jamk

Uhka-riskimallinnus itsepalveluna

Helena Harju

Opinnäytetyö, AMK
Joulukuu 2024
Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Helena Harju

Uhka-riskimallinnus itsepalveluna

Jyväskylä: Jyväskylän ammattikorkeakoulu. Joulukuu 2024, 106 sivua.

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Digitalisaatio on johtanut yhä monimutkaisempaan teknologiseen ympäristöön, mikä altistaa yhteiskuntaa erilaisille uhille ja häiriöille. Tietoturva on keskeisessä asemassa tämän ympäristön suojelussa. Tiedon luottamuksellisuus, eheys ja saatavuus ovat tietoturvan perusta. Tietoturvasta huolehtiminen vaatii jatkuvaa tietoturvauhkien ja -riskien tunnistamista sekä riskienhallintaa. Opinnäytetyössä kehitettiin toimeksiantajan käyttöön tietoturvaan liittyvä uhka-riskimallinnuksen itsepalvelumalli. Tavoitteena oli kehittää konkreettisen mallin lisäksi käyttöön liittyvät tukimateriaalit ja tehdä mallista sellainen, että se tulee ajan myötä luonnolliseksi osaksi kehitys- ja ylläpitoprosessia.

Menetelmänä käytettiin tutkimuksellista kehittämistoimintaa, joka yhdistää ratkaistavan käytännön ongelman ja tutkimukselliset periaatteet. Teoriapohjana toimivat systemaattisen kirjallisuuskatsauksen kautta saatu tieto sekä toimeksiantajan sisäiset materiaalit. Työssä toteutettiin myös asiantuntijoiden taustahaastatteluja.

Opinnäytetyön tuloksena syntyi uhka-riskimallinnuksen uusi itsepalvelumalli, jonka kautta käyttäjät voivat tunnistaa tietoturvauhkia ja -riskejä, analysoida ja arvioida ne, sekä tehdä hallintatoimenpiteitä. Käyttö ei vaadi tietoturvan tai riskienhallinnan syvällistä asiantuntemusta, vaikka mallin taustalla onkin tietoturvan tärkeimpiä viitekehyksiä ja standardeja.

Säännöllisessä käytössä itsepalvelumalli liittyy osaksi kehitys- ja ylläpitoprosessia, käyttäjien tietoturvatietoisuus kasvaa, ja hallintatoimenpiteitä toteutettaessa toimeksiantajan tietoturvallisuuden taso paranee. Mallia on mahdollista kehittää huomioimaan erilaisia kohderyhmiä sekä uusia riskinäkökulmia. Malli on skaalautuva ja joustava eikä se ole organisaatiosidonnainen. Uhka-riskimallinnuksen itsepalvelumalli tarjoaa kattavan ja tehokkaan lähestymistavan tietoturvariskien hallintaan.

Toimeksiantaja piti mallia onnistuneena ja käyttökelpoisena. Mallia voisi jatkokehittää esimerkiksi käytettävyystestauksen kautta sekä luomalla erilaisia kohderyhmiä huomioivia lisäosia.

Avainsanat (asiasanat)

tietoturvallisuus, kyberturvallisuus, uhkamallinnus, riskimallinnus, riskien arviointi, riskienhallinta, tietoturvariski, tietoturvauhka

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Helena Harju

Threat and Risk Modeling as a Self-Service

Jyväskylä: JAMK University of Applied Sciences, December 2024, 106 pages.

Degree Programme in Information and Communications Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Digitalization has led to an increasingly complex technological environment, exposing society to various threats and disruptions. Information security plays a crucial role in protecting this environment. The confidentiality, integrity, and availability of information are the foundation of information security. Ensuring information security requires continuous identification and management of security threats and risks. In this thesis a self-service threat and risk modeling tool related to information security was developed for the client. The goal was to develop the modeling tool itself and also supporting materials related to its use, and making the tool a natural part of the development and maintenance process over time.

The method used was research-based development, which combines solving practical problems with research principles. The theoretical basis was formed by information obtained through a systematic literature review and the client's internal materials. Background interviews for the experts were also conducted.

The result of the thesis was a new self-service threat and risk modeling tool through which users can identify information security threats and risks, analyze and assess them, and implement risk management measures. Its use does not require deep expertise in information security or risk management, even though the model is based on key information security frameworks and standards.

With regular use, the self-service tool becomes part of the development and maintenance process, increases users' information security awareness and improves the client's overall information security level when implementing risk management measures. The tool can be developed to consider different target groups and new risk perspectives. It is scalable and flexible, not tied to any specific organization. The self-service threat and risk modeling tool offers a comprehensive and effective approach to managing information security risks.

The client found the model successful and useful. It could be further developed, for example, through usability testing and by creating add-ons that consider different target groups.

Keywords/tags (subjects)

information security, cybersecurity, threat modeling, risk modeling, risk assessment, risk management, information security risk, information security threat

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

Taulukot

Sanasto

Eheys (engl. integrity)

Tietojen luvattoman muokkaamisen tai tuhoamisen estäminen sekä sen varmistaminen, että tiedot ovat kiistämättömiä ja tiedon aitous on varmistettavissa (NIST CSRC n.d.).

IEC

International Electrotechnical Commission, kansainvälinen sähkötekninen komissio

ISMS (engl. Information Security Management System)

Tietoturvallisuuden hallintajärjestelmä

ISO

International Organization for Standardization, kansainvälinen standardointijärjestö

Jäännösriski (engl. residual risk)

Riskin käsittelyn jälkeen jäljellä oleva riski (ISO/IEC 27000:2020, 12)

Kyberturvallisuus (engl. cyber security)

Digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuus; kyberturvallisuuden häiriytyminen aiheutuu usein toteutuneesta tietoturvauhasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Kyberturvallisuus tarkoittaa myös yleisesti toimia, joilla suojataan mm. viestintä- ja tietojärjestelmiä sekä niissä olevia tietoja ja niiden käyttäjiä kyberuhilta. (Kyberturvallisuuden sanasto 2018, 22; Paananen ym. 2024, 10.)

