihe ja myös monet eri yritykset sekä teknologiat voidaan liittää jollain tapaa Zero Trustiin ja niitä voidaan käyttää mallin edistämiseen omassa ympäristössään. Tässä vaiheessa tulee kuitenkin muistaa yhä, että Zero Trust arkkitehtuuri ei ole saavutettavissa pelkästään yhdellä tuotteella tai palvelulla. Zero Trust on yhä trendikäs aihe, joka voi tarjota monelle yritykselle markkinoinnin kannalta hyvän sauman kohottaa yrityksen tietoturvailmettä ja herättää asiakkaiden huomiota.

Edellisessä kappaleessa käsiteltiin Zero Trustin toteutuksessa oleellisena olevia ympäristön struktuuriin ja hallintaan liittyviä menetelmiä. Zero Trust on malli mahdollisimman monenlaisen yrityksen avuksi, minkä takia on tärkeää muistaa, että eri ympäristöissä toteutettuna myös Zero Trustin keskeisimpänä pidetyt periaatteet sekä työkalut vaihtelevat. Tässä kappaleessa käsitellään kuvitteellisen tapausesimerkin avulla konkreettisemmin palveluita- ja teknologioita, jotka tukevat Zero Trustin ajatusmallia ja joiden avulla Zero Trust ympäristöä kohti on mahdollisuus kehittyä. Esittelen Zero Trustiin liitettäviä palveluita ja järjestelmiä pääosin pienen, 50–100 henkilön yrityksen näkökulmasta. Esimerkkinä käytän kuviossa 6 hahmottelemaani yksinkertaista IT-ympäristöä, joka koostuu työntekijöistä, heidän työlaitteistaan, identiteetti- ja laitehallintajärjestelmästä sekä SaaS-tuotteista. Samassa kuviossa on myös kuvailtu yksinkertaistettuna prosessi, jolla lailla kertakirjautuminen ja pääsynvalvonta yrityksen SaaS-tuotteisiin kulkee. Alakappaleissa kuvailen tarkemmin esimerkkiyrityksen ympäristöä ja esittelen Zero Trustia tukevia menetelmiä ja palveluita.

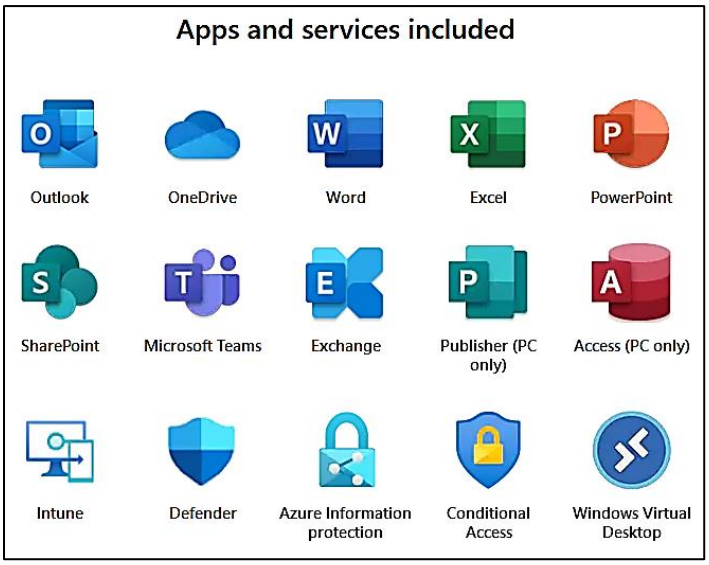


Kuvio 6. Esimerkkiyrityksen yksinkertainen IT-ympäristö ja SaaS-palveluun kirjautuminen

5.1 Identiteetti- ja laitehallinta

Esimerkkiyritys käyttää käyttäjiensä identiteetti- ja laitehallintaan Microsoftin palveluita. Yrityksellä on Microsoft 365 Business lisenssi jokaiselle käyttäjälleen, mikä sisältää useita eri palveluita (kuvio 7) mukaan lukien sähköpostin (Outlook), tiimityöskentelyalustan (Microsoft Teams), pilvitallennustilaa (OneDrive ja SharePoint) sekä laitehallintajärjestelmän (Intune). Yritys käyttää näitä kaikkia palveluita pilvessä, eikä yrityksen tarvitse hallinnoida järjestelmiä omilta fyysisiltä palvelimilta. (Microsoft 365 Business.)

Käyttäjien hallinnointiin yrityksen ylläpitäjät käyttävät Microsoft Azure palveluun sisältyvää Active Directorya. Active Directory sisältää oleellisimpana yrityksen käyttäjät, käyttäjäryhmät ja yrityksen käyttämät sovellukset, jotka Active Directoryyn on liitetty. Käyttäjäryhmät ovat luotu Active Directoryyn tiimeittäin, eli jokaisella tiimillä on oma ryhmänsä, johon tiimin jäsenet kuuluvat. Lisäksi myös yrityksen kolmella ylläpitäjillä on oma ryhmänsä. Ylläpitäjät ovat konfiguroineet Microsoftiin kirjautumisen niin, että käyttäjien täytyy määrittää vahva salasana ja monivaiheinen todennus omalle tililleen ensimmäisen kerran, kun he kirjautuvat uudelle käyttäjälleen sisään. Monivaiheisen todennuksen vaiheet ovat kuvattuna kappaleen 4.2 kuviossa 3. (Microsoft Azure 2019.)



