Kyberturvallisuus ja Azure AD -identiteettien suojaaminen Conditional Accessilla

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Hämeen ammattikorkeakoulu, tietojenkäsittelyn koulutusohjelma

syksy, 2019

Antti Syrjänen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutusohjelma
Hämeenlinnan korkeakoulukeskus

Tekijä Antti Syrjänen **Vuosi** 2019

Työn nimi Kyberturvallisuus ja Azure AD -identiteettien suojaaminen Conditional Accessilla

Työn ohjaaja/t Erkki Laine

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli suojata Azure Active Directoryn (Azure AD) identiteetit ehdollisen pääsyn käytännöillä, sekä kasvattaa lukijan ymmärrystä tieto- ja kyberturvallisuudesta. Kyberturvallisuuden ymmärtäminen on tärkeää, sillä tämä bittien maailma on jo vahvasti osa meidän arkipäiväämme, ilman sitä emme saisi maksettua laskuja verkkopankissa tai tallennettua puhelimella otettuja kuvia pilvipalveluihin.

Työ on jaettu teoria ja käytännön osuuteen. Teoriaosuudessa käsitellään kyberturvallisuutta, sekä fyysisen maailman ja kybermaailman eroavaisuuksia. Teoriaosuus sisältää myös tietoturvallisuuden peruskäsitteet.

Käytännön osiossa keskitytään Azure Active Directory -identiteettien suojauskäytäntöihin, sekä tarkastelemme sisäänkirjautumislokitietoja. Käytännön osio on suunniteltu käyttäjille, joilla on perustason ymmärrys Microsoftin Office 365 -pilvipalvelusta.

Avainsanat Azure Active Directory, Tietoturva, Kyberturvallisuus

Sivut 30 sivua, joista liitteitä 0 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Hämeenlinna University Centre

Author Antti Syrjänen **Year** 2019

Subject Cyber security and protecting Azure AD- identities with Conditional Access

Supervisors Erkki Laine

ABSTRACT

The purpose of this thesis was to protect Azure Active Directory identities with conditional access policies and to increase the reader's understanding of information and cybersecurity. Understanding cybersecurity is important because this world of bits is already very much a part of our daily lives, without which people would not be able to pay their online bills or save their phone images to the cloud.

The work is divided into theoretical and practical parts. The theory section deals in depth with cyber security and how the laws of the physical world differ from the cyber world. The theory section also contains the basic concepts of security.

The Policy section focuses on Azure Active Directory Identity Protection policies and looks at the login log information. The Practice section is designed for users who have a basic understanding of Microsoft's Office 365 cloud service.

Keywords Azure Active Directory, Information security, Cyber security

Pages 30 pages including appendices 0 pages

KÄSITELUETTELO

Azure Active Directory
Azure Active Directory on Microsoftin pilvipohjainen pääsyn- ja identiteetinhallintapalvelu, jonka avulla käyttäjät voivat kirjautua Office 365-palveluun ja käyttää sen resursseja.

Brute-force attack
Väsytyshyökkäyksessä (Brute-force attack) rikollinen toimija pyrkii arvaamaan käyttäjätunnuksen salasanan.

Conditional Access
Conditional Access (ehdollisen pääsyn käytäntö) on Microsoft Azure Active Directoryssä oleva identiteettien suojausominaisuus, jolla voidaan luoda sisäänkirjautumisehtoja, jotka aktivoituvat, kun ensimmäisen tekijän todennus on suoritettu loppuun.

CSV
CSV (Comma-Separated Values) on tiedostomuoto, jolla tallennetaan taulukonmuotoista tietoa tekstitiedostoon.

Exchange Active Sync
Exchange Active Sync on Microsoftin kehittämä protokolla, mobiilisähköpostisovelluksia varten.

IMAP-protokolla
IMAP-protokolla on sähköpostiviestin lukemiseen tarkoitettu protokolla.

JSON
JSON (JavaScript Object Notation) on avoimen standardin tiedostomuoto tiedonvälitykseen.

Kyber
Kyber-etuliitteellä tarkoitetaan ei fyysistä bittien maailmaa.

Kybertoimintaympäristö
Kybertoimintaympäristöllä tarkoitetaan digitaalista rinnakkaistodellisuutta.

Kyberturvallisuus
Kyberturvallisuuden tarkoitus on varmistaa kybertoimintaympäristön luotettavuus ja se, että sen toiminnasta voidaan huolehtia.

Kyberavaruus
Kyberavaruus on nimitys virtuaaliulottuvuudelle, joka muodostuu tietokoneyhteyksien välille.

MFA

Multi-factor authentication (Monimenetelmäinen todennus) on keino suojata Office 365-Identiteettejä. Palveluun kirjautuessa käyt-täjältä vaaditaan vielä toinen todentamismenetelmä. Jolloin käyttäjä saa kertakäyttökoodin tekstiviestinä tai puhelin soittona.

POP3-protokolla
POP-protokolla (Post Office Protocol version 3) on sähköpostin hakemiseen tarkoitettu protokolla.

SMTP-protokolla
SMTP-protokolla (Simple Mail Transfer Protocol) on sähköpostiviestin välittämiseen tarkoitettu protokolla.

SISÄLLYS

1 JOHDANTO

Tässä opinnäytetyössä käsitellään tietoturvaa. Se on ajankohtainen aihe, koska tietomurtoja tapahtuu jatkuvasti ja yritysten on varauduttava suojaamaan tietojärjestelmänsä näiltä uhkilta.

Vuoden 2018 kesäkuussa nousi pintaan suuri määrä kotimaisiin yrityksiin kohdistuneita Office 365-sähköpostien kalastelu ja tietomurtoyrityksiä, ne aiheuttivat useille yrityksille tuntuvia kuluja ja tappioita. Hyökkäysten kohteena ovat erityisesti yritysten johtoryhmien jäsenet ja laskuja käsittelevät työntekijät. Käyttäjätunnusten kalastelun onnistuessa rikolliset pyrkivät asettamaan sähköpostitileille sääntöjä, joilla he saavat kopiot kaikista kaapatun tilin sähköposteista. Rikolliset hyödyntävät kaapattua tiliä myös uusien kalastelu- ja huijausviestien lähettämiseen. (Kyberturvallisuuskeskus, 2018)

Toiminnallinen opinnäytetyöni jakautuu teoria ja käytännön osioon. Valitsin teoria osan aiheeksi kyberturvallisuuden, koska se on lähes päivittäinen keskustelun aihe ja on myös usein uutisotsikoissa. Käytännön osio on myös hyvin ajankohtainen, sillä yritysten ja organisaatioiden Office 365 -pilvipalveluiden tietomurtoyritykset ovat joka päiväisiä. Tietomurtojen torjuminen on tärkeää tiedon luottamuksellisuuden ja eheyden kannalta.

Teoriaosassa käydään läpi tietoturvallisuuden peruskäsitteet sekä käsitellään kyberturvallisuutta hyvin syvällisesti, mutta silti asiaan perehtymättömälle lukijalle ymmärrettävällä tasolla. Teoriaosan tarkoitus on kasvattaa lukijan ymmärrystä kyberturvallisuudesta, sekä kuinka fyysisen maailman lainalaisuudet muuttuvat astuessa kybermaailmaan.

Käytännön osiossa pyritään suojaamaan Azure Active Directory -identiteetit tietomurroilta. Azure Active Directory tarjoaa useita työkaluja ja mahdollisuuksia vaikuttaa käyttäjätilien suojaukseen. Opinnäytetyössä otetaan käyttöön monimenetelmäinen todennus hyödyntäen ehdollisen pääsyn käytäntöjä, sekä estetään yleisimmät salasanat ja määritetään salasanoille elinkaari. Identiteetteihin kohdistuvat suojaustoimenpiteet vaikuttavat osittain myös ohjelmiston käyttömukavuuteen ja tarkoituksena on optimoida käyttömukavuus ja tietoturva.

Keskeisimmät tutkintakysymykset ovat:
Mitä on kyberturvallisuus?
Miten monimenetelmäinen todennus otetaan käyttöön?
Miten Office 365 -identiteetti voidaan suojata tietomurroilta?

2 TIETOTURVALLISUUDEN KÄSITTEET

Tietoturvallisuus käsitteenä on hyvin laaja. Tiedon arvoon perustuva klassinen määritelmä sisältää luottamuksellisuuden, käytettävyyden ja eheyden. Nykyisin tätä klassista määritelmää pidetään puutteellisena, koska siinä ei huomioida laitteistojen, tietoliikenne- tai tietojärjestelmien merkitystä. Laajennettuun tietoturvallisuuden määritelmään kuuluu lisäksi kiistämättömyys ja pääsynvalvonta. Joissakin esityksissä käsitteisiin on myös lisätty autenttisuus, joka tarkoittaa tietojärjestelmään liitettyjen laitteiden sekä käyttäjien luotettavaa tunnistusta. Tämä käsite on luottamuksellisuuden ja kiistämättömyyden edellytys, joten se on usein jätetty pois määrittelystä. (Hakala, Vainio & Vuorinen, 2006, s. 4-5; ks. Rousku, 2014, s. 47)

Luottamuksellisuuden tarkoitus on, että tietojärjestelmässä olevia tietoja voi käsitellä vain ne henkilöt, joilla on siihen oikeus. Luottamuksellisuus toteutetaan tavallisesti käyttöoikeuksien hallinnalla, käyttäjätunnuksilla ja salasanoilla. Yrityksissä oikeudet määritetään käyttäjän työtehtävän mukaan niin että käyttäjä pääsee käsiksi tarpeellisiin tiedostoihin ja pystyy työskentelemään yrityksen tietojärjestelmissä. (Hakala ym., 2006, s. 4-5; ks. Rousku, 2014, s. 47-48)

Käytettävyys merkitsee sitä, että yrityksen tietojärjestelmät ja tiedot ovat saatavilla oikeassa muodossa riittävän nopeasti. Käytettävyyttä voidaan ylläpitää riittävän tehokkailla tieto- ja tietoliikennejärjestelmälaitteilla ja että käytettävät sovellusohjelmat ovat mahdollisimman yhteensopivia tallennettujen tietojen käsittelyyn. Käytettävyyttä lisää myös, että käyttäjä saa haluamansa tiedon järjestelmästä itselleen sopivassa muodossa, kuten yhteenvetoina tai valmiina raportteina. Yhteiskunta on muuttumassa yhä enemmän ympärivuorokautiseen suuntaan, jolloin palveluiden ja tietojen on oltava käytettävissä kaiken aikaa. (Hakala ym., 2006, s. 4-5; ks. Rousku, 2014, s. 50-51)

Eheys on kattavasti käsitettynä sitä, että tallennetut tiedot tietojärjestelmässä pitävät paikkansa eivätkä sisällä tahattomia tai tahallisia virheitä. Käytännössä tämä tarkoittaa sitä, että tietoja voivat muuttaa vain sellaiset käyttäjät, joilla on siihen käyttöoikeus ja vain sallituilla keinoilla. Eheyttä tavoitellaan etupäässä ohjelmistoteknisin ratkaisuin. Sovellusohjelmiin määritellään erilaisia syötteen varmistuksia tai syöttörajoitteita, tiedonsiirto- ja tallennusoperaatioihin tiivisteitä tai varmistusyhteenvetoja. Laitteistotason virheet pyritään estämään virheenkorjaavilla muisteilla tai väylillä. Tietoliikennejärjestelmissä pyritään hyödyntämään korjausmekanismeilla varustettuja laitteita ja protokollia. Eheyden ylläpitoon soveltuvat myös useimmat salakirjoitusmenetelmät ja tuotteet. (Hakala ym., 2006, s. 4-5; ks. Hallikainen, 2017a)

Kiistämättömyys tarkoittaa tietojärjestelmän kykyä identifioida ja tallentaa tietojärjestelmässä toimivan käyttäjän tiedot luotettavasti.