Luottamuksellisuus (engl.confidentiality)

Varmuus siitä, että tietoja ei paljasteta luvattomille henkilöille, prosesseille tai laitteille. Luottamuksellisuus varmistetaan tietojen tallennuksen ja varastoinnin, käsittelyn ja siirron aikana. (NIST CSRC n.d.)

NIST

National Institute of Standards and Technology, Yhdysvaltain kauppaministeriön alainen standardisointi- ja teknologiainstituutti

Palvelu

Toimeksiantajan yläkäsite, jonka alla on järjestelmä tai useampia. Palvelu hoitaa jotain kokonaisuutta ja sillä on vastuuhenkilö.

Riskienhallinta (engl. risk management)

Koordinoitu toiminta, jolla organisaatiota johdetaan ja ohjataan riskien osalta (SFS-ISO 31000:2018, 6)

Saatavuus (engl. availability)

Varmistetaan tietojen oikea-aikainen ja luotettava saatavuus ja käyttö niille, joilla on oikeus tietoja käyttää. (NIST CSRC n.d.)

Uhka-riskimallinnus

Toimeksiantajan tapa yhdistää tietoturvauhkien ja tietoturvariskien mallinnus- ja käsittelyprosessit (tietoturvauhkien ja -riskien tunnistaminen, analysointi ja käsittely).

1 Johdanto

Digitalisaatio koskettaa laajasti koko yhteiskuntaa maailmanlaajuisista ratkaisuista aina yhden ihmisen tasolle saakka. Digitaalinen maailma tulee vastaan kaikilla elämänalueilla ja laajenee koko ajan. Tieto ja prosessit siirtyvät fyysisestä muodosta digitaaliseen. Käytettävät teknologiset ratkaisut ovat entistä monimutkaisempia, ja monimutkaistuminen vain jatkuu. Tietoa liikkuu tieto- ja viestintäpalveluissa sekä tietoverkoissa koko ajan enemmän. (Kansallinen riskiarvio 2023, 23; Limnéll, Majewski & Salminen 2014, 235.)

Digitaalisten järjestelmien ja tietoverkkojen lisääntynyt käyttö sekä toisaalta niiden monimutkainen infrastruktuuri altistavat yhteiskunnan toimijoita erilaisille kyberuhille ja häiriöille (Kansallinen riskiarvio 2023, 24-25). Kyberturvallisuus on tavoitetila, jossa digitaalisen ja verkottuneen yhteiskunnan toiminta turvataan. Tämän toimintaympäristön häiriytyminen aiheutuu usein toteutuneesta tietoturvauhasta, joten kyberturvallisuutta tavoiteltaessa tietoturva on keskeinen tekijä. Suomen kyberturvallisuusstrategiassa määritellään Suomen keskeiset toimintalinjat tähän liittyen. (Kyberturvallisuuden sanasto 2018, 22.)

Uudistettu Suomen kyberturvallisuusstrategia vuosille 2024-2035 hyväksyttiin syksyllä 2024. Kyberturvallisuus nähdään strategiassa erottamattomana osana Suomen kokonaisturvallisuutta. Digitalisoituvassa yhteiskunnassa kyberturvallisuudella on entistä tärkeämpi merkitys. Kyberuhilta suojaavat toimenpiteet auttavat tieto- ja viestintäverkkojen sekä yhteiskunnan infrastruktuurin toimimisessa kaikissa olosuhteissa. Sekä kyberturvallisuusstrategiassa että Kansallisessa riskiarviossa 2023 nähdään kyberturvallisuus keskeisenä osana yhteiskunnan häiriötöntä toimintaa. Digitaalisten järjestelmien ja niiden tarjoajien ja käyttävien riippuvuudet toisistaan voivat olla merkittäviä, jolloin yksittäisetkin häiriöt voivat ketjuuntua ja aiheuttaa suuria ongelmia. Tietoturvanäkökulmasta näillä häiriöillä voi olla vaikutusta tietojen saatavuuteen, luottamuksellisuuteen ja eheyteen. (Paananen, Soikkeli, Starck, Aro, Kuusisto, Rusila & Tuulensuu 2024, 10; Kansallinen riskiarvio 2023, 24.)

Tietoturvan laiminlyönnistä voi aiheutua vakavia seurauksia niin ihmisille, organisaatioille kuin yhteiskunnallekin. Tietoturvauhat ja niihin liittyvä rikollisuus kuten tietomurrot tai tietoverkkovakoilu tai -tiedustelu vaikuttavat pahimmillaan todella häiritsevästi yhteiskunnan toimintaan ja voivat sisältää myös kansalaisten perusoikeuksien loukkauksia sekä kansallista turvallisuutta vaarantavia

vaikutuksia. (Paananen ym. 2024, 15; Kansallinen riskiarvio 2023, 25.) Jokaisen toimijan sekä jopa yksittäisen ihmisen tulee varautua tietoturvauhkiin, tunnistaa riskit ja miettiä, miten riskejä voisi vähentää, poistaa tai miten niiltä voisi suojautua. On oltava valppaana ja ylläpidettävä omaa tietotaitoa (Järvinen 2022, 278).

Sekä julkisella sektorilla että muuallakin sääntely tietoturva-asioiden ympärillä on lisääntynyt sitä mukaa kun hyökkääjät kehittävät uusia tapoja aiemman sääntelyn kiertämiseksi (Paananen ym. 2024, 14). Tietoturvallisuuteen panostamalla saadaan lisättyä ja ylläpidettyä asiakkaiden ja kumppaneiden luottamusta (SFS-EN ISO/IEC 27001:2023, 6). Toimijan mahdollisuudet toteuttaa omaa strategiaansa paranevat, kun tietoturvallisuutta lisätään. Tämä vähentää myös taloudellisten menetysten ja mainehaittojen syntymistä. Tietoturvallisuuden lisääminen tuo monia hyötyjä ja parhaimmillaan jopa varmistaa toimijan olemassaolon ja perustan. (Death 2023.)