Kuvio 7. Microsoft Business 365 lisenssiin sisältyviä palveluja. (Microsoft 365 Business)

Toinen suosittu palvelu identiteetinhallintaan Microsoftin lisäksi on Googlen G-Suite, joka tarjoaa hyvin samankaltaiset palvelut kuin Microsoftin 365 Business-lisenssi. WPBeginnerin sivuston editorien vuoden 2020 tammikuussa julkaistussa vertailussa G-Suite määriteltiin paremmaksi vaihtoehdoksi pienemmille yrityksille sen yksinkertaisuuden ja helpon hallinnan vuoksi. Microsoftin palveluja taas pidettiin optimaalisena yritykselle,

jonka ympäristö muodostuu pääosin Windows-työpöytäkoneista. Loppujen lopuksi kuitenkin Microsoftin ja Googlen palvelut ovat arvostelussa hyvin tasavertaisesti arvioitu niin turvallisuuden, käytettävyyden, ominaisuuksien kuin hinnoittelunkin suhteen, joten valintaan vaikuttaa todennäköisimmin loppujen lopuksi se, kumpi palvelu on entuudestaan tutumpi asiakkaalle.

Ylläpitäjät hallinnoivat Microsoftin Intune järjestelmässä kaikkia yrityksen tietokoneita ja mobiililaitteita. Intune järjestelmään yrityksen ylläpitäjät pääsevät Microsoftin Azure-portaalista. Intunessa ylläpitäjät voivat hallinnoida kaikkia laitteitaan niiden sijainnista huolimatta. Yritys on luonut laitteilleen Intunessa profiileja, joilla he määrittelevät tiettyjä tietoturvavaatimuksia eri laitteilleen. Intunesta voi seurata laitteiden statusta ja tulostaa raportteja tarkasteltavaksi. Jos yrityksen laitteelta puuttuu joitain turvallisuusasetuksia, niin se näkyy Intunen portaalissa poikkeuksena hyväksytyistä laitteista, joilla turvallisuusasetukset laitteella kohtaa yrityksen asettamat määritykset. Lähtökohtaisesti kuitenkin Intune hallitsee tietokoneita niin, että tietoturva-asetukset pysyvät aina päällä ja käyttäjällä on mahdollisimman vähän itse oikeuksia muokata kriittisimpiä suojausasetuksia. (Microsoft Azure 2019.)

Laitehallintajärjestelmäksi on kuitenkin olemassa paljon muita palveluita, jotka saattavat olla esimerkiksi tiettyyn käyttöjärjestelmään keskittyneitä. Esimerkiksi Jamf (https://www.jamf.com/) on kokonaan Applen laitteiden hallintaan kehitetty järjestelmä, ja erikoistuu Applen laitteiden natiiviasetusten hallintaan. Jamf tarjoaa yrityksen IT-henkilöstölle alustan hallita kaikkia Apple laitteitaan sekä niiden turvallisuutta ja applikaatioita. Jamfin avulla yritys voi toimittaa uuden laitteen työntekijälle niin, ettei heidän tarvitse itse tehdä laitteella mitään, vaan työntekijän ensimmäisen kerran laitteen avatessaan se yhdistää ja synkronisoi automaattisesti sille määritellyt turvallisuusasetukset järjestelemästä.

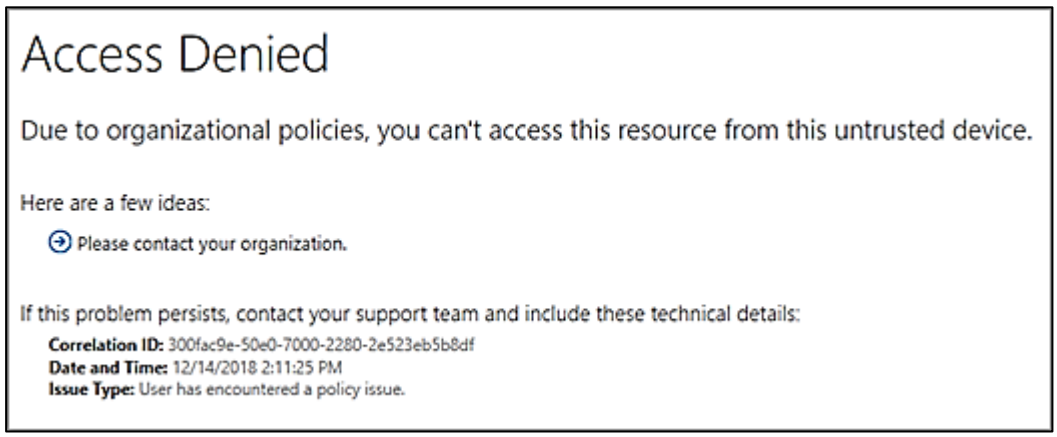
5.2 Sovellukset ja palvelut pilvessä

Yrityksen palvelut ja sovellukset, joita he käyttävät Microsoftin tarjoamien palvelujen lisäksi, ovat erilaisia SaaS (Software as a Service) tuotteita. Yritys tarvitsee ulkoisia palveluja työntekijöiden palkanlaskentaan ja työtuntikirjaukseen, intranettiin ja asiakashallintajärjestelmään. Kaikkiin palveluihin käyttäjät kirjautuvat Microsoftin tunnuksilla, koska ylläpitäjät ovat valinneet sovellukset käyttöönsä osaksi myös sen perusteella, että niihin on mahdollista konfiguroida kertakirjautuminen (SSO). Kertakirjautumisen kautta käyttäjät kirjautuvat joka palveluun Microsoftin käyttäjätunnuksen, salasanan ja monivaiheisen todennuksen yhdistelmällä.

