Korkeakoulun työharjoitteluprosessin tietoturvallisuuden kehittäminen

Julius Alenius

2020 Laurea

Laurea-ammattikorkeakoulu

Korkeakoulun työharjoitteluprosessin tietoturvallisuuden kehittäminenError! No text of specified style in document.

Julius Alenius
Tietojenkäsittely
Opinnäytetyö
Toukokuu, 20202020

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittely
Tietojenkäsittelyn koulutusohjelma
Tradenomi (AMK)

Julius Alenius

Korkeakoulun IT-harjoitteluprosessin tietoturvallisuuden kehittäminen Error! No text of specified style in document.

2020 2020 Sivumäärä 43

Tämän opinnäytetyön tavoite oli osana organisaation laajuista riskienhallintaprosessia analysoida suomalaisen korkeakoulun IT-harjoitteluprosessin tietoturvallisuuden tasoa sekä löytää niiden pohjalta kehitysehdotuksia parantamaan prosessin tietoturvallisuutta. Opinnäytetyön toissijainen tarkoitus on toimia tapaustutkimuksena muille opetusalalla toimiville organisaatioille. Toimeksiantajana opinnäytetyössä toimi tutkittu ammattikorkeakoulu, jonka nimi on tietoturvallisuussyistä vedetty pois opinnäytetyöstä.

Opinnäytetyössä esitetään kehitysehdotuksia parantamaan tutkitun ammattikorkeakoulun IT-harjoitteluprosessin tietoturvallisuutta käyttäen menetelmänä asiantuntijoiden teemahaastattelua sekä lomakekyselyä joka lähetettiin nykyisille ja entisille harjoittelijoille. Lisäksi tietoperustana toimi myös päämenetelmänä toiminut potentiaalisten ongelmien analyysi eli POA jonka tavoitteena oli löytää ja analysoida tietoturvariskejä IT-harjoitteluun liittyen.

Tutkimuksen tuloksena löydettiin ja analysoitiin kaksikymmentäseitsemän eri riskiä liittyen IT-harjoitteluprosessiin jotka lajiteltiin riskikohtaisesti kategorioittain. Niiden ja haastatteluiden sekä kyselyiden perusteella esitettiin neljä keskeistä kehitysehdotusta kehittämään IT-harjoitteluprosessia. Kehitysehdotuksina esitettiin auditointi, liiketoiminnallisten vaikutusten analyysi, tietoturvakoulutus sekä turvallisuusselvitys.

Asiasanat: tietoturva, riskienhallinta, riskianalyysi, turvallisuusjohtaminen

Laurea University of Applied Sciences **Abstract**

Degree Programme in Business Information Technology
Bachelor's Thesis

Julius Alenius

Development of Information Security Practices of a university of applied sciences' IT-Traineeship process

2020 2020 Pages 43

The goal of this Bachelor's thesis was to analyse and develop the information security level of a university of applied sciences' IT traineeship process as part of an organization wide risk management process and to find development suggestions based on the findings of the subsequent research. At the same time a secondary goal of this thesis was to act as a case study for other organizations in the education industry. The client for this thesis was the subject university of applied sciences, the name of which has been redacted from this paper for information security reasons.

This thesis presents development ideas to improve the state of information security of IT-trainee process in the subject university using themed interviews and form questionnaires as research methods. Potential problem analysis acted as the primary method an information base for this thesis that aimed to discover and analyse risks relating to the IT trainee process.

As a result twenty seven individual risks were found and further categorized into separate categories. Based on the analysed risks and interviews and questionnaires, four development ideas were presented as follows: security audit, business impact analysis, information security training and security clearance inspection.

Keywords: information security, risk management, risk analysis, security governance

Sisällys

1 Johdanto

On jo kliseistä puhua siitä, kuinka tietotekniikka on valtaamassa työelämän jokaista osa-aluetta, sillä niin on ollut jo kauan. Erinäisten prosessien siirtäminen nopeasti ja vaivattomasti käytettäviin tietoteknisiin järjestelmiin tuo organisaatioille suurta arvoa mutkattomien, tehokkaiden sekä nopeiden prosessien myötä. Erityisesti ammattikorkeakoulujen järjestelmissä käsitellään valtavia määriä asiakkaiden sekä sidosryhmien dataa, ja erilaiset verkossa tarjottavat opintokokonaisuudet ovat mullistaneet ja tulevat mullistamaan opetusalaa. Organisaatiossa työskentelevät tarvitsevat päivittäisessä työssään tietokoneen lisäksi taustalla pyöriviä järjestelmiä, jotka mahdollistavat etätyöskentelyn esimerkiksi tunneloidun VPN- järjestelmän tai työtehtävien suorittamisen erilaisien järjestelmien avulla. Kaikki tämä vaatii tietoturvallisuutta varmistamaan, että käyttäjien ja sidosryhmien data prosessoidaan sekä käytetään turvallisesti.

Opinnäytetyö on osa organisaation laajuista riskienhallintaprosessia, jonka tavoite on koko organisaation koordinoitu johtaminen riskien osalta tutkimuksen kohteena toimineessa organisaatiossa eli kohdeorganisaatiossa. Tämä opinnäytetyö keskittyy korkeakoulun tietohallinnon service desk- palveluun osana tätä kokonaisuutta.

Tämän opinnäytetyön tavoitteena on tarjota tutkimuksen kohteena toimineelle ammattikorkeakoululle tutkittuja sekä perusteltuja ehdotuksia kehittämään harjoitteluprosessia riskienhallinnan sekä tietoturvan osalta, mutta myös tarjota muille lukijoille kuvauksen siitä minkälaisia tietoturvauhkia sekä haasteita riskienhallintaprosessille ammattikorkeakouluissa voi liittyä ja miten niihin voi vastata. Lopuksi tullaan vielä käymään läpi opinnäytetyön tekijän pohdintoja opinnäytetyöprosessista, tutkimuksen toteutuksesta sekä kohdeorganisaatiosta.

Tähän tutkimukseen on kerätty aineistoa keskisuuresta suomalaisesta ammattikorkeakoulusta jonka servicedesk- palvelut on tuotettu pääosin IT-harjoittelijoiden kautta, eli toisin sanoin kyseisen ammattikorkeakoulun tietohallinto rekrytoi sisäisesti opiskelijoitaan suorittamaan harjoittelujaksoaan servicedeskiin. Tutkimuksessa selvitetään minkälaisia riskejä kohdistuu harjoittelijoiden toimintaan, ja pyritään hahmottamaan tutkitun ammattikorkeakoulun IT-harjoitteluprosessin tietoturvan taso. Havaintojen perusteella tässä tutkimuksessa tullaan esittämään kehitysehdotuksia parantamaan IT-harjoitteluprosessin käytänteitä sekä tukikeinoja riskienhallintaprosessille pääasiassa IT-harjoitteluprosessin saralta.

2 Työn lähtökohdat

Tämä opinnäytetyö tehtiin osana riskienhallintaprosessia, jonka tavoite on kehittää ammattikorkeakoulun harjoittelutoimintaa turvallisemmaksi ja siten omalta osaltaan taata tietoturvallinen ympäristö ammattikorkeakoulun henkilöstölle sekä opiskelijoille. Tutkimus sai

alkunsa, kun tutkimuskohteessa työskentelevä toimihenkilö teki aloitteen riskianalyysistä tai riskien kartoituksesta organisaatiossa, jossa opinnäytetyön tekijä suoritti työharjoitteluaan. Tämä tutkimus on osa kohdeorganisaationa toimineen kokonaisvaltaista turvallisuustrategiaa.

2.1 Tutkimuskohde

Tämän tutkimuksen kohteena on toiminut keskisuuri etelä-suomalainen ammattikorkeakoulu. Tutkimuskohteen valintaan on vaikuttanut opinnäytetyön tekijän suorittama harjoittelujakso IT ServiceDeskissä tutkimuskohteena olleen ammattikorkeakoulun tietohallinnossa.

Tutkitussa ammattikorkeakoulussa työskentelee vuosittain noin kymmenestä- kahteentoista tietojenkäsittelyn opiskelijaa (IT-asiantuntija, Liite 4) servicedesk- palvelussa joka vastaa IT-lähituen, laitehallinnan sekä päivittäisten IT- tehtävien toteutuksesta jokaisessa ammattikorkeakoulun toimipisteessä, ja jonka palveluja käyttää koko ammattikorkeakoulun henkilöstö ja opiskelijat. Harjoittelijat käyttävät päivittäisissä tehtävissään tunnuksia, joilla on laaja pääsy ammattikorkeakoulun eri järjestelmiin ja laitteisiin. Tämä tarkoittaa sitä, että harjoittelijat pystyvät halutessaan tekemään muutoksia järjestelmiin sekä heillä on pääsy suureen määrään heille kuulumatonta tietoa. Erään IT-asiantuntijan (Liite 4) mukaan erityisesti IT- harjoittelijat muodostavat suurimman maineriskin ammattikorkeakoululle, sillä heillä on pääsy henkilöstön dataan.

2.2 Tutkimusongelma sekä tutkimuskysymykset

Tutkimuksen pääpaino on riskienhallinnassa sekä hyvien tietoturvallisten käytänteiden määrittelyssä. Harjoittelijan sekä IT-asiantuntijoiden roolien erilaisten työnkuvien myötä opinnäytetyön tekijä esittää hypoteesin, että näkemykset hyvien käytänteiden osalta sekä kokemukset niiden toteutumisesta voivat vaihdella harjoittelijoiden ja asiantuntijoiden kesken. Tutkimuksessa käytetään aineiston keräyksessä määrällisen sekä laadullisen tutkimuksen menetelmiä kyselylomakkeen ja teemahaastatteluiden muodossa, joita käytetään myös testaamaan tätä hypoteesia.

Tämä tutkimus pyrkii tarjoamaan kehitysehdotuksia sekä ideoita IT-harjoittelijoiden toiminnan tietoturvalliseen johtamiseen, joita voidaan hyödyntää riskienhallintaprosessissa osana koko organisaation laajuista turvallisuusstrategiaa. Tutkimus pyrkii siis vastaamaan kysymykseen siitä, miten ammattikorkeakoulut voisivat kehittää IT-harjoitteluprosessiaan tietoturvallisuuden osalta. Tutkimuksessa pyritään myös osoittamaan, miksi organisaatioiden tulisi ottaa tietoturvallisuus huomioon paitsi IT-harjoittelun, mutta myös muiden prosessien osalta niiden jokaisella osa-alueella.

Tutkimuksessa on tarkoitus kartoittaa kohdeorganisaation IT-harjoitteluprosessin tietoturvallisuustason nykytila sekä kerätyn aineiston pohjalta tarjota kehitysehdotuksia organisaation tietohallinnolle parantamaan harjoitteluprosessia tietoturvallisempaan

suuntaan. Joten ulkopuolelle tämän tukimuksen aiheesta on rajattu operatiiviset toimenpiteet kuten esimerkiksi järjestelmien käyttöönotto tai jatkoanalyysin tekeminen tutkimusten tulosten pohjalta.

Aineisto on kerätty yhdestä ammattikorkeakoulusta, mutta tämä tutkimus pyrkii kerätyn aineiston perusteella esittämään kehitysehdotuksia, jotka voivat olla toteutuskelpoisia myös muissa organisaatioissa, joissa toimii IT-harjoittelijoita.

Tässä tutkimusraportissa esitetään myös tutkimuksen tavoitteisiin liittyvää teoriaa tietoturvan määritelmistä, menetelmistä sekä kuvataan tietoturvan vaikutus ja osallisuus koko organisaation turvallisuustrategiaan. Näin pyritään luomaan kokonaiskuva organisaation eri osa-alueiden tietoturvatarpeista sekä demonstroidaan mikä tietoturvan rooli on organisaation kokonaisturvallisuudessa. Teoriaosuudessa käydään myös läpi yleisiä tietoturvariskejä ja niiden hyökkäysvektoreita sekä määritetään riski.

2.3 IT-harjoittelijat

IT- harjoittelijat työskentelevät IT- tuen tehtävissä ja harjoittelijoiden työnkuvaan kuuluu monipuolisesti asiakaspalvelun ja teknisen tuen tarjoaminen sekä laitteiden ja tunnusten ylläpito. Harjoittelijat ovat vastuussa myös työpyyntöjen ja tapausten välittämisestä eteenpäin organisaation sisäisille IT- asiantuntijoille sekä ulkoisille toimijoille kuten palveluntarjoajille. IT- harjoittelijat työskentelevät pääsääntöisesti ennalta määritellyssä kampuksessa vaihdellen sijaintia aika ajoittain.

Asiakkaat koostuvat pääosin ammattikorkeakoulun henkilöstöstä ja opiskelijoista, jotka voivat luoda työpyyntöjä tikettijärjestelmän avulla IT-tukeen tai vaihtoehtoisesti saapua fyysisesti paikalle IT- tuen tiloihin, joissa asiakkaita autetaan ensin paikan päällä, ja tarvittaessa tapauksesta luodaan tapaus tikettijärjestelmään selvitystä varten. Tähän lukeutuu käyttäjien ohjeistusta ja avustamista tietoteknisten laitteiden ja ammattikorkeakoulun sähköisten palvelujen käytössä, pienimuotoista laitehuoltoa sekä sovellustenhallintaa asennusten ja vikatilanteiden hallinnan muodossa. Harjoittelijat ovat myös omalta osaltaan vastuussa käytöstä poistuvien laitteiden käsittelystä sekä uusien laitteiden, kuten puhelimien ja tietokoneiden luovutuksesta esimerkiksi uusille työntekijöille. Vaikka harjoittelijan työnkuva on itsenäistä, työskentelee heidän tukenaan vakituisia IT- asiantuntijoita ylläpitäjinä, jotka varmistavat muiden vastuidensa lisäksi paikallisen IT-tuen toiminnan pysyvän esteettömänä ja tehokkaana. Ylläpitäjät ratkaisevat myös vaativampia IT- tapauksia sekä perehdyttävät ja neuvovat harjoittelijoita.

2.4 Keskeiset käsitteet

Service desk	Kommunikaatiokeskus, jonka tehtävä on toimia kontaktipisteenä asiakkaille ja varmistaa ajankohtainen tuki.
Arkaluontoinen data	Dataa, johon käsiksi pääsy aiheettomasti voi aiheuttaa vahinkoa organisaatiolle tai järjestelmälle.
Hyökkäysvektori	Reitti haavoittuvuuden hyödyntämiseksi. Tekijä, joka mahdollistaa haavoittuvuuden hyväksikäyttämisen (Laurio 2014).
Haittaohjelma	Ohjelma, joka aiheuttaa tarkoituksenmukaisesti ei-toivottuja toimintoja tietojärjestelmässä.
SQL	Structured Query Language. Kieli, jolla pystytään manipuloimaan tietokantojen tietokenttiä.
Palvelin	Ohjelma tai laite, joka tarjoaa toiminnallisuuksia muille järjestelmille yleensä tietokoneverkon kautta.
Sessio	Väliaikainen tiedonvälitys kahden laitteen tai käyttäjän ja laitteen välillä.
Autentikaatio	Käyttäjän tai prosessin identiteetin todentaminen.
XML	Extensible markup language. Merkintäkielien standardi, jolla pystytään tallentamaan ja määrittelemään dataa ohjelmistojen lähdekoodissa.
Palvelunestohyökkäys	Distributed Denial of Service eli DDoS. Hyökkäys, jossa pyritään ruuhkauttamaan tai keskeyttämään palvelinten toiminta kohdentamalla niihin suuri määrä liikennettä.
Akkrediointi	Virallinen todistus siitä, että sertifikaatteja myöntävä taho toimii kansainvälisten standardien mukaisesti (ISO 2020).
Sertifiointi	Kirjallinen todiste siitä, että tuote, palvelu tai järjestelmä vastaa tiettyjä vaatimuksia (ISO 2020).

