Marko Nikulainen

ZERO TRUST -KONSEPTIN HYÖDYNTÄMINEN ENERGIAYHTIÖSSÄ

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Tieto- ja viestintätekniikka

2022

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä/Tekijät	Marko Nikulainen
Työn nimi	Zero Trust -konseptin hyödyntäminen energiayhtiössä
Toimeksiantaja	Kotkan Energia
Vuosi	2022
Sivut	45 sivua, liitteitä 0 sivua
Työn ohjaaja(t)	Vesa Kankare

TIIVISTELMÄ

Opinnäytetyön aiheena oli selvittää Zero Trust -konseptin hyödyntämistä energiayhtiössä. Työn toimeksiantajana toimii Kotkan Energia. Tutkimuksen tarkoituksena oli selvittää mitä muutoksia Zero Trust -konsepti aiheuttaa tuotantoverkkoon sekä OT-verkkoon. Tavoitteena oli lisäksi tehdä suunnitelma käyttöönotosta.

Tutkimusongelmana opinnäytetyössä on selvittää, kuinka Zero Trustin käyttöönotto voidaan tehdä olemassa olevaan verkkoinfrastruktuuriin. Aiheen teoreettisen selvityksen lisäksi tehdään suunnitelma energiayhtiölle Zero Trust -arkkitehtuurin käyttöönotosta.

Opinnäytetyön teoriaosuudessa tarkastellaan Zero Trust -konseptin pääperiaatteita, Zero Trust -arkkitehtuurin lähestymistapoja sekä perinteisen OT-verkon Purdue-mallia. Teoriaosuudessa tutustutaan myös suunnittelun eri vaiheisiin sekä kolmen eri valmistajan ratkaisuihin Zero Trustin käyttöönotossa niin IT-verkon kuin OT-verkon osalta. Tutkimus toteutettiin kehittämistutkimuksena. Aineisto koostui pääasiassa dokumentaatioista sekä aiemmista tutkimuksista.

Opinnäytetyön lopputuloksena on kattava teoria Zero Trust -konseptista, siihen liittyvistä käsitteistä ja Zero Trust -arkkitehtuurin suunnittelun malleista. Lopputuloksena toteutettiin konkreettinen suunnitelma Zero Trust -arkkitehtuurin hyödyntämisestä energiayhtiössä.

Perinteinen yritysverkko on suljettu, jossa pääsynhallinta toteutetaan pääosin ulkoreunalla. Zero Trust -konseptin periaate on poistaa luottamus verkosta ja siirtyä identiteetin vahvistamiseen sekä sovellusten ja palveluiden suojaamiseen. Zero Trust -arkkitehtuurin periaatteet ovatkin toteutettavissa monin eri tavoin, kuten tehostetun identiteetin tai mikrosegmentoinnein. Täydellisempää ratkaisua tarjoaa ohjelmistopohjaiset verkot ja koneoppiminen.

Asiasanat: Zero Trust, OT-verkko, Purdue-malli, tietoturva

South-Eastern Finland University of Applied Sciences

Degree	Bachelor of Engineering
Author (authors)	Marko Nikulainen
Thesis title	Utilizing the Zero Trust -concept in an energy company
Commissioned by	Kotkan Energia
Time	2022
Pages	45 pages
Supervisor	Vesa Kankare

ABSTRACT

The topic of the thesis was to explore how to utilize the Zero Trust concept in an energy company. The work is commissioned by Kotkan Energia. The purpose of the study was to find out what changes the Zero Trust concept causes to the production network and the OT network. Furthermore, the goal was to make a plan for deployment.

The research problem in the thesis is to find out how to make Zero Trust deployment into existing network infrastructure. In addition to the theoretical study of the subject, a plan is being made for the energy company to introduce the Zero Trust architecture.

The theory portion of the thesis examines the main principles of the Zero Trust concept, the approaches to the Zero Trust architecture, and the Purdue model of the traditional OT network. The theory section also explores the different stages of design and the solutions of three different manufacturers for Zero Trust deployment for both IT and OT network. The research was carried out as development research. The data consisted mainly of documentation as well as previous researches.

The result of the thesis is a comprehensive theory of the Zero Trust concept, related concepts and models of Zero Trust architecture design. As a result, a concrete plan to utilise the Zero Trust architecture in the energy company was implemented.

The traditional business network is closed, where access control is carried out mainly on the outer edge. The principle of the Zero Trust concept is to remove trust from the network and move to identity strengthening and protecting applications and services. The principles of Zero Trust architecture are feasible in a variety of ways, such as enhanced identity or microsegmentation. A more complete solution is provided by software-based networks and machine learning.

Keywords: Zero Trust, OT network, Purdue model, cybersecurity

SISÄLLYS

1 JOHDANTO

Opinnäytetyössä on tarkoitus tutkia Zero Trust -konseptin vaatimuksia verkkoinfrastruktuurille. Työssä tarkastellaan, kuinka Zero Trust -arkkitehtuuria hyödynnetään ja otetaan käyttöön energiayhtiössä. Mitä arkkitehtuurin käyttöönotto vaatii olemassa olevalta verkkoinfrastruktuurilta, millaisia asioita tulee ottaa huomioon suunnittelussa ja kuinka käyttöönotto toteutetaan Cisco ISE -työkaluin?

Zero Trust -konsepti on vielä melko tuore ilmiö, eikä aiheesta löydy paljon tietoa suomen kielellä tuotettuna. Zero Trust -konsepti on mielenkiintoinen vaatimuksineen ja se yhdistelee hyvässä suhteessa opiskeltuja asioita kyberturvallisuuden ja tietoverkkojen suhteen.

Opinnäytetyöstä on odotettavissa tutkielma Zero Trust -arkkitehtuurin vaatimuksista olemassa olevaan verkkoinfrastruktuuriin, sekä kuinka arkkitehtuuri on otettavissa käyttöön energiayhtiön verkkoinfrastruktuuriin. Työn tilaajalle tavoitteena on toimia ohjenuorana suunnittelussa. Tavoitteena on myös toimia dokumenttina tuotantoon käyttöönottovaiheessa.

Aiheesta tiedetään lähtötilanteessa yleisellä tasolla perusajatus. Zero Trust -konsepti muuttaa aiempaa ajattelua sisäverkosta ja sen verkkoliikenteestä niin, että ”älä luota mihinkään, identifioi kaikki” (Buck ym. 2021). Tämä aiheuttaa varsinkin olemassa oleviin perinteisiin verkkoinfrastruktuureihin uusia vaatimuksia.

Työn toimeksiantajana toimii Kotkan Energia. Kotkan Energia on Kotkan kaupungin kokonaan omistama energiakonserni, jonka pääliiketoimintaa ovat kaukolämpöpalvelut, energian tuotanto ja sähköverkkopalvelut (Kotkan Energia 2021).

2 TUTKIMUSASETELMA

Zero Trust -konsepti IT-verkossa on perusajatukseltaan selvä, mutta on epäselvää millaisia vaatimuksia ja muutoksia se aiheuttaa tuotantoverkossa ja varsinkin OT-verkossa. Tutkimusongelmaksi muodostuu Zero Trust -

arkkitehtuurin käyttöönotto olemassa olevaan verkkoinfrastruktuuriin. Opinnäytetyössä pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

- Onko Zero Trust -arkkitehtuuria mahdollista ottaa vaiheittain käyttöön tuotantoverkossa?
- Mitä Zero Trust -arkkitehtuurin käyttöönotto vaatii?
- Mitä asioita tulee huomioida suunnitteluvaiheessa?

Koska opinnäytetyö pyrkii muutokseen työn toimeksiantajalle, on kyseeseen valittu interventionistinen tutkimusote (Kananen 2017, 10). Samalla suunnitellaan Zero Trust -arkkitehtuurin käyttöönottoa olemassa olevan verkkoinfrastruktuuriin pohjautuen.

Opinnäytetyö pohjautuu tutkittuun tietoon ja aiempaan teoriapohjaan, joten työhön soveltuva tutkimusote on kehittämistutkimus. Opinnäytetyön aikataulujen puitteissa on myös mahdollista olla mukana muutosprosessissa, jolloin tutkimusote siirtyy toimintatutkimukseksi (Kananen 2017, 13). Aineiston keruun päämenetelmänä toimii sekundäärinen aineisto. Aineiston muodostaa pääasiassa dokumentaatiot, aiemmat tutkimukset, white paperit, verkkosivut sekä nykyisen verkkoinfrastruktuurin dokumentaatio. Primääriaineisto painottuu muistiinpanoihin.

Koska opinnäytetyön interventioprosessin muutoksella ei ole selviä mitattavia arvoja, aineiston analyysimenetelmänä käytetään prosessin raportointia (Kananen 2017, 67). Opinnäytetyön luotettavuuden arvioinnissa käytetään muutoksen toimivuutta ja vaikutusta. Myös Pernaa käyttää näitä määreitä artikkelissaan (2013, 8), lisäten vielä muun muassa siirrettävyyden. Mikäli opinnäytetyössä ollaan mukana muutosprosessissa, luotettavuus arvioidaan myös testaamisen muodossa.

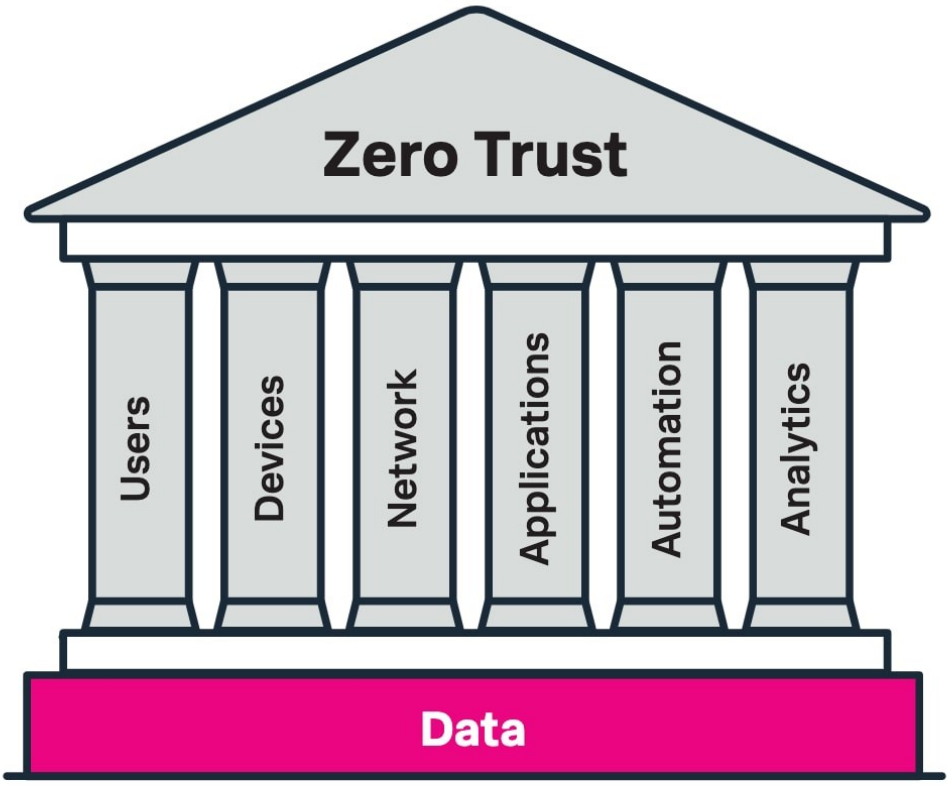
3 ZERO TRUST -KONSEPTI

Zero Trust -konsepti on saanut alkunsa vuonna 2010, kun Forrest Research yhtiön analyytikko John Kindervag esitteli raportin (2010) ”No More Chewy Centers: Introducing The Zero Trust Model Of Information Security”. Raportti esittelee yleiset ongelmat liittyen perinteisiin verkkojen suunnitelmiin, jotka pohjautuvat luotettuihin ja epäluotettuihin alueisiin.

Zero Trust -konseptin hyödyntämisessä lisätään yhtiön verkkoon tietoturvaa myös sisäiseen liikenteeseen. Perinteisesti yhtiön sisäverkko on ollut luotettava, eikä sisään päässeeltä käyttäjältä, laiteelta tai ohjelmalta vaadita lisätunnistautumista. Zero Trustissa tämä ajatustapa muutetaan niin, ettei mikään osa ole luotettava, vaan pääsy pyydettyyn resurssiin autentikoidaan joka kerta sekä kaikki liikenne salataan. Tästä syntyy konseptin yhteydessä käytetty kuvaus: ”never trust, always verify”. (Bobbert & Scheerder 2020, 5–6; Rose ym. 2020, 4–7; Buck ym. 2021.)

Zero Trust -konseptin kolme pääperiaatetta esiteltiin Kindervagin raportissa (2010, 8–9):

1. Varmista kaikkien resurssien käyttö turvallisesti sijainnista riippumatta.
2. Ota käyttöön vähimmän käyttöoikeuden strategia ja valvo tarkasti pääsyoikeuksia.
3. Tarkista ja kirjaa kaikki liikenne.



Kuva 1. Zero Trustin peruspilarit (The American Council for Technology 2019)

Zero Trust -konsepti rakentuu useamman peruspilarien varaan. Yksi malli peruspilareista on kuvattuna kuvan 1 tapaan. Osassa määrityksiä automaatio ja analytiikka on niputettu yhteen tai korvattu omaan määritykseen paremmin sopivalla termillä.

Käyttäjät

Microsoft luonnehtii omassa dokumentissaan (2022) käyttäjät identiteetiksi, olipa sitten kyseessä henkilö, palvelu tai IoT-laite. Kun identiteetti yrittää käyttää resurssia, tarkistetaan identiteetti vahvalla todennuksella ja varmistetaan, että pääsy on kyseisen identiteetin mukainen ja tyypillinen. Vähimmän käyttöoikeuden periaatetta tulee noudattaa.

Cybersecurity and Infrastructure Security Agency määrittää (2021, 6–7) tämän pilarin olevan Zero Trust -konseptin ydin. Vähimmän käyttöoikeuden periaate riippuu kyvystä varmistaa vastaanotettava identiteetti. Tämän takia Zero Trustin malli siirtyy pois pelkän sanasanan käyttämisestä kohti useamman tekijän yhdistelmää, jossa todennetaan identiteetti koko palvelun tai tiedon vuorovaikutuksen ajan.

The American Council for Technology määrittää (2019, 6) samalla tavoin luotettavien käyttäjien jatkuvan autentikoinnin ensiarvoisen tärkeäksi. Tämä kattaa identiteetin sekä teknologiat kuten valtuutus, käyttöoikeuksien hallinta, monivaiheinen autentikointi, jatkuva seuranta sekä käyttäjän luotettavuuden hallinta ja validointi. Tärkeitä ovat myös teknologiat käyttäjien vuorovaikutuksen turvaamiseksi ja suojaamiseksi, kuten perinteiset web-yhdyskäytävän ratkaisut.