Vaikka yrityksellä on käytössään pääsääntöisesti vain yksi autentikointitunnus, kaikilla työntekijöillä on silti salasanamanageri-sovellus yrityksen puolesta. Salasanamanageri on palvelu, jossa voi generoida vahvoja salasanoja ja tallentaa ne sovellukseen pääsalasanan taakse. Esimerkkiyrityksen työntekijät luovat vahvan pääsalasanan, jolla he avaavat salasanamanagerin silloin, kun heidän tarvitsee tallettaa jotain yksinkertaista tietoa turvalliseen paikkaan tai generoida salasana yrityksen uuteen palveluun, jossa ei ole kertakirjautumismahdollisuutta. Gilbertson (2020) on listannut 1Password-nimisen tuotteen markkinoiden parhaaksi salasanamanageriksi. 1Password voi toimia salasanojen hallitsemispaikan lisäksi myös monivaiheisen todennuksen tarjoajana. 1Passwordin etuna toimii myös sen mukautuvuus moneen eri ympäristöön, jolloin sen käyttäminen on nopeaa ja vaivatonta automaattisen tunnusten syötön avulla.

Pääsynvalvonnan suhteen ylläpitäjät ovat määrittäneet Microsoft Azuren Active Directoryssä, että vain tiettyjen tiimien jäsenillä tulee olla oikeudet asiakashallintajärjestelmään. Kaikki työntekijät eivät tarvitse työssään asiakkaiden tietoja, joten heidän ei myöskään kuulu saada pääsyä asiakashallintajärjestelmään. Sen sijaan ylläpitäjille on määritelty jokaiseen sovellukseen oman käyttäjäryhmänsä perusteella pääsy, jolla he saavat peruskäyttäjää laajemmat oikeudet sovelluksiin. Ylläpito-oikeuksia esimerkkiyrityksen ylläpitäjät käyttävät kertakirjautumisen hallinnointiin sovelluksen puolella, sekä tarkistaakseen käyttäjien statuksia säännöllisin väliajoin. Jos yritykseen saapuu uusi työntekijä, ylläpitäjät luovat käyttäjän Microsoftin hallintaportaalin puolella ja lisäävät hänet oikeisiin ryhmiin, jolloin käyttäjä saa automaattisesti hänelle kuuluvan pääsyn yrityksen käyttämiin sovelluksiin ja palveluihin. Jos yrityksestä taas poistuu työntekijä, niin käyttäjätili poistetaan Microsoftin järjestelmästä, jolloin hänen pääsynsä muihinkin palveluihin automaattisesti katkeaa. Yrityksen käyttäjien hallinnoiminen on turvallisempaa ja tehokkaampaa, kun sitä tarvitsee tehdä vain yhdestä portaalista.

Pääsynvalvontaan esimerkkiyritys on myös asettanut ehtoja laitteiden osalta. Jotta työntekijä pääsee kirjautumaan yrityksen käyttämään sovellukseen kertakirjautumista käyttäen, laite jolta käyttäjä haluaa kirjautua, täytyy olla rekisteröity yrityksen laitehallintajärjestelmään ja sen täytyy vastata sille asetettuja turvallisuusvaatimuksia. Mikäli jotain laitehallinnassa vaadittuja turvallisuusasetuksia puuttuu, tai käyttäjä yrittää kirjautua esimerkiksi omalta henkilökohtaiselta tietokoneeltaan, hänen pääsynsä sovellukseen estetään (kuvio 8).



Kuvio 8. Pääsy yrityksen resursseihin voidaan estää tuntemattomilta laitteilta. (Microsoft Docs SharePoint 2020)

5.3 Toimistoverkko

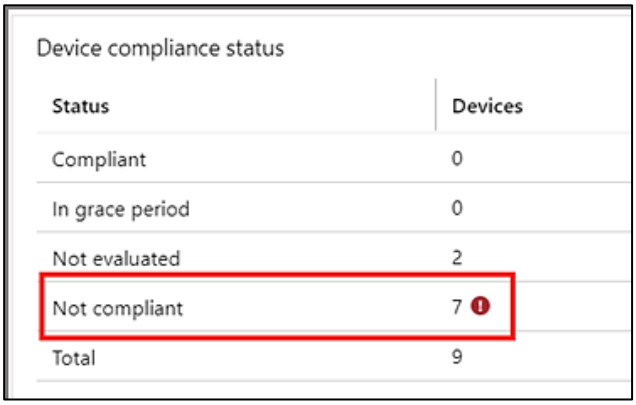
Esimerkkiyrityksellä on toimisto kerrostalorakennuksessa, jossa työntekijät pääsääntöisesti työskentelevät. Työntekijät yhdistävät yrityksen langattomaan verkkoon aina, kun he tekevät töitä toimistolla. Työntekijät ovat ohjeistettu siitä, että vaikka yrityksellä on oma salasanalla suojattu verkkoyhteys, niin siihen yhdistettynä ollessa tulee noudattaa samoja tietoturvaohjeita, kuin kaikkien muidenkin verkkojen kanssa, esimerkiksi kahvilan julkisessa wifi-yhteydessä.