Kiistämättömyyttä tavoitellaan pääasiassa kahdesta eri syystä. Halutaan vahvistaa tiedon alkulähde. Toiseksi tilanteissa, joissa tietoja on käytetty väärin tai luvattomasti ja järjestelmän omistaja harkitsee oikeudellisia toimija käyttäjää vastaan. Kiistämättömyydessä hyödynnetään biometrisiä tunnisteita ja salausmenetelmiin liittyviä tunnistustoimintoja. Salaustekniikoita hyödyntävinä käyttäjätunnistusmenetelminä käytetään usein pieniä mukana kuljetettavia älykortteja tai muita laitteita, laitteeseen on tallennettu käyttölupa ja käyttäjän henkilötiedot. Käyttöluvalle voidaan määrittää myös vanhenemispäivä, jonka jälkeen käyttölupa täytyy uusia tai laite ei päästä kirjautumaan tietojärjestelmään. Biometrisessä tunnistuksessa käytetään sormenjälki-, kasvontunnistus- ja silmänpohjantunnistuslaitteita. (Hakala ym., 2006, s. 5; ks. Hallikainen, 2017b)

Pääsynvalvonnalla rajoitetaan tietojenkäsittelyinfrastruktuurin käyttöä. Organisaatiot pyrkivät estämään tietoliikenneyhteyksien ja laitteiden käytön ulkopuolisilta tai haluavat rajoittaa omaa henkilökuntaa käyttämästä niitä omiin tarkoituksiinsa. Tietojärjestelmän luvaton käyttö kuormittaa tietoliikenneverkkoja sekä laitteita ja saattaa altistaa organisaation tietojärjestelmän haittaohjelmille. Jos pääsyn valvonta pettää, se voi johtaa eheys- ja luottamuksellisuusongelmiin. Langattomien verkkojen yleistyttyä pääsynvalvontaan on jouduttu kiinnittämään enemmän huomiota, ei toivotut toimijat voivat pyrkiä tietoverkkoon niin että heidän ei tarvitse fyysisesti päästä kohteen lähettyville vaan voivat murtaa langattoman verkon salasanan ja sitä kautta hyödyntää tietoliikenneverkkoa. (Hakala ym., 2006, s. 5-6; ks. Karvi, 2012)

3 KYBERTURVALLISUUS

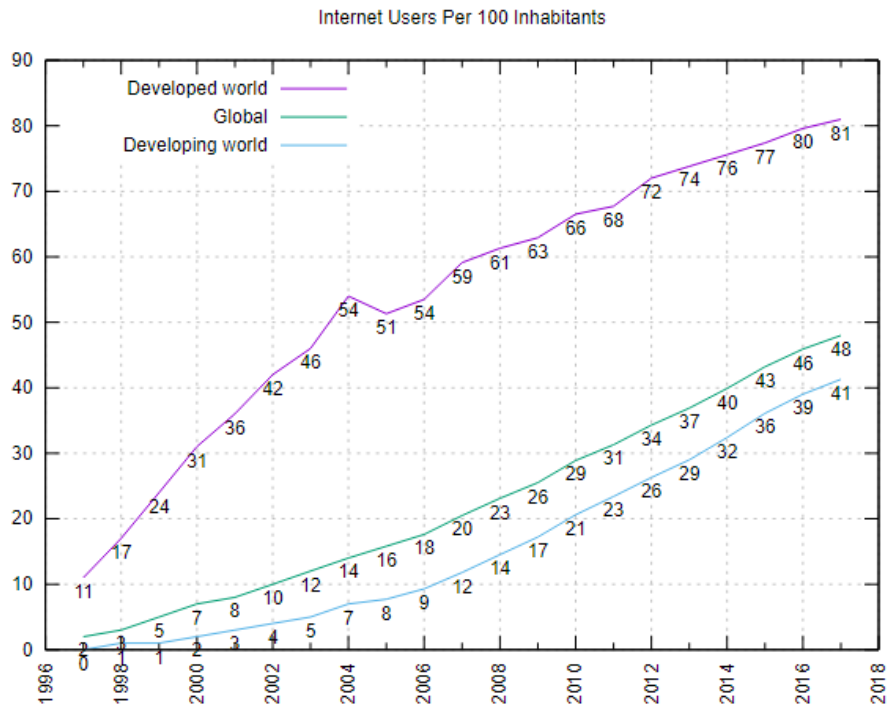
Verrattaessa tietoturvallisuuteen kyberturvallisuus kattaa huomattavasti suuremman kokonaisuuden. Kyberturvallisuuden tarkoitus on varmistaa kybertoimintaympäristön luotettavuus ja se, että sen toiminnasta voidaan huolehtia. Kybertoimintaympäristöllä tarkoitetaan sähköisessä muodossa olevia tietojenkäsittelyyn tarkoitettuja tietojärjestelmiä. Kybertoimintaympäristöön kohdistuvat uhat eivät aina tule sähköisiä kanavia pitkin, ne voivat syntyä myös luonnonilmiöiden tai inhimillisten erehdysten seurauksena. (Rousku, 2014, s. 54-57; ks. Puro, 2017)

Tietoturva ja kyberturvallisuus eroavat toisistaan niin, että tietoturvalla suojataan tietojärjestelmässä käsiteltäviä tietoja ja kyberturvallisuudella torjutaan, ennaltaehkäistään tai lievennetään negatiivisia vaikutuksia ja suojaudutaan niiden tekijöiltä. Tämä tekee kyberturvallisuudesta uhkapainotteista. Tietoturvan pettäessä kyberympäristö voi toimia toisin kuin on tarkoitus. Esimerkiksi vaikutus lentokentällä voisi olla, että lennot lähtevät väärään suuntaan tai väärään aikaan. (Peltomäki, Norppa, 2015, s. 67-68; Limnéll, Majewski & Salminen, 2014, s. 1)

Limnellin ym. (2014, s. 15) mukaan ”Kyberturvallisuus on tasapainottelua mahdollisuuksien ja uhkien välillä”. Tasapainottelu mahdollisuuksien ja uhkien välillä on haastavaa, jos ei omista peruskäsitystä kybermaailmasta. Kyberturvallisuudessa on tärkeää ottaa huomioon kaksi asiaa. Ensinnäkin kyberuhkat ovat kiistattomia ja vakavimmillaan voivat vaikuttaa koko organisaation kybertoimintaympäristöön. Välinpitämättömyyden kustannukset voivat nousta organisaatioissa ja yhteiskunnissa merkittäviksi. Toiseksi on muistettava kyberturvallisuuden tuomat positiiviset mahdollisuudet. Kybermaailma tarjoaa hallinoille, yrityksille ja muille organisaatioille alati mahdollisuuksia toiminnan tehostamiseen ja laajentamiseen, kustannusten alentamiseen ja uusien palveluiden kehittämiseen. Etsiessä tasapainoa mahdollisuuksien ja uhkien välille on tärkeää huomioida kunkin organisaation tilanne ja erityispiirteet. (Limnéll ym., 2014, s. 15; ks. Limnéll & Tuominen, 2014)

Kybermaailmassa vallitsevat lainalaisuudet on myös syytä omaksua. Kybermaailma on dynaaminen ympäristö, joka on globaali, ympärivuorokautinen sekä ajallisesti ja maantieteellisesti rajaton. Tämä bittien maailma muuttuu ja kehittyy hurjalla vauhdilla, jota on vaikea käsittää. Esimerkiksi uusia teknologisia ratkaisuja julkaistaan lähes päivittäin ja kehityksen vauhti vain kiihtyy. (Limnéll ym., 2014, s. 16)

Internetin valtava kehitys näkyy myös käyttäjä määrien kasvuna, kuten kuva 1. havainnollistaa. Kehittyneiden maiden kansalaisista puolet olivat vuonna 2005 internetin käyttäjiä, kun luku vuonna 2018 on jo noin 80 prosenttia. Maailmasta löytyy vielä valtioita, jotka eivät ole kytkeytyneet globaaliin kyberympäristöön. (Limnéll ym., 2014, s. 18)



Kuva 1. Internetin käyttäjät 100 asukasta kohden (Limnéll ym., 2014, s. 18)

Ihmiset siirtyvät internetin myötä yhä laajenevissa määrin globaaliin virtuaaliseen ympäristöön, jossa palveluita kulutetaan ja tuotetaan sekä elämää eletään kulttuurista, paikasta ja ajasta riippumattomasti. Internet yhdistää ihmisten lisäksi esineitä, koneita ja palveluita tavoilla, joita emme menneinä vuosina osanneet edes ajatella. (Limnéll ym., 2014, s. 18-19)

Kaikkien merkityksellisintä on internetin sähköisen viestinnän vaikuttavuus yhteiskunnan eri osa-alueisiin ja tiedon määrä, jota tuotetaan maailmassa joka päivä. Useat pitävät tätä ihmisen kehityksen kannalta merkittävämpänä asiana kuin sähkön käyttöönottoa tai kirjapainoa. Esimerkiksi pankkisektori on täysin siirtynyt sähköistä tietoa hyödyntävään toimintamalliin. Tämän myötä alan arvoketjut ja rakenteet ovat muuttuneet täysin. (Limnéll ym., 2014, s. 19)

Älypuhelinten, teknologian ja internetin yleistyminen kokonaisuudessaan on saanut meidät luottamaan rahojemme säilymiseen verkkopankissa, tekemään etätöitä, siirtymään useissa palveluissa aikaisempaa enemmän itsepalveluihin ja hankkimaan ostokset nettikaupoista. Samaan aikaan sosiaalisesta mediasta on tullut merkityksellinen asenne- ja mielipidevaikuttamisen tapahtumapaikka. (Limnéll ym., 2014, s. 19)

3.1 Kyber

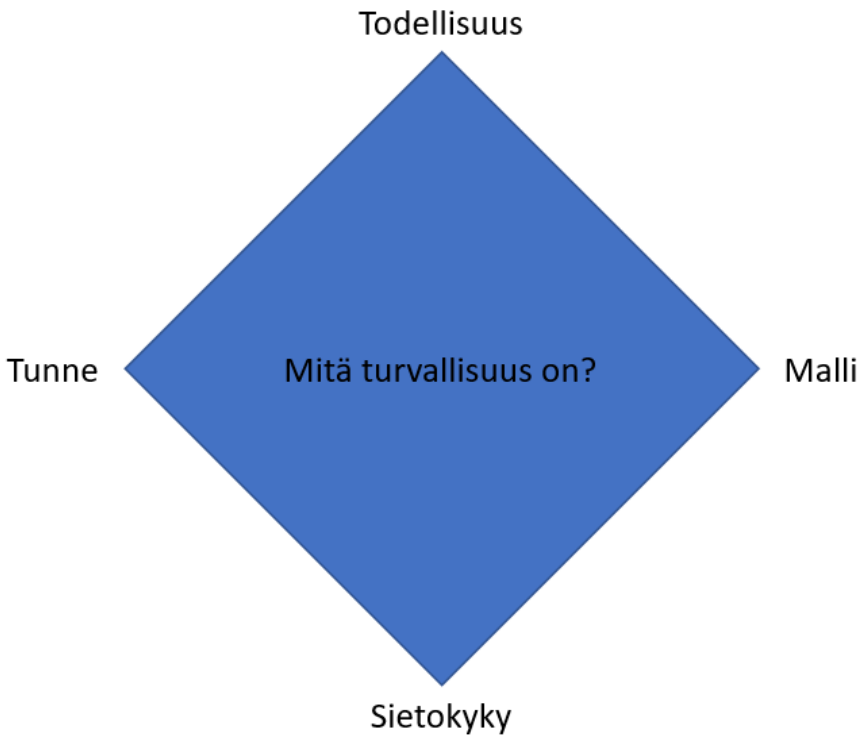
Sana kyber tulee kreikan sanasta kybereo – ohjata, hallita, opastaa. On olemassa fyysinen ja kybermaailma. Fyysiseen maailmaan kuuluvat esimerkiksi polkupyöräsi, matkalaukkusi ja työpöytäsi. Tämä atomien maailma on

konkreettista ja silmin havaittavaa. Kyber-etuliitteellä tarkoitetaan ei fyysistä maailmaa, tähän maailmaan kuuluvat internet, erilaiset mobiilisovellukset, sosiaalinen media sekä tietoverkot ja -järjestelmät. Kiteytettynä kyber on bittienmaailma, joka vaikuttaa päivittäiseen elämäämme, vaikka emme sitä aina osaisi ajatella. (Limnéll ym., 2014, s. 29; ks. tsk, 2018)

3.2 Turvallisuus

Turvallisuus on todellisuutta, tunnetta, sietokykyä ja opittuja malleja. Turvallisuus on tunnetta siitä, kuinka turvalliseksi tunnemme itsemme tässä hetkessä ja ympäristössä. Tunne on myös subjektiivinen, joka tarkoittaa sitä, että sama tilanne voi vaikuttaa yksilöllisesti eri ihmisten turvallisuuden tunteeseen. Todellisuus on kollektiivinen käsitys asioiden oikeasta tilasta, puutteellinen ymmärrys todellisuudesta voi johtaa turvallisuuden illuusioon. Tällöin kun emme ole tietoisia asioiden todellisesta tilasta tunnemme itsemme turvalliseksi. (Limnéll ym., 2014, s. 34; ks. Eskola, 2008)

Turvallisuutta rakennetaan opituista ja kehitettävistä malleista. Käytännössä minkälaisia prosesseja, tapoja ja tekniikoita yrityksessä halutaan kehittää turvallisuuden parantamiseksi. Keskeisin osa turvallisuutta on kykymme sietää yleisestä turvallisuuden tilasta poikkeavia tilanteita. Kun sietokyky on heikko, pienet ja suuret häiriötilanteet voivat vaivata meitä tai aiheuttaa paniikkia. (Limnéll ym., 2014, s. 34-35; ks. Limnéll & Tuominen, 2014)



Kuva 2. Turvallisuuden neljä osatekijää. (Limnéll ym., 2014, s. 34)

Kokonaisturvallisuuden kehittämiseen tarvitaan kaikkia neljää turvallisuuden osatekijää (Kuva 2.). Kybermaailmassa todellisuus muuttuu suurella vauhdilla ja ymmärryksen on pysyttävä tässä muutoksessa mukana. Jos emme pysty ymmärtämään näitä ympärillämme tapahtuvia muutoksia, perustuu tunteemme turvallisuudesta vääriin oletuksiin. Tällöin on mahdotonta luoda turvallisuutta parantavia malleja sekä vahvistaa sietokykyä. (Limnéll ym., 2014, s. 36)