3 Tietoturva ja riskienhallinta

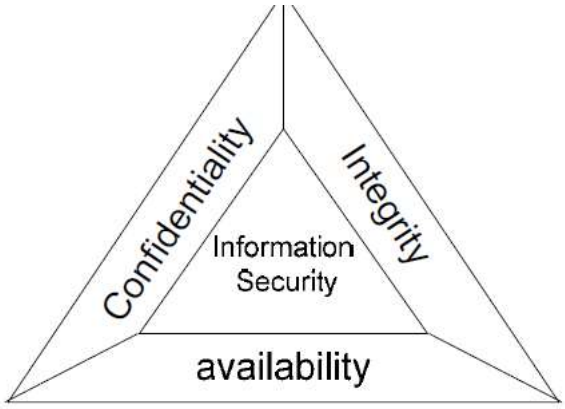
Tässä luvussa tarkastellaan mitä tietoturvallisuus tarkoittaa sekä mikä on sen rooli osana suurempaa kokonaisuutta organisaatiossa. Luvussa käydään läpi myös riskienhallinnan merkitystä organisaatiossa sekä sitä, millä tavalla se on vuorovaikutuksessa

tietoturvallisuuden kanssa. Tässä luvussa myös esitellään yleisimpiä tietoturvariskejä jotka voivat kohdistua ammattikorkeakoulun kaltaiseen organisaatioon.

3.1 CIA Tietoturvallisuuden määritelmänä

CIA on yleisesti tunnistettu ja hyväksytty tapa määritellä tietoturvallisuutta ja dominoiva tapa kuvata tietoturvallisuus kirjallisuudessa (Lundgren & Möller 2017, 420).

CIA eli Confidentiality, Integrity ja Availability (suomeksi luottamuksellisuus, eheys ja saatavuus) on Osei-Brysonin ym. (2008) mukaan tietoturvan kolme ominaisuutta jotka yhdessä muodostavat CIA-kolmion, eli mallin jossa kolme osa-alueta muodostavat yhdessä tietoturvan käsitteen. Luottamuksellisuus tarkoittaa suojautumista luvattomalta pääsyltä dataan tai tietoon järjestelmistä, ja mikäli luottamuksellisuutta pidetään yllä organisaatiossa varmistetaan, että vain luvalliset tahot pystyvät pääsemään käsiksi organisaation dataan ja järjestelmiin. Eheys varmistaa, että organisaation data pysyy ehjänä ja muuttamattomana. Saatavuus tarkoittaa datan tai järjestelmien häiriöiden ja niihin kohdistuvien palvelunesto sekä datanesto hyökkäyksien torjumista (Osei-Bryson ym. 2008) ja sen myötä takaa valtuutetuille tahoille pääsyn järjestelmään tai voimavaraan vaadittaessa (Lundgren & Möller 2017, 423). Saatavuuden tavoitteena on myös pyrkiä palauttamaan järjestelmät häiriöiden tai hyökkäysten sattuessa. Kun tarkastellaan riskienhallinnan tavoitteita ja menetelmiä voidaan luoda yhteys jokaiseen CIA-kolmion osa-alueeseen. Riskiä arvioidessa voidaankin peilata havaintoja CIA-kolmioon (kuvio 1), jolloin pystytään asettamaan riskit omiin viitekehyksiinsä.



Kuvio 1: CIA- malli (Osei-Bryson ym. 2008, 11)

3.2 Vasta-argumentointia CIA-kolmiolle

Lundgren ja Möller (2017, 422-439) esittävät artikkelissaan vasta-argumentteja CIA-kolmiolle. Heidän mukaansa CIA-kolmio on liian laaja mutta samaan aikaan myös liian suppea, eli se esittää ristiriitaisia implikaatioita turvallisuudesta kuvaamalla epäturvalliset tilanteet turvallisiksi ja turvalliset tilanteet epäturvallisiksi. Esimerkiksi tarkastellessa CIA-kolmion

saatavuus (Availability) osiota, voidaan argumentoida että sen määritelmä on ristiriitainen. Joissain tilanteissa Lundgrenin ja Möllerin (2017, 423) mukaan on tarpeellista, että järjestelmä ei ole haluttaessa saatavilla kuten aikalukon osalla. Aikalukon toimintaperiaate on, että se tarjoaa turvallisuutta eväämällä pääsyn resurssiin ennalta määritettyyn aikaan asti, jolloin se olisi ristiriidassa saatavuuden määritelmän kanssa, sillä siihen ei pääsisi käsiin vaadittaessa. Jos taas katsottaisiin aikalukon vertauskuvaa siten että tilanteessa on vain priorisoitu luottamuksellisuutta ja eheyttä, mutta ei kuitenkaan koeta, että turvallisuus on rikottu, voidaan tehdä johtopäätös, että saatavuus ei ole kriittinen osa turvallisuutta.

Artikkelissaan he käyttävät myös vertauskuvaa avoimesta taideteoksesta, jossa jokainen voi muokata teoksen sisältöä ilman että se tuottaa problematiikkaa, vaikka teoksen eheys on rikkoutunut. Tämän vertauskuvan on tarkoitus osoittaa että CIA-kolmion kapeat määritelmät eivät pysty mukautumaan erilaisten järjestelmien luomiin olosuhteisiin.

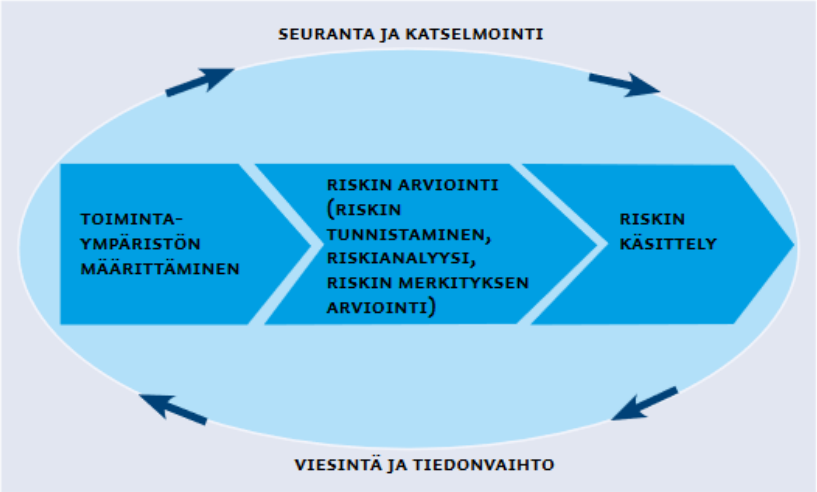
He esittelevät artikkelissaan vaihtoehtoisen mallin, joka perustuu suhteellisille yhteyksille eri sidosryhmien välillä ja, Lundgrenin ja Möllerin (2017, 428) esittämää mallia kutsutaan nimellä asianmukaisen pääsyn määritelmä (Appropriate Access Definiton), lyhennettynä AA englanninkielisen termin mukaan. AA- mallissa turvallisuus määritellään turvallisuuden kohteen, eli objektin suhteesta sidosryhmään ja toimijaan. Näin sidosryhmän vaatimukset siis luovat viitekehyksen objektin turvallisuuden määritelmälle. AA-malli kuvataan artikkelissa (Lundgren & Möller 2017, 428) seuraavasti: ”Objekti on turvallinen, mikäli jokaisella toimijalla on asianmukainen pääsy jokaiseen objektin osa-alueeseen suhteessa sidosryhmään”.

Opinnäytetyön tekijän mielestä AA- malli tarjoaa vaihtoehdon riskienhallintaprosessiin CIA-kolmiolle, mutta AA-mallin sidosryhmäpainotteinen periaate tarkoittaa sitä, että järjestelmien turvallisuusmääritelmät voivat vaihdella sidosryhmästä riippuen. Se tuo mukautuvuutta, mutta myös vaatii suuremman resurssimäärän ylläpitämiseen ja määrittelyyn. CIA-kolmio ei ole järjestelmä tai objektikohtaisesti mukautuva määritelmä, mutta sen staattisuus mahdollistaa viitekehyksien luomisen usealle eri järjestelmälle samanaikaisesti.

3.3 Riskienhallinta

Riskienhallinta on johtamista, jossa pyritään riskien osalta koordinoiden ohjaamaan organisaatiota. Riskienhallintaprosessiin kuuluu riskin tunnistaminen, analyysi ja niiden merkityksen arviointi. Siten se on kokonaisprosessi, joka pyrkii määrittämään toimintaympäristön ja arvioimaan siihen kuuluvat riskit ja niiden käsittelyn (Martikainen, S. & Ranta, T. 2017). Kuviossa 2 (Martikainen, S. Ranta, T. 2017) havainnollistetaan riskienhallintaprosessi esittämällä se jatkuvana prosessina, joka sisältää lineaarisen jatkumon toimintaympäristön määrittämisestä riskien käsittelyyn. Kuvattuna on prosessi, jossa joka osa-alueessa suoritetaan tulosten katselmointia sekä prosessinkulun seurantaa. Jotta organisaatio

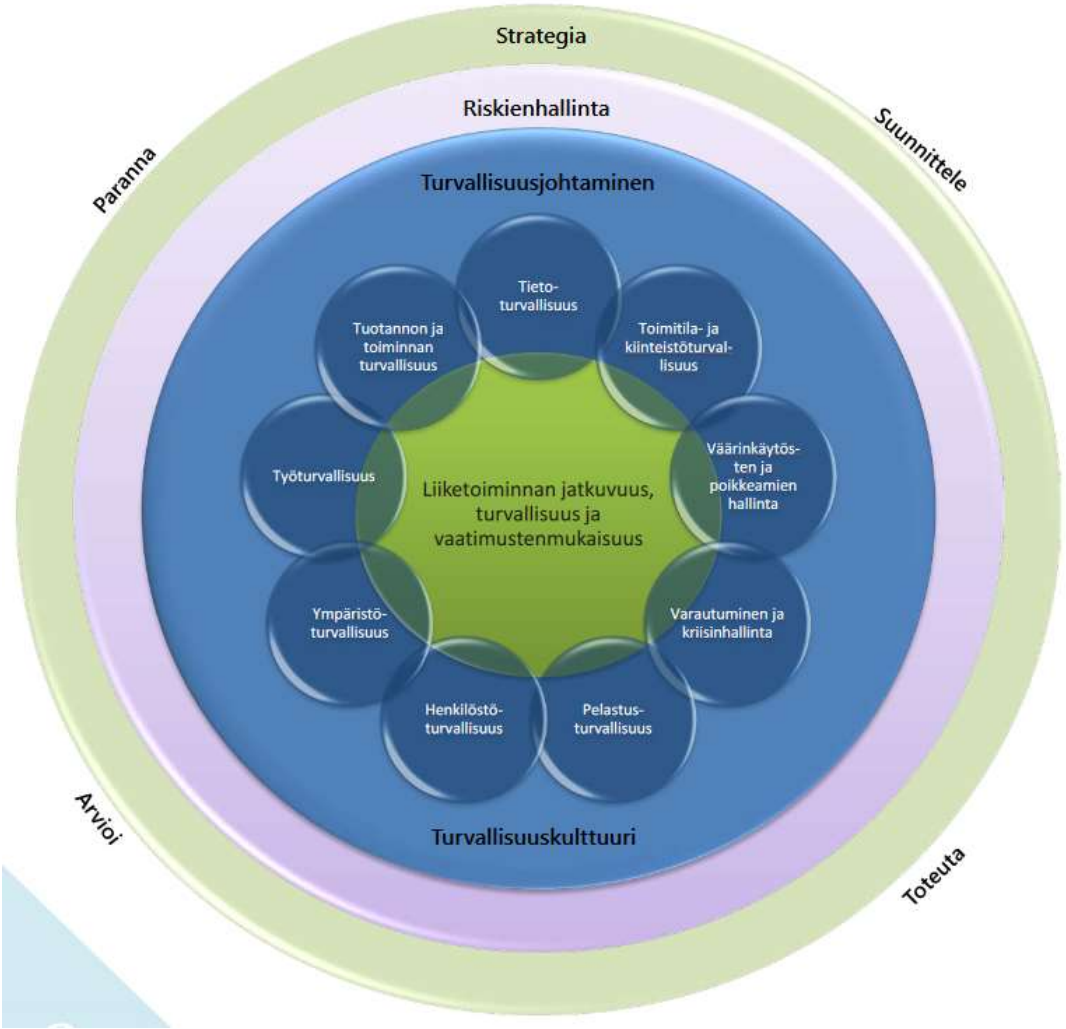
voi hyötyä riskienhallintaprosessista, on tärkeää, että sen tulokset pystytään kommunikoida muulle organisaatiolle, näin riskinkäsittelyprosessi luo uuden prosessin perustuen aiemmin saatun tietoon.



Kuvio 2: Riskienhallintaprosessi (Martikainen, S. Ranta, T. 2017)

Riskienhallinnalle ominaista on koordinoitu sekä ajantasainen toiminta, sekä sen tulee perustua parhaaseen käytettävissä olevaan tietoon. Riskienhallinta on myös tukevana osana organisaation jatkuvassa kehittymisessä, sillä se on osa päätöstentekoprosessia sekä laajempaa organisaation turvallisuus strategiaa.

Elinkeinoelämän keskusliitto (2016) kuvaa mallissaan (kuvio 3) yritysturvallisuuden kokonaisuuden ja sen sisältämät osa-alueet. Yritysturvallisuuden mallissa riskienhallinta kattaa sisäänsä turvallisuusjohtamisen ja kaikki sen osa-alueet, joista tässä tutkimuksessa keskitytään tietoturvaan sekä sen vuorovaikutukseen riskienhallintaprosessissa. Mallin ulkolaidoilla olevat toimenpiteet ”suunnittele”, ”toteuta”,”arvioi” ja paranna” voidaan yhdistää kuviossa 2 avainasemassa oleviin seurantaan ja katselmointiin sekä viestintään ja tiedonvaihtoon. Yritysturvallisuusmalli havainnollistaa sitä, kuinka riskienhallintaprosessi sisältää laajan kokonaisuuden, mutta on myös osa kokonaisvaltaista turvallisuustrategiaa.



