Johan Fabricius

# Identiteetin- ja pääsynhallinnan kehittäminen – case Veho

Opinnäytetyö

Tekniikan ylempi ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus

2024

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu


| | |
|---|---|
| Tutkintonimike | Insinööri (ylempi AMK) |
| Tekijä | Johan Fabricius |
| Työn nimi | Identiteetin- ja pääsyhallinnan kehittäminen – case Veho |
| Toimeksiantaja | Veho Oy Ab |
| Vuosi | 2024 |
| Sivut | 75 sivua, liitteitä 12 sivua |
| Työn ohjaaja | Vesa Kankare |


## TIIVISTELMÄ


Identiteetin- ja pääsynhallinnan rooli organisaatioiden kyberturvallisuuden toteuttamisessa on kasvanut vuosi vuodelta. Siitä on tullut entistä tärkeämpi osa organisaatioiden suojautuessa uusia uhkia vastaan. Samalla erilaisten järjestelmien määrä organisaatioissa on kasvanut hurjasti, ja näihin liittyvä identiteetin- ja pääsynhallinta on monimutkaistunut. Aiemmin voitiin myös ajatella sisäverkon olevan muuri, jonka sisäpuolella kaikki on turvassa. Työn tekemisen siirtyessä enemmän sisäverkon ulkopuolelle on ollut pakko alkaa ajatella toisin.

Työn tavoitteena oli tarkastella, minkälaisia lakeja, asetuksia, standardeja ja parhaita käytäntöjä liittyy organisaation identiteetin- ja pääsynhallinnan toteuttamiseen, ja miten nykytila vastaa näihin vaatimuksiin. Uusia lakeja ja asetuksia on tullut kohtuullisen paljon lyhyessä ajassa, uusimpana näistä loppuvuodesta 2024 voimaan astuva NIS2 sekä siihen liittyvä kansallinen lainsäädäntö. Toisena tärkeänä kohteena työssä oli tutkia, minkälaisia uhkia sekä riskejä huonosti hoidetusta identiteetin- ja pääsynhallinnasta voi organisaatiolle aiheutua, ja miten näitä uhkia voitaisiin torjua sekä riskejä minimoida. Pahimmillaan näiden uhkien ja riskien toteutuminen voi aiheuttaa liiketoiminnan loppumisen.

Tutkimusmenetelmäksi valittiin tutkimuksellinen kehittämistutkimus. Tutkimuskysymysten kautta haettiin vastauksia parhaisiin käytäntöihin, uhkiin, lakien ja asetusten vaatimuksiin sekä siihen, minkälaisia kehitystoimenpiteitä tulisi tehdä, jotta näihin vaatimuksiin pystyttäisiin vastaamaan. Kysymyksiin saatujen vastausten kautta pystyttiin hahmottamaan nykytilan haasteet ja luomaan alustavat raamit suuremmalle kehitystyölle.

Työssä saatiin tuloksena tietoa nykytilasta ja sen vaatimuksiin vastaavuudesta sekä määritettyä toimenpiteitä, jotka toteuttamalla saadaan vietyä identiteetin- ja pääsyhallintaa organisaatiossa uudelle tasolle. Lopputuotoksena luotiin kaksi taulukkoa, joiden avulla organisaatiot voivat arvioida oman ympäristönsä nykytilaa verrattuna tämän hetken parhaisiin käytäntöihin sekä NIS2-vaatimuksiin identiteetin- ja pääsynhallinnan osalta.



**Asiasanat:** identiteetti, lait, asetukset (säädökset), kyberturvallisuus

South-Eastern Finland University of Applied Sciences

| | |
|---|---|
| Degree | Master of Engineering |
| Author | Johan Fabricius |
| Thesis title | Development of Identity and access management development – case Veho |
| Commissioned by | Veho Oy Ab |
| Time | 2024 |
| Pages | 75 pages, 12 pages of appendices |
| Supervisor | Vesa Kankare |

## ABSTRACT


Identity and access management has become an increasingly important part of organizations' cybersecurity when they are protecting themselves against new threats. At the same time, the number of systems has grown wildly, and the related identity and access management processes have become more complex. In the past, it was also possible to think that organization's internal network was a wall and everything inside was safe. As the nature of work has changed and moved increasingly beyond the internal network, we are forced to start thinking differently.

The objective of this thesis was to examine what laws, regulations, standards, and best practices are applied in relation to implementing identity and access management in organizations. Multiple new laws and regulations have entered into force in quite a short time, most recently NIS2 and the related national legislation coming into force in 2024. Another important aim in this thesis was to investigate what threats and risks arise for organizations from poorly managed identity and access management and how those threats and risks can be minimized. In the worst-case scenario, these threats and risks might end business completely.

In this thesis, design based study was chosen as the research method. The focus was on examining best practices, cybersecurity threats, requirements stated in laws and regulations and the measures that should be taken to meet these requirements. Against this background challenges in the current stage were identified, and were created a preliminary framework for future development.

The result of the thesis is a presentation of the commissioner's current stage and compliance readiness. Also, the actions that could improve the commissioner's identity and access management were specified. In this study, two tables where created, that the commissioner can use to assess the current state of their operational and compare it to the best practices and to the requirements of NIS for identity and access management.



**Keywords:** identity, law, decree, cybersecurity

**SISÄLLYS**


1 JOHDANTO ..... 6

2 TUTKIMUSASETELMA ..... 7

2.1 Tutkimusongelma, tutkimuskysymykset ja tutkimuksen tavoitteet ..... 7

2.2 Tutkimusmenetelmät ..... 10

2.3 Työn rajaukset ja terminologia ..... 12

2.4 Teoreettinen viitekehys ..... 15

3 LAIT JA ASETUKSET ..... 17

3.1 EU:n yleinen tietosuoja-asetus – GDPR ..... 17

3.2 Tietosuojalaki (1050/2018) ..... 20

3.3 Laki yksityisyyden suojasta työelämässä (759/2004) ..... 21

3.4 NIS2 ..... 22

4 STANDARDIT JA PARHAAT KÄYTÄNNÖT ..... 26

4.1 NIST ..... 26

4.2 ISO 27001 ja ISO 27002 ..... 28

4.3 Parhaat käytännöt ..... 30

4.3.1 Sailpoint ..... 31

4.3.2 One Identity ..... 33

4.3.3 Veritis ..... 36

5 IDENTITEETIN- JA PÄÄSYNHALLINNAN VAATIMUKSET ..... 38

5.1 Tietoturvapolitiikka ..... 38

5.2 Identiteetinhallinta ..... 39

5.3 Pääsynhallinta ..... 40

5.4 Pääsyoikeudet ..... 41

5.5 Vähimpien oikeuksien periaate (Principle of Least Privilege) ..... 42

5.6 SSO ..... 43

5.7 Hallintaoikeudet ..... 43

5.8 Ohjeistukset, koulutukset ja kurinpito ..... 44

5.9 Vastuut ..... 44
5.10 Roolipohjaiset käyttöoikeudet (RBAC) ..... 45
5.11 MFA ..... 45
5.12 Zero Trust ..... 46
5.13 Vaaralliset työyhdistelmät ..... 47
5.14 Valvontatoimet ja lokienhallinta ..... 48
6 IDENTITEETIN- JA PÄÄSYNHALLINNAN YHTEYS TIETOTURVAAN ..... 50
6.1 Sosiaalinen manipulointi ..... 51
6.2 Kiristyshaittaohjelmat ..... 52
7 KEHITTÄMISPROJEKTI ..... 53
7.1 Kehittämiskohteet, olemassa olevat käytännöt ja prosessit ..... 53
7.2 Tarkennusta vaativat kohteet ..... 55
7.3 Vaatimuksiin vastaaminen ..... 55
7.4 Identiteetin- ja pääsynhallinnan järjestelmät ..... 56
8 TULOKSET ..... 57
8.1 Parhaat käytännöt identiteetin- ja pääsynhallinnan toteuttamiseen yritysmaailmassa ..... 57
8.2 Mahdollisia uhkia huonosti hoidetusta identiteetin- ja pääsynhallinnasta ..... 59
8.3 Lainsäädännöstä ja asetuksista nousevat vaatimukset ..... 62
8.4 Kehitystoimenpiteet parhaiden käytäntöjen ja vaatimusten käyttöönotolle ..... 63
8.5 Identiteetin- ja pääsynhallinnan järjestelmät ..... 64
9 JOHTOPÄÄTÖS ..... 65
10 POHDINTA ..... 68
LÄHTEET ..... 72

LIITTEET

Liite 1. Instant 27001 – NIS2 artikla 21 vs. ISO 27001:2022
Liite 2. NIS2-vaatimukset yhdistettynä ISO 27001:2022 -standardiin
Liite 3. Parhaat käytännöt vs. nykytila – vertailutaulukko

# 1 JOHDANTO

Identiteetin- ja pääsynhallinta on keskeinen osa tämän päivän kyberturvallisuutta. Sen avulla varmistetaan käyttäjille luotavien sähköisten identiteettien ja niihin liittyvien pääsyoikeuksien oikeellisuus ja ajantasaisuus. Ilman identiteetin- ja pääsynhallinnan prosesseja, käytäntöjä ja politiikkoja on vaikeaa, ellei mahdotonta, suojata sähköisiä identiteettejä sekä organisaation tietoa.

Tässä opinnäytetyössä tarkastellaan ja arvioidaan organisaation tämänhetkistä tilaa identiteetin- ja pääsynhallinnan (Identity and Access Management, IAM) osalta, sekä pyritään etsimään keinoja nykytilanteen parantamiseksi ja ongelmakohtien korjaamiseksi. Tärkeintä identiteetin- ja pääsynhallinnan alueella on oikein määritellyt ja toimivat prosessit sekä käytännöt. Ilman oikein määritettyjä prosesseja ja käytäntöjä ei millään järjestelmällä pystytä korjaamaan näitä puutteita.

Mahdolliset puutteet näissä käytännöissä ja prosesseissa heijastuvat yleensä uuden työntekijän aloittaessa organisaation palveluksessa. Ensimmäiset työpäivät, ehkä jopa viikot, menevät odotellessa oikeuksia niihin järjestelmiin, joihin käyttäjän tulisi päästä. Joskus kenelläkään ei välttämättä ole edes tietoa, mitä kaikkia järjestelmiä käyttäjän tulisi päästä aloittaessaan käyttämään. Oikein määritellyillä prosesseilla ja käytännöillä näitä haasteita pystytään vähentämään tai poistamaan ne jopa kokonaan. Prosessiin voidaan yhdistää myös muita identiteetin- ja pääsynhallinnan ulkopuolisia asioita, kuten työvälineiden tai työsuhdeauton tilaaminen, jo ennen työsuhteen alkua. Tällöin käyttäjäkokemus on äärimmäisen paljon sekavaa ja paljon työtä aiheuttavaa vaihtoehtoa parempi.

Heijasteet ovat mahdollisia myös työntekijän siirtyessä tehtävistä toisiin tai lopettaessa työnantajan palveluksessa. Tällöin käyttäjälle voi jäädä vanhaan tehtävään liittyviä pääsyoikeuksia tai joihinkin järjestelmiin jää oikeuksia käyttäjän lopettaessa.

Toimeksiantaja on Veho Oy Ab, joka toimii Mercedes-Benz-henkilöautojen ja Daimler-hyötyajoneuvojen jälleenmyyjänä ja jakelijana Suomessa, Ruotsissa,

Virossa, Latviassa ja Liettuassa. Veho-konsernissa työskentelee yli 2000 työntekijää, joista noin 1250 Suomessa ja yli 750 Ruotsissa ja Baltian maissa. Henkilöstö koostuu eri alojen ammattilaisista myynnistä mekaanikkoihin ja logistiikan asiantuntijoista hallinnon ihmisiin. Konsernin liikevaihto vuonna 2021 oli yli 1600 M€. (Veho 2023.)

# 2 TUTKIMUSASETELMA

Tämän luvun tarkoituksena on avata tarkemmin, minkälaisia tavoitteita työllä on. Mihin kysymyksiin haetaan vastauksia, miten vastauksia pyritään löytämään. Minkälaisia rajauksia työlle on asetettu sekä mitä tutkimusmenetelmiä ja teoreettista viitekehystä tullaan hyödyntämään.

## 2.1 Tutkimusongelma, tutkimuskysymykset ja tutkimuksen tavoitteet

Vuosien varrella on otettu käyttöön uusia järjestelmiä, ja järjestelmien määrä on kasvanut kasvamistaan. Nykyisellä tavalla, jolla käyttäjien identiteettejä ja pääsynhallintaa hoidetaan, sekä nykyisten prosessien ja käytäntöjen mukaan toimiminen on hyvin hankalaa. Ilman keskitettyä identiteetin- ja pääsynhallinnanjärjestelmää ja hyvin määriteltyjä ja toimivia prosesseja ja käytäntöjä alkaa olla vaikeaa, ellei jopa mahdotonta toimia turvallisesti.

Prosessit ja käytännöt eivät tällä hetkellä ole myöskään yhdenmukaiset kaikissa toimintamaissa, vaan ne vaihtelevat hyvinkin paljon eri maiden välillä. Nämä prosessit ja käytännöt tulisi korjata ja saattaa yhdenmukaiseksi koko konsernin laajuisesti. Prosessien ja käytäntöjen tulisi olla myös sisäisten sekä ulkoisten käyttäjien osalta samanlaiset – ensin syntyy digitaalinen identiteetti, johon voidaan sitoa erilaisia käyttäjätunnuksia, joille on määritettyinä erilaisia oikeuksia. Tällä hetkellä tässäkin on eroavaisuuksia ja suuri osa ulkoisten käyttäjien oikeuksista tilataan esimerkiksi sähköpostitse.

Automaation aste on tällä hetkellä kohtuullisen vähäinen ja tätä tulisi myös kasvattaa. Näin saataisiin erilaiset käyttäjästä johtuvat virheet vähenemään, sekä voitaisiin poistaa turhia oikeuksia käyttäjiltä automaation hoitaessa asioita, lisäksi tämä toisi kustannustehokkuutta. Aukotonta kirjausketjua (audit

trail) ei ole myöskään saatavilla minkään järjestelmän osalta täydellisesti. Joidenkin järjestelmien osalta on mahdollista saada jotain tietoa, mutta se ei ole aukotonta ja 100 % varmaa.

Käyttöoikeuksien luomisessa käytetään hyvinkin paljon niin sanottuja mallitunnuksia. Näissä tapauksissa joltain olemassa olevalta käyttäjältä kopioidaan toiselle käyttäjälle kaikki oikeudet, jolloin vähimpien oikeuksien malli (least privilege principle) ei toteudu. Lähestulkoon poikkeuksetta käyttäjä saa liikaa oikeuksia, jopa järjestelmiin, joihin ei niitä ollenkaan tarvitsisi. Käyttäjien siirtyessä tehtävästä toiseen vanhat oikeudet jäävät voimaan. Samoin käyttäjän siirtyessä pois organisaation palveluksesta saattaa oikeuksia jäädä joihinkin järjestelmiin, jolloin näiden järjestelmien hyödyntäminen voi olla pahimmillaan edelleen käyttäjän toimesta mahdollista.

Kaikki käyttöoikeudet tulisi saada keskitetysti haettavaksi identiteetin- ja pääsynhallinnan (Identity and Access Management, IAM) -järjestelmän kautta. Tämä mahdollistaisi ja varmistaisi, että käyttäjät saavat tarvitsemansa oikeuden nopeasti ja oikein. Työntekijän roolin muuttuessa käyttöoikeudet kohdejärjestelmiin muuttuisivat vastaamaan uuden roolin tarpeita. Näin saadaan myös varmistettua, että organisaatiosta poistuneille käyttäjille ei jää käyttöoikeuksia mihinkään järjestelmiin. IAMin avulla pystytään varmistamaan myös, ettei käyttäjille pääse muodostumaan vaarallisia käyttöoikeusyhdistelmiä (Separation of Duty [SoD]). Sen avulla pystytään luomaan työnkulut käyttöoikeuksien hyväksymiselle. Sillä voidaan myös seurata ja raportoida käytössä olevat käyttöoikeudet käyttäjä tai järjestelmätasoisesti. Sillä voidaan luoda loogisia rooleja tai ryhmiä ja saadaan automatisoitua käyttöoikeuksien antaminen näiden perusteella. Lisäksi reaaliaikaisesti voidaan tarkastaa käyttäjän oikeudet kaikkiin organisaation järjestelmiin.

Identiteetin- ja pääsynhallinnan prosessien ja käytäntöjen omistajuus ei myöskään ole oikein kenenkään vastuulla eikä omistuksessa. Osittain vastuu on HR-yksiköllä ja osittain digitaalisten palveluiden vastuulla. Tästä aiheutuu haasteita, koska asioita hoidetaan useamman tahon toimesta tietämättä, mitä vaatimuksia tai olemassa olevia prosesseja on jo rakennettu esimerkiksi käyttäjätunnuksen attribuutteihin liittyen tai minkälaisia muutoksia eri tahot tekevät toisistaan tietämättä. Pahimmillaan tämä saattaa johtaa jonkin järjestelmän

toiminnan lakkaamiseen tai erilaisiin virheisiin olemassa olevien käyttöoikeuksien osalta – käyttäjälle tulee liikaa oikeuksia tai tarvittavat oikeudet poistuvat. Näiden ongelmien selvittely on myös hankalaa, koska prosessit ja käytännöt eivät ole keskitetysti yhden tahon vastuulla. Näiden lisäksi, kun identiteetin- ja pääsynhallinnan prosessit ja käytännöt on rakennettu HR-järjestelmän jatkeeksi, voi HR-yksikkö tietämättään rikkoa joidenkin käyttäjien tai vaikka kaikkien käyttäjien pääsyn järjestelmiin, muuttamalla HR-järjestelmän toiminnallisuuksia tai vaikkapa muuttamalla keskitetysti jonkun tietyn attribuutin tietosisällön.

Haasteita on myös muun muassa sen suhteen, että ei ole välttämättä aivan selvää, minkä tahon vastuulla on minkäkin järjestelmän pääsynhallinta. Kenen pitäisi antaa lupa oikeuksien lisäämiseen järjestelmään ja kenen pitäisi sitten varsinaisesti tehdä muutokset järjestelmän pääsynhallintaan ja luvittaa käyttäjälle tarvittavat oikeudet.

Tässä opinnäytetyössä pyritään löytämään vastaukset seuraaviin tutkimuskysymyksiin:

1. Mitä parhaita käytäntöjä ja vaatimuksia on olemassa identiteetin- ja pääsynhallinnan suorittamiseen yritysmaailmassa?

2. Mitä uhkia organisaatiolle aiheutuu huonosti hoidetusta identiteetin- ja pääsynhallinnasta?

3. Minkälaisia vaatimuksia lainsäädäntö tai asetukset aiheuttavat organisaatioiden identiteetin- ja pääsynhallinnalle?

4. Minkälaisia kehitystoimenpiteitä tulee tehdä, jotta parhaat käytännöt saadaan käyttöön ja vaatimuksiin pystytään vastaamaan?

Näillä tutkimuskysymyksillä pyritään hakemaan vastaukset tämän hetken suurimpiin kipupisteisiin ja siihen, miten nämä saadaan korjattua. Vastauksien kautta saatavien korjaustoimenpiteiden voidaan olettaa vievän organisaation identiteetin- ja pääsynhallinnan kypsyyden aivan uudelle tasolle.

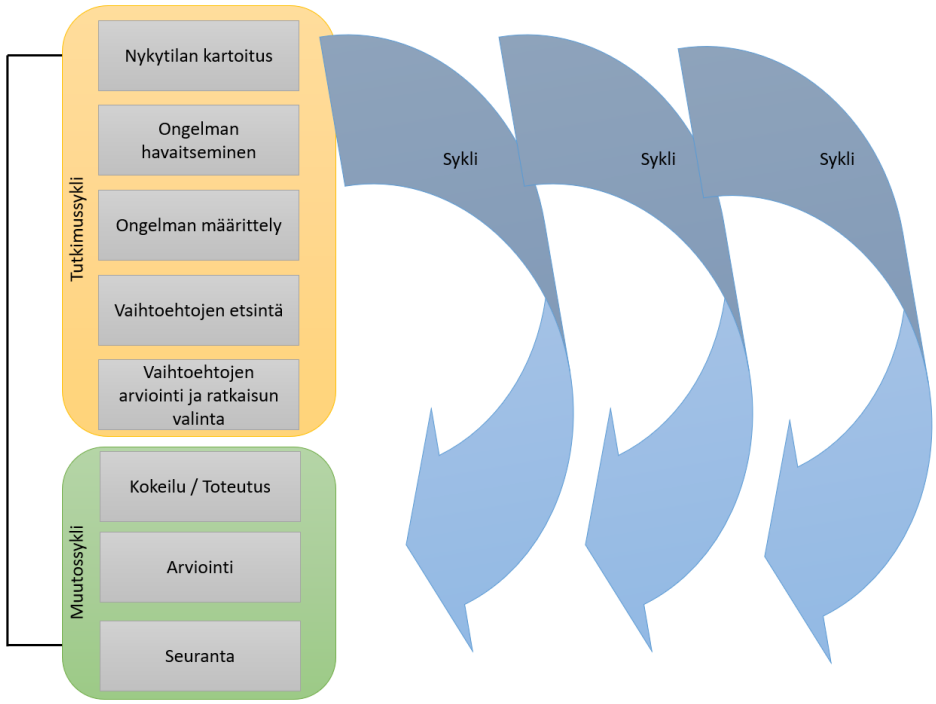
## 2.2 Tutkimusmenetelmät

Tutkimusmenetelmäksi työhön valikoitui kehittämistutkimus. Menetelmä on valittu, koska työssä on tarkoitus kehittää olemassa olevia identiteetin- ja pääsynhallinnan prosesseja ja saada aikaan pohja tulevaisuuden prosesseille ja käytännöille sekä mahdollistaa näiden perusteella mahdollisimman helppo käyttöönotto jollekin teknologialle.

Tutkimuksellisessa kehittämistyössä ei ole pääosassa teoria vaan käytäntö, jolle haetaan tukea teoriasta. Tuloksista saatu hyöty konkretisoituu niitä käytäntöön siirrettäessä sekä uusia kehitettyjä ideoita implementoitaessa. Kehittämistyössä on keskeisintä luoda uusia ratkaisuja sekä muokata ja soveltaa jo olemassa olevia ratkaisuja. (Ojansalo ym. 2015, 20.)

Perinteisillä tutkimuksilla pyritään kuvaamaan, selittämään tai ymmärtämään ilmiöitä, mutta ne eivät pyri tuottamaan varsinaista muutosta. Interventiotutkimuksissa taas pyritään poistamaan ongelmia, tuottamaan muutosta, tehdään asiat toisin tai keksitään nykyistä parempia ratkaisuja. Näin toteutetuista tutkimuksista voidaan käyttää nimitystä interventiotutkimukset. Interventio tarkoittaa sitä tekijää, jonka avulla muutos saadaan aikaan. Kehittämistutkimus on yksi interventiotutkimuksista. (Kananen 2017, 10.)

Kehittämistutkimus ei ole kehittämistutkimus, vaan pelkkä tutkimustyö, ellei siinä ole tutkimuksellista otetta sekä tutkimusosiota. Kehittämistutkimus on puhtaasti kvantitatiivista tutkimusta tai yhdistelmä kvantitatiivista sekä kvalitatiivista tutkimusta, kuitenkin siten, että tavoitteena on muutoksen aikaansaaminen. Kehittämistutkimus käynnistyy nykytilan kartoituksella, jonka yhteydessä määritetään kehittämisen kohde, eli ongelma. Jotta interventio onnistuu, tulee ongelma määritellä ja ongelmaan vaikuttavat tekijät analysoida. Kehittämistutkimuksen ylätason syklit ovat suunnittelu, toiminta, havainnointi ja seuranta. Kananen (2015) on avannut näiden syklien vaiheita tarkemmalla tasolla kuvassa 1 (kuva 1). (Kananen 2015, 39–41.)




Kuva 1. Kehittämissyklin vaiheet (Kananen 2015, 42)

Ongelman korjaamiseksi tulee löytää syyt, joista ongelma johtuu ja kun nämä syyt on löydetty, voidaan ongelmia alkaa poistamaan. Optimaalisimman keinon käyttäminen ei ole aina mahdollista ja on jopa mahdollista, että ongelmia ei saada välttämättä edes korjattua. Muutosten toteuttaminen ja korjausten tekeminen vaatii aina suunnitelmallisuutta. Oikean ratkaisun löytäminen ei vielä tarkoita sitä, että korjaava ratkaisu olisi mahdollista viedä käytäntöön. (Kananen 2015, 40–42.)

Muutostyössä on kolme vaihetta, jotka ovat suunnittelu-, toteutus- ja arviointivaihe ja näistä muodostuu kokonaisprosessi (Ojansalo ym. 2015, 22). Projektissa tullaan hyödyntämään myös ulkopuolisten konsulttien apua sisäisten resurssien lisäksi. Projektissa on myös järkevää käyttää jotain työkalua työnohjaamisessa sekä etenemisen seurannassa. Kanban-taulu on yksi hyvä ja käytettävä työkalu tähän.

Alussa tullaan käymään läpi olemassa olevaa dokumentaatiota, jotta saadaan kartoitettua nykytila tarkemmin ja löydetään ne prosessit, joiden kehittämiseen tullaan keskittymään, sekä löydetään muut mahdolliset suurimmat ja tärkeim-

mät kehityksen kohteet. Työn tavoitteena on luoda identiteetin- ja pääsynhallintaa varten prosessit ja käytännöt, jotka mahdollistavat palvelun globaalin tuottamisen samalla mallilla kaikissa toimintamaissa.

### 2.3 Työn rajaukset ja terminologia

Työssä ei tulla ottamaan käyttöön mitään uutta teknologiaa. Työ tulee keskittymään enemmän nykytilan haasteiden kuvaamiseen, prosessien ja käytäntöjen kehittämiseen sekä pidemmän tähtäimen tavoitetilan kuvaamiseen. Uuden teknologian valinnan ja käyttöönoton tulisi olla mahdollista kohtuullisen pienellä vaivalla työn tulosten perusteella. Jos nähdään järkeväksi kustannusten ja ajankäytön näkökulmasta, voidaan olemassa olevia järjestelmiä kehittää, mutta tämäkään ei ole ensisijainen lähtökohta. Työssä tullaan keskittymään tietosuojan ja tietoturvan näkökulmiin identiteetin- ja pääsynhallinnan osalta, koska ne ovat tärkeä osa kokonaisuutta. Toisaalta varsinaisiin kyberuhkiin ja näiden riskien toteutumiseen ei työssä tulla syventymään, koska niiden käsittely tulisi paisuttamaan työtä valtavasti. Työn ulkopuolelle on rajattu myös asiakkaiden identiteetinhallintaan liittyvät asiat.

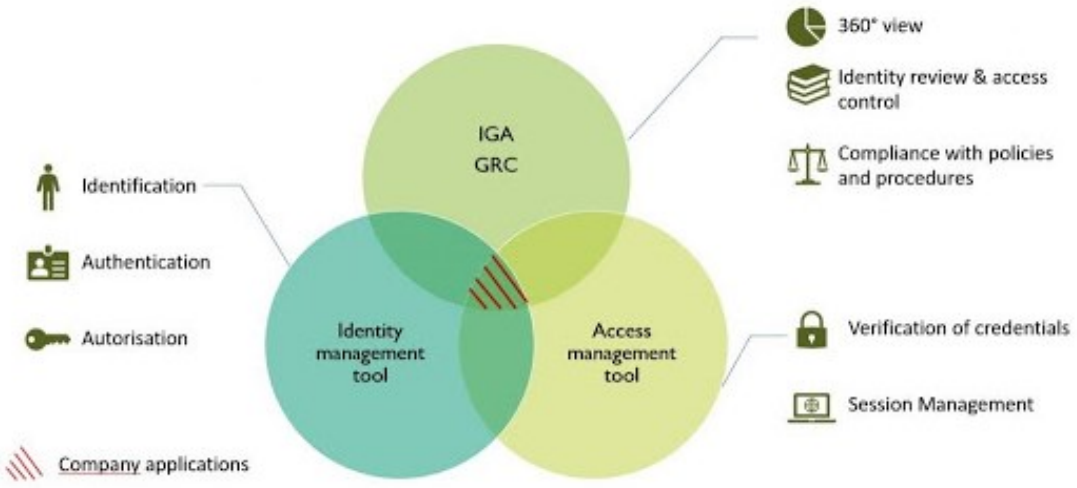
Tietotekniikan käsitteistöön on vakiintumassa malli, jossa digitaalinen identiteetti (digital identity) ja henkilöllisyyskäsite (identity) eroavat toisistaan. Henkilöllä voi olla useita identiteettejä – yksi identiteetti organisaation tietojärjestelmiin, toinen identiteetti kaupan kanta-asiakasjärjestelmään ja kolmas esimerkiksi johonkin sosiaalisen median palveluun, mutta vain yksi henkilöllisyys. Tietojärjestelmissä esitettyjä kohteita, eli digitaalisia identiteettejä hallitaan identiteetinhallinnan (Identity management, IdM) prosesseilla. Pääsynhallinnan (access management, AM) käsite on usein identiteetinhallinta-käsitteen aisaparina. Tällä tarkoitetaan prosessia, jossa käyttäjän identiteetti tunnistetaan ja todetaan, onko käyttäjällä tarvittava pääsy kyseiseen tietojärjestelmään ja minkälaiset oikeudet järjestelmän käyttämiseen on. Nämä kaksi käsitettä muodostavat yhdessä identiteetin- ja pääsynhallinnan yläkäsitteen (identity and access management, IAM). (Linden 2017, 10–11.)