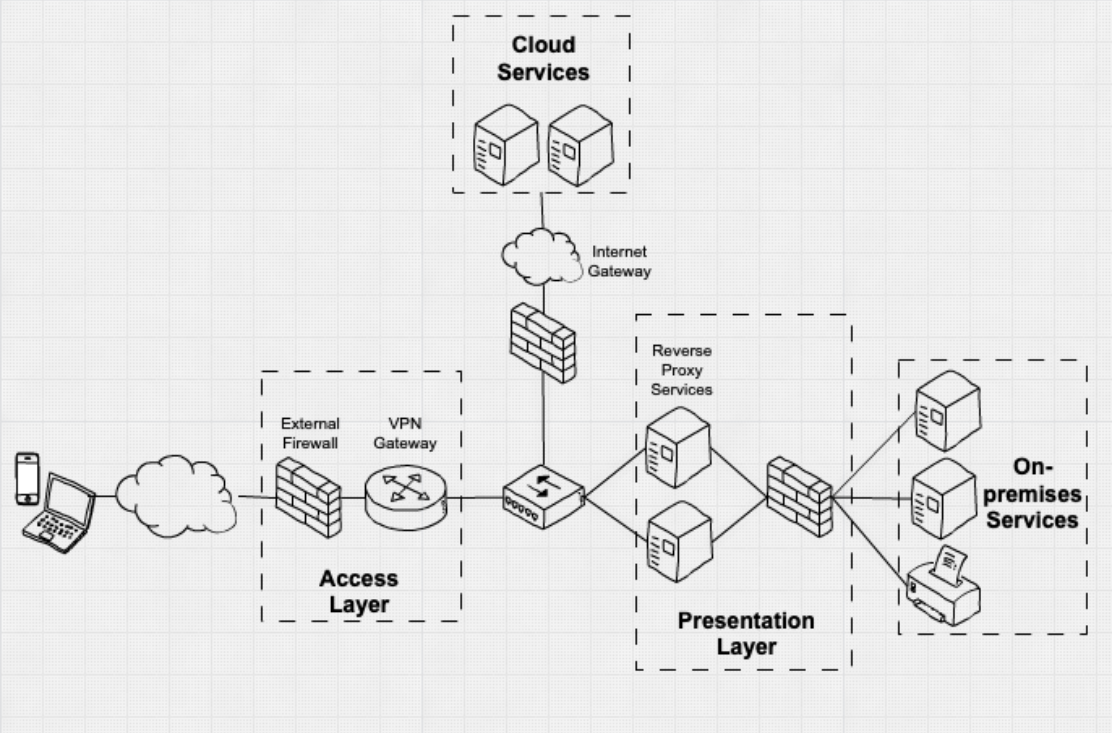
Laitteet

Laitteella kuvataan mitä tahansa laitetta, joka voi olla yhteydessä verkkoon, kuten IoT-laitteet, älypuhelimet, kannettavat tietokoneet, palvelimet omassa konesalissa tai pilvipalveluna, BYOD-laitteet ja niin edelleen. Näiden laitteiden inventointi, luotettavuuden arviointi ja luvattomien laitteiden pääsynhallinta on perustavanlaatuinen ominaisuus Zero Trustin lähestymistapaan. (The American Council for Technology 2019, 6; Cybersecurity and Infrastructure Security Agency 2021, 8–9; Microsoft 2022.)

Verkko

The American Council for Technology esittää määritelmässään (2019, 6), että Zero Trust -verkkoa kuvattaisiin joskus kehättömiksi. Tämä kuitenkin on harhaanjohtavaa, sillä Zero Trust -verkko yrittää siirtää kehät sisään verkon reunalta ja segmentoida sekä eristää kriittiset tiedot muista tiedoista. Kehä on edelleen olemassa, vaikkakin paljon rakeisemmalla tavalla. Perinteisen infrastruktuurin palomuurin kehä ”linna ja vallihauta” -lähestymistapa ei riitä. Kehän on siirryttävä lähemmäksi tietoja mikrosegmentoimalla suojausten ja ohjausten vahvistamiseksi.

National Cyber Security Center määrittää (2021b) ”linna ja vallihauta” -lähestymistavan perinteiseksi VPN-etäyhteydeksi, jossa on vahva ulkokehä ja useampia sisäisiä kerroksia, jotka erotetaan palomuureilla. Tästä mallista käytetään termiä ”Walled Garden”. Tämä malli on esitettynä kuvassa 2.



Kuva 2. Walled Garden -malli (National Cyber Security Center 2021b)

Kuvan 2 mukaiset avainkomponentit yleisellä tasolla kuvattuna ovat Access Layer, jonka tehtävä on todentaa etäyhteyttä pyytävän päätelaitteen. Verkkoliikenne on loukussa täällä, ellei se voida autentikoida paikallisiin palveluihin. Presentation Layer hoitaa välityksen sisäisiin palveluihin politiikan perusteella. Ydinverkko koostuu On-premises palveluista. Lisäksi on Internet-

yhdyskäytävä, joka tarjoaa pääsyn välityspalvelimen kautta sivustoille ja yrityksen pilvipalveluihin.

Cybersecurity and Infrastructure Security Agency suosittaa (2021, 10–11) yhdenmukaistamaan verkon segmentoinnin ja suojaukset sovellusten työnkulkujen mukaan, perinteisen implisiittisen luottamuksen sijaan. Microsoft määrittääkin (2022) tämän tärkeäksi, jotta näkyvyys paranee ja sivusuuntainen liikkuminen verkon yli estyisi.

The American Council for Technology mainitsee (2019, 6) vielä ohjelmistopohjaiset verkot, jotta näkyvyys tehdä dynaamisia poliitikkoja ja luottamuspäätöksiä verkko- ja dataliikenteestä olisi mahdollista. Kyky segmentoida, eristää ja hallita verkkoa on edelleen keskeinen turvallisuudelle ja välttämätön Zero Trust -verkolle.

Sovellukset

The American Council for Technology määrittää (2019, 6) sovelluskerroksen turvaamisen ja asianmukaisen hallinnan sekä konttien ja virtuaalisten koneiden hallinnan keskeiseksi osaksi Zero Trust -arkkitehtuurissa. Kyky tunnistaa ja hallita sovelluspinoa helpottaa tekemään tarkempia ja rakeisempia päätöksiä pääsyoikeuksille.

Microsoft mainitsee (2022) myös tärkeäksi määrittää kontrollit ja tekniikat varjo-IT:n löytämiseksi. Muun muassa McAfee määrittää (s.a.) varjo-IT:n lyhyesti tietotekniikan hankkeisiin, joita hallinnoidaan IT-osaston ulkopuolella ja tietämättä. Myös sovellusten asianmukaiset sisäiset käyttöoikeudet, reaaliaikainen analytiikka, epänormaalin käyttäytymisen seuranta ja käyttäjien toimien hallinta ovat tärkeitä.

Automaatio

The American Council for Technology (2019, 7) mainitsee tietoturva-automaation reagointityökaluja tehtävien automatisoinnin työnkulkujen avulla samalla mahdollistaen loppukäyttäjän valvonnan ja vuorovaikutuksen.

Microsoft määrittää (2022) automaation tärkeyden sillä, että lisääntynyt näkyvyys tuottaa suuremman määrän asiaankuuluvia hälytyksiä. Automaation

avulla tämä tietovirta tulee paremmin hallittavaksi ja luottamus tapahtuman vahvistamiseen kasvaa.

Analytiikka

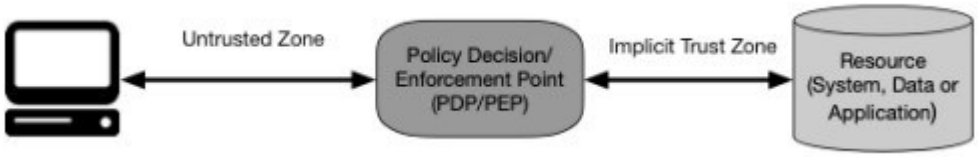
The American Council for Technology (2019, 7) dramatisoi määritelmässään analytiikan tärkeyttä ”uhkaa, jota ei näe tai ymmärrä, ei voida torjua”. Työkalujen hyödyntämistä kuten tiedonhallintaa, kehittyneitä analytiikka-alustoja, käyttäjän käyttäytymisen analytiikkaa sekä muita analytiikkajärjestelmiä voidaan käyttää reaaliaikaiseen seurantaan tapahtumista ja suunnata puolustusta älykkäämmin. Keskittyminen analyysiin tapahtumatiedoista voi auttaa kehittämään ennakoivia turvatoimenpiteitä ennen varsinaista tapahtumaa.

Data

Kaiken perustana on data. Data on se, jota halutaan suojella. Microsoft määrittää (2022) datan pysymistä turvassa, vaikka se poistuisi organisaation hallitsemista laitteista, sovelluksista, infrastruktuurista tai verkosta. Dataa tulisi luokitella, nimiöidä, salata ja rajoittaa pääsyä noiden määritteiden perusteella.

3.1 Zero Trustin teoreettinen malli

Rose ym. (2020, 5) kuvaa dokumentissaan, kuinka Zero Trustin teoreettisessa mallissa pääsy erotellaan ei-luotettuun alueeseen sekä implisiittisesti luotettavaan alueeseen. Mallin tavoitteena on pienentää implisiittinen luotettava alue mahdollisimman pieneksi tuoden päätöksenteko käyttöoikeudesta mahdollisimman lähelle resurssia. Kuvassa 3 on kuvattuna Zero Trustin teoreettinen malli, jossa päätöksenteko käyttöoikeudesta tuodaan mahdollisimman lähellä resurssia. Käyttöoikeus myönnetään Policy Decision Pointin ja vastaavan Policy Enforcement Pointin välillä.



Kuva 3. Zero Trustin teoreettinen malli (Rose ym. 2020)

IETF kuvaa dokumentissaan (2000, 4–6) näitä pääsynhallinnan kahdeksi arkkitehdin tärkeäksi elementiksi. Näiden kahden elementin kommunikointi alkaa

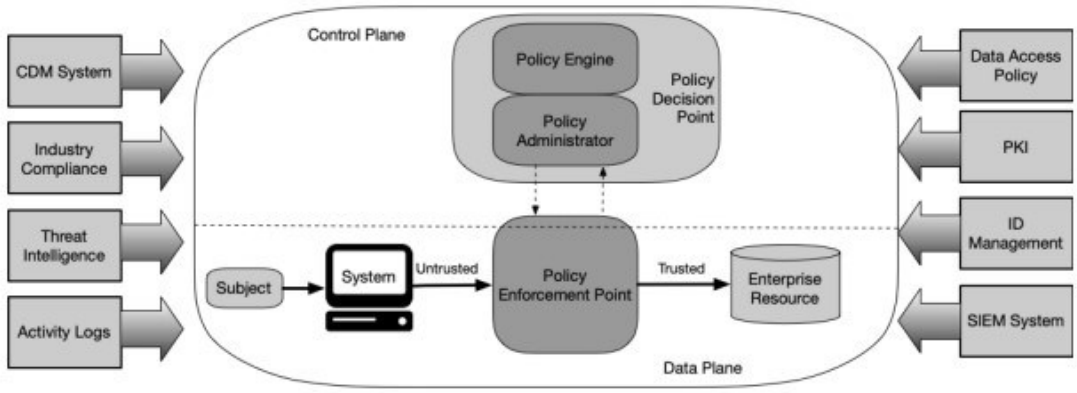
Policy Enforcement Pointin (PEP) toimesta. PEP vastaanottaa ilmoituksen tai viestin, joka vaatii politiikan päätöstä. PEP muotoilee tästä pyynnön, jonka se lähettää Police Decision Pointille (PDP). PDP palauttaa päätöksen PEP:lle, joka panee täytäntöön tämän hyväksyen tai hyläten pyynnön.

Järjestelmän on varmistettava, että kohde on autentikoitu ja pyyntö on pätevä. PDP/PEP antaa asianmukaisen tuomion, jotta kohde pääsee resurssiin. Tämä tarkoittaa, että Zero Trust koskee kahta perusaluetta: autentikointia ja valtuutusta. Järjestelmän tulisi pystyä vastaamaan esimerkiksi seuraavanlaisiin kysymyksiin: mikä on luottamuksen taso kohteen henkilöllisyydestä tätä ainutlaatuista pyyntöä varten? Onko pääsy resurssiin sallittu, kun otetaan huomioon luottamuksen taso suhteessa kohteen henkilöllisyyteen? Onko pyyntöön käytetyllä laitteella oikea turvallisuuskanta? Onko muita tekijöitä, jotka tulisi ottaa huomioon ja jotka muuttavat luottamustasoa (esimerkiksi aika, kohteen sijainti, kohteen turvallisuuskanta)?

Jotta PDP/PEP voi olla mahdollisimman tarkka, implisiittisen luottamusvyöhykkeen on oltava niin pieni kuin mahdollista. Zero Trust tarjoaa joukon periaatteita ja käsitteitä PDP:n/PEP:n siirtämisestä lähemmäksi resurssia. Ajatuksena on nimenomaisesti autentikoida ja valtuuttaa kaikki aiheet, resurssit ja työnkulut, jotka muodostavat yrityksen resurssit.

3.2 Zero Trustin loogiset komponentit

Rose ym. (2020, 9–10) kuvaa dokumentissaan Zero Trustin loogisia komponentteja, jotka muodostavat Zero Trust -arkkitehtuurin käyttöönoton. Näitä komponentteja voidaan käyttää paikallisena palveluna tai pilvipohjaisen palvelun kautta. Kuvan 4 käsitteellinen malli osoittaa komponenttien välisen suhteen ja niiden vuorovaikutuksen. Tämä on ihanteellinen malli, joka näyttää loogiset komponentit ja niiden vuorovaikutukset. Zero Trust -arkkitehtuurin loogiset komponentit käyttävät erillistä Control Planea kommunikointiin, kun sovellustiedot kommunikoivat Data Planella.



Kuva 4. Zero Trustin loogiset komponentit (Rose ym. 2020)

Kuvan 4 mukaisesti Rosen ym. (2020, 9–10) mukaan PDP jaotellaan kahteen loogiseen komponenttiin: Policy Engineen (PE) ja Policy Administratoriin (PA). PE on vastuussa lopullisesta myöntämispäätöksestä resurssiin pääsystä. PE käyttää tehtyjä politiikkoja sekä ulkoisista lähteistä saatua tietoa luottamusalgoritmin syötteenä myöntämistä, kieltämistä tai peruuttamista varten. PE on parina PA kanssa. PE tekee ja kirjaa päätöksen (kuten hyväksytty tai evätty), ja PA on vastuussa yhteyden perustamisesta ja/tai sulkemisesta kohteen ja resurssin välillä. Jos istunto on hyväksytty ja pyyntö autentikoitu, PA määrittää PEP sallia istunnon aloitus. Jos istunto evätään tai aiempi hyväksyntä perutaan, PA signaloi PEP sammuttamaan yhteyden. Jotkut toteutukset voivat käsitellä PE ja PA yhtenä palveluna. PA kommunikoi PEP:n kanssa luotaessa yhteyttä. Tämä viestintä tapahtuu Control Planen kautta. PEP on yksi looginen komponentti Zero Trust -arkkitehtuurissa, mutta se voidaan jakaa kahteen eri komponenttiin: asiakkaaseen (esimerkiksi agentti kannettavassa tietokoneessa) ja resurssiin (esimerkiksi yhdyskäytävän komponentti resurssin edessä, joka ohjaa pääsyä). Loogisena komponenttina toimii myös yhden portaalin komponentin, joka toimii portinvartijana yhteyttä varten. PEP:n ulkopuolella on luotettu alue, jossa resurssit sijaitsevat. Ydinkomponenttien lisäksi Zero Trust -arkkitehtuuri käyttää ja tarvitsee useita tietolähteitä, jotka antavat dataa PE päätöksen tekoa varten.

4 ZERO TRUST -ARKKITEHTUURIN LÄHESTYMISTAPOJA

Kuten Romness ym. (2022) mainitsee artikkelissaan, Zero Trust on arkkitehtoninen lähestymistapa, joten sen määrittelyssä ja lähestymistavoissa on lukuisia muunnelmia. Yhteinen piirre kuitenkin kaikille näille on resurssien

saatavuuden valvominen mahdollisimman rakeisesti sekä identiteetin vahvistaminen joka kerta ennen pääsyn myöntämistä.