Opinnäytetyön aiheena oli uhka-riskimallinnus itsepalveluna. Työ tehtiin toimeksiantajalle, joka on julkishallinnon toimija. Toimeksiantajan tietoturvanäkökulmasta tekemät uhka-riskimallinnukset, sekä yleisesti ajatellen muutkin tietoturvanäkökulmasta tehtävät uhkamallinnukset ja riskimallinnukset, ovat erittäin tärkeitä, koska ne auttavat tunnistamaan ja arvioimaan tietoturvauhkia ja -riskejä. Toimeksiantaja käsittelee asiakastietoja, joten on erityisen tärkeää, että tiedot säilyvät CIA-triadin mukaisesti luottamuksellisina, eheinä ja saatavilla (SFS-EN ISO/IEC 27000:2020, 9; Nieles, Dempsey & Yan Pillitteri 2017, 2-3). Tietoturvallinen toiminta on toimeksiantajan toiminnan perusta. Tietoturvanäkökulman pitää läpileikata koko organisaatio kaikkine toimintoineen ja osa-alueineen, joten toimeksiantaja tekee tietoturvan eteen töitä monin tavoin. Yksi näistä toimintatavoista on tietoturvaan liittyvä uhka-riskimallinnus, josta tämän opinnäytetyön avulla kehitettiin itsepalvelumalli.

Aiemmin toimeksiantajan uhka-riskimallinnukset on toteutettu palvelun suunnitteluvaiheessa kertaluontoisesti ja tietoturva-asiantuntijavetoisesti. Palvelun elinkaaren eri vaiheissa uhka-riskimallinnuksia on toteutettu harvemmin. Koska tietoturva-asiantuntijoiden resurssit olivat rajalliset ja toisaalta haluttiin vahvistaa tekijöiden ymmärrystä oman palvelunsa kokonaisuudesta, oli opinnäytetyön konkreettisena tavoitteena toteuttaa uhka-riskimallinnukseen itsepalvelumalli. Tavoitteena oli, että palvelu voi käyttää itsepalvelumallia aina tarvitessaan ilman, että sitä tarvitsisi tilata erikseen. Myöskään tietoturva-asiantuntijoiden vapautuvia resursseja ei tarvitsisi jäädä odottamaan.

Tietoturva-asiantuntijat olisivat edelleen tarvittaessa tai aiheen niin vaatiessa tukena uhka-riskimallinnuksen tekemisessä, mutta kattavilla ohjeilla ja prosesseilla palvelu suoriutuisi asiasta suurimmassa osassa tapauksia itsenäisesti. Uhka-riskimallinnuksen itsepalvelumallin tarkoitus oli muuttaa suunnitteluvaiheen kertaluontoinen menettely sellaiseksi, että uhka-riskimallinnus olisi toteutettavissa säännöllisesti koko palvelun elinkaaren ajan. Näin palvelun tietoturvallisuus lisääntyisi verrattuna siihen, että asiaan syvennytään vain kerran.

Opinnäytetyön tulokseksi odotettiin konkreettista uutta itsepalvelumallilla toteutettavaa uhka-riskimallinnustyökalua, johon on liitetty liittyvät ohjeet, prosessit ja koulutusmateriaalit. Pidemmän tähtäimen odotuksia itsepalvelumallin käyttöön liittyen olivat, että uhka-riskimallinnuksesta saadaan toistuva ja pysyvä käytäntö, ja että palvelu pystyisi syventämään osaamistaan ja ymmärrystään omasta palvelustaan tietoturvauhkien ja -riskien osalta. Uhka-riskimallinnuksen itsepalvelumallin päivittämisen ja kehittämisen kautta tietoturvayksikkö voisi nostaa esille uusia riskinäkökulmia organisaation tarkasteltavaksi.

Opinnäytetyön tutkimusmenetelmäksi valittiin tutkimuksellinen kehittämistoiminta, joka on työelämän kehittämistoiminnan ja tutkimuksen välimaastossa. Tutkimuksellisesta kehittämistoiminnasta käytetään myös nimitystä tutkimuksellinen kehittämistyö tai soveltava tutkimus (Tuomi & Latvala 2022). Tutkimuksellisessa kehittämistoiminnassa käytännön ongelmat ja kysymykset ohjaavat työtä, mutta siinä hyödynnetään tutkimuksellisia periaatteita (Toikko & Rantanen 2009, 22). Teoriapohjana toimi systemaattinen kirjallisuuskatsaus ja uhka-riskimallinnuksen aiempaan tilaan perehdyttiin lisäksi tekemällä asiantuntijoille taustahaastatteluja sekä tutustumalla toimeksiantajan sisäisiin materiaaleihin.

Aihe oli tietoturvaan liittyvänä ajankohtainen ja siinä kehitettiin uusi toimintamalli. Toimeksiantajan esittämistä ehdotuksista aihe valittiin sen kiinnostavuuden lisäksi sen vuoksi, että aihe oli toimeksiantajalle merkityksellinen. Opinnäytetyöllä kehitettiin konkreettisesti uhka-riskimallinnusta ja saatiin käyttöönotettavaksi itsepalvelumalli tukimateriaaleineen. Ilman tätä opinnäytetyötä kehittämistyö olisi aiheen tärkeydestä huolimatta jäänyt tässä laajuudessa tekemättä tai ainakin merkittävästi viivästynyt niukoista käytettävissä olevista resursseista johtuen. Itsepalvelumallia käyttämällä tunnistetaan tietoturvan kannalta olennaisia asioita, joiden korjaaminen parantaa toimeksiantajan tietoturvan tasoa.