Sähköinen identiteetti koostuu erilaisista attribuuteista. Kerätyt attribuutit muodostavat käyttäjätietokannan skeeman. Yhden attribuuteista tulee sisältää yk-

silöivä tunniste, jolla käyttäjät voidaan erottaa toisistaan. Yksilöivänä tunnisteena voidaan käyttää esimerkiksi käyttäjätunnusta, sähköpostiosoitetta, henkilötunnusta, työntekijänumeroa tai passin numeroa. (Linden 2017, 11–12.)

Identiteettien hallinnointiratkaisu (Identity Governance and Administration, IGA) pitää sisällään viitekehyksen ja tietoturvaratkaisuja, joiden avulla voidaan tehokkaasti vähentää identiteetteihin liittyvä riskejä liiketoiminnassa. IGAn avulla voidaan automatisoida käyttäjätilien, roolien ja käyttöoikeuksien luonti, poisto, sekä hallinnointi organisaation sisäisille ja ulkoisille käyttäjille. Näin saadaan virtaviivaistettua sekä automatisoitua prosesseja käyttäjien, salasanojen, käytäntöjen, identiteettien elinkaarten ja käyttöoikeuksien hallintaan sekä pääsyn tarkistukseen liittyen. IGA mahdollistaa organisaatioille paremman näkyvyyden käyttäjien identiteetteihin ja pääsyoikeuksiin, jolloin voidaan paremmin hallita, kuka pääsee mihinkin järjestelmään ja milloin. Identiteetinhallinta antaa organisaatiolle mahdollisuuden tehdä enemmän vähemmällä, parantaa tietoturvakyvykkyyksiään ja vastata mahdollisiin auditointeihin sekä skaalautua kasvuun. (Fortra s.a.)

IAM ja IGA ovat molemmat hyvinkin samankaltaisia, mutta eroavat toiminnaltaan kuitenkin toisistaan. Molemmilla ratkaisuilla hallinnoidaan identiteettejä sekä pääsynhallintaa ja niihin liittyviä prosesseja. IAM ratkaisulla hallitaan politiikat ja pääsynhallinta järjestelmiin. IGAn avulla tuodaan lisäksi auditointiin ja vaatimustenmukaisuuteen liittyvät toiminnallisuudet sekä elinkaarenhallinta, analytiikka, raportointi ja lokittaminen mukaan helpottamaan toimintaa. IGAn voisi todeta toteuttavan tietynlaista 360-näkymää identiteetteihin ja pääsynhallintaan liittyen. Sen avulla voidaan myös täyttää erilaisia regulaatioihin liittyviä vaatimuksia ja se myös mahdollistaa tarkastus- ja vaatimustenmukaisuusvaatimusten täyttämisen esimerkiksi GDPR:n osalta. IGAn avulla voidaan myös havaita erilaiset rikkomukset, kuten luvaton käyttö, heikot kontrollit sekä käytäntöihin liittyvät rikkomukset. IGAn, IAMin ja IdM:n välistä suhdetta on kuvattu kuvassa 2. (Fryzel, 2021.)




Kuva 2. IGAn, IAMin ja IdM:n väliset suhteet toisiinsa (Fryzel, 2021)

Monesti on myös hyvä tuottaa pääsynhallintaa erilaisten roolien mukaan. Eli pyritään löytämään organisaation käyttäjistä yhdistäviä tekijöitä, joiden perusteella käyttäjät voidaan määrittää rooleihin. Näiden roolien perusteella voidaan sitten antaa yhdellä kertaa käyttäjälle oikeudet käyttää useampia järjestelmiä ja näiden järjestelmien sisällä voi sitten olla eritasoisia oikeuksia. Tämä helpottaa sekä ylläpitäjien että myös käyttäjien toimintaa, koska rooli voi olla linkitettynä vaikkapa käyttäjän titteliin ja täten jo automaattisesti tulee sitten oikeuksia järjestelmiin, ilman erillistä oikeuksien anomista. Tämän lisäksi voidaan myös määrittää kaikille käyttäjille perusoikeudet, jotka tulevat kaikille käyttäjille automaattisesti. Yleisesti tällaisia oikeuksia ovat esimerkiksi pääsy sähköpostiin, Teamsiin, organisaation intranettiin ja sitä kautta erilaisiin aineistoihin sekä HR-järjestelmään, josta käyttäjä voi anoa esimerkiksi lomansa ja ilmoittaa poissaoloistaan.

Tässä työssä keskitytään digitaaliseen identiteettiin ja sen hallintaan sekä pääsynhallintaan. Työ on rajattu koskemaan pelkästään organisaation suomalaisten käyttäjien identiteettien- ja pääsynhallintaa. Työ tulee toimimaan myös hyvänä pohjana muiden maiden identiteetin- ja pääsynhallintaan ja ideaalisesti kaikissa maissa hallinta tapahtuisi keskitetysti samoilla prosesseilla ja samalla teknologialla.

## 2.4 Teoreettinen viitekehys

Teoreettisena viitekehyksenä työssä toimivat erilaiset lait ja asetukset. NIS2-direktiivi tarjoaa hyvät lähtökohdat sille, miten organisaatioiden odotetaan Euroopan unionin näkökulmasta toteuttavan kyberturvallisuuteen liittyvää suojautumista ja varautumista. NIS2:n mukaan toimijoiden tulisi lisätä erilaisia kyberhygieniankäytäntöjä, kuten identiteetin- ja pääsynhallintaa, nollaluottamuksen periaatetta, ohjelmistopäivityksiä, verkon segmentointia, laitteiden konfigurointia ja käyttäjien kouluttamista – käyttäjän manipulointiin, kyberuhkiin ja verkkourkintaan liittyen (NIS2-direktiivi Loihde trust s.a.). Näistä tämän työn alueelle eniten osuvat luonnollisesti identiteetin- ja pääsynhallinnan tehtävät mutta myös käyttäjien kouluttaminen sekä tietyllä tapaa myös nollaluottamuksen periaate (Zero Trust). Nollaluottamuksen periaatteeseen työssä ei kuitenkaan tulla ottamaan suuremmin kantaa, koska se olisi liian laaja aihe käsitellä tämän työn yhteydessä.

Hyvänä lähteenä toimii myös NIST (National Institute of Standards and Technology). NIST on osa Yhdysvaltain kauppaministeriötä ja sen tehtävä on edistää Yhdysvaltojen innovaatioita ja teollisuuden kilpailukykyä (NIST 2009). NIST tuottaa myös paljon erilaisia tieteen ja teknologian standardeja, joita voidaan hyödyntää muun muassa organisaation kyberturvallisuuden parantamiseen.

Myös yleinen tietosuoja-asetus (General Data Protection Regulation – GDPR) asettaa huomioitavia asioita identiteetin- ja pääsynhallinnan järjestelmien suunnittelulle. GDPR astui voimaan 25.5.2018 ja oli voimaan astuessaan suurin muutos tietosuoja-alueella vuosikymmeniin. Kaikessa täysin automaattisessa tai osittain automaattisessa henkilötietojen käsittelyssä tulee soveltaa tietosuoja-asetusta. Kokonaisuutena henkilötietojen käsittelyn määritelmä on laaja, ja siihen sisältyy muun muassa tietojen kerääminen, tallentaminen, säilyttäminen, muokkaaminen, luovuttaminen, levittäminen, yhdistäminen sekä poistaminen. Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön liittyviä tietoja. Luonnollisen henkilön tunnistaminen voidaan toteuttaa suorasti tai epäsuorasti tunnistetietojen, kuten henkilötunnuksen, nimen, sijaintitietojen, verkkotunnistetietojen, yhden tai useamman

henkilölle tunnusomaisen kulttuurillisen, taloudellisen, psyykkisen, fyysisen, fysiologisen, sosiaalisen tai geneettisen tekijän tai tekijöiden perusteella. Myös pseudonyymit tunnisteet ovat henkilötietoja identiteetin- ja pääsynhallinnanjärjestelmissä. Asetusta sovelletaan myös muun muassa evästeisiin sekä IP-osoitteisiin ja nämä tulkitaan myös henkilötiedoiksi. (Linden 2017, 66.)

Erilaiset standardit toimivat työssä myös erinomaisina lähteinä. Yksi erinomainen lähde työssä on ISO 27002-standardi, josta saadaan monia huomioitavia asioita, kuten miten identiteetin- ja pääsynhallinnan prosessit tulisi toteuttaa ja mitä niissä tulisi huomioida, jotta kyseisen sertifikaatin määrittämä tietoturvallisuuden taso voitaisiin saavuttaa (SFS-EN ISO/IEC 27002:2022, 7).

Huomioitavaa on, että ISO 27002 tarjoaa vain lähtökohdan ja pohjan sille, mitä organisaatio voi tehdä tietyn tietoturvallisuustason saavuttamiseksi, mutta sen tarjoamaa tietoa ei välttämättä voida soveltaa sellaisenaan. Pelkästään puhtaasti teknologian keinoin ei voida myöskään saavuttaa täydellistä tietoturvaa, vaan tarvitaan myös toimivia prosesseja, sääntöjä, toimintaperiaatteita, erilaisia menettelyjä, sekä ohjelmisto- ja laitteistotoimintoja. (SFS-EN ISO/IEC 27002:2022, 7.)

Pääasiallisena aineistona tutkimuksessa hyödynnetään tutkimuksen aikana läpikäytyjä aiemmin tuotettuja dokumentteja, erilaisia teknisiä ja prosessiin sekä käytäntöihin liittyviä havaintoja ja palautteita, joita kerätään työn edetessä. Nämä kaikki ovat Kanasen (2017, 42–43) mukaan aineistonkeruumenetelmiä interventiotutkimusta tehtäessä. Kaikkien kehittämistutkimusten yläkäsitteenä voidaan pitää interventiotutkimusta (Kananen 2017, 10).

Lisäksi aiheesta on kirjoitettu jonkin verran opinnäytetöitä ja erilaisia julkaisuja, joista on saatavilla paljon hyödyllistä tietoa myös tähän työhön. Zero Trust -tietoturva-arkkitehtuurista saadaan myös identiteetin- ja pääsynhallintaan palasia. Organisaatiossa laadittua tietoturvapolitiikkaa ja siihen kirjattuja linjauksia tullaan myös hyödyntämään työssä.

Tällä viitekehyksellä saadaan hyvä selkänoja sille, miten organisaation ja organisaatioiden ylipäänsä tulisi hoitaa identiteetin- ja pääsynhallinnan proses-

seja ja mitä tulisi huomioida, jotta toiminta olisi kyberturvallisuuden näkökulmasta mahdollisimman pitkälle suojattua ja riskejä olisi saatu vähennettyä mahdollisimman paljon. Kyberturvallisuus on kuitenkin viime kädessä riskien hallintaa.

# 3 LAIT JA ASETUKSET

Luvussa 3 avataan kansallisia lakeja sekä EU-tasoisia direktiivejä ja asetuksia, joilla on vaikutusta identiteetin- ja pääsynhallinnan toteuttamiseen.

## 3.1 EU:n yleinen tietosuoja-asetus – GDPR

Globalisaatio ja teknologian kehittyminen nopeasti ovat tuoneet henkilötietojen suojaamiseen uusia haasteita. Henkilötietoja kerätään sekä jaetaan nyt huomattavasti enemmän kuin aiemmin. Teknologia on myös mahdollistanut yksityisten organisaatioiden ja viranomaisten hyödyntää henkilötietoja omissa toiminnoissaan entistä laajemmin. Luonnolliset henkilöt myös jakavat yhä useammin omia henkilötietojaan maailmanlaajuisesti kaikkien saataville. Tulevaisuudessa teknologia tulee todennäköisesti helpottamaan henkilötietojen vapaata liikkumista unionin sisällä sekä tietojen siirtämisen myös kolmansiin maihin ja kansainvälisille organisaatioille sekä järjestöille. Teknologian voidaan myös olettaa hoitavan henkilötietojen korkeatasoisen suojaamisen. Tämä kehitys on aiheuttanut tarpeen vahvalle ja johdonmukaiselle tietosuojakehykselle. Luonnollisilla henkilöillä tulisi olla mahdollisuus valvoa omia henkilötietojaan. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 2.)

Tietomurtojen ja henkilötietojen väärinkäytösten estäminen on GDPR:n ydin ja sen vuoksi onkin hyvinkin yllättävää, että asetuksessa ei määritellä selkeästi identiteetin- ja pääsynhallintaa missään kohtaa. GDPR:n artikla 32 määrittelee henkilötietojen käsittelyn turvallisuusvaatimukset. Tähän sisältyy muun muassa tarve varmistaa käsittelyn jatkuva luottamuksellisuus ja eheys samalla, kun järjestelmät tulee pystyä palauttamaan käyttöön nopeasti mahdollisen fyysisen tai teknisen vian sattuessa. Nämä asiat on pystyttävä näyttämään toteen: että on kyky toimia tämän mukaisesti ja oikeasti näin myös toimitaan. Identiteetin- ja pääsynhallinta vähentää tietojen katoamiseen ja luvattomaan käyttöön liittyvää riskiä. Sen avulla voidaan rajoittaa pääsyä yritysverkkoihin ja

järjestelmiin, sekä suojata rekisteröidyn, että järjestelmän käyttäjän henkilöllisyyttä. (OpenText 2018a.)

GDPR asettaa tiukat vaatimukset henkilötietojen käsittelylle. Keskitetyn identiteetin- ja pääsynhallinnan avulla saadaan henkilötiedot suojattua laittomalta ja luvattomalta käsittelyltä käyttäen luotettavaa todennusta ja käyttöoikeuksien hallintaa. Käyttämällä monivaiheista tunnistautumista voidaan tehdä todennuksesta entistäkin varmempaa. Näin toimimalla voidaan varmistaa pelkästään valtuutettujen käyttäjien pääsy niihin resursseihin, joihin se on tarpeen. Mahdollisesti on myös syytä harkita työntekijöiden roolipohjaista todentamista sisäisen identiteetin- ja pääsynhallinnan yksinkertaistamiseksi ja vahvistamiseksi. IAM-alusta vaatii myös federoitua todennusta, jotta käyttöoikeuksia voidaan myöntää ja peruuttaa nopeasti myös kumppaneilta ja tilapäisiltä työntekijöiltä. IAMin avulla on mahdollista myös nähdä nopeasti ja helposti, mihin henkilötietoihin mahdollinen tietoturvaloukkaus on vaikuttanut. (OpenText 2018a.)

Tiedon minimointi on myös yksi GDPR:n peruslähtökohdista. Eli vain toiminnan kannalta oleelliset tiedot saadaan tallentaa. Identiteetin- ja pääsynhallinnan avulla voidaan helposti ja keskitetysti hallita omia työntekijöitä, asiakkaita ja kumppaneita koskevia käyttö- ja valtuustietoja. Sen avulla voidaan myös määritellä, kuinka kauan käyttäjällä on pääsy järjestelmiin ja kuinka kauan tietoja on säilytettävä. Tämä mahdollistaa käyttäjätilin oikea-aikaisen ja perustellun poistamisen käytöstä. Yksi suurimmista takaovista erilaisille hakkereille ovat niin sanotut ”haamutilit”, joista kukaan ei tiedä, miksi ne ovat olemassa, mihin niitä käytetään tai mihin niillä on oikeuksia. Identiteetin- ja pääsynhallinnan avulla tätä kyberturvallisuusriskiä pystytään pienentämään ja samalla myös noudatetaan tiedon minimointivaatimuksia. (OpenText 2018a.)

Monella organisaatiolla on identiteetin- ja pääsynhallinnan strategiassaan kolme elementtiä: työntekijät, yhteistyökumppanit ja alihankkijat sekä asiakkaat:

1. Työntekijöiden osalta tulee tietää mihin kaikkiin järjestelmiin heillä on pääsy ja minkälaiset oikeudet heillä näihin järjestelmiin on. Tämä on tärkeää varsinkin niiden järjestelmien osalta, joissa käsitellään henkilö-

tietoja. Erilaiset muutokset työntekijöiden rooleissa tulisi pystyä hallitsemaan nopeasti ja roolin muuttuessa tulisi pystyä poistamaan vanhat oikeudet ja myöntää uudet oikeudet. Vanhoja oikeuksia ei saisi käyttäjille jäädä roikkumaan. Lisäksi on tärkeää tunnistaa ja poistaa niin sanotut ”haamutilit”. Tutkimusten mukaan jopa neljännes kaikista tileistä on passiivisia ja hakkerit käyttävät niitä yhä useammin kohteinaan.

2. Yhteistyökumppaneita ja alihankkijoita on nykyään lähes jokaisessa organisaatiossa ja siten usein myös näillä henkilöillä voi olla pääsy henkilötietoja sisältäviin järjestelmiin. Tämä on usein myös tärkeää, jotta yhteistyö eri toimijoiden kesken onnistuu. Jos olet rekisterinpitäjä, sinun on kyettävä varmistamaan oikeanlainen pääsy organisaation ulkopuolella säilytettäviin tietoihin.
3. Asiakkaiden osalta monet organisaatiot mahdollistavat digitaalisten identiteettien luomisen organisaation verkkopalveluihin. Moniin näistä liittyy itsepalvelupalvelukyvykkyyksiä ja usein myös mahdollisuus käyttää yksinkertaisia salasanoja autentikointiin. Tämä on haavoittuvuus, joka tulee hoitaa, ja johon tulee soveltaa samoja GDPR:n käsitteitä tietojen minimoisen suhteen ja kuinka käyttäjät tulee suojata. (OpenText 2018b.)

Perinteisesti tätä haastetta on lähestytty yksinkertaisilla manuaalisilla pääsynhallinnan kontrolleilla, jotka ovat perustuneet Active Directory -ryhmiin. Haittapuolena näissä on se, että nämä prosessit ovat hitaita, hankalia ja kalliita, eivätkä ne myöskään skaalaudu. Lisäksi käyttäjäkohtainen valvonta ja hallinta on ongelmallista. GDPR:n myötä organisaatioiden on ollut pakko muuttaa identiteetin- ja pääsynhallinnan strategiaansa. Strategiassa on nyt huomioitava myös omien työntekijöiden lisäksi ulkopuoliset kumppanit, alihankkijat sekä mahdolliset asiakkaat. Identiteetin- ja pääsynhallinnan hallintaohjelman kautta on mahdollista luoda dynaamisia ja kattavia autorisointi- ja autentikointikyvykkyyksiä koko organisaatiolle sekä kumppaniverkostolle. Näin saadaan suojattua pääsy henkilötietoihin ja minimoitua riskejä. (OpenText 2018b.)

### 3.2 Tietosuojalaki (1050/2018)

Tietosuojalaki täsmentää ja täydentää EU:n yleistä tietosuoja-asetusta (EU 679/2016) ja sen kansallista soveltamista. Lakia sovelletaan tietosuoja-asetuksen 2 artiklan mukaisesti. Jos rekisterinpitäjän toimipaikka sijaitsee Suomessa, sovelletaan rekisterinpitäjän tai henkilötietojen käsittelijän toimintaan Suomen lakia. Tietosuojalaki on myös korvannut henkilötietolain (523/1999). (Tietosuojalaki 1050/2018, 1. §, 2. §.)

Lain mukaan henkilötietojen käsittelyn lainmukaisuus täyttyy tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdan mukaisesti, jos:

1) *kysymys on henkilön asemaa, tehtäviä sekä niiden hoitoa julkisyhteisössä, elinkeinoelämässä, järjestötoiminnassa tai muussa vastaavassa toiminnassa kuvaavista tiedoista siltä osin kuin käsittelyn tavoite on yleisen edun mukainen ja käsittely on oikeasuhtaista sillä tavoiteltuun oikeutettuun päämäärään nähden;*

2) *käsittely on tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi;*

3) *käsittely on tarpeen tieteellistä tai historiallista tutkimusta taikka tilastointia varten ja se on oikeasuhtaista sillä tavoiteltuun yleisen edun mukaiseen tavoitteeseen nähden; tai*

4) *henkilötietoja sisältävien tutkimusaineistojen, kulttuuriperintöaineistojen sekä näiden kuvailutietoihin liittyvien henkilötietojen käsittely arkistointitarkoituksessa on tarpeen ja oikeasuhtaista sillä tavoiteltuun yleisen edun mukaiseen tavoitteeseen ja rekisteröidyn oikeuksiin nähden.*

(Tietosuojalaki 1050/2018, 4 §.)

Tietosuojarikoksista määrättävät rangaistukset on säädetty rikoslain 38 luvun 9 §:ssä. Rikoslain 38 luvun 3 ja 4 §:ssä on säädetty rangaistukset viestintäsalaisuuden loukkauksesta sekä törkeästä viestintäsalaisuuden loukkauksesta. Tietomurtoihin ja törkeisiin tietomurtoihin liittyvät rangaistukset on määritetty rikoslain 38 luvun 8 ja 8 a §:ssä. Tietosuojalain vaitiolovelvollisuuden (35 §) ja salassapitovelvollisuuden (36 §) rikkomisesta tuomiot tulevat rikoslain 38 luvun 1 tai 2 §:n mukaan, ellei teko ole rikoslain 40 luvun 5 §:n mukaan rangaistava, tai ellei muualla laissa ole säädetty ankarampaa rangaistusta. (Tietosuojalaki 1050/2018, 26. §.)

Rangaistukset edellä mainituista teoista vaihtelevat sakkorangaistuksista kahden vuoden vankeuteen (Rikoslaki 19.12.1889/39, 38 luku).

### 3.3 Laki yksityisyyden suojasta työelämässä (759/2004)

Laissa säädetään työntekijään liittyvistä henkilötietojen käsittelyn yleisistä edellytyksistä, huumausaineiden käyttöä koskevien tietojen käsittelystä, testien ja tarkastusten suorittamista koskevista vaatimuksista, kameravalvonnasta työpaikalla ja työnantajalle kuuluvien sähköpostiviestien hakemisesta ja avaamisesta. (Laki yksityisyyden suojasta työelämässä 13.8.2004/759, 2. §.)

Henkilötietojen käsittelyn yleisinä edellytyksinä saadaan käsitellä vain työsuhteen kannalta tarpeellisia tietoja. Näiden tietojen tulee liittyä työsuhteen osapuolten velvollisuuksien ja oikeuksien mahdollistamiseen tai mahdollisten työtehtävien erityisluontoisuudesta johtuvien etuisuuksien tarjoamiseen työntekijälle. Lähtökohtaisesti kaikki työntekijästä tarvittavat tiedot on kerättävä työntekijältä itseltään. Jos tietoja kerätään muualta, on tähän oltava työntekijän suostumus. Poikkeuksena tähän ovat tehtävät, joissa työntekijä suorittaa tehtäviä laissa säädetyn tehtävän osalta ja viranomainen luovuttaa tietoja työnantajalle tai jos laissa on erikseen säädetty tietojen keräämisestä ja saamisesta. Työnantaja on velvollinen ilmoittamaan etukäteen työntekijälle tätä koskevien tietojen hankkimisesta muualta, kuin työntekijältä itseltään. Henkilöluottotietoja hankittaessa työnantajan tulee ilmoittaa työntekijälle, mistä rekisteristä luottotietoja ollaan hankkimassa. Turvallisuusselvityslaissa (726/2014) on säädetty turvallisuusselvityksen hakemisesta. Alaikäisten kanssa työskentelevien rikostaustan selvittämisestä on määrätty lasten kanssa työskentelevien rikostaustan selvittämiseksi annetussa laissa (504/2002). Rikosrekisteristä saatavien tietojen osalta on säädetty rikosrekisterilaissa (770/1993). Työnantajan on ilmoitettava työntekijälle etukäteen muualta hankituista tiedoista, ennen kuin niitä voidaan hyödyntää työntekijää koskevassa päätöksenteossa. (Laki yksityisyyden suojasta työelämässä 13.8.2004/759, 3. §, 4. §.)

### 3.4 NIS2

NIS2-direktiivi on päivitetty versio alkuperäisestä NIS-direktiivistä, joka hyväksyttiin vuonna 2016 ja joka tuli voimaan toukokuussa 2018. Alkuperäinen tarkoitus NIS-direktiiveillä on ollut parantaa Euroopan taloudelle olennaisten ja kriittisten palveluiden tuottajien kyberturvallisuutta koko Euroopan unionin alueella. NIS2-direktiivi on hyväksytty virallisesti marraskuussa 2022 ja se tuli voimaan 16.1.2023. Jäsenvaltioilla on aikaa 17.10.2024 asti saattaa direktiivin määrittämät toimenpiteet osaksi kansallisia lainsäädäntöjä. (OKTA 2023b, 4.)

Suomessa kansallisen lainsäädännön valmistelu direktiivin osalta on käynnissä liikenne- ja viestintäministeriön työryhmässä. Tämän suosituksen tarkoituksena on auttaa valvovaa viranomaista sekä NIS2-toimialoja kyberturvallisuusvaatimusten toteuttamisessa. Se sisältää esimerkkejä sekä todennusmenetelmiä kyberturvallisuuden riskienhallinnan toimenpiteistä. Suosituksesta löytyy viittaukset yleisiin viitekehyksiin sekä standardeihin, mutta siinä ei varsinaisesti käydä läpi minkään viitekehyksen tai standardin käyttöönottoa. Suositus tulee julkisesti lausuttavaksi ja eduskunnan käsittelyyn kevään 2024 aikana. Lainsäädännön hyväksymisen jälkeen suositus tullaan julkaisemaan kaikkien hyödynnettäväksi. (Kyberturvallisuuskeskus 2023.)

Laiksi NIS2-direktiivi astuu lokakuussa 2024. Direktiivissä määritetään sekä kriittiseksi luokitellut, että erittäin kriittiseksi luokitellut sektorit. Kriittisiä sektoreita ovat kemikaaliala, tutkimustoiminta, digitaaliset palvelut kuten markkinapaikat ja hakukoneet, elintarvikeala, jätehuolto, posti- ja kuriiripalvelut sekä valmistavan teollisuudenalalta esim. lääkintälaitteet. Erittäin kriittisiksi on määritelty finanssiala ja sen infrastruktuuri, julkishallinto, energia-ala, tietoturvapalveluita sekä tietototurvan hallintapalveluita tuottavat ICT-toimijat, avaruus, juoma- ja jätevesi, liikenne, terveydenhuolto ja digitaalisen infrastruktuurin sektorit. Laki vaikuttaa riskienhallintaan, yritysvastuuseen, kyberpoikkeamien ilmoitus- ja raportointivelvoitteisiin, liiketoiminnan jatkuvuuden ja kriisinhallintakyvyn varmistamiseen ja ylläpitämiseen, riittävien kyberturvallisuuden teknisten ja menetelmällisten keinojen varmistamiseen, turvallisuuden huomioimiseen hankinnoissa, ihmisten osaamisen ja tietoturvaorientaation varmistamiseen sekä kyberturvatoimenpiteiden vaikuttavuuden arvioimiseen. Lainsää-

däntö ei vaikuta pelkästään kriittiseen organisaatioon itseensä, vaan sitä sovelletaan lainsäädännön piirissä olevien toimijoiden koko toimitusketjuihin, eli organisaation vastuu ulottuu myös kumppaneihin. NIS2-direktiivin vaatimuksia voi siis kohdistua organisaatioihin joko suoraan, tai välillisesti. NIS2-direktiivin vaatimusten täyttäminen on oletusarvoisesti helpompaa, jos organisaatiolla on jokin tietoturvan hallintajärjestelmä, kuten ISO 27001 käytössään. Hallintajärjestelmästä huolimatta organisaatioiden on varmistettava vaatimusten täyttämisestä, sekä toteutettava tarvittavat ja riittävät toimenpiteet kybersietoisuuden ja operatiivisen riskienhallintakyvyn toteuttamisesta. Tämä tarkoittaa sitä, että sidosryhmillä on oltava riittävä tietoisuus, ymmärrys ja osaaminen. (Asikainen 2024.)