Alkuperäisen konseptin esitellyt yritys Forrest Research on jatkokehittänyt Zero Trust -konseptia, joka heidän määritelmällänsä kulkee nimellä Zero Trust eXtended (ZTX) Ecosystem. Julkaistun dokumentin mukaan alkuperäinen Zero Trust -konsepti ymmärrettiin liian tietoverkkokeskeisesti, jossa keskityttiin vain pääsääntöisesti segmentoimaan verkkoa käyttäen seuraavan sukupolven palomuureja. (Cunningham 2018, 3.)

The American Council for Technologyn mukaan (2019, 7) myös Gartnerin kehittämä Continuous Adaptive Risk and Trust Assessment -malli on yksi Zero Trust -arkkitehtuurin lähestymistapa. Gartnerin määritelmä tälle lähestymistavalle on, kuinka turvallisuutta kehitetään jäykästä ja reaktiivisesta kohti joustavaa ja ennakoivaa. Tässä lähestymistavassa jatkuva monitorointi ja analytiikka ovat keskiössä, mahdollistaen nopean havainnoinnin ja reagoinnin poikkeavaan käyttäytymiseen. (Forcepoint 2017, 2–3.)

Alkuperäiseen Forrest Researchin Zero Trust -konseptiin perustuen National Institute of Standards and Technology antoi oman määritelmänsä Zero Trust -arkkitehtuurin lähestymistapaan. National Institute of Standards and Technology on Yhdysvaltojen liittovaltion hallituksen ulkopuolinen virasto, jonka tehtävänä on edistää tekniikkaa, mittaustiedettä ja standardeja pitääkseen amerikkalaiset yritykset kilpailukykyisinä (National Institute of Standards and Technology 2022).

National Institute of Standards and Technology on kuvannut dokumentissaan (Rose ym. 2020, 11) lähestymistavat kolmeen malliin: tehostettuun identiteettiin, mikrosegmentaatioon ja Software Defined Perimeteriin. Dokumentissa kuvataan, että kukin lähestymistapa toteuttaa kaikki Zero Trustin toimintatavat, mutta se voi käyttää yhtä tai kahta tärkeimpänä ohjaavana politiikkana. Täydellinen Zero Trust -ratkaisu käyttää näitä kaikkia kolmea lähestymistapaa.

Tähän opinnäytetyöhön on valittu National Institute of Standards and Technologyn määritelmän mukainen lähestymistapa. Opinnäytetyöhön valittujen valmistajien ratkaisuja tarkastellaan myöhemmin.

4.1 Tehostettu identiteetti -malli

Tehostetun identiteetin -mallissa käytetään toimijoiden identiteettiä politiikan luomisen keskeisenä osana. Tässä mallissa yrityksen resurssien käyttöoikeudet perustuvat identiteettiin ja määriteltyihin ominaisuuksiin. Ensisijainen vaatimus resurssin käyttöoikeudelle määräytyy myönnettyihin käyttöoikeuksiin. Muut tekijät, kuten käytetty laite, resurssin tila ja ympäristötekijät voivat muuttaa lopullista luottamustason tulosta. Tulosta voidaan räätälöidä myös niin, että myönnetään vain osittainen pääsy tiettyyn tietolähteeseen verkon sijainnin perusteella. Mallia käytetään organisaatiossa, joissa on käytössä avoin verkko, vierailijaverkko tai usein käytössä olevia ei-organisaation hallinnoimia laitteita (esimerkiksi kolmannen osapuolen urakoitsija). Malli sopii myös hyvin käytettäväksi pilvipohjaisiin sovelluksiin tai palveluihin, joihin ei saada organisaation omia Zero Trust -komponentteja käyttöön. Tällaisia on monet Software as a Service -palvelut. (Rose ym. 2020, 11–12.)

4.2 Mikrosegmentaatio-malli

Mikrosegmentaatio-mallissa verkkoinfrastruktuuriin sijoitetaan yhdyskäytävän turvakomponentti toimimaan politiikan täytäntöönpanopisteenä yksittäisen tai pienen ryhmän resurssin suhteen. Näitä ovat älykkäät kytkimet, reitittimet tai seuraavan sukupolven palomuurit, jotka antavat tai estävät pääsyn pyydettyyn resurssiin. Vaihtoehtoisesti myös päätelaitteeseen asennettavaa ohjelmaa voidaan käyttää. Tässä mallissa edellytetään identiteetin hallinto-ohjelman toimimista täysin, perustuen kuitenkin yhdyskäytävän komponentteihin, jotka toimivat politiikan täytäntöönpanopisteinä suojaten resursseja luvattomalta käytöltä ja löytymiseltä. (Rose ym. 2020, 12.)

4.3 Software Defined Perimeter -malli

Software Defined Perimeter -mallissa käytetään hyväksi verkkoinfrastruktuurin overlay- ja underlay-verkkoja. Yleensä tämä tehdään OSI-kerroksella seitsemän, mutta on myös mahdollista toteuttaa alemmilla kerroksilla. Tässä mallissa Zero Trust -komponentti hoitaa verkon kontrollerin virkaa, joka perustaa ja konfiguroi verkon. Tästä mallista käytetäänkin usein nimitystä Software Defined Perimeter ja usein se sisältää konsepteja ohjelmistopohjaisesta verkosta

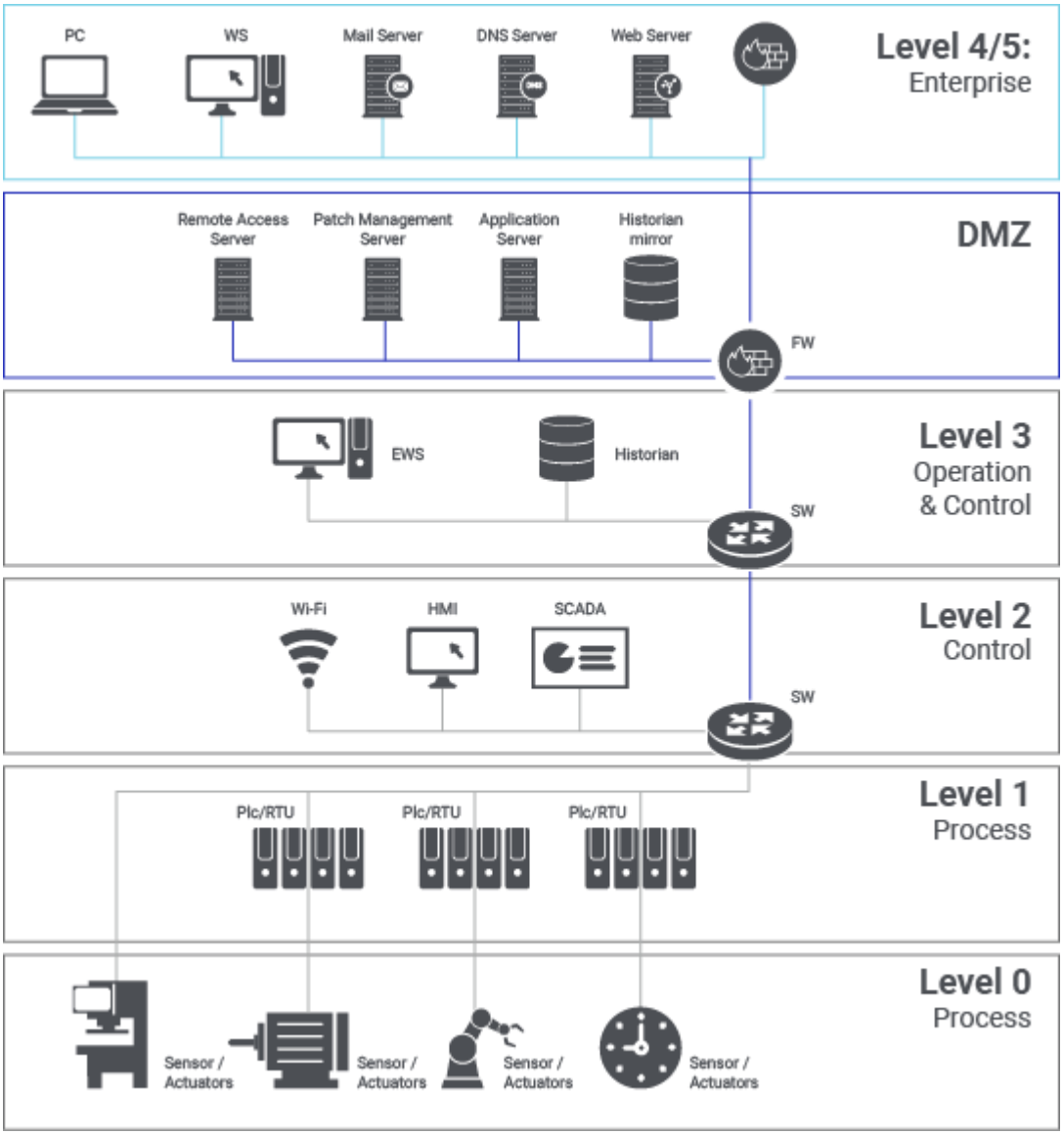
ja oivaltavasta verkosta. Yleisin toteutustapa on agentti/yhdyskäytävä-malli, jossa agentti luo salatun kommunikaatiokanavan resurssin välille. Erilaisia muunnoksia tästä mallista voi olla esimerkiksi virtuaalisissa verkoissa tai ei-IP-pohjaisissa verkoissa. Siksi tätä mallia pidetään edistyksellisimpänä toteutuksena. (Rose ym. 2020, 12–13; Koilpillai & Murray 2020, 6.)

VMware määrittää (s.a.) oivaltavan verkon olevan teknologiakonsepti, jonka tavoitteena on soveltaa syvempää älykkyyttä ja aiottua tilaa korvaamaan verkkojen konfiguroinnin manuaaliset prosessit ja verkko-ongelmiin reagoiminen. Sen sijaan verkon ylläpitäjät määrittelevät lopputuloksen tai liiketoiminnan tavoitteen, tarkoituksen ja verkon ohjelmisto selvittää miten tämä tavoite saavutetaan tekoälyn ja koneoppimisen ansiosta.

5 TEOLLISUUSAUTOMAATIOVERKKOJEN NYKYTILA

Purdue-malli, muodollisemmin Purdue Enterprise Reference Architecture (PERA), on rakenteellinen malli teollisuuden valvontajärjestelmän (ICS) turvallisuudelle, joka koskee fyysisiä prosesseja, antureita, valvontaa, toimintaa ja logistiikkaa. Theodore J. Williamsin ja Purduen yliopistokonsortion jäsenten 1990-luvulla kehittämä Purdue Enterprise Reference Architecture määrittelee tuotantolinjoissa käytettävän kriittisen infrastruktuurin eri tasot ja miten ne voidaan turvata. (Williams ym. 2001, 16.)

Zscaler (s.a.) on kuvannut Purdue-mallin infrastruktuurin tasot kuvan 5 mukaisesti.



Kuva 5. Perinteinen Purdue-mallin mukainen ICS-järjestelmä (Zscaler s.a.)

Level 4/5 Enterprise

Taso 4 ja/tai 5 on tyypillisesti IT-verkko sellaisena kuin sen tunnemme.

DMZ tai Industrial DMZ

Demilitarisoitu taso, joka sisältää turvajärjestelmät kuten palomuurit. Tasoa käytetään IT- ja OT-maailmojen erottamiseen tai ilmarakoon. Tässä IT- ja OT-maailmat lähentyvät, mikä lisää OT-järjestelmien hyökkäyspintaa. Tasosta voidaan käyttää myös numerollista ilmausta 3.5.

Level 3 Operation & Control

Tasolla 3 hallitaan tuotannon työnkulkua ohjaamosta. Käyttöjärjestelmiin perustuvia räätälöityjä järjestelmiä, kuten Windowsia, käytetään erähallinnan suorittamiseen, tietojen tallentamiseen sekä toimintojen ja laitoksen

suorituskyvyn hallintaan. Tämä taso koostuu myös tietokannoista tai historioitsijoista operaatiotietojen tallentamiseksi.

Level 2 Control

Supervisory Control And Data Acquisitionia (SCADA) käytetään fyysisten prosessien valvontaan, seuraamiseen ja hallintaan. SCADA voi hallita järjestelmiä pitkillä etäisyyksillä laitosten fyysisestä sijainnista, kun taas Distributed Control System (DCS) ja Programmable Logic Controllers (PLC-laitteet) otetaan yleensä käyttöön laitoksessa. DCS- ja PLC-laitteisiin liitetty ihmisen ja koneen käyttöliittymä mahdollistaa perusvalvonnan ja seurannan, kun taas SCADA-järjestelmät yhdistävät tiedot ja lähettävät sen ylävirtaan historioitsijan tallentamista varten tasolle 3. PLC:ssä ei yleensä ole näppäimistöjä ja näyttöjä. Remote Terminal Unitsin (RTU) avulla operaattorit voivat kirjautua SCADA-järjestelmiin. Tämän kerroksen laitteet ja strategiat kommunikoivat tyypillisesti modbus- ja dnp3-protokollien kautta, ja datadiodit voivat auttaa vahvistamaan turvallisuutta.

Level 1 Process

Fyysisten prosessien tunnistaminen ja manipulointi tapahtuu tällä tasolla prosessiantureilla, analysaattoreilla, aktuaattoreilla ja niihin liittyvillä instrumenteilla. Tehokkuuden parantamiseksi anturit kommunikoivat yhä enemmän suoraan toimittajan seurantaohjelmistonsa kanssa pilvessä matkapuhelinverkkojen kautta.

Level 0 Process

Määrittää todelliset fyysiset prosessit.

Energiayhtiössä ja muissa teollisissa ympäristöissä, ongelman aiheuttaa ICS-järjestelmän ulottaminen Zero Trust -konseptiin koko infrastruktuurin tasolla. Perinteinen OT-järjestelmä on suunniteltu aikana, jolloin tietoturva ei ole ollut ohjaava tekijä. Nykyisin myös OT-järjestelmä on yhteydessä yrityksen muuhun verkkoinfrastruktuuriin, jolloin tämä aiheuttaa ongelman Zero Trust -konseptin implementointiin. Vaikka Purdue-malli pyrkii tuomaan OT-järjestelmään tietoturvaa, perinteinen OT-verkko on usein flat-mallinen. Tällöin koko OT-verkko on samassa osoitealueessa. Tämä tulee huomioida suunnittelussa, jotta muutokset OT-verkkoon eivät aiheuta tuotantolaitokseen häiriötilannetta.

Zero Trust -arkkitehtuuri tulee vaatimaan aktiivista monitorointia sekä politiikkojen hienosäätöä, joten järjestelmää ylläpitävä resurssi on huomioitava henkilöstössä. Zero Trust -arkkitehtuurin käyttöönotto tulee olemaan aikaa vaativa prosessi, joten myös tämä on hyvä huomioida henkilöstöresursseissa. (Jacobs s.a.)

6 SUUNNITTELU

Zero Trustin suunnitteluun ja käyttöönottoon löytyy ohjeita niin valmistajilta kuin virastoilta. Ohjeet koostuvat ja painottavat hieman eri asioita riippuen mihin ympäristöön Zero Trustia on tarkoitus ottaa käyttöön. Yleisohjeita löytyy niin valmistajilta kuin virastoilta.