Kuvio 3: Organisaation turvallisuustrategiamalli (Elinkeinoelämän keskusliitto. 2016, 3)

3.4 Riski

Riskille ei ole olemassa yleisesti hyväksyttyä määritelmää (Terje, 2012, 4- 5; Wolke, 2017, 1). Kuitenkin ISO (International Organization for Standards) standardissa ISO/IEC 27000:2018 määrittelee riskin ”epävarmuudeksi jonkin tavoitteen saavuttamisesta”. Tietoturvakontekstissa tämä kuitenkin tarkoittaa riskin sisältävän mahdollisuuden siitä, että uhat hyödyntävät haavoittuvuuksia ja aiheuttavat näin vahinkoa organisaatiolle. Riskiin usein liittyy myös ajatus seuraamuksista tai tapahtumista. Tässä tutkimuksessa päämenetelmänä käytetyssä potentiaalisten ongelmien analyysissä pyrittiin arvioimaan riskiä ensin havainnoimalla jokin uhka ja haavoittuvuus minkä jälkeen pohdittiin mahdollisia seuraamuksia mikäli uhka pystyy hyödyntämään löydettyä haavoittuvuutta. Yhdessä edelläolevat muodostavat riskin. Samaa mieltä ovat Taylor ym. (2013) jotka toteavat että riski on yhdistelmä uhkia ja haavoittuvuuksia.

Opinnäytetyön tekijän esittämässä esimerkissä Mikko Malliton on jättänyt autonsa talvirenkaiden vaihdon viimepintaan ja äkilliset yöpakkaset ovat yllättäneet autoilijan. Tiet ovat jäätyneet, mutta Mikko päättää silti lähteä autollaan aamulla töihin. Tässä tapauksessa yöpakkasten jäädyttämä tie muodostaa uhan. Mikon auton huonosti jäällä pitävät kesärenkaat taas ovat haavoittuvuus. Näiden elementtien yhtäaikainen olemassaolo muodostaa riskin siitä, että Mikko aiheuttaa työmatkallaan liikennevahingon joutuessaan autollaan liirtoon. Riskitekijät (uhka, haavoittuvuus) voivat myös tietyissä olosuhteissa esimerkiksi toistuessaan muodostaa uuden, vakavuudeltaan suuremman riskin.

3.5 Korkeakoulun yleisiä tietoturvauhkia

Tässä kappaleessa esitellään yleisesti tunnistettuja riskejä jotka voivat esiintyä ammattikorkeakouluympäristössä. Tietoturvariskit ovat monipuolisia ja ne kohdistuvat organisaatioon erilaisten hyökkäysvektorien kautta. Inhimilliset, tahattomat riskit ovat usein sisäisien toimijoiden aiheuttamia, kun taas tuottamukselliset riskit voivat myös olla ulkoisten tekijöiden vaikutuksen tuotoksia. Tässä opinnäytetyössä tehdyssä POA-analyysissä yritettiin löytää ja arvioida tutkimuskohteena toimineen ammattikorkeakoulun tiettyyn prosessiin vaikuttavia riskejä, mutta tässä kappaleessa esitellään yleisesti tietoturvariskejä, jotka ovat potentiaalisia riskejä kaikille ammattikorkeakouluille.

Riskit voivat vaikuttaa eri organisaatioihin eri tavoin johtuen erityyppisistä tietojärjestelmäratkaisuista. Esimerkiksi palvelunestohyökkäys voi aiheuttaa erilaisia vaikutuksia organisaatioon, joka tuottaa palvelinratkaisunsa sisäisesti, kun taas palvelinratkaisunsa ulkoistaneella organisaatiolla päävastuu tietoliikenteen jatkuvuudesta kuuluu palveluntarjoajalle. Koska organisaatiot ovat kuitenkin riippuvaisia näistä palveluista, on tärkeää että riskienhallinnassa ja tietoturvasuunnittelussa tiedostetaan erilaiset riskit, jotka voivat vaikuttaa organisaatioon. Ammattikorkeakoulut ovat alttiita tietoturvariskeille, ja sen osoittaa IBM:n (2020) vuoden 2020 uhkaindeksi, joka asetti opetusalan seitsemänneksi hyökätyimmäksi alaksi vuonna 2019, kohoten vuodelta 2018 kahdella sijalla.

3.5.1 Sosiaalinen manipulaatio

Eräs IT-asiantuntija (Liite 4) näkee sosiaalisen manipulaation, ja eritoten käyttäjätietojen varastamisen sekä haittaohjelmien levityksen sähköpostin välityksellä yhdeksi suurimmista uhista kohdeorganisaatiolle. Sosiaalisella manipulaatiolla (eng. social engineering) tarkoitetaan ympäristöön ja olosuhteisiin vaikuttamista tavoitteena muuntaa sosiaalista käyttäytymistä siten että halutun sosiaalisen toiminnan todennäköisyys on suuri (Podgorecki ym. 1996, 6). Sen määritelmä on kuitenkin laaja ja nykyään yleisesti ajatellaan että käytännössä katsoen se kattaa kaiken tavoitteellisen sosiaalisen interaktion kuten valehtelun, markkinoinnin tai vaikka palkkaneuvottelun (Hadnagy, C. & Wilson, P. 2010, 1). Sosiaalista manipulaatiota on käytetty ihmiskunnan historian aikana eritoten totalitaaristen valtioiden

politiikassa, jossa valtionjohto kontrolloi ihmisten sosiaalista toimintaa haluttuun suuntaan propagandan ja jopa väkivallan avulla (Podgorecki ym. 1996, 7). Kuitenkin tietoturvan kannalta ajateltuna sosiaalinen manipulaatio voi tarkoittaa esimerkiksi salatun tai herkkäluontoisen tiedon hankintaa huijaamalla tai jopa kiristämällä.

Norvannon (2018, 192) mukaan sosiaalisen manipulaation voi jakaa kahteen ryhmään; ihmispohjaiseen ja teknologiapohjaiseen manipulaatioon. Ihmispohjainen manipulaatio nojaa henkilökohtaiseen vuorovaikutukseen, kun taas teknologinen sosiaalinen manipulaatio perustuu johonkin digitaaliseen rajapintaan, kuten ponnahdusikkunoihin tai haitalliseen sähköpostiliitteeseen. Norvanto (2018, 190) toteaa teknologian ja ajan kehittyessä ohjelmistojen haavoittuvuuksien vähenevän, mutta ihmisten olevan alttiimpia hyökkäyksille kuin ikinä. Siitä syystä tehokkaat hyökkäykset ovat usein sosiaalisia teknisien hyökkäyksien sijaan ja inhimillinen puoli jää usein kyberturvallisuudessa teknisempien osa-alueiden, kuten palomuuri tai IDS- järjestelmien varjoon. Norvanto (2018, 196 – 197) kuvaa yleisiä sosiaalisen manipulaation tekniikoita seuraavasti:

Phishing- hyökkäykset ovat yksi yleisimpiä sosiaalisen manipulaation taktiikoita joilla hyökkääjät yrittävät päästä käsiksi dataan tai järjestelmään. Tyypillisessä phishing-hyökkäyksessä lähetetään kohteelle huolellisesti luotu sähköposti, joka ei nopealla vilkaisulla herätä lukijassa hälytyskelloja. Sähköpostiin on kuitenkin lisätty linkki tai liite, jota lukijaa kehotetaan klikkaamaan. Kun lukija klikkaa linkkiätai avaa liitteen, lataa hän tietämättään haittaohjelman. Phishing- hyökkäyksissä satetaan myös ohjata kohde väärennetylle kirjautumissivulle, johon kirjautuessa hyökkääjä saa tunnustiedot.

Verukehyökkäyksissä (eng. pretexting) hyökkääjä luo kuvitteellisen tilanteen joka vaatii uhrilta reaktion, esimerkiksi yhteydenotto pankilta tai viranomaiselta. Verukehyökkäyksissä tarkoitus on luoda luottamussuhde kohteeseen, mikä mahdollistaa oikean reaktion, ja oikein tehtynä voi saada työntekijän unohtamaan tietoturvalliset käytännöt (Norvanto, E. 2018, 196).

Syötitys (eng. baiting) ja quid pro quo -hyökkäykset ovat hyökkäyksiä, joissa uhri houkutellaan lataamaan haitallinen ohjelma tai syöttämään tietojaan lupauksella palkinnosta tai hyödystä. Yleisiä syöttitekniikoita ovat tarjota uhrille ilmaisia tuotteita, kuten musiikkia ja elokuvia, tavoitteena saada uhri klikkaamaan linkkiä tai antamaan tietojaan, tai naamioida haitallinen ohjelma normaaliksi sovellukseksi tai sovelluspäivitykseksi.

Hieman haastavampi tekniikka hyödyntää ihmisten uteliaisuutta, on jättämällä haitallisen ohjelman sisältävä muistitikku tai muu vastaava laite vaikkapa parkkihalliin, josta uhri sen löytää. Mikäli uhrin uteliaisuus ottaa vallan, asettaa tämä muistitikun koneeseensa selvittääkseen sen sisällön, mutta asentaakin haittaohjelman tietokoneelleen. Quid pro quo -tekniikka eroaa syötittämisestä siten että siinä tarjotaan hyötyä tai palvelua vastineeksi

toteutetusta toimesta. Esimerkkinä tästä voi olla tilanne, jossa hyökkääjä ilmoittaa uhrille tarvitsevansa tämän käyttäjätunnuksen ja salasanan antaakseen ilmaisen lahjan.

Typosquatting tarkoittaa sitä, kun hyökkääjä luo kopion tunnetusta sivustosta, mutta asettaa domain-nimen hieman erilaiseksi. Tavoite on saada uhri kirjoittaessaan osoitteen virheellisesti, uskomaan että on päässyt oikealle sivustolle ja syöttämään esimerkiksi käyttäjätunnustietojaan, jotka välittyvät hyökkääjälle.

Jos tarkastelee yllä olevia esimerkkejä, voidaan luoda johtopäätös, että sosiaalinen manipulointi voi kohdistua mihin tahansa organisaatioon, jossa työskentelee ihmisiä, jotka käyttävät työssään viestintävälineitä. Sosiaaliselta manipulaatiolta voi olla vaikea suojautua, mutta ensimmäinen askel on tietämys erilaisista hyökkäystekniikoista ja tekemällä turvallisuustiedottamisesta henkilökohtaisempaa jolloin työntekijät ovat motivoituneempia olemaan valppaita. (Hadnagy, C. & Wilson, P. 2010, 340-344).

3.5.2 Yleisimmät uhat verkkosovelluksille (OWASP 2017)

Tässä kappaleessa käydään lyhyesti läpi OWASP- säätiön laatimaa listaa yleisimmista web applikaatioriskeistä tällä hetkellä. OWASP (The Open Web Application Security Project) on vuonna 2001 perustettu voittoa tavoittelematon säätiö, jonka tavoitteena on mahdollistaa organisaatioille luotettavien sovellusten tuottaminen ja hankkiminen kaikkialla maailmassa. Voittoa tavoittelemattomana säätiönä se tarjoaa palveluitaan maksuttamana. OWASP tuottaa kansainvälisen yhteisön ohjelmiston avoimen lähteen projekteja sekä tarjoaa koulutusta ja konferensseja. Vuodesta 2004 se on ollut virallisesti voittoa tavoittelemattomana hyväntekeväisyysjärjestönä Yhdysvalloissa (OWASP 2020).

Säätiö julkaisee päivittyvää listaa kymmenestä yleisimmästä tietoturvauhkasta verkossa. OWASP:in lista antaa yleiskuvan organisaatioille, jotka omistavat tai ovat tekemisissä web-applikaatioiden kanssa siitä minkälaisia hyökkäysvektoreita potentiaaliset hyökkääjät voivat käyttää.

Tutkimuksen kohteena olleessa ammattikorkeakoulussa on käytössä useita web-applikaatioita kuten verkkosivuja, chat-palveluita, selainpohjaisia tiketöintijärjestelmiä sekä muita verkkosovelluksia. Vaikka näitä palveluja on kohdeorganisaatiossa pitkälti ulkoistettu, on silti hyvä olla tietoinen niihin kohdistuvista uhkista. OWASP (2017) on koonnut listaansa kriittisimmät uhat seuraavasti:

Injektioilla (eng. Injections) tarkoitetaan hyökkäystä, jossa käyttäjä syöttää haitallisia komentoja tai esimerkiksi SQL-kyselyjä sovellukseen, jotka isäntäpalvelin suorittaa. Tämä voi tapahtua missä tahansa missä käyttäjän syöttämää dataa prosessoidaan. Applikaatio on haavoittuvainen injektiohyökkäyksille, jos käyttäjän syöttämälle datalle ei suoriteta

applikaatiossa tarkistuksia eikä sille ole asetettu tarpeeksi kattavia sääntöjä, kuten esimerkiksi erikoismerkkien kieltämistä. Yleisimpiä injektiohyökkäyksiä ovat SQL-injektiot.

Rikkonainen autentikaatio (eng. Broken Authentication). Mikäli applikaatio ei toteuta riittävää sessionhallintaa tai käyttäjänhallintaa, voi käyttäjien identiteetti tulla väliaikaisesti varastetuksi. Yleisiä hyökkäysvektoreita ovat hyökkäykset, joissa käytetään hyväksi salasanalistoja tai vuodettuja käyttäjätietoja, joita on saatavilla internetistä. Tällaisia riskejä vastaan pystyy suojautumaan huolehtimalla, että organisaation salasanakäytännöt ovat riittävät sekä parantamalla autentikaation turvallisuutta esimerkiksi ottamalla käyttöön kaksivaiheisen autentikaation.

Arkaluontoisen datan altistuminen (eng. Sensitive data exposure) tapahtuu, Jos applikaatio ei tarjoa riittäviä keinoja turvaamaan arkaluontoista dataa. Puutteellisen salauksen myötä hyökkääjä voi saada käsiinsä esimerkiksi luottokortti- tai terveystietoja. Yleisimmin tämän riskin hyökkäysvektorina toimii salausavainten nappaaminen tai man in the middle -hyökkäykset jossa asiakkaan ja isännän välinen yhteys ohjataan hyökkääjän läpi jolloin tämä pääsee käsiksi kulkevaan dataan. Tältä riskiltä voidaan suojautua varmistamalla, että arkaluontoinen data on luokiteltu oikein ja se käsitellään asianmukaisella tavalla. On myös tärkeää huolehtia, että datan salaus on ajan tasalla ja käytetyt protokollat ovat luotettuja ja turvallisia.

Ulkoiset XML-entiteetit (eng. XML external entities). Vanhat tai huonosti konfiguroidut XML prosessorit voivat käsitellä viittauksia ulkoisiin entiteetteihin XML-dokumenttien sisällä. Ulkoisilla entiteeteillä voidaan päästä käsiksi sisäisiin applikaation tiedostoihin.