2 Tutkimusasetelma

Tässä luvussa tarkastellaan tämän opinnäytetyön keskeisiä kehittämiskysymyksiä, määritellään työn rajaukset ja esitellään käytetyt menetelmät sekä opinnäytetyön rakenne. Näiden osa-alueiden kautta pyritään luomaan selkeä käsitys opinnäytetyön sisällöstä ja lähestymistavasta sekä perustelemaan valittujen menetelmien soveltuvuus kehittämiskysymyksiin.

2.1 Kehittämiskysymykset

Opinnäytetyön tavoitteena oli toteuttaa uhka-riskimallinnuksen itsepalvelumalli, luoda sen käyttöön liittyvät ohjeet, prosessit, koulutusmateriaalit ja toteuttamiseen käytettävät perustyökalut, sekä kehittää mallia sellaiseksi, että se pitkällä tähtäimellä nivoutuu jatkuvaksi osaksi normaalitoimintaa ja siten parantaa palvelun tietoturvallisuuden tasoa. Kehittämiskysymykset, joihin opinnäytetyössä vastattiin, olivat:

1. Millainen on toimeksiantajan tarpeita palveleva uhka-riskimallinnuksen itsepalvelumalli?
2. Millaisia tukiprosesseja ja ohjeistuksia on rakennettava, jotta palvelu voi käyttää itsepalvelumallia?
3. Mitä tarvitaan, jotta uhka-riskimallinnuksen tekeminen muuttuu pysyväksi osaksi palvelun toimintaa?

2.2 Opinnäytetyön rajaus

Opinnäytetyö rajattiin koskemaan nimenomaan tietoturvaan liittyviä uhkia ja riskejä, ei kaikkia uhkia ja riskejä, joita palvelu tunnistaa. Toimeksiantaja on käyttänyt aiemminkin uhka-riskimallinnusta nimenomaisesti tietoturvauhkien ja -riskien tunnistamiseen. Riskien aihealueita ei ollut tarkoituksenmukaista tästä laajentaa, sillä muiden uhkien ja riskien hallintaan toimeksiantajalla on omat menettelynsä.

Uhka-riskimallinnuksen toteuttamista rajattiin lisäksi niin, että uhka-riskimallinnukseen käytettävä työkalu tehdään toimeksiantajalla jo laajassa käytössä olevilla järjestelmillä eli Atlassian-tuoteperheen Confluencella ja Jiralla. Tähän opinnäytetyöhön liittyen toimeksiantajalla ei ollut mahdollista lähteä kilpailuttamaan ja ostamaan ulkopuolisia järjestelmiä, joita markkinoilla oli tarjolla. Uhka-

riskimallinnustyökalun kehittämisen jälkeinen käyttöönottovaihe ei myöskään sisältynyt opinnäytetyöhön. Sen valmistelevat toimenpiteet eli esimerkiksi käyttöönottosuunnitelma, viestintäsuunnitelma ja tukimateriaalit tehtiin osana tätä työtä. Toimeksiantajan sisäiset materiaalit rajattiin tietoturvasyistä tämän opinnäytetyöraportin ulkopuolelle. Valmista uhka-riskimallinnusmateriaalia ja siihen liittyviä seikkoja on esitelty tässä raportissa siltä osin kuin se on mahdollista toimeksiantajan tietoturvaa tai tietojen luottamuksellisuutta vaarantamatta.

2.3 Menetelmäkuvaus

2.3.1 Tutkimuksellinen kehittämistoiminta

Tutkimuksellinen kehittämistoiminta lähtee yleensä liikkeelle käytännön ongelmista, ja tietoa tuotetaan käytännön toimintaympäristössä. Tutkimuksellisen kehittämistoiminnan apuna käytetään tutkimuksellisia asetelmia ja menettelyjä. Tarkoituksena on, että konkreettisen ongelman ratkaisemisen lisäksi tuotetaan tietoa myös laajempaan keskusteluun. (Tuomi & Latvala 2022.) Tähän opinnäytetyöhön tutkimuksellinen kehittämistoiminta valittiin sen vuoksi, että aihe oli kehittämislähtöinen konkreettinen asia: malli piti saada uusittua itsepalveluna toteutettavaksi. Tutkimuksellisessa kehittämistoiminnassa tavoitellaan konkreettista muutosta mutta pyritään samalla myös perusteltuun tiedon tuottamiseen (Toikko & Rantanen 2009, 21-24). Tutkimuksellisessa kehittämistoiminnassa hyödynnetään tutkimuksellista logiikkaa. Se korostaa Toikon ja Rantasen (2009) mukaan tiedonkeruun systemaattisuutta, dokumentaation ja analyysin huolellisuutta sekä perusteltujen johtopäätösten läpinäkyvyyttä. Tutkimuksellisessa kehittämistoiminnassa hyödynnetään myös kehitysprojekteille tyypillistä tarkkaa tavoitteiden määrittelyä, prosessia ja tulosten arviointia. (Toikko & Rantanen 2009, 157.)