Muun muassa Ison-Britannian National Cyber Security Center on julkaissut (2021a) yleisiä periaatteita, jotka ovat tärkeitä Zero Trust -arkkitehtuuria suunniteltaessa. Tässä painotetaan heti alkuun, että on tärkeää tietää ja tunnistaa arkkitehtuuri, johon Zero Trustin konseptia ollaan tuomassa. Samaa tärkeyttä painottaa myös Rose ym. (2020, 37) omassa ohjeistuksessaan lisäten, että vajavainen tieto voi johtaa liiketoimintaprosessin epäonnistumiseen, jos Policy Engine estää pyynnöt riittämättömien tietojen vuoksi. Tämä on erityinen ongelma, jos yrityksellä on tuntemattomia varjo-IT:n käyttöönottoja.

Arkkitehtuurin kartoituksen jälkeen on tärkeää tehdä riskianalyysi. Rose ym. (2020, 37) tuo esille tähän Risk Management Frameworkin, joka on Yhdysvaltojen liittohallituksen ohje, standardi ja prosessi riskienhallinnalle National Institute of Standards and Technologyn kehittämien tietojärjestelmien turvaamiseksi (National Institute of Standards and Technology 2020, 1–2). Myös National Cyber Security Center suosittaa riskianalyysin tekoa, lisäten tähän vielä uhkamallinnuksen (2021a). Suomen Standardisoimisliitolta löytyy ISO/IEC 27005:2018 -standardi, joka ohjeistaa tietoturvariskien hallintaan (SFS 27005:2018).

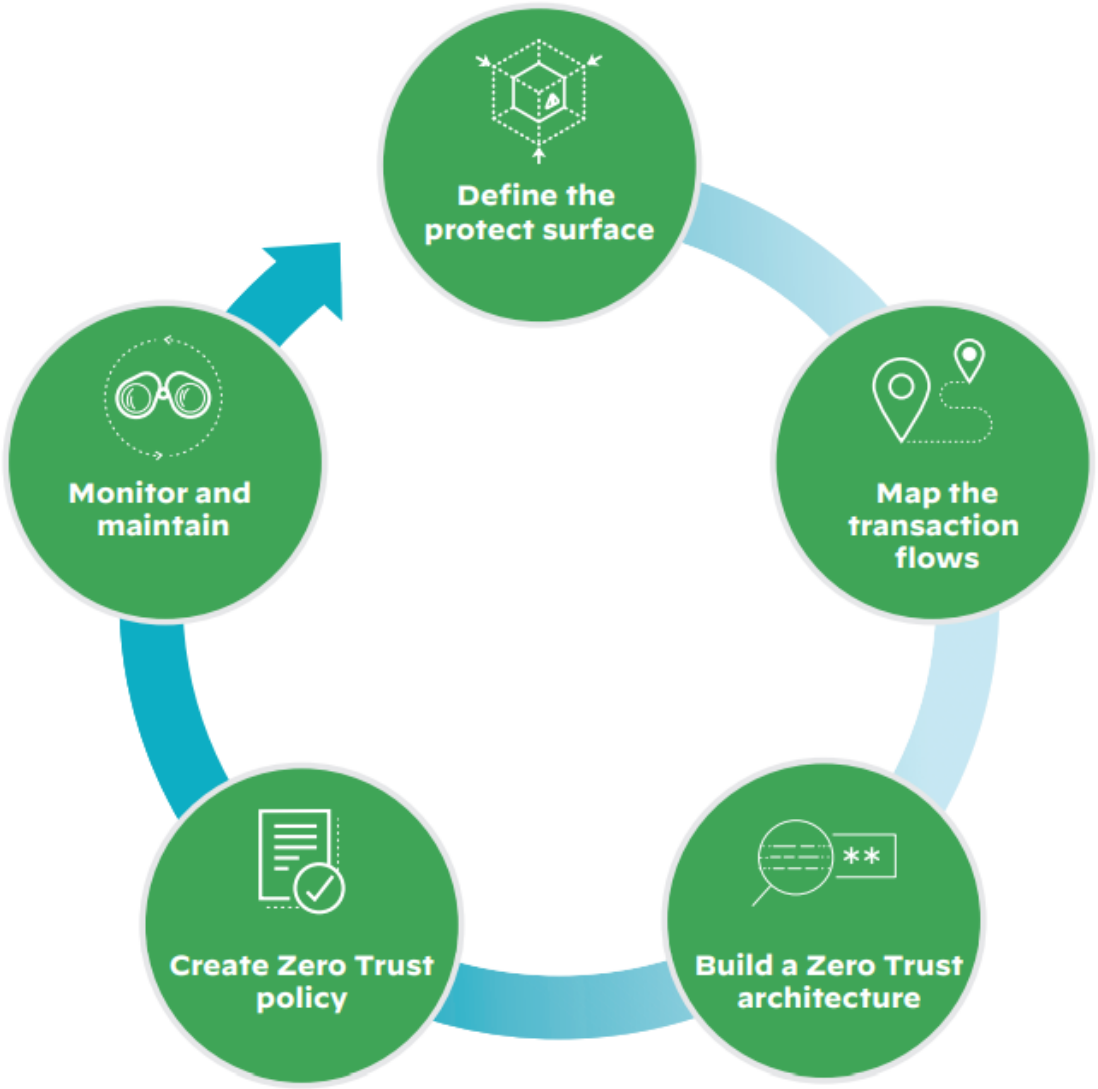
National Cyber Security Center tuo esille (2021a) identiteetin, joka on yksi tärkeimmistä tekijöistä päätettäessä, annetaanko pääsyä resurssiin. Tätä identiteettiä kuvastaa ihminen, palvelu tai laite. Myös Rose ym. (2020, 38) painottaa identiteetin tärkeyttä, tuoden esille ryhmän käyttäjiä, joilla on erityisiä

oikeuksia, kuten kehittäjät ja ylläpitäjät. Nämä käyttäjät vaativat lisävalvontaa, sillä heillä saattaa olla yleinen lupa käyttää kaikkia yrityksen resursseja.

Rose ym. (2020, 40) tuo esille oikeanlaisen yritysprosessin valinnan tärkeyttä. Jotkin yrityksen prosessit sopivat paremmin eri Zero Trustin lähestymistapaan kuin toiset. Samoin eri valmistajien tuotteet sopivat paremmin eri Zero Trustin lähestymistapaan kuin toiset. Rose ym. ehdottaakin mallintamaan olemassa olevan yritysprosessin pilottiohjelmaksi. National Cyber Security Center painottaa (2021a) omassa ohjeistuksessa standardien merkitystä. Standardit mahdollistavat laitteiden ja palveluiden yhteen toimivuuden. Esimerkki tämmöisestä on autentikointi ja valtuutus, jossa muun muassa OAuth- tai SAML-standardit tarjoavat yhteen toimivuuden.

Kattava monitorointi on yksi avain tekijä Zero Trust -konseptissa. National Cyber Security Center korostaakin (2021a) tätä tärkeyttä sillä, että tulee tietää mitä toimintoja laitteet, käyttäjät ja palvelut suorittavat ja mitä tietoja he käyttävät. Seurannan tulisi linkittyä takaisin asetettuihin politiikkoihin. Rose ym. (2020, 40–41) tuo esille vaihtoehdon, jossa suunniteltu ja luotu politiikka toimisi tarkkailu- ja monitorointitilassa alkuun. Tällä varmistettaisiin, että luodut politiikat olisivat tehokkaita ja toimivia. Samalla yritys saisi käsityksen resurssin käyttöpyynnöistä, käyttäytymisestä ja kommunikaatiokuvioista.

Valmistajista Palo Alto Networksilla ja Fortinetillä on toistensa kaltaiset ohjeistukset laadittu Zero Trust -arkkitehtuuria suunniteltaessa. Palo Alto Networks suosittaa (2021a) käyttämään Zero Trust -arkkitehtuuria suunniteltaessa kuvan 6 mukaista suunnittelukehää. Kehä on viisivaiheinen ja jokaista suojapintaa kohden kehämalli pyörähtää ympäri.



Kuva 6. Palo Alto Networksin suosittelema Zero Trustin suunnittelukehä (Palo Alto Networks 2021a)

Suojapinnan määritteleminen on Zero Trust -arkkitehtuuria suunniteltaessa tarkistuslistan ensimmäinen kohta. Fortinet määrittää (s.a.) tämän tärkeyden niin, että hioen tätä vältytään hukkumiselta politiikkojen ja työkalujen käyttöönotossa koko verkon alalta. Määrittelyssä tulisi keskittyä arvokkaimpaan digitaaliseen omaisuuteen. Palo Alto Networks esittelee (2021a, 10–11) tätä työtä helpottaakseen DAAS-menetelmän käyttöä. DAAS on lyhenne sanoista Data, Applications, Assets ja Services. Jokainen kriittinen DAAS-elementti on joko osa suojapintaa tai itse suojapinta. Jokainen suojapinta mikrosegmentoidaan omakseen käyttäen seuraavan sukupolven palomuuria.

Kriittisten DAAS-elementtien ja käyttäjien väliset tapahtumavirrat kartoitetaan seuraavaksi Palo Alto Networksin ohjeen (2021a, 11–12) mukaan. Tämä auttaa ymmärtämään niiden keskinäisiä riippuvuuksia. Kenellä on

liiketoiminnallisia syitä käyttää kutakin elementtiä, millä tavalla ja milloin. Kartoitus auttaa ymmärtämään miten luodaan suojauspolitiikka, joka sallii vain valtuutettujen käyttäjien pääsyn tiettyihin tietoihin ja resursseihin määritettyjen sovellusten avulla käyttäen vähimmän käyttöoikeuden periaatetta.

Kun on ymmärrys suojapinnasta ja tapahtumavirroista, aloitetaan Zero Trust -arkkitehtuurin suunnittelu sen perusteella, mikä on arvokasta. Palo Alto Networks suosittaa (2021a, 12) kehitettäessä arkkitehtuuria pitämään mielessä helppokäyttöisyyden, ylläpidon sekä joustavuuden suojapinnan ja liiketoiminnan muutosten suojaamiseksi. Zero Trust -arkkitehtuurin kulmakivi on Palo Alto Networksin mukaan (2021a, 12) mikrosegmentointi. Mikrosegmentointi tulisi tehdä OSI-mallin tasolla seitsemän, jotta haitallinen sivusuuntainen liikenne saadaan estettyä. Palo Alto Networks suosittaa käyttämään myös muita heidän tuotteitansa, jotta saadaan automatisoitua mahdollisimman paljon. Fortinet muistuttaa (s.a.), että jokainen suunnitelma on tehty tietyn suojapinnan ympärille, joten ei ole olemassa yhtä ainoaa ratkaisua.

Arkkitehtuurin luonnin jälkeen on seuraavana vuorossa politiikkojen luonti. Palo Alto Networks määrittää (2021a, 14–17) tämän sallittujen sääntöjen listaksi, joiden avulla vain valtuutetut käyttäjät voivat käyttää tiettyjä resursseja määritettyjen sovellusten avulla oikeaan aikaan oikeissa paikoissa. Jos liikenne ei vastaa sääntöä, palomuuri estää liikenteen automaattisesti. Politiikat perustuvat Kipling-menetelmään. Vastaaminen Kiplingin kuusilukuisiin kysymyksiin kuka, mitä, milloin, missä, miksi ja miten osoittaa, kuinka voidaan päättää salliako vai estää liikenne. Myös Fortinet suosittaa (s.a.) käyttämään Kipling-menetelmää politiikkojen luontiin. Alla olevassa taulukossa 1 on esiteltynä tarkennukset kysymysten rakenteisiin.

Taulukko 1. Kipling-metodin rakenne

Kuka	Kenellä on pääsy resurssiin. Kyseessä voi olla henkilö tai laite.
Mitä	Mitä applikaatiota käytetään resurssiin pääsyssä. Mitä korkeammalle OSI-kerroksella päästään, sitä tarkemmaksi politiikka pystytään kirjoittamaan.
Milloin	Mihin aikaan pääsyä resurssiin pyydetään.
Missä	Missä pyydetty resurssi sijaitsee. Voidaan käyttää myös pyytäjän sijaintia.
Miksi	Miksi resurssiin halutaan päästä, sisältääkö se arkaluontoisia tietoja. Mikäli tietoon päästään käsiksi, tuleeko se ilmoittaa valvontaviranomaisille.
Miten	Miten pääsy tietoon sallitaan. Varmistetaan vähimmän käyttöoikeuden periaatetta, kirjataan kaikki liikenne, luetaan myös suojattua liikennettä, varmistetaan päätelaitteen eheys.

Monitorointi ja ylläpito on tärkeää, koska se voi varoittaa mahdollisista ongelmista aikaisemmin ja tarjota mahdollisuuden verkon suorituskyvyn optimointiin. Fortinet erittelee (s.a.) tässä erikseen raportit, analytiikan ja lokit. Säännöllisesti tai jatkuvasti tuotetuilla raporteilla voidaan merkitä epänormaalia käyttäytymistä. Raporteilla voidaan analysoida myös Zero Trust -järjestelmän vaikutuksia henkilöille ja järjestelmän suorituskykyyn. Analytiikka ottaa järjestelmän luomaa tietoa ja antaa vihjeitä, kuinka hyvin järjestelmä toimii. Analytiikan avulla voidaan myös seurata muun muassa käyttäjien käyttäytymismalleja. Lokit antavat pysyviä, aikaleimattuja tietoja järjestelmän toiminnasta. Niitä voidaan analysoida manuaalisesti tai käyttää apuna työkaluja, kuten koneoppimista. Palo Alto Networks määrittää (2021a, 17) ylläpidon tärkeyttä, sillä sekä yritys että verkko elävät ajan myötä. Ennaltaehkäisyjärjestelmän ylläpito onkin jatkuva prosessi.

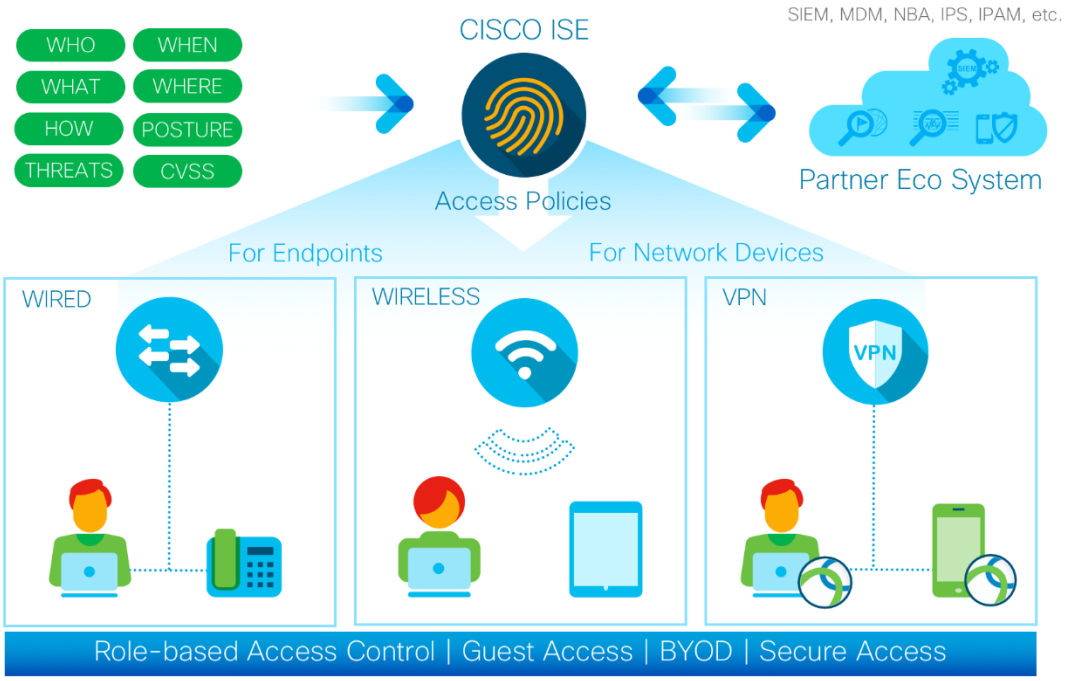
Rose ym. (2020, 36) kuvaa dokumentissaan Zero Trust -arkkitehtuurin toteuttamista pikemminkin matkana kuin infrastruktuurin tukkukauppa. Organisaation tulisi pyrkiä asteittain toteuttamaan Zero Trustin periaatteet, prosessimuutokset ja teknologiaratkaisut, jotka suojaavat sen arvokkaimpia tietovaroja. Useimmat yritykset jatkavat toimintaansa hybridinä Zero Trustin ja kehäpohjaisen mallin tilassa määrittelemättömän ajan. On epätodennäköistä, että mikään merkittävä yritys voi siirtyä Zero Trustiin yhden tekniikkaa päivittävän syklin aikana. Yrityksen on varmistettava, että yhteiset elementit (esimerkiksi identiteettihallinta, laitehallinta, tapahtumien kirjaaminen) ovat riittävän joustavia toimimaan yhdessä Zero Trust -arkkitehtuurin ja kehäpohjaisen mallin hybridiarkkitehtuurissa. Kuinka yritys siirtyy Zero Trust -strategiaan, riippuu sen nykyisestä kyberturvallisuustasosta ja -toiminnoista. Yrityksen tulisi saavuttaa

lähtötaso ennen kuin se on mahdollista ottaa käyttöön merkittävä Zero Trustiin keskittynyt ympäristö. Tämä lähtötaso sisältää resurssien, aiheiden, liiketoimintaprosessit, liikennevirrat ja riippuvuuskartoitukset, jotka on tunnistettu ja luetteloitu yritykselle.