Rikkonainen pääsykontrolli (eng. Broken access control). OWASP:in mukaan on yleistä, että web-sovelluksiin ei usein säädetä riittäviä kontrolleja sille mitä käyttäjilä on oikeus tehdä, mikä voi johtaa siihen, että hyökkääjät hyödyntävät näitä puutteita ja pääsevät käsiksi dataan, joka ei ole heille tarkoitettu. Hyökkääjät voivat käyttää esimerkiksi URL-kenttää ohittamaan pääsykontrollin. Estämään näitä iskuja yksi suositeltu menetelmä on asettaa kaikki oikeudet evätyksi vakiona, ja sallia oikeuksia käyttäjille tapauskohtaisesti.

Virheellinen turvallisuuskonfiguraatio (eng. Security misconfiguration). Virheelliset turvallisuuskonfiguraatiot ovat yksi yleisimmistä ongelmista web-sovelluksissa. Esimerkiksi liian runsassanaiset virheilmoitukset paljastavat hyökkääjälle potentiaalisesti hyödyllistä informaatiota. Myös sovelluksen komponenttien päivitysten laiminlyöminen suurentaa tietoturvariskiä.

Cross-site scripting (XXS). XXS-hyökkäykset ovat OWASP:in mukaan toiseksi yleisin riski tällä hetkellä, ja niitä pystytään suorittamaan tätä nykyä myös automatisoiduilla työkaluilla. Yleensä ne kohdistuvat uhrin selaimeen, ja niitä on kolmea erilaista. Heijastavissa XSS hyökkäyksissä (eng. Reflected XSS) web-sovellus tuottaa HTML-tulosteen, jossa on osittain käyttäjän syöttämää dataa, ja näin hyökkääjä pystyy suorittamaan HTML- tai javascript-syötteitä uhrin selaimessa. Yleensä tämän mahdollistaa haitallinen linkki jota uhri klikkaa. Säilytetyssä XSS hyökkäyksessä (eng. Stored XSS) web-sovellus voi tallentaa haitallista käyttäjän syöttämää dataa, joka aktivoituu, kun sitä myöhemmin tarkastellaan toisen käyttäjän tai ylläpitäjän toimesta. Dokumenttioliomallia hyödyntävissä eli DOM-XSS hyökkäyksissä sovellukset sisällyttävät dynaamisesti hyökkääjän kontrolloimaa dataa sivustolle, joka mahdollistaa hyökkääjälle pääsyn kontrolloimaan sovellusta.

Epäturvallinen sarjoituksen poisto (eng. Insecure deserialization). Kun sovellus säilöö ja sisällyttää dataa myöhempää käyttöä varten ja säilöttävälle datalle ei ole määritelty tarvittavia kontrolleja, on hyökkääjällä potentiaalisesti mahdollisuus kyseistä dataa muokkaamalla esimerkiksi antaa itselleen järjestelmänvalvoja oikeudet tai suorittaa haitallista koodia. Tähän riskiin pystyy varautumaan asettamalla tiukat rajoitteet sarjoitettavalle datalle.

Komponenttien käyttäminen, jossa on tunnettuja haavoittuvuuksia. Monet web-sovelluksissa käytettävät komponentit tarvitsevat toimiakseen samat oikeudet kuin itse sovellus. Näin ollen epäturvalliset komponentit voivat tarjota hyökkääjille mahdollisuuksia aiheuttaa vahinkoa sovelluksella. Mikäli web-sovellus käyttää paljon eri komponentteja voi niiden turvallisuuden seuraaminen olla vaikeaa. Mikäli komponentissa on tunnettuja haavoittuvuuksia voi sille löytyä jopa valmiita hyökkäysmalleja hyökkääjien käytettäväksi. Hyvä päivitystenhallinta ja versionhallinta ovat hyviä puolustuskeinoja vähentämään riskiä että sovellus käyttää epäturvallisia komponentteja.

Riittämätön lokinpito ja monitorointi ovat usean toteutuneen riskin takana. Hyökkääjät hyödyntävät riittämättömästä monitoroinnista ja lokinpidosta seuraavaa hidasta reagointinopeutta toteuttaakseen hyökkäyksiään onnistuneesti. Monitorointia voi parantaa varmistamalla, että tärkeät tapahtumat kuten kirjautumiset, palvelintapahtumat ja epäilyttävät tapahtumat tallennetaan lokiin ja niitä pystyy seuraamaan. Myös toiminnan palautussuunnitelma ja muut varotoimenpiteet vähentävät riittämättömän monitoroinnin ja lokinpidon aiheuttamaa riskiä.

4 Menetelmät

Tässä kappaleessa kuvataan menetelmiä, joita käytettiin tämän tutkimuksen aineiston keräämiseen ja sen analysointiin. Menetelmien valintaan vaikutti rajattu aihealue sekä määrällisen aineiston saatavuuden puute, tästä syystä tutkimuksessa käytettiinkin pitkälti laadullisen tutkimuksen menetelmiä. Tutkimus sai alkunsa opinnäytetyön tekijän osallistumisesta potentiaalisten ongelmien analyysiriiheen, ja siksi se on myös opinnäytetyössä tehdyn tutkimuksen päämenetelmä. Potentiaalisten ongelmien analyysiä tukemaan on valittu menetelmiä, jotka täydensivät siitä saatua aineistoa, tarjosivat tukevia näkökantoja sekä vastasivat omalta osaltaan määriteltyihin tutkimuskysymyksiin.

Relibiliateettia opinnäytetyöhön tuo omalta osaltaan sen nojaaminen asiantuntijoiden lausuntoihin niin POA-prosessin aikana kuten haastatteluissa. Asiantuntijoilla on vuosien kokemus tutkittavasta ympäristöstä ja ammattitaitonsa ja työtehtäviensä vuoksi pystyvät arvioida organisaation sisäisiä trendejä. POA sitoi tutkimuksen oikeaan osa-alueeseen ja kohteeseen organisaatiossa, mutta samaan aikaan se käsitteli tietoturvan ulkopuolella olevia, yleisesti turvallisuuteen liittyviä asioita kuten työtapaturmat tai työterveys. Vaikka yhteys tietoturvaan on mahdollista tehdä, validiteetin varmistamiseksi POA-prosessista on opinnäytetyöhön valikoitu ne osa-alueet, jotka koskevat IT-harjoitteluprosessin tietoturvallisuutta. Valikoidut osa-alueet esitettiin tietohallinnon asiantuntijoille ja todettiin olevan relevantteja tietoturva-aiheeseen.

4.1 Laadullinen riskianalyysi

Laadullinen riskianalyysi pyrkii priorisoimaan riskejä tarkastellen todennäköisyyksiä sekä toteutuvien riskien vaikutuksia organisaatioon tai kohteeseen myöhempää analyysiä tai toimenpiteitä varten (ISO 2017). Toisin kuin kvantitatiivisessa riskianalyysissä jossa tarkastellaan lukuja ja tehdään päätelmiä sekä laskelmia riskien vaikutuksista tilastotietojen avulla, kvalitatiivinen riskianalyysi pyrkii tarjoamaan tietoperustan tuleville riskinhallinnan prosesseille havaitsemalla ja määrittelemällä riskejä (ISO 2017). Tässä tutkimuksessa käytetyt menetelmät kuten haastattelut, kyselyt sekä Potentiaalisten Ongelmien Analyysi ovat luonteeltaan pääpiirteittäin laadullisia menetelmiä. Laadullisen ja kvantitatiivisten menettelyjen välillä on käyty kiivasta väittelyä jo 70-luvulta asti, ja se jatkuu yhä (Norman,

T. 2009, 53). Hänen mukaansa paras tapa toteuttaa riskianalyysi on käyttää molempia menettelyjä täydentämään toisiaan. Norman (2009, 54) perustelee sitä sillä, että kvantitatiivisilla menettelyillä pystytään käsittelemään laajaa aluetta, kun taas laadullinen analyysi keskittyy yleensä pienempään alueeseen. Koska tämän opinnäytetyön aihealue käsittää kohdeorganisaatiossa vain yhden prosessin, tekijä uskoo laadullisten menettelyjen olevan riittäviä.

4.2 Potentiaalisten ongelmien analyysi

Potentiaalisten Ongelmien Analyysi on alunperin kehitetty suurteollisuutta varten minkä vuoksi sen kyky tunnistaa riskejä on hyvä, (PK-RH 2012) ja sitä käytetään osana riskienhallintaa. POA-analyysin avulla voidaan tunnistaa sekä arvioida riskien vakavuutta tai laajuutta pohtien riskikohtaisesti kuinka usein se toteutuu sekä kuinka todennäköinen se on. Sen lisäksi arvioinnissa huomioidaan myös kuinka suuria vahinkoja riskit potentiaalisesti voivat aiheuttaa (PK-RH 2012). POA-analyysimenetelmä toteutetaan pienryhmässä lukumäärältään noin kolmesta neljään osallistujaa, joka koostuu henkilöistä, joilla on tietämystä analysoitavasta aiheesta. Tähän voi lukeutua työntekijöitä, johtajia, sunnittelijoita sekä asiantuntijoita, joilla on asianmukaista tietoa esimerkiksi riskienhallinnasta. Ryhmään tulisi kuitenkin kuulua organisaation jäseniä, jotka edustavat erilaisia työtehtäviä sekä henkilö, joka valitaan ryhmän vetäjäksi. Vetäjän tulisi tuntea POA- analyysin periaatteet, ja menetelmä sekä pystyä ohjaamaan POA- aivoriihiä. Vetäjän tulisi myös olla ”sopivan ulkopuolinen” (PK-RH 2012).

Potentiaalisten ongelmien analyysi voidaan toteuttaa tarvittaessa useana palaverikertana, jolloin ryhmä kokoontuu yhteen käsittelemään analyysiä. POA:n kohteet tulisi kuitenkin rajata kattamaan haluttu organisaation alue, jotta analyysin tulokset olisivat tarkkoja sekä relevantteja. POA- palaveri koostuu vaiheista jonka aikana ryhmän jäsenet pohtivat sovitun rajauksen mukaisesti asiaankuuluvia riskejä, jotka taltioidaan, arvioidaan ja sovitaan mahdollisista toimenpiteistä. Tämä toteutetaan siten, että vetäjä antaa ryhmälle joukon avainsanoja, jotka liittyvät rajattuun aiheeseen. Tällainen voisi olla esimerkiksi ”henkilöstö”. Tämän lisäksi annetaan joukko toisia avainsanoja, jotka toimivat vihjeinä mahdollisille riskeille. Tämä voidaan toteuttaa taulukon muodossa selkeyden vuoksi. Kun avainsanat on laadittu, ryhmä ideoi riskejä hiljaisen aivoriihen tapaan kirjoittamalla paperille riskejä liittyen avainsanoihin ja jakamalla niitä eteenpäin. Näin saadaan kokoelma koottuja riskejä joita analysoidaan syvemmin seuraavissa vaiheissa.

Liitteessä 3 on Suomen riskienhallintayhdistyksen esimerkkejä avainsanoista, joita potentiaalisten ongelmien analyysin vetäjä voi käyttää aktivoimaan hiljaisen aivoriihen edistymistä ehdottamalla avainsanoja ja näin ruokkia keskustelua. Kun ryhmä on koonnut ja taltioinut aivoriihen tulokset kirjaamalla riskit ylös, nämä tulisi arvioida antamalla niille esimerkiksi numeerinen luku vastaamaan niiden riskitasoa.

Tämän tutkimuksen päämenetelmänä käytetyssä POA-analyysissä riskien taso arvioitiin asettamalla kaksi lukua asteikolla yhdestä kolmeen joista ensimmäinen edusti riskin toteutumisen todennäköisyyttä, ja toinen sen toteutumisen myötä aiheutuvaa vahinkoa organisaatiolle eli vakavuutta. Todennäköisyydelle annetussa arvossa numero yksi tarkoitti että riski on hyvin epätodennäköinen ja numero kolme että riski on todennäköinen. Seurauksen vakavuudelle annettu numero yksi tarkoitti lievästi haitallisia vaikutuksia, kun taas numero kolme merkitsi erittäin haitallista vaikutusta. Tämän jälkeen todennäköisyys kerrottiin vakavuudella, ja sen tulos kerrottiin kolmella muodostaen seuraavanlaisen yhtälön: Todennäköisyys x Vakavuus x 3 = Riskitaso. Taulukon 1 esimerkissä POA- tiimi on tullut siihen johtopäätökseen, että kyseinen riski on epätodennäköinen, mutta jos se toteutuu voi organisaatiolle aiheutua siitä suurta vahinkoa. Luku kahdeksantoista edustaa siis tämän riskin vakavuutta. Tämän jälkeen ryhmä sopii varotoimenpiteistä sekä mahdollisista muista toimenpiteistä riskiin liittyen.

Esimerkki:

Kohde	Ongelma (riski)	Riskitaso
Tietosuoja	Työntekijä lähettää salassapidettävää materiaalia suojaamattoman yhteyden kautta.	2 x 3 = 18

Taulukko 1: Riskien arviointimalli

4.3 Kysely- sekä haastattelututkimus

Tutkimuksen tavoitteisiin kuului tutkia kohdeorganisaation IT-harjoitteluprosessin parhaiden tietoturvallisten käytänteiden toteutumista, jotta pystytään arvioimaan sen nykytilannetta paremmin. IT-harjoitteluprosessiin liittyy useita tekijöitä ja sidosryhmiä, joiden merkitys prosessissa on erilainen. Tässä tutkimuksessa on käytetty haastatteluja sekä kyselyä tutkimaan näiden sidosryhmien näkemyksiä tietoturvan tilanteesta kohdeorganisaatiossa. Tämä korostuu eritoten siksi koska määrällistä aineistoa oli opinnäytetyön tekijälle saatavilla vähän.

Kysely ja haastattelu ovat menetelmiä, jotka nojautuvat samankaltaiseen rakenteeseen, esitettyihin kysymyksiin ja vastauksiin. Kirjassaan Tuomi (2018) erottelee nämä kaksi menetelmää tarkastelemalla tiedonantajan toimintaa; kyselyssä tiedonantajat vastaavat kysymyksiin täyttämällä omatoimisesti kyselylomakkeen joko valvotussa tilaisuudessa tai kotonaan, kun taas haastattelussa kysymykset esitetään suullisina ja vastaukset taltioidaan tiedonkerääjän eli haastattelijan toimesta. Brinkmannin (2013, 46) mukaan haastattelun erottaa normaalista keskustelusta siitä että haastattelu on etukäteen suunniteltu ja sen tuloksia analysoidaan tarkemmin jonkin ennaltamääritellyn suunnitelman mukaan. Erilaisia tapoja toteuttaa kysely tai haastattelu on useita, ja toteutustavan valintaan vaikuttaa esimerkiksi tutkittava aihe. Tässä tutkimuksessa on käytetty haastatteluja, kuten myös kyselyä. Tarkemmin lomakekyselyä sekä teemahaastattelua.