Opinnäytetyössä yhdistettiin tutkimuksellinen menetelmä ja kehitysprojekti. Tiedonkeruu toteutettiin systemaattisesti ja toimeksiantajan materiaaleihin perehdyttiin tarkasti. Toimeksiantajan asiantuntijoille toteutettiin taustahaastatteluja ja näin saatiin syvempää tietoa aiheesta. Dokumentaatiossa pyrittiin siihen, että kaikki olennainen tieto on kirjattu opinnäytetyöhön. Analyysi ja johtopäätökset pyrittiin perustelemaan hyvin. Kehitysprojektimaisuutta opinnäytetyöhön tuli siitä, että aikataulu muokattiin yhdessä toimeksiantajan kanssa, määriteltiin osatavoitteet mitä missäkin jaksossa valmistuu, sekä seurattiin prosessia ja tuloksia säännöllisesti. Toimeksiantajan kanssa ol-

tiin säännöllisesti yhteydessä myös vaatimusmäärittelyjen osalta. Vaatimusmäärittelyt tarkentuivat työn edetessä. Opinnäytetyön tavoitteena oli saavuttaa tuloksia, jotka voisivat edistää myös laajempaa keskustelua. Toimeksiantaja totesi, että uhka-riskimallinnuksen itsepalvelumallin lopputulos kiinnostaa myös muita toimijoita. Opinnäytetyössä tuotettiin tietoa, jota voidaan kokeilla ja mahdollisesti ottaa käyttöön myös muissa organisaatioissa. (Toikko & Rantanen 2009, 156-157.)

2.3.2 Systemaattinen tiedonhaku

Systemaattinen katsaus (engl. systematic review) on tieteellinen tapa kerätä aineistoa. Prisma statement (Prisma - Transparent Reporting of Systematic Reviews and Meta-Analyses 2024) oli tähän sopiva apuväline. Sitä käytettiin opinnäytetyössä systemaattisen tiedonhaun varmistamiseksi. Prisma-taulukon avulla tietokannoista, rekistereistä, internet- ja muista lähteistä etsityt tiedot tulivat kattavammin käsitellyiksi kuin ilman taulukkoa. Systemaattinen katsaus lähteisiin varmisti, että lähteiden valintaa ei tehty vain tekijän mieltymykset tai suosikit huomioiden, vaan menettely oli systemaattista ja asianmukaista.

“Prisma 2020 flow diagram for new systematic reviews which included searches of databases, registers and other sources” koostui tiivistetysti kolmesta vaiheesta: tunnistaminen (engl. identification), seulonta (engl. screening) ja sisällyttäminen (engl. included). Tunnistamisvaiheessa tehtiin hakuja tietokantoihin ja internetlähteisiin, ja kerättiin tiedot siitä, paljonko mistäkin tietokannasta tai muusta lähteestä tuli osumia milläkin haulla. Mikäli jo tässä huomattiin duplikaatteja eli sama lähde toiseen tai useampaan kertaan, ne poistettiin. Lisäksi poistettiin ne, joihin ei ole pääsyä. Lukumäärät merkittiin muistiin. Seulontavaiheessa lähteitä tarkasteltiin tarkemmin. Lähteestä tarkasteltiin otsikkoa ja tiivistelmää. Jos lähde ei esimerkiksi hakusanasta huolimatta liittynyt aiheeseen, oli vanhentunut tms., se poistettiin ja sille merkittiin syynsä mukainen luokitusnumero. Lukumäärät merkittiin jälleen muistiin. Tämän jälkeen jäljelle jääneet lähteet seulottiin vielä kerran tarkemmalla tasolla. Ne, joita ei poistettu, otettiin mukaan lopulliseen tutkimukseen. Jokainen vaihe kuvattiin ja dokumentoitiin Prisma-taulukkoon. (Prisma - Transparent Reporting of Systematic Reviews and Meta-Analyses 2024.)

Teorialähteiksi haettiin opinnäytteitä, tutkimuksia sekä artikkeleja aihealueelta. Hakulähteinä olivat ArXiv (tieteellisten artikkeleiden julkaisupalvelu), Finna (opinnäytteet ja tutkimukset), IEEE (tie-

tokanta, jossa on IEEE:n (Institute of Electrical and Electronic Engineers) ja IET:n (Institution of Engineering and Technology) julkaisuja), JanetFinna (kansainväliset artikkelit), O'Reilly (ammattikirjallisuus), SFS Online (Suomen standardisoimisliiton tietokanta) sekä Theseus (opinnäytteet) ja internethaut. Systemaattisen tiedonhaun kautta tulleiden lähteiden lisäksi lähteiksi tuli tutkimusmenetelmiin liittyvää kirjallisuutta sekä termistöä sekä mm. kaupallisten riskimallinnuspalvelujen internetsivuja. Taulukossa 1 on käyty läpi tunnistamisvaiheen hakuosumien määrät ja tunnistamisvaiheessa tehdyt poistamiset.

Taulukko 1. Tunnistamisvaiheen tulokset

Hakupaikka	Hakuosumia eri hauilla (kpl)	Joista duplikaatteja (kpl)	Joista rajattuja tms. (kpl)	Jäljelle jäi (kpl)
ArXiv	216	-	- ei aiheeseen liittyvä 208	**8**
DuckDuckGo	212	49	- ei aiheeseen liittyvä 64 - epäkelpo 1 - rajattu 8 - liian vanha 4 - ei tuo uutta 7 - muu syy (esim. kurssimainos) 3	**76**
Finna	57	32	- ei aiheeseen liittyvä 19	**6**
IEEE	698	-	- ei aiheeseen liittyvä 691	**7**
JanetFinna	133	2	- ei aiheeseen liittyvä 103 - liian vanha 7	**21**
O'Reilly	198	19	- ei aiheeseen liittyvä 172	**7**
SFS	5	-	-	**5**
Theseus	922	107	- rajattu 96 - ei aiheeseen liittyvä 635	**84**
Yhteensä	**2 441**	**209**	**2018**	**214**