Rose ym. (2020, 39) suosittaa dokumentissaan aloittamaan ensimmäistä siirtymistä Zero Trust -arkkitehtuuriin vähäriskisellä liiketoimintaprosessilla, jotta häiriöt eivät vaikuta kielteisesti koko organisaatioon. Kun tarpeeksi kokemusta on saatu, kriittisemmät liiketoimintaprosessit voivat tulla vaihtoehdoksi. Liiketoimintaprosessit, jotka hyödyntävät pilvipohjaisia resursseja tai joita etätyöntekijät käyttävät, ovat usein hyviä ehdokkaita Zero Trust -arkkitehtuurille.

6.1 Cisco

Ciscon Zero Trust -arkkitehtuuri rakentuu heidän Identity Service Engine -järjestelmän (ISE) ympärille. Cisco kuvaa ISE-järjestelmää dokumentissaan (s.a., 1) seuraavan sukupolven identiteetti- ja pääsynvalvonta-alustana. ISE-järjestelmä kerää reaaliaikaista asiayhteyteen liittyvää tietoa verkoista, käyttäjistä ja laitteista. Näitä tietoja käytetään ennakoivien päätösten tekemiseen sitomalla identiteetti verkkoelementteihin kuten kytkimiin, langattoman verkon ohjaimiin tai virtuaalisen verkon yhdyskäytäviin. Kuvassa 7 on esitettynä Ciscon ISE-järjestelmän yleiskuvaus.

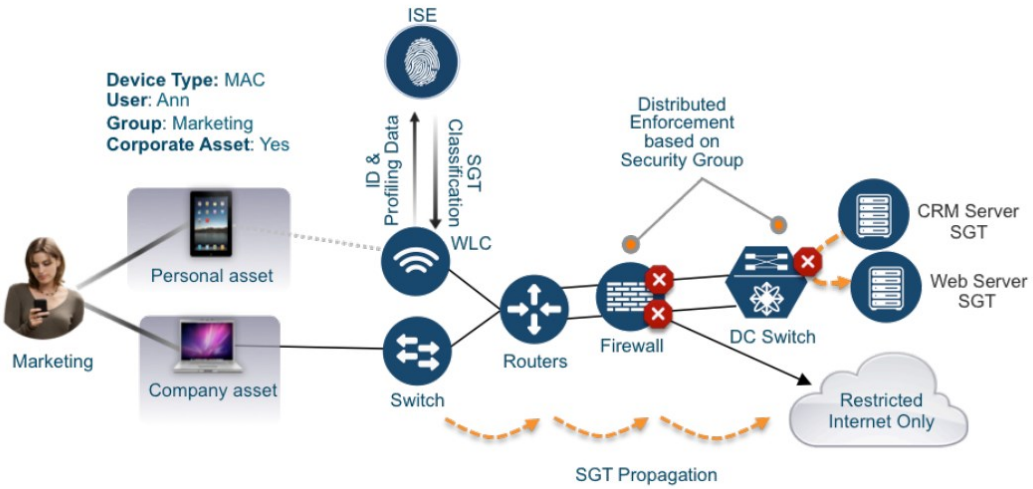


Kuva 7. Cisco ISE-järjestelmän yleiskuvaus (Cisco s.a.)

Ciscon ekosysteemi Zero Trust -arkkitehtuurille pohjautuu useampaan eri järjestelmään, joita voidaan lisätä käyttöön yrityksen tarpeiden mukaan. ISE-järjestelmä on näistä kuitenkin se keskeisin. Seuraavissa kappaleissa käydään läpi opinnäytetyön kannalta tärkeimmät Ciscon järjestelmät, joilla Zero Trust -arkkitehtuuria voi laajentaa.

Identiteetin hallinta hoidetaan ISE-järjestelmällä ja sitä voidaan laajentaa Cisco Duo-järjestelmään. Duo-järjestelmä tuo mukanaan muun muassa monivaiheisen tunnistautumisen, laitteen luotettavuuden arvioinnin, salasanattomuuden ja kertakirjautumisen. (Cisco Duo 2020.)

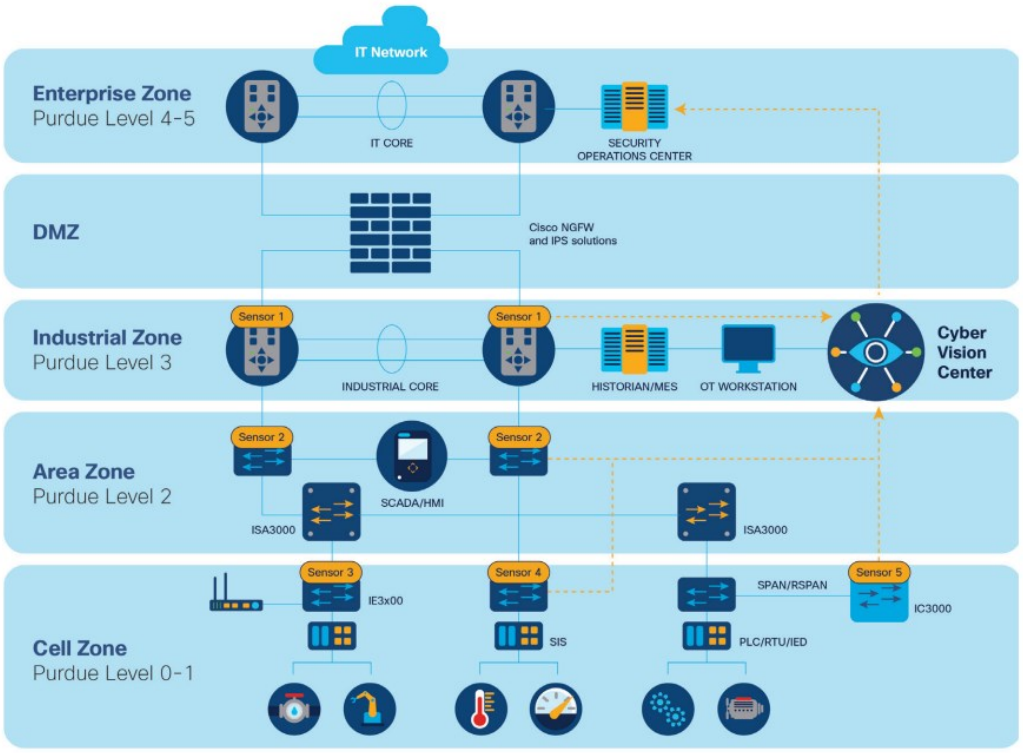
Mikrosegmentaatiota varten ekosysteemi laajentuu TrustSecillä. TrustSec ei itsessään ole järjestelmä, vaan kyseessä on sateenvarjotermi. TrustSec tuo Ciscon verkkolaitteisiin turvallisuuteen liittyviä parannuksia, joilla tehostetaan käyttäjien, päätelaitteiden ja verkkolaitteiden identiteettiä. Näitä on muun muassa politiikkaan perustuva pääsynhallinta. TrustSecin tärkein komponentti on Cisco ISE-järjestelmä. (Cisco 2015.)



Kuva 8. Cisco TrustSecin yleiskuvaus (Cisco 2015)

Kuvassa 8 on yleiskuvaus TrustSecin toiminnasta. Tässä päätelaite autentikoidaan joko 802.1X-protokollaa käyttäen (kuvan 8 Company asset), MAC Authentication Bypass -protokollaa (MAB) käyttäen (kuvan 8 Personal asset) tai WebAuthia käyttäen (kuvan 8 Personal asset). ISE-järjestelmän politiikkojen perusteella myönnetään tagi, jota kuljetetaan verkossa mukana. Täytäntöönpanopisteellä pääsy resurssiin hyväksytään, hylätään tai myönnetään rajattu oikeus.

Ciscon ratkaisu Software Defined Perimeter -malliin on heidän Cisco DNA Center -järjestelmänsä. Kyseessä on oivaltava verkko -ratkaisu. Cisco ISE- että Cisco DNA Center -järjestelmät tulee integroida toisiinsa, jotta täydellinen ratkaisu saadaan aikaiseksi. (Cisco 2022.)



The placement of the sensors must make it possible to monitor the different interconnection points of the industrial system:

Sensor 1: Interconnection between the IT-based network and the OT network (Historian flow, Statistics, Driving)

Sensor 2: Process network between PLCs and Windows machines (supervision and control-command flow, SCADA station, engineering)

Sensor 3: Wireless interconnection or remote maintenance (DSL, LTE or MPLS router)

Sensor 4: Flow control between control systems and between control systems and safety systems

Sensor 5: Connection with the physically open field network.

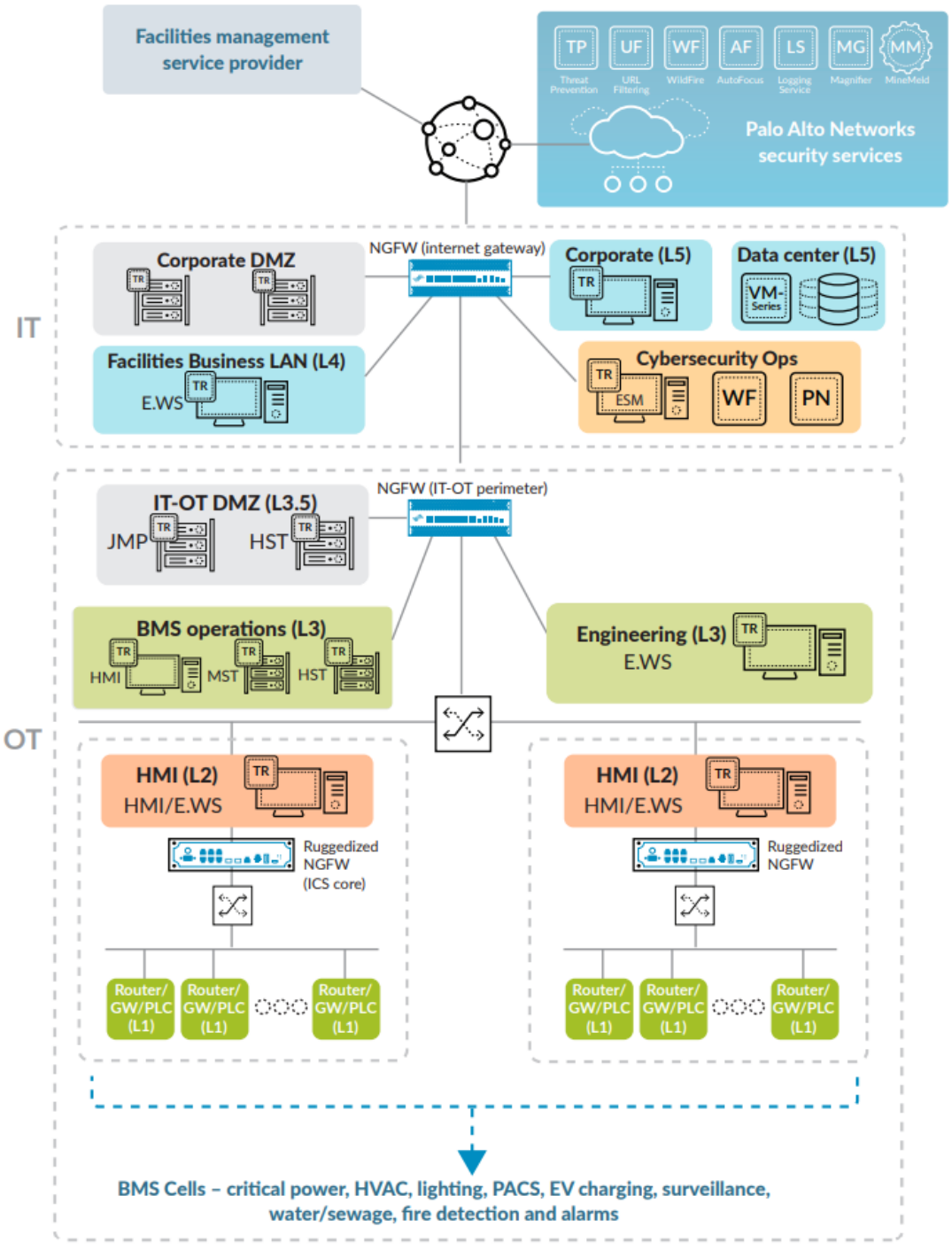
Kuva 9. Ciscon ratkaisu Purdue-mallin mukaiseen OT-järjestelmään (Cisco 2019)

Zero Trustin ulottaminen OT-järjestelmään tapahtuu Ciscon ekosysteemissä Cyber Vision -järjestelmällä, joka tuo näkyvyyden OT-verkon liikenteeseen ja tapahtumiin. Tätä järjestelmää on periaatetasolla kuvattuna kuvassa 9. Cyber Vision -järjestelmää voidaan tämän jälkeen kasvattaa muun muassa Cisco ISE-järjestelmällä. (Cisco 2019, 12–14.)

6.2 Palo Alto Networks

Kuten Ciscolla, myös Palo Alto Networksillä on heidän oma ekosysteeminsä rakennettuna Zero Trustin ympärille. Heidän ratkaisunsa Zero Trust -arkkitehtuurista pohjautuu vahvasti heidän seuraavan sukupolven palomuurituotteen ympärille, jota tukemaan tuodaan useita muita tuotteita.

Palo Alto Networksin ratkaisu ulottaa Zero Trustia OT-järjestelmään on tuoda heidän seuraavan sukupolven palomuurit Purdue-mallin tasojen reunalle. Kuvassa 10 on kuvattuna heidän ratkaisunsa Purdue-mallin mukaiseen OT-järjestelmään.



Kuva 10. Palo Alto Networksin ratkaisu Purdue-mallin mukaiseen OT-järjestelmään (Palo Alto Networks 2021b)

Dokumentin (2021b) mukaan kaikki liikenne tulisi kulkea palomuurin kautta, eikä suoraa yhteyttä tasojen välillä olisi. Tätä järjestelmää on mahdollista laajentaa Palo Alto Networksin ekosysteemissä muilla tuotteilla, jotka tuovat

mukanaan muun muassa koneoppimista lokiseurantaan sekä ohjelmistopohjaisia verkkoja.