Jokaisella yrityksen tietokoneella ja mobiililaitteella on laitehallinnasta asetettujen tietoturvamääritysten lisäksi käytössään VPN (Virtual-Private Network) ohjelmisto, joita esimerkkiyrityksen ylläpitäjät hallinnoivat keskitetysti. VPN on aina tietokoneissa päällä, kun ne ovat yhdistettynä verkkoihin. VPN salakirjoittaa käyttäjän liikenteen, joka estää ulkopuolisia hyökkääjiä näkemästä liikenteen sisältöä selkokielellä. Ohjelma mahdollistaa käyttäjille yksityisyyden julkisissa verkoissa ja suojelee dataa, jota käyttäjä käsittelee yhteyksissään. VPN on tekniikka, jota voidaan hyödyntää kaikissa verkkoon liitetyissä laitteissa, ja joka on myös kuluttajille tarpeellinen lisä oman tietoturvansa parantamiseksi. (Siciliano 2020.)

5.4 Monitorointi

Esimerkkiyrityksen toimiston verkko on rakennettu Ubiquitin laitteilla, jotka tarjoavat mukanaan hallinnointisovelluksen, johon ylläpitäjät voivat kirjautua webbiselaimella verkon sisällä. Kirjautumisen vahva salasana on generoitu salasanamanagerin avulla ja tallennettu salasanamanagerin pääsalasanan taakse. Ubiquitin oma monitorointisovellus tarjoaa yrityksen pienikokoiselle verkolle tarpeeksi näkyvyyttä, raportteja ja asetuksia. Esimerkkiyrityksen ylläpitäjillä on ainoastaan tarve monitoroida omassa verkossaan tapahtuvaa liikennettä.

Toimiston verkkonsa lisäksi monitorointia suoritetaan esimerkkiyrityksessä Microsoft Azuren palvelussa. Azuressa yrityksen ylläpitäjät seuraavat järjestelmään liitettyjen laitteidensa statusta (kuvio 9) ja reagoivat heti huomaamiinsa poikkeuksiin tai puutteisiin laitteiden tietoturvatasossa. He voivat myös seurata liikennettä yhdistettyihin, käytössä oleviin pilvisovelluksiin ja aloittaa tutkimaan mahdollisesti epäilyttäviltä vaikuttavia toimintoja.



Kuvio 9. Microsoft Azuren Intune-järjestelmässä laitteiden statusta voi helposti seurata (Microsoft Docs Intune 2019)

Isommat yritykset, joilla on esimerkiksi paljon omia applikaatioita pilvipalvelimilla, saattavat tarvita laajempaa, keskitettyä monitorointiohjelmaa, joka kykenee skaalautumaan myös pilvipalvelimille. ThousandEyes on alusta verkon monitorointiin, joka pyrkii tarjoamaan näkyvyyden liikenteen koko matkasta lähteestä kohteeseen. Tämä sisältää jokaisen pisteen, jonka kautta liikenne kulkee, riippumatta näiden kyseisten pisteiden palveluntarjoajista. Pilvipalveluita käyttäessä liikenne kulkee useiden eri verkkojen läpi ennen kuin liikenne saapuu itse kohteeseen, mikä voi tuottaa haasteita selvittää vikojen syitä silloin, kun oma verkko, sekä pilvipalvelimen verkko näyttää olevan kunnossa, mutta yhteys ei silti toimi. ThousandEyesin tarjoamalta alustalta voi kuitenkin nähdä yhteydet koko matkalta ja vikatilanteiden selvittäminen sen avulla on nopeampaa. Yhteyksien testaamiseen ThousandEyes tarjoaa omia pilviagenttejaan ympäri maailmaa, joilta voi simuloida liikennettä omille pilvipalvelimilleen ja testata sijainnin vaikutusta yhteyksien laatuun. (Besana 2015.)

Monitorointiin sisältyy jatkuva ympäristön tarkkailu ja sen kehittäminen tarkkailussa havaitsemien puutteiden perusteella, jotta ympäristö pysyisi mahdollisimman kestävänä erilaisten hyökkäysten estämisessä. Yritys voi myös käyttää penetraatiotestaajia saadakseen laajemmin tietoa ympäristönsä turvallisuudesta. Kiinnostava vaihtoehto erilaisten ympäristöjen Zero Trust-tason testaamiselle on Guardicore-yrityksen kehittelemä Infection Monkey-työkalu. Infection Monkey tarjoaa yrityksille automatisoitua,

simuloitua penetraatiotestausta, jonka voi käynnistää useammalta eri alustalta yrityksen valinnan mukaan. Guardicoren mukaan, Infection Monkey testaa ympäristöä Zero Trustin periaatteita vastaan ja luo sitten raportin muun muassa ympäristön mikrosegmentoinnin ja identiteetin tarkastuksen tasosta. Infection Monkey ottaa huomioon Zero Trust-viitekehyksessä huomioon otettavat eri osa-alueet, joihin sisältyy ainakin verkot, käyttäjät, laitteet ja dataa. Simuloidun testauksen perusteella saatu raportti tarjoaa yritykselle tietoa puutteista ja lähtökohdan lähteä parantamaan kokonaisuutta. (Infection Monkey powered by Guardicore.)