Hakuja tehtiin mahdollisimman uusiin lähteisiin. Haut rajattiin pääasiassa vuosille 2020-2024. IT-alalla tiedon kehitysvauhti on nopeaa, ja toisaalta uusistakin lähteistä kertyi osumia riittävästi. Yleisillä hakutermeillä kuten ”riskienhallinta”, ”tietoturva”, ”risk modeling” (amerikanenglanti) tai ”risk modelling” (brittienglanti) tuli tuloksia tuhansittain, englanniksi pahimmillaan jopa yli 55 miljoonaa hakutulosta. Tämä johtui pitkälti siitä, että riskienhallinta ja riskimallinnus ovat ilmiöitä, jotka tulevat vastaan jokaisella tieteen saralla ja elämänalueella. Hakuja piti rajata sen vuoksi mm. niin, että haussa oli mukana sekä ”risk modeling” (riskimallinnus) että ”information security” (tietoturva), koska opinnäytetyön uhka-riskimallinnus liittyi nimenomaisesti tietoturvariskeihin. Näin hausta palautui sellaisia osumia, jotka olivat enemmän aihepiiriin kuuluvia. Liian suppeaa ja vain

tiettyyn toimialaan kohdistuvaa hakua ei kuitenkaan kannattanut tehdä, koska toimialasta riippumatta riskienhallinnassa prosessina voi löytyä kiinnostavia yhtäläisyyksiä.

Tieteellisissä tietokannoissa hakua rajattiin siten, että tutkimukset ja artikkelit olivat vertaisarvioituja ja niihin oli open access eli pääsy ilman jäsenyyksiä tai rekisteröitymisiä. Kansainvälisiä artikkeleita etsiessä rajauksia tehtiin tiettyihin julkaisuihin, esimerkiksi International Journal of Information Security -nimiseen englanninkieliseen tutkimusjulkaisuun, koska sen artikkelit olivat lähempänä opinnäytetyön aihetta. Opinnäytetöiden julkaisupalvelussa Theseuksessa haut ”riskienhallinta” AND ”tietoturva”, ”tietoturvariski”, ”uhkamallinnus”, ”riskimallinnus” ja ”tietoturvariskien tunnistaminen” toivat yhteensä 922 osumaa joista 107 oli duplikaatteja, 96 rajattuja eli niihin ei ollut pääsyä, ja 635 osumaa oli opinnäytetyön aiheen ulkopuolelta. Runsaan rajattujen määrän selitti aiheena oleva tietoturva. Jos opinnäytetyö on tehty yritykselle heidän tietoturvansa tilasta, on ymmärrettävää, ettei työ ollut julkisesti saatavilla. Theseuksesta jäi seulontavaiheeseen siis 84 osumaa. Tähän samaan tapaan toimittiin kaikkien eri tietokantojen kanssa.

Internethauissa tuli runsaasti päällekkäisiä osumia ja myös saman pääsivuston alaisia osumia. Internethauista poistui seulontavaiheessa paljon sivuja, jotka eivät olleet tieteellisiä tai sisälsivät lähinnä mainoksia jostain tuotteesta, joka ei kuitenkaan liittynyt uhka-riskimallinnuksiin millään lailla. Tietyt sivustot kuten NIST (mm. https://www.nist.gov, https://csrc.nist.gov) ja OWASP (mm. https://owasp.org/www-project-threat-dragon/) toistuivat usein eri alasivuineen, ja niitä otettiinkin lähteeksi, koska ne sisälsivät erittäin kattavia ja tietoturvakentällä laajasti käytettyjä viitekehyksiä ja malleja.

Kansainvälisissä artikkeleissa tuli esiin, että uhkamallinnuksia ja riskimallinnuksia käsiteltiin siellä todella paljon esimerkiksi matemaattisiin riskien todennäköisyyslaskentakaavoihin, lohkoketjuihin, tekoälyn hyödyntämiseen, koneoppimiseen (engl. Machine Learning), suuriin kielimalleihin (engl. Large Language Models) sekä toisaalta IoT-laitteisiin (engl. Internet of Things, esineiden internet), 6G:hen tai vaikkapa avaruusmekaniikan riskienhallintaan liittyen. Nämä tieteelliset artikkelit olivat suurelta osalta liian teoreettisia tämän opinnäytetyön pohjaksi. Uhka-riskimallinnuksen itsepalvelumallin käyttäjän ei tarvitse esimerkiksi miettiä riskikertoimien osatekijöitä ja niihin liittyviä monimutkaisia laskukaavoja kertoimineen, koska riskien arvioinnissa toimitaan toimeksiantajan oman riskimatriisin pohjalta. Uhka-riskimallinnus tehtiin toimeksiantajan käytössä jo olevilla välineillä,

joten myöskään tekoälyä ja siitä tehtyä riskienhallinnan tutkimusta ei esimerkiksi voinut tässä vaiheessa opinnäytetyöhön yhdistää.

Systemaattisen tiedonhaun kokonaistuloksena käytiin läpi yhteensä 2 441 lähdettä, joista 214 jäi jatkoarviointiin. Näistä opinnäytetyöhön valikoitui lopulta 46 lähdettä. Taulukossa 2 on käyty läpi tiedonhaun seulontavaihe ja sisällyttämisvaihe. Seulontavaiheessa tehtiin ensimmäisessä osassa lähteen otsikon ja tiivistelmän tarkastelu tai internetsivun sisällön pintapuolinen tarkastelu, jonka kautta poistettiin 75 osumaa. Seulontavaiheen toisessa osassa käytiin lähde läpi tarkalla tasolla, ja tehtiin vielä toinen poistaminen. Ne, joita ei poistettu, otettiin mukaan opinnäytetyöhön. Systemaattisen tiedonhaun avulla lähteet saatiin käytyä läpi kirjallisuuskatsausta varten monipuolisesti ja kattavasti. Lähteet ohjasivat joissain tilanteissa uusille lähteille.