6.3 Fortinet

Kuten Palo Alto Networksillä, myös Fortinetillä on kokonainen ekosysteemi rakennettuna Zero Trustin ympärille. Samoin kuin Palo Alto Networksillä, myös Fortinetillä Zero Trust -arkkitehtuurin ratkaisu pohjautuu vahvasti heidän seuraavan sukupolven palomuuri tuotteen ympärille. Myös Fortinetiltä löytyy useita muita tuotteita tukemaan Zero Trust -ratkaisua.

Fortinetin ratkaisu ulottaa Zero Trustia OT-järjestelmään on tuoda heidän seuraavan sukupolven palomuurit Purdue-mallin tasojen reunalle. Kaikki liikenne tulisi kulkea palomuurin kautta, eikä suoraa yhteyttä tasojen välillä olisi. Järjestelmää on mahdollista laajentaa Fortinetin ekosysteemin muilla tuotteilla, joilla voidaan tuoda älyä verkon hallintaan, hoidetaan identiteetin hallintaa sekä useilla monitorointiin liittyvillä tuotteilla. (Fortinet 2021.)

7 ZERO TRUST -ARKKITEHTUURIN KÄYTTÖÖNOTTO

Yhtiön aiempi ekosysteemi pohjautuu vahvasti Ciscon tuoteperheen ympärille, joten suunnitelmassa on käytetty Ciscon ekosysteemin tuotteita ja heidän ratkaisujaan.

Yhtiö koostuu päätoimipisteestä sekä kahdesta voimalaitoksesta, joissa molemmissa on Purdue-mallin mukainen OT-järjestelmä käytössä. Yhtiöllä on sekä pilvi- että paikan päällä olevaa palvelimia. Muutoin nykyinen verkkoinfrastruktuuri on perinteinen kehämalli, jossa suojaus hoidetaan sisäverkon reunalla.

Työntekijöillä on yhtiön hyväksymät kannettavat tietokoneet käytössään. Työntekijöidensä autentikoimiseen käytetään Microsoft AD -valtuutusta. Tietokoneet päätoimipisteessä käyttävät langallista verkkoa. Työntekijöiden muut kannettavat laitteet voidaan liittää päätoimipisteessä langattomaan verkkoon, johon kirjaudutaan yhteisellä tunnuksella ja salasanalla. Vierailijoille on oma langaton verkko, jolla tarjotaan pelkkä internetyhteys. Etäyhteyksiä varten työntekijän tulee ottaa VPN-yhteys päätoimipaikan verkkoon.

Ajankohdallisesti yhtiöllä on suunnitelmissa uusia heidän langaton verkkonsa yhtiön päätoimipisteellä. Koska kyseinen elementti ei ole yrityksen kriittistä toimintaa, toimii langaton verkko alustana Zero Trustin käyttöönotolle sekä käyttökokemusten saantiin.

Zero Trust -arkkitehtuurin suunnitteluun on valittu kehämallin käyttö. Kehämallin mukaan suunnittelu aloitetaan suojapinnan määrittelyllä. Yrityksen DAAS inventaari on tässä kohtaa suositeltavaa päivittää ajan tasalle. Näin saadaan määriteltyä kriittiset, suojattavat elementit, jotta Zero Trustin hyöty saadaan täysimääräisesti käyttöön.

7.1 DAAS

Yrityksen suojapinnan kartoituksessa käytettiin hyväksi DAAS-menetelmää. Kriittiset elementit määriteltiin ja ne on esitelty alla taulukossa 2.

Taulukko 2. DAAS elementtien määrittely

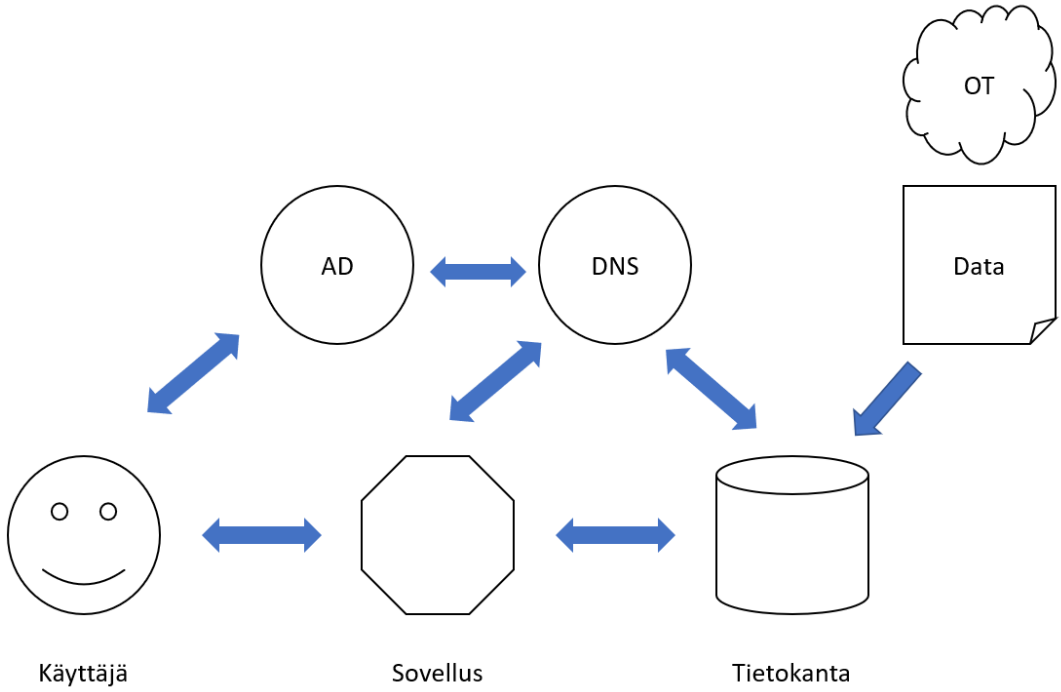
Data	Kriittistä dataa yritykselle on tuotantoprosessista muodostuva data, henkilöstön data sekä henkinen omaisuus, kuten tutkimus- ja kehitystieto.
Application	Kriittiset sovellukset yritykselle on tuotantoprosessin analysointisovellus sekä kehitystyöhön liittyvä sovellus.
Assets	Yritykselle kriittistä omaisuutta on palvelimet IT järjestelmässä sekä IT-OT rajapinnassa olevat laitteet.
Services	Kriittisiä palveluita on DNS, AD

Taulukosta 2 voidaan nähdä, että yrityksen kriittiset toiminnot ovat IT-järjestelmään painottuvia. Huomioitavaa onkin, että OT-järjestelmän huoltosopimus edellyttää järjestelmän olevan toimittajan dokumentaation mukainen. OT-järjestelmään tuodut dokumentaation ulkopuoliset elementit katkaisevat toimittajan tuen. OT-järjestelmästä kerättyä dataa voidaan pitää kriittisenä, sillä sen pohjalta tehdään analyyseja sekä kehitystyötä.

Yrityksen kriittiset elementit on näin määritelty ja suojapinnat voidaan suunnitella näiden mukaan.

7.2 Tietovirrat

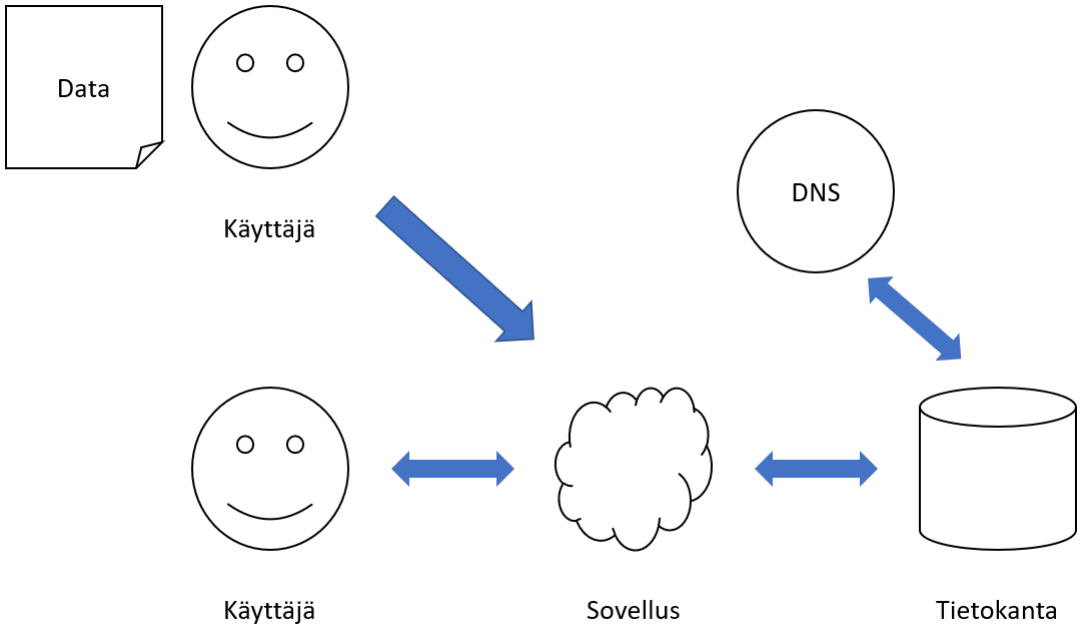
Tietovirroilla pyritään selvittämään ja kuvaamaan käyttäjien ja sovellusten tietovirtojen kulkua ja keskinäisiä riippuvuuksia. Yksi yrityksen tietovirroista on käyttäjien käyttämä analysointisovellus, joka hakee tietonsa tietokannasta. Tietokantaan tuotetaan dataa tuotantoprosessista.



Kuva 11. Yrityksen eräs tietovirroista kuvattuna

Kuvassa 11 on esitettynä analysointisovellukseen liittyvä tietovirta. Kuvasta näkee myös keskinäisiä riippuvuuksia. Data tietokantaan tulee OT-järjestelmän kautta. Sovellus lukee tätä tietokannassa olevaa dataa analysointia varten. Käyttäjän tulee autentikoitua Active Directoryn kautta, sillä sovellus sijaitsee yrityksen hallinnoimilla tietokoneilla.

Toisena tietovirtana kuvataan yrityksen henkilöstön dataa. Tässä datan tuottaa henkilö itse ja sovellus on pilvipalveluna. Sovellus hakee tietonsa tietokannasta.



Kuva 12. Yrityksen eräs tietovirta kuvattuna

Kuvassa 12 on esitettynä henkilöstön dataan liittyvä tietovirta. Tässä käyttäjä itse tuottaa datan, joka sovelluksen kautta tallennetaan tietokantaan. Dataan on sovelluksen kautta pääsy tietyillä käyttäjäryhmillä, kuten henkilöstöosastolla. Sovellus on pilvi- ja selainpohjainen, joten se on avoinna internettiin. Tietokanta, johon data tallennetaan, sijaitsee yrityksen tiloissa.

7.3 Kipling-metodi

Tietovirtojen kartoituksen jälkeen pystytään määrittelemään Kipling-metodia hyväksikäyttäen tietoturvapolitiikat suojattaville resursseille.

Taulukossa 3 on esiteltynä kuvan 11 tietovirran turvapolitiikka Kipling-metodia hyväksikäyttäen.

Taulukko 3. Tietoturvapolitiikka Kipling-metodia hyväksikäyttäen

Kuka	**Mitä**	**Milloin**	**Missä**	**Miksi**	**Miten**
Analysoija	Analyysi	Työaika	Palvelin	Datalla ei laajennettua turvaa.	Kirjataan liikenne, luetaan suojattua liikennettä, varmistetaan päätelaitteen eheys.

Analysointisovelluksen ollessa pelkästään yrityksen hallinnoimilla koneilla ainoastaan työtehtävien vaatimilla henkilöillä on kyseiseen sovellukseen käyttöoikeus. Ainoastaan kyseisellä sovelluksella on pääsy tietokannan dataan. Pääsy dataan rajoitetaan työaikaan Suomen aikavyöhykkeellä. Lisäksi varmistetaan, että pyyntö sovellukselta dataan menee ainoastaan halutun palvelimen dataan. Data itsessään ei ole kriittistä, jotta sille tarvitsisi laajennettua turvaa. Kyseinen data tuotetaan OT-järjestelmästä, eikä se sisällä arkaluontoista informaatiota. Kaikki liikenne kuitenkin kirjataan sekä suojattu liikenne puretaan ja varmistetaan päätelaitteen eheys.

Taulukossa 4 on esiteltynä kuvan 12 tietovirran turvapolitiikka Kipling-metodia hyväksikäyttäen.

Taulukko 4. Tietoturvapolitiikka Kipling-metodia hyväksikäyttäen

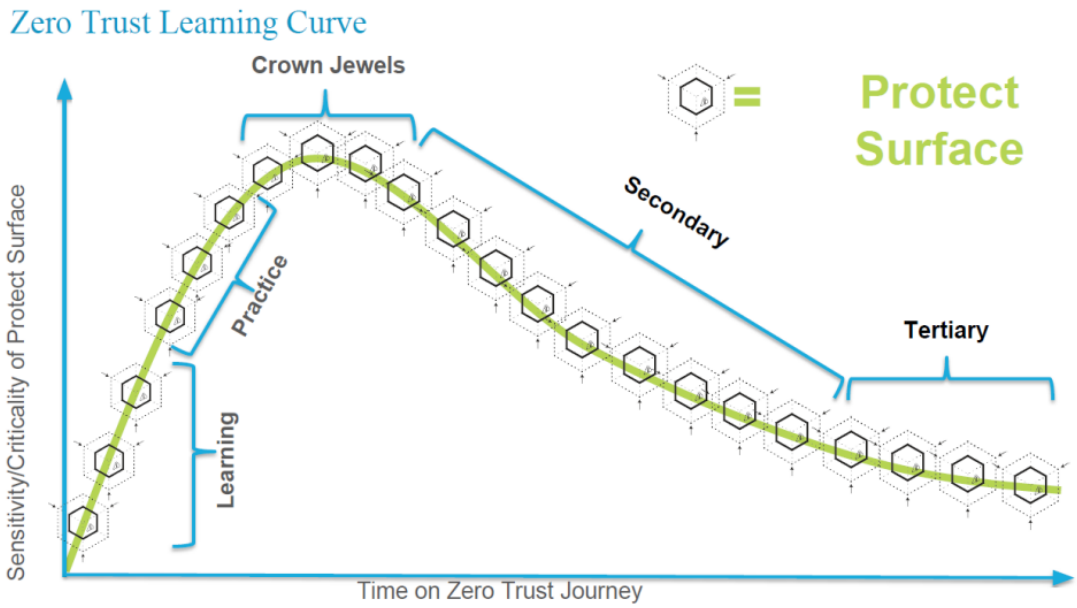
Kuka	**Mitä**	**Milloin**	**Missä**	**Miksi**	**Miten**
HR	HR_cloud	Työaika	Suomi	Datalla laajennettu turva, sisältää henkilöstön arvokasta tietoa.	Kirjataan kaikki liikenne, luetaan suojattua liikennettä, varmistetaan päätelaitteen eheys.
Kaikki	HR_cloud	Koska tahansa	Suomi	Datalla laajennettu turva, sisältää henkilöstön arvokasta tietoa.	Vähimmän käyttöoikeuden periaate, Kirjataan kaikki liikenne, luetaan suojattua liikennettä.