Turvallisuus on myös tavoitetila, johon pyritään tekemällä toimia, jotka lisäävät turvallisuutta. Usein turvallisuuden kartoittaminen aloitetaan uhkien arvioimisella. Uhka on vaaraa, haittaa tai epävarmuutta ilmentävä tekijä, joka voi vaikuttaa toimintaympäristöömme. Uhkien kartoituksella pystytään paremmin ymmärtämään tavoiteltavaa turvallisuustasoa. (Limnéll ym., 2014, s. 34)

Turvallisuuden kolme ulottuvuutta, kohde, uhka ja keinot ovat keinoja arvioida turvallisuutta. Nämä kolme ulottuvuutta ovat kiinteästi vuorovaikutuksessa keskenään. Kohde määrittää mitä tai ketä turvataan ja kuinka vahvasti sekä mitä tapahtuu, jos turvallisuus pettää. Jos turvattavia kohteita on useampi, täytyy ne priorisoida tärkeysjärjestykseen. Uhka-arvioissa arvioidaan vakavuusastetta, sekä mitkä uhkat voivat meille tärkeitä arvoja vaarantaa. Uhkana voidaan pitää mitä tahansa kielteistä asiaa, joka voi haitata yrityksen toimintaa. Keinot ovat toimia, joihin ryhdytään turvattavan kohteen turvaamiseksi uhkaavilta tekijöiltä. Nämä kolme turvallisuuden ulottuvuutta koskevat fyysistä- että kybermaailmaa. (Limnéll ym., 2014, s. 37-38)

3.3 Kyberturvallisuuden uhkakuvat

Kyberkeskusteluissa korostuu usein kybermaailman negatiivinen näkökulma. Negatiivisen puolen jäsentämisessä voidaan käyttää kolmea käsitettä: Haavoittuvuus, riski ja uhka. Nämä kolme käsitettä ei ole yksi ja sama asia, vaikkakin ne vaikuttavat toisiinsa. (Limnéll ym., 2014, s. 105)

Haavoittuvuus, riski ja uhka omaavat kaikki samanlaisia ominaisuuksia, kuten niiden rajallisuus ja suhteellisuus (aika, kyky, resurssit, vahingoittavuus). Kuitenkin toiminnoiltaan, piirteiltään ja vastatoimiltaan nämä käsitteet ovat huomattavan erilaisia. Lisäksi nämä kolme käsitettä ovat aina tilanne- ja toimijakohtaisia. (Limnéll ym., 2014, s. 105)

3.3.1 Haavoittuvuus

Tietotekniikassa haavoittuvuudella tarkoitetaan heikkoutta, joka mahdollistaa toimijalle keinon heikentää järjestelmän tieto- ja toimintavarmuutta. Haavoittuvuus muodostuu, jos järjestelmässä on vika tai heikkous. Tämän

lisäksi toimijalla täytyy olla pääsy järjestelmään ja kyky hyödyntää kyseistä vikaa tai heikkoutta. Haavoittuvuus on piirre, joka on suhteellinen ja järjestelmän sisäinen. Järjestelmän haavoittuvuuksia pystytään vähentämään systemaattisen tunnistamisen, luokittelemisen, lieventämisen ja korjaamisen keinoin. (Limnéll ym., 2014, s. 110; ks. Neptunet, 2013)

Haavoittuvuutta pidetään yleisemmin uhkasta jäljelle jäävänä osuutena, kun siitä on poistettu palautumis- ja sietokyky. Mitä korkeampi toimijan palautumis- ja sietokyky on, sitä vähemmän haavoittuvainen tämä on tietynlaisten uhkien edessä. (Limnéll ym., 2014, s. 110)

Kybermaailman ulkopuolella haavoittuvuus tunnetaan myös usein materiaalisina, teknologisina tai osaamiseen viittaavina heikkouksina. Yhteiskunnan suurimmat haavoittuvuudet materiaalisesti ovat sen tietoverkoissa ja järjestelmissä. Toisin sanoen kriittisessä infrastruktuurissa sekä kriittisessä informaatioinfrastruktuurissa, joita useimmiten hallinnoidaan kybermaailmasta käsin. Materiaalisiakin tekijöitä suurempi yhteiskunnan haavoittuvuus on sen henkisen sietokyvyn puute ja naiivi luottamus niin yhteiskunnan kuin etenkin kybermaailman toimivuuteen. (Limnéll ym., 2014, s. 110-111)

3.3.2 Riski

Riski on asia, joka sisältyy kaikkeen toimintaan ja sitä ei voi sivuuttaa. Riskiä ei voida pitää myöskään ongelmana koska ongelmat ovat seurauksia jostain tapahtuneesta. Riski kuvastaa jonkin negatiivisen tapahtuman mahdollisuutta tulevaisuudessa. Riski muuttuu ajan myötä, eikä se ole itsessään hyvä eikä huono asia. Riskeihin voidaan suhtautua monella eri tavalla, kuten välttämällä niitä, rajaamalla tai lieventämällä niitä, omaksumalla ne sekä oppimalla elämään niiden kanssa. (Limnéll ym., 2014, s. 108; ks. virtual.vtt, n.d.b)

Ongelmat on mahdollista sivuuttaa riskien todennäköisyyslaskelmalla. Se muodostetaan arvioimalla todennäköisyyttä tulevaisuudessa tapahtuvasta negatiivisesta asiasta ja sen todennäköisistä vaikutuksista. Riskilaskelmassa voidaan käyttää myös omaisuuden ja sen arvon vastaan kohdistuvaa uhkaa ja uhkan toteutumista vaikutusten tulona. Jos riskin toteutumisen todennäköisyyttä ei voida arvioida tai tietää, jää riski arvioimatta ja toimija joutuu toimimaan epävarmuudessa. Epävarmuus painostaa valmistautumaan pahimpaan, joka voi johtaa herkästi ali- tai ylilyönteihin, luottamattomuuteen, turvallisuuden illuusioon tai resurssien hukkaamiseen. (Limnéll ym., 2014, s. 108)

Riskitietoisuus ja riski käsitteenä ovat lähivuosikymmeninä läpäisseet niin julkisen kuin yksityisen hallinnon. Kybermaailma ei ole ainut missä tämä on tapahtunut, sillä riskienhallinnasta on tullut varsinainen järjestäytymisperiaate hallinnolle. Tapahtumien, asioiden ja prosessien lopputulemiin voidaan vaikuttaa ihmisten päätöksen teolla sen sijaan että ne olisivat

kohtalon tai rakenteiden etukäteen määräämiä. Uhkat, joita voidaan vain torjua, kääntyvät riskeiksi, joita vastaan voidaan toimia monimuotoisemmin. (Limnéll ym., 2014, s. 108)

3.3.3 Riskienhallinta

Riskienhallinnan voimin pyritään toteuttamaan lakkaamatonta muutosta, koska valtiohallinnolla ja yrityksillä ei ole muita mahdollisuuksia. Tällä metodilla pyritään arvioimaan ja tunnistamaan riskejä sekä kehittämään, toteuttamaan ja valitsemaan vaihtoehtoja riskin hallitsemiseksi organisaatiossa. Riskienhallinta heijastaa organisaation ideaaleja ja arvoja esimerkiksi vastuullisuuteen ja luotettavuuteen liittyen. Riskienhallinta on systemaattinen ja keskeytymätön ajatteluprosessi. Alla olevassa taulukossa 1. käsitellään riskienhallinta prosessit (Limnéll ym., 2014, s. 108; ks. virtual.vtt, n.d.a)

Systemaattinen ja jatkuva ajatteluprosessi	
	Kaikki mahdolliset riskit.
	Ongelmat ja katastrofit ennen kuin ne realisoituvat.
Toimintatapojen luomisprosessi	
	Mahdollisesti toteutuvien vaikutusten minimoiminen.
	Riskien välttäminen.
	Toteutuvien vaikutusten kanssa toimiminen.
Tunnistetut ja tiedostetut riskit	
	Vaikutuksista on olemassa arvio.
	Riskit pystytään laittamaan tärkeysjärjestykseen.
	Riskeihin pyritään vaikuttamaan käytettävissä olevin keinoin.
	Arvioidaan hankittavilla kyvykkyyksillä mahdollisesti aikaan saatava lisävaikutuskyky.
	Ulkoistetaan osa riskeistä esimerkiksi vakuuttamisella.
	Hyväksytään jäljelle jäävät riskit ja pyritään toimimaan mahdollisten negatiivisten vaikutusten kanssa.

Taulukko 1. Riskienhallinta prosessit (Limnéll ym., 2014, s. 109-110)

Riskienhallinta muodostuu täten riskienhallinta suunnittelusta, riittävästä viestinnästä, raportoinnista, koordinoinnista, korjaavien toimenpiteiden toteuttamisesta, jatkuvasta riskien kehittymisen seuraamisesta sekä riskien aikaisesta tunnistamisesta ja analysoinnista. (Limnéll ym., 2014, s. 110)

Riskiajattelu heijastuu kybermaailman lainalaisuuksista. Aika ei ole enää rajoittava tekijä riskiajattelussa, sillä tulevaisuuden sukupolvet kokevat meidän päätöksemme vaikutukset. Tilakaan ei ole enää rajoite, sillä riskit voivat ylittää kansalliset ja organisatoriset rajat. Nyky-yhteiskunnan sisältämistä riskeistä ei voida pitää vastuullisena ketään. Syyllisten tunnistettavuuden ja vahinkojen laskettavuuden heikennettyä ei ole mahdollista korvata vahinkojen aiheuttamia vaikutuksia niille, joiden elämiin toteutuneet

riskit ovat koskettaneet. Tästä syystä toimijoiden on kasvettava ketteriksi, sietokykyisiksi ja joustaviksi. (Limnéll ym., 2014, s. 110)

3.3.4 Uhka

Uhka on toimintaa, jolla pyritään pakottamaan kohde toimimaan halutulla tavalla ja saada sitä kautta aikaan negatiivisen vaikutuksen kohteen intresseissä. Uhkasta tulee pakottavaa, kun kohteen toimintavaihtoehdot saadaan minimoitua. Uhkan muodostamisessa olennaisinta on kiristysluonteinen kommunikointi kohteelle. Kommunikoinnin tarkoitus ei ole vielä vahingoittaa kohteen toimintaympäristöä vaan lisätä uhkan uskottavuutta. Kyberuhkien filosofia on samanlainen, ainoastaan toimintaympäristö poikkeaa. (Limnéll ym., 2014, s. 105-106; ks. Seppälä, 2011)

Kohteen arviot uhkan vakavuudesta ja uskottavuudesta muodostuvat uhkaajan kyvyistä ja tämän halukkuudesta toteuttaa uhattu toimi. Uhkan vakavuuteen vaikuttaa myös kohteen riippuvuus kyseisestä tietojärjestelmästä tai toiminnoista, joita kohtaan uhkakuva kohdistetaan. Uhka sekä turvallisuus koostuvat uhkan todellisuudesta ja siihen liittyvistä uskomuksista. (Limnéll ym., 2014, s. 105-106)

Usein kyberuhkien kohdalla uhka ei johdu suoraan toimijasta, vaan se on rakenteeltaan abstraktimpi. Kohdistamattomien abstraktien uhkien arvioiminen on järkiperäisesti vaativaa, se voi olla uhka, joka on mahdollisesti vahingollinen tai epämiellyttävä toimi tai vaara, jota voidaan pitää potentiaalisena uhkana tietylle toimijalle. Kyberuhka rakentuu usein liioitellun uhkakuvan ympärille. Negatiivinen liioittelu tapahtuu monesti, kun uhkaa ei tunneta tai ymmärretä täysin. Tämän seurauksena onkin tärkeää lisätä ihmisten ymmärrystä tätä bittienmaailmaa kohtaan. (Limnéll ym., 2014, s. 106)

Uhka saadaan torjuttua estämällä mahdollisesti haitallisen uhkan toteutuminen. Ennaltaehkäisyllä on suuri merkitys uhkiin ja niiden muodostumiseen. Mitä aikaisemmin kehityskulkuun pystytään vaikuttamaan, sitä pienemmillä resursseilla se pystytään torjumaan. Kyberuhkiin voidaan vaikuttaa myös fyysisen maailman resursseilla, kuten taloudellisella tai poliittisella vaikutusvallalla. Vaikka uhka on torjuttu se ei tarkoita, että kaikilta sen haitallisilta vaikutuksilta pystyttäisiin välttymään, torjuntatoimenpiteet voivat aiheuttaa myös negatiivisia sivuvaikutuksia. Mutta sen pahimmat vaikutukset pystyttiin torjumaan. Kaikkia fyysisen eikä kybermaailman uhkia voida torjua eikä täydellistä kyberturvallisuutta ole olemassa. (Limnéll ym., 2014, s. 106)