Taulukko 2. Seulonta- ja sisällyttämisvaiheiden tulokset

Hakupaikka	Tunnistamis-vaiheen jälkeen jääneet osumat (kpl)	Seulontavaiheen alkuosassa poistetut (kpl)	Seulontavaiheen toisessa osassa poistetut (kpl)	Sisällyttämis-vaiheeseen jäi (kpl)
ArXiv	8	-	- tarkemman syventymisen jälkeen sisältö ei ollut aiheeseen liittyvä 8	**0**
DuckDuckGo	76	- rajattu 1 - duplikaatti 3 - muu syy (esim. luotettavuus) 60	- kysely, kehittämisprojekti tms., joka ei hyödyntänyt opinnäytetyötä tieteellisesti 1	**11**
Finna	6	- duplikaatti 1	- tarkemman syventymisen jälkeen sisältö ei ollut aiheeseen liittyvä 3	**2**
IEEE	7	-	- tarkemman syventymisen jälkeen sisältö ei ollut aiheeseen liittyvä 7	**0**
JanetFinna	21	- rajattu 2 - duplikaatti 3 - muu syy (esim. luotettavuus) 5	- tarkemman syventymisen jälkeen sisältö ei ollut aiheeseen liittyvä 6 - muu syy esim. toistuva aihe, liian ylätasolla tms. 1	**4**
O'Reilly	7	-	- tarkemman syventymisen jälkeen sisältö ei ollut aiheeseen liittyvä 1 - muu syy esim. toistuva aihe, liian ylätasolla tms. 2	**4**
SFS	5	-	-	**5**
Theseus	84	-	- kysely, kehittämisprojekti tms., joka ei hyödyntänyt opinnäytetyötä tieteellisesti 8 - tarkemman syventymisen jälkeen sisältö ei ollut aiheeseen liittyvä 56	**20**
Yhteensä	**214**	**75**	**93**	**46**

Yksittäisiä lähteitä löytyi systemaattisen tiedonhaun lisäksi ajankohtaisia asioita seuraamalla LinkedIn -verkkopalvelussa julkaistujen uutisten kautta. Esimerkiksi Suomen Kyberturvallisuusstrategian 2024-2035 (Paananen ym. 2024) julkaisemisesta tehdyn uutisen kautta päädyttiin tutkimaan kyseistä strategiaa, ja ottamaan myös se tämän opinnäytetyön lähteeksi. Tausta-aineistoa opinnäytetyöhön kerättiin lisäksi toimeksiantajan sisäisestä ohjeistuksesta ja koulutusmateriaaleista. Toimeksiantajan materiaalit olivat organisaation sisäisiä ja niistä voi käydä ilmi myös tietoturvaan liittyviä luottamuksellisia asioita, joten niitä ei tietosuoja- ja tietoturvasyistä avattu tässä opinnäytetyössä enempää. Opinnäytetyötä varten haastateltiin yhteensä kymmenen tietoturva-asiantuntijaa, joista osa oli esihenkilöitä. Taustahaastatteluilla saatiin selville esimerkiksi aiemman uhka-riskimallinnuksen taustoja, kehittämistyön tarkempia vaatimusmäärittelyjä sekä hyviä näkökulmia ja ideoita uhka-riskimallinnuksen itsepalvelumallin kehittämistä huomioiden.

2.4 Opinnäytetyön rakenne

Ensimmäinen luku on johdanto. Siinä on esitelty opinnäytetyön aihe, sen tausta ja merkitys. Toisessa luvussa käsitellään kehittämiskysymyksiä, määritellään tutkimuksen rajaukset ja esitellään käytetyt menetelmät sekä opinnäytetyön rakenne. Luvussa kolme määritellään opinnäytetyön teoreettinen viitekehys. Aluksi käydään läpi aiempaa tutkimusta, kirjallisuutta sekä aiheeseen liittyviä opinnäytetöitä. Tämän jälkeen tarkastellaan keskeisiä käsitteitä ja viitekehyksiä, uhkamallinnus- ja riskienhallintamenetelmiä sekä -työkaluja. Viimeisenä käydään läpi riskienhallinnan kokonaisuus. Luvussa neljä kerrotaan uhka-riskimallinnuksen itsepalvelumallin rakentamisesta, sen lähtökohdista ja sisällöstä. Luvussa viisi käsitellään opinnäytetyön tulokset: itsepalvelumalli ja siihen liittyvät materiaalit. Siinä kerrotaan myös mallin vaatimustenmukaisuudesta, mittareista ja liittymäpinnoista sekä käyttöönotosta. Luvussa kuusi arvioidaan opinnäytetyötä monipuolisesti kehittämiskysymyksiin vastaamisen, luotettavuuden, validiteetin ja eettisyyden, sekä toteutuksen ja tulosten osalta. Luvussa seitsemän esitetään vielä kehittämisehdotuksia ja jatkotutkimusaiheita, joita nousi esiin tämän opinnäytetyön tekemisen aikana.

3 Teoreettinen viitekehys

Tässä luvussa määritellään opinnäytetyön teoreettinen viitekehys. Aluksi käsitellään aiempaa tutkimusta, kirjallisuutta ja aiheeseen liittyviä opinnäytetöitä. Seuraavaksi pureudutaan opinnäytetyön keskeisiin käsitteisiin: mitä tarkoittavat mm. tietoturva, CIA-triadi, uhka, riski ja haavoittuvuus

ja mikä on näiden suhde toisiinsa. Tämän jälkeen käydään läpi ISO-standardeja ja NIS2 -direktiiviä sekä NISTin viitekehyksiä ja kerrotaan, miten ne liittyvät opinnäytetyöhön. Tämän jälkeen esitellään uhka- ja riskimallinnuksiin käytettäviä työkaluja. Luvun päättää riskienhallinnan kokonaisuuden tarkastelu.