6 Zero Trustin johdannaiset ja tulevaisuus

Opinnäytetyön yhteenvetona voidaan todeta, että Zero Trust malli on viitekehys, joka kattaa laajan alueen koko yrityksen ympäristön tietoturvasta. Viitekehyksen toteuttamiseen käytettäviä tiettyjä palveluita tai edes teknologioita ei ole rajattu tarkemmin kenenkään puolesta. Ytimenä säilyy Zero Trustin ajatus, mutta eri yrityksillä ovat omanlaisensa näkemyksensä sen parhaisiin käytäntöihin. Lähteitä Zero Trustiin liittyen on löydettävissä runsaasti netistä ja suuri osa niistä on erilaisten yritysten tekemiä mallinnuksia Zero Trust kokonaisuudesta. Zero Trust säilyy sovellettavissa olevana mallina, mikä antaakin yrityksille varaa luovuuteen ja joustavuuteen sen toteuttamisessa, säilyttäen kuitenkin sen pääajatuksen. Googlen kehittämää tietoturvan BeyondCorp-mallia, sekä Gartnerin kehittämää CARTA-mallia kuvaillaan monesti Zero Trust malleiksi, vaikka niillä onkin omat nimensä, joissa Zero Trustia ei mainita.

Googlen kehittämä tietoturvamalli BeyondCorp on Zero Trust viitekehyksen kanssa samoilla lähtölinjoilla; perinteinen tietoturvamalli ei palvele enää tarpeeksi kattavasti nykypäivän yrityksiä tietoturvan näkökulmasta. Googlen mukaan nykypäivän yrityksissä työtä tehdään useista eri vaihtuvista sijainneista ja tämän takia perinteisen tietoturvamallin ydin ei enää skaalaudu tarpeeksi joustavasti uudenlaiseen ympäristöön. BeyondCorpin Zero Trust-mallissa kuitenkin painotetaan, että luottamuksen antaminen lopulta käyttäjälle on väistämätöntä, jotta yhteydet eri resursseihin ylipäätänsä toimii. Luottamus myönnetään kuitenkin käyttäjälle vasta silloin, kun on varmistettu henkilön identiteetti, laitteen tila ja pyynnön hyväksymiseen vaikuttavat muut säännöt, jotka yritys on hallintapuolella resurssille määritellyt. Tarkistusprosessin mahdollistamiseksi henkilö sekä laite tulee olla yhdistetty yrityksen järjestelmään, ja laitteen status tulee olla automaattisesti vahvistettavissa. Vasta sitten, jos käyttäjän pyyntö kaikin puolin tulkitaan oikeelliseksi, hänelle myönnetään pääsy järjestelmään. Uudestaan järjestelmään pääsyä pyytäessään, käydään läpi sama tunnistautumisprosessi, eikä käyttäjälle voida myöntää oikeuksia edellisen kerran perusteella. (Saltonstall 2019.)

BeyondCorpin, kuten Zero Trustin, ydin on reaaliaikaisessa, dynaamisessa autentikoinnissa ja pääsynvalvonnassa. Kuten edellisessä kappaleessa kuvailemassani esimerkkiyrityksessä, BeyondCorp- mallissa kaikki pyynnöt päästä palveluihin sisään myönnetään keskitetyn identiteetinhallinnan kautta, joka tarkistaa identiteetin ja laitteen statuksen. Keskeisimmät kohdat BeyondCorpin onnistumisessa on laitehallinta, jossa määritellään turvallisuusmääräykset. BeyondCorpin tarkoituksena on olla myös käyttäjille mahdollisimman huomaamaton ja helppo, mutta silti erittäin tietoturvallinen tapa päästä

sisään resursseihin. Myös datan keräämisen keskittäminen yhteen paikkaan on oleellinen asia BeyondCorpin skaalautuvuutta ja kestävyyttä ajatellen. (Dwyer 2017.)

Gartner-yrityksen kehittämä CARTA malli tulee sanoista Continuous Adaptive Risk and Trust Assessment (suom. jatkuva, mukautuva riskien ja luottamuksen arviointi). CARTA malli keskittyy riskien ja tietoturvan strategiseen hallintaan, jatkuvasti mukautuvien järjestelmien ja käytäntöjen pohjalta. Zero Trustia pidetään CARTA-mallin edellytyksenä, ja on siis avainasemassa CARTAn toteuttamisessa. CARTAn ideana on kehittää Zero Trustia painottamalla ympäristön riskienhallintaa ja jatkuvaa analysointia. (Hines 2019.)

Molemmat malleista ovat siis samankaltaisia ideansa puolesta ja kytköksissä Zero Trustiin. Toivon mukaan tulevaisuudessa on odotettavissa useampien, isompien yritysten julkaisemia Zero Trust mallinnuksia. Myös yhä useampi tuotteen valmistaja voi käyttää Zero Trustin ajankohtaisuutta hyväkseen ja alkaa kehittää tuotteitaan tietoturvallisempaan suuntaan. Toivottavasti silti Zero Trust nimeä ei sen trendikkyydestä johtuen käytettäisi markkinoinnissa harhaanjohtavasti jostain sellaisesta tuotteesta tai palvelusta, joka ei tosiasiassa tue mallin periaatteita.