Uhkien vaikutuksilta suojautuminen ja niihin varautuminen on tärkeää. Parhaiten kyberuhkilta suojaudutaan järjestämällä kyberturvallisuuden perusasiat kuntoon, kasvattamalla kaikkien tietoisuutta ja toimintakykyä sekä ylläpitämällä tietoturvaa. Kyberturvallisuuden haasteet tulee tunnistaa ja niihin pitää reagoida. Nämä keinot ovat ainut tapa suojautua

tunnistamattomalta kyberuhkalta. Tunnistamatonta kyberuhkaa kutsutaan myös nimellä ”musta joutsen”. Kybermaailma kehittyy ja muuttuu jatkuvasti, jonka seurauksena tilanteen tasalla pysyminen on mahdotonta. (Limnéll ym., 2014, s. 107)

Kyberhyökkäyksen kohdistuessa organisaatioon, oleellinen tavoite on toimintakyvyn ylläpitäminen, hyökkäyksen mahdollisimman pikainen keskeyttäminen ja toimintojen palauttaminen normaalitilaan. Suojautuessa kyberhyökkäykseltä on myös mahdollista ryhtyä moninaisiin offensiivisiin vastatoimenpiteisiin. (Limnéll ym., 2014, s. 107)

Kyberuhkat voivat olla joko organisaation sisäisiä tai ulkopuolisia. Sisäiset uhkat ovat keskeisiä tietopääoman, talouden ja maineen perustalta. Sisäisissä uhkissa lähteinä ovat pääasiassa tyytymättömät entiset tai nykyiset työntekijät tai tyytymättömät alihankkijat ja kumppanit. Sisäisen uhkan aiheuttajalla ei tarvitse olla syvällistä osaamista tunkeutumisesta tietojärjestelmiin, -koneisiin tai -verkkoihin, sillä tyypillisesti uhkan aiheuttajalla on riittävät käyttöoikeudet tai heillä on mahdollisuus hankkia sellaiset, varastaakseen tietoa tai vahingoittaakseen toimijaa. Tällöin tietoturva ei pysty tunnistamaan toimia hyökkäykseksi vaan tavalliseksi resurssienkäytöksi. Sisäinen uhka tarkoittaa myös työntekijöitä, jotka tietämättään tuovat haittaohjelman organisaation järjestelmään. (Limnéll ym., 2014, s. 107).

Voimassa olevien kyberuhkien osalta hyökkäysten raportointi on erittäin tärkeää. Monet eri toimijat keräävät onnistuneista kyberhyökkäyksistä tietoa ja kokoavat tutkimustiedon yhteen ja analysoivat sen sekä jakavat tutkimustulokset julkisesti eteenpäin. Tällä kasvatetaan tietoisuutta uhkista ja lisätään niiden tunnettavuutta, jolloin odottamattomilta uhkilta vältytään. Organisaatioiden tulisi hyödyntää avointa tietoa ja käyttää sitä riskiarvioinneissa ja ottaa riskienhallinnassa huomioon tunnistetut kyberuhkat. On myös tärkeää jakaa avoimesti tietoa ja raportteja onnistuneista kyberuhkien torjunnoista sekä menestyksekkäästä toiminnan palauttamisesta. (Limnéll ym., 2014, s. 107)

3.4 ATTAT-Kaava

Fyysisen maailman lainalaisuudet muuttuvat astuessamme kybermaailmaan. Tässä bittien maailmassa selviytyäkseen on välttämätöntä ymmärtää nämä eroavaisuudet pystyäkseen tehokkaasti hyödyntämään kybermaailman tuomia mahdollisuuksia. Lainalaisuudet ovat tiivistettävissä viiteen osa-alueeseen: Aika, tila, tunnistamattomuus, asymmetrisyys ja tehokkuus. Näistä viidestä osa-alueesta koostuu ATTAT-kaava, joka vaikuttaa turvallisuuden todellisuuteen sekä turvallisuuskokemukseemme. ATTAT-kaavan huomiotta jättäminen voi johtaa epäonnistumiseen ja strategisen edun menettämiseen. Tämä kaava käsittää avaintekijät, jotka ovat välttämättömiä tehokkaalle ja menestyksekkäälle toiminnalle kybermaailmassa. (Limnéll ym., 2014, s. 63)

Kybermaailma on erittäin dynaaminen ympäristö, jossa useat lainalaisuudet ovat hyvin erilaisia suhteessa fyysiseen maailmaan. Kybermaailmassa menestyäkseen on hyödynnettävä dynaamisia keinoja ja toteutettava moderneja turvallisuusratkaisuja. Tietojärjestelmien haavoittuvuudet eivät oikeuta kyberhyökkäyksiin, mutta tekevät niistä houkuttavampia kohteita. (Limnéll ym., 2014, s. 63)

3.4.1 Aika, tila ja tunnistamattomuus

Yksi inhimillisen elämän keskeisiä osia on aika. Fyysisessä maailmassa kaikki toiminta vie aikaa tai niille on aikansa. Toiminnan valmistelu ja toteuttaminen pystytään havaitsemaan etukäteen myös ulkopuolelta. Esimerkiksi sotilaallinen hyökkäys ohjuksilla, vaikka ohjukset ovat nopeita, ei hyökkäys koskaan ole täysin välitön. Ohjuksella on lentoaikansa ennen kuin se tavoittaa kohteensa. Nykyteknologialla pystytään jäljittämään ohjusten laukaisupaikka, joka antaa aikaa tehdä vastatoimia. (Limnéll ym., 2014, s. 63-64)

Fyysisen ja kybermaailman aika käsitys poikkeaa merkittävästi toisistaan. Tässä bittien maailmassa asiat tapahtuvat välittömästi ilman ennakkovaroitusta. Hyvin valmisteltu kyberhyökkäys voidaan toteuttaa lähestulkoon välittömästi. Ajallisesti tarkasteltuna sijainnilla ei ole merkitystä, hyökkäyksen voi laukaista viereisestä korttelista tai vaikka toiselta puolelta maailmaa. Ajan merkitys heikkenee, mutta toisaalta aika myös pitenee. (Limnéll ym., 2014, s. 64)

Tietojärjestelmässä uinunut haittaohjelma voi olla horrostilassa jopa vuosia ja odottaa laukaisevaa tekijää tai käskyä. Jotta järjestelmään päästään tunkeutumaan, se voi vaatia paljon aikaa ja valtavasti resursseja, usein myös riittävän päättäväinen taho siinä onnistuu. (Limnéll ym., 2014, s. 64)

Tila ja aika kietoutuvat kybermaailman lainalaisuuksissa hyvin läheisesti yhteen. Maantieteen vuoksi fyysinen kaupankäynti, liikkuminen ja voimankäyttö ovat rajoitettuja verrattaessa kybermaailmaan, jossa kuka tahansa voi kommunikoida kellonajasta riippumatta kenen tai minkä tahansa kohteen kanssa. Kybermaailmassa etäisyydet häviävät eikä käyttäjien välisellä matkalla ole merkitystä. Työntekijöiden ei tarvitse olla työpaikalla käyttääkseen työpaikan resursseja, virtuaaliteknologia ratkaisut mahdollistavat samojen resurssien käytön paikasta riippumatta. (Limnéll ym., 2014, s. 65)

Kybermaailma on myös keinotekoinen tila, jota pystytään muokkaamaan turvallisuuden ja vaatimusten mukaiseksi. Bittien maailmalla on pysyväisluonteinen arkkitehtuuri ja valtaosa sen rakennetuista kerroksista on jollakin tasolla muokattavissa. Kybertila muuttuu ennakoimattomasti jatkuvien teknologiapäivitysten ja verkostojen muutosten takia, joka mahdollistaa kybertilan muokkaamisen pitkäjänteisesti tavoiteltuun suuntaan. Tämä

muutos vaatii taustalleen kybertilassa vaikuttavien kansainvälisten tahojen välisiä sopimuksia. (Limnéll ym., 2014, s. 65-66)

Kybertilassa tehdyt toimet voivat ilmetä usein yllättävissä kohteissa ja toimien syntyperää on lähes mahdotonta todeta. Kyberhyökkäys yritystä kohtaan voidaan toteuttaa mistä vain ajallisesti ja maantieteellisesti rajattomassa digitaalisessa maailmassa. Yksikin henkilö voi toteuttaa kyberhyökkäyksen, jos hänellä on riittävästi motivaatiota, osaamista ja aikaa. (Limnéll ym., 2014, s. 66)

Fyysisen ja kyberulottuvuuden tunnistamislogiikat eroavat toisistaan. Tunnistaminen voidaan määritellä identiteetin tai sijainnin osoittamiseksi. Kybermaailmassa toimijan tunnistaminen on haastavaa ja siksi kyberrikoksia tapahtuu tänä päivänä paljon. Kybermaailmassa rikoksesta kiinni jääminen on pieni varsinkin, jos osaat peitellä toimintaasi. Tunnistamista vaikeuttaa se, että vaikka toimijan sijainti voitaisiin määritellä, ei pystyttäisi todentamaan, että kuka yhteyttä todellisuudessa käyttää. Toimija pyrkii pysyttelemään tunnistamattomana silloin kun se tukee hänen tavoitteitaan. (Limnéll ym., 2014, s. 67)

Kybermaailma mahdollistaa lukuisat identiteetit ja tunnistamattomana toimimisen. Toimija voidaan tunnistaa varmasti vain hänen omasta ilmoittautumisestaan. Tunnistamattomuus heikentää myös kykyä vastatoimintaan, vastatoimen kohdistaminen väärään kohteeseen voi tuottaa uuden pahantahtoisen toimijan sekä heikentää pelotteen logiikkaa. Tunnistamattomuuteen kuulu myös, että eri toimijoiden kyberkyvykkyyksiä on erittäin vaikea havainnoida. (Limnéll ym., 2014, s. 67)

3.4.2 Asymmetrisyys

Alkuperältään asymmetria käsite on hyvin vanha, asymmetriassa toimijoiden relatiivinen voima, strategia ja taktiikka poikkeavat toisistaan huomattavasti. Se on jotakin, mitä voimasuhteiltaan runsaasti heikompi hyödyntää suhteessa vahvempaan. (Limnéll ym., 2014, s. 68)

Kybermaailma mahdollistaa uusia tapoja asymmetriselle toiminnalle. Vaikka kyberoperaation toteuttamistapa olisi symmetrinen ovat operaatiot luonteeltaan asymmetrisiä. Kyberavaruudessa asiantuntijuus ja osaaminen ovat ihmisten tai laitteiden määrää merkityksellisempiä. Kybertoimet ovat asymmetrisiä, koska muutama toimija voi käyttää niitä lukuisia vastaan ilman että heillä olisi käytössään suuria määriä resursseja, jonka seurauksena esteet fyysiseen maailmaan verrattuna ovat vähäiset. (Limnéll ym., 2014, s. 68)

Hyökkääjällä on etu suhteessa puolustajaan, joka korostaa asymmetrisyyttä kybermaailmassa. Fyysisen maailman sodan käynnissä käytetään usein periaatetta, että hyökkääjällä tulisi olla ainakin kolminkertainen ylivoima suhteessa puolustajaan ja jokainen onnistunut tai epäonnistunut

hyökkäys kuluttaisi resursseja. Kybermaailmassa tämä periaate ei päde, kyberhyökkäyksiä voidaan toteuttaa lukemattomia kertoja ilman että se kuluttaisi hyökkääjän resursseja. Hyökkäystä voidaan kutsua menestyksekkääksi, jos yksikin miljoonista tunkeutumisyrityksestä onnistuu. Puolustajalle tämä hyökkäys on asymmetrinen haaste, jossa on kyse haavoittuvuuksista. (Limnéll ym., 2014, s. 69)

Tämä bittienmaailman asymmetrinen ja monimutkainen luonne vaikeuttaa voiton, häviön ja vahingon arvioimista. Toimijoiden tapa laskea menestystä tai häviötä ei ole yhteismitallinen, vaan jokainen toimija mittaa tulosta omalla mittapuullaan. Välittömien kustannusten tai voittojen ohella täytyy huomioida epäsuorat ja kerrannaisvaikutukset, näiden tunnistaminen ja arvon laskeminen on vaativaa. Investointeja kybertuvallisuuteen vältellään usein suurien kustannusten vuoksi, vaikka näitä kustannuksia ei todennäköisesti koskaan voida verrata niihin taloudellisiin, maineenhallinallisiin tai toiminta kyvyllisiin vahinkoihin, joita voi seurata korjaamattomista haavoittuvuuksista. Haavoittuvuuksia hyödyntävä haittaohjelma on käyttökelpoinen vain niin kauan kuin kohteen heikkous on korjattu, korjauksen seurauksena siitä tulee käyttökelvoton. (Limnéll ym., 2014, s. 69)