NIS2-direktiivi koskee kaikkia yli 10M€ liikevaihtoa tekeviä tai yli 50 henkeä työllistäviä yrityksiä, joiden tarjoamat palvelut ovat Euroopan taloudelle tai yhteiskunnalle tärkeitä. Myös EU:n ulkopuolella toimivat organisaatiot ovat direktiivin piirissä, jos ne tarjoavat palveluita EU:n sisällä toimiville organisaatioille. Direktiivissä on poikkeuksia pienille organisaatioille, mutta suuret organisaatiot tulevat todennäköisesti vaatimaan myös pieniltä toimijoilta samoja vaatimuksia, joita direktiivi edellyttää suuremmilta toimijoilta. Tämän vuoksi myös pienempien organisaatioiden olisi hyvä valmistautua ja noudattaa direktiivin vaatimuksia pystyäkseen kilpailemaan muiden kanssa. (OKTA 2023b, 4.)

NIS2-direktiivi edellyttää riskien vähentämiseksi sen alaisten tahojen toteuttavat oikeasuhteisia ja asianmukaisia toimenpiteitä sekä teknisesti, että organisatorisesti, verkko- ja tietojärjestelmien sekä fyysisen ympäristön osalta mukaan lukien datakeskukset. Viranomaisille raportointi tietoturvaloukkauksista on myös vaadittu osa NIS2-direktiiviä. Raportointivaatimukset digitaalisia palveluita ja infrastruktuuria tarjoavien osalta ovat myös tiukempia kuin muilla. (OKTA 2023b, 4.)

OKTA on luonut tarkistuslistan NIS2-vaatimustenmukaisuuden tarkistamiseksi ja sieltä löytyy myös identiteetin- ja pääsynhallintaan liittyen huomioitavia kohtia. Kohta kaksi on tiukenna pääsynhallintaa. Tämä tulisi toteuttaa estämällä luvattomat pääsyt kaikkiin järjestelmiin ja eri käyttäjätileihin. Toimenpide on äärimmäisen ratkaisevassa roolissa, kun halutaan estää tietomurtoja. Tämä voidaan toteuttaa käyttämällä identiteettien hallintaan alustaa, jolla voidaan

keskitetysti hallita käyttäjiä ja joka mahdollistaa tarkkojen, yksityiskohtaisten valtuuskäytäntöjen määrittämisen. Ainoastaan niiden henkilöiden, joilla oikeasti tulee olla oikeus käyttää järjestelmiä tai resursseja ja suorittaa toimintoja, tulee sallia järjestelmiin ja sovelluksiin, kaikkien muiden toiminta tulee estää. Avaintekijänä tässä on siis ottaa käyttöön vahva identiteetinhallinta, jotta voidaan tiukentaa pääsynhallintaa. Kohdassa kolme puhutaan, kuinka hallintatunnusten käytönhallinta (Privileged Access Management, PAM) tulisi suojata. Hyökkääjät pyrkivät hyödyntämään tällaisia tilejä käynnistääkseen hyökkäyksiä, kaataakseen kriittistä infrastruktuuria ja häiritäkseen olennaisia palveluita. Suojaaminen saadaan toteutettua rajoittamalla järjestelmänvalvojan tilejä ja vaihtamalla näiden salasanoja säännöllisesti. Avaintekijänä tässä on hyödyntää vähimpien oikeuksien mallia. Neljännessä kohdassa mainitaan, että käyttöön tulisi ottaa kalastelulta suojattu monivaiheinen tunnistautuminen. Sosiaalista manipulointia hyödyntävät hyökkäykset ovat lisääntyneet ja lisääntyvät päivä päivältä, ja tämän takia NIS2 vaatii organisaatioita ottamaan käyttöön kalastelulta suojatun monivaiheisen tunnistautumisen (MFA). Näin voidaan tarjota ylimääräinen suojakerros tunnistautumiseen työntekijöille, asiakkaille ja muille osapuolille, vaikeuttamatta kuitenkaan itse todentamisprosessin käyttäjäkokemusta. Muissa kohdissa mainitaan muun muassa uudelleen vähimpien oikeuksien periaate ja nollaluottamuksen periaate (Zero Trust), jotka molemmat ovat olennaisia osia identiteetin- ja pääsynhallintaa. Identiteetin mainitaan myös olevan peruskivi kriittiseen tietoon pääsyssä. Oikein rakennetulla identiteetinhallinnalla organisaatioilla on mahdollisuus suorittaa pääsynhallintaa, vahvistaa tunnistautumista ja luoda näkyvyys kokonaisuuteen luotettavan kirjausketjun (audit trail) avulla. (OKTA 2023a.)

Ennen lakien voimaan astumista organisaatioiden olisi hyvä alkaa valmistautua. Valmistautumista voi suorittaa identiteetin- ja pääsynhallinnan osalta muun muassa:

- tunnistamalla, arvioimalla ja käsittelemällä riskejä
- arvioimalla tietoturvan tämänhetkistä tasoa
- hallintatunnusten katselmoinnilla
- nollaluottamuksen (Zero Trust) periaatteella.

Verkko- ja tietojärjestelmiin sekä fyysiseen ympäristöön liittyvät riskit tulisi tunnistaa ja pyrkiä minimoimaan näiden riskien toteutumista. Eli luoda toimenpiteet, joilla löydettyihin riskeihin pystytään vastaamaan. Tulisi havaita esimerkiksi tunnukset, joiden salasanoja ei ole vaihdettu, sekä liiallisilla oikeuksilla

määritetyt tai passiiviset tilit. Hallintatunnusten käyttöä tulisi rajoittaa sekä pakottaa näille salasanojen vaihtaminen. Määrittää käyttöön vähempien oikeuksien periaate kaikille tileille, ottaa käyttöön kalastelun kestävät tunnistautumismenetelmät sekä nollaluottamuksen (Zero Trust) periaate. Näin saadaan aikaan monikerroksinen tietoturvallinen ratkaisu, joka lähtökohtaisesti jo pienentää riskejä kokonaisuudessaan. (OKTA 2023b, 5–6.)

Turvallisuuden hallinta on vaikeaa, koska siihen liittyy monimutkaisessa vuorovaikutuksessa teknologia, ihmiset ja prosessit. Identiteetillä on tässä kokonaisuudessa ratkaiseva rooli kyberturvallisuusstrategioiden, kyberhygienian ja regulaatioiden kuten NIS2:n vaatimusten täyttämisessä. Identiteetti toimii perustana, jonka päälle voidaan rakentaa tietoturvapolitiikat, erilaiset toimintatavat ja IT-järjestelmät, joiden kautta voidaan määrittää pääsy esimerkiksi kriittistä tietoa sisältäviin järjestelmiin. Sillä pystytään todentamaan käyttäjien identiteetit, käyttöoikeudet, pääsynhallinta sekä valtuutukset. Hyvin rakennetulla identiteetinhallintajärjestelmällä pystytään varmistamaan, että ainoastaan valtuutetuilla henkilöillä on pääsy heidän tarvitsemiinsa resursseihin ja siten, että käytössä on myös vähimpien oikeuksien periaate, eli mitään ylimääräisiä oikeuksia henkilöillä ei ole. Monivaiheisella tunnistautumisella voidaan myös saada entisestään lisäturvaa identiteettien suojaamiseen. Identiteetinhallinnalla pystytään helpottamaan NIS2 vaatimusten täyttämistä seuraavilla keinoilla:

1. Pääsynhallinta. Oikein määritetyt ja hallitut yksilölliset identiteetit varmistavat, että vain valtuutetut käyttäjät voivat suorittaa toimenpiteitä, käyttää resursseja organisaation verkossa sekä tietojärjestelmissä.

2. Todennus ja valtuutus. Ennen käyttöoikeuksien myöntämistä voidaan vaatia monivaiheista tunnistautumista, joka varmistaa identiteetin omistajuuden sitä käyttävälle henkilölle. Todennuksen ja valtuutuksen avulla organisaatio voi myös määrittää tarvittaessa erittäin tarkkoja valtuuskäytäntöjä. Näin voidaan varmistaa, että käyttäjällä on vain roolin ja vastuun mukaiset oikeudet.

3. Häiriöiden hallinta. Identiteetinhallinnalla on keskeinen rooli tietoturvahäiriöiden tapahtuessa. Tällaisen tapahtuman yhteydessä oikein hallittujen identiteettien avulla voidaan seurata ja jäljittää järjestelmissä tapahtuneita tapahtumia ja näin ollen auttaa häiriöiden selvittelyssä, löytää mahdollisesti syitä miksi näin kävi ja korjata löydetyt ongelmakohdat.

4. Vaatimustenmukaisuuden valvonta. Verkko- ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi NIS2 edellyttää organisaatioilta toimenpiteitä. Identiteettienhallinnalla avulla on mahdollista näyttää toteen, kuka on käyttänyt järjestelmää, milloin järjestelmää on käytetty ja minkälaisilla oikeuksilla järjestelmään on käytetty. Hallintajärjestelmästä on myös mahdollista ottaa raportti edellä mainituista asioista ja näin saadaan aikaan myös tarvittava dokumentaatio tapahtumista.

(OKTA 2023b, 7–8.)

Jos toimija jättää noudattamatta NIS2-direktiivin määrittämiä asetuksia, sille voidaan määrätä hallinnollisia sakkoja. Sakkojen määrä määräytyy toimijan toimialasta ja kriittisyydestä riippuen. Sakot erittäin kriittisten toimijoiden osalta ovat 10M€ tai 2 % globaalista liikevaihdosta, sen mukaan kumpi on suurempi. Sakko kriittisten toimijoiden osalta on 7M€ tai 1,4 % globaalista liikevaihdosta, sen mukaan kumpi on suurempi. Lisäksi toimijat, jotka eivät noudata NIS2-direktiiviä voivat menettää kokonaan toimintaedellytyksenä sekä organisaation toimitusjohtajalta voidaan estää hänen tehtävänsä hoitaminen. Tämä on määritetty 32 artiklan 5 kohdassa. (OKTA 2023b, 11.)

Toimijoilla on raportointivelvoite tietoturvahäiriöiden tapahtuessa viranomaiselle. Raportoinnille on määritetty aikarajat, joiden aikana raportoinnin tulee tapahtua. Ennakkoilmoitus viranomaiselle on toimitettava 24 tunnin kuluessa, siitä hetkestä, kun ensimmäisen kerran on saatu tieto häiriöstä. 72 tunnin kuluessa viranomaiselle on ilmoitettava mistä häiriöstä on kyse, mikä on häiriön vakavuus ja minkälaisia vaikutuksia häiriöllä on. Loppuraportti on toimitettava viranomaiselle 1 kuukauden kuluessa. (Kattainen 2023.)

# 4 STANDARDIT JA PARHAAT KÄYTÄNNÖT

Luku 4 kuvaa erilaiset standardit ja parhaat käytännöt, joiden avulla voidaan toteuttaa identiteetin- ja pääsynhallinnan prosesseihin ja käytäntöihin liittyvät toimet.

## 4.1 NIST

NIST on tuottanut julkaisun NIST Digital Identity Guidelines (SP 800-63). Kyseinen julkaisu pitää sisällään 4 osaa. Nämä osat ovat:

- Perusosa, digitaalinen identiteettimalli ja riskienhallinta

- Osa A, henkilöllisyyden todistaminen ja kirjautuminen
- Osa B, autentikaatio ja elinkaarenhallinta
- Osa C, federaatiot ja hyväksynnät.

Dokumentaatiossa kuvatut henkilöllisyyden varmistamisen osat ovat:

IAL, jolla viitataan henkilöllisyyden todentamisprosessiin

AAL, jolla viitataan todennusprosessiin

FAL, jolla viitataan vahvistusprotokollaan, jota käytetään federoidussa ympäristöissä todennus- ja attribuuttitietojen (jos saatavilla) viestintään.

(Grassi ym. 2017, 2–3.)

Viimeisin merkittävä versio (SP 800-63-3) on tullut ulos kesäkuussa 2017 ja parhaillaan on menossa isompi päivitys tähän julkaisuun liittyen. Vuodesta 2017 maailma on muuttunut tälläkin osa-alueella aika paljon ja sen takia päivitys on aiheellinen (NIST 2023, 11–12). Päivitetty julkaisu on valmistumassa tämän hetken tietojen mukaan vuoden 2024 toisella kvartaalilla (NIST 2020).

Tunnistautumisen toiminnan kulmakiviksi klassinen ajattelutapa määrittelee kolme tekijää:

- Jotain mitä tiedät (esimerkiksi salasana tai PIN-koodi)
- Jotain mitä sinulla on (esimerkiksi ID-kortti tai salausavain)
- Jotain mitä olet (esimerkiksi sormenjälki tai jokin muu biometrinen tieto).

Yksivaiheisessa tunnustautumisessa (single-factor authentication) vaaditaan yksi edellä mainituista tekijöistä, useimmiten se on jotain mitä tiedät, esimerkiksi salasana. Jos käytetään useampaa saman tekijän tietoa, kuten esimerkiksi PIN-koodia ja salasanaa, tämä ei täytä monivaiheista tunnistautumista (multi-factor authentication), koska molemmat tekijät ovat jotain mitä tiedät. Monivaiheiseen tunnistautumiseen vaaditaan useamman kuin yhden tekijän käyttämistä. Eli esimerkiksi PIN-koodi (jotain mitä tiedät) ja sormenjälki (jotain mitä sinä olet) yhdessä toteuttavat monivaiheisen tunnistautumisen. Monivaiheisella tunnistautumisella pystytään täyttämään korkeampia turvallisuusvaatimuksia, kuin yksivaiheisella tunnistautumisella. Mitä useampia menetelmiä käytetään, sen varmempia voidaan olla todennuksen oikeellisuudesta. (Grassi ym. 2017, 12.)

AAL kuvaa todennusprosessin vahvuutta. AAL1 on yksivaiheinen tunnistautuminen ja se pystytään toteuttamaan periaatteessa millä tahansa autentikointitekijällä. AAL2 on monivaiheinen tunnistautuminen, jossa vaaditaan kaksi eri autentikointitekijää ja se on turvallisempi kuin yksivaiheinen tunnistautuminen. AAL3 on korkein taso ja se vaatii yleensä jonkinlaisen laitteistopohjaisen autentikaattorin käyttämisen ja lisäksi todentajan henkilöllisyys tulee pystyä varmistamaan luotettavasti. (Grassi ym. 2017, 10.)

### 4.2 ISO 27001 ja ISO 27002

ISO 27000 -sarjan keskeisin viitekehys on ISO 27001. Sarjaan sisältyy useampia dokumentteja, joista jokainen kuvaa jonkin tietoturvanhallinnan osa-alueen ja siihen liittyviä kontrolleja. ISO 27001 – standardi kuvaa parhaat käytännöt tietoturvan hallintajärjestelmälle (ISMS), toteutusvaatimukset, sekä tiedon siitä, mitä tulee tehdä, jotta standardin vaatimustenmukaisuus voidaan täyttää.

ISO 27002 on laajennus ISO 27001 – standardiin ja siinä on kuvattu tietoturvan valvontaan liittyvät hallintatoimenpiteet. Nämä samat toimenpiteet ovat lueteltuina myös ISO 27001 – standardin liitteessä A, mutta siellä niitä on kuvattu vain muutamilla virkkeillä. ISO 27002 – standardissa nämä asiat on avattu noin sivun mittaisilla kuvauksilla siitä, miten toimenpiteet toimivat, mikä niiden tavoite on ja kuinka ne voidaan ottaa käyttöön. (Irwin, 2019.)

ISO 27001 ja ISO 27002 eroavat toisistaan kolmella merkittävällä tavalla. Tarkkuustaso ISO 27001:ssä ei ole samaa luokkaa, kuin ISO 27002:ssa. Tämä johtuu siitä, että jos kaikki tiedot olisi viety yhtä tarkalle tasolle, siitä olisi tullut liian monimutkainen ja vaikeasti ymmärrettävä. ISO 27001 pitää sisällään yleiskuvauksen jokaiseen ISMS:n osa-alueeseen ja tarkemmat tiedot löytyvät lisästandardeista. Sertifiointi voidaan suorittaa ISO 27001 -standardia vasten, mutta ISO 27002:lle ei ole sertifiointia. Tälle syynä on se, että ISO 27002 on lisästandardi ja pitää sisällään vain yhden tietyn osa-alueen näkökannan ja ISO 27001 on hallintastandardi ja pitää sisällään täyden listan niistä vaatimuksista, jotka sen täyttämiseksi vaaditaan. (Irwin, 2019.)

ISO 27001 kuvaa, miten tietoturvallisuuden hallintajärjestelmä luodaan, toteutetaan, ylläpidetään ja miten sen jatkuvasta parantamisesta huolehditaan.

Näin voidaan varmistaa tiedon luottamuksellisuus, eheys ja saatavuus. Lisäksi voidaan näyttää sidosryhmille, että riskit ovat asianmukaisesti hallittuja. Hallintajärjestelmän osalta on määritettävä olennaiset sidosryhmät ja heidän vaatimuksensa, sekä mihin näistä vaatimuksista hallintajärjestelmä tulee vastaamaan. Jos hallintajärjestelmän luomiseen ja ylläpitämiseen ei ole ylimmän johdon sitoutumista on käytännössä turha lähteä hallintajärjestelmää rakentamaan. Sen ylläpitäminen vaatii kuitenkin muun muassa resursseja, linkitystä organisaation prosesseihin, tietoturvapolitiikan määrittämisen ja jatkuvaa parantamista ja nämä ovat ilman johdon tukea ja sitoutumista vaikeasti saavutettavissa. (SFS-EN 27001:2023, 6–8.)

ISO 27002 - standardi (SFS-EN 27002:2022) pitää sisällään organisaatiota, henkilöstöä, fyysisiä ja teknologisia hallintakeinoja koskevia kuvauksia. Näistä organisaatioon liittyvissä hallintakeinoissa on osioita, jotka koskevat myös identiteetin- ja pääsynhallinnan osa-alueita. Muun muassa pääsynhallinnalle, identiteetinhallinnalle, pääsyoikeuksille ja ylläpito-oikeuksille on omat lukunsa. Näitä on avattu tarkemmin tämän opinnäytetyön myöhemmissä luvuissa. (SFS-EN 27002:2022, 17.)

Instant 27001 -niminen organisaatio on luonut taulukon, jonka avulla voidaan NIS2:n artiklan 21 vaatimukset yhdistää ISO 27001-standardiin (liite1.) ISO 27001 sertifikaatti ei ole edellytys täyttää NIS2 vaatimuksia, mutta se voi auttaa NIS2 vaatimusten täyttämisessä. (Instant27001.)

Pelkästään teknologian avulla saavutettavalla tietoturvalla on rajansa ja sitä tulisikin laajentaa erilaisilla prosesseilla sekä hallinnollisilla menettelyillä, kuten erilaisilla politiikoilla. Tietoturvallisuuteen liittyvillä vaatimuksilla on kolme päälähdettä. Ensimmäisenä lähteenä on riskien arviointi, jossa tulee huomioida sekä organisaation liiketoiminnan yleiset tavoitteet, että liiketoimintastrategia. Tästä olisi saatava lopputuloksena hallintakeinot, joilla riskejä voidaan hallita, sekä hyväksymiskriteerit, joiden avulla jäännösriskit voidaan hyväksyä. Lait, asetukset, viranomaismääräykset sekä erilaisten sopimusten kautta tulevat vaatimukset ja niiden täyttäminen toimivat toisena lähteenä. Viimeinen lähde liittyy organisaation omaan toimintaansa kehittämät periaatteet, liiketoimintavaatimukset sekä tavoitteet, jotka koskevat tiedon elinkaarta ja sen kaikkia vaiheita. (SFS-EN 27002:2022, 7–8.)

ISO 27002 tarjoaa organisaatioiden käyttöön hallintakeinoja, joilla riskiä voidaan muuttaa tai säilyttää riski. Hallintakeinot määritetään riskien arvioinnin jälkeen. Esimerkkinä voidaan pitää vaikka tietoturvapolitiikkaa, jos vain luodaan tietoturvapolitiikka, niin riskit eivät muutu mihinkään, mutta kun tietoturvapolitiikkaa aletaan toteuttaa, saadaan riskiä muutettua. Eli jalkauttaminen on tietoturvapolitiikan kohdalla äärimmäisen tärkeää. Keinoja määritettäessä on huomioitava kaikki kansainväliset ja kansalliset lait ja asetukset, jotka ovat voimassa. ISO 27002 voidaan pitää pohjana, kun lähdetään määrittämään organisaatiokohtaisia ohjeita, mutta kaikkia siinä määritettyjä asioita ei kuitenkaan voida kaikissa organisaatioissa hyödyntää. (SFS-EN 27002:2022, 8.)

Jos halutaan ottaa käyttöön tietoturvanhallintajärjestelmä, tulisi käydä läpi ISO 27001 sisältö ja poimia sieltä oman organisaation toimintaan oleellisesti liittyvät osat ja keskittyä niihin. ISO 27002 kannattaa käydä läpi sen jälkeen, kun on tunnistettu ne käytännöt, joita halutaan lähetä toteuttamaan ja katsoa miten nämä saadaan toteutettua. (Irwin, 2019.)

### 4.3 Parhaat käytännöt

Identiteetin- ja pääsynhallinnan saralla on julkaistu monenlaisia parhaita käytäntöjä pääsääntöisesti eri IdM- / IAM-järjestelmiä tuottavien yritysten toimesta. Parhaita käytäntöjä on julkaistu myös eri pilvipalveluiden tuottajien toimesta, kuten Microsoftin, Googlen ja Amazonin. Parhaat käytännöt pyrkivät vastaamaan laissa, direktiiveissä ja suosituksissa määritettyihin asioihin ja antamaan ohjeet ja toteutustavat, miten nämä vaatimukset voidaan täyttää tai vaihtoehtoisesti kuvaamaan parhaat käytännöt jonkin alustan suojaamiseen. Parhaat käytännöt ovat yleensä jonkin tahon subjektiivinen näkemys aiheeseen, eikä se välttämättä kuitenkaan ole se paras tapa toteuttaa tietoturvaa, eli näiden osalta tulee olla hyvinkin kriittinen. Tässä opinnäytetyössä on paneuduttu Sailpointin, One Identityn ja Veritiksen tekemiin parhaisiin käytäntöihin. Kaikilla kolmella taholla on hyvinkin samankaltaisia havaintoja, mutta myös eroja löytyy.

### 4.3.1 Sailpoint

Sailpoint on julkaissut vuonna 2022 seitsemän kohdan parhaat käytännöt listan. Listan avulla voidaan määrittää identiteetin- ja pääsynhallinnan strategia. Aluksi tulisi kuvata tavoitetila, johon pyritään. Ellei tavoitetilaa ole määritetty, ei voida tietää mihin ollaan matkalla. Kaikki korkean riskin järjestelmät pitäisi saada tavalla tai toisella kokonaan poistettua ympäristöstä tai vähintäänkin minimoitua riskiä näissä järjestelmissä. Riskiä saadaan pienenettyä haavoittuvuuksien hallinnalla, kryptaamisella, segmentoinnilla, erilaisilla integraatioilla, sekä oikein toteutetulla pääsynhallinnalla. (Sailpoint, 2022.)

Työsuhteen aloittamiseen (onboarding) ja lopettamiseen (offboarding) liittyvät prosessit tulisi automatisoida. Nämä prosessit tulisi olla määritettyinä sekä organisaation sisäisille että ulkoisille toimijoille. Automatisointia helpottaa, jos voidaan luoda erilaisia rooleja, joiden perusteella oikeuksia järjestelmiin annetaan. Yksittäinen rooli voi sisältää oikeuksia moniin eri järjestelmiin. Roolit tulisi luoda niin, että ne eivät sisällä ylimääräisiä oikeuksia. Joidenkin järjestelmien osalta automatisointi voi olla hankalaa, jopa mahdotonta, mutta silti tulisi käyttää etukäteen sovittuja prosesseja myös näihin manuaalisen provisioinnin piirissä oleviin järjestelmiin. Automaatiolla voidaan säästää sekä aikaa että rahaa, ja lisäksi myöskään orpotilejä ei jää ympäristöihin. Ellei automaatiota ole käytettävissä, tulisi jatkuvasti tarkastaa, ettei järjestelmiin jää orpotilejä. Nämä ovat hakkereille todellisia kultakaivoksia, kun vanhat käyttämättömät tilit jäävät lojumaan järjestelmiin ja odottamaan jonkin pahantahtoisen tahon hyödyntävän näitä. (Sailpoint 2022.)

Nollaluottamuksen (Zero Trust) periaate tulisi ottaa osaksi toimintaa. Kaikki toimet pitäisi aina varmistaa, ja oikeuksia tulisi olla vain juuri sen verran, että niillä työnteko mahdollistuu, ei yhtään ylimääräistä. Tekoäly (AI) ja koneoppiminen (ML) pitäisi saada käyttöön myös identiteetin- ja pääsynhallinnan toimenpiteisiin. Uusien työskentelytapojen, uusien sovellusten ja digitaalisen transformaation myötä IT:n alkaa olla perinteisin menetelmin mahdotonta pysyä perässä muun muassa siitä, mistä kaikkialta ihmiset voivat järjestelmiin kirjautua, ja millä laitteilla kirjautumiset tapahtuvat. Tekoälyä ja koneoppimista

voidaan myös käyttää automatisoinnissa sekä erilaisten päätösten tekemisissä, kuten käyttöoikeuspyyntöjen ja roolimallien yksinkertaistamisessa. (Sailpoint 2022.)

Kun toiminta on muuttunut ja kasvanut räjähdysmäisesti käyttäjien, järjestelmien, sovellusten, tietokantojen ja datan osalta, tulisi identiteettien osalta olla riittävä näkyvyys kaikkiin tapahtumiin. Identiteetin- ja pääsynhallinnan osalta pitäisi siis pystyä luomaan 360-näkymä, jonka avulla voidaan nähdä reaaliaikaisesti, mitä ympäristössä tapahtuu, mitä resursseja ja sovelluksia käytetään, kuka niitä käyttää, ja onko käyttäjien toiminnassa poikkeamia normaaliin. (Sailpoint 2022.)

Suurimmat haasteet identiteetin- ja pääsynhallinnan projekteissa ovat yleisesti muun muassa johdon tuen ja rahoituksen puute, käyttäjien osallistamatta jättäminen, heikko kommunikointi projektin hyödyistä ja huono ymmärrys kokonaisuudesta. Oikein ja hyvin toteutetun identiteetin- ja pääsynhallinnan ratkaisun arvon ymmärtäminen on yksi tärkeimmistä asioista, jotta projektit tällä alueella voivat onnistua. Projektit kannattaa myös paloitella pienempiin osiin, eikä yrittää tehdä kokonaisuutta kerralla kuntoon. Ei myöskään saa tuudittautua siihen tunteeseen, että ensimmäisen käyttöönoton jälkeen kaikki olisi valmista. Identiteetin- ja pääsynhallinta on jatkuvasti muuttuva ja jatkuvaa panostusta vaativa äärimmäisen tärkeä kokonaisuus sekä kyberturvallisuuden onnistumisen, että riskien minimoimisen kannalta. (Sailpoint 2022.)

Vaikka teknologia voikin auttaa nopeuttamaan ja automatisoimaan identiteetin- ja pääsynhallinnan prosesseja sekä karsimaan kuluja, se ei voi ratkaista kaikkia ongelmia. Järjestelmästä ja sen toiminnallisuuksista tulisi jatkuvasti oppia lisää ja kehittää sekä hienosäätää pääsynhallinnan politiikkoja ja prosesseja. Täydellinen organisaation sitoutuminen on vaatimus identiteetin- ja pääsynhallinnan onnistumiselle. Tänä päivänä on välttämätöntä hoitaa kunnolla identiteetin- ja pääsynhallinnan prosessit, käytännöt, politiikat ja järjestelmät, jotta voidaan minimoida organisaation riskit tietomurroille ja kyberhyökkäyksille. Näin saadaan myös minimoitua näiden aiheuttamat vahingot organisaation arvolle, mainehaitoille, sekä toiminnalle. (Sailpoint 2022.)