Lomakekysely on Tuomen (2018) mukaan hyvä keino testata hypoteeseja sekä kvantifioida aineistoa. Kuitenkin hän myös toteaa että lomakekysely on usein määrällisen, ei laadullisen tutkimuksen menetelmä, mutta sitä pystytään soveltamaan laadullisessa tutkimuksessa. Esimerkiksi tässä tutkimuksessa lomake kysely toteutetaan pienelle ihmisryhmälle joka on helposti jaotettavissa laadullisiin luokkiin; nykyisiin ja entisiin harjoittelijoihin. Tämä tekee lomakekyselystä tämän tutkimuksen kontekstissa laadullisen menetelmän.

Opinnäytetyön tekijä luonnehtisi teemahaastattelua puoliavoimeksi haastattelumuodoksi, sillä Tuomen (2018) mukaan teemahaastattelussa käytetään ennaltamääritettyä haastatelurakennetta kuitenkin mukautuen haastateltavan vastauksien perusteella. Kysymyksiä voidaan siis tarkentaa tai uudelleensuunnata haastattelun edetessä, jotta saadaan mahdollisimman paljon tietoa halutusta aiheesta, eli teemasta.

5 Tutkimuksen toteutus

Päämenetelmänä tutkimuksessa käytettiin POA-analyysiä. Aloite prosessiin tuli ammattikorkeakoulun taholta, ja opinnäytetyön tekijä kutsuttiin osaksi POA-analyysiryhmää. Tutkimuksen ensimmäinen vaihe oli POA:n toteutus. POA toteutettiin useassa eri vaiheessa, jossa ryhmä kokoontui analysoimaan havaintojaan sekä kirjaamaan ne POA-taulukkoon (liite 1). Ryhmään kuului opinnäytetyön tekijän lisäksi IT- sekä turvallisuusasiantuntijoita ammattikorkeakoulun sisältä, joilla työtehtäviensä osalta oli tietämystä analyysissä käsiteltävästä aihealueesta eli IT-harjoittelijoista sekä organisaation turvallisuustavoitteista. Ryhmän tapaamisia oli yhteensä neljä, ja ne ajoittuivat kesälle 2019 kuukausille kesä-elokuu.

5.1 POA

Ensimmäisellä tapaamiskerralla vetäjän johdolla käytiin läpi POA-analyysin periaatteet, prosessin tavoitteet sekä menetelmät. Ensimmäisen tapaamisen aikana myös aloitettiin POA-analyysin ensimmäinen vaihe, jossa ryhmän jäsenet kirjoittivat paperilapuille ylös noin kolme uhkaa tai heikkoavaisuutta liittyen IT-harjoittelijoihin, minkä jälkeen laput kierrätettiin ympäri pöytää antaen jokaiselle mahdollisuuden lisätä havaintojaan/mietteitään. Tämä toistettiin kunnes saatiin kasaan mahdollisimman laaja kirjo erilaisia uhkia. Kun ryhmä oli koonnut kaikki aivoriihen tulokset, luotiin niille Taulukon 5 osoittamalla tavalla kohteet/kategoriat tyypeittäin. POA-ryhmä määritti havaitut riskit seuraaviin kategorioihin:

Pääsyoikeudet.	Tässä kategoriassa olevat riskit liittyivät harjoittelijoiden tunnusten kohotettuun pääsyoikeuksiin ja komplikaatioihin joita tämä voi aiheuttaa. Tähän kategoriaan sisältyy tuottamuksellisia sekä tahallisia toimia.
Perehdytys.	Tähän kategoriaan liittyy riskejä, jotka voivat ilmaantua uusien harjoittelijoiden perehdytykseen liittyen.
Terveys.	Tässä kategoriassa on riskejä liittyen työhyvinvointiin sekä harjoittelijoiden yleiseen terveyteen. Tämä kategoria on kuitenkin rajattu ulos tämän tutkimuksen aiheesta.
Tahalliset.	Tässä kategoriassa tarkastellaan niitä riskejä, joiden toteutuminen johtuu inhimillisestä aikomuksellisesta ja/tai suunnitellusta teosta.
Tuottamukselliset.	Tämän kategorian riskit johtuvat teoista ja toimista, joiden taustalla ei ole aikomuksellisuutta tai suunnitteellisuutta mutta ovat kuitenkin inhimillisesti toteutettuja.
Rekry	Rekrytointiprosessiin liittyviä riskejä.

Taulukko 2: Riskien kategoriat

Ryhmä kokosi löydetyt riskit edellä mainitun (taulukko 2) mukaisesti kategorioihin, jonka jälkeen osoitettiin kirjuri, joka siirsi muodostetun taulukon sähköiseen muotoon.

Ryhmä kokoontui tämän jälkeen vielä kolme kertaa, käyttäen kokousvälineenä kokoushuoneita sekä etäyhteyttä pikaviestintäohjelmien avustuksella. Seuraavien kokousten aikana tavoitteena oli käydä läpi jokainen riski ja ensin pohtia vakavimpia mahdollisia seurauksia sekä sitä kuinka todennäköinen kyseisen riskin toteutuminen on käyttäen laskutoimitusta (kts. Taulukko 2) kuvaamaan riskin vakavuutta. Tässä vaiheessa myös pohdittiin mahdollisia alustavia toimenpiteitä riskinhallinnalle mikäli sellaisia oli tiedossa. POA-prosessin loppuvaiheessa ennen viimeistä tapaamiskertaa opinnäytetyön tekijän tehtävä oli määritellä sekä rajata tässä tutkimuksessa käsiteltävät riskit aihealueen puitteissa, jonka jälkeen ryhmä kokoontui käsittelemään sekä hyväksymään opinnäytetyön tekijän havainnot. Tähän tutkimukseen valikoitui sellaisia riskejä, joiden seuraamukset vaikuttavat tunnuksiin tai niiden käyttöön sekä riskit jotka ovat suoraan yhteydessä tunnuksiin joko hallinnollisella, inhimillisellä tai teknisellä tasolla.

5.2 Haastattelut ja kysely

Tutkimuksen seuraavan vaiheen aikana opinnäytetyön tekijä keräsi aineistoa teemahaastattelujen muodossa. Haastateltaviksi valikoitui POA-ryhmän jaseniä, jotka työnkuvansa sekä tehtävänsä vuoksi pystyvät tarjoamaan tutkimuksen kannalta oleellista tietoa omien työnkuviensa puitteissa. Yhteydenpitoa joidenkin asiantuntijoiden kanssa on pidetty yllä koko tukimuksen toteutuksen ajan, ja lisätietoja on saatu esimerkiksi pikäviestintäpalveluiden ja sähköpostin välityksellä.

IT-asiantuntijoiden haastatteluissa sovellettiin teemahaastattelumenetelmää, ja haastattelujen tarkoituksena oli kerätä aineistoa liittyen asiantuntijoiden harjoitteluprosessin kannalta avainasemassa oleviin työtehtäviin. Haastatteluja toteutettiin kolme kappaletta, ja haastatellut asiantuntijat olivat kaikki osa POA-tiimiä. Näin saatiin aineistossa esille myös asiantuntijoiden yksilöllisiä näkemyksiä. Asiantuntijoiden työtehtävät koostuivat tietoturvasta, käyttäjänhallinnasta sekä servicedesk-palvelun koordinoinnista ja johtamisesta.

Kysely toteutettiin Googlen Google Forms -kyselyalustapalvelun avulla nimettömänä. Lomakekyselyä varten haettiin kohdeorganisaatiosta tutkimuslupa. Kun tutkimuslupa oli myönnetty, lähetettiin kyselylomake Discord-pikaviestinsovelluksen välityksellä yhteensä 25:lle entiselle ja nykyiselle harjoittelijalle. Kysely lähetettiin myös sähköpostilla IT-harjoittelijoiden esimiehelle kohdeorganisaatiossa, joka välitti sen opinnäytetyön tekijän pyynnöstä nykyisille IT-harjoittelijoille, jotka eivät olleet pikaviestintäpalvelussa.

Kysely koostui kahdeksasta kysymyksestä, joista kolme ensimmäistä olivat taustakysymyksiä selvittämään olivatko harjoittelijat tällä hetkellä suorittamassa harjoitteluaan ja jos olivat, niin minä vuonna harjoittelu suoritettiin. Tämän jälkeen harjoittelijoilta kysyttiin tietoturva-alan opintotaustoista sekä harjoittelijoita pyydettiin arvioimaan osaamistaan ennen harjoittelua. Sen jälkeen kysyttiin harjoittelijoiden mielipidettä siitä olivatko he saaneet tarpeeksi kattavaa perehdytystä tietoturva aiheista sekä servicedeskin ja sen asiakkaiden eli organisaation opiskelijoiden ja henkilöstön tietoturva-käytänteiden tuntemusta. Lopuksi harjoittelijoille annettiin mahdollisuus antaa avointa palautetta/tietoa.

6 Tutkimuksen tulokset

Tutkimuksen aineiston perusteella on pystytty paikantamaan puutekohtia kohdeorganisaation IT-harjoittelun tietoturvallisuuden, sekä organisaation yleisen tietoturvan osalta sekä todettu osa-alueita joissa tietoturva on jo toteutettu hyväksi todettuja tietoturvallisuuskäytäntöjä käyttäen. Näin on pystytty tunnistamaan alueet joissa kehitystarve on suurin.

6.1 POA:n havaintoja

Potentiaalisten ongelmien analyysissä pyrittiin löytämään riskejä kappaleessa 4.2 kuvatulla tavalla asettaen ne kategorioihin ”pääsyoikeudet”, ”perehdytys”, ”tahalliset”, ”tuottamukselliset” ja ”rekry”. Tässä kappaleessa tarkastellaan, miten riskitasot jakaantuivat arvioitujen riskien osalta eri kategorioiden kesken, mutta kohdeorganisaation pyynnöstä ja tietosuojakäytäntöjä noudattaen tarkemmat tiedot löydetyistä riskeistä ovat tarkasteltavissa erillisessä salatussa liitteessä.

Riskien mittaaminen on oleellinen osa riskianalyysiä, joka mahdollistaa riskien arvioimisen ja toimivan riskinhallinnan (Wolke 2017, 9) sekä antaa tärkeää tietoa riskien priorisointiin. POA-ryhmä käytti sivuilla 23 kuvattua metodia mittaamaan riskien vakavuutta, jossa riskeille määritettiin numeerinen arvo. Kvalitatiivisen riskianalyysin tarkkuudelle on oleellista, että riskien vakavuuden asteet ovat helposti ymmärrettävissä ja yhtenäiset (Taylor ym. 2013, 28). Siksi aineiston keräämisvaiheen jälkeen POA-analyysin tulokset muutettiin paremmin ymmärrettävään muotoon. Se toteutettiin muodostamalla asteikko analyysissä asetetuista arvoista ja kuvaamalla ne termein Taulukon 3 mukaisella tavalla.

Vakavavuusarvo (taulukko 1:n mukaan)	
27	Äärimmäisen vakava
18	Erittäin vakava
12	Vakava
9	Melko vakava
8	Uhkaava
6	Lievä
4	Alhainen

Taulukko 3: Vakavuusarvot

Oheiseen asteikkoon (taulukko 3) on otettu vaikutteita Yhdistyneen kuningaskunnan kabinetin kanslian (National Risk Register of Civil Emergencies 2017 edition 2017) riskien määrittelyasteikosta, jonka myös Taylor ym. (2013, 29) esittävät. Seuraavissa luvuissa esitetyissä kehitysehdotuksissa on käytetty tukevana työkaluna yllä olevaa asteikkoa arvioimaan kehityskohteen tarvetta sekä priorisointia.

Kerätyn aineiston perusteella, alan aineistoon nojaten, tutkimuksen tuloksena syntyi kehitysehdotuksia tutkimuksen kohteena olevan organisaation IT-harjoitteluprosessin tietoturvallisen toiminnan parantamiseksi.

6.1.1 Pääsyoikeudet

Tässä kategoriassa analysoitiin riskejä, jotka liittyvät harjoittelijoiden pääsyoikeuteen organisaation, sen sidosryhmien tai henkilökunnan dataan sekä järjestelmiin. Koska harjoittelijoilla on korotettu pääsy valtaosaan kohdeorganisaation laitteista ja järjestelmistä, tuottaa se riskin siitä että pääsyoikeuksia käytetään väärin. Yhteensä pääsyoikeuksiin liittyen löydettiin kahdeksan riskiä (Liite 1). Niistä POA määritti äärimmäisen vakavia (27) riskejä yhteensä kolme kappaletta sekä erittäin vakavia (18) riskejä löydettiin myös yhteensä kolme kappaletta. Loput kaksi löydettyä riskiä saivat arvokseen vakava (12) sekä melko vakava (9).

6.1.2 Perehdytys

Kun uusi työntekijä saapuu organisaatioon on tärkeää, että perehdytettäville annettava tieto on ajantasaista sekä vastaa perehdytettävän työtehtäviä. Myös perehdyttäjän tulee tuntea työtehtävä, johon hän uutta työntekijää perehdyttää. Erään IT-asiantuntijan (Liite 4) mukaan kohdeorganisaatiossa suorittaa harjoittelujaksoaan vuosittain noin kymmenestä kahteentoista tietojenkäsittelyn alemman AMK:n opiskelijaa. Harjoittelujaksot ovat kuuden kuukauden mittaisia ja porrastettuja siten että pidemmän aikaa työskennelleet IT-harjoittelijat pystyvät perehdyttämään aloittavia harjoittelijoita. Opinnäytetyön tekijän mielestä IT-harjoittelun kannalta perehdytyksen merkitys korostuu, sillä koska harjoittelija on organisaatiossa vain vähän aikaa, laajaa työkokemusta työtehtävistä ei ehdi kertyä. Harjoittelijoiden työnkuvan ja työkalujen vuoksi on myös tärkeää, että työkaluja osataan käyttää asianmukaisesti, jotta minimoidaan riskien toteutuminen.

POA-tiimi pohti perehdytykseen liittyviä riskejä ja tunnisti yhteensä 11 eri riskiä. Niistä äärimmäisen vakavia (27) oli vain kaksi, kun taas eniten riskejä oli arvioitu perehdytys kategoriassa uhkaavaksi (8) yhteensä neljä kappaletta (liite 1). Vakavia (12) riskejä löydettiin kaksi, erittäin vakavia (18) yksi ja alhaisia (4) sekä lieviä (6) myös yksi.

6.1.3 Tahalliset

Tahallisten riskien olennainen tunnuspiirre on tietoinen toiminta tai harkittu teko. Tässä kategoriassa luetellut riskit siis sisältävät edellä mainitut ominaisuudet, minkä vuoksi tässä kategoriassa on päällekkäisyyksiä sekä yhteneväisyyksiä riskeihin muissa kategorioissa. Tahallisia riskejä tunnistettiin yhteensä viisi (liite 1). kaksi näistä oli äärimmäisen vakavia (27), kaksi uhkaavia (8), sekä yksi erittäin vakava (18) riski.