3.4.3 Tehokkuus

Tehokkaalla kyberiskulla ei tarkoiteta koko internetin kaatamista, hyökkäyksen luonne voi olla tunkeutuminen suojaamattomaan järjestelmään ja verkostoihin, viestinnän tai kaupankäynnin häiritsemistä, tiedon manipuloimista ja elintärkeän infrastruktuurin sabotointia. Keskeisenä tekijänä tehokkuudelle on kyky tehdä useita asioita kerralla, samassa yhteydessä, eri ulottuvuuksissa ja silmänräpäyksessä. Yhteiskuntien verkostoituessa yhä pidemmälle, sitä merkittävämpää on suojella verkostoja ja niissä sijaitsevaa dataa ja tämän datan tuottamaa vaurautta. (Limnéll ym., 2014, s. 69-70)

Kenellä tahansa on mahdollisuus rakentaa kyberkyvykkyyttä ja teho on yksi vaikuttavammista lainalaisuuksista. Ei-valtiolliset toimijat voivat saada aikaan merkittäviä vaikutuksia muutamalla kyseenalaisella tavalla. Toimijat voivat kaupallistaa jalostamansa kyberkyvykkyydet ja valtiot sekä ei-valtiolliset tahot voivat käyttää näitä hyväkseen. Toimijat voivat myös liittoutua valtioiden kanssa, joka mahdollistaa toimijoiden pääsyn valtioiden kyberkykyihin, tällöin valtiolle jää mahdollisuus kieltää osallisuutensa kybertoimiin. Fyysisen maailman toimintatavat ovat yleisesti kankeampia kuin kybertoimet. Kybermaailmaa voidaan hyödyntää yhtäaikaisesti useisiin tarkoituksiin, esimerkiksi vakoiluun, elintärkeän suojaamiseen ja vahingoittamiseen, sekä propagandaan. Kyberavaruus mahdollistaa pääsyn paikkoihin, joita muuten olisi lähes mahdotonta tavoittaa. (Limnéll ym., 2014, s. 70)

Tehokkuutta voidaan hyödyntää myös hyväntahtoisessa toiminnassa. Tuotanto- ja palveluketjujen välivaiheita voidaan vähentää. Asiakkaille voidaan mahdollistaa myös pääsy tuotantoprosessin eri vaiheisiin. Suorituskyky paranee, kun ketjut lyhenevät ja niiden kautta tapahtuva prosessi nopeutuu. Yritysten perustaessa nettikauppoja kauppaa voidaan käydä kellon ympäri ei siis vain aukioloaikoina. Tämä vaikuttaa yritysten henkilöstö-, markkinointi ja kiinteistökuluihin. Kuluttajana tämä helpottaa ostovertailujen tekemistä ja hankintoja voidaan tehdä maailmanlaajuisesti ja useasta nettikaupasta yhtäaikaisesti. (Limnéll ym., 2014, s. 70)

Joukkoistaminen kuvastaa kybermaailman tehokkuutta parhaimmillaan. Joukkoistamista on työpanoksen tai rahoituksen keräämistä ihmisjoukolta, mikä tapahtuu yleensä internetin avustuksella. Rahoitus- työtehtävä delegoidaan ennalta määräämättömälle ryhmälle ihmisiä ja näiden ihmisten kokemus, ideat ja taito valjastetaan toimeksiannon toteuttamiseen. Lopputuotos syntyy vähäisin kustannuksin sekä toiminnan avoimuus turvaa paremman laadun ja innovatiivisuuden. Yritys voi halutessaan ulkoistaa jonkin tuotteensa ilmiasun suunnittelun kybermaailmaan. Kertomalla mitä haluaa, kustannus ehdot ja aikataulun. Lopputuloksena voi olla kymmeniä tai satoja valmiita ehdotuksia, joista yritys voi valita varteenotettavimman. Hyötyjä voidaan myös käyttää kriisitilanteissa, kun välittömiä yhteydenottoja ja sosiaaliseen mediaan lisättyjä silminnäkijätietoja koordinoidaan mahdollisimman laajan ja todellisen tilannekuvan hankkimiseksi. Silminnäkijä havainnot ja informaatio liikkuvat sosiaalisessa mediassa usein ripeämmin kuin yleisessä valtamediassa ja siksi se mahdollistaa ennakkovaroituksen. Tästä syystä mediatalot tarkkailevat sosiaalista mediaa ja ihmisten päivityksiä hyvin aktiivisesti. Tehokkuus on ilmiselvä seuraus kaikkien lainalaisuuksien synergiasta. (Limnéll ym., 2014, s. 69-70)

4 SUOJAUSSUUNNITELMA

Suunnitelmana on suojata Office 365 -pilvipalvelun identiteetit tietomurroilta, joita yritykset ovat kohdanneet lähivuosina. Rikolliset pyrkivät kalasteluviesteillään saaman käyttäjän salasanan, jonka jälkeen sähköpostitunnusta hyödynnetään muihin rikollisiin toimiin. Alla olevassa kuvassa 3 esitetään tietojenkalastelun eri vaiheet.

Kuva 3. Tietojenkalastelun vaiheet. (Tietoturvan vuosi 2018, 2018, s. 9.)

Office 365 -pilvipalvelun suojaustoimenpiteet toteutetaan ottamalla käyttöön monimenetelmäinen todentaminen ehdollisen pääsyn käytäntöjä hyödyntäen. Identiteettejä suojatessa otetaan myös huomioon tekniset haavoittuvuudet, joita rikolliset ovat hyödyntäneet ohittaessaan monimenetelmäisen todennuksen.

Monimenetelmäisen todentamisen haavoittuvuudet korjataan estämällä asiakassovellukset, jotka käyttävät POP-, IMAP- ja SMTP-protokollia sekä Exchange ActiveSyncia. Ehdollisen pääsyn käytännöt määritetään niin että käyttäjältä vaaditaan aina monimenetelmäinen todentaminen, kun laite ei ole yrityksen omassa lähiverkkoyhteydessä.

Azure Active Directory tallentaa myös sisäänkirjautumislokitiedot, joiden tarkastelu voi olla haastavaa, jos kirjautumistapahtumia on paljon. Helpottaaksemme lokitietojen käsittelyä, viedään tiedot Microsoftin Power BI -pilvisovellukseen, joka luo lokitiedoista visuaalisen ja selkeän raportin. Raportin pohjalta määritämme myös ehdon, jolla rajoitamme pilvipalveluun pääsyä eri maista tai maanosista.

5 AZURE ACTIVE DIRECTORY JA SUOJAUSTOIMET

Azure AD (Azure Active Directory) on Microsoftin pilvipohjainen pääsyn- ja identiteetinhallintapalvelu, jonka avulla käyttäjät voivat kirjautua Office 365-palveluun ja käyttää sen resursseja. Azure AD -pilvipalvelu on tarkoitettu IT-järjestelmävalvojien käyttöön, IT-järjestelmävalvojat voivat pilvipalvelun avulla säädellä sovellusten ja sovellusresurssien käyttöä. (Microsoft, 2019a)

Azure AD -pilvipalvelu mahdollistaa myös identiteettien suojaamisen tavoilla, jotka soveltuvat pilvipalveluympäristöön. Suojaamiskeinot, joita käytetään tässä työssä ovat monimenetelmäinen todentaminen, ehdollisen pääsyn käytännöt sekä salasanakäytännöt.

5.1 Azure AD -ryhmät

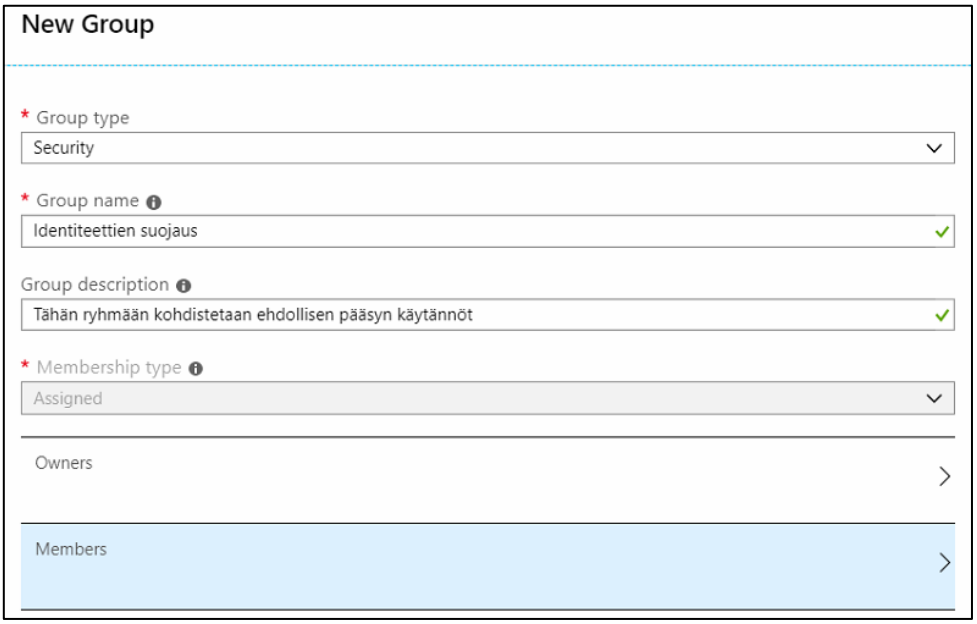
Azure AD -pilvipalveluun voi määrittää Security sekä Office 365 -ryhmiä. Office 365-ryhmien tarkoitus on luoda työtiloja käyttäjille, jossa voidaan jakaa resursseja, pitää kokouksia ja lähettää sähköpostia. Taulukossa 2 esitetään Office 365-ryhmän maksimirajoitukset.

Taulukko 2. Office 365 -ryhmärajoitukset. (Microsoft, 2019c)

Kuvaus	Maksimi määrä
Omistajia per ryhmä	100
Ryhmiä, joita käyttäjä voi luoda	250
Ryhmiä, joita pääkäyttäjä voi luoda	500 000
Ryhmän jäsenmäärä	Yli 1000 vaikka vain 1000 voi ryhmä keskustella samanaikaisesti
Tiedostojen tallennus	1 teratavu + 10 gigatavua tilattua käyttäjää kohden ja kaikki ostetut lisätallennustilat.
Ryhmä sähköpostin koko	50GB

Security-ryhmiä käytetään, kun kohdistetaan ehtoja ja sääntöjä käyttäjiin. Ehdollisen pääsyn käytännöt tulevat pakolliseksi kaikille yrityksen Office 365 -identiteeteille, joten tätä varten luodaan vain yksi Security-ryhmän.

Ryhmälle on määritettävä tyyppi, nimi, jäsenyystyyppi, omistajat ja jäsenet (Kuva 4). Jäsenyyden tyypiksi valitaan osoitettu (Assigned), jolloin ryhmään täytyy lisätä käyttäjät manuaalisesti.



Kuva 4. Uuden ryhmän luominen.

Jäsenyyden tyypiksi voidaan valita myös dynaaminen käyttäjä tai laite, jolloin ryhmään luodaan sääntö, jonka perusteella käyttäjät automaattisesti liittyvät ryhmien jäseniksi. Tässä opinnäytetyössä ei hyödynnetä dynaamisia ryhmiä.

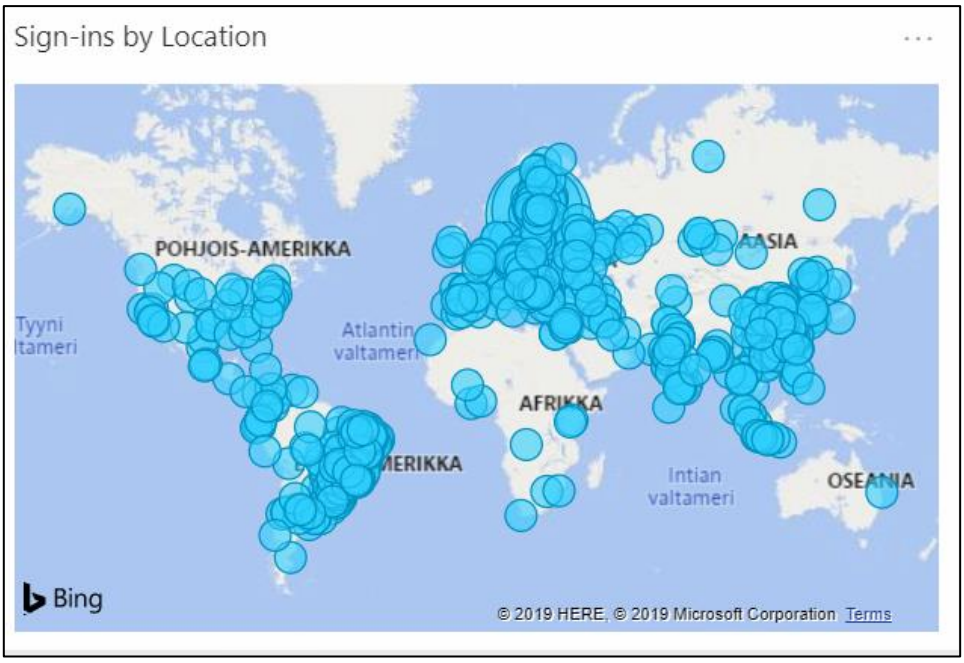
5.2 Sisäänkirjautumislokien valvonta Azure AD -pilvipalvelussa

Azure AD -pilvipalvelussa voidaan tarkastella sisäänkirjautumislokitietoja organisaatio tai käyttäjä kohtaisesti. Kirjautumislokiin jää useita tunnistetietoja, päivämäärä, kellonaika, käyttäjätunnus, sovellus, kirjautumisen status sekä sijainti. Usein jo pelkän sijainnin perusteella voidaan päätellä, että onko käyttäjätilille kirjautuja itse käyttäjä vai jokin ulkopuolinen toimija. Azure AD -pilvipalvelusta voidaan ladata halutulta aikaväliltä lokitiedostot CSV tai JSON muodossa. Taulukossa 3 on esimerkki Exceliin tuoduista lokitiedoista, taulukkoon on valittu kaikki epäonnistuneet sisäänkirjautumiset. Taulukossa 3 olevat käyttäjänimet ja sähköpostiosoitteet ovat poistettu tarkoituksenmukaisesti.