3.1 Kirjallisuuskatsaus

3.1.1 Aiheeseen liittyvä tutkimus ja muu kirjallisuus

Kuten aiemmin todettiin, riskienhallinta on niin laaja ja kaikenkattava aihe, että siihen liittyviä teoksia ja tutkimuksia sekä artikkeleita on kirjoitettu miljoonittain. Uhkien ja riskien mallinnusta täytyy tehdä alasta riippumatta koko yhteiskunnassa, joten osumia löytyi kaasuputkista ja laivanrakennuksesta aina sosiaalialan tietojärjestelmiin asti. Riskienhallintaa on kaikkialla, ja tietoturva-aihealue muodostaa siitä vain yhden osan. Uhka-riskimallinnukseen suoraan liittyviä tutkimuksia löytyi vain yksi, koska yleisempää on tehdä erikseen uhkamallinnus ja riskimallinnus tai riskianalyysi. Tietoturvauhkiin tai -riskeihin liittyvästä tutkimuksesta ja muusta kirjallisuudesta nousi esiin neljä keskeistä aihealuetta, joiden mukaan tarkastelua tehdään: 1. tietoturvaan liittyvät strategiat ja johtaminen, 2. uhkamallinnus ja tekniset analyysit, 3. riskienhallinta, riskienhallintatyökalut ja organisaation tietoturvatason arviointi sekä 4. tietoturvatietoisuus ja henkilöstön osaaminen.

Tietoturvaan liittyvät strategiat ja johtaminen

Johdon sitoutuminen nousi esiin tärkeimpänä asiana tietoturvallisuuden, tietoturvallisuuden hallintajärjestelmän (ISMS) sekä riskienhallinnan toteuttamisessa. Johdon pitää asettaa selkeät tietoturvatavoitteet, laatia tietoturvapolitiikka, määritellä roolit ja vastuutehtävät ja varata riittävät resurssit. Tehtävien ohjeiden, määräysten ja politiikkojen tulee olla toimeenpantavissa ja noudatettavissa. Tietoturvan merkitys ja lainsäädännölliset velvoitteet on viestittävä koko organisaatiolle. Työntekijöiden osaaminen on varmistettava, jotta kaikki ymmärtävät oman roolinsa ja toimintansa tärkeyden tietoturvallisuuden tavoitteiden saavuttamiseksi. (Calder 2023; Nair & Geershma 2023; Death 2023.)

Perusajatuksena esimerkiksi tietoturvallisuuden hallintajärjestelmällä on tukea organisaation muutosta tietoturvallisemmaksi. Muutokset koskevat organisaatiossa sekä ihmisiä, prosesseja että tek-

nologiaa. Jotta muutos voidaan viedä menestyksellä läpi, tarvitaan 1. avointa vuoropuhelua sidosryhmien kanssa sekä sen huolehtimista, että heidän tarpeensa ja huolenaiheensa huomioidaan tietoturvaratkaisuja suunniteltaessa, 2. tasapainoa tietoturvallisuuden ja käytettävyyden välillä, jotta organisaatio pystyy edelleen toimimaan tehokkaasti, ja 3. yhteistyön ja yhteisymmärryksen edistämistä. (Death 2023.)

Salmisen (2022) teoksessa Muutoksen johtaminen käsiteltiin muutoksen toteuttamista organisaatiossa. Hän käyttää käsitettä muutosmatka, ja siihen kuuluvat vaiheet ovat 1. lähtötilanteen kartoitus, 2. muutosmatkasuunnittelu, 3. suunnitelman toteutusvaihe sekä 4. muutoksen onnistumisen arvioiminen ja saavutetun muutoksen ankkurointi. Teoksessa viitataan Peter Druckerin lausahdukseen ”kulttuuri syö strategioita aamupalakseen”. Tämä on käyttöönottovaiheessa hyvä muistaa, sillä lähtötilanteen organisaatiokulttuuri säätelee sitä, kuinka organisaatio toimii, ja miten juuri tämä muutos on mahdollinen. Tärkeitä asioita ovat myös selkeä ja innostava muutosvisio ja huolellinen perusasioiden määrittely ja kuvaus yhteisen ymmärryksen saavuttamiseksi. Muutoksen onnistuminen edellyttää luottamusta eri osapuolten välillä. Salminen (2022) puhuu muutosenergiasta, jonka pitäisi säilyä koko muutosprosessin ajan. ”Muutosenergian säilyttämiseksi ovat muutosprosessin alkuvaiheen pienetkin onnistumiset erittäin tarpeellisia, ja niiden viestimiseen koko henkilöstölle kannattaa kiinnittää erityistä huomiota.” (Salminen 2022, 26-27, 52, 60, 73, 124, 129.)

Limnéll, Majewski ja Salminen (2014) korostavat kyberstrategian tärkeyttä osana liiketoiminnan strategiaprosessia. Sen avulla voidaan suojautua liiketoiminnalle merkityksellisiltä kyberuhilta sekä hyödyntää kybermahdollisuuksia, jotka tukevat organisaation kasvu- ja tehokkuustavoitteita. Kyberturvallisuus käsitteenä on laajempi ja kokonaisvaltaisempi kuin tietoturvallisuus, ja koska maailmanlaajuista kyberekosysteemiä ei hallitse kukaan yksittäinen taho, on tärkeää keskittyä sen eri osien turvallisuuteen. Parhaan suojan kyberuhkia vastaan tarjoavat perusasioiden kunnossapito: tietoisuuden lisääminen, toimintakyvyn kehittäminen ja tietoturvan ajantasaisuus. (Limnéll ym. 2014, 28, 55-56, 75, 107, 161-162.)

Uhkamallinnus ja tekniset analyysit

Uhkia voi arvioida paremmin, kun tarkastelee Yhdistyneen kuningaskunnan hallituksen tiedustelu- ja turvallisuusviraston GCHQ:n alaisen kansallinen kyberturvallisuuskeskuksen (NCSC, National Cyber Security Centre) määrittelemää neljää osa-aluetta: 1. kyvykkyys (engl. capability; uhkaajan kyvykkyys tehdä hyökkäys), 2. aikomus (engl. intent; mitä uhkaaja aikoo saavuttaa), 3