### 4.3.2 One Identity

One Identityn mukaan identiteettien- ja pääsynhallinnan hallinta ei ole kertaalleen tehtävä asia, jonka voi sitten vain unohtaa. Se on kriittinen osa organisaation infrastruktuuria ja vaatii jatkuvaa ylläpitoa ja hallintaa. Identiteetin- ja pääsynhallinnan ei tulisi myöskään olla pelkästään IT:n asia, vaan IT:n tulisi vain ylläpitää sen hallintaan tarvittavia työkaluja ja muun organisaation tulisi oikeasti hallita identiteettejä. (One Identity 2022, 2.)

Henkilöstöhallinnon tulisi hallita sekä organisaation omien, että myös ulkoisten työntekijöiden, kuten konsulttien ja muun ulkoisen työvoiman tietoja. Lähestulkoon kaikki näistä ihmisistä tarvitsevat jonkinlaisia oikeuksia organisaation järjestelmiin. HR-järjestelmän tulisi sisältää mahdollisimman paljon tietoa näistä käyttäjistä ja sitä tulisi hyödyntää organisaation sisäisten työntekijöiden tietolähteenä identiteetin- ja pääsynhallinnan järjestelmälle. Ideaalissa tilanteessa pystytään tarjoamaan jonkinlainen portaali tietojen tarkastamiseen sekä korjaamiseen. (One Identity 2022, 2.)

Yhdellä integroidulla järjestelmällä tulisi hoitaa kokonaisvaltaisesti identiteetin- ja pääsynhallinnan toimenpiteet identiteettien koko elinkaaren ajalta. IT:n vastuu identiteetin- ja pääsynhallinnan osalta alkaa yleensä tästä kohtaa. Keskeiset järjestelmät tulisi tunnistaa ja liittää osaksi identiteetin- ja pääsynhallinnan järjestelmää. Yleensä käytössä on hakemistopalvelu, esimerkiksi Microsoft Active Directory, viestintäjärjestelmä kuten Exchange Server tai M365 ja toiminnanohjausjärjestelmä kuten SAP. Keskeisten järjestelmien tunnistamisen jälkeen ne liitetään osaksi identiteetinhallinnan arkkitehtuuria ja hallintaa. Näiden järjestelmien integroinnilla yleensä saavutetaan niin sanotut nopeat voitot, koska näiden järjestelmien käyttäjämäärät ovat suurimmat ja ne ovat eniten käytettyjä järjestelmiä. Muut järjestelmät voidaan integroida osaksi identiteetin- ja pääsynhallintaa myöhemmin. Taustalla jokaiseen näistä järjestelmistä voi olla käyttäjällä erilliset tunnukset, mutta integraatioiden avulla käyttäjä kokee käyttävänsä yhtä ja samaa identiteettiä kaikkiin järjestelmiin. (One Identity 2022, 2.)

Yleensä IT:n tulee vastata kysymykseen, ”Kenelle on oikeudet ja minne?”. IT koordinoi identiteettien- ja pääsynhallinnan tietoa ja tarjoaa näitä tietoja organisaation muille tahoille. Ajatuksena on tarjota keskitetty portaali, jonka kautta organisaation eri tahot voivat reaaliaikaisesti nähdä mitä oikeuksia käyttäjille on annettu ja tarvittaessa hakea uusia tai poistaa olemassa olevia oikeuksia. Portaalin kautta käyttäjät voivat pyytää lupaa niihin resursseihin, joihin heidän tulee päästä. Uusien oikeuksien hakemisessa tulisi hyödyntää työnkulkuja. Pyyntöihin voidaan määrittää erilaisia työnkulkuja tarpeiden mukaan. Jotkin pyynnöt voivat vaatia ensin esihenkilön hyväksynnän, ja sen jälkeen vielä järjestelmien omistajat voivat joko hyväksyä tai hylätä pyynnöt. Näin saadaan siirrettyä vastuuta pois IT:ltä sinne, minne se oikeasti kuuluisikin, eli järjestelmien omistajille ja liiketoiminnalle. Lisäksi voidaan määrittää erilaisia rooleja, joihin voidaan sitoa useampia pääsyoikeuksia. Myös näihin rooleihin voidaan määrittää erilaisia hyväksyntäketjuja tarpeiden mukaan. Talouteen liittyvät käyttöoikeudet ja roolit voivat vaatia huomattavasti tarkempia hyväksyntäketjuja, sekä hyväksyntää useammalta taholta, kuin vaikkapa koko organisaation laajuisen viestinnän toteuttaminen. (One Identity 2022, 3.)

Automatisoinnilla voidaan kustannuksia vähentää, mutta myös parantaa laatua sekä vähentää virheitä. Alkuun tulisi löytää ne järjestelmät, joiden automatisoinnilla voidaan vaikuttaa suurimpaan osaan käyttäjistä. Yleensä näitä ovat sähköposti, ERP ja tietokannat ja näiden pääsynhallinta. Ei sovi myöskään unohtaa organisaatiosta poistuvia tai tehtäviä vaihtavia käyttäjiä. Poistumisesta ja tehtävien muuttumisesta johtuvat prosessit ovat manuaalisesti toteutettuina monesti todella monimutkaisia sekä paljon aikaa vieviä tehtäviä. Kun käytetyimmät ja vaikuttavimmat järjestelmät on löydetty, tulisi keskittyä näiden osalta automatisoimaan joiner (uuden työntekijän), mover (tehtäviä vaihtavan) ja leaver (organisaatiosta poistuvan) identiteetin prosessit. Tämän jälkeen olisi hyvä ottaa mukaan esimerkiksi käyttäjätunnusten lukituksen avaaminen ja muita tehtäviä, joiden automatisoinnilla myös vähennetään manuaalista työtä sekä virheitä. (One Identity 2022, 3–4)

Identiteetin- ja pääsynhallinnan järjestelmällä voidaan myös vastata erilaisten lakien ja säädösten vaatimuksiin, sekä täyttää nämä vaatimukset ja näin ollen täyttää vaatimustenmukaisuus. Organisaation tulisi pystyä dokumentoimaan ja määrittämään ne roolit, joiden täytyy pystyä hallitsemaan tietoja, sekä myös

ne roolit, joilla tulee olla pääsy tarkastelemaan tämänhetkisiä valtuutuksia. Tähän liittyen tulisi määrittää säännöstö, jonka jokainen osuus on linkitettynä johonkin vastuulliseen rooliin. Turvallisuuden lisäämiseksi tulisi näiden sääntöjen tarkastaminen integroida osaksi identiteetin- ja pääsynhallinnan järjestelmää. Näin saadaan automatisoitua ja poistettua myös virheiden mahdollisuutta ja pystytään vastaamaan vaatimustenmukaisuuden vaatimuksiin. (One Identity 2022, 4.)

Tunnuksien ja käyttöoikeuksien uudelleensertifiointi on myös todella tärkeä ja turvallisuutta lisäävä osa identiteetin- ja pääsynhallintaa. Uudelleensertifiointi tarkoittaa sitä, että esihenkilöt, järjestelmien omistajat, ylläpitäjät, tietoturvapäälliköt tai muut valtuutetut tahot tarkastelevat myönnettyjä käyttöoikeuksia säännöllisesti. Näin voidaan varmistua siitä, että kenelläkään ei ole ylimääräisiä oikeuksia järjestelmiin. Tässä tulisi huomioida myös roolien tarkastaminen, eli käydä läpi olemassa olevat roolit ja rooleihin kohdistuvat käyttöoikeudet ja niiden ajantasaisuus. (One Identity 2022, 4.)

Ideaalissa tilanteessa kaikki pääsyoikeuksien hallinta tapahtuisi roolien kautta. Roolit tulisi saada vastaamaan oikeita työtehtäviä ja tehtävänimikkeitä. Alkuun tarvitsee tehdä mahdollisesti paljonkin inventointia ja työtä tärkeimpien roolien tunnistamiseksi sekä näiden oikeuksien määrittämiseksi. Kun tämä on saatu tehtyä, voidaan käyttäjille tarjota itsepalveluportaali, jonka avulla käyttäjä voi pyytää pääsyoikeuksia niihin tarpeisiin, joihin roolien kautta ei pystytä vastaamaan. Käyttäjän pyyntö sitten hyväksytään tai hylätään niiden tahojen toimesta, joille vastuu on määritetty. IT:n ei siis tarvitse olla tässä ketjussa mukana ollenkaan. Jokaiselle roolille tulee olla määritettynä omistaja tai omistajat, jotka voivat luoda uusia rooleja, muokata tai poistaa olemassa olevia rooleja. (One Identity 2022, 5.)

Oikealla työkalulla organisaatio voi täyttää edellä mainituista parhaista käytännöistä suurimman osan. Valitettavan usein organisaatiot eivät kuitenkaan näin toimi, vaan yrittävät hoitaa asian adhoc IAMin, kotikutoisten työkalujen ja kolmannen osapuolen työkalujen sekamelskalla. Näin monesti saadaan perustarpeet täytettyä, mutta ne täyttyvät turvallisuuden ja tehokkuuden kustannuksella. Tämä on toisaalta ymmärrettävää, koska kunnollisen identiteetin- ja pääsynhallinnan järjestelmän täydellinen käyttöönotto on kallis ja aikaa vievä

projekti. Monesti IT:n maturiteetti ohjaa identiteetin- ja pääsynhallinnan kyvykkyyksiä, ei se, mitä tarpeita organisaatiolla oikeasti olisi. (One Identity 2022, 5.)

### 4.3.3 Veritis

Organisaatioiden tulee sisällyttää identiteetin- ja pääsyhallinnan työkalut ja prosessit osaksi tietoturvasuunnitelmia. On olemassa toimenpiteitä, joita kaikkia organisaatioiden tulisi noudattaa hallitakseen identiteetin- ja pääsynhallinnan toimia. Identiteetin- ja pääsynhallinnan parhaita käytäntöjä noudattamalla organisaatiot voivat määrittää ketkä pääsevät arkaluonteisiin tietoihin ja milloin pääsy on mahdollista. Mahdollisten uhkien ja riskien toteutumisen varalta tulee olla kokonaisuuden kattava tieto organisaation IT-infrastruktuurista. Kaksi tärkeintä sisääntulokohtaa kaikkien kyberuhkien toteutumisessa ovat identiteetti ja pääsyoikeudet. Digitalisaation ja pilvipalveluiden käyttöönottamisen kasvu on entisestään kasvattanut näiden riskien konkretisoitumista. Identiteetin- ja pääsynhallinnan ratkaisuilla on myös mahdollista vastata erilaisiin vaatimuksiin, joita lait ja direktiivit asettavat. Identiteetin- ja pääsynhallinnan tulee olla osa tietoturvapolitiikkaa ja sillä, miten se sinne on määritettynä, on myös suuri vaikutus, miten mahdollisia riskejä saadaan minimoitua. (Veritis s.a.)

Identiteetin- ja pääsynhallinnan avulla helpotetaan digitaalisen identiteetin hallintaa ja voidaan määrittää, kenellä on pääsy esimerkiksi sensitiiviseen tietoon. Identiteetin- ja pääsyhallinnan apuna voidaan käyttää muun muassa kertakirjautumista (SSO). Kaksivaiheinen todennus, monivaiheinen todennus (MFA) ja hallintatunnusten hallinta (PAM) ovat muita teknologioita, joita voidaan hyödyntää. Identiteetin- ja pääsynhallinta on kaikenkokoisten organisaatioiden hyödynnettävissä. (Veritis s.a.)

Veritiksen mukaan ensimmäisenä tulisi määrittää selkeä visio identiteetin- ja pääsynhallinnalle. Identiteetin- ja pääsynhallinnan toteuttaminen ei voi onnistua ilman ymmärrystä siitä, miten teknologia ja liiketoimintaprosessit saadaan yhdistettyä toimimaan yhdessä ja kuinka niiden avulla voidaan hallita identiteettejä ja näiden pääsyä organisaation tietoon ja sovelluksiin. Alusta asti tulisi pyrkiä huomioimaan kaikki nykyiset ja tulevat tarpeet mahdollisimman tarkasti. Roolit käyttäjien ja sovellusten välillä tulisi määrittää erilaisten oikeuksien,

sääntöjen ja käytäntöjen suhteen. Pääsyoikeudet tulisi linkittää tehtäviin. Tulisi pyrkiä huomioimaan identiteetin- ja pääsynhallinnan tarpeet koko organisaation laajuisesti. (Veritis s.a.)

Seuraavaksi tulisi luoda vahva perusta identiteetin- ja pääsynhallinnan tekemiselle. Identiteetin- ja pääsynhallinnan teknologian tarjoamat ominaisuudet ja teknologian yhdistäminen muuhun olemassa olevaan teknologiaan tulisi varmistaa. Kaikki organisaation käytössä olevat sovellukset ja alustat tulisi arvioida riskien osalta. Arvioinnista tulisi käydä ilmi sovellusten ja alustojen versiot, käyttöjärjestelmät, kolmannen osapuolen sovellukset, mahdolliset räätälöinnit ja teknologiset rajoitukset sekä mahdollisuudet. (Veritis s.a.)

Tekeminen tulisi vaiheistaa. Vaiheistamisella voidaan välttää liiallinen monimutkaisuus IAM käyttöönotossa. Sidosryhmien tietoisuutta tulisi kasvattaa kouluttamalla heitä käyttöönotettavaan teknologiaan. Koulutukset tulisi räätälöidä eri tahojen tarpeisiin kohdistuviksi. IT:n osalta kouluttamisen tulisi olla erityisen syvällistä ja kaikkien IT:n tahojen tulisi ymmärtää mitä identiteetin elinkaaren eri vaiheissa tapahtuu ja on mahdollista tehdä. Koulutuksen ei tulisi olla kertaluontoista, vaan jatkuvaa ja sen tulisi olla yhtä-aikaista uusien kyvykkyyksien ja muuttuvien prosessien kanssa. (Veritis s.a.)

Identiteettiä tulisi alkaa pitää keskiössä suojaamisen osalta. Aiemmin verkonturvallisuus on ollut keskiössä, mutta nyt asiat ovat muuttuneet ja identiteetistä on tullut keskeinen osa turvallisuutta. Tämän muutoksen takana on muun muassa pilvipalveluiden räjähdysmäinen kasvu, sekä etätyökulttuurin muutos. Monivaiheinen tunnistautuminen on todella tärkeä osa identiteetin- ja pääsynhallintaa. Sen tulisi olla pakotettuna organisaation kaikille käyttäjille normaaleista käyttäjistä järjestelmänvalvojiin ja johtajiin saakka. Kertakirjautuminen mahdollistaa yhden identiteetin käyttämisen kaikkiin mahdollisiin palveluihin, sijaitsevatpa ne sitten pilvessä tai omassa konesalissa. Kertakirjautuminen tulisi myös olla käytössä kaikissa järjestelmissä, joihin se on mahdollista toteuttaa. Nollaluottamuksen (Zero Trust) käyttöön ottaminen vahvistaa turvallisuutta. Tässä mallissa kaikki autentikointiyritykset nähdään uhkana, kunnes ne on validoitu, tulevatpa ne organisaation sisäverkosta tai ulkoverkosta. (Veritis s.a.)

Salasanapolitiikan tulisi olla käytössä. Politiikan tulisi pitää sisällään asetukset, joilla voidaan varmistaa salasanojen olevan vahvoja, salasanat tulisi säännöllisesti vaihtaa, ne eivät myöskään saisi sisältää peräkkäisiä toistuvia merkkejä. Hallintatilien suojaaminen on äärimmäisen tärkeää organisaation turvallisuuden kannalta. Hallintatilien määrä tulisi rajoittaa mahdollisimman pieneksi ja ne tulisi pystyä eristämään riskien minimoimiseksi. Säännölliset auditoinnit pitäisi ottaa käyttöön, jotta voidaan varmistua siitä, että ainoastaan tarvittavilla henkilöillä on tarvittavat oikeudet. Monesti käyttäjät myös pyrkivät hakemaan lisää oikeuksia helpottaakseen töidensä hoitamista, vaikka näille ei oikeasti olisi edes tarvetta. Auditoinneilla tällainen toiminta pystytään huomaamaan ja siihen voidaan puuttua. (Veritis s.a.)

Yksi kyberrikollisten käyttämistä keinoista päästä sisään järjestelmiin ja verkkoon ovat heikot tai toistuvasti käytetyt salasanat. Tätä riskiä vastaan voidaan suojautua salasanattomalla kirjautumisella. Käyttöönotto voidaan toteuttaa monella tavalla, muun muassa biometrisellä tunnistautumisella, SMS-pohjaisella tai sähköpostipohjaisella kirjautumisella. (Veritis s.a.)

# 5 IDENTITEETIN- JA PÄÄSYNHALLINNAN VAATIMUKSET

Yleisenä lähtökohtana voidaan todeta, että kaikkien hallintakeinojen osalta tulee varmistaa lakeihin, asetuksiin ja viranomaismääräyksiin liittyvien vaatimusten noudattaminen. Organisaation tulee viestiä toimintaperiaatteet ja laaditut politiikat kaikille tärkeimmille sidosryhmille. Näin voidaan pyrkiä varmistaa tietoturvan säilyminen ja riskien minimointi kaikissa tapauksissa.

## 5.1 Tietoturvapolitiikka

Identiteetin- ja pääsynhallinta on myös äärimmäisen tärkeä osa tietoturvapolitiikkaa ylätasolla. Tämän lisäksi olisi hyvä olla määritettynä erillinen identiteetin- ja pääsynhallinnan politiikka, joka määrittää tarkemmalla tasolla tähän liittyvät prosessit, toimintaperiaatteet ja vastuut.

Ylimmän johdon hyväksymät tietoturvapolitiikka ja toimintaperiaatteet tulee määrittää. Tietoturvapolitiikka ja toimintaperiaatteet tulee säännöllisin aikavälein katselmoida ja aina, kun tulee merkittäviä muutoksia ympäristöön, ne tulee päivittää. Ylimmän johdon tulee myös hyväksyä aina kaikki muutokset,

jotka politiikkaan tehdään. Kun tietoturvapolitiikka ja toimintaperiaatteet on määritetty, ne tulee viestiä henkilöstölle ja sidosryhmille. Olisi myös hyvä olla jonkinlainen mekanismi, jolla voidaan varmistaa, että tieto on jalkautunut. (SFS-EN 27002:2022, 19.)

Tietoturvapolitiikan tulisi johtaa organisaation liiketoimintastrategiasta ja erilaista liiketoiminnan vaatimuksista. Siinä tulee huomioida myös lainsäädäntö, viranomaismääräykset sekä organisaation sopimuksista tulevat vaatimukset. Politiikan tulisi sisältää määritelmä tietoturvallisuudelle. Minkälaisiin vaatimuksiin politiikka pyrkii vastaamaan. Politiikasta tulisi löytyä periaatteet, joiden perusteella kaikki tietoturvaan liittyvä toiminta on organisoitu. Miten organisaation on sitoutunut hallintajärjestelmän jatkuvaan parantamiseen sekä tietoturvallisuuden vaatimusten täyttymiseen. Roolit, jotka ovat vastuussa tietoturvaan hallintaa liittyvien asioiden hoitamiseen, tulisi olla määritettyinä. Kaikki prosessit, joiden avulla käsitellään poikkeamat ja poikkeukset tulee myös määrittää. (SFS-EN 27002:2022, 19.)

Tietoturvapolitiikan lisäksi tulisi määrittää alemman tason toimintaperiaatteita tai politiikkoja, joilla täydennetään tietoturvapolitiikassa määritettyjä asioita. Näitä toimintaperiaatteilla pystytään vastaamaan organisaation eri kohderyhmien tarpeisiin ja ne määrittävät tarkemmat toimenpiteet ja hallintakeinot. Näiden toimenpiteiden ja hallintakeinojen tulee olla linjassa tietoturvapolitiikan kanssa, ja ne täydentävät tarkemmalla tasolla tietoturvapolitiikassa määritettyjä periaatteita. (SFS-EN 27002:2022, 19.)

### 5.2 Identiteetinhallinta

Koko identiteetin elinkaari tulee pystyä hallitsemaan. Näin voidaan tunnistaa organisaation tietoja käyttävät henkilöt ja järjestelmät sekä näiden pääsyoikeuksien oikeanlainen hallinta. Yksittäinen käyttäjätunnus on sidottava vain yhteen henkilöön, joka on vastuussa kaikesta tällä identiteetillä tehtävistä toimenpiteistä. Yhteiskäyttötunnuksia ei tulisi olla, ellei ole jotain liiketoiminnallista tarvetta tai toiminnallista syytä, jonka takia henkilökohtaista tunnusta ei ole mahdollista käyttää. Tällöinkin tulee dokumentoida ja erikseen hyväksyttää yhteiskäyttötunnuksen luonti ja sille määritettävät käyttöoikeudet. Palvelutunnuksille tulee myös olla prosessi, kuinka niitä hallitaan. Tämän prosessin tulisi

olla erillään muiden tunnusten hallitsemisprosesseista. Käyttöoikeudet tulee poistaa heti tai tunnus tulee lukita, kun tarvetta käytölle ei enää ole olemassa. Organisaation tulisi myös määrittää tukiprosessi, jossa on kuvattu, kuinka identiteetteihin liittyvät muutokset käsitellään ja miten esimerkiksi luotettavasti tunnistetaan muutoksia pyytävä henkilö. (SFS-EN 27002:2022, 38–39.)

Identiteettien luomiseen liittyy monia toimenpiteitä, joiden perusteella voidaan tehdä päätös identiteetin myöntämisestä tai hylkäämisestä. Pyynnöllä tulisi olla jonkinlaiset liiketoiminnalliset tarpeet. Sähköistä identiteettiä hakevan henkilön identiteetti tulisi tarkistaa. Jos kaikki on kunnossa ja hyväksyntäprosessista on tullut myöntävä päätös, tulisi olla prosessi, kuinka sähköinen identiteetti luodaan ja mitä mahdollisia perusoikeuksia kaikille sähköisille identiteeteille määritetään. Myös sähköisten identiteettien perumisella ja poistamisella tulisi olla prosessit määritettynä. (SFS-EN 27002:2022, 39.)

### 5.3 Pääsynhallinta

Luvallinen pääsy tietoihin tulee varmistaa ja luvaton pääsy estää. Tähän liittyy sekä fyysisen, että ohjelmallisen pääsyn hallinta. Tiedon omistajan tulisi määrittää pääsynhallintaan liittyvät tietoturvallisuutta sekä liiketoiminnallisia vaatimuksia koskevat toimintaperiaatteet ja viestiä nämä kaikille oleellisille sidosryhmille. Vaatimusten ja periaatteiden tulisi huomioida seuraavia asioita:

- ketkä tarvitsevat pääsyn ja minkälaisia oikeuksia tulee määrittää
- *sovellusten turvallisuus*
- fyysinen turvallisuus, jota tuetaan kulunvalvonnalla
- kuinka tietoa saa jakaa, ja miten tiedon luokittelu vaikuttaa vaatimuksiin
- hallintaoikeuksien rajoittaminen
- *tehtävien eriyttäminen ja jääviys*
- sopimuksista, lainsäädännöstä ja viranomaismääräyksistä tulevat velvoitteet
- oikeuksien hakemisen, myöntämisen ja hallinnoinnin eriyttäminen
- oikeuspyyntöjen hyväksymismenettelyn noudattaminen
- *pääsyoikeuksien hallinta*
- *lokikirjaukset.*

(SFS-EN 27002:2022, 36–37.)

## 5.4 Pääsyoikeudet

Pääsyoikeuksien myöntämiselle ja poistamiselle tulee olla määritettynä prosessit. Prosessien tulee sisältää myöntämisen osalta erilaisten hyväksyntäketjujen kautta saatava hyväksyntä pääsyoikeuksien myöntämiselle. Tietojen omistajilta tai johdolta tulee saada hyväksyntä oikeuksien myöntämiseen. Tässä tulee huomioida myös roolien eriyttäminen oikeuksien hyväksynnän ja toteuttamisen suorittamisen osalta. Oikeuksia ei tulisi myöskään aktivoida, ennen kuin koko hyväksyntäketju on hyväksytysti saatu prosessin mukaisesti loppuun. Vaikka pääsyoikeuksien myöntäminen kloonaamalla on tietyllä tapaa helppo ja tehokas tapa, ei näin kuitenkaan tulisi toimia. Kloonaamisella monesti annetaan liikaa pääsyoikeuksia, eikä näin ollen toteuteta vähimpien oikeuksien periaatetta. Organisaatiolla tulisi myös olla keskitetty rekisteri, josta voidaan nähdä kaikki myönnetyt pääsyoikeudet. (SFS-EN 27002:2022, 41–43.)

Oikeudet tulisi poistaa välittömästi kaikilta käyttäjiltä, jotka eivät enää ole organisaation palveluksessa. Jos on tiedossa, että työsuhteisiin on tulossa muutoksia irtisanomisten tai organisaatiomuutosten myötä, olisi hyvä jo etukäteen katselmoida, mikä on syynä työsuhteen muutokselle ja mistä aloite tähän on tullut. Minkälaiseen omaisuuteen käyttäjällä on pääsy ja mitkä ovat käyttäjän vastuut. Varsinkin organisaation toimesta päättyvien tai muuttuvien työsuhteiden osalta tulisi tarkastella pääsyoikeudet ennen kuin käyttäjää informoidaan. Näissä tilanteissa voi työntekijän puolelta ilmetä tyytymättömyyttä ja halua tehdä vahinkoa organisaatiolle, jolloin on äärimmäisen tärkeää hoitaa oikeuksien poistaminen heti, joissain tapauksissa jopa etukäteen. (SFS-EN 27002:2022, 42.)

Pääsyoikeuksia voidaan myöntää luonnollisille henkilöille tai loogiselle kohteelle, esimerkiksi koneelle, laitteelle tai palvelulle. Hallinnan yksinkertaistamiseksi voidaan hyödyntää rooleja, jotka määritellään käyttäjäryhmille. Pääsynhallinnan kaksi yleisintä periaatetta ovat:

- henkilöille määritetään pääsyoikeudet vain sellaiseen tietoon, johon työtehtävien hoitamiseksi on tarvetta
- teknologiaan annetaan pääsy vain siihen osaan infrastruktuurista, johon on tarve.

Sääntöjä määritettäessä tulisi käyttää vähimmän oikeuden periaatetta (principle of least privilege). Pääsynhallinnan toteuttamisessa voidaan käyttää pakollista pääsynhallintaa (MAC), rooliperustaista pääsynhallintaa (RBAC), harkinnanvaraista pääsynhallintaa (DAC) tai attribuutteihin perustuvaa pääsynhallintaa (ABAC). (SFS-EN 27002:2022, 37–38.)

### 5.5 Vähimpien oikeuksien periaate (Principle of Least Privilege)

Vähimpien oikeuksien periaatteella (Principle of Least Privilege, PoLP) viitataan malliin, jossa käyttäjällä on minimaaliset käyttöoikeudet työtehtävien suorittamista varten. Tätä pidetään laajasti kyberturvallisuuden yhtenä parhaimmista käytännöistä. Kyseistä mallia voidaan soveltaa esimerkiksi järjestelmiin ja sovelluksiin ja niiden käyttöön vaadittaviin oikeuksiin. Vähimpien oikeuksien periaatteen valvonta edellyttää keskitettyä tapaa hallita ja suojata hallintatunnuksia. Se voi auttaa tasapainoilemaan kyberturvallisuuden vaatimustenmukaisuuden vaatimusten sekä loppukäyttäjien tarpeiden välillä. Tällä saadaan myös pienennettyä kyberhyökkäysten pinta-alaa, koska nykyisin useimmat hyökkäyksistä perustuvat juuri hallintatunnusten hyödyntämiseen. Kun hallintatunnusten määrää sekä niihin liitettyjä oikeuksia rajoitetaan, saadaan myös kyberhyökkäysten pinta-alaa pienenettyä. Näin saadaan estettyä haittaohjelmien leviäminen, myöskään haittaohjelmahyökkäykset (esimerkiksi SQL-injentiot) eivät pysty hyödyntämään korotettuja oikeuksia lateraaliseen leviämiseen. (CyberArk s.a.)