Taulukko 3. AAD-kirjautumislokitiedostot.

Date (UTC)	User	Username	Location	Status
31.5.2019 14:33	Käyttäjänimi	Sähköpostiosoite	Warrenton, Missouri, US	Failure
31.5.2019 14:24	Käyttäjänimi	Sähköpostiosoite	Villa Constitucion, Santa Fe, AR	Failure
31.5.2019 14:04	Käyttäjänimi	Sähköpostiosoite	Simferopol, Krym Avto-nomna Respublika, UA	Failure

Azure ADsta voidaan viedä valmiita raportteja myös Microsoftin Power BI-sovellukseen. Ottamalla käyttöön Azure Active Directory Logs -sovellus, voidaan helposti hakea kaikki kirjautumislokitiedot portaalista. Power BI-raportti on visuaalisesti selkeä ja helppo tulkita. Alla olevassa kuvassa 6 on sijaintiin perustuva Power BI-raportti, johon on valittu vain epäonnistuneet sisäänkirjautumiset.



Kuva 5. Valmis raporttipohja Azure ADsta Power BI-pilvisovellukseen.

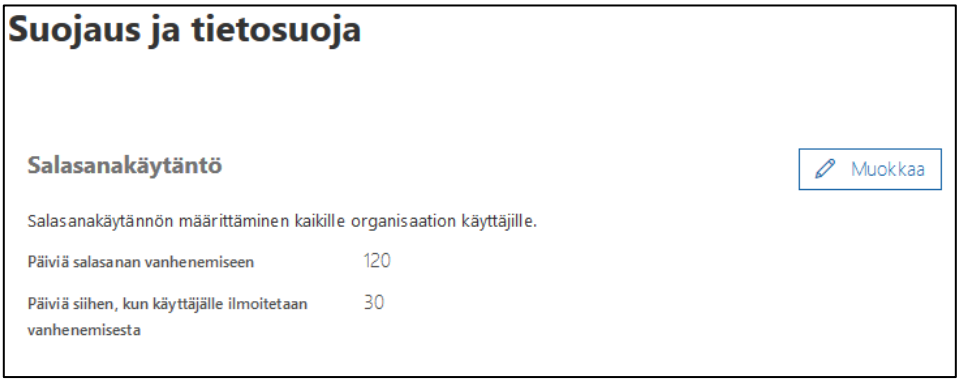
Kuvan 5 Power BI-raportti kertoo karun totuuden väsytyshyökkäysten määrästä ja laajuudesta. Raportista selviää myös, että hyökkäyksiä tehdään lähes 800 kertaa yhden vuorokauden aikana. Hyökkäys on hajautettu, joka tarkoittaa sitä, että toimijalla on käytössään useita eri IP-osoitteita ja he tekevät maksimissaan 3 hyökkäystä per IP-osoite. Tämä hankaloittaa omalta osaltaan hyökkäysten hidastamista.

Väsytyshyökkäyksessä (Brute-force attack) rikollinen toimija pyrkii arvaamaan käyttäjätunnuksen salasanan. Tämä hyökkäys toimii parhaiten, kun toimija saa arvata salasanoja ilman keskeytyksiä. Azure ADsta ei löydy

ominaisuutta, jolla voisi estää väsytyshyökkäykset, mutta keinoja, jolla sitä voidaan hidastaa.

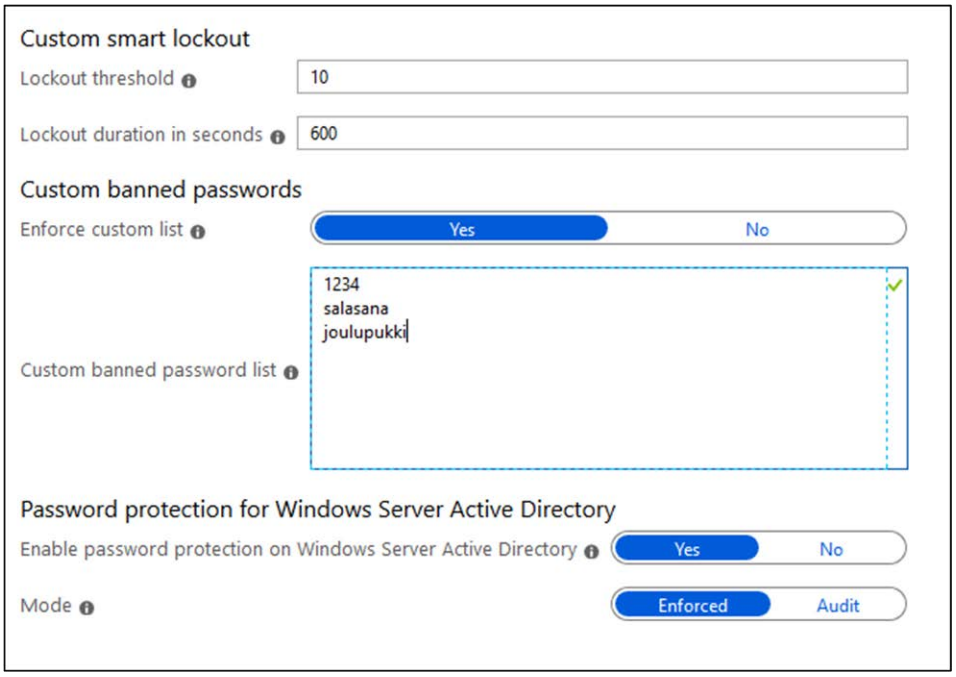
5.3 Salasanakäytännöt

Identiteeteille voidaan määrittää myös salasanan vanhenemispäivä, jonka jälkeen käyttäjän on pakko vaihtaa salasanansa. Asetuksista määritetään, kuinka monta päivää salasana on voimassa ja milloin käyttäjä saa ilmoituksen vanhenevasta salasanasta. pilvipalvelussa tehty salasanan vanhenemiskäytäntö vaikuttaa suoraan kaikkiin käyttäjiin. Kuvassa 6 on valikko, josta asetuksia määritetään.



Kuva 6. Office 365 salasanakäytäntö.

Azure AD -pilvipalvelun todennusmenetelmissä voidaan määrittää myös salasanakäytäntöjä. Salasanakäytännöissä (kuva 8.) voidaan asettaa epäonnistuneiden sisäänkirjautumisen maksimimäärä, jonka jälkeen tili lukitaan halutuksi ajaksi. Kuvassa 8 epäonnistuneita sisäänkirjautumisia sallitaan 10 kappaletta, jonka jälkeen tili lukittautuu 600 sekunnin ajaksi. Tämä on myös keino hidastaa käyttäjätileihin kohdistuvaa väsytyshyökkäystä.

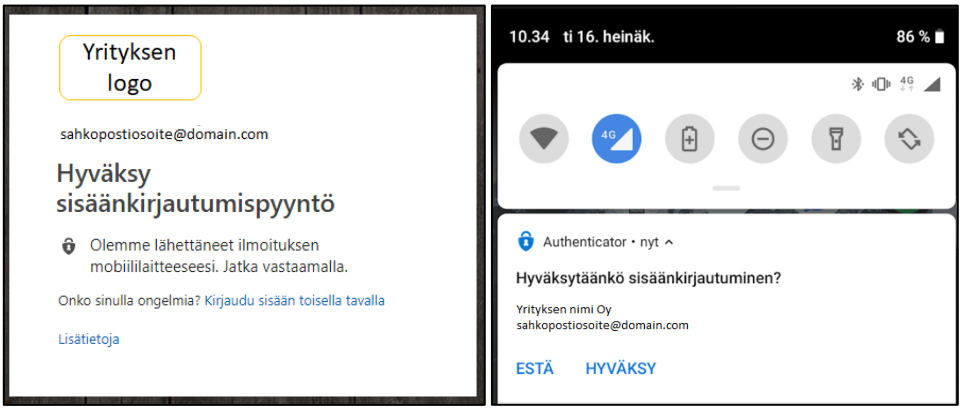


Kuva 7. Azure AD-todennusmenetelmät.

Salasanakäytännöissä voidaan myös hallita tai estää tunnettuja ja heikkoja salasanoja. Jos tilaksi on valittu pakotettu (Enforced) käyttäjä saa ilmoituksen estetystä salasanasta eikä pysty määrittämään tätä salasanaa Office 365-tililleen. Estetyt salasanat voidaan myös määrittää tarkkailutilaan (Audit), jolloin käyttäjä voi määrittää itselleen estetyn salasanan ja tästä jää tieto Azure AD-portaalin lokitietoihin. Salasanojen estolistaan voi lisätä maksimissaan 1000 sanaa.

5.4 Multifactor authentication (MFA)

Monimenetelmäinen todentaminen (MFA) on keino suojata Office 365-Identiteettejä. Palveluun kirjautuessa käyttäjältä vaaditaan vielä toinen todentamismenetelmä. Jolloin käyttäjä saa kertakäyttökoodin tekstiviestinä tai puhelin soittona. Käyttäjät voivat myös ottaa käyttöönsä Authenticator -mobiilisovelluksen, jolla kirjautumisvahvistuksia voidaan hyväksyä tai hylätä. Authenticator -mobiilisovellus nopeuttaa vahvistuspyyntöjen hyväksymistä, kuvassa 9 Office 365-palvelu vaatii kirjautumisen vahvistamista jonka seurauksena käyttäjä saa ilmoituksen siitä mobiilisovellukseensa.



Kuva 8. Kuvassa vasemmalla on MFA vahvistuspyyntö ja oikealla ilmoitus pyynnöstä Authenticator -mobiilisovelluksessa

MFA käyttöönotto vaatii käyttäjältä yhteystiedot, joita voivat olla puhelinnumero, vaihtoehtoinen puhelinnumero, sähköpostiosoite ja vaihtoehtoinen sähköpostiosoite. Jos käyttäjällä ei ole määritettynä autentikointiyhteystietoa, kysytään tiedot käyttäjältä, kun tilille kirjaudutaan ensimmäisen kerran.

6 EHDOLLISEN PÄÄSYN KÄYTÄNNÖT PARANTAVAT TIETOTURVAA

Ehdollisen pääsyn käytännöt (Conditional Access) ovat Azure AD -pilvipalvelusta löytyvä ominaisuus, jolla voidaan parantaa identiteettien tietoturvaa. Pilvipalvelussa luodut ehdot voidaan kohdistaa ryhmä tai käyttäjä kohtaisesti. Ehdon perusteella pilvipalvelu tekee automaattisia pääsynhallintapäätöksiä, päätökset voivat olla esimerkiksi palveluun sisäänkirjautumisen estäminen tai pääsynvalvonta voi vaatia käyttäjältä monimenetelmäistä tunnistautumista. (Microsoft, 2019b)

Ehtoon määritetään toimeksianto, edellytykset ja pääsynhallintakäytännöt. Toimeksianto käytäntöön valitaan käyttäjät tai ryhmä, johon käytäntö kohdistetaan sekä Office 365-pilvisovellukset, joihin halutaan vaikuttaa. Edellytykset määrittävät milloin ehto astuu voimaan, näitä voivat olla sijainti, sovellusalusta tai asiakassovellus. Pääsynhallinnasta voidaan joko estää kirjautuminen tai esimerkiksi vaatia käyttäjältä monimenetelmäistä todentamista.

Ehdollisen pääsyn käytännöt aktivoituvat, kun ensimmäisen tekijän todennus on suoritettu loppuun. Alla oleva taulukko 3 havainnollistaa ehdollisen pääsyn käyttötapauksen, jossa jokin toimija pyrkii kirjautumaan Intiasta käsin yrityksen Office 365 Sharepoint-pilvipalveluun käyttäen sovellusalustana androidia. Automaattinen pääsynvalvonta tarkastaa ehdot ja tekee päätöksen sen mukaisesti.