Ennen kaikkea Zero Trustin ideologiaan tulisi kiinnittää huomiota yritysten tietoturvatiimeissä ja alkaa omaksua mallin periaatteita. Periaatteita omaksuessa myös ajatuksia avautuu sille, että miten mallia voisi alkaa edistämään omassa ympäristössään. Ympäristössä saattaa jo sellaisenaan olla valmiuksia toteuttaa Zero Trustia kohti meneviä toiminnallisuuksia. Toivon mukaan Zero Trust malli haarautuisi myös tulevaisuudessa kuluttajille kohdistettuun suuntaan, jolloin jokainen voisi heijastaa mallia henkilökohtaiseen tietoturvaansa. Kuluttajille suunnatun Zero Trust mallin avulla voisi saada konkreettisia esimerkkejä tietoturvan parantamiseen niin, että ohjeet ovat helposti ymmärrettävissä kenelle tahansa. Erilaisten verkkolaitteiden ja tekniikoiden saavuttaessa myös kuluttajat, on mielestäni tärkeää, että jokainen ymmärtäisi ainakin perusteet oman tietoturvansa vahvistamisesta ja ylläpitämisestä.

7 Opinnäytetyöprosessin arviointi

Opinnäytetyön tekeminen Zero Trust aiheesta oli opettavainen monella tapaa. Olen oppinut itse Zero Trustista ja ymmärtänyt, että mikä tahansa yritys voi kehittää ympäristöään viitekehyksen suuntaan. Koin prosessin myös todella motivoivaksi ja työtä tehdessäni sain jatkuvasti ajatuksia siitä, miten voisin kehittää omaa henkilökohtaista tietoturvaani tai heijastaa oppimaani työssäni. Opinnäytetyötä tehdessäni minulla ei ollut hetkeäkään epäilystä siitä, ettenkö tulisi hyötymään opituista asioista. Työni päätökseen saatuani koko prosessista jäi positiivinen mielikuva.

Vaikka hankaluuksia ei opinnäytetyön tekemisessä juurikaan ollut, niin joitain haasteita tuli silti vastaan. Zero Trustista on niin laajasti tällä hetkellä netissä artikkeleita ja erilaisia kirjoituksia, minkä takia alussa koin vaikeaksi valita sopivia lähteitä. Onnistuin kuitenkin yhdistelemään useita lähteitä tavoitteideni mukaisesti kokonaisuudeksi. Lähdemateriaali oli pääsääntöisesti englanninkielistä, mikä saattoi välillä hankaloittaa joidenkin termien kääntämistä suomen kielelle. Valtionhallinnon tietoturvasanasto (https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto) pitää sisällään kuitenkin useita englannin kielestä käännettyjä tietoturvasanoja, mistä pystyi aina tarpeen tullessa tarkistamaan, jos oma käännös ei kuulostanut aivan oikealta. Toivon, että tulevaisuudessa Zero Trustista löytyisi enemmän myös suomenkielistä materiaalia, jotta se tavoittaisi mahdollisimman monenlaisia ihmisiä. Lähteissä olin kuitenkin erityisen tyytyväinen siihen, että melkein kaikki niistä olivat viimeaikaisia, eli julkaistu vuosina 2017–2020.

Opinnäytetyöni lopputulos tarjoaa sekä yksityisille ihmisille kuin yrityksille tiiviin suomenkielisen kuvauksen Zero Trustista tietoturvan mallina. Kokonaisuuden kielelliseen esitykseen kiinnitettiin erityistä huomiota, jotta aiheen voisi ymmärtää mahdollisimman laaja kirjo ihmisiä eri lähtökohdista. Ymmärtämisen helpottamiseksi on vielä lisätty sanasto opinnäytetyön liitteisiin. Toivon, että tästä opinnäytetyöstä olisi hyötyä niin yksityishenkilöillekkin kuin ammattilaisillekkin, jotka ovat kiinnostuneet tutustumaan Zero Trustiin eri näkökulmista.

Lähdeluettelo

Accenture. 2019. The cost of cybercrime. Luettavissa: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50. Luettu: 13.2.2020.

AppNeta. 2015. AppNeta: Application Performance Monitoring for All. Luettavissa: https://www.appneta.com/pdf/appneta-apm-for-all-2015.pdf. Luettu: 8.3.2020.

Atlassian. Understanding Zero Trust Security. Luettavissa: https://www.atlassian.com/dam/jcr:a3650ca8-5483-4206-ac10-dcfc3b7353ba/Zero-Trust-Whitepaper.pdf. Luettu: 29.2.2020

Armstrong, S. How to Monitor SaaS Applications. Luettavissa: https://www.appneta.com/pdf/How_to_monitor_saas_applications.pdf. Luettu: 8.3.2020

Barracuda. Network Firewalls. Luettavissa: https://www.barracuda.com/glossary/network-firewall. Luettu: 15.2.2020

Beadle, J. 2018. Gartner Top 10 Security Projects for 2018. Luettavissa: https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018/. Luettu: 7.3.2020

Besana, D. 2015. ThousandEyes review: network monitoring for the cloud era. Luettavissa: https://www.routerfreak.com/thousandeyes-review/. Luettu: 11.3.2020.