Yksi hyvä esimerkki liiallisista oikeuksista on Edward Snowdenin tapaus. Snowdenille annettiin oikeuksia, joilla oli mahdollista päästä käsiksi todella suureen tietoaineistoon, joka oli määrätty salassa pidettäväksi. Snowden oli aiemmin kehittänyt myös varmistusjärjestelmän NSA:n käyttöön. Hänellä oli myös pääkäyttäjätasoiset oikeudet muun muassa Sharepointiin ja todennäköisesti samalla tunnuksella myös muualle verkkoon. Tämä kaikki mahdollisti hänelle pääsyn erittäin salaisiksi määritettyihin asiakirjoihin. (Rousku 2014, 93–96)

## 5.6 SSO

Kertakirjautuminen (Single Sign-On, SSO), mahdollistaa käyttäjän pääsyn moneen eri järjestelmään yhdellä kirjautumisella. Se tehostaa ja nopeuttaa käyttöä sekä vähentää salasanan palautuksia ja lisää käyttömukavuutta. Käyttäjän tarvitsee muistaa vain yksi tunnus ja salasana, jota hyödyntäen hän pystyy käyttämään useampaa järjestelmää. Näin saadaan myös keskitettyä käyttäjän tunnistautuminen sekä voidaan mahdollistaa vahva tunnistaminen. Kertakirjautumista voidaan hyödyntää sekä verkkosovelluksiin (web SSO), että clientpohjaisiin työasemasovelluksiin (eSSO, Enterprise Single Sign-On). (Kertakirjautuminen Loihde Trust s.a.)

## 5.7 Hallintaoikeudet

Hallintaoikeuksia tulisi olla käytössä mahdollisimman vähän ja niiden käyttöä olisi rajoitettava mahdollisuuksien mukaan. Ainoastaan luvallisille käyttäjille, järjestelmille ja palveluille tulisi määrittää hallintaoikeuksia. Hallintaoikeuksia työtehtäviensä hoitamiseen tarvitsevat käyttäjät täytyy pystyä yksilöimään. Hallintaoikeuksia tulisi myöntää ainoastaan henkilöille, joilla on pätevyys tehdä hallintatoimenpiteitä ja näissäkin tulisi huomioida vähempien oikeuksien periaate. Hallintaoikeuksien käyttämiseen voidaan vaatia normaalia tunnusta vahvempaa tunnistautumista, eikä näitä tunnuksia tulisi käyttää normaaleihin päivittäisiin toimenpiteisiin, kuten sähköpostin lukemiseen tai verkon selailuun. Perusrutiinien hoitamista varten tulisi olla erilliset tunnukset. (SFS-EN 27002:2002, 93–94.)

Kaikki hallintatunnuksilla tehtävät toimenpiteet tulee kirjata ja näin syntyviä lokeja tulisi säilyttää riittävän kauan mahdollisia myöhemmin suoritettavia auditointitarkoituksia varten. Katselmoinnit hallintaoikeuksien osalta tulisi suorittaa säännöllisesti sekä esimerkiksi organisaatiomuutosten yhteydessä. Geneeristen hallintatunnusten (kuten ’root’) käyttäminen tulisi lähtökohtaisesti estää tai vähintäänkin tunnistautumistiedot tulisi hallita ja suojata riittävällä tasolla. Yhtenä parhaana käytäntönä voidaan hyödyntää tilapäisten hallintaoikeuksien käyttämistä, esimerkiksi jonkin huoltotoimenpiteen tai muutoksen suorittamiseksi. Näin toimimalla ei tarvitse myöntää pysyviä hallintaoikeuksia, vaan hallintatunnukselle myönnetään vain väliaikaisesti korotetut oikeudet. (SFS-EN 27002:2002, 93–94.)

### 5.8 Ohjeistukset, koulutukset ja kurinpito

Organisaation johto vastaa siitä, että politiikat ja toimintaperiaatteet ovat kaikille osapuolille helposti saatavilla, selkeät ja niiden sisältö on läpikäyty ohjeistusten tai koulutusten muodossa. Myös jonkinlainen kuittaus läpikäynnistä olisi saatava kaikkien tahojen osalta. Uusien merkittävien muutosten yhteydessä tulee myös katselmoida, että tieto on saavuttanut kaikki tahot. (SFS-EN 27002:2022, 19–20.)

Organisaation tulee varmistaa, että kaikki tarvittavat tahot ymmärtävät tietoturvapolitiikan sisällön sekä seuraukset mahdollisesta politiikan rikkomisesta. Tietoturvapolitiikan rikkomisesta organisaation olisi määritettävä kurinpitoprosessi, jonka mukaisesti tällaisessa tilanteessa toimitaan. (SFS-EN 27002:2022, 71–72.)

### 5.9 Vastuut

Johto vastaa viime kädessä kaikesta tietoturvaan liittyvistä toimenpiteistä organisaatiossa. Johdon vastuulla on varmistaa, että koko henkilöstö tietää tietoturvaan liittyvät vastuunsa ja myös tuntee organisaation tietoturvapolitiikan ja siihen liittyvät toimintaperiaatteet. Johdon tulee myös selkeästi osoittaa tukensa kaikille tietoturvaan liittyville organisaation politiikoille, periaatteille ja hallintakeinoille ja noudattaa myös itse näitä vaatimuksia. Johto varmistaa henkilöstön riittävän kouluttamisen ja osaamisen tietoturvaan liittyviin asioihin. Myös riittävän resursoinnin määrittäminen, jolla varmistetaan tietoturvaan liittyvien hallintakeinojen ja prosessien toteuttaminen, on johdon vastuulla. (SFS-EN 27002:2022, 23.)

Käyttäjien vastuulla on pitää tunnistautumistietonsa henkilökohtaisina ja näitä tietoja ei saa muiden kanssa jakaa. Jos jokin salasana paljastuu, tulee se viipymättä vaihtaa. Salasanojen osalta tulisi välttää yksittäisiin sanoihin perustuvia salasanoja. Salasanojen ei tulisi olla helposti arvattavissa kohdehenkilöön helposti liitettävissä olevien tietojen, kuten puhelinnumeron, nimen tai syntymäajan kautta. Samaa salasanaa ei tulisi käyttää useassa järjestelmässä, vaan kaikissa tulisi olla yksilölliset salasanat. Salalauseet ovat hyvä esimerkki

vahvasta salasanasta, näin salasanasta saadaan pitkä ja se on helposti muistettavissa. Salalauseisiin on hyvä pyrkiä sijoittamaan myös erikoismerkkejä sekä aakkosnumeerisia merkkejä. (SFS-EN 27002:2022, 40.)

### 5.10 Roolipohjaiset käyttöoikeudet (RBAC)

Roolipohjaiset käyttöoikeudet ovat olleet käytössä jo 1970-luvulta saakka. Silloin yksittäisissä kaupallisissa sovelluksissa alettiin käyttämään organisaation käyttäjän rooliin pohjautuvia käyttöoikeuksia. Tällöin ei vielä ollut vielä mitään yhteneväisyyttä eri sovellusten välillä. Ensimmäinen varsinainen malli roolipohjaisiin käyttöoikeuksiin luotiin vuonna 1992, jolloin Ferraiolo ja Kuhn loivat ensimmäisen muodollisen mallin. Vuonna 2000 Sandhu, Ferraiolo ja Kuhn loivat roolipohjaisille käyttöoikeuksille yhtenäisen mallin ja ehdottivat tämän mallin perusteella roolipohjaisten käyttöoikeuksien standardoimista. Vuonna 2004 ANSI (American National Standards Institute) ja INCITS (International Committee for Information Technology Standards) hyväksyivät tuon ehdotetun mallin ja siitä määritettiin alan standardi. (Ferraiolo & Kuhn 2016.)

Roolipohjainen käyttöoikeusmalli on lähtökohtaisesti rakennettu pitämään huolen, ettei vaarallisia työyhdistelmiä pääse syntymään. Ryhmien ja roolipohjaisen käyttöoikeusmallin välinen ero on siinä, että ryhmään voidaan liittää suoraan käyttäjiä tai ryhmiä ja näin oikeudet sidotaan suoraan käyttäjään. Roolipohjaisessa mallissa oikeudet on määritetty rooliin, ei suoraan käyttäjään. Roolien kautta pystytään myös aktivoimaan käyttäjälle jokin osajoukko rooleista, kun ryhmän kautta tulee yhdellä kertaa kaikki oikeudet mitä ryhmään on määritettynä. Roolipohjainen käyttöoikeusmalli mahdollistaa myös monen suhde moneen -käyttöoikeussuhteiden rakentamisen käyttäjien ja oikeuksien välille. (Ferraiolo & Kuhn 2016.)

Käyttämällä rooleja pääsyoikeuksien määrittämiseen voidaan pääsynhallintaa yksinkertaistaa. (SFS-EN 27002:2022, 37.)

### 5.11 MFA

Monivaiheisessa tunnistautumisessa (Multifactor Authentication, MFA) vaaditaan kahden tai useamman todennustekijän käyttämistä, jotta kirjautuminen

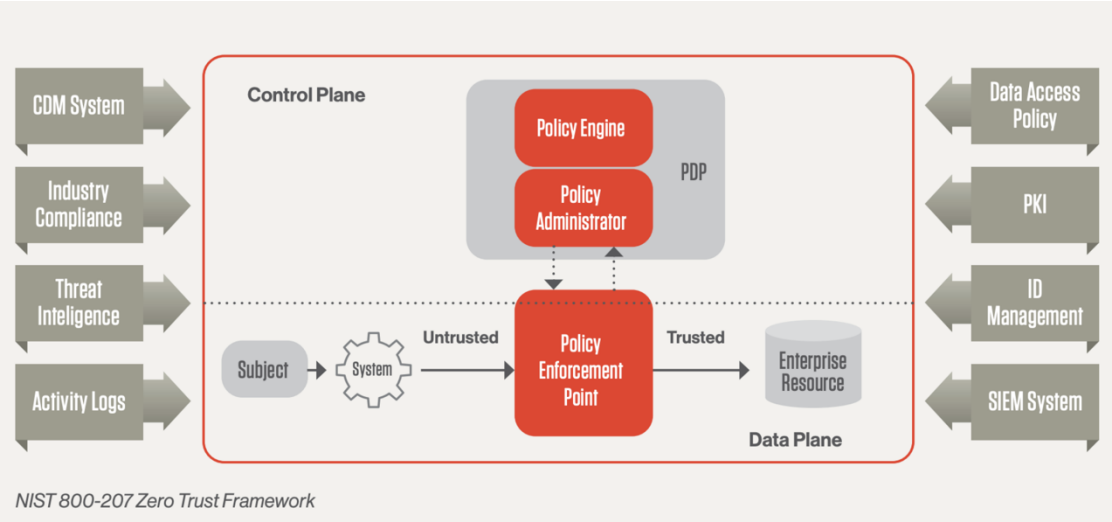
palveluun tai järjestelmään mahdollistuu. Monesti tunnistusmenetelminä käytetään salasanan ja varmistussoiton tai salasanan ja mobiilisovelluksen yhdistelmää. Monivaiheinen tunnistautuminen hankaloittaa rikollisten tietojenkalastelua, mutta ei tee sitä mahdottomaksi. Vaikka rikolliset onnistuisivat huijaamaan käyttäjältä salasanan, eivät he pääse silti kirjautumaan mihinkään ilman erillistä toisen vaiheen tunnistautumista, joka toteutetaan esimerkiksi käyttäjän puhelimella. (Helsingin yliopisto s.a.)

Microsoftin tekemän tutkimuksen mukaan tutkimusjakson aikana tileistä, joissa oli MFA käytössä säilyi turvassa 99,99 %. Kokonaisuutena MFA pienentää riskiä identiteetin vaarantumisesta 99,22 % koko käyttäjäkunnasta ja 98,56 % niistä, joiden käyttäjätunnukset ja salasanat on jo saatu rikollisesti haltuun. MFA-sovellusten on myös todettu olevan turvallisempia, kuin SMS-pohjaisten tunnistamisten, molempien silti ollessa huomattavasti turvallisempia kuin jättää MFA kokonaan käyttämättä. Viimeisten vuosikymmenten aikana Microsoft, Google ja Okta ovat tuoneet käyttöön enemmän riskiperusteisen todennuksen teknologiaa, joka pienentää riskiä menettää käyttäjätiedot rikollisten käsiin. Tässä hyödynnetään passiivisia signaaleja, joilla tunnistetaan epänormaalia toimintaa. Metodeina voidaan käyttää esimerkiksi IP-paikannusta, laitteen ja IP-osoitteen mainetta sekä eri lokaatioista tapahtuvien kirjautumisyritysten välistä aikaa. Jos epätavallista toimintaa havaitaan, esitetään käyttäjälle lisähaaste, jolla varmistetaan käyttäjän oikeutus resurssiin päästäkseen. Lisähaaste voi olla koodi, joka toimitetaan käyttäjän hallussa olevaan laitteeseen. (Mayer ym. s.a. 1–2.)

### 5.12 Zero Trust

Zero Trust on viitekehys, jossa kaikilta käyttäjiltä vaaditaan jatkuvaa validointia, autentikointia ja autorisointia riippumatta siitä, ovatko käyttäjä organisaation sisäverkossa vai tulevatko sisään ulkoverkosta. Perinteisiä verkon reunoja ei Zero Trust -viitekehyksessä tunneta. Verkot voivat olla paikallisia, pilvessä sijaitsevia verkkoja tai hybrid-verkkoja ja verkkoihin liittyvät käyttäjät ja resurssit voivat sijaita missä tahansa. NIST on luonut standardin NIST 800-207 vastaamaan Zero Trust -viitekehykseen. Kyseisen standardin vaatimukset on esitetty kuvassa 3. Vuonna 2021 Bidenin hallinto on määrännyt Yhdysvaltain liit-

tovaltion virastot noudattamaan NIS 800-207 -standardia vastatakseen kasvaneisiin korkean profiilin tietoturvaloukkauksiin. Tämän takia standardi on käynyt läpi hyvin kattavan validoinnin kaupallisten asiakkaiden ja myyjien sekä valtion viranomaisten toimesta. Tästä syystä monet pitävät sitä defacto-standardina myös yksityiselle sektorille. (Raina 2023.)




Kuva 3. NIST 800-207 Zero Trust -viitekehys

Ilman kunnollista identiteetin- ja pääsynhallintaa, ei voida toteuttaa käyttäjien ja laitteiden tunnistamista kaikissa tilanteissa, sekä antaa vain niitä oikeuksia ja pääsyä verkkoon, dataan ja muihin organisaation resursseihin, jotka ovat sillä hetkellä tarpeen (Tivi 2021).

Zero Trust -arkkitehtuurin käyttöönotto pystytään organisaatiossa hoitamaan tehokkaasti, kun identiteetti asetetaan keskiöön. Kun toteutetaan Zero Trustin perusperiaatetta ”älä luota, epäile aina”, voidaan ennakoivasti havaita mahdollisia uhkia. Tämä mahdollistaa myös reagoinnin, ennen kuin tietomurto ehtii realisoitua. (Okta 2021, 6.)

### 5.13 Vaaralliset työyhdistelmät

Vaarallisilla työyhdistelmillä viitataan periaatteeseen, jossa yhdelläkään käyttäjillä ei tulisi antaa liikaan oikeuksia, joilla järjestelmän väärinkäyttäminen mahdollistuu. Esimerkiksi laskun hyväksyjä ei saa olla sama henkilö, joka tarkastaa laskun. Tehtävien eriyttäminen voidaan suorittaa joko staattisesti tai

dynaamisesti. Staattisessa mallissa määritetään ne roolit, joita samalla käyttäjällä ei saa olla. Dynaamisessa mallissa pakotetaan esimerkiksi kaksi eri henkilö suorittamaan tehtävää. (Separation of Duty (SoD) NIST s.a.)

Petoksiin, tietoturvallisuuden hallintakeinoihin ja virheisiin liittyviä riskejä voidaan vähentää eriyttämillä keskenään ristiriitaiset tehtävä- ja vastuualueet toisistaan. Näin voidaan estää tilanteet, joissa yksi henkilö voisi suorittaa keskenään ristiriitaisia tehtäviä. Organisaation tulisi määrittää ne tehtävät ja vastuualueet, jotka tulee eriyttää. Esimerkkejä näistä ovat muun muassa sovellusten käyttö ja hallinta, pääsyoikeuksien pyytäminen, hyväksyminen ja myöntäminen, tietoturvan hallintakeinojen suunnittelu, auditointi ja varmennus. (SFS-EN 27002:2022, 22.)

Hyvä käytäntö on, että sama henkilö, joka tekee varsinaisen suunnittelun ja toteutuksen, ei voi olla samaan aikaan myös hyväksymässä sekä katselmoimassa näitä muutoksia. Huolehtimalla, että on olemassa listat vaarallisista työyhdistelmistä ja ettei tällaisia pääse syntymään, saadaan riskiä pienennettyä. (Rousku 2014, 96–97.)

Jos tehtäviä ei pystytä eriyttämään, mikä on varsin tavallista varsinkin pienissä organisaatioissa, tulisi käyttöön ottaa mahdollisuuksien mukaan teknistä valvontaa, kirjausketjuja, tapahtumien kirjaaminen lokiin sekä mahdollisesti esihenkilöiden suorittamaa valvontaa. Jos käytössä on roolipohjainen pääsynhallinta, tulee varmistua siitä, että henkilö ei voi saada roolien kautta ristiriitaisia oikeuksia. Automaatiota tulisi hyödyntää, jos rooleja on paljon näiden ristiriitojen tunnistamisessa ja poistamisessa. Suunniteltaessa hallintakeinoja eriyttämiseen liittyen, tulisi huomioida mahdollinen pahantahtoisuus. (SFS-EN 27002:2022, 22.)

### 5.14 Valvontatoimet ja lokienhallinta

Organisaation tulee määrittää tarvittavien lokien vaatimukset. Mitä tietoja lokeihin halutaan tallentaa ja kirjata, sekä miten lokit tullaan suojaamaan ja minkälaisia vaatimuksia on lokien käsittelylle. Tästä tulisi koostaa dokumentti, joka pitää sisällään lokienhallintaan liittyvät toimintaperiaatteet. (SFS-EN 27002:2022, 114.)

Lokeihin tulisi sisällyttää muun muassa:

- käyttäjätunnus tieto
- mitä toimintoja kyseisellä tunnuksella on hoidettu
- tarkka aika, milloin tehtäviä on suoritettu
- millä laitteella tehtäviä on suoritettu ja mistä sijainnista yhteys on muodostettu
- mistä verkko-osoitteista tehtäviä on suoritettu.

Näiden lisäksi on hyvä harkita myös seuraavien tapahtumien kirjaamista:

- onnistuneet ja epäonnistuneet kirjautumiset
- erilaiset järjestelmän konfiguraatioon liittyvät muutokset
- hallintatunnusten käyttäminen
- eri tietoturvakomponenttien pois kytkeminen
- uusien identiteettien luonti tai olemassa olevien poistaminen
- kaikki pääsynhallintaan liittyvät hälytykset.

Kaikkien järjestelmien tulisi käyttää samaa aikalähdettä, jotta voidaan mahdollisen tietoturvapoikkeaman jälkeen luoda luotettava aikajana tapahtumista. (SFS-EN 27002:2022, 114.)

Lokit tulisi suojata mahdollisimman hyvin ja tehokkaasti. Millään oikeuksilla varustetuilla käyttäjillä ei tulisi olla oikeutta poistaa tai muuttaa lokeihin liittyviä kirjauksia omien toimiensa osalta. Tämä mahdollistaisi käyttäjien manipuloida omia tekemisiään lokeista ja näin peitellä mahdollisesti jälkiään. Muutenkin pääsy lokeihin tulisi olla vain tarvittavilla henkilöillä. Jos lokeja on tarpeen lähettää kolmansille osapuolille, tulee varmistua, ettei lähetettävät lokit sisällä arkaluonteisia tietoja tai henkilötietoja. (SFS-EN 27002:2022, 115.)

Lokien analysointi tulee tehdä vain niiden asiantuntijoiden toimesta, joilla on tähän tarvittava osaaminen. Analysointimenetelmät tulee olla määritettyinä, ennen kuin lokeja lähdetään analysoimaan. Monesti lokeissa on myös tietoa, joka ei ole oleellista jonkin poikkeaman tarkastelun kannalta. Tätä varten olisi hyvä olla käytössä apuohjelmia tai työkaluja, joilla oleellinen tieto voidaan saada helposti ja nopeasti esille. Näin päästään tarkemmin ja nopeammin tutkimaan oleellisia tietoja ja saada parempi kuva mitä on tapahtunut. (SFS-EN 27002:2022, 115–116.)

Valvontatoimien avulla voidaan havaita mahdolliset poikkeavat toimet ja tietototurvahäiriöt. Valvontaan tulisi käyttää jotain työkalua, joka kykenee reaaliaikaiseen valvontaan tai joka mahdollistaa valvonnan toteuttamisen määräajoin.

Työkalun tulee kyetä käsittelemään suurta määrää tietoa ja mukautua jatkuvasti muuttuvaan ympäristöön sekä tuottaa reaaliaikaisesti ilmoituksia. Valvontajärjestelmän tulisi kyetä valvomaan verkkoa, järjestelmiä ja sovelluksia ja niissä tapahtuvia poikkeamia. Myös hallintatunnuksiin liittyviä tapahtumia ja normaalien tunnusten pääsyä järjestelmiin, kriittisiin sovelluksiin, valvontajärjestelmiin ja verkkolaitteisiin tulisi kyetä valvomaan. (SFS-EN 27002:2022, 116–117.)

Organisaation tulisi kyetä määrittämään vertailukohta normaaliin käyttäytymiseen, jotta pystyttäisiin löytämään poikkeamia. Vertailukohtaa määritettäessä tulisi huomioida käyttäjien ja käyttäjäryhmien normaalit käyttöajat ja lokaatiot, joista käyttö tapahtuu, sekä minkälaista kuormitusta järjestelmille tulee normaaliaikana ja huippukäyttöhetkinä. Näin pystytään valvontatyökalulla näkemään poikkeamat, kuten epämääräisistä IP-osoitteita tai verkkoalueista tuleva liikenne, sovellusten tai prosessien sammuttaminen, luvaton käyttö ja erilaiset luvattomat skannaukset, joilla pyritään saamaan ympäristöstä lisää tietoa. (SFS-EN 27002:2022, 117.)

Jos käytössä on automatisoitu valvontajärjestelmä, tulisi tähän määrittää hälytysten lähettäminen eri kanavia pitkin, kun tietyt kynnysarvot ylittyvät. Väärien positiivisten hälytysten estämiseksi järjestelmää tulee hienosäätää vertailukohtaan nähden. Käytössä tulee olla riittävästi koulutettua henkilöstöä, joka pystyy reagoimaan nopeasti mahdollisiin hälytyksiin. Tällä voidaan varmistaa, että mahdolliset poikkeamat käsitellään heti ja niistä aiheutuva mahdollinen leviäminen isompaan osaan organisaatiota saadaan estettyä. Poikkeavat tapahtumat tulee viestiä kaikille olennaisille sidosryhmille ja näin saadaan parannettua prosessia ja hallintamenetelmiä. (SFS-EN 27002:2022, 117–118.)

# 6 IDENTITEETIN- JA PÄÄSYNHALLINNAN YHTEYS TIETOTURVAAN

Monille organisaatioille tietoturvauhkiin varautuminen on äärimmäisen paljon voimavaroja syövä tekijä. Vaikka hyökkäykset jatkuvasti kehittyvät, silti suurin osa niistä alkaa edelleen samoista heikkouksista, eli identiteeteistä ja pääsyoikeuksista. Monessa organisaatiossa on ymmärretty identiteettien ja pääsyoi-

keuksien yhteys tietoturvaan, mutta valitettavan harvoin ymmärretään kuitenkaan, miten tärkeästä asiasta on kysymys. Kaikki nykyaikaiset kyberturvallisuusstrategiat tulisi rakentaa identiteettilähtöisesti. (OKTA 2021, 2.)

Todennäköisimmin kyberhyökkäyksen uhriksi joutuvat ne organisaatiot, jotka eivät riittävästi suojaa tietojaan ja identiteettejään. Hyökkäyksistä aiheutuvat taloudelliset menetykset, sekä regulaatioiden kautta mahdollisesti lankeavat sakot voivat olla suuriakin, mutta näistä muodostuva haitta on vain lyhytaikainen. Pidempiaikaiset vahingot tulevat organisaation maineelle ja brändille aiheutuvista vahingoista ja niistä ei välttämättä ole mahdollista toipua ollenkaan. (OKTA 2021, 2.)

Kyberhyökkäysten määrät ovat kasvaneet vuosi vuodelta ja niitä kohdistuu erilaisiin organisaatioihin, valtiollisiin tahoihin sekä yksityishenkilöihin. Yksi suuri muutoksen aiheuttaja on etätöiden lisääntyminen, ja sen takia suojattavan pinta-alan kasvaminen. Etätöihin siirtyminen on myös altistanut kaikki organisaatioiden sovellukset uhan alle, koska niihin tulee päästä nyt sekä sisäverkosta, että ulkoverkosta. Hyökkääjät pyrkivät hyödyntämään tätä mahdollisuutta tietojenkalastelulla (phishing), sosiaalisella manipuloinnilla (social engineering) sekä myös hyödyntämällä organisaatioissa työskenteleviä pahantahtoisia käyttäjiä ja heidän hallussaan olevia identiteettejä sekä pääsyoikeuksia. Verizonin mukaan tietomurroista 81 % toteutetaan varastetuilla tai heikoilla identiteeteillä ja 91 % murroista käynnistyy tietojenkalasteluhyökkäyksistä. Identiteetti on keskiössä, kun pyritään suojaamaan pilvisovelluksia, laitteita ja verkkoja. (OKTA 2021, 2.)

### 6.1 Sosiaalinen manipulointi

Sosiaalisella manipuloinnilla pyritään vaikuttamaan uhriin siten, että hän tekee jotain, mikä ei ole hänen etujensa mukaista, esimerkiksi antaa jotain arkaluontoista tietoa tai tekee jonkin virheen. Uhria voidaan houkutella avaamaan tiedostoja, dokumentteja tai haitallista sisältöä sisältävä sähköposti tai vierailemaan sivustolla, johon on upotettu haitallista koodia. Nämä toimet voivat isossa kuvassa hyödyntää jotain teknologiaa, mutta niiden hyödyntämiseen tarvitaan kuitenkin inhimillinen tekijä. Yleensä sosiaalisen manipuloinnin kei-

noja käytetään hyökkäyksen alussa, jotta saadaan jalansija hyökkäyksen kohteena olevaan tahoon, mutta niitä voidaan hyödyntää myös hyökkäyksen myöhemmissä vaiheissa. (Lella ym. 2023, 7.)

Sosiaaliseen manipulointiin liittyvä termejä ovat muun muassa tietojenkalastelu (phishing), kohdennettu tietojenkalastelu (spear phishing), valaanpyynti (whaling), tietojenkalastelu tekstiviestillä (smishing) sekä äänikalastelu (vishing). Tietojenkalastelu palveluna (Phishing-as-a-Service, PhaaS) on kasvava trendi. ”Palvelua” saa ostettua alhaisimmillaan 15 $ päivässä ja näin toimimalla tahot, joilla ei ole juurikaan osaamista kyberturvallisuuden alueella voivat tehtailla hyvinkin monimutkaisia hyökkäyksiä. FBI:n mukaan tietojenkalastelu on eniten käytetty digitaalinen rikos. IBM X-Forcen mukaan tietojenkalastelua käytettiin 41 %:ssa tapauksista ensimmäisenä askeleena jalansijan saavuttamiseksi. Verizon DBIRin mukaan 82 %:iin kaikista tapauksista liittyi jonkinlainen inhimillinen tekijä kuten tietojenkalastelu, tunnusten varastaminen, väärinkäytös tai ihan yksinkertaisesti virhe. ESET:n mukaan vuoden 2022 neljän viimeisen kuukauden aikana kyberuhat muutoin vähenivät, mutta tietojenkalastelu kasvoi. (Lella ym. 2023, 70–72.)

### 6.2 Kiristyshaittaohjelmat

Kiristyshaittaohjelmat ovat hyökkäyksiä, joissa jokin taho tekee kyberhyökkäyksen, asentaa haittaohjelman koneelle ja kryptaa kaiken koneella olevan tiedon. Tämän jälkeen kone on käyttökelvoton ja palatusta varten pitäisi sitten maksaa lunnaat, jota vastaan hyökkääjä sitten joko antaa kryptauksen purkamiseen koodin tai jättää antamatta. Yleensä lunnaat pyydetään Bitcoineina, koska niiden jäljittäminen on hyvin hankalaa. Kiristämistä voidaan tehdä myös uhkaamalla jakaa saadut tiedot julkisesti saataviksi esimerkiksi pimeän verkon (Dark Web) puolella. (Das 2022.)

Identiteetin- ja pääsynhallinnan avulla voidaan taistella hyvinkin voimakkaasti kiristyshaittaohjelmia vastaan. Käyttämällä roolipohjaista pääsynhallintaa ja vähimpien oikeuksien periaatetta, voidaan vaikeuttaa kiristyshaittaohjelmien leviämistä ja jopa pääsyä organisaation sisälle. Tähän hyvänä lisänä voidaan hyödyntää myös monivaiheista tunnistautumista, joka tuo lisäkerroksen hyökkääjien läpäistäväksi. (Das, R. 2022.)