Taulukko 3. Ehdollisen pääsyn käytäntö

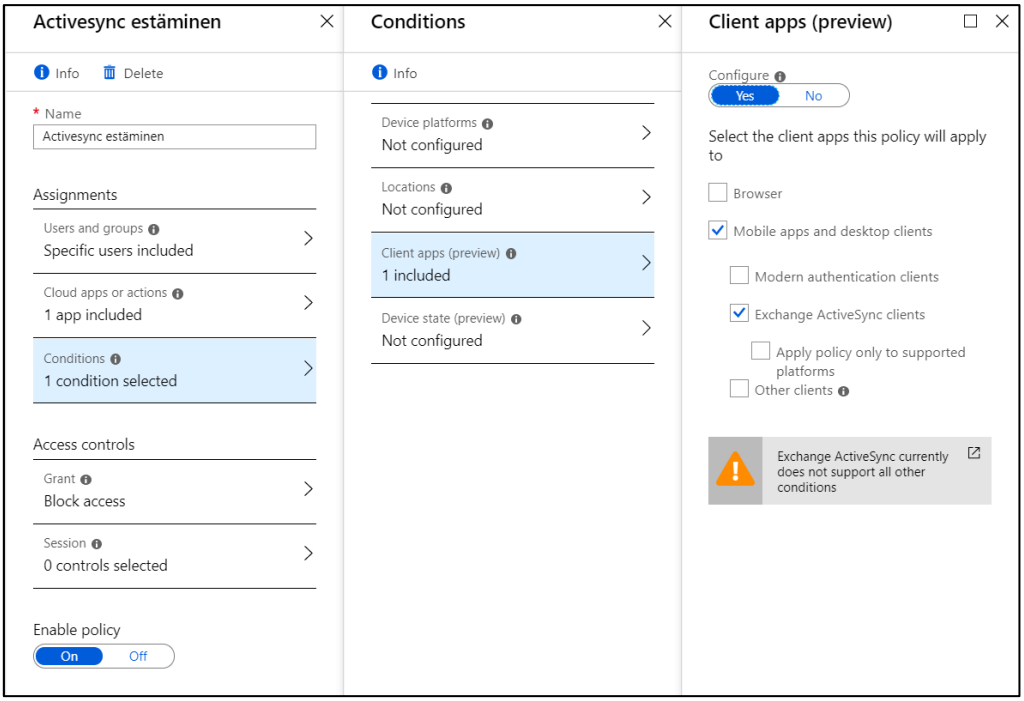
<table>
<tr><th>Kun tämä tapahtuu</th><th>Toimi näin</th></tr>
<tr><td>Pääsy yritys tehdään:
- Pilvisovellukseen Sharepoint
- Käyttäjäryhmästä Markkinointi</td><td rowspan="4">Estä sovellukseen pääsy</td></tr>
<tr><td>Toteutuneet ehdot</td></tr>
<tr><td>Ehto 1: Kirjautuminen maasta Intia</td></tr>
<tr><td>Ehto 2: Sovellusalusta Android</td></tr>
</table>

Ehdollisen pääsyn käytäntöjä ei ole tarkoitettu ensimmäiseksi rivisuojaukseksi, joka tarkoittaa, että sillä ei voida estää DOS-palvelunesto- tai väsytyshyökkäyksiä. (Microsoft, 2019b)

6.1 Legacy ja ActiveSync -asiakassovellusten estäminen

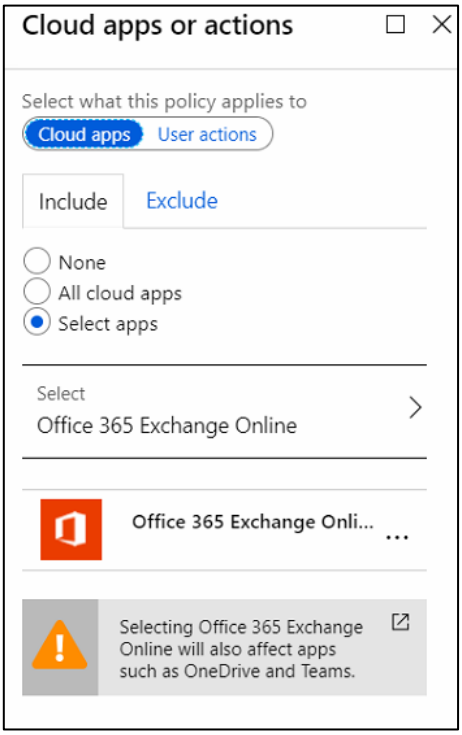
Jokaiselle ehdolle luodaan oma käytäntö ja nimetään käyttötarkoituksen mukaan, tämä helpottaa jatkossa käytäntöjen ylläpitoa ja mahdollista vian etsintää. Monimenetelmäisen todennuksen luotettavuuden osalta on

oleellista estää niin sanotut Legacy-asiakassovellukset, jotka käyttävät POP3, IMAP ja SMTP protokollaa, sekä Exchange ActiveSync-asiakassovellukset (kuva 9.). Ehdon astuessa voimaan käyttäjät voivat käyttää vain Microsoft Outlook-sähköpostiasiakassovellusta, joka tukee modernia-autentikointia.



Kuva 9. Ehdollisen pääsyn käytäntö, Exchange ActiveSync estäminen.

Toimeksianto kohdistetaan Office 365 Exchange Online -sovellukseen sekä aikaisemin luotuun Security-ryhmään, jolloin asetetut ehdot kohdistuvat vain ryhmään kuuluville käyttäjille. Toimeksianto voidaan kohdistaa myös suoraan kaikkiin yrityksen portaalissa oleviin käyttäjiin. Tämän ryhmän käyttäminen ei ole suositeltavaa, jos määritettyjä ehtoja ei ole testattu. Pahimmassa tapauksessa pääkäyttäjä voi estää kaikkien, tai jopa itsensä pääsyn pilvipalveluun, eikä ole varmaa saako palveluntarjoaja Microsoftkaan tätä ongelmaa ratkaistua.

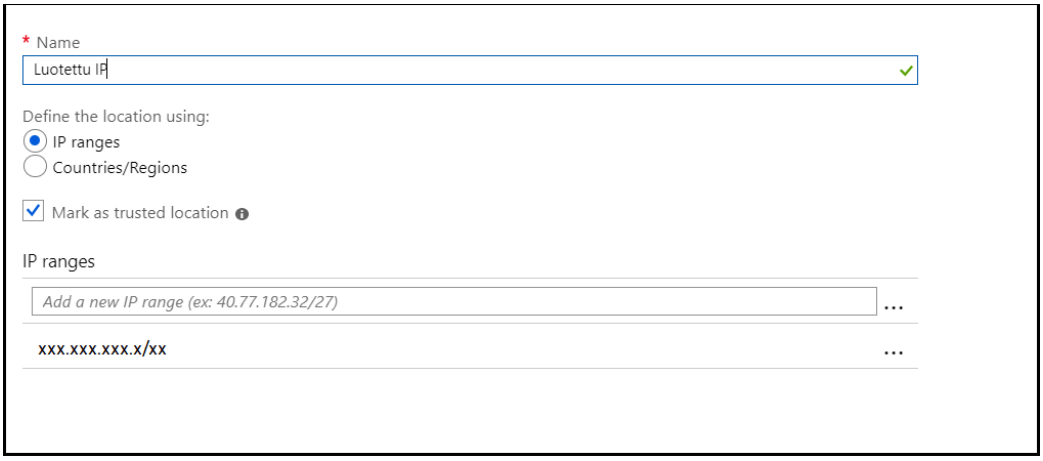


Kuva 10. Ehdon kohdistaminen sovellukseen.

Edellytyksiksi määritetään Exchange ActiveSync sekä POP, IMAP ja SMPT-protokollia käyttävät asiakassovellukset (Kuva 10.). Pääsynhallintakäytännöksi asetetaan pääsyn estäminen, jolloin kun edellytykset täyttyvät automaattinen pääsynhallinta estää sisäänkirjautumisen.

6.2 Sijaintiin perustuva ehto

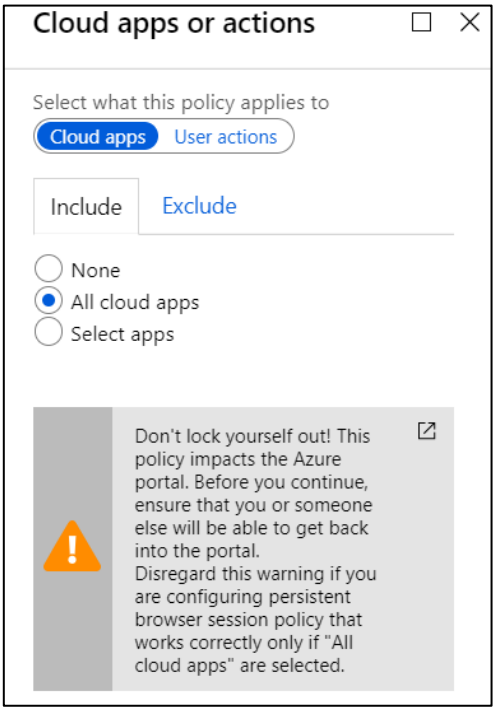
Pilvisovelluksiin pääsyä voidaan rajoittaa tai hallita myös sijainnin perusteella. Tässä luvussa määritetään ehto, jolla luokitellaan edellytykset, milloin käyttäjiltä vaaditaan monimenetelmäistä tunnistautumista. Esimerkissä yrityksellä on käytössään yksi toimipiste sekä staattinen julkinen IP-osoite, jota työntekijät käyttävät. Ensiksi määritetään luotettu sijainti, joka todennetaan yrityksen julkisella IP-osoitteella (kuva 11.).



Kuva 11. Luotetun sijainnin määritys.

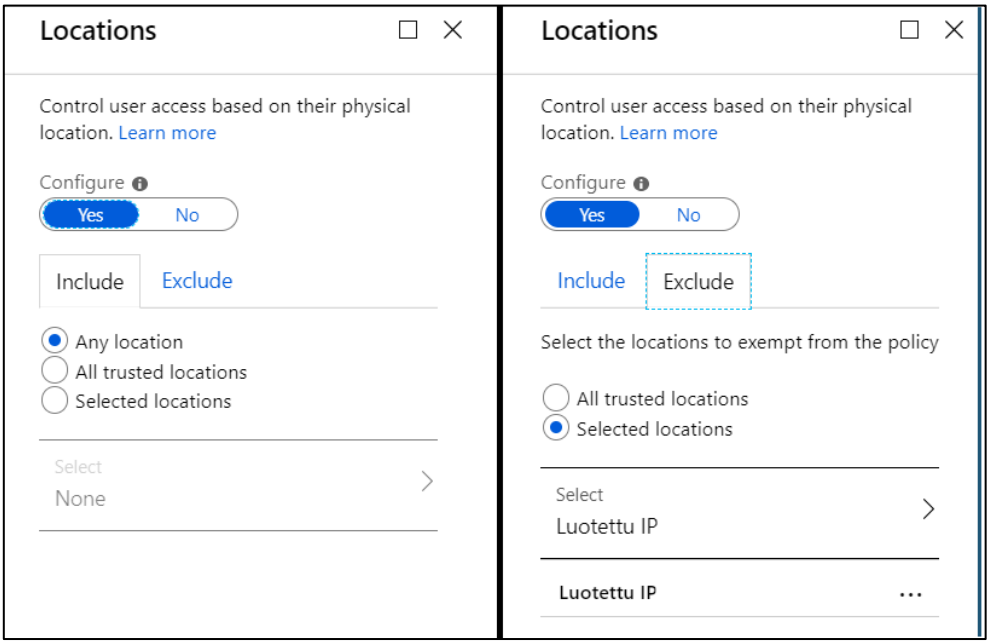
Luotettua sijaintia määrittäessä on tärkeää, että IP-alueet ovat yritykselle vakiintuneita ja luotettavia.

Toimeksianto määritetään samaan tapaan kuin Legacy ja ActiveSync ehdossa, paitsi että tässä tapauksessa kohdistus tehdään kaikkiin pilvisovelluksiin (Kuva 12.). Kun ehtoja kohdistetaan kaikkiin pilvisovelluksiin varoittaa palvelu mahdollisesta riskistä, jossa pääkäyttäjä voi sulkea itsensä ja kaikki yrityksen käyttäjät ulos kaikista pilvisovelluksista (kuva 13.).



Kuva 12. Toimeksiannon kohdistaminen kaikkiin pilvisovelluksiin.

Edellytykset ovat tässä ehdossa sijainti ja asiakassovellukset. Kuvassa 14 sijainti edellytys kohdistetaan kaikkiin sijainteihin pois lukien yrityksen IP-osoite. Asiakassovelluksiksi valitaan selain, mobiili- ja työpöytäsovellukset.