6.1.4 Tuottamukselliset

Ero tuottamuksellisissa riskeissä tahattomiin riskeihin on se, että vaikka ne toteutuvat ihmisten toimesta, ei niihin liity harkinta tai tietoinen toiminta. Kuitenkin huolimattomuus tai välinpitämättömyys voi johtaa tuottamuksellisiin riskeihin, vaikka edellä mainittuja ominaisuuksia ei ole pakko esiintyä vaan riskit voivat johtua inhimillisistä virheistä.

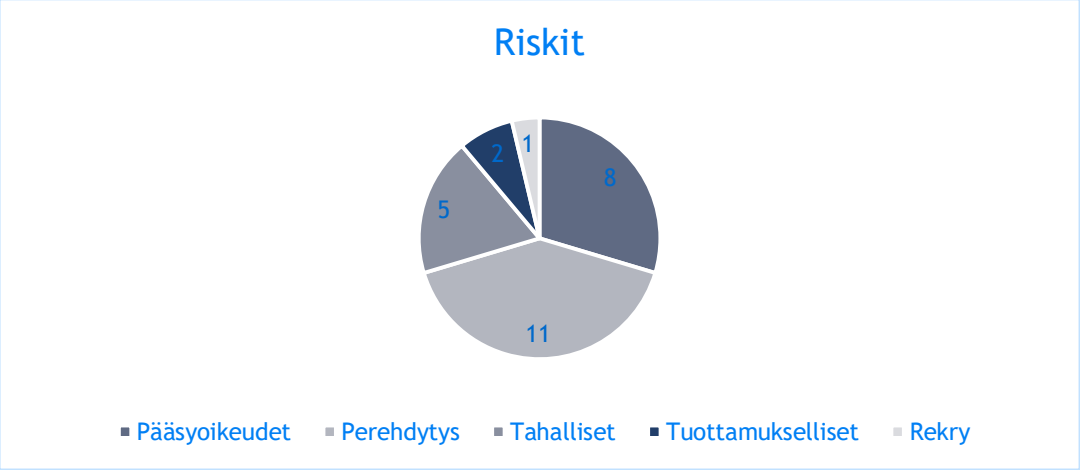
Tuottamuksellisia riskejä POA-tiimi löysi kaksi kappaletta, jotka kummatkin arvioitiin vakaviksi (12) riskeiksi (liite 1). Toinen riskeistä edusti huolimattomuuden tai välinpitämättömyyden aiheuttamia riskejä, kun taas toinen voitaisiin tulkita inhimilliseksi virheeksi.

6.1.5 Rekry

Rekrytointiin voi liittyä tietoturvariskejä, tässä tapauksessa POA-tiimi tunnisti yhden riskin liittyen rekrytointiin ja se arvioitiin äärimmäisen vakavaksi riskiksi (27).

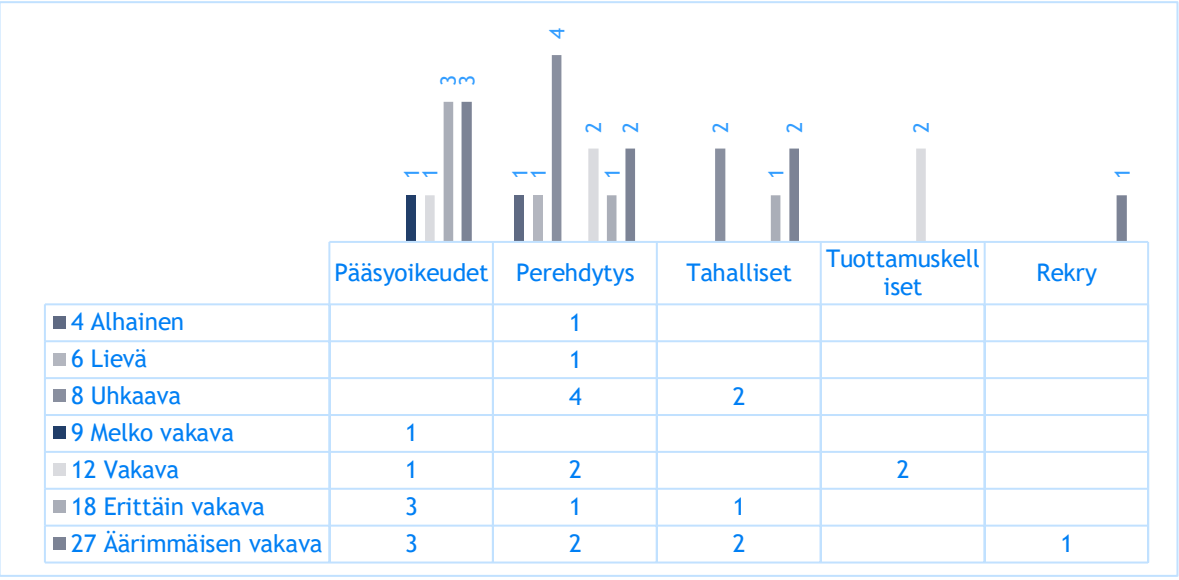
6.1.6 POA yhteenveto

Kuten kuvio 4 osoittaa, selvästi eniten riskejä, 41% kaikista löydetyistä riskeistä liittyi perehdytykseen. Pääsyoikeudet olivat toiseksi suurin kategoria 31% osuudella. Myös tahalliset riskit ovat isossa osassa 19% osuudella. Tuottamuksellisten riskien osuus on 7% ja rekrytointiin liittyvät riskit 4%.



Kuvio 4: Riskien jakauma

On kuitenkin otettava huomioon, että riskikategoriat on huomioitava kokonaisvaltaisesti. Tämä tarkoittaa sitä että pelkkä riskien lukumäärä ei riitä. Jos tarkastellaan riskitasoja, huomataan että vakavimmiksi arvioidut riskit löytyvät ”pääsyoikeudet”-kategoriassa. Myös perehdytykseen liittyy vakavia riskejä, ja ”tahalliset”- kategoria pääsyoikeuksien tapaan koostuu lähes yksinomaan vakavista riskeistä.



	Pääsyoikeudet	Perehdytys	Tahalliset	Tuottamuskelliset	Rekry
4 Alhainen		1			
6 Lievä		1			
8 Uhkaava		4	2		
9 Melko vakava	1				
12 Vakava	1	2		2	
18 Erittäin vakava	3	1	1		
27 Äärimmäisen vakava	3	2	2		1

Kuvio 5: Riskitasojen jakauma

Kuvion 5 perusteella voidaan todeta, että pääsyoikeudet sekä perehdytys ovat osa-alueita, joihin liittyy paljon riskejä ja joihon kohdeorganisaation tulisi kiinnittää huomiota. Myös muut opetusalalla olevat organisaatiot voivat käyttää yllä olevaa dataa vertailukohteena omiin analyyseihinsa.

6.2 Lomakekyselyn tulokset

Lomakekysely lähetettiin yhteensä noin 23 henkilölle, joista kyselyyn vastasi kahdeksan eli noin 34 prosenttia. Vastausaika oli 12.3.2020–5.4.2020. Koska vastanneiden osuus otannasta on alle puolet, kyselyn tuloksia ei voida pitää luotettavana mittaamaan IT-harjoittelijoiden konsensusta kysymyksen aiheista. Kuitenkin se antaa arvokasta suuntaa antavaa tietoa kohdeorganisaation turvallisuusjohtamiseen sekä harjoitteluprosessin kehittämiseen.

Kyselyn tavoitteena oli selvittää, mikä on kohdeorganisaation harjoittelijoiden oma näkemys tietoturvaosaamisestaan, minkälaisena he näkevät tietoturvaosaamisen tason tietohallinnon ulkopuolella ja onko harjoittelulla ollut vaikutusta harjoittelijoiden tietoturva-osaamiseen. 50% vastaajista suoritti tällä hetkellä harjoitteluaan, ja puoliskosta, jotka olivat jo suorittaneet harjoittelunsa 50% oli suorittanut harjoittelunsa vuoden 2019 aikana ja 50% vuonna 2018. Vastaajista 87,5% ilmoitti myös opiskelleensa tietoturva-alan opintoja ennen harjoittelujaksoaan.

Vastanneista 62 prosenttia, arvioi tietoturvatietämyksensä tason ennen harjoittelujaksoaan asteikolla yhdestä neljään numerolla 3, ja 37,5% vastanneista arvioi tietämyksensä numerolla 2. Niistä, jotka olivat jo suorittaneet harjoittelunsa, 100% arvioi tietämyksensä tason harjoittelun jälkeen olevan 3. Voidaan siis huomata että harjoittelulla on ollut kehittävä vaikutus. Tämä näkyy seuraavassa kysymyksessä, jossa kysyttiin kokevatko harjoittelijat saaneensa tarpeeksi kattavan perehdytyksen tietoturvallisesta toiminnasta työtehtäviinsä. Vaikka POA löysi useita riskejä liittyen perehdytykseen, enemmistö harjoittelijoista (62,5%) kokee perehdytyksen olevan riittävä. Kuitenkin 37,5% koki päinvastoin. Tämä tarkoittaa karkeasti arvioiden vuosittain noin neljää harjoittelijaa, jotka ovat saaneet riittämättömän perehdytyksen tietoturvallisesta toiminnasta.

Seuraavassa kysymyksessä kysyttiin, kuinka harjoittelijat arvioisivat parhaiden tietoturvallisten käytäntöjen toteutumisen harjoittelunsa aikana yleisesti kohdeorganisaation servicedesk-palvelussa asteikolla yhdestä neljään. 50% vastaajista arvioi tietoturvallisten käytäntöjen toteutuneen numerolla 3, ja 37,5% vastasi numerolla 4. 12,5% vastaajista antoi arvosanan 2. Suurin osa harjoittelijoista näyttää siis kokevan tietoturvallisuuden olevan hyvällä mallilla.

Jotta saataisiin vertailukohde, harjoittelijoilta kysyttiin myös heidän kokemuksiaan asiakkaidensa, eli kohdeorganisaation opiskelijoiden sekä henkilöstön tietämystä

tietoturvallisista käytänteistä asteikolla yhdestä viiteen. 25% vastasi arvosanalla 4, kun taas 37,5% vastasi arvosanalla 3 ja 37,5% arvosanalla 2. Lopuksi kyselylomakkeessa annettiin mahdollisuus avoimeen vastaukseen tai lisätietoon mutta yksikään vastaajista ei tähän vastannut.

Lomakekyselyn perusteella voidaan esittää suuntaa antava toteamus, että harjoittelijat kokevat tietoturvallisuuden toteutumisen olevan kohdeorganisaation IT-harjoittelussa yleisesti hyvällä mallilla. Kuten aiemmin todettiin, tämä ei kuitenkaan vielä tarjoa luotettavaa dataa harjoittelijoiden näkemyksistä ja on myös otettava huomioon, että vastanneista valtaosa oli opiskellut tietoturva-alan opintoja ennen harjoitteluaan mikä omalta osaltaan saattaa vaikuttaa harjoittelijoiden näkemyksiin. Lomakekyselyn tulokset myös tukivat hypoteesia siitä että asiantuntijat ja harjoittelijat kokevat tietoturvallisuuden erilailla, sillä valtaosa harjoittelijoista piti esimerkiksi perehdytystä riittävänä, kun taas POA:ssa perehdytys arvioitiin yhdeksi kriittisimmistä osa-alueista.

6.3 Haastattelut

Haastatteluissa kysyttiin kysymyksiä asiantuntijoiden työtehtävien puitteissa ja liittyen työharjoitteluprosessiin. Ensimmäinen haastateltava toimi kohdeorganisaatiossa käyttäjähallinnan pääkäyttäjänä. Hänen (Liite 4) mukaansa käyttäjähallintaan liittyviä vakavia riskejä ei ole toteutunut viimeisen kymmenen vuoden aikana, kuitenkin lievempiä riskejä, kuten liiallisten käyttöoikeuksien myöntämisiä, tapahtuu vuosittain ”kohtuullisen usein”. Hän nostaa esille myös realisoituneita tilanteita, joissa harjoittelun keskeydyttyä harjoittelijan tunnuksia ei ole suljettu ajoissa, mikä mahdollistaa harjoittelijan pääsyn järjestelmiin työsuhteen päättymisen jälkeen. Näitä hänen mukaansa tapahtuu alle kymmenen vuodessa.

Seuraava haastateltu IT-asiantuntija vastasi tutkitusta service desk-palvelusta ja oli IT-harjoittelijoiden esimies. Hänen mukaansa yksi suurimmista uhista liittyen hänen työtehtäväänsä (haastattelija esitti kysymyksessä esimerkkinä työtehtävistä rekrytoinnin) on sellaisen harjoittelijan palkkaaminen, joka saattaisi olla motivoitunut vuotamaan arkaluontoista dataa ulkomaille esimerkiksi henkilökohtaisten taustojensa vuoksi. Kyseinen IT-asiantuntija myös toteaa tämän olevan osasyynä riskianalyysiprosessin käynnistämiseen koskien harjoitteluprosessia. Haastattelussa hän myös toteaa, että harjoittelijoiden perehdyttämisosaamisen taso on vaihtelevaa, mikä on vuosien 2017 - 2019 aikana johtanut paikoin perehdytyksessä saadun tiedon vääristymiseen virallisesta ohjeistuksesta.

Kolmas haastateltu toimi kohdeorganisaatiossa tietoturva-asiantuntijana, ja vastaa hallinnollisen tietoturvan kehittämisestä ja teknisestä tietoturvasta muiden asiantuntijoiden ohella. Kuten aiemmin kappaleessa 3.5.1 todettiin, erään IT-asiantuntijan (Liite 4) mukaan sosiaalinen manipulaatio ja haitalliset sähköpostin välityksellä kulkevat phishing-hyökkäykset

ovat yksi suurimmista uhista kohdeorganisaatiolle, ja ne kohdistuvat pitkälti johdon henkilöstöön. Mutta koska sosiaaliseen manipulaatioon ja eritoten phishing-hyökkäyksiin vaikuttaa käyttäjien oma toiminta, koskee uhka kaikkea henkilöstöä. Hänen mukaansa ”onnistuneita” phishing-hyökkäyksiä ei ole toistaiseksi ilmentynyt aikana, jona hän on toiminut työtehtävässä.

Yhteistä kaikkien asiantuntijoiden näkemyksissä oli se, että vakavia toteutuneita tietoturvariskejä ei ole organisaatiossa tai harjoitteluprosessissa todettu aiemmin.