Maaliskuussa 2023 nähtiin kaikkien aikojen ennätys kiristyshaittaohjelmahyökkäysten määrässä. 459 kiristyshaittaohjelmahyökkäystä yhden kuukauden aikana on todella suuri määrä ja kasvua vuoden 2022 maaliskuuhun on peräti 62 %. Kolme aktiivisinta kiristyshaittaohjelmaa Euroopan alueella vuonna 2023 olivat LockBit 3.0, PLAY, BlackCat (ALPHV), CL0P ja Black Basta. Näistä kolmea ensimmäisenä mainittua käytettiin vuoden 2023 aikana 322 hyökkäyksessä. (Lella ym. 2023. 55–58.)

# 7 KEHITTÄMISPROJEKTI

Projektin tavoitteena oli käydä läpi nykytila ja mitä toimenpiteitä tulisi tehdä, jotta nykytila saataisiin vastaamaan parhaisiin käytäntöihin. Tärkeässä roolissa oli automaatioasteen kasvattaminen ja prosessien kehittäminen siten, että ne voitaisiin tulevaisuudessa monistaa kaikkien toimintamaiden käyttöön. Projektin laajuus myös hieman muuttui ja kasvoi opinnäytetyön tekemisen aikana. Tarkasteluun tuli muutamia kaupallisia tuotteita, joiden kyvykkyyksiä organisaation tarpeita vasten peilattiin.

## 7.1 Kehittämiskohteet, olemassa olevat käytännöt ja prosessit

Koska ei ollut mitään varsinaista järjestelmää, jota olisi voitu kehittää, projekti aloitettiin nykytilan kartoituksella. Dokumentaatiota nykytilasta löytyi jonkin verran. Kaikkea ei kuitenkaan ollut dokumentoitu, vaan osa dokumentaatiosta oli kommentteina muun muassa scripteissä. Tieto oli myös kohtuullisen laajalle levinneenä eri dokumentteihin ja lokaatioihin. Tälle hajallaan olevalle tiedolle perustettiin Teams-kanavaan oma kansio, johon dokumentit kerättiin. Dokumentteja pyrittiin myös mahdollisuuksien mukaan yhdistämään, sekä luotiin uutta dokumentaatiota esimerkiksi piirtämällä prosessikuvauksia nykytilasta.

Kuten tutkimuksesta käy ilmi, tulisi vastuu identiteetin- ja pääsynhallinnan osalta olla selkeästi määritettynä. Tämä ei kuitenkaan ole tällä hetkellä organisaatiossa vallitseva tila. Vastuu tulisi selkiyttää ja riittävä resursointi – sekä henkilöstön, että rahoituksen osalta – varmistaa, jotta pystytään vastaamaan lakien ja säädösten vaatimuksiin sekä toimimaan parhaiden käytäntöjen mukaan. Vastuuta tulisi myös jakaa IT:stä muualle organisaatioon. Parhaiden

käytäntöjen mukaan IT:n tulisi käytännössä vastata vain identiteetin- ja pääsynhallinnan alustan ylläpidosta ja hoitaa järjestelmän päivitykset sekä muut teknologiaan liittyvät asiat. Liiketoiminnan vastuulla tulisi olla pääsyoikeuksien ja roolien määrittäminen sekä muut pääsynhallintaan liittyvät toimenpiteet. Näin on määritetty myös organisaation tietoturvapolitiikassa, jossa on määritetty liiketoimintasovellusten pääsynhallinnan vastuu ratkaisupäälliköille ja sovellusvastaaville. Kohdeorganisaatiossa näistä rooleista osa on myös IT:n sisällä, mutta osa on myös liiketoiminnan puolella. IT:n tulee tietenkin tukea liiketoimintaa niissä asioissa, joissa heillä on parempi osaaminen ja ymmärrys, kuten monivaiheisen tunnistautumisen määrittämisessä ja hallinnoinnissa tai muissa teknologiaan liittyvissä asioissa identiteetin- ja pääsynhallinnan alueella.

Identiteetin- ja pääsynhallintapolitiikka puuttuu tällä hetkellä, vaikka se on yksi tärkeimmistä lähtökohdista hyvän identiteetin- ja pääsynhallinnan toteuttamisessa. Ilman politiikkaa identiteetin- ja pääsynhallinnan toteuttaminen on haastavaa, koska ei ole selkeää määritystä halutulle toimintatavalle. Politiikka määrittää pohjan, jonka päälle kaikki identiteetteihin ja pääsynhallintaan liittyvät toimenpiteet, prosessit ja käytännöt rakennetaan. Politiikan kautta saadaan myös muun muassa määritykset sille, miten identiteettien elinkaari kokonaisuudessaan hoidetaan, miten pääsynhallinta toteutetaan ja miten näihin liittyvät hyväksyntäketjut rakennetaan.

Prosessit tulee käydä tarkasti läpi ja pyrkiä ratkaisemaan niihin liittyvät haasteet viipymättä. Prosessit on luotu sen hetkisen parhaan osaamisen ja käytettävissä olevien työkalujen pohjalta. Vaatimukset ovat kuitenkin kasvaneet vuosi vuodelta ja nykyiset työkalut ja prosessit eivät enää vastaa vaatimuksiin riittävällä tasolla.

Tutkimuksen mukaan prosessien määrittäminen ja jatkuva kehittäminen on tärkeä osa identiteetin- ja pääsynhallinnan kehittämistä. Prosessien kuvaamisessa on paljon tehtävää. Varsinkin oikeuksien poistoprosessit ja muutosprosessit ovat lähestulkoon kokonaan kuvaamatta ja prosessit määrittämättä. Tämä aiheuttaa monia haasteita toimintaan. Käyttäjille kertyy liikaa oikeuksia

ja käyttäjien irtisanoutuessa tai poistuessa muutoin organisaation palveluksesta saattaa oikeuksia jäädä roikkumaan ja syntyä orpotilejä, jotka ovat odottamassa hyökkääjien löytämistä.

### 7.2 Tarkennusta vaativat kohteet

Osaamisen kasvattamiseen ja ohjeistuksen laatimiseen tulisi käyttää varsin paljon aikaa. Tämä auttaisi taklaamaan monia haasteita, joita tällä hetkellä ympäristössä on sekä auttaisi selkiyttämään tavoitetilan suunnittelussa ja siihen pääsemisessä. Koulutukset ja ohjeistukset identiteetin- ja pääsynhallinnan osalta tulisi suunnitella eri kohderyhmille sopiviksi ja huomioida myös kohderyhmien lähtötaso.

### 7.3 Vaatimuksiin vastaaminen

Organisaation tietoturvapolitikassa oli määritettynä tiettyjä identiteetin- ja pääsynhallintaan oleellisesti liittyviä asioita. Siitä löytyy maininta vähimpien oikeuksien periaatteesta ja liiketoimintasovellusten pääsynhallinnasta toteuttamisen vastuusta, joilla molemmilla on hyvinkin vahva linkki identiteetin- ja pääsynhallintaan.

Nykytila ei siis myöskään vastaa tietoturvapolitiikan vaatimuksiin. Nämä puutteet tulisi aivan ensimmäisenä korjata ja saattaa näiltä osin asiat kuntoon. Vähimpien oikeuksien periaate ei tällä hetkellä toteudu, mutta se olisi ehdottoman tärkeä saada kuntoon mahdollisimman nopeasti. Jos tätä ei korjata on hyvin todennäköistä, että monilla käyttäjillä on oikeaan tarpeeseen nähden aivan liian laajat oikeudet. Monissa hallintatunnuksissa on myös liikaa oikeuksia, joten myös hallintatunnusten osalta tulisi käydä läpi oikeat tarpeet. Sovelluskohtaisesta pääsynhallinnasta vastuulliset henkilöt tulisi nimetä mahdollisimman nopeasti. Tämä helpottaisi esimerkiksi roolien määrittämisessä sekä prosessiymmärryksen lisäämisessä sekä IT:n että liiketoiminnan osalta.

Laista ja asetuksista tulee vaatimuksia organisaation identiteetin- ja pääsynhallinnan toteuttamiseen. Näiden huomioiminen on jäänyt organisaatiossa liian pieneen rooliin ja tämä vaatii tulevaisuudessa entistä enemmän panostusta, jotta voidaan täyttää vaatimustenmukaisuus. Tietyiltä osin vaatimuksia

jo täytetään, mutta nämä tulevat tietynlaisina sivuosumina muiden järjestelmien ja prosessien vaatimustenmukaisuuden täyttämisestä. Esimerkiksi tietosuojan vaatimuksiin vastaaminen omalta osaltaan tuottaa vaatimustenmukaisuutta myös identiteetin- ja pääsynhallintaan, vaikka varsinaista panostusta identiteetin- ja pääsynhallinnan osalta ei ole tehty. Toisaalta panostuksen puute identiteetin- ja pääsynhallinnan puolella aiheuttaa myös puutteita tietosuojan osalta. Ei voida olla täysin varmoja, että pääsy eri tietoverkkoihin on rajoitettu vain pääsyn tarvitseville tai että tietojen katoaminen olisi täysin estetty ja luvaton käyttö olisi minimoitu. Jotkin osa-alueet taas ovat täytettyinä oikeinkin hyvin, kuten monivaiheinen tunnistautuminen, joka on pakotettuna käyttöön suurimmalla osalla käyttäjistä.

NIS2-direktiivin tuodessa uusia vaatimuksia tietoturvaan liittyen tulee nämä myös huomioida. Koska ISO 27001 -standardissa on jo määritettynä NIS2-direktiivin täyttämiseksi vaadittavia asioita, hyödynnettiin ISO 27001 standardia täyttämään nämä identiteetin- ja pääsynhallinnan vaatimukset.

Joitakin asioita on jo nyt hoidettu hyvin, ja ne täyttävät osaltaan vaatimustenmukaisuuden, mutta tekemistä on myös paljon, jotta voidaan todeta organisaation täyttävän täysin tulevan NIS2n ja siihen liittyvän kansallisen lainsäädännön vaatimukset.

### 7.4 Identiteetin- ja pääsynhallinnan järjestelmät

Projektin aikana huomattiin vaatimuksia olevan niin paljon, että niiden täyttäminen nykytilan mukaisilla toimenpiteillä on mahdotonta. Tämän takia projektiin otettiin mukaan myös kevyt kartoitus muutamien toimijoiden järjestelmistä. Tätä ennen luotiin organisaation päättäville tahoille ratkaisuehdotus eri vaihtoehdoista. Ehdotuksessa oli kolme vaihtoehtoa:

1. Nykytilan edelleen kehittäminen ilman oikeaa järjestelmää
2. Perustarpeet täyttävän järjestelmän käyttöönottaminen
3. Kaiken kattavan identiteetin- ja pääsynhallinnan järjestelmän käyttöönotto.

Vaihtoehtojen välisen kustannuserot arvioitiin ensimmäisen osalta noin kymmenen tuhannen euron arvoiseksi, toisen osalta kokoluokka kasvoi sadantuhannen euron luokkaan ja kolmannen osalta puhuttaisiin jo noin miljoonan eu-

ron panostuksesta. Myös toteutusten kestoissa olisi huomattavia eroa ensimmäisen kestäessä vain joitain viikkoja, toisaalta myös saavutettavat hyödyt olisivat pienimmät. Toisen vaihtoehdon osalta kesto olisi joitain kuukausia ja hyötyjä jo huomattavasti ensimmäistä enemmän. Kolmannen vaihtoehdon keston arvioitiin olevan jopa vuosia, koska tässä vaihtoehdossa aivan kaikki prosessit ja organisaation toimintatavat olisi muutettava täysin. Toisaalta on hyvä pitää mielessä myös se, että identiteetin- ja pääsynhallinnan ei voi koskaan olettaa olevan valmis vaan se vaatii jatkuvaa kehittämistä. Esityksen pohjalta päädyttiin kevyeen kasvojenkohotukseen ja lähdettiin vertailemaan muutamaan tähän kategoriaan osuvaa järjestelmää.

# 8 TULOKSET

Kehitysprojektin lopputuotoksena oli tarkoitus saada aikaan paremmin toimivat prosessit, jotka helpottavat eri osapuolten toimintaa. Työn alussa nykytilan tutkimisen jälkeen päästiin miettimään, miten prosesseja voitaisiin:

- yksinkertaistaa
- kehittää
- saada myöhemmin monistettua kaikkiin toimintamaihin
- miten ne täyttävät lainsäädännön vaatimukset sekä vastaavat parhaisiin käytäntöihin.

Toisaalta jo heti alussa nykytilaa kartoitettaessa nähtiin niin perustavia haasteita, joiden takia alkuperäistä tutkimussuunnitelmaa olisi pitänyt muuttaa. Tähän ei kuitenkaan ollut valitettavasti mahdollisuutta, joten tutkimus päätettiin toteuttaa alkuperäisen suunnitelman mukaisesti. Tutkimuskysymyksiin vastaamalla saatiin hyvää tietoa siitä, minkälaisia riskejä on olemassa ja mitä toimenpiteitä tilanteen korjaamiseksi tulisi tehdä. Näiden vastausten pohjalta olisi myös hyvä lähteä suunnittelemaan jatkokehitystä ja aloittaa identiteetin- ja pääsynhallinnan toteuttaminen puhtaalta pöydältä. Seuraavissa luvuissa on esitetty vastauksia tutkimuskysymyksiin.

## 8.1 Parhaat käytännöt identiteetin- ja pääsynhallinnan toteuttamiseen yritysmaailmassa

Ensimmäisenä tutkimuskysymyksenä oli etsiä parhaat käytännöt ja vaatimukset identiteetin- ja pääsynhallinnan hoitamiseen. Tähän kysymykseen vastaukset löytyivät Sailpointin, One Identityn ja Veritiksen parhaista käytän-

nöistä. Näiden toimijoiden parhaat käytännöt on esitetty työn luvussa 4.3. Kuvassa 4 on nähtävissä Veritiksen 12 parasta käytäntöä identiteetin- ja pääsynhallinnan toteuttamiseksi.


Kuva 4. Veritis 12 parasta käytäntöä identiteetin- ja pääsynhallinnan toteuttamiseen (Veritis s.a.)

Näiden kolmen toimijan parhaista käytännöistä koostettiin alkuun listaus, jossa oli kaikkien edellä mainittujen toimijoiden parhaat käytännöt. Sailpointilla parhaita käytäntöjä oli seitsemän (7), One Identityllä kahdeksan (8) ja Veritiksellä kaksitoista (12). Näistä saadaan siis kokonaismääräksi kaksikymmentä seitsemän (27). Tätä joukkoa vastaan ei ole järkevää lähteä tekemään vertailua nykytilasta. Alkuun täytyy karsia pois turhat ja epäolennaiset käytännöt. Veritiksen käytännöistä löytyy muun muassa yksi käytäntö siitä, miten IAM käyttöönotto tulisi vaiheistaa ja se ei ollut validi tässä vaiheessa. Tämän jälkeen yhdistettiin samaa asiaa tarkoittavat käytännöt. Tämän karsinnan ja yhdistämisen jälkeen jäljelle jäi kahdeksantoista (18) oikeasti tärkeää ja huomioitavaa käytäntöä. Nämä jäljelle jääneet käytännöt on esitetty liitteessä 3.

Näitä käytäntöjä verrattiin organisaation olemassa oleviin käytäntöihin ja teknologiaan. Näin saatiin rakennettua taulukko, josta voidaan nähdä nykytilan puutteet ja haasteet. Käytäntöjen toteutumista nykytilaa vasten mitattiin kolmiportaisella asteikolla:

1. Toteutuu täysin

2. Toteutuu osittain
3. Ei toteudu

Tämän arvioinnin tuloksena saatu dokumentti sisältää organisaation sisäistä tietoa, jota ei sen arkaluontoisuuden takia voida tähän työhön lisätä.

Nykytilan ja parhaiden käytäntöjen vertailussa yksi (1) asia toteutuu täysin, kahdeksan (8) toteutuu osittain ja yhdeksän (9) ei toteudu. Eli yhteenvetona voidaan todeta, että tekemistä on varsin paljon. Ensimmäisenä suurena puutteena identiteetin- ja pääsyhallinnan vision ja politiikan puuttuminen. Toisena suurena puutteena keskitetyn identiteetin- ja pääsynhallinnan järjestelmän puute. Nämä aiheuttavat sen, ettei parhaisiin käytäntöihin, lainsäädäntöön tai asetuksiin pystytä täysin vastaamaan. Tätä puutetta on tähän asti pyritty korvaamaan itse tehdyillä scripteillä ja niiden päälle rakennetuilla automaatioilla.

## 8.2 Mahdollisia uhkia huonosti hoidetusta identiteetin- ja pääsynhallinnasta

Toisena tutkimuskysymyksenä oli, mitä uhkia organisaatiolle aiheutuu huonosti hoidetusta identiteetin- ja pääsynhallinnasta. Tähän löytyi vastauksia, kun tarkasteltiin erilaisia uhkakuvia. Moniin uhkiin ja niiden toteutumiseen vaaditaan jonkinlainen liitäntä identiteetteihin- ja pääsynhallintaan. Usein kyberhyökkäykset käynnistyvät jonkinlaisen tietojenkalastelun kautta, jolla hyökkääjä pyrkii saamaan ensimmäisen jalansijan kohde organisaatioon. Tästä ei monesti ole pitkä matka siihen, että organisaation tärkeimmät tunnukset on myös murrettu ja hyökkääjällä on täysi pääsy organisaation kaikkeen tietoon ja järjestelmiin. Kuvassa 5 on Enisan näkemys vuoden 2022 ”tärkeimmistä” hyökkäysvektoreista.


Kuva 5. Tärkeimmät hyökkäysvektorit 2022 (Lella ym. 2022, 8)

Näistä uhista suurimmassa osassa käytetään hyväksi tavalla tai toisella mahdollisia identiteetin- ja pääsynhallinnan heikkouksia. Heikot salasanat, monivaiheisen tunnistuksen puute, loki kirjauksien puute ja näiden valvonta, vähimpien oikeuksien periaatteen noudattamatta jättäminen ja automaation puute ovat esimerkkejä identiteetin- ja pääsynhallinnan heikkouksista, joita hyödyntämällä hyökkääjä voi saada jalansijan organisaatioon.

Organisaatiossa oli jo käytössä kohtuullisen laajasti monivaiheinen tunnistautuminen. Selvitettäväksi jatkokehittämiseen jäi, missä on vielä puutteita monivaiheisen tunnistamisen osalta ja korjata nämä puutteet mahdollisimman nopeasti, jotta hyökkääjillä olisi yksi kerros lisää selvitettävänä ja puolustajalla yksi kerros enemmän aikaa reagoida.

Yksi selkeä puute löydettiin vähimpien oikeuksien periaatteen toteutumisesta. Käytössä ei ole selkeää prosessia sille, miten toimitaan, kun käyttäjä vaihtaa työtehtäviä – poistetaanko vanhat oikeudet ja lisätään uudet vai lisätäänkö uudet vain vanhojen päälle. Ei myöskään löydetty selkeää prosessia, miten toimitaan kaikkien järjestelmien osalta, kun käyttäjä poistuu organisaation palveluksesta. Osa järjestelmistä on tietyllä tapaa automaation piirissä ja käyttäjätunnukseen aktiivihakemiston kautta liitettyjen ryhmäjäsenyyksien poistaminen

poistaa oikeudet näistä järjestelmistä, mutta sama ei tapahdu manuaalisen hallinnan piirissä olevissa järjestelmissä. Näihin voikin jäädä edelleen pääsyoikeuksia, jotka ovat pahimmillaan käyttäjän käytettävissä, vaikka organisaation sähköinen identiteetti olisikin poistettu.

Koska organisaatiolla ei ole toimivaa ja automatisoitua järjestelmää identiteetin- ja pääsynhallintaan niin järjestelmiin jää monesti roikkumaan orpoja tilejä, joita rikolliset sitten pyrkivät hyödyntämään. Järjestelmän puute aiheuttaa myös sen, että näiden orpotilien hyödyntämistä ei välttämättä huomata, koska mistään ei nähdä, että näitä tilejä on pyritty hyödyntämään järjestelmiin kirjautumiseen tai että niillä olisi tehty useita virheeseen päättyneitä kirjautumisyrityksiä, kun tunnusta on yritetty murtaa.

Jos myöskään monivaiheinen tunnistautuminen ei ole käytössä, ja vähimpien oikeuksien periaate ei toteudu, on hyvin suuri riski joutua onnistuneen hyökkäyksen uhriksi. Hyökkääjän saadessa jo heti alussa haltuunsa tunnuksen, jolla on myös hallintaoikeuksia, ei hyökkääjän tarvitse juurikaan nähdä vaivaa päästäkseen kiinni organisaation kaikkein tärkeimpään tietoon.

Näiden syiden takia organisaatioiden tulisi panostaa riittävästi identiteetin- ja pääsynhallinnan toteuttamiseen riittävällä tasolla. Riittävän tason määrittäminen on aina tehtävä organisaatiokohtaisesti eikä siihen ole olemassa yksiselitteisiä vastauksia. Monesti ISO 27001 -vaatimuksiin sopivan tietoturvan hallintamallin rakentaminen ja ylläpitäminen on liian raskasta ja vaativaa, mutta toisten organisaatioiden toiminnan kannalta se voi olla jopa edellytys toiminnalle. Toisaalta ISO 27001 ja varsinkin ISO 27002 tarjoavat hallintakeinoja, jotka toteuttamalla kyberturvallisuuden tasoa identiteetin- ja pääsynhallinnan osalta voidaan merkittävästi kasvattaa.

Suurin osa löydöksistä on niin vahvassa yhteydessä kunnolliseen identiteetin- ja pääsynhallinnan järjestelmään, että niille ei nykytilanteessa ja käytössä olevilla välineillä voida tehdä oikein mitään. Toki prosesseja voidaan lähteä parantamaan, mutta toimenpiteiden ollessa pelkästään ihmisen muistin varassa on hyvin todennäköistä, että tilanne ei parane ilman kunnollista identiteetin- ja pääsynhallinnan järjestelmän käyttöönottoa ja ennen sitä tapahtuvaa vision, tahtotilan sekä politiikan määrittämistä.

### 8.3 Lainsäädännöstä ja asetuksista nousevat vaatimukset

Kolmas tutkimuskysymys selvitti, minkälaisia vaatimuksia identiteetin- ja pääsynhallinnalle kohdistuu lainsäädännöstä ja asetuksista. Vaatimuksia asettavat lainsäädännöt ja asetukset ovat ainakin:

- EU:n yleinen tietosuoja-asetus (GDPR)
- Tietosuojalaki
- Laki yksityisyydensuojasta työelämässä
- NIS2.

EU:n yleinen tietosuoja-asetus on ollut tullut voimaan 24.5.2016 ja se soveltaminen on alkanut 25.5.2018. GDPR:n ydin on tietomurtojen ja henkilötietojen väärinkäytösten estäminen ja siinä on siten suora linkki myös identiteetin- ja pääsynhallintaan. Keskeisiä kyvykkyyksiä, joilla GDPR:n vaatimuksiin voidaan vastata ovat muun muassa monivaiheinen tunnistus, roolipohjainen pääsynhallinta, tiedon minimointi ja federaatio.

Tietosuojalaki tarjoaa tarkennuksia GDPR:ään ja pitää sisällään kansallisen soveltamisen vaatimukset GDPR:n osalta. Kansallinen tietosuojalaki tuli voimaan 1.1.2019 ja korvasi samalla henkilötietolain. Rikoslaissa on määritetty tietosuojalaissa määritetyistä tietosuojarikkomuksista seuraavat rangaistukset, jotka vaihtelevat teon mukaan sakkorangaistuksesta kahden vuoden vankeuteen.

Yksityisyydensuoja työelämässä -laki määrittää, miten työntekijästä tietoa saadaan eri järjestelmiin kerätä ja mitä tietoa niihin saadaan tallentaa. Lähtökohtaisesti kaikki tieto on kerättävä henkilöltä itseltään ja ainoastaan tarpeelliset työsuhteen kannalta oleelliset tiedot saadaan kerätä.

NIS2 direktiivi ja siihen liittyvä kansallinen lainsäädäntö on astumassa voimaan lokakuussa 2024. NIS2 asettaa vaatimuksia hyvin monelle organisaatiolle ja noudattamatta jättämisestä on mahdollista saada sakkoja, joilla voi olla tuntuvia vaikutuksia organisaation toimintaan. Sakkojen lisäksi toimitusjohtajalta voidaan evätä tehtävänsä hoitaminen eli siinäkin mielessä organisaatioiden johdolta aletaan edellyttää toimia tietoturvan parempaan hallitsemi-

seen. Yhtenä tärkeänä osana näiden vaatimusten täyttämisessä on identiteetin- ja pääsynhallinta, jota ei voida enää pelkästään kotikutoisilla menetelmillä hoitaa.

Kuten Asikainen (2024) on todennut, ISO 27001 -standardin omaavilla organisaatioilla on paremmat edellytykset täyttää NIS2-direktiivin vaatimukset. Tämän takia ISO 27001-standardin pohjalta laadittiin vaatimusmäärittely, johon on pyritty tunnistamaan kaikki identiteetin- ja pääsynhallintaan joko suorasti tai epäsuorasti liittyvät vaatimukset. Tämän vaatimusmäärittelyn vaatimuksiin vastaamalla pystytään suurelta osin täyttämään NIS2-direktiivin asettamat vaatimukset identiteetin- ja pääsynhallinnan osalta. Taulukko on liitteenä (liite 2) ja hyödynnettävissä myös muiden organisaatioiden tarpeisiin. Tämä ei kuitenkaan tarkoita sitä, että organisaation tulee hakea myös sertifiointia ISO 27001-standardille, vaan tällä pyritään pelkästään auttamaan NIS2-direktiivin vaatimusten täyttämisessä identiteetin- ja pääsynhallinnan osalta. Läpikäynnissä tunnistettiin yhdeksän (9) suoraan liitännäistä ISO 27001:sta identiteetin- ja pääsynhallinnan alueelle kohdistuvaksi. Epäsuoria liitännäisiä tunnistettiin kuusitoista (16) kappaletta. Instant27001-organisaation tekemä taulukko on liian laaja pelkästään identiteetin- ja pääsynhallinnan vaatimusten täyttämiseen NIS2:n osalta ja tämän takia päädyttiin luomaan oma vaatimusmäärittely.

### 8.4 Kehitystoimenpiteet parhaiden käytäntöjen ja vaatimusten käyttöönotolle

Neljäs ja viimeinen tutkimuskysymys tarjosi vastauksia siihen, minkälaisia kehittämistoimenpiteitä tulee tehdä, jotta parhaat käytännöt saadaan käyttöön ja erilaisiin vaatimuksiin pystytään vastaamaan.

Tämä onkin sitten se kaikista vaikein kysymys vastattavaksi. Organisaation kypsyystaso identiteetin- ja pääsynhallinnan osalta on sen verran matala, että lähtökohtaisesti työ täytyisi aloittaa aivan alusta. Ensin tulisi määrittää strategia ja visio, joiden avulla voidaan määrittää mitä tavoitetta kohti ollaan menossa. Identiteetin ja pääsynhallinnanpolitiikka tulisi määrittää. Vastuut eri järjestelmien identiteetin- ja pääsynhallinnan toteuttamisen osalta tulisi määrit-

tää. Näiden toimenpiteiden jälkeen tulisi tehdä arviointia minkälaista teknologiaa, prosesseja ja niiden kehitystä sekä toimintatapojen muutosta tarvittaisiin isossa kuvassa päämäärien saavuttamiseksi.

Tietyt asiat ovat jo paikallaan, mutta perusta, jonka päälle kaikki on tällä hetkellä rakennettu, on kuin korttitalo mannerlaattojen raja-alueilla. Voi olla, että riskit eivät koskaan toteudu nykyiselläkään rakenteella, mutta riskejä voitaisiin pienentää huomattavasti toimimalla toisin.

## 8.5 Identiteetin- ja pääsynhallinnan järjestelmät

Kuten todettua, kehittämisprojektiin lisättiin lennossa myös muutaman identiteetin- ja pääsynhallinnan järjestelmän vertailu. Järjestelmiä vertailuun otettiin kolme (3) kappaletta ja vertailu on esitetty taulukossa 1.