Bednarz, A. 2019. What is microsegmentation? How getting granular improves network security. Luettavissa: https://www.networkworld.com/article/3247672/what-is-microsegmentation-how-getting-granular-improves-network-security.html. Luettu: 22.2.2020

Blesa, I. 2019. Cyber-security with intelligent network monitoring. Luettavissa: https://www.techradar.com/news/cyber-security-with-intelligent-network-monitoring. Luettu: 5.3.2020

Bradley, T. 2019. The standard cybersecurity model is fundamentally broken. Luettavissa: https://www.forbes.com/sites/tonybradley/2019/10/07/the-standard-cybersecurity-model-is-fundamentally-broken/. Luettu: 16.2.2020

Chickowski, E. 2019. A Beginner’s Guide to Microsegmentation. Luettavissa: https://www.darkreading.com/edge/theedge/a-beginners-guide-to-microsegmentation/b/d-id/1335849. Luettu: 22.2.2020

Chow, J. 2017. Zero-Trust Model: Never Trust, Always Verify. Luettavissa: https://www.centrify.com/blog/zero-trust-model/. Luettu: 7.3.2020

Cloudflare. What is access control? Luettavissa: https://www.cloudflare.com/learning/access-management/what-is-access-control/. Luettu: 7.3.2020

Continuum Product Team. 2019. Everything You Need To Know About Mobile Device Management (MDM. Luettavissa: https://www.continuum.net/resources/mspedia/everything-to-know-about-mobile-device-management-mdm). Luettu: 7.3.2020

Covington, R. 2019. 5 steps to simple role-based access control. Luettavissa: https://www.csoonline.com/article/3060780/5-steps-to-simple-role-based-access-control.html. Luettu: 8.3.2020

Dwyer, I. 2017. Fundamentals of the BeyondCorp “Zero Trust” Security Framework. Luettavissa: https://dzone.com/articles/fundamentals-of-the-beyondcorp-zero-trust-security. Luettu: 10.3.2020

Friedman, J. 2017. The definitive guide to Micro-Segmentation. Luettavissa: https://cdn2.hubspot.net/hubfs/407749/Downloads/Illumio_eBook_The_Definitive_Guide_to_Micro_Segmentation_2017_08.pdf. Luettu: 7.3.2020

Gilbertson, S. 2020.The Best Password Managers to Secure Your Digital Life. Luettavissa: https://www.wired.com/story/best-password-managers/. Luettu: 11.3.2020

Givati, M. 2018. Harness the Benefits of Micro-Segmentation. Luettavissa: https://www.guardicore.com/micro-segmentation/benefits-micro-segmentation/. Luettu: 7.3.2020

Guida, R. 2019. Why Multi-Factor Atuhentication Isn’t Foolproof. Luettavissa: https://www.avanan.com/blog/why-2-factor-authentication-isnt-foolproof. Luettu: 7.3.2020

Hines, C. 2019. Zero trust vs. Gartner CARTA. Is one actually part of the other? Luettavissa: https://www.zscaler.com/blogs/corporate/zero-trust-vs-gartner-carta-one-actually-part-other. Luettu: 11.3.2020

Infection Monkey powered by Guardicore. Luettavissa: https://www.guardicore.com/infectionmonkey/zero-trust.html#benefits. Luettu: 22.3.2020

Kaita. Lokienhallinta ja SIEM. Luettavissa: http://kaita.fi/tiedon-turvaaminen/lokienhallinta-ja-siem/. Luettu: 8.3.2020.

Kuparinen, K. 2018. Kertakirjautumisen hyödyt. Luettavissa: https://blog.avoine.fi/kirjoitukset/kertakirjautuminen-eli-sso/. Luettu: 8.3.2020.

Mayne, M. 2016. Don’t rely on castles and moats to protect your data – build a healthy immune system instead. Luettavissa: https://securityintelligence.com/dont-rely-on-castles-and-moats-to-protect-your-data-build-a-healthy-immune-system-instead/. Luettu: 15.2.2020

Microsoft 365 Business. Microsoft 365 | Business. Luettavissa: https://www.microsoft.com/en-us/microsoft-365/business#compareProductsRegion. Luettu: 11.3.2020.

Microsoft Azure. 2019. What is Conditional Access? Luettavissa: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview. Luettu: 11.3.2020.

Microsoft Docs SharePoint. 2020. Control access from unmanaged devices. Luettavissa: https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices. Luettu: 11.3.2020.

Microsoft Docs Intune. 2019. Monitor Intune Device compliance policies. Luettavissa: https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor. Luettu: 22.3.2020

National Cyber Security Centre. 2019. Github repository. Zero trust architecture design principles. Luettavissa: https://github.com/ukncsc/zero-trust-architecture/. Luettu: 8.3.2020

Palo Alto Networks. What is Zero Trust? Luettavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture. Luettu: 16.2.2020

Petikäinen, S. 2013. Valtiovarainministeriön Vahti-ohjeet, 3. Tietoturvallisuus – mitä se on? Luettavissa: https://www.vahtiohje.fi/web/guest/691. Luettu: 13.2.2020

Petters, J. 2019. What is Zero Trust? A Security Model. Luettavissa: https://www.varonis.com/blog/what-is-zero-trust/. Luettu: 15.3.2020

robertchahin. 2018. The SSO Wall of Shame. Luettavissa: https://sso.tax/. Luettu: 11.3.2020

Saltonstall, M. 2019. What is BeyondCorp? What is Identity-Aware Proxy? Luettavissa: https://medium.com/google-cloud/what-is-beyondcorp-what-is-identity-aware-proxy-de525d9b3f90. Luettu: 10.3.2020

Sande, S. 2019. Zero Trust, a new way to look at network security. Luettavissa: https://blog.macsales.com/48549-zero-trust-a-new-way-to-look-at-network-security/. Luettu: 15.2.2020

Security Roundtable. John Kindervag. Luettavissa: https://www.securityroundtable.org/contributor/john-kindervag/. Luettu 7.3.2020

ShortestPathFirst. 2019. Interview with John Kindervag, the Godfather of Zero Trust Networking. Youtube-video, 7:31, julkaistu 30.4. https://www.youtube.com/watch?v=yo6Z7fIJ11A#action=share

Siciliano, R. 2020. What a VPN Does to Protect Your Computer. Luettavissa: https://www.thebalance.com/how-vpn-protects-your-computer-and-privacy-4148267. Luettu: 22.3.2020.