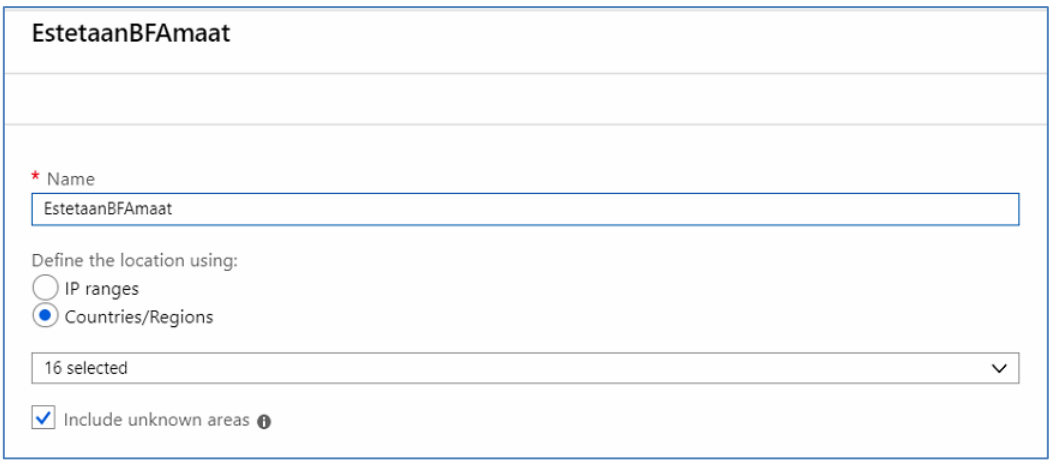
Kuva 13. Sijaintiin perustuva edellytys.

Pääsynhallintakäytäntönä vaaditaan monimenetelmäistä todennusta kaikista sijainneista pois lukien luotettusijainti. Jos todennus epäonnistuu, sisäänkirjautuminen hylätään.

6.2.1 Sisäänkirjautumisen estäminen maakohtaisesti

Vaikka Office 365 -pilvipalveluun vaaditaan monimenetelmäinen tunnistautuminen, on mahdollista, että käyttäjä erehdyksissään luovuttaa vahvistus pin-koodin tietojenkalastelusivustolle tai hyväksyy mobiilisovelluksesta tulleen kirjautumisilmoituksen. Vaikka rikollinen toimija olisi jo onnistunut murtautumaan käyttäjän Office 365-pilvipalveluun, voidaan pääsy pilvisovelluksiin vielä estää ehdollisen pääsyn käytännöllä.

Kuvassa 14 on valittu Power BI -raportin perusteella 16 maata sekä tunnistamattomat alueet, joista halutaan estää pääsy Office 365 -pilvipalveluun.



Kuva 14. Estettyjen maiden määrittäminen

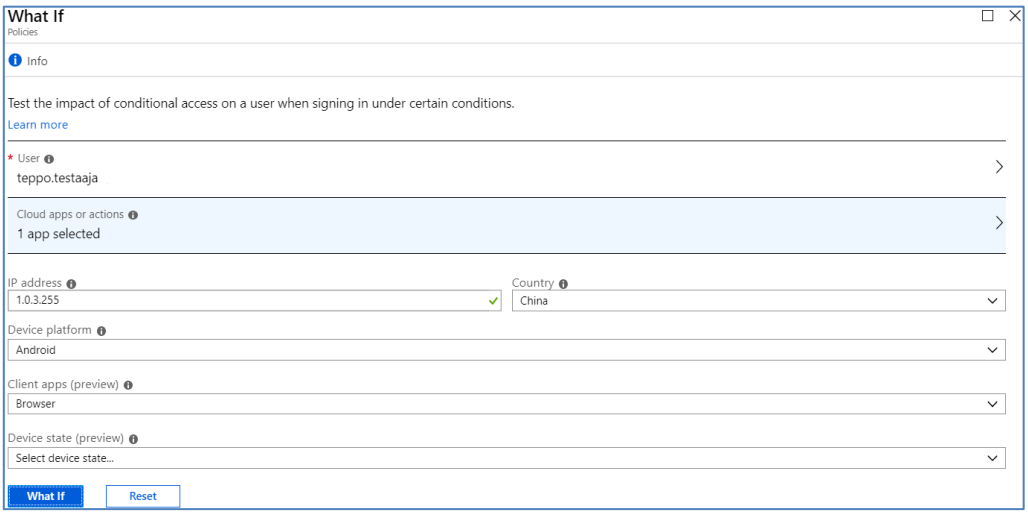
Sijaintiin perustuva ehto voidaan määrittää IP-alueittain tai maa kohtaisesti. Listalta löytyy 250 eri maata, ehtoon voidaan lisätä myös kohteet, joiden maata tai maanosaa ei voida vahvistaa. Tämä ehto estää pääsyn kaikkiin Office 365 -pilvisovelluksiin, joka tarkoittaa myös sitä, että käyttäjät, jotka matkustavat estettyihin maihin eivät voi käyttää yrityksen Office 365 -pilvipalvelua.

Kun estetystä sijainnista kirjaudutaan Office 365 -pilvipalveluun, käyttäjälle ilmoitetaan, ettei se täytä resurssin käyttöön vaadittuja ehtoja (kuva 15).

Kuva 15. Ilmoitus estetystä resurssien käytöstä.

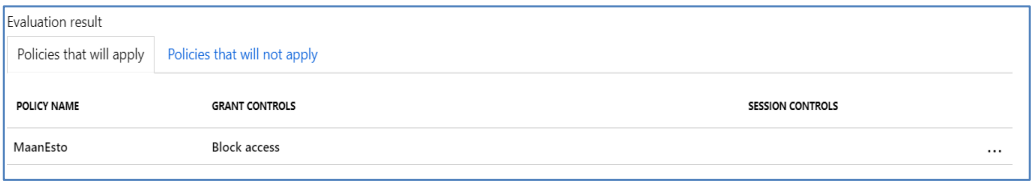
6.3 What If -toiminto

Ehdollisen pääsyn menetelmiä voidaan testata nopeasti What If -toiminnon avulla. What If -toiminolla voidaan testata kaiken tyyppisiä ehtoja, joita ehdollisen pääsyn käytännöissä pystytään määrittämään. Kuvassa 15 testataan aikaisemmin luotua sijaintiin perustuvaa ehtoa, jonka tarkoitus oli estää pilvipalveluun pääsy valituista maista. Testissä käytettiin käyttäjää, johon ehdollisen pääsyn käytäntö oli kohdistettu, sekä maa, joka on estettyjen sijaintien listalla.



Kuva 16. What If -toiminto, ehdon testaaminen.

Testituloksen mukaan ehto toimii odotetulla tavalla. (kuva 16.) What If -toiminnosta voidaan tarkistaa myös ehdot, jotka ovat kohdistettu testattavaan käyttäjään mutta eivät toteudu.



Kuva 17. Testin tulos.

7 YHTEENVETO

Opinnäytetyön tavoite oli vastata seuraaviin tutkintakysymyksiin: Mitä on kyberturvallisuus? Miten monimenetelmäinen todennus otetaan käyttöön? Miten, Office 365 -identiteetti voidaan suojata tietomurroilta?

Tutkintakysymykset muokkaantuivat työn edessä ja aihepiiri osoittautui erittäin laajaksi. Käytännön osaa työstäessäni tein vielä useita rajauksia aihealueeseen, koska muuten opinnäytetyö olisi kasvanut liian massiiviseksi. Tutkintakysymyksiin vastaaminen meni kokonaisuudessaan suunnitelman mukaan.

Teoriaosassa halusin käsitellä kyberturvallisuutta popularisoidulla tasolla, joka muutti myös omaa käsitystäni tästä bittien maailmasta ja sen luonteesta. Vaikka lähteiden määrä ei ole suuri, kybermaailma mahdollisti keinon tutustua kirjojen kirjoittajiin. Esimerkiksi Jarno Limnéll, joka on yksi Kyberturvallisuus -kirjan kirjoittajista. Hän on kyberturvallisuuden professori Aalto-yliopistossa sekä koulutukseltaan sotatieteiden tohtori. Jarno Limnéll kirjoittaa myös aktiivisesti Yhteiskunta -nimistä blogia iltalehden verkkopalvelussa.

Käytännön osa rakentui suojaussuunnitelman mukaisesti, eikä ongelmia määrityksen aikana tullut. Suojaussuunnitelmassa huomioitiin kyberturvallisuuskeskuksen ilmoittamat vaarat ja monimenetelmäisessä todennuksessa olevat haavoittuvuudet. Pilvipalveluiden suojaamiseksi ei riitä enää vahva salasana, koska rikolliset toimijat ovat onnistuneet luomaan erittäin luotettavan näköisiä tietojenkalastelusivustoja. Monimenetelmäinen todennus hyödyntäen ehdollisen pääsyn käytäntöjä suojaa Azure AD -identiteettiä vielä vaikka salasana olisi jo rikollisten hallussa.

Sijaintiin perustuvaa ehtoa en toteuttaisi enää samalla tavalla. Ehto hidastuttaa pilvipalvelun saatavuutta ja aiheuttaa turhautumista käyttäjissä. Ehdollisen pääsyn käytäntöihin voidaan määrittää myös ehto, joka vaatii monimenetelmäisen todennuksen vain laitteilta, jotka eivät ole luotettuja. Tämä on toimiva ratkaisu, jos käyttäjät käyttävät paljon muuta kuin yrityksen verkkoyhteyttä.

Opin työn aikana syventämään ymmärrystäni tieto- ja kyberturvallisuudesta, sekä suojaamaan Azure Active Directory -identiteetit tavoilla, jotka sopivat pilvipalveluympäristöön. Oman haasteensa käytännönosuudessa toi muutokset joita Microsoft teki pilvipalveluympäristöönsä. Näitä olivat käyttöliittymään tehdyt muutokset ja uudet ominaisuudet, joita palveluun ilmestyi lähes kuukausittain.

LÄHTEET

Seppälä, P. (2011). Uhka käsitteenä. Haettu 13.6.2019 osoitteesta: https://www.doria.fi/bitstream/handle/10024/74127/StratL3_16w.pdf?sequence=1

Eskola, S. (2008). Turvallisuus käsitteenä. Haettu 13.6.2019 osoitteesta: https://www.doria.fi/bitstream/handle/10024/74107/StratL3_10.pdf?sequence=1&isAllowed=y

Hakala, M. Vainio & M. Vuorinen O. (2006). *Tietoturvallisuuden käsikirja.* Jyväskylä: Docendo Finland Oy.

Hallikainen, A. (2017a). Saatavuus, eheys ja luottamuksellisuus ovat tietoturvan peruskäsitteitä. Helsingin kaupunki. Haettu 10.7.2019 osoitteesta: https://www.youtube.com/watch?v=Eg5Y7nq7vZg

Hallikainen, A. (2017b). Tietoturva työpisteellä: Todennus, kiistämättömyys ja vaatimustenmukaisuus. Helsingin kaupunki. Haettu 10.7.2019 osoitteesta: https://www.youtube.com/watch?v=p86s2Yvo5Tc

Karvi, T. (2012). Tietoturvan perusteet. Haettu 1.8.2019 osoitteesta: https://www.cs.helsinki.fi/u/karvi/perusteet-luku1-bea_12.pdf

Kyberturvallisuuskeskus. (2018). Varoitus Office 365 kohdistuneista hyökkäyksistä. Haettu 11.2.2019 osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota

Limnéll, J. Majewski, K. & Salminen, M. (2014). *Kyberturvallisuus.* Jyväskylä: Docendo Oy.

Limnéll, J. & Tuominen, T. (2014). Mitä on kyberturvallisuus ja miksi se koskettaa meitä jokaista?. Haettu 10.8.2019 osoitteesta: https://www.youtube.com/watch?v=qr6ZuuR_rPU&t=165s

Microsoft. (2019a). What is Azure Active Directory? Haettu 10.7.2019 osoitteesta: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

Microsoft. (2019b). What is Conditional Access? Haettu 13.8.2019 osoitteesta: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Microsoft. (2019c). Overview of Office 365 Groups for administrators. Haettu 12.8.2019 osoitteesta: https://docs.microsoft.com/en-us/office365/admin/create-groups/office-365-groups?view=o365-worldwide

Neptunet. (2013). Mitä ovat tietoturva-aukot. Haettu 12.8.2019 osoitteesta: https://neptunet.net/2013/05/27/30-3-2018mita-ovat-tietoturva-aukot/

Peltomäki, J. & Norppa, K. (2015). Rikos meni verkkoon. Helsinki: Talentum Media Oy ja tekijät

Puro, J. (2017). Mikä on tietoturvan ja kyberturvallisuuden ero?. Haettu 20.7.2019 osoitteesta: https://www.itewiki.fi/blog/2017/03/mika-on-tietoturvan-ja-kyberturvallisuuden-ero/

Rousku, K. (2014). *Kyberturvaopas. Tietoturvaa kotona ja työpaikalla.* Helsinki: Talentum Media Oy

Tietoturvan vuosi 2018. (2018). Haettu 5.3.2019 osoitteesta: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Vuosikatsaus_2018_tulostettava_sivuttain.pdf

Tsk. (2018). TEPA-termipankki. Haettu 10.7.2019 osoitteesta: http://www.tsk.fi/tepa/fi/haku/kyber-

virtual.vtt. (n.d.a). Mitä riskienhallinta on?. Haettu 8.10.2019 osoitteesta: http://virtual.vtt.fi/virtual/pkrh/startti-riskienhallintaan/mita-riskienhallinta-on.html

Virtual.vtt. (n.d.b). Mitä ovat riskit?. Haettu 8.10.2019 osoitteesta: http://virtual.vtt.fi/virtual/pkrh/startti-riskienhallintaan/mita-ovat-riskit/index.html