7 Kehittämisehdotuksia

On muistettava, että riskienhallinta on alati jatkuva prosessi (kts. kuvio 2), ja koska riski on määritelmältään arvaamaton, tulisi kaikki organisaation prosessit ja alueet säännöllisesti arvioida uudelleen, vaikka ne olisi aiemmissa arvioinneissa todettu riittäviksi. Tämä tarkoittaa sitä, että aivan kuten kehitysprosesseissa, tulisi tietoturvan olla osana organisaation jokaista prosessia. Käytännössä tämä tarkoittaa sitä, että organisaation prosesseja tulisi tietoturvallisuuden osalta arvioida omina kokonaisuuksinaan säännöllisin aika-ajoin. Tämä antaisi viitekehyksen organisaation turvallisuustrategian toteuttamiseen sekä kokonaiskuvan tietoturvallisuuden toteutumisen trendeistä. Tutkimuksen alue, eli IT-harjoitteluprosessi, kuuluu osaksi organisaation tietohallinnon tai vastaavan elimen arviointia.

7.1 Auditointi

Yhtenä menetelmänä arvioimaan organisaation, ja erityisesti IT-harjoittelun ja muun tietohallinnon prosessien tietoturvan tilannetta, on tekninen tietoturva-auditointi. Tekninen tietoturva-auditointi *(eng. computer security audit)* on systemaattinen organisaation IT-järjestelmien turvallisuuskäytäntöjen arviointi, jossa auditoijalla on täysi tietämys organisaation toiminnoista ja järjestelmistä (Popescu ym. 2008). Auditoinnin avulla pystytään selvittämään tarkemmat tekniset puutteet järjestelmistään. Auditointi olisi suositeltavaa toteuttaa ulkoisesti, sillä silloin eliminoidaan mahdolliset eturistiriidat ja varmistetaan auditoinnin objektiivisuus. Auditoinnin avulla pystytään paremmin paikallistamaan järjestelmien puutekohdat sekä kehityskohteet. Myös Suomessa on tietoturva-alan yrityksiä, joiden palveluksia organisaatio voi käyttää suorittamaan tietoturva-auditointi. Suomen akkrediointipalvelu FINAS pitää yllä rekisteriä akkredioimistaan palveluntarjoajista, jotka pystyvät sertifioimaan järjestelmiä esimerkiksi ISO-standardien mukaan. Sertifikaatti kertoo yrityksen, prosessin tai järjestelmän vastaavan standardien vaatimuksia, ja näin ollen on luotettava ja vastaa odotuksia (ISO 2020). Auditoinnin avulla pystytään löytämään mitattavia kehityskohteita organisaation prosesseissa, sekä esimerkiksi täydentämään tämän tutkimuksen tuloksia.

7.2 Liiketoiminnallisten vaikutusten analyysi

Tutkitussa organisaatiossa IT- harjoittelijoiden työnkuvaan kuuluu sellaisten järjestelmien käyttö, joilla on mahdollista aiheuttaa vakaviakin haittoja organisaatiolle tahallisesti tai tahattomasti. Organisaation maineeseen kohdistuvat vahingot pystytään arvioimaan loogisella päättelyllä sekä nojaten organisaation toimintastrategiaan, mutta liiketoiminnalliset vahingot vaativat konkreettisempaa arviointia, jotta esimerkiksi tässä tutkimuksessa käytetyn potentiaalisten ongelmien analyysin havainnot pystyisivät syvemmin sitomaan osaksi organisaation turvallisuustrategiaa. Mutta miten tämä toteutetaan?

Liiketoiminnallisten vaikutusten analyysin tavoite on määrittää liiketoiminnalliset seuraukset organisaation ydinprosesseille tietojärjestelmien toiminnan pysähtyessä tai häiriöiden aikana (Thomas R 2010, 81). Liiketoiminnallisten vaikutusten analyysi on työkalu, joka täydentää riskinarviointiprosessia tuoden konkretiaa riskianalyysin tuloksille. Sen avulla voidaan havainnollistaa riskien vaikutuksia sekä määrittää priorisointi riskien kontrollointitoimenpiteille liiketoiminnan palautusprosessin aikana. Ilman liiketoiminnallisten vaikutusten analyysiä, on organisaation vaikea erottaa tärkeimmät liiketoiminnalliset prosessit siinä tilanteessa, kun riski on toteutunut ja organisaation on aloitettava kontrollointitoimenpiteiden toimellepano. Koska liiketoiminnallisten vaikutusten analyysi pyrkii myös määrittämään erilaisille tapauksille rahallisen haittavaikutuksen, auttaa se myös tieto-ja turvallisuus vastaavia argumentoimaan riskienhallintaprosessin havaintoja organisaation jäsenille ja sidosryhmille. Thomas, R:n (2020, 82) mukaan organisaatioiden on tärkeää tehdä molemmat, riskianalyysi sekä liiketoiminnallisten vaikutusten analyysi.

Liiketoiminnallisten vaikutusten analyysi toteutetaan ensin luomalla taulukko 3:en kaltainen taulukko, johon määritellään luokat riskien seurauksille. Näiden luokkien määrittämiseen voidaan käyttää apuna toteutettua riskianalyysiä ja sen tuloksia, esimerkiksi potentiaalisten ongelmien analyysiä. Taulukko 3 esittää esimerkin tällaisesta seurausluokkataulukosta, jossa riskien seurauksille on myös luotu kuvaavia kysymyksiä, jotka auttavat vaikutusten määrittelyssä.

Category	If the Asset Was Unavailable:
Competitive disadvantage	What would be the impact to our competitive standing?
Direct business loss	What would be the impact to our business revenues or profits?
Loss of public confidence or reputation	What would be the impact to our customer confidence, our public image, shareholder or supplier loyalty?
Poor morale	What would be the impact to our employee morale
Fraud	What level of goods, services or funds be diverted?
Wrong management decisions	What would be the impact to management having access to information to make informed business decisions?
Business disruption	What other applications, programs, systems, or business processes would be impacted?
Legal liability	Could the organization be in breach of legal, regulatory, or contractual obligations?
Privacy loss	Could our customers, clients, or employees suffer loss of personal privacy information?
Safety risk — "Risk"	What would be the impact to our customers, clients, and employee's health and safety?

Taulukko 4: Riskien seurausten luokat (Thomas, R. 2010, 84)

Taulukko 3 ei kuitenkaan vielä tarjoa konkreettisia vaikutuksia esitetyille seurausluokille, joten seuraava askel on selvittää kyseiset vaikutukset. Yksi työväline on haastatella asiantuntijoita sekä henkilöitä, jotka ovat vastuussa asianomaisista prosesseista, esimerkiksi organisaation liiketalousosaston henkilöstöä selvittämään rahalliset vaikutukset. Tässä vaiheessa tulisi myös selvittää kuinka kauan prosessi on toimimattomana riskin toteutuessa, näin luodaan viitekehys määrittelemään prosessin toiminnan häiriöitymisen vaikutukset. Tämän vaiheen tuloksista voidaan luoda esimerkiksi taulukko 4:en kaltainen taulukko, jossa jokaiselle seuraukselle on määritetty arvo kuvaamaan vaikutusten yhteisvaikutuksia sekä määritelty seurauksille eri liiketoiminnalliset vaikutukset, kuten esimerkiksi arvioitu rahallinen menetys.

Impact Value	Intangible Loss (Dollar Loss Difficult To Estimate)				Tangible Loss
	Health/Safety	Interruption of Production Impact	Public Image	Environmental Release	Financial ($)
1	Loss of life or limb	1 week	Total loss of public confidence and reputation	Permanent damage to environment	More than 10M
2	Requires hospitalization	3 days	Long-term blemish of company image	Long-term (1 year or more) damage to environment	1,000,001 to 10M
3	Cuts, bruises requiring first aid	1–2 days	Temporary blemish of company image	Temporary (6 months to 1 year) damage	100,001 to 1M
4	Major exposure to unsafe work environment	1 day	Company business unit image damaged	Department non-compliant	50,001 to 100K
5	Little or no negative impact Minor exposure to unsafe work environment	<4 hours	Little or no image impact	Little or no impact	0 to 50K

Taulukko 5: Seurauksien liiketoiminnalliset vaikutukset (Thomas R 2010, 85)

7.3 Tietoturvakoulutus

Potentiaalisten Ongelmien Analyysin tuloksien perusteella yksi tietoturvallisen IT-harjoittelun kompastuskivistä on perehdytyksen sekä työtehtäväkohtaisen koulutuksen puutteellisuus ja epäyhdenmukaisuus. IT-harjoittelijoille osoitetussa lomakekyselyssä 37,5% vastanneista koki perehdytyksen olleen riittämätön. Koska erään IT-asiantuntijan (Liite 4) mukaan harjoittelijoita on vuosittain töissä servicedesk-palvelussa noin 12, tämä tarkoittaisi karkeasti laskettuna noin neljää vuosittaista harjoittelijaa, jotka eivät saa tarvittavaa perehdytystä. Yhdistävä tekijä useassa tunnistetussa riskissä oli harjoittelijoiden tiedon puute käytössä olevista järjestelmistä tai tietämättömyys IT-alan parhaista käytänteistä. Näiden riskien toteutumisen todennäköisyyden minimoimiseksi olisi suositeltavaa, että organisaatio kouluttaisi harjoittelijansa toimimaan parhaiden tietoturvallisten käytänteiden mukaisesti.

Koulutuksen tulisi olla yhteneväinen sekä työtehtävään räätälöity koulutuspaketti osana harjoittelijan perehdytystä. Tekemällä tietoturvakoulutuksesta yhteneväisen minimoidaan riskiä siitä, että perehdyttäjien vaihtuessa harjoittelijat saavat eriävää tai puutteellista tietoa. Harjoittelijoiden kouluttaminen tuo myös lisäarvoa IT-tukipalveluille, sillä harjoittelijat pystyvät tukitilanteissa tarjoamaan asiantuntevaa ohjeistusta sekä luotettavammin reagoimaan mahdollisiin organisaation IT-järjestelmiin tai sidosryhmiin kohdistuviin hyökkäyksiin. Mikäli kyseisellä ammattikorkeakoululla on sisäistä asiantuntijuutta tai opetusmateriaalia, voidaan näitä hyödyntää opetuspaketin kokoamisessa, mutta markkinoilla on opetuspalveluita tarjoavia yrityksiä. Kuitenkin koulutuspaketti olisi toteutettava yhteistyössä organisaation tietoturva-asiantuntijoiden sekä tietohallinnon vastuuhenkilöiden kanssa, jotta voidaan varmistaa, että koulutus vastaa harjoittelijoiden työtehtäviä.

7.4 Turvallisuusselvitys

Ammattikorkeakoulussa IT-harjoittelijat työskentelevät organisaatioissa, jotka käsittelevät arkaluontoista tietoa kuten organisaation sekä sen sidosryhmien henkilötietoja sekä opiskeluun liittyvää dataa, esimerkiksi projektimateriaalia. Koska ammattikorkeakouluille on tyypillistä olla vuorovaikutuksessa ulkopuolisten tahojen kuten yritysten kanssa, on ammattikorkeakoulun käsittelemä data potentiaalisesti arvokasta. Tästä syystä CIA:n (Confidentiality, Integrity, Availability) toteutumisen kannalta on tärkeää, että henkilöt, joilla on pääsy organisaation tai sen sidosryhmien omistamaan dataan, ovat luotettavia, ja että kyseisten henkilöiden luotettavuus on todistettavissa. Myös EU:n tietosuoja-asetuksen GDPR:n (General Data Protection Regulation) artiklan 5 kohdan 2 mukaan organisaation on pystyttävä demonstroimaan artiklan 5 säätämien periaatteiden toteutuvan organisaatiossa. Tämän takia organisaatioiden olisi hyvä tuottaa taustaselvitys aiemmin mainituista henkilöistä. Taustaselvitys antaa organisaatiolle varmuutta siitä, että arkaluontoista

materiaalia käsittelevät henkilöt ovat mahdollisimman luotettavia. Taustaselvitys myös auttaa (organisaatiota) kohtaamaan GDPR:n sanelemat vaatimukset.

Suomessa suojelupoliisi toteuttaa yrityksille turvallisuusselvityksiä, joita työnantaja hakee lähettämällä hakemuksen suojelupoliisille. Tähän tarvitaan myös selvityksen kohteen hyväksyntä. Suojelupoliisi (2020) voi toteuttaa kolmea eri henkilöturvallisuusselvitystä: suppea turvallisuusselvitys henkilöille, jotka pääsevät osana työtehtäviään turvallisuuden kannalta merkittävään asemaan, perusmuotoinen turvallisuusselvitys, joilla työtehtävissään on mahdollisuuksia vaikuttaa valtion turvallisuuteen, sekä laajoja turvallisuusselvityksiä ihmisille, jotka käsittelevät yksityiskohtaisia henkilötietoja kuten terveys- tai varallisuustietoja. Laaja turvallisuusselvitys voi ulottua myös tutkittavan henkilön läheisiin. Ammattikorkeakoulu todennäköisesti hyödyntäisi suppeaa turvallisuusselvitystä. Turvallisuusselvitys ei kuitenkaan ota kantaa henkilön sopivuudesta tehtävään, vaan turvallisuusselvityksen lopputulosta tulisi käyttää rekrytoijan tukena arvioimaan hakijan soveltuvuutta.

8 Yhteenveto

Tämän tutkimuksen aikana opinnäytetyön tekijä tutustui tutkitun ammattikorkeakoulun tietohallinnon toimintaan sekä sen turvallisuustrategian toteutusperiaatteisiin. Organisaatio oli jo opinnäytetyön tekijälle tuttu siellä suoritetun työharjoittelun osalta. Koska työharjoitteluprosessi IT-palvelussa oli rajattu osaksi opinnäytetyön aihealuetta, oli tutkimuksen suunnitteluvaiheessa otettava tämä huomioon. Eturistiriitojen välttämiseksi opinnäytetyön varsinainen aineistonkeräysvaihe suoritettiin työharjoittelun ja näin myös kohdeorganisaation ja opinnäytetyön tekijän välisen työsuhteen loppumisen jälkeen.

Koska määrällistä dataa oli opinnäytetyön tekijän käytettävissä vähän, ja koska riskinarviointi ja hallinta on luonteeltaan subjektiivista relibiliateetin toteuttaminen oli haasteellista. Määrällinen data ja kvantitatiiviset menettelyt aineiston keräyksessä, esimerkiksi järjestelmien lokitiedot sekä kirjattu ja todennettu tietoturvapoikkeamahistoria olisivat tuoneet tutkimukselle tietoperustan, joka olisi ollut objektiivista ja näin ollen reliabiliteetin kannalta luotettavampaa.

Muita haasteita tutkimukseen toi tutkimusaineiston arkaluontoisuus. Tutkimus on edellyttänyt vuorovaikutusta kohdeorganisaation turvallisuus sekä tietoturva- asiantuntijoiden kanssa varmistamaan, että tutkimus ei vaaranna organisaation tietoturvaa paljastamalla salattua tietoa. Tästä syystä esimerkiksi POA:n tarkat tulokset asetettiin salatuiksi, ja samaten kohdeorganisaation nimi on vedetty pois raportista. Kaikesta huolimatta tutkimuksessa ei kohdattu kriittisiä esteitä, ja aineiston keräys oli onnistunutta sekä yhteistyö tutkittavan organisaation kanssa sujui hyvin ja joustavasti.