Smith, R. 2011. The Field-Grade CTO. Luettavissa: https://www.questia.com/library/journal/1G1-255839496/the-field-grade-cto. Luettu: 7.3.2020

Soare, B. 2020. SECURITY ALERT: Microsoft releases critical security updates to fix major vulnerabilities. Luettavissa: https://heimdalsecurity.com/blog/security-alert-microsoft-patch-tuesday-january-2020/. Luettu: 8.3.2020

Tirronen, H. 2003. Tietoturva ja tietosuoja. Luettavissa: http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva.html. Luettu: 13.2.2020

Trulioo. 2018. Identity Authentication – Are They Who They Say They Are? Luettavissa: https://www.trulioo.com/blog/identity-authentication/. Luettu: 29.2.2020

Ubiquiti. Verkkosivut. Luettavissa: https://www.ui.com/. Luettu: 5.3.2020.

Ubiquiti Unifi Controller Demo. Luettavissa: https://demo.ubnt.com/. Luettu: 11.3.2020.

VAHTI, Valtionhallinnon tietoturvallisuuden johtoryhmä. 2008. Valtionhallinnon tietoturvasanasto 8/2008. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229¨. Luettu: 8.3.2020

Vathera, P. 2018. Miten web toimii. TCP/IP-pino. Luettavissa: https://punomo.fi/tvt-ict-tekniikka/miten-web-toimii-tcp-ip-pino/. Luettu: 7.3.2020

WPBeginner. 2020. G Suite vs Office 365 Comparison – Which One is Better? Luettavissa: https://www.wpbeginner.com/opinion/g-suite-vs-office-365-comparison-which-one-is-better/. Luettu: 11.3.2020

Wilson, M. 2020. 10 Best Network Monitoring Tools & Software. Luettavissa: https://www.pcwdld.com/best-network-monitoring-tools-and-software. Luettu: 5.3.2020

Xenonstack. 2019. What is Adaptive Security Architecture and Best Practises. Luettavissa: https://www.xenonstack.com/insights/adaptive-security/. Luettu: 8.3.2020

Zhang, E. 2019. What is Role-Based Access Control (RBAC)? Examples, Benefits, and More. Luettavissa: https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more. Luettu: 8.3.2020

Liitteet

Liite 1. Käsitteet

Zero Trust

John Kindervagin vuonna 2010 kehittämä uudenlainen tietoturvan viitekehys, jossa pyritään poistamaan luottamuksen tuomaa hyökkäyspinta-alaa IT-ympäristöissä.

“Castle-and-moat”-malli

Perinteinen tietoturvamalli, jossa suojauksen ydin on sisäverkkoa suojaava palomuuri. Palomuuri suodattaa liikennettä sisäverkon ja ulkoverkon, päättäen luotetaanko sisään tulevaan liikenteeseen.

Ulkoverkko, WAN

Internet, joka tarkoittaa julkisten, ei-yksityisten verkkojen muodostamaa kokonaisuutta.

Sisäverkko, LAN

Yksityinen, sisäinen verkkoyhteys esimerkiksi yrityksen toimistolla tai kuluttajan kotona.

Palomuuri

Sovellus tai fyysinen laite, joka suodattaa verkkoliikennettä ja pyrkii estämään haitallisen liikenteen etenemisen.

Intranet

Yrityksen sisäiset sivut esimerkiksi yrityksen tärkeille tiedotteille, dokumenteille ja ohjeille. Sisältää yleensä luottamuksellista dataa yrityksestä.

Hyökkäysvektori

Väylä tai keino hyökätä sisään, tai käyttää hyväksi jotain ulkopuolisilta rajoitettua resurssia, palvelua tai dataa.

Penetraatiotestaus

Ennalta sovittuihin kohteisiin ja ennalta sovittujen rajoitusten puitteissa tehtävää hyökkäystestausta.

Resurssi

Esimerkiksi jokin dokumentti, sovellus, palvelu tai laite.

IoT-laite (Internet of Things)

Laite, joka on yhdistetty verkkoon ja jota voi hallinnoida verkkoyhteyden välityksellä.

Mikrosegmentointi

Yrityksen ympäristön jaottelemista pienempiin kokonaisuuksiin tietoturvan edistämiseksi, kohteen luonteen ja tyypin perusteella.

Vähimmäisoikeuksien periaate (principle of least priviledge)

Periaate, jonka mukaan käyttäjällä tulee olla vain ne oikeudet resursseihin, joita hän tarvitsee työnsä tekemiseen. Tunnettu myös minimioikeuksina.

GDPR

Tietosuojan parantamiseen kehitelty EU:n tietosuoja-asetus.

ISO 27001

Tietoturvan tasoa arvioiva, tunnettu tietoturvasertifikaatti.

Software as a Service (SaaS)

Jonkun tietyn sovelluksen käyttäminen palveluna niin, että ylläpidon pilvessä hoitaa sovelluksen palveluntarjoaja.

Konfigurointi

Asetusten määrittelemistä ja toteuttamista.