Taulukko 1. Identiteetin- ja pääsynhallinnan järjestelmien vertailu

| Järjestelmä | Vaatimus / kyvykkyys | Kommentit | +/- |
|---|---|---|---|
| Järjestelmä 1 | Vaatimuksiin vastaaminen | Ei tarjoa vielä kaikkia kyvykkyyksiä tarpeisiin nähden | - |
| Järjestelmä 1 | Käyttöönotto | Helppo | + |
| Järjestelmä 1 | Olemassa oleva osaaminen | Osamista on jonkin verran, mutta vaatii myös kouluttamista | + |
| Järjestelmä 1 | Käyttöliittymä | Erillinen käyttöliittymä ITSM:n lisäksi | - |
| Järjestelmä 1 | Kehitys | Kehittyy nopeasti, mutta kehitykseen ei pystytä vaikuttamaan | - |
| Järjestelmä 1 | Integroitavuus | Integroitavuus kohtuullisen hyvä, mutta ei täytä kaikkia tarpeita | - |
| Järjestelmä 1 | Lisensointi | Tarvitsee todennäköisesti lisälisensointia, tämä nostaa kustannuksia | + |
| Järjestelmä 1 | Hinta | Hinta ei vielä täysin tiedossa. Uusia ominaisuuksia tulossa, näiden hinta ei tiedossa | - |
| Järjestelmä 2 | Vaatimuksiin vastaaminen | Täyttää kaikki tämän hetken tarpeet | + |
| Järjestelmä 2 | Käyttöönotto | Kohtuullisen helppo | + |
| Järjestelmä 2 | Olemassa oleva osaaminen | Osamista on jonkin verran, mutta vaatii myös kouluttamista | + |
| Järjestelmä 2 | Käyttöliittymä | ITSM ja IAM / IGA mahdoolista saada samaan järjestelmää, yksi käyttöliittymä loppukäyttäjille | + |
| Järjestelmä 2 | Kehitys | Kehitys mahdollista organisaation tarpeiden mukaan, mm. konnektorit eri järjestelmiin | + |
| Järjestelmä 2 | Integroitavuus | Valmiit konnektorit moniin onprem ja pilvipohjaisiin järjestelmiin | + |
| Järjestelmä 2 | Lisensointi | Vaatii uutta lisensointia | - |
| Järjestelmä 2 | Hinta | Hinta on kustannustehokas | + |
| Järjestelmä 3 | Vaatimuksiin vastaaminen | Vastaa tämän hetkisiin tarpeisiin | + |
| Järjestelmä 3 | Käyttöönotto | Helppo | + |
| Järjestelmä 3 | Olemassa oleva osaaminen | Osaamista on taustalla oleviin työkaluihin | + |
| Järjestelmä 3 | Käyttöliittymä | Erillinen käyttöliittymä ITSM:n lisäksi | - |
| Järjestelmä 3 | Kehitys | Ei tiedossa miten kehitystä on mahdollista saada | - |
| Järjestelmä 3 | Integroitavuus | Valmiit konnektorit moniin onprem ja pilvipohjaisiin järjestelmiin | + |
| Järjestelmä 3 | Lisensointi | Vaatii uutta lisensointia | - |
| Järjestelmä 3 | Hinta | Hinta on kustannustehokas | + |

Järjestelmä 1 oli tietyllä tapaa jo organisaation käytössä, mutta ei siinä laajuudessa, että sitä voitaisiin varsinaisesti pitää keskitettynä identiteetin- ja pääsynhallinnan järjestelmänä. Järjestelmässä oli vielä myös vaatimuksiin ja tarvittaviin kyvykkyyksiin nähden sellaisia puutteita, joiden takia sen tarkempaa

analyysiä ei nähty tarpeellisena. Myös järjestelmän hinta ja lisensointi olivat epävarmoja vertailuajankohtana.

Järjestelmä 3 vastasi toiminnallisuuksiltaan ja teknologialtaan organisaation nykytilan teknologiaa. Siinä nähtiin tiettyjä positiivisia asioita kuten se, että osaamista niihin teknologioihin löytyy jo. Toisaalta heikkoutena nähtiin näiden teknologioiden kyvykkyydet. Järjestelmä 3 on myös tietyllä tapaa sidoksissa Järjestelmän 1:n teknologiaan ja rakentuu pitkälti tämän järjestelmän teknologiapinon päälle. Siinä mielessä myös kustannuksiin voisi olla tulevaisuudessa tulossa muutoksia, tämä nähtiin yhtenä heikkoutena.

Järjestelmä 2 tarjosi parhaat vastineet vaatimuksille ja kyvykkyyksille kustannustehokkaasti. Hyvät integraatiokyvykkyydet ilman lisäkehitystä nähtiin hyvänä ja positiivisena asiana sen lisäksi, että järjestelmään on mahdollista kehittää myös muita tarpeellisia rajapintoja kustannustehokkaasti. Myös se tosiasia, että tämä järjestelmä olisi mahdollista toteuttaa samaan käyttöliittymään ITSM-järjestelmän kanssa helpottaisi loppukäyttäjäkokemusta operoinnin tapahtuessa yhden käyttöliittymän kautta. Valintamme oli siis tässä kohtaa Järjestelmä 2.

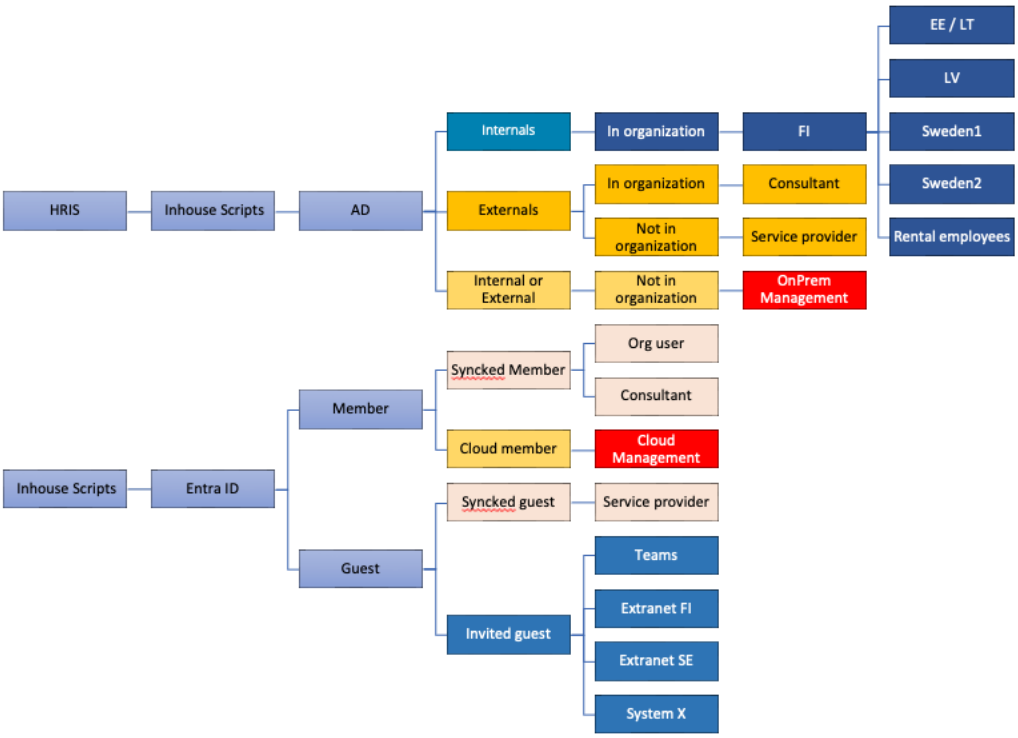
Järjestelmän 2:n osalta käynnistettiin sopimusneuvottelut sekä suunnittelu käyttöönottoprojektin osalta, joka olisi alustavan suunnitelman perusteella toteutettavissa kahdessa vaiheessa. Ensimmäisessä vaiheessa hoidettaisiin ulkoisten käyttäjien kuten konsulttien identiteetin- ja pääsynhallinta ja toisessa vaiheessa organisaation sisäisten käyttäjien identiteetin- ja pääsynhallinta. Näillä vaiheistuksilla saataisiin projektia vietyä eteenpäin rasittamatta liikaa organisaation eri toimintoja ja kuitenkin samaan aikaan saadaan aikaan myös huomattavia parannuksia identiteetin- ja pääsynhallintaan. Käyttöönotto järjestelmän osalta ei kuitenkaan kuulunut projektin alkuperäiseen suunnitelmaan ja se jääkin tehtäväksi jatkokehityksenä.

# 9 JOHTOPÄÄTÖS

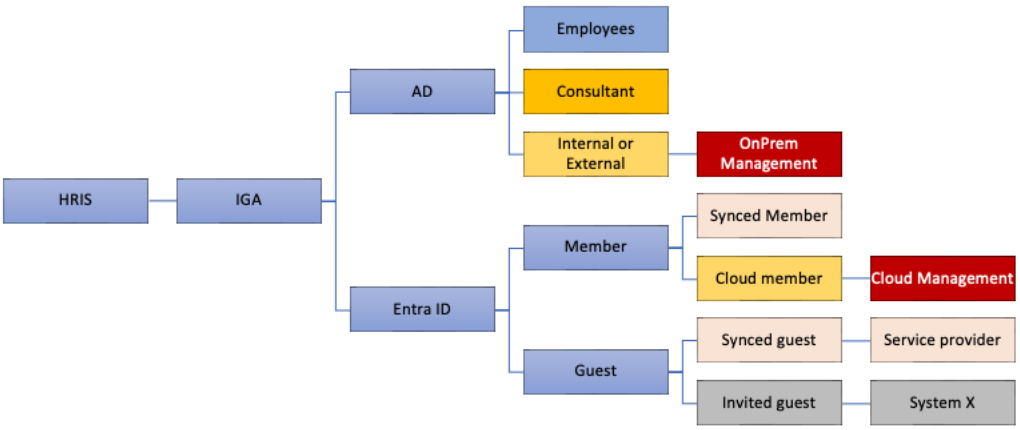
Kehitysprojektin alkuperäisenä tavoitteena oli kehittää olemassa olevia prosesseja ja parantaa automaation astetta identiteetin- ja pääsynhallinnan

osalta. Tätä ei kuitenkaan pystytty täysin toteuttamaan puutteellisten lähtötietojen takia. Toisenlaisilla pohjatiedoilla työn tavoitteet olisi määritetty toisin. Oma alustava arvio nykytilasta oli optimistisempi, kuin mitä tilanne oikeasti olikaan. Tämä aiheutti haasteita työn tekemisen suhteen ja lopputulos ei tietyllä tapaa vastaa alkuperäiseen tarpeeseen. Toisaalta nyt saatujen työn tulosten kautta on mahdollista oppia ja saada hyvät lähtökohdat identiteetin- ja pääsynhallinnan kehittämiselle. Työtä on kuitenkin edelleen paljon tehtävänä mutta nyt on selkeä suunta, miten tilannetta saadaan parannettua ja mitä toimenpiteitä se vaatii.

Joitain prosessin osia pyrittiin kuitenkin kartoittamaan ja määrittämään tavoitetilaa näiden osalta. Kuvassa 6 on nykytila ja kuvassa 7 tavoitetila. Käytännössä tavoitteena on siis yksinkertaistaa nykytilannetta ja saattaa prosesseja helpommin monistettaviksi kaikkiin toimintamaihin.




Kuva 6. Nykytila




Kuva 7. Tavoitetila

Identiteetin- ja pääsynhallinnan visio, tavoitetila ja pääsynhallintapolitiikka olisi määriteltävä ensimmäisenä. Näin saadaan määritettyä selkeät tavoitteet, joita lähdetään tavoittelemaan. Näille tavoitteille voidaan määrittää vaiheet, kuinka maaliin voidaan päästä. Suurin osa prosesseista vaati kehittämistä, jotta harmonisointi kaikkiin maihin voitaisiin toteuttaa, tämä mahdollistaisi myös jonkin kaupallisen tuotteen käyttöönoton. Lisäksi paikalliseen lainsäädäntöön ja asetuksiin tulee tutustua, jotta voidaan varmistaa vaatimustenmukaisuuden täyttäminen.

Organisaatiossa määritetyn tietoturvapolitiikan vaatimuksiin ei tällä hetkellä pystytä vastaamaan. Vähimpien oikeuksien periaate ei toteudu, eikä myöskään liiketoimintasovellusten osalta voida siirtää vastuuta pääsynhallinnasta ratkaisupäälliköiden tai sovellusvastaavien niskaan, jos ei käytettävissä ole kunnollista identiteetin- ja pääsynhallinnan ratkaisua, eikä selkeitä määritettyjä prosesseja kuinka tulisi toimia. Kaikkia näitä haasteita ei pystytä nykyisellä konfiguraatiolla ja käytössä olevalla teknologialla poistamaan vaan se vaatisi identiteetin- ja pääsynhallinnanjärjestelmän käyttöönottamisen.

Jatkokehityksenä tulisi luoda myös dokumenttipohjat, joiden avulla voitaisiin määrämuotoisesti ja yhtenevästi kuvata sovelluskohtaiset identiteetin- ja pääsynhallinnan vaatimukset. Dokumentti voisi sisältää esimerkiksi tiedot:

- sovelluksen sisäisistä rooleista sekä niiden mallintamisesta identiteetin- ja pääsynhallinnan järjestelmään
- hyväksyntäketjuista
- tunnistautumistavoista
- myönnettyjen oikeuksien auditointi tavoista sekä määräajoista
- käyttäjätunnuksesta tarvittavista attribuuteista.

Tämä auttaisin identiteetin- ja pääsynhallinnan käytäntöjen luomisessa hallintajärjestelmään sekä toisi tekemiseen tarvittavaa struktuuria.

## 10 POHDINTA

Veritiksen (Veritis s.a) erille nostama – lähde liikkeelle loppu mielessä – pätee kyllä äärimmäisen hyvin moneen asiaan. Jos tällä mentaliteetilla olisi lähdetty tämän työn tekemiseen olisi todennäköisesti saatu aikaan parempia tuloksia sekä vielä enemmän hyötyjä. Nyt lopputulos osittain lässähtää, kun alussa ei tehty ennen projektin määrittämistä tarpeeksi esikartoitusta nykytilasta. Jos olisi lähdetty liikkeelle siitä, että onko organisaatiossa määritetty identiteetin- ja pääsynhallinnan strategiaa, visiota, politiikkaa tai tahtotilaa olisi projektin sisältö ollut erilainen. Todennäköisesti liikkeelle olisi lähdetty näiden määrittämisestä, ne olisivat olleet työn tavoitteena ja sitä kautta lopputulos olisi ollut toisenlainen. Tämän jälkeen myös asioiden kehittäminen olisi ollut helpompaa ja koko tekemiselle olisi ollut vankka selkänoja. Jälkiviisaus se on parasta viisautta ja sen takia ei kannata jäädä murehtimaan liikoja vaan ottaa tästä opit talteen. Ja niitä oppeja tuli tämän matkan varrella useita.

Organisaatioiden johdon on tänä päivänä entistä syvällisemmin tutustuttava erilaisiin kyberturvallisuuden vaatimuksiin. Näitä vaatimuksia tulee muun muassa lainsäädännöstä ja asetuksista. Johdon tulee myös tunnistaa oma vastuunsa näihin vaatimuksiin vastaamisessa. Tätä vastuuta ei voi ulkoistaa vaan johto on aina viime kädessä vastuussa. Johdon vastuulla on riittävän resursoinnin (henkilöstön sekä rahoituksen) varmistaminen. Näiden resurssien avulla voidaan tehdä toimenpiteitä, joilla kyberturvallisuuden riskejä sekä uhkia voidaan pienentää tai ne voidaan mahdollisesti jopa hetkellisesti poistaa. Riskeihin ja uhkiin vastaaminen vaatii siis jatkuvaa panostusta, eikä voida tuudittautua hetkeksikään hyvän olon tunteeseen – kun tähänkään asti ei ole mitään sattunut niin tuskin sattuu myöhemminkään. Jos näin toimitaan, mennään pahasti pieleen ja seuraukset voivat olla katastrofaalisia.

Ilman organisaation tarpeisiin ja vaatimuksiin vastaavaa identiteetin- ja pääsynhallinnan järjestelmää on todella vaikea täyttää lakien ja asetusten vaatimuksia. Myöskään parhaisiin käytäntöihin tai standardien vaatimuksiin ei pys-

tytä vastaamaan ilman oikeanlaista järjestelmää. Tänä päivänä erilaisia liiketoimintasovelluksia ja järjestelmiä on niin paljon, että ainoastaan automaatioilla ja oikealla identiteetin- ja pääsynhallinnan järjestelmällä voidaan vastata niistä aiheutuviin haasteisiin. Oikeanlaisella järjestelmällä ja automaatioilla voidaan myös saavuttaa niin suuria hyötyjä, että suurin osa järjestelmän hankkimisesta aiheutuneista kuluista sekä vuotuisista lisenssikustannuksista saadaan kuitattua muun muassa virheiden vähenemisen, kasvaneen järjestelmän turvallisuuden ja manuaalisten työvaiheiden poistumisen kautta.

Lakien ja asetuksen tulkinta on myös todella aikaa vievää puuhaa. Jotta niistä pääsee jyvälle ja saa oikeastaan mitään konkreettista irti, joutuu käyttämään aika paljon aikaa ja tämä on tietyllä tapaa hyvin kuluttavaa. Monesti lakien ja asetusten määrityksissä ei ole mitään konkreettista, miten tulisi oikeasti toimia. Nämä konkretiat löytyvät paremmin parhaista käytännöistä ja erilaisista standardeista kuten ISO 27001 ja ISO 27002. Tämä ei kuitenkaan tarkoita sitä, että lakien ja asetusten läpikäymisen voisi jättää välistä. Tähän työhön voisi ehkä kuitenkin olla järkevää käyttää jotain niihin perehtynyttä kumppania. Kumppani voisi luoda yhteenvedon niistä asioista joihin organisaation tulee keskittyä vaatimukset täyttääkseen. Näin toimien kustannus on todennäköisesti pienempi, kuin oman asiaa tuntemattoman henkilöstön aiheeseen tutustumiseen käyttämään aikaan kuluvat kustannukset. Lisäksi on todennäköisempää, että kaikki tarvittavat asiat tulee huomioitua ostamalla yhteenveto kumppanilta.

Organisaation tulisi viestiä myös eri politiikkojen päivityksestä riittävällä tavalla organisaation henkilöstölle ja muille tärkeille sidosryhmille. Itse huomasin tietoturvapolitiikan päivittyneen opinnäytetyön viime metreillä. Onneksi mitään isompia muutoksia ei ollut tullut ja tehdyillä muutoksilla ei onneksi ollut vaikutusta tämän opinnäyte työn toteuttamiseen. Ei voida kuitenkaan olettaa, että henkilöstö ja sidosryhmät omatoimisesti ymmärtäisivät säännöllisin väliajoin käydä tarkistamassa, ovatko dokumentaatiot päivittyneet. Suurin ongelma kommunikaation puutteessa on se, että henkilöstö ja sidosryhmät saattava käyttää pitkäänkin olettamusta vanhojen linjausten voimassa olemisesta ja näin ollen toimia väärin ja vastoin uusia linjauksia.

Identiteetin- ja pääsynhallinnan suunnitteleminen ja siitä huolehtiminen ei voi olla yksin IT-osastojen tekemistä, siihen tulee omalta osaltaan velvoittaa myös muita organisaation osia kuten HR-osasto. Myös liiketoiminnalla on merkittävä rooli roolien ja pääsynhallinnan määrittämisessä sekä hallinnoimisessa. Jos organisaatiolla on toimintaa useammassa maassa, tulisi identiteetin- ja pääsynhallinnan prosesseissa huomioida mahdolliset erot toimintamaiden lakien ja asetusten osalta. Näillä saattaa olla hyvinkin merkittävää vaikutusta siihen, miten vaatimuksiin pystytään vastaamaan ja ne voivat vaikuttaa myös prosesseihin sekä teknologian valintaan.

Yksityisen sektorin organisaatioiden kannattaisi joissain tapauksissa hyödyntää myös julkisen sektorin toteuttamia linjauksia ja vaatimuksia. Näissä on monesti jopa aivan konkreettisia toimenpiteitä, miten asioita voidaan tai pitää jonkin vaatimuksen saavuttamiseksi toteuttaa. Yhtenä hyvänä esimerkkinä tästä on Salmisen omassa opinnäytteessään luoma tehtävien ja niihin liittyvien viranomaisvaatimusten ja suositusten välinen yhteys (Salminen 2022, liite 2). Tästä olisi todennäköisesti moniin yksityisen puolen organisaatioiden identiteetin- ja pääsynhallinnan haasteisiin saatavissa apua.

Oman osaamisen kannalta opinnäytetyö oli todella mielenkiintoinen ja uutta osaamista tuli moneen asiaan. Se myös vahvisti jo aiemmin ollutta näkemystä identiteetin- ja pääsynhallinnan keskeisestä asemasta kyberturvallisuuden toteuttamisessa. Toisaalta opinnäytetyön tekeminen oli todella haastavaa oman työtilanteen takia. Samaan aikaan oli käynnissä monia suuria projekteja ja niiden lisäksi vielä niin sanotut normaalit työtehtävät. Sitten kun opinnäytetyöhön kunnolla pääsi paneutumaan, lähinnä aikataulupaineen takia, kirjoittaminen ja työn edistäminen sujui ihan kohtuullisen hyvin. En kuitenkaan voi mitenkään lämpimästi suositella tätä tyyliä kenellekään, joka yrittää ruuhkavuosien keskellä perheellisenä samaan aikaan käydä vielä täysipäiväisesti töissä.

Työn edistäminen oli hyvinkin itsenäistä, toimeksiantajan ohjaajalta ei juurikaan tullut ohjausta. Toisaalta meillä oli kuitenkin hyvä ja paljon organisaation historiaakin tunteva tiimi. Näiden henkilöiden kanssa tuli moneen otteeseen asioita palloteltua ja sparrailtua ja sai muutenkin tukea tekemiseen. Suuri kiitos teille.

Muutamia vinkkejä muille opinnäytetyön tekijöille. Kannattaa olla tarkka hakiessaan erilaisia lainsäädäntöön liittyviä aineistoja Finlexistä, ettei käy kuten minulle. Eli käytin aivan turhaan aikaani vanhentuneiden lakien tarkasteluun – valitse ajantasainen lainsäädäntö ja keskity pelkästään niihin, ellet sitten oikeasti halua tarkastella myös poistuneita lakitekstejä. Lainatessa tekstiä lähteistä kannattaa heti laittaa ylös mistä lainasi ja mitä, muuten voi olla haastavaa kaivella näitä jälkikäteen. Ja oppilaitosten ohjeituksiin on hyvä tutustua aiemmin kuin myöhemmin, niin välttyy monelta päänsäryltä.

Vaikka työ ei aivan täysin toteutunut kuten alussa määritettiin, tiedän tästä kuitenkin olevan paljon hyötyä sekä tilaajaorganisaatiolle että myös itselleni. Organisaatio saa listan konkreettisista toimenpiteistä, jotka täyttämällä on mahdollista viedä organisaation kypsyystaso aivan uudelle tasolle identiteetin- ja pääsynhallinnan osalta. Näiden toimenpiteiden suorittamisen jälkeen pystytään vastaamaan paremmin lakien ja asetusten vaatimuksiin nyt ja tulevaisuudessa. Itse opin työtä tehdessä paljon uutta ja oma ammatillinen osaaminen karttui oikein mukavasti.

## LÄHTEET

Asiakainen, M. 2024. NIS2-direktiivi ja laki kyberturvallisuuden riskienhallinnasta – mistä on kyse? WWW-dokumentti. Saatavissa: https://gofore.com/nis2-direktiivi-ja-laki-kyberturvallisuuden-riskienhallinnasta-mista-on-kaan-kyse/ [viitattu 21.1.2024].

CyberArk. s.a. Principle of Least Privilege. WWW-dokumentti. Saatavissa: https://www.cyberark.com/what-is/least-privilege/ [viitattu 1.4.2024].

Das, R. 2022. Ransomware and Idenity and Access Management. WWW-dokumentti. Saatavissa: https://platform.keesingtechnologies.com/ransomware-and-identity-and-access-management/ [viitattu 11.4.2024].

Enisa. 2023. Enisa threat landscape 2023. PDF-dokumentti. Saatavissa: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport [viitattu 11.4.2024].

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.

Grassi, P., Garcia, M. & Fenton, J. 2017. Digital Identity Guidelines. PDF-dokumentti. Saatavissa: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf [viitattu 17.3.2024].

Ferraiolo, D. & Kuhn, R. 2016. Role Based Access Control RBAC. WWW-dokumentti. Päivitetty 22.6.2020. Saatavissa: https://csrc.nist.gov/Projects/Role-Based-Access-Control/faqs [viitattu 8.4.2024].

Fortra s.a. WWW-dokumentti. Saatavissa: https://www.coresecurity.com/blog/whats-difference-between-iam-iga-and-pam. [viitattu 26.11.2023].

Fryzel, C. 2021. Defining IAM and IGA. HumanID. WWW-dokumentti. Saatavissa: https://human-id.org/blog/defining-iam-and-iga/ [viitattu 26.11.2023].

Helsingin yliopisto. s.a. Monivaiheinen tunnistautuminen (MFA). WWW-dokumentti. Saatavissa: Monivaiheinen tunnistautuminen (MFA) | Opiskelijan digitaidot (helsinki.fi) [viitattu 1.4.2024].

Instant27001. s.a. WWW-dokumentti. Saatavissa: https://instant27001.com/iso-27001-use-cases/nis-2-0/ [viitattu 21.1.2024].

Irwin, L. 2021. ISO 27001 vs. ISO 27002: What's the difference. WWW-dokumentti. Saatavissa: https://www.itgovernance.co.uk/blog/understanding-the-differences-between-iso-27001-and-iso-27002 [viitattu 3.4.2024].

Kananen, J. 2015. Kehittämistutkimuksen kirjoittamisen käytännön opas: Miten kirjoitan kehittämistutkimuksen vaihe vaiheelta. Jyväskylä: Juvenes Print.

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona: opas opinnäytetyön ja pro gradun kirjoittajalle. Jyväskylä. Jyväskylän ammattikorkeakoulun julkaisuja 232. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 12.11.2023].

Kattainen, P. 2023. Mikä on NIS2 ja miten se vaikuttaa liiketoimintaasi? WWW-dokumentti. Saatavissa: https://www.advania.fi/blogi/mika-on-nis2-ja-miten-se-vaikuttaa-liiketoimintaasi [viitattu 24.3.2024].

Kyberturvallisuuskeskus. 2023. Traficom laatii suositusta NIS2-direktiivin kyberturvallisuuden riskienhallinnan toimenpiteistä. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-laatii-suositusta-nis2-direktiivin-kyberturvallisuuden-riskienhallinnan [viitattu 22.1.2024].

Laki yksityisyyden suojasta työelämässä 13.8.2004/759

Lella, I., Tsekmezoglou, E., Theocharidou, M., Magonara, E., Malatras, A., Svetozarov Naydenov, R., Ciobanu, C. 2023. Enisa threat landscape 2023. PDF-dokumentti. Saatavissa: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport [viitattu 7.4.2024].

Linden, M. 2017. Identiteetin- ja pääsynhallinta. WWW-dokumentti. Saatavissa: https://trepo.tuni.fi/bitstream/handle/10024/128471/linden_identiteetin_ja_paasynhallinta.pdf?sequence=1 [viitattu 26.11.2023].

Loihde Trust. s.a. Kertakirjautuminen - SSO. WWW-dokumentti. Saatavissa: https://www.loihdetrust.com/palvelut/kertakirjautuminen-sso/ [viitattu 1.4.2024].

Loihde Trust. s.a. NIS2-direktiivi. WWW-dokumentti. Saatavissa: https://www.loihdetrust.com/nis2-direktiivi/?gad=1&gclid=CjwKCAjwpJWoBhA8EiwAHZFzfnQ4tQpqsBME-BAYj4RrRJsbU8IZ81qciliA2nMZ1xjKdNXMse1Rb-BoCqYcQAvD_BwE [viitattu 27.10.2023].

Mayer, L., Romero, S., Bertoli, G., Burt, T., Wainert, A. & Ferres, J. s.a. How Effective is multifactor authentication at deterring cyberattacks? WWW-dokumentti. Saatavissa: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW166ID?culture=fi-fi&country=fi [viitattu 1.4.2024].

NIST. 2009. About NIST. WWW-dokumentti. Päivitetty 11.1.2022. Saatavissa: https://www.nist.gov/about-nist [viitattu 28.11.2023].

NIST. s.a. Separation of Duty (SOD). WWW-dokumentti. Saatavissa: https://csrc.nist.gov/glossary/term/separation_of_duty [viitattu 4.4.2024].