Tärkeimpänä havaintona tulisi nostaa esiin miten viestintä ja vuorovaikutus ovat tärkeässä osassa estämässä tietoturvariskien toteutumista. Tutkimuksen aikana havaittiin, että iso osa organisaation kohtaamista tietoturvariskeistä liittyy teknisen tietotaidon ja tietoturvallisten käytäntöjän ymmärtämisen puutteeseen, ja se avaa ovet sosiaaliselle manipulaatiolle kuten myös tuottamuksellisille riskeille. Monelle organisaatiolle kustannustehokkain ensiaskel voikin juuri olla tiedottamisen lisääminen ja tiedon levittäminen organisaatiossa.

9 Oman oppimisen arviointi

Pidin opinnäytetyöprojektia todella opettavaisena. Olin opiskellut ennen opinnäytetyön aloittamista tietoturva-alan opintoja ja oli innostavaa päästä tekemään opinnäytetyö aiheesta johon olin opinnoissani erikoistunut. Pidin myös siitä, että vaikka opinnäytetyötutkimuksen luonne oli hyvin itseohjautuva ja vaati oma-aloitteisuutta ja yksintyöskentelyä, pääsin kuitenkin toteutusvaiheessa työskentelemään alan ammattilaisten kanssa osallistumalla potentiaalisten ongelmien analyysiin osana aivoriihipienryhmää. Pidin tätä kokemusta yhtenä opettavaisimmista projektin aikana, sillä pääsin keskustelemaan tietoturva aiheista ihmisten kanssa jotka olivat alan ammattilaisia sekä tunsivat organisaation hyvin vuosien kokemuksen kautta. Koin että panostani ryhmässä arvostettiin vaikka kokemusta ja tietotaitoa minulta ei löytynytkään yhtä paljon kuin muilta ryhmän jäseniltä.

Opinnäytetyöprosessin aikana olen erityisesti oppinut katsomaan organisaatioiden erilaisia prosesseja isommalla kaavalla. Olen oppinut miten tietoturvallisuus on tärkeä osa kaikkea organisaatiossa tapahtuvaa toimintaa, ja kuinka se ulottuu paljon laajemmalle alueelle kuin vain tietotekniikkaan. Käytyäni keskustelua alan ammattilaisten kanssa olen ymmärtänyt kuinka pienetkin asiat voivat vaikuttaa tietoturvallisuuteen ja miten riskejä analysoidessa löydetään yllättäviäkin syy-seuraus suhteita oikeanlaisilla menetelmillä. Opinnäytetyö tuki hyvin tietoturva-alan opintojani, sillä pääsin kertaamaan paljon jo aiemmissa opinnoissa läpi käymää teoriaa, sekä aineistoa etsiessä löysin myös paljon uutta asiaa. En ollut aiemmin toteuttanut kyselyitä tai haastatteluita tällaisessa muodossa, joten pidin sitä virkistävänä vaihteluna ja haastavana kokemuksena.

Työn aihe koki muutoksia kirjoittamisen aikana, ja sitä suunnattiin keväällä 2020 uudestaan paremmin vastaamaan sitä mitä se käsitteli. Lopputuloksena valmis työ on hyvin erilainen kuin se suunnitelma minkä laadin syksyllä 2019, kuitenkin muutokset olivat välttämättömiä sillä näin työni tuottaa kohdeorganisaatiolle enemmän arvoa ja kuten aiemmin totesin, vastaa paremmin aihealuetta. Kaikki tämän jälkeen uskon että osaan vastaisuudessa paremmin suunnitella omaa työtäni sekä ottaa paremmin huomioon mahdolliset muutokset, sekä analysoida sitä mitä olen tekemässä paremmin jotta projektini ovat joustavampia. Kaikesta huolimatta olen kuitenkin tyytyväinen lopputulokseen.

Lähteet

Painetut

Norman, T. 2009. Risk Analysis and Security Countermeasure Selection. Florida: CRC Press LLC

Brinkmann, S. 2013. Understanding Qualitative Research Ser.: Qualitative Interviewing. Yhdistynyt kuningaskunta: Oxford University Press, Incorporated.

Podgorecki, Alexander, Shields &Prof. J.G Alexander. 1996. Social Engineering. Canada: MQUP

Hadnagy, C. Wilson, P. 2010. Social Engineering : The Art of Human Hacking. Yhdysvallat: John Wiley & Sons, Incorporated

Metsämuuronen, J. 2006. Laadullisen tutkimuksen käsikirja. Helsinki: International Methelp

Taylor, Alexander, Finch & Sutton. 2013. Information Security Management Principles. 2 painos. BCS Learning & Development Limited

Wolke, T. 2017. De Gruyter Textbook Ser. Risk Management. Saksa: Walter de Gruyter GmbH

Terje, A. 2012. Foundations of Risk Analysis. 2 painos. John Wiley & Sons, Incorporated

Osei-Bryson, K. Ko, M. Dorantes, C. 2008. Investigating the impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms. Researchgate.net. Texas: Department of Information Systems and Technology Management College of Business, the University of Texas.

Wilton, P. Colby, J. 2005. Wrox beginning guides, Beginning SQL. John Wiley & Sons, Incorporated

Norvanto, E. 2018. The Human Layer of Cybersecurity – the Art of Social Engineering, Handbook on Cyber Security - The Common Security and Defence Policy of the European Union. Luxembourg: The Publications Office of the European Union.

Tuomi, J. Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. 2 painos. Kustannusosakeyhtiö Tammi.

Sähköiset

International Organization for Standardization 2020. Certification & conformity, Certification. Viitattu 10.4.2020. https://www.iso.org/certification.html

Laurio, J. 2014. Mitä ovat hyökkäyspinta ja hyökkäysvektori? Viitattu 5.4.2020. https://www.nixu.com/fi/blog/mita-ovat-hyokkayspinta-ja-hyokkaysvektori

IBM 2020. X-Force Threat Intelligence Index 2020. Viitattu 16.3.2020. https://www.ibm.com/security/data-breach/threat-intelligence

Suojelupoliisi 2020. Turvallisuusselvitykset. Viitattu 7.3.2020. https://www.supo.fi/turvallisuusselvitykset

OWASP 2020. About the OWASP Foundation. Viitattu 10.3.2020. https://owasp.org/about/

OWASP 2017. OWASP Top 10. Viitattu 10.3.2020. https://owasp.org/www-project-top-ten/

Martikainen, S. Ranta, T. 2017. Turvallinen Tapahtuma – opas oppilaitosten ja korkeakoulujen tapahtumajärjestäjälle. Viitattu 13.2.2020. https://www.theseus.fi/bitstream/handle/10024/115581/Laurea%20julkaisut%2066.pdf?sequence=6&isAllowed=y

Suomen riskienhallintayhdistys 2012. PK-RH Riskienhallinta, Potentiaalisten Ongelmien Analyysi. Viitattu 13.11.2019. https://www.pk-rh.fi/tools/poa-analyysi.html#main

International Association for Standardization 2018. ISO/IEC 27000:2018. Viitattu 3.12.2019. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

UK Cabinet Office 2017. National Risk Register of Civil Emergencies 2017 edition. Viitattu 12.12.2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf

International Association for Standardization 2017. ISO/IEC/IEEE 24765:2017. Viitattu 12.12.2019. https://www.iso.org/obp/ui#iso:std:iso-iec-ieee:24765:ed-2:v1:en:term:3.3258

Popescu, G. Popescu, A. Popescu, C. 2008. Conducting an information security audit. Viitattu 15.2.2020. https://doaj.org/article/5c0a23c813ea4519a417e6a8bb7da47a

Elinkeinoelämän Keskusliitto 2016. Elinkeinoelämän yritysturvallisuusmalli. Viitattu 15.3.2020. https://ek.fi/wp-content/uploads/yritysturvallisuus_2016.pdf

Julkaisemattomat

Kuviot

Taulukot

Liitteet

Liite 1: POA analyysilomake (salattu)
Liite 2: Kyselyn vastaukset

Aikaleima	Oletko tällä hetkellä suorittamassa harjoittelua Laurean ServiceDeskissä?	Jos et, milloin suoritit harjoittelusi? (Vuoden tarkkuudella)	Olitko opiskellut tietoturva-alan opintoja ennen harjoittelujaksoasi?	Miksi oli tietämykseesi tasoa parhaista tietoturvallisista käytännöistä ennen harjoittelujaksoasi Laureassa?	Jos olet jo suorittanut harjoittelujaksosi, mikä oli tietämyksesi taso parhaista tietoturvallisista käytännöistä harjoittelujaksosi jälkeen?	Koetko, että olet saanut tarpeeksi kattavan perehdytyksen tietoturvallisesta toiminnasta työtehtävissäsi?	Miten arvioisit parhaiden tietoturvallisten käytäntöjen toteutumisen ServiceDeskin toiminnassa harjoittelusi aikana?	Miten arvioisit ServiceDeskin asiakkaiden (Opiskelijat, Laurean henkilökunta) yleisen tietämyksen tason tietoturvallisesta toiminnasta/käytänteistä?
12.3.2020 klo 18.18.51	Ei	Talvi-Syksy 2018	Ei	2	3	Kyllä	4	3
14.3.2020 klo 14.46.09	Kyllä		Kyllä	3		Kyllä	4	4
17.3.2020 klo 11.14.21	Ei	2019	Kyllä	3	3	Ei	3	3
17.3.2020 klo 11.39.54	Ei	2019	Kyllä	3	3	Kyllä	3	2
17.3.2020 klo 12.44.33	Kyllä		Kyllä	3		Kyllä	4	3
31.3.2020 klo 18.15.55	Ei	2018	Kyllä	2	3	Kyllä	3	4
31.3.2020 klo 16.56.57	Kyllä		Kyllä	2		Ei	3	3
2.4.2020 klo 21.05.30	Kyllä		Kyllä	3		Ei	2	2

Taulukko 6: Kyselyn vastaukset

Liite 3: POA- avainsanoja

Kohde	Asiat. Mitä muuta?	Ilmiöt, ongelmat. Mitä muita?
Ihmiset	Opastus • Uusi työntekijä • Vieraat • Esimies • Johtaja • Huoltomies	Sairaana • Huolimattomuus • Stressi • Rikos • Loppuunpalaminen • Avunsaanti • Kiire • Ei paikalla • Virheet • Osaaminen • Kielitaito • Toimintaohjeet • Turvallisuusohjeet • Skandaali • Moraali • Viina • Koulutus • Perehdyttäminen
Ympäristö	Liikenne • Rakenteet • Luonto • Jätteet	Liikkuminen • Pimeä • Liukas • Melu • Luvat • Häiriö
Rakennukset	Oma • Naapurit • Varasto • Työtilat • Julkiset tilat	Vuokrasuhde • Suojaus & vartiointi & valvonta • Muuttaminen • Kulkijat • Puhtaus ja siisteys • Remontti
Kuljetukset, varastointi	Suomessa • Ulkomailla • Sisäiset kuljetukset • Lastaus • Purku	Kolarit • Pysähtyminen • Pilaantuminen • Suojaus • Aikataulut • Väärään paikkaan
Tuotantoprosessi	Koneet ja laitteet • Työvälineet • Tietokoneet • Käyttöönotto • Koekäyttö • Kunnossapito • Sisäiset kuljetukset ja varastointi • Alihankkija	Käyttöhäiriö • Keskeytyminen & seisokki • Kunto • Tuotteen laatu • Rikkoutuminen • Väärinkäyttö, virheet • Valvonta, tarkastus • Säätö • Siivous, puhdistus • Kapasiteetti • Valmistettavan tuotteen vaihto • Pullonkaula • Hävikki • Riippuvuus
Tiedonkulku ja tiedonhallinta	Tiedot • Kokemukset • Puhelimet • Asiantuntijat • Puhelimet • Sähköposti • Arkistot • Tietokoneiden tietokannat • Ohjeiden ja käsikirjojen säilytys • Tilitoimisto	Kiire • Loma • Lakko • Hätätilanne, poikkeustilanne • Ymmärtäminen • Kielivaikeudet • Luottamuksellisuus • Luotettavuus • Tärkeät tiedot • Kriittiset viestit • Konsultit • Insinöörikieli
Materiaalit, raaka-aineet, energia	Valmistusmateriaalit • Prosessimateriaalit • Apuaineet / tarvikkeet • Sähkö	Laatu • Saatavuus • Riittävyys • Alihankkija • Toimitukset • Riippuvuus • Varasto
Keskittymät	Henkilöitä • Tietoa • Omaisuutta • Energiaa • Polttoainetta • Liikennettä • Muu keskittymä	Paljon samassa paikassa • Vähän samassa paikassa • "Kaikki munat samassa korissa" • Liikaa • Luvat • Suojaus, jakaminen
Onnettomuudet	Estäminen • Pelastautuminen • Toipuminen	Hälytykset • Hallinta • Kaikkien pelastus • Varasuunnitelmat
Projektit ja kehittäminen	Tuotekehitys • Toiminnan kehittäminen • Konsultit • Vienti • Menekki • Oikeudet	Kehittelyriskit • Rahoitus • Vientimaat • Vallankumoukset • Markkinoiden katoaminen • Muiden ja omat patentit
Ilmasto, sää	Ulkomailla • Sisällä • Ulkovarastossa • Kuljetuksissa	Sade • Vesi, tulva • Lumi, jää, routa, pakkanen • Helle, aurinko • Ukkonen, salama • Suojaus
Myynti, markkinointi, asiakaspalvelu	Asiakas • Asiakastarve • Toimitukset • Huolto • Neuvonta • Asiakaspalaute	Tärkeimmät • Väärinkäyttö • Tuntemus • Tarjonta • Kysyntä
Liikeriskit	Markkinointi • Yritysvakoilu • Rahoitus • Verot • Tiedot (asiakkaat, tuotteet, valmistus) • Investoinnit • Kilpailijat • Vientimaat • Politiikka • Yrittäjäjärjestöt	Läpilyönti • Huonot uutiset • Markkinoiden katoaminen • Velkaantuminen • Valuuttakurssit • Maksuhäiriö • Seuranta • Sopimukset • Strategia • Suunnittelu • Laskelmat • Suhdanteet • Lama • Olosuhteet • Hintakilpailu • Harmaa talous
Lainsäädäntö, standardit, perusvaatimukset	Luvat • Hyväksyminen • Määräystenmukaisuus • Oikeudellinen vastuu	Uusi lainsäädäntö • Kiristyvät säädökset • EU-direktiivit • Standardit • Paikalliset säädökset • Työehtosopimukset
Muut	Mikä tahansa! • Mikä puuttuu listoista!	Vika, vaurio • Vuoto, tukos • , Palo, räjähdys, karkaava reaktio • Myrkyllisyys, säteily, sähköisku • Tukehtuminen • Melu, tärinä • Maailman muutokset

Taulukko 7: POA-avainsanoja

Liite 4: IT- asiantuntijoiden haastattelut (salattu)