Henkilöstön tietojen käsittelyyn käytetty sovellus HR_cloud sijaitsee kolmannen osapuolen pilvipalveluna, johon jokaisella yhtiön henkilöllä on jonkinlainen pääsyoikeus. Tämän johdosta luodaan kaksi käyttäjäryhmää, HR ja kaikki. HR-ryhmän pääsy dataan rajataan työaikaan. Pyyntö täytyy tulla Suomesta, sillä kolmannen osapuolen sovellus sijaitsee Suomessa. Datalla on laajennettu turva, sillä se sisältää henkilöstön arkaluontoista tietoa. Data salataan tietokantaan ja luodaan GDPR:n mukaiset prosessit. HR-ryhmällä on pääsy koko dataan. Kaikki liikenne kirjataan, suojattu liikenne puretaan ja varmistetaan päätelaitteen eheys. Toisena ryhmänä on kaikki, jotka saavat päästä

koska tahansa dataan. Mukaan tuodaan kuitenkin vähimmän käyttöoikeuden periaate, sillä sallitaan pääsy vain omaan dataan. Varmistus päätelaitteen eheydestä poistetaan, sillä pyynnöt voivat tulla henkilön omalta laitteelta.

7.4 Zero Trust -arkkitehtuuri

Zero Trust -arkkitehtuurin rakennus aloitetaan yrityksen ei-kriittisistä elementeistä. On tärkeää saada opiskeltua ja harjoiteltua Zero Trustin käyttöönottoa, ennen kuin sitä aletaan ottamaan käyttöön kriittisille elementeille. Yrityksen tapauksessa IT-järjestelmästä johtuvat OT-järjestelmän häiriöt eivät saa tulla kyseeseen.

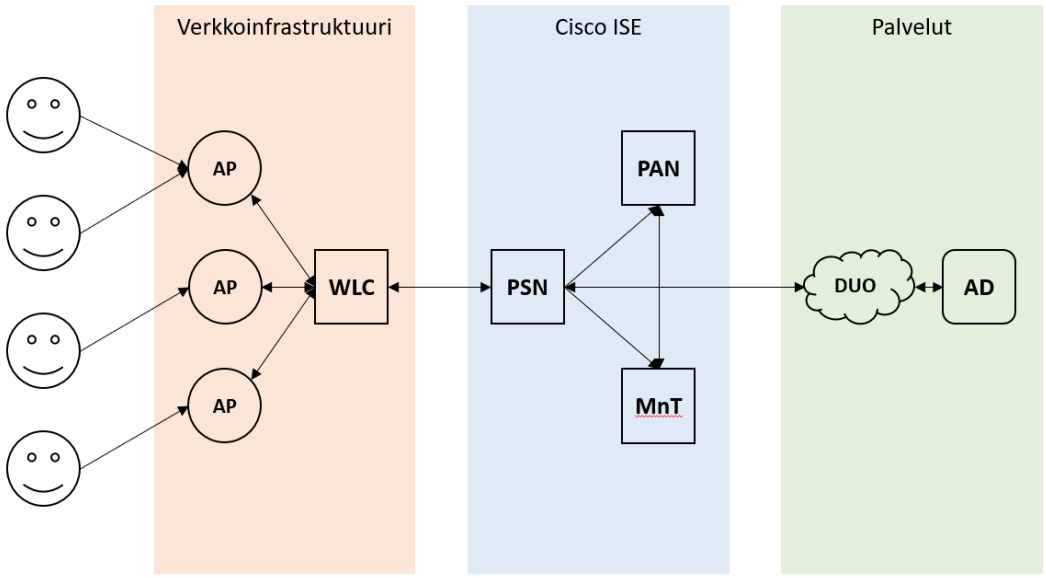


Kuva 13. Zero Trust -arkkitehtuurin vaiheet (Palo Alto Networks 2021a)

Kuvassa 13 onkin esitelty Zero Trustin oppimiskäyrää suhteessa suojapinnan kriittisyyteen.

Yrityksen päätoimipisteen langattoman verkon uusinta on tähän hyvä oppimistilanne, sillä kyseessä ei ole yrityksen kriittinen elementti. Langattoman verkon lähestymistavaksi sopii tehostettu identiteetti. Tehostetun identiteetin mukaisesti langattomaan verkkoon kirjautuminen toteutetaan monivaiheisena autentikoimisena. Myös käytetyn päätelaitteen eheys tarkistetaan. Tämä voidaan Ciscon ekosysteemissä toteuttaa Duo-palvelun avulla, joka toteuttaa molemmat. Tämä mahdollistaa valitulle tai valituille käyttäjäryhmille työskentelyn

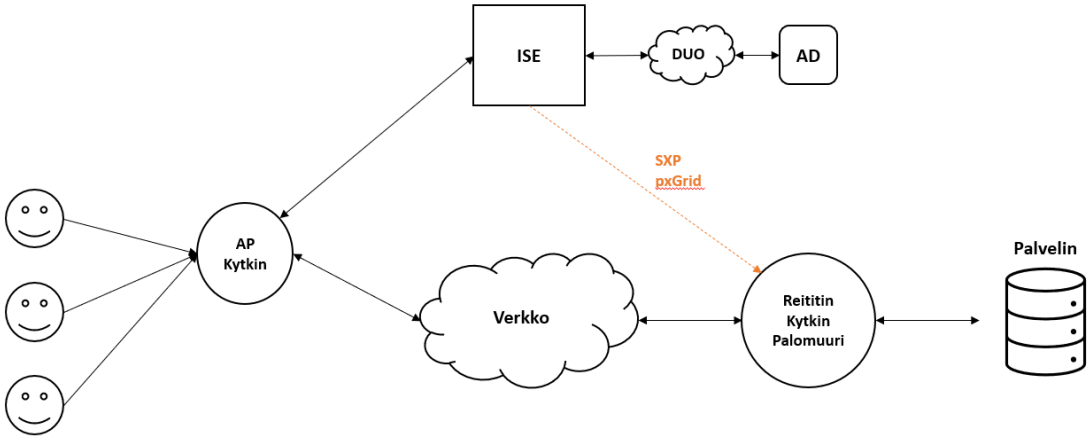
paikkariippumattomasti langattoman verkon kantoalueen sisällä. Näin voidaan toteuttaa tarkasti määritelty pilotointi, jossa pääsy yrityksen kriittiselle elementille sallitaan langattomaan verkkoon autentikoineelta käyttäjäryhmältä. Vierailijoille sekä henkilöstön omille laitteille tarjotaan pelkästään internetyhteys.



Kuva 14. Langattoman verkon looginen topologia

Yllä olevassa kuvassa 14 kuvataan langattoman verkon looginen topologia Cisco ISE -ratkaisulla toteutettuna. Tukiasemien hallinnointi tapahtuu kontrollerin (WLC) kautta. Cisco ISE pilkkoutuu kolmeen eri komponenttiin. Policy Service Node (PSN) toimeenpanee turvapolitiikat. Policy Administration Node (PAN) antaa graafisen käyttöliittymän konfiguraatiota varten. Samalla se visualisoi monitorointi-noden tuottaman tiedon. Monitoring and Troubleshooting Node (MnT) kerää lokitietoa. Korkeaa saavutettavuutta haluttaessa PAN tulisi kahdentaa. Korkeaa luotettavuutta haluttaessa MnT tulisi kahdentaa. Edelleen jos korkeaa vikasietoisuutta haluttaessa PSN voidaan kahdentaa, kolmentaa ja niin edelleen.

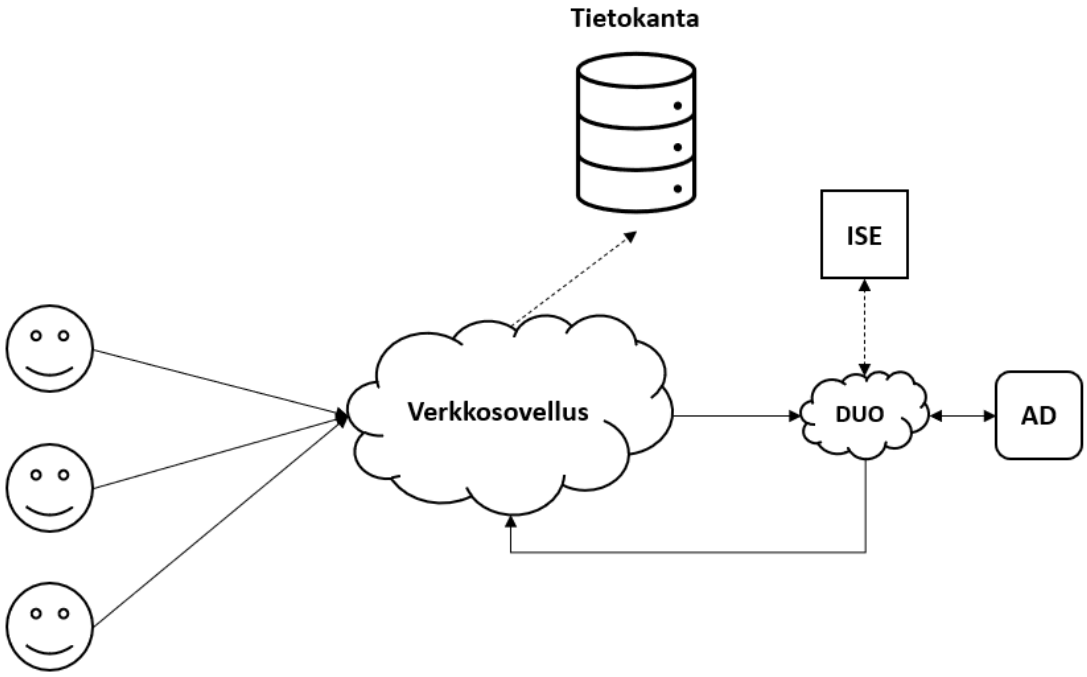
Seuraavaksi toteutetaan OT-järjestelmän analysointiin liittyvä käyttöönotto. Tähän lähestymistavaksi sopii mikrosegmentointi. Mikrosegmentoinnilla mahdollistetaan ainoastaan analysointisovelluksen pääsy dataan. Kipling-metodia hyväksikäyttäen kirjoitetaan pääsypolitiikka. Tehostettu identiteetti tulee olla käytössä kyseiselle käyttäjäryhmälle.



Kuva 15. Ciscon mikrosegmentaation looginen topologia

Kuvassa 15 on esiteltynä mikrosegmentaation looginen topologia. Cisco ISE -ratkaisussa mikrosegmentaatioon käytetään TrustSec-ratkaisua. Sallitut käyttäjäryhmät mapataan omalla tagilla. Tämän mappauksen hoitaa kytkimet, tukiasemien kontrolleri tai palomuuri varmistaen ISE-järjestelmästä tiedon. Mappaus voidaan tehdä staattisena tai dynaamisena, jolloin ISE lähettää tiedon täytäntöönpanopisteelle. Tähän voidaan käyttää joko Scalable Group Tag Exchange (SXP) protokollaa tai avointa, Ciscon standardoimaa (RFC 8600) pxGrid protokollaa. Tieto kuljetetaan Ethernet-kehyksen mukana ja täytäntöönpanopisteenä toimii palvelinta lähinnä oleva verkkolaite, kuten esimerkiksi kytkin.

Seuraavana toteutetaan henkilöstön dataan liittyvä käyttöönotto. Tähän lähestymistapana sopii tehostettu identiteetti.



Kuva 16. Cisco DUO looginen topologia

Kuvassa 16 on kuvattuna henkilöstön dataa käsittelevän verkkosovelluksen looginen topologia, toteutettuna Cisco Duo -palvelulla. Tässä verkkosovellukseen kirjautuessa ohjataan käyttäjä Duon monivaiheiseen tunnistautumiseen. Duon Beyond-laajennuksella hoidetaan päätelaitteen turvallisuus. Duo integroidaan ISE-järjestelmään, jotta turvapolitiikkojen hallinta on keskitettyä.

7.5 OT-järjestelmä

Kuten luvussa 7.1 on mainittu, ei yhtiöllä ole mahdollisuutta tehdä muutoksia OT-järjestelmään. Valitun toimittajan kanssa tehty huoltosopimus määrittää, että järjestelmä on toteutettu tietyin konfiguraation ja komponentein, eikä sitä oleellisesti voi muokata.

Kun on tarve uusia järjestelmiä ja tehdä pitkäaikaisia hankintoja, tulisi laitevalmistajaa valittaessa huomioida jo tarjouspyyntövaiheessa Zero Trustin käyttöönotto OT-järjestelmässä.

Alla olevassa taulukossa 5 on kuvattuna asioita, jotka voisi ottaa huomioon tarjouspyyntövaiheessa.

Taulukko 5. Suositukset laitevalmistajalle

Tietovirtojen kuvaus	Laitevalmistajan tulisi kuvata ylätasolla tietovirtojen kulku OT-järjestelmässä. Näin saadaan yleiskuva liikennevirrasta sekä sovellusten välisistä riippuvuuksista.
Purdue-malli	Purdue-mallin tasojen välinen liikenne kulkee gateway-laitteen kautta. Tasot eivät suoraan kommunikoi toistensa kanssa. Purdue-mallin tasojen 2 ja 1 (HMI ja prosessilaitteet) väliin tehdasolosuhteita kestävät gateway-laitteet. Tällä suojataan kriittiset toiminnot.
Integrointi	Integrointi laitevalmistajan omien gateway-laitteiden ja tilaajan hallinnointisovelluksen välillä. Mikäli tilaaja ei saa toimittaa omia gateway-laitteita, laitevalmistajan oman gateway-laitteen tulee tukea avointa pxGrid-protokollaa.

7.6 Jatkosuunnitelma

Yhtiön jatko Zero Trustin käyttöönotossa jatkuu, kun saatua oppia ja kokemusta on kerrytetty. Seuraava käyttöönotettava vaihe voisi olla tehostetun identiteetin ulottaminen jokaiseen verkkolaitteeseen (kytkimet, reitittimet ja niin edelleen), joka yrityksen hallinnassa on mukaan lukien OT-järjestelmän rajapinnoilla olevat laitteet. Näin suojapinnan kartoitukseen käytetyn DAAS-menetelmän mukaiset resurssit olisivat suojattuna Zero Trust -arkkitehtuurin mukaisesti. Näin ollen Zero Trustin oppimiskäyrässä olisi saavutettu huippu. Näin kokemusta olisi saavutettu myös kriittisempien resurssien osalta.

Seuraavana vaiheena käyttöönotossa voisi olla tehostetun identiteetin ulottaminen koko henkilöstöön, niin langallisessa kuin langattomassa verkossa. Tämä tehostaisi tietoturvaa käyttäjien ja heidän päätelaitteiden osalta, sekä mahdollistaisi henkilöstölle vapaamman työskentelyn paikasta riippumatta.

Zero Trustin käyttöönoton seuraavana vaiheena voisi olla mikrosegmentoida muita mahdollisia sovelluksia tai palveluita. Nämä tulisi kartoittaa ensin ja tähän kehämallin käyttö on suositeltavaa.

Viimeisimpänä käyttöönoton vaiheena voisi olla kertakirjautumisen (single sign-on) että salasanattomuuden (passwordless) ulottaminen yrityksen infrastruktuuriin. Molemmat nämä pystytään toteuttamaan Cisco Duo -järjestelmällä. Tämä mahdollistaisi henkilöstölle sujuvampaa työnkulkua, kun yhdellä kirjautumisella hoituisi useampi palvelu. Samoin salasanoista luopuminen

tehostaisi tietoturvaa, kun salasanat korvattaisiin esimerkiksi biometrisellä tunnistautumisella.