NIST. 2020. Roadmap: NIST Special Publication 800-63.4 Digital Identity Guidelines. WWW-dokumentti. Päivitetty 17.3.2023. Saatavissa: https://www.nist.gov/identity-access-management/roadmap-nist-special-publication-800-63-4-digital-identity-guidelines [viitattu 19.1.2024].

NIST. 2023. NIST's Digital Identity Guidelines Update – Kicking off Revision 4!. PDF-dokumentti. Saatavissa: https://www.nccoe.nist.gov/sites/default/files/2023-01/digital-identity-guidelines-kickoff-revision-4-presentation.pdf [viitattu 20.1.2024].

Ojansalo, K., Moilanen & T., Ritakoski, J. 2015. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. 3.-4. painos. Helsinki: Sanoma Pro Oy.

One Identity s.a. 8 Best Practices for Identity and Access Management. PDF-dokumentti. Saatavissa: https://www.oneidentity.com/whitepaper/8-best-practices-for-identity-and-access-management827122/ [viitattu 19.11.2023].

OKTA. s.a. 2023a. Your NIS2 compliance checklist: 7 steps to prepare. PDF-dokumentti. Saatavissa: https://www.okta.com/sites/default/files/2023-09/Okta NIS2 Compliance Checklist.pdf [viitattu 23.3.2024].

OKTA. s.a. 2023b. Why Identity is Important Whils Preparing for NIS2 Compliance. PDF-dokumentti. Saatavissa: https://www.okta.com/sites/default/files/2023-09/Okta NIS2 Compliance Whitepaper.pdf [viitattu 24.3.2024].

OKTA. 2021. Identity is key to stopping these 5 cyber security attacks. PDF-dokumentti. Saatavissa: https://www.okta.com/sites/default/files/2021-06/Okta_Identity-Is-Key-to-Stopping-These-5-Cyber-Security-Attacks.pdf [viitattu 7.4.2024].

OpenText 2018a. How Identity and Access Management helps meet the data protection requirements of GDPR. WWW-dokumentti. Saatavissa: https://blogs.opentext.com/how-identity-and-access-management-helps-meet-the-data-protection-requirements-of-gdpr/ [viitattu 25.12.2023].

OpenText 2018b. Identity and Access Management is pivotal for GDPR compliance. WWW-dokumentti. Saatavissa: https://blogs.opentext.com/identity-and-access-management-is-pivotal-for-gdpr-compliance/ [viitattu 25.12.2023].

Raina, K. 2023. Zero Trust security explained: principles of the Zero Trust model. WWW-dokumentti. Saatavissa: What is Zero Trust Security? Principles of the Zero Trust Model (crowdstrike.com) [viitattu 1.4.2024].

Rikoslaki 19.12.1889/39

Rousku, K. 2014. Kyberturvaopas: Tietoturvaa kotona ja työpaikalla. Viro: Print Best.

Sailpoint. 2022. 7 Best Practices for Identity Security. WWW-dokumentti. Saatavissa: https://www.sailpoint.com/identity-library/7-best-practices-for-identity-security/ [viitattu 27.3.2024].

Salminen, T. 2022. Identiteetin- ja käyttövaltuushallinnan kehittäminen Sipoon kunnassa. Ylempi amk - opinnäyte. PDF-dokumentti. Saatavissa: https://www.theseus.fi/handle/10024/747649 [viitattu 15.4.2024].

SFS-EN ISO/IEC 27001:2023. 2023. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

SFS-EN ISO/IEC 27002:2022. 2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot.

Tivi. 2021. Tiedätkö, mihin kaikkeen työntekijälläsi on oikeudet? WWW-dokumentti. Saatavissa: https://www.tivi.fi/kumppanisisallot/elisa/tiedatko-mihin-kaikkeen-tyontekijallasi-on-oikeudet/ [viitattu 12.12.2023].

Veho. About Us. 2022. WWW-dokumentti. Saatavissa: https://vehocompany.com/en/about-us/ [viitattu 29.12.2023].

Veritis. s.a. Best Practices for Effective 'Identity and Access Management (IAM) Implementation. WWW-dokumentti. Saatavissa: https://www.veritis.com/blog/best-practices-for-identity-and-access-management-iam-implementation/ [viitattu 31.3.2024].

Instant 27001 – NIS2 artikla 21 vs. ISO 27001:2022

| NIS 2 article 21 | ISO 27001:2022 |
|---|---|
| Policies on risk analysis and information system security | 5.2 Policy;<br>6.1.2 Information security risk assessment;<br>6.1.3 Information security risk treatment;<br>A.5.1 Policies for information security |
| Incident handling | A.5.24 Information security incident management planning and preparation;<br>A.5.25 Assessment and decision on information security events;<br>A.5.26 Response to information security incidents;<br>A.5.27 Learning from information security incidents |
| Business continuity, such as backup management and disaster recovery, and crisis management | A.5.29 Information security during disruption<br>A.5.30 ICT readiness for business continuity;<br>A.8.13 Information backup;<br>A.8.14 Redundancy of information processing facilities |
| Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers | A.5.19 Information security in supplier relationships;<br>A.5.20 Addressing information security within supplier agreements;<br>A.5.21 Managing information security in the ICT supply chain |
| Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure | A.5.19 Information security in supplier relationships;<br>A.5.20 Addressing information security within supplier agreements |

| NIS 2 article 21 | ISO 27001:2022 |
|---|---|
| Policies and procedures to assess the effectiveness of cybersecurity risk-management measures | 9.1 Monitoring, measurement, analysis and evaluation;<br>9.2 Internal audit;<br>9.3 Management review;<br>A.5.35 Independent review of information security;<br>A.5.36 Compliance with policies and standards for information security |
| Basic cyber hygiene practices and cybersecurity training | A.5.1 Policies for information security;<br>A.6.3 Information security awareness, education and training |
| Policies and procedures regarding the use of cryptography and, where appropriate, encryption | A.8.24 Use of cryptography |
| Human resources security, access control policies and asset management | A.5.15 Access control;<br>A.5.16 Identity management;<br>A.5.17 Authentication information;<br>A.5.18 Access rights;<br>A.5.9 Inventory of information and other associated assets;<br>A.6.1-A.6.8 People controls |
| The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate | A.5.14 Information transfer;<br>A.5.17 Authentication information;<br>A.8.5 Secure authentication;<br>A.8.20 Network controls;<br>A.8.21 Security of network services |

NIS2-vaatimukset yhdistettynä ISO 27001:2022 -standardiin

| Liitäntä identiteetin- ja pääsynhallintaan | Hallintakeinon tunniste ISO27001 | Tietoturvan osa-alueet | Lyhyt kuvaus hallintakeinosta |
|---|---|---|---|
| Epäsuora | 5.1 | Hallintotapa ja ekosysteemi<br>Kriisinkestävyys | Tietoturvapolitiikka ja kohdennettavat toimintaperiaatteet on määriteltävä, ylimmän johdon on hyväksyttävä ne, ne on julkaistava, niistä on viestittävä asiaankuuluville henkilöstön jäsenille ja sidosryhmille, näiltä on saatava kuittaus tietojen vastaanottamisesta ja ne on katselmoitava suunnitelluin aikavälein ja aina kun tapahtuu merkittäviä muutoksia. |
| Epäsuora | 5.2 | Hallintotapa ja ekosysteemi<br>Suojaaminen<br>Kriisinkestävyys | Tietoturvaroolit ja -vastuut on määriteltävä organisaation tarpeiden mukaisesti. |
| Suora | 5.3 | Hallintotapa ja ekosysteemi | Keskenään ristiriitaiset tehtävät ja vastuualueet on eriytettävä toisistaan. |
| Suora | 5.15 | Suojaaminen | Säännöt, joilla hallitaan fyysistä ja ohjelmallista pääsyä tietoihin ja niihin liittyviin omaisuueriin on laadittava ja toteuttava liiketoimintaa ja tietoturvallisuutta koskevien vaatimusten mukaisesti. |
| Suora | 5.16 | Suojaaminen | Identiteettien koko elinkaarta on hallittava. |
| Suora | 5.17 | Suojaaminen | Tunnistautumistietojen osoittamista ja hallintaa on ohjattava hallintaprosessilla, johon sisältyy henkilöstön perehdyttäminen tunnistautumistietojen asianmukaiseen käsittelyyn. |
| Suora | 5.18 | Suojaaminen | Pääsyoikeuksia tietoihin ja niihin liittyviin omaisuuseriin on myönnettävä, katselmoitava, muokattava ja poistettava organisaation pääsynhallintaa koskevien toimintaperiaatteiden ja sääntöjen mukaisesti. |

| Liitäntä identiteetin- ja pääsynhallintaan | Hallintakeinon tunniste ISO27001 | Tietoturvan osa-alueet | Lyhyt kuvaus hallintakeinosta |
|---|---|---|---|
| Epäsuora | 5.23 | Hallintotapa ja ekosysteemi Suojaaminen | Pilvipalveluiden hankinnan, käytön ja hallinnan sekä käytön lopettamisen prosessit on laadittava organisaation tietoturvavaatimusten mukaisesti. |
| Epäsuora | 5.27 | Puolustus | Tietoturvahäiriöistä saatua tietämystä on hyödynnettävä tietoturvallisuuden halllintakeinojen vahvistamisessa ja parantamisessa. |
| Epäsuora | 5.28 | Puolustus | Organisaation on laadittava ja toteutettava menettelyt tietoturvatapahtumiin liittyvien todisteiden yksilöimiseen, keräämiseen, muuhun hankkimiseen ja säilyttämiseen. |
| Epäsuora | 5.29 | Suojaaminen Kriisinkestävyys | Organisaation on suunniteltava, miten se ylläpitää riittävää tietoturvallisuustasoa häiriön aikana. |
| Epäsuora | 5.31 | Hallintotapa ja ekosysteemi Suojaaminen | Lakeihin, asetuksiin, viranomaismääräyksiin ja sopimuksiin perustuvat tietoturvallisuuden kannalta tärkeät vaatimukset sekä organisaation toimintamalli niiden täyttämistä varten on yksilöitävä, dokumentoitava ja pidettävä ajantasalla. |
| Epäsuora | 5.34 | Suojaaminen | Organisaation on tunnistettava ja täytettävä vaatimukset, jotka koskevat tietosuoja ylläpitämistä ja henkilötietojen suojaamista, sisältäen sovellettavat lait ja viranomaismääräykset ja sopimusvaatimukset. |
| Suora | 5.37 | Hallintotapa ja ekosysteemi Suojaaminen Puolustus | Tietojenkäsittelypalveluita koskevat toimintaohjeet on dokumentoitava ja niiden on oltava kaikkien niitä tarvitsevien henkilöstön jäsenten saatavilla. |
| Epäsuora | 6.3 | Hallintotapa ja ekosysteemi | Organisaation ja tärkeimpien sidosryhmien henkilöstön on saatava tietoturvaopastusta ja - koulutusta, ja heidän tietojaan organisaation tietoturvapolitiikan, kohdennettujen toimintaperiaatteiden ja menettelyjen muutoksista on päivitettävä säännöllisesti, siinä laajuudessa kuin se on heidän toimenkuvansa kannalta merkityksellistä. |

| Liitäntä identiteetin- ja pääsynhallintaan | Hallintakeinon tunniste ISO27001 | Tietoturvan osa-alueet | Lyhyt kuvaus hallintakeinosta |
|---|---|---|---|
| Epäsuora | 6.5 | Hallintotapa ja ekosysteemi | On määritettävä tietoturvavastuut ja -velvollisuudet, jotka jäävät voimaan työsuhteen päättymisen tai muuttumisen jälkeen. Niistä on viestittävä olennaisille henkilöille ja sidosryhmille, ja niiden noudattaminen on varmistettava. |
| Suora | 8.3 | Suojaaminen | Pääsyä tietoihin ja muihin niihin liittyviin omaisuuseriin on rajoitettava pääsynhallintaa koskevien kohdennettujen toimenpiteiden mukaisesti. |
| Suora | 8.4 | Suojaaminen | Lähdekoodien, kehittämistyökalujen ja ohjelmistokirjatojen luku- ja kirjoitusoikeuksia on hallitava asianmukaisesti. |
| Suora | 8.5 | Suojaaminen | On toteutteva turvallisen pääsyn teknologiat ja menettelyt, jotka perustuvat tietoja koskeviin pääsyrajoituksiin ja pääsynhallintaa koskeviin kohdennettuihin toimintaperiaatteisiin. |
| Epäsuora | 8.10 | Suojaaminen | Tietojärjestelmiin, laitteisiin tai mihin tahansa muuhun tallennusvälineeseen varastoidut tiedot on poistettava, kun niitä enää tarvita. |
| Epäsuora | 8.11 | Suojaaminen | Tietojen peittämistä on käytettävä organisaation pääsynhallintaa koskevien ja muiden asiaan liittyvien kohdennettujen toimintaperiaatteiden sekä liiketoiminnallisten vaatimusten mukaisesti ottaen huomioon olennainen lainsäädäntö. |
| Epäsuora | 8.15 | Suojaaminen Puolustus | On luotava tapahtumalokeja, joihin tallennetaan toiminnot, poikkeamat, vikaantumiset ja muut olennaiset tapahtumat. Nämä lokit on säilytettävä, ja niitä on suojattava ja analysoitava. |
| Epäsuora | 8.17 | Suojaaminen Puolustus | Organisaatiossa käytettävien tietojenkäsittelyjärjestelmien kellojen on oltava synkronoituja hyväksyttävien aikalähteiden kanssa. |
| Epäsuora | 8.31 | Suojaaminen | Kehitys-, testaus- ja tuotantoympäristöt on erotettava, ja niitä on suojattava. |

| Liitäntä identiteetin- ja pääsynhallintaan | Hallintakeinon tunniste ISO27001 | Tietoturvan osa-alueet | Lyhyt kuvaus hallintakeinosta |
|---|---|---|---|
| Epäsuora | 8.32 | Suojaaminen | Tietojenkäsittelypalveluihin ja tietojärjestelmiin tehtäviä muutoksia on hallittava muutoksenhallintamenettelyillä. |

Parhaat käytännöt vs. nykytila – vertailutaulukko

**Toteutuu täysin 0**
**Toteutuu osittain 0**
**Ei toteudu 0**

| Toimittaja / käytäntö | Sisältö | Toteutuminen |
|---|---|---|
| Sailpoint 6. | **6. Utilize Artificial Intelligence (AI) and Machine Learning (ML) (Sailpoint)**<br>Digital transformation, work from anywhere, and adoption of new enterprise apps have introduced so many user entities and points of access that it has become overwhelming to IT departments to keep up with access controls and governance. A human-based identity security approach can only scale so much and has its limitations.<br><br>Organizations need to leverage technologies built on a foundation of AI and ML that can reduce the identity security friction so their operational processes can keep pace with the change of business. With AI and ML organizations can gain new visibility and insight into specific user access needs and risks associated with user access. AI and ML can also help automate and streamline identity processes and decisions such as access requests, role modeling, and access certifications, driving greater efficiencies across an organization. | |
| One Identity 1. | **1. Define your workforce (One Identity)**<br>Your organization's workforce is managed by your personnel or human resources department. They also have to manage information about people who are not employees, such as contractors and consultants.<br><br>Most of these people require access to company resources. The first best practice is to use your HR systems as much as possible as an authoritative source of data for your identity and access management system. This will help you avoid repetitive work, errors, inconsistencies and other problems as the IAM system grows. Ideally, you'll provide some kind of managed front-end, such as a web-based interface that can be used to verify the quality of the imported data, revise data as needed and so on. | |
| | **2. Define identities (One Identity)**<br>The next best practice is to implement a single, integrated system that provides end-to-end management of employee identities and that retires orphaned or unneeded identities at the appropriate time. This is where IT responsibility formally begins in the identity management lifecycle. Typically, you'll identify the following:<br>• A primary directory service (often Active Directory)<br>• A messaging system (such as Exchange Server or Lotus Notes)<br>• A primary Enterprise Resource Planning (ERP) system (such as SAP)<br>Once identified, these crucial systems are integrated into the overall identity management architecture. Why focus on these three kinds of systems? Primarily because they deliver a "quick win," providing identity integration across the mostvisible and most-used resources that users interact with on a daily basis. More systems can be integrated later.<br><br>In reality, each disparate system will continue to have its own user accounts. Your integrated system simply maps identities to these accounts, and you'll often use a web-based front-end to manage that mapping process. There will invariably be a few identities that can't be automatically mapped, and the front-end will allow those to be handled on an exception basis. | |

| | | |
|---|---|---|
| One Identity 2.<br>Sailpoint 7. | **7. Centralize Your System (Sailpoint)**<br>With such an explosion of activity (including number of users, applications, databases, and portals), it's imperative that IT teams have broader visibility across all identities. But as an enterprise scales, it becomes increasingly difficult to get a 360-degree view into identity security. The best practice here is to create a centralized system so security teams have broader visibility into resource and application access, user behavior and anomaly tracking across the entire organization. This means that your organization will need to select an identity security solution that can provide this centralized view into every user identity. | |
| One Identity 3. | **3. Provide knowledge and control to business owners (One Identity)**<br>You also need to regularly answer the question, "Who has access to what?" IT coordinates the inventory of identities and permissions and provides that information to business data owners and custodians. Again, a web-based front-end is ideal for this. The idea is to let business data owners manage access to their data and to provide central reporting and control over those permissions. | |
| One Identity 4. | **4. Implement workflow (One Identity)**<br>Although technology is always about embracing change, unmanaged change causes problems. Implementing a "request and approval" workflow provides an efficient way to manage and document change. A self-service user interface (often web-based) enables users to request permission to resources they need. Data owners and custodians can respond to these requests, helping the business ensure appropriate access, while removing IT from the decision-making role in permissions management.<br><br>You might begin by defining different kinds of permission sets, each with its own workflows. This enables different kinds of data and tasks to be treated appropriately, depending upon their sensitivity. Take the time to define who can control that list of services, who is responsible for managing workflow designs and so on. For example, financial data might require more extensive approvals when changing permissions than company-wide information (such as details about the next company picnic), which might be changed with relatively little workflow required. | |
| | **5. Automate provisioning (One Identity)**<br>You need to manage new users, users who leave the organization and users who move or are promoted or demoted within the organization. Provisioning,<br>deprovisioning and re-provisioning are often timeconsuming manual tasks, and automating them can not only reduce overhead but also reduce errors<br>and improve consistency.<br><br>These provisioning tasks typically involve connections to numerous systems, including email, ERP and databases. Prioritize these systems so that the most important and visible ones can be automated first, and clearly define and document the flow of data between these systems and your identity management toolset. Focus first on automating the basic add/change/delete tasks for user accounts, and then integrate additional tasks such as unlocking accounts. | |

| | | |
|---|---|---|
| One Identity 5.<br>Sailpoint 4. | **4. Automate Onboarding and Offboarding (Sailpoint)**<br>Identity security involves the task of onboarding and offboarding an organization's workers. When onboarding a new employee, contractor, vendor, or partner, for example, IT always needs to assess which privileges and permissions the worker should be granted based on their unique user roles. But for large enterprises, this can be extremely complex, especially if there is only a manual process of provisioning in place which often leads to a high margin of error.<br><br>Fortunately, with an Identity Security solution in hand, companies can automate onboarding and offboarding processes, saving IT departments time and money, increase productivity by ensuring new employees have the access they need from day one, and reduce risk by quickly deprovisioning users as needed (such as when they leave or move to another department within the company). | |
| One Identity 8. | **8. Manage roles (One Identity)**<br>Permissions are best assigned to job roles rather than to individuals. Making those roles correspond to real-life job tasks and job titles is a powerful way to manage identities and access over the long term. A certain amount of inventorying and mining will be needed to accurately identify the major roles within your organization, based at least, in part, on the resource permissions currently in force. Through user self-service IT shopping cart, users request access to the appropriate resources and services. This way, a user can request access to "non-personal human resources information" (for example) without needing to understand the underlying technical details required to make that happen. Once a user places such a request, the owner or custodian of the affected data has the opportunity to review and either approve or deny the request—taking IT out of the permissions management loop entirely.<br><br>You'll also need to define who will manage these roles in order to ensure that roles are created, modified and deactivated only by authorized individuals following the proper workflow. | |
| | **1. Clearly Define IAM Vision (Veritis)**<br>The critical fundamental for successful Identity and Access Management (IAM) implementation is understanding it as a combination of technology solutions and business processes to manage identities and access corporate data and applications.<br><br>Start to tie in business processes with your IAM program from the concept stage itself.<br>Build your current and future IT capabilities, such as cloud-based implementations based on the current IT and network infrastructure.<br>Engineer the roles between users and applications regarding privileges, rules, policies, and constraints.<br>Map access privileges to business roles, identify excessive privileges, accounts, and redundant/dead groups.<br>Make sure to fulfill all auditing requirements to be in line with compliance regulations, privacy, and data governance policies. This will help the teams make informed decisions.<br>Take the enterprise-wide approach in implementing authorization procedures, security, and management, integration across domains part of your IAM architecture. | |

| | | |
|---|---|---|
| Veritis 1.<br>Sailpoint 1.<br>One Identity 6. | **1. Begin with the End in Mind (Sailpoint)**<br>The impetus for an identity security solution is usually the result of a pain point within the enterprise. Perhaps the helpdesk is overburdened with access requests and password resets. Maybe the organization recently failed a compliance audit, or the IT team has discovered excess user permissions. It could also be that the adoption of cloud-based applications has decreased security visibility while increasing the complexity of the IT ecosystem. Or worse, perhaps you've experienced a data breach.<br><br>As with any large enterprise project, the first step is to determine where you want to end up. This means aligning the project to the organization's overall strategic objectives. You can't reach a destination if you don't know where you're going.<br><br>**6. Become compliant (One Identity)**<br>Many companies are now affected by one or more industry or governmental regulations, and your identity management system can play a central, beneficial role in helping you become and remain compliant. You'll need to focus on clearly defining and documenting the job roles that have control over your data, as well as the job roles that should have access to auditing information. Define compliance rules step by step, and assign each step to a responsible job role. Integrate rule checking in your identity management system and workflow operations to help automate remediation of incorrect actions; this will help improve consistency and security as well as compliance. | |
| Veritis 2.<br>Sailpoint 2 | **2. Develop A Strong Foundation (Veritis)**<br>This requires a comprehensive evaluation of IAM product capabilities and its sync with organizational IT. This should be followed by an effective risk assessment of all organizational applications and platforms.<br><br>The assessment should ideally cover:<br><br>Comparison between standard and in-house, and their versions<br>Identification of OS, third-party apps currently in use and mapping with the functionalities offered by the IAM program<br>Customizations made to fulfill new requirements<br>Technological capabilities and limitations<br>Don't forget to involve IAM Subject Matter Experts (SMEs) in standardizing and enforcement of the IAM policy.<br><br>**2. Eliminate High-Risk Systems (Sailpoint)**<br>Historically, organizations have been hesitant to move from on-premises solutions to those in the cloud because of potential security threats. But on-prem data centers and applications are, in fact, riskier than their cloud-based counterparts. This is because cloud service providers offer a wealth of security capabilities that can't be matched by onsite resources. Furthermore, onsite data systems require considerable manpower, money and resources to keep hackers and data breaches at bay, with more resources required every day. This is not sustainable.<br><br>By sunsetting legacy systems and switching to a cloud service provider, enterprises can boost security through patch management, segmentation, encryption, integrations, and secure access requirements | |

| | | |
|---|---|---|
| Veritis 4. | **4. Stakeholder Awareness (Veritis)**<br>Unlike usual training sessions, the IAM program-related stakeholder awareness program should cover detailed training on the underlying technology, product abilities, and scalability factors.<br><br>Each IAM solution implementation awareness program should have an approach tailored to the requirements of different user communities.<br><br>More than anyone, IT teams require detailed know-how of the IAM program and its core activities. Even the Operations team should be aware of the capabilities across different stages of the IAM lifecycle.<br><br>The training process should be a continuous activity and should happen in tandem with the changing processes or emerging capabilities. | |
| Veritis 5. | **5. Consider Identity as Primary Security Perimeter (Veritis)**<br>Organizations should shift from the traditional focus on network security to considering identity as the primary security perimeter. With the explosion of cloud and remote working culture, network perimeter is becoming increasingly porous, and perimeter defense can't be effective. Centralize security controls around user and service identities. | |
| Veritis 6. | **6. Enforce Multi-Factor Authentication (Veritis)**<br>Enable Multi-Factor Authentication (MFA) for all your users, including administrators and C-suite executives. It checks multiple aspects of a user's identity before allowing access to an application or database, instead of regular sign-in aspects. MFA is an integral part of identity and access management. | |
| Veritis 7. | **7. Establish Single Sign-On (Veritis)**<br>Organizations must establish Single Sign-On (SSO) for their devices, apps, and services so users can use the same set of credentials to access the resources they need, wherever and whenever. You can achieve SSO by using the same identity solution for all your apps and resources, whether on-premises or in the cloud. | |
| Veritis 8.<br>Sailpoint 5. | **8. Implement Zero-Trust Policy (Veritis)**<br>The zero-trust model assumes every access request as a threat until verified. Access requests from both inside and outside of the network are thoroughly authenticated, authorized, and scrutinized for anomalies before granting permission.<br><br>**5. Embrace a Zero Trust Approach to Security (Sailpoint)**<br>Zero trust is a network security framework that is becoming essential for every enterprise, and Identity Security is the cornerstone of an effective zero trust strategy. The zero trust approach dictates that no user or application – whether inside or outside of an organization's network – should automatically be trusted until their identity has been fully verified. This is also known as the principle of never trust, always verify. In addition, a successful identity-centric Zero Trust model relies on the principle of least privilege, ensuring that all users have the least amount of access to do their job successfully — no more, no less.<br><br>With more and more employees now working entirely outside of a corporate network – and using multiple devices across various applications – organizations need to fully embrace the zero trust philosophy in order to better protect critical systems and data. | |
| Veritis 9. | **9. Enforce a Strong Password Policy (Veritis)**<br>Implement an organization-wide password policy to ensure users set strong passwords for access. Make sure that employees update their passwords regularly and avoid using sequential and repetitive characters. | |

| | | |
|---|---|---|
| Veritis 10. | **10. Secure Privileged Accounts (Veritis)**<br>Securing privileged accounts is imperative to protect critical business assets. Limiting the number of users having privileged access to the organization's critical assets reduces the chance of unauthorized access to a sensitive resource. You must isolate the privileged accounts from the risk of being exposed to cybercriminals. | |
| Veritis 11.<br>Sailpoint 3.<br>One Identity 7. | **11. Conduct Regular Access Audits (Veritis)**<br>Organizations must regularly conduct access audits to review all the granted accesses and check if they are still required. As users often request additional access or want to revoke their access, these audits help you manage such requests accordingly.<br><br>**3. Routinely Review and Remove Orphaned Accounts (Sailpoint)**<br>Within every organization, there is constant change particularly in regard to the workforce. For example, when a user moves to a different area of the organization, or leaves, that user's access needs to be adjusted or properly removed from the network. Failure to deprovision and remove an account leads to what's called an "orphaned" account — it contains the previous user's data but no longer has an assigned user.<br><br>Left undetected, orphaned accounts are a goldmine for hackers. These accounts can allow them to gather credentials and ultimately take on the identities of these previous users, leading to security breaches and attacks. This is why it's essential for enterprises to have comprehensive onboarding and offboarding measures in place.<br><br>**7. Check and recheck (One Identity)**<br>In a well-designed identity management system, permissions are typically assigned to job roles rather than to individuals, but organizations are still likely to simply assign permissions as needed and never review them again. This practice invites security risks.<br><br>Permissions require periodic recertification—<br>you need to review who has access to what and determine whether or not they should still have those permissions. Define job roles within your organization that can recertify permissions, such as system owners, managers, information security officers and so forth. Recertification can be defined<br>in a workflow in which data owners and custodians review a current permission set and verify the accuracy (or inaccuracy) of that set. The idea is to regularly make sure that the roles and people who have permissions to resources should continue to have those permissions.<br><br>This process should also include recertification of job role membership to ensure that the users assigned a given job role are still performing that role within the organization. | |
| Veritis 12. | **12. Implement Passwordless Login (Veritis)**<br>Passwordless login is the process of authenticating users without the need for a password. It prevents scenarios where cybercriminals leverage weak and repetitive passwords to gain access to the network. Passwordless login can be implemented through various approaches, including email-based login, SMS-based login, and biometrics-based login. | |

Lähteet

7 Best Practices for Identity Security | SailPoint
8 Best Practices for Identity and AM (oneidentity.com)
Identity and Access Management Implementation: Best Practices (veritis.com)