8 TULOKSET

Tutkimusasetelman kysymyksiin saatiin haettua vastaus sekä teoriapohjalta että toteutusosassa. Olemassa olevien infrastruktuurien käyttöönotto tulee tehdä vaiheittain, jotta yrityksen kriittisiä toimintoja ei häirittäisi. Zero Trust -arkkitehtuurin käyttöönotto helpottuu ja nopeutuu, mitä tarkemmin yrityksessä on jo hoidettuna tietoturvaa. Zero Trustin käyttöönottoa suunniteltaessa on tärkeää huomioida sen käyttökohteet. Huolellinen suunnittelu ehkäisee mahdolliset sudenkuopat. Koska muutokset ovat suositeltavaa tehdä vaiheittain, tulee Zero Trust -konseptin käyttöönotto koko verkkoinfrastruktuurin tasolla viemään aikaa. Tämä vaatiikin sitoutumista koko yritykseltä.

Laitevalmistajat toteuttavat omat Zero Trust -ratkaisunsa hieman eri tavoin kuin Zero Trust -arkkitehtuurin lähestymistavat antavat ymmärtää. Laitevalmistajat esittelevät koko ekosysteeminsä, jolloin lähestymistavoista jokainen toteutuu riippuen mitä tuotteita laitevalmistajalta otetaan käyttöön. Zero Trust -arkkitehtuurin lähestymistavat onkin parempi mieltää suojapinnan mukaan, jolloin valittu lähestymistapa menee suojapinnan mukaan.

Loogisina komponentteina Ciscon ratkaisu erosi kahdesta muusta selvemmin. Cisco on selvemmin jaotellut omassa ratkaisussaan Policy Decision Pointin omiksi elementeikseen (ISE) ja Policy Enforcement Pointin omaksi verkkolaitteekseen (kytkimet, reitittimet ja palomuurit). Palo Alto Networks ja Fortinet ovat paketoineet nämä kaikki heidän seuraavan sukupolven palomuurin sisään. Sekä Palo Alto Networks että Fortinet toteuttavat oman ratkaisunsa agentti/yhdyskäytävä-mallina.

Kaikkien kolmen laitevalmistajan ratkaisut Zero Trust -arkkitehtuurin ulottamiseksi OT-järjestelmään eivät juurikaan poikenneet toisistaan. Jokaisessa ratkaisussa Purdue-mallin tasojen reunoille tuotiin verkon turvalaite, pääasiassa palomuuri. Tätä mallia ei voitane pitää täydellisenä Zero Trust -arkkitehtuurina, mutta OT-järjestelmän vaatimukset aiheuttavat tähän haasteita. IoT-laitteet eivät juuri tue vahvaa tunnistautumista, eikä niihin ole jälkeenpäin

asennettavissa ohjelmistoja. Valmistajien esittelemät mallit ovatkin lähinnä verkon segmentointia pienempiin osiin. Lisäturvaa ne kuitenkin tuovat, sillä Purdue-mallia pidetään melko vajavaisena tietoturvan osalta nykypäivänä. Tämän osalta tullaankin näkemään kehitystä, sillä Yhdysvaltojen presidentti on antanut kesällä 2021 asetuksen, jolla määrätään Zero Trustin käyttöönottoa liittovaltion kriittisiin OT-järjestelmiin (White House 2021).

Tunnetuin Zero Trust -konseptin käyttöönotoista isossa yrityksessä on Googlen BeyondCorp. Tähän opinnäytetyöhön ei BeyondCorpia kuitenkaan otettu mukaan tarkasteluun, sillä sen ulottaminen OT-järjestelmään on erittäin vaikeaa vahvan pilvipohjaisuuden takia. BeyondCorp käyttää muun muassa Software as a Service -mallia.

Yritykselle suunniteltiin onnistuneesti Zero Trust -konseptin mukainen ratkaisu. Siinä käytettiin lähestymistapana sekä tehostettua identiteettiä että mikrosegmentaatiota. Teoriatiedon mukaisesti nämä kaksistaan täyttävät Zero Trustin määritelmän. Zero Trust -arkkitehtuurin suunnittelussa käytettiin kehämallia ja näin saatiin yritykseltä kuvattua DAAS-menetelmällä kriittiset suojapinnat sekä niiden tietovirrat. Kipling-metodia hyväksikäyttäen saatiin luotua turvapolitiikat. Kehämallia jouduttiin toistamaan, jotta kriittisten elementtien tietovirrat saatiin riittävän tarkasti kuvattua ja oikeanlaiset turvapolitiikat muodostettua.

Konseptin mukaista täydellistä ratkaisua ei saatu rakennettua, sillä Software Defined Perimeter -mallin mukaista Zero Trust -ratkaisua ei toteutettu. Tämän mallin ulottaminen yrityksen käyttöön ei nähty tarpeelliseksi. Yritykselle riittävää turvaa saatiin toteutettua tehostetulla identiteetillä sekä mikrosegmentaatiolla.

9 JOHTOPÄÄTÖKSET

Opinnäytetyö voidaan todeta onnistuneeksi, sillä teoriaosassa haetaan vastaus tutkimusasetelman kysymyksiin ja ongelmiin. Teoriaosassa syvennetään suunnittelun eri vaiheita sekä tutustutaan kolmen eri valmistajan ratkaisuihin. Kaksi näistä tosin ovat melkeinpä toistensa kopiot, ainoastaan tuotenimet vaihtuvat. Suunnitteluosassa toteutetaan Zero Trust -konseptin mukainen

arkkitehtuuri, joka määritelmän mukaan täyttää vaaditut kriteerit. Opinnäytetyön aikataulujen puitteissa ei valitettavasti ollut mahdollista osallistua yrityksen ensimmäisen vaiheen Zero Trustin käyttöönottoon.

Suunnitteluosassa on toteutettu muutos olemassa olevaan verkkoinfrastruktuuriin ja tuotu siihen Zero Trust -konseptin mukainen ratkaisu. Suunnitelmaa apuna käyttäen on se siirrettävissä tuotantoverkkoon. Suunnitelmaa on mahdollista käyttää myös tukemaan tulevia suunnitelmia.

Ensimmäisenä jatkokehitysehdotuksena tulisi tutkia Zero Trust -konseptin huonoja puolia. Millaisia rasitteita se tuo yritykselle suunnitteluun, käyttöönottoon ja ylläpitoon. Samalla voisi tutkia millaisia ongelmia hybridimallin ylläpitäminen aiheuttaa.

Toisena jatkokehitysehdotuksena voisi tutkia, miten Industry 4.0 on tietoturva ratkaistu ja kuinka Zero Trust -konsepti olisi tähän käyttöönotettavissa.

LÄHTEET

The American Council for Technology. 2019. Zero Trust Cybersecurity Current Trends. PDF-dokumentti. Saatavissa: https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf [viitattu 24.1.2022].

Bobbert, Y. Scheerder, J. 2020. Zero Trust Validation: From Practical Approaches to Theory. PDF-dokumentti. Saatavissa: https://isaca.nl/wp-content/uploads/2020/12/Bobbert-Y.-Scheerder-J.-2020-Zero-Trust-Validations_From-practical-approaches-to-theoryo.pdf [viitattu 1.11.2021].

Buck, C. Olenberger, C. Schweizer, A. Völter, F. Eymann, T. 2021. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. WWW-dokumentti. Saatavissa: https://doi.org/10.1016/j.cose.2021.102436 [viitattu 30.10.2021].

Cisco. 2015. Cisco TrustSec Quick Start Configuration Guide. PDF-dokumentti. Saatavissa: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/configuration-guide.pdf [viitattu 16.3.2022].

Cisco. 2019. Industrial Cybersecurity: Monitoring & Anomaly Detection. PDF-dokumentti. Saatavissa: https://www.cisco.com/c/dam/en/us/solutions/internet-of-things/cisco-cyber-vision-ebook.pdf [viitattu 21.2.2022].

Cisco. 2022. Cisco DNA Center 2.3.2.0. PDF-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.pdf [viitattu 25.3.2022].

Cisco. s.a. Overview of Cisco ISE. PDF-dokumentti. Saatavissa: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_overview.pdf [viitattu 18.2.2022].

Cisco Duo. 2020. Duo Beyond Overview. WWW-dokumentti. Saatavissa: https://duo.com/docs/beyond-overview [viitattu 16.3.2022].

Cunningham, C. 2018. The Zero Trust eXtended (ZTX) Ecosystem. Extending Zero Trust Security Across Your Digital Business. PDF-dokumentti. Saatavissa: https://www.cisco.com/c/dam/m/en_sg/solutions/security/pdfs/forrester-ztx.pdf [viitattu 28.3.2022].

Cybersecurity and Infrastructure Security Agency. 2021. Zero Trust Maturity Model. PDF-dokumentti. Saatavissa: https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf [viitattu 23.3.2022].

Forcepoint. 2017. A Risk-Adaptive Approach. Realizing the Gartner CARTA Framework In Present-Day Security. PDF-dokumentti. Saatavissa: https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Forcepoint/Forcepoint-1-4YCDU8P.pdf [viitattu 28.3.2022].

Fortinet. s.a. Zero Trust Security Model. WWW-dokumentti. Saatavissa: https://www.fortinet.com/resources/cyberglossary/how-to-implement-zero-trust [viitattu 25.2.2022].

Fortinet. 2021. A Solution Guide to Operational Technology Cybersecurity. PDF-dokumentti. Saatavissa: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-operational-technology-design-guide.pdf [viitattu 28.2.2022].

IETF. 2000. A Framework for Policy-based Admission Control. Tekstitiedosto. Saatavissa: https://www.ietf.org/rfc/rfc2753.txt [viitattu 15.4.2022].

Jacobs, L. s.a. Zero Trust Segmentation Through VLAN Insertion for ICS/SCADA. Videoleike. Saatavissa: https://f1.media.brightcove.com/4/1050259881001/1050259881001_6032272788001_6032265275001.mp4?pubId=1050259881001&videoId=6032265275001 [viitattu 31.10.2021].

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona. Opas opinnäytetyön ja pro gradun kirjoittajalle. E-kirja. Jyväskylä: Jyväskylän ammattikorkeakoulu. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 25.10.2021].

Kerman, A. Borchert, O. Rose, S. 2020. Implementing a zero trust architecture. PDF-dokumentti. Saatavissa: https://www.nccoe.org/sites/default/files/library/project-descriptions/zt-arch-project-description-draft.pdf [viitattu 31.10.2021].

Kindervag, John. 2010. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. PDF-dokumentti. Saatavissa: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf [viitattu 17.11.2021].

Koilpillai, J. Murray N. A. 2020. Software Defined Perimeter (SDP) and Zero Trust. PDF-dokumentti. Saatavissa: https://www.trac-car.com/Software-Defined-Perimeter-and-Zero-Trust.pdf [viitattu 21.11.2021].

Kotkan Energia. 2021. Tietoa meistä. WWW-dokumentti. Saatavissa: https://www.kotkanenergia.fi/tietoa-meista/konserni/kotkan-energia/ [viitattu 26.10.2021].

Kunnari, I. 2020. Zero Trust -tietoturvan nykymalli. Haaga-Helian ammattikorkeakoulu. Tietojenkäsittelyn koulutusohjelma. Opinnäytetyö. PDF-dokumentti. Saatavissa: https://urn.fi/URN:NBN:fi:amk-202004024346 [viitattu 26.10.2021].

National Institute of Standards and Technology. 2020. Security and Privacy Controls for Information Systems and Organizations. PDF-dokumentti. Saatavissa: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf [viitattu 29.3.2022].

National Institute of Standards and Technology. 2022. About NIST. WWW-dokumentti. Saatavissa: https://www.nist.gov/about-nist [viitattu 28.3.2022].

McAfee. s.a. What Is Shadow IT? WWW-dokumentti. Saatavissa: https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-shadow-it.html [viitattu 23.3.2022].

Microsoft. 2022. Zero Trust Guidance Center. WWW-dokumentti. Saatavissa: https://docs.microsoft.com/en-us/security/zero-trust/ [viitattu 23.3.2022].

National Cyber Security Center. 2021a. Zero trust architecture design principles. WWW-dokumentti. Saatavissa: https://www.ncsc.gov.uk/collection/zero-trust-architecture [viitattu 16.2.2022].

National Cyber Security Center. 2021b. Device Security Guidance. WWW-dokumentti. Saatavissa: https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/network-architectures [viitattu 23.3.2022].

Palo Alto Networks. 2021a. Best Practices Implementing Zero Trust with Palo Alto Networks. PDF-dokumentti. Saatavissa: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/best-practices/9-0/zero-trust-best-practices/zero-trust-best-practices.pdf [viitattu 24.2.2022].

Palo Alto Networks. 2021b. ICS and SCADA Industry. PDF-dokumentti. Saatavissa: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/scada-ics-solution-brief [viitattu 24.2.2022].

Pernaa, J. 2013. Kehittämistutkimus tutkimusmenetelmänä. PDF-dokumentti. Saatavissa: https://tuhat.helsinki.fi/ws/files/127650174/2013_Pernaa_KT_tutkimusmenetelmana_KT_kirja.pdf [viitattu 31.3.2022].

Romness, P. Chester, H. Miller, S. Belanger, X. Barton, T. Zero Trust Architecture: Rethinking Cybersecurity for Changing Enviroments. WWW-dokumentti. Saatavissa: https://er.educause.edu/articles/2022/2/zero-trust-architecture-rethinking-cybersecurity-for-changing-environments#fn3 [viitattu 28.3.2022].

Rose, S. Borchert, O. Mitchell, S. Connelly S. 2020. Zero Trust Architecture. PDF-dokumentti. Saatavissa: https://doi.org/10.6028/NIST.SP.800-207 [viitattu 28.10.2021].

SFS. 2018. SFS-ISO/IEC 27005:2018. Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta. PDF-dokumentti. Saatavissa: https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/738504.html.stx [viitattu 2.3.2022].

Teerakanok, S. Uehara, T. Inomata, A. 2021. Migrating to Zero Trust Architecture: Reviews and Challenges. WWW-dokumentti. Saatavissa: https://doi.org/10.1155/2021/9947347 [viitattu 27.10.2021].

Terva, P. 2019. Zero Trust -arkkitehtuuri. Kaakkois-Suomen ammattikorkeakoulu. Tieto- ja viestintätekniikka. Opinnäytetyö. PDF-dokumentti. Saatavissa: https://urn.fi/URN:NBN:fi:amk-202003093195 [viitattu 26.10.2021].

Westerberg, J. 2021. Verkon tietoturva Zero Trust -konseptissa. Yritysverkon mukauttaminen Zero Trust -konseptiin. Jyväskylän ammattikorkeakoulu.

Master's Degree Programme in Information Technology, Cyber Security. Opinnäytetyö. PDF-dokumentti. Saatavissa: https://urn.fi/URN:NBN:fi:amk-202105189337 [viitattu 26.10.2021].

White House. 2021. Executive Order on Improving the Nation's Cybersecurity. WWW-dokumentti. Saatavissa: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ [viitattu 31.3.2022].

Williams, T. Rathwell, G. Li, H. 2001. A handbook on master planning and implementation for enterprise integration programs. PDF-dokumentti. Saatavissa: http://www.pera.net/Pera/Report160%281996%29Handbook/PERA_Handbook.pdf [Viitattu 16.3.2022].

VMware. s.a. What is intent-based networking (IBN?). WWW-dokumentti. Saatavissa: https://www.vmware.com/topics/glossary/content/intent-based-networking.html [viitattu 25.3.2022].

Zscaler. s.a. What Is the Purdue Model for ICS Security? WWW-dokumentti. Saatavissa: https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security [viitattu 15.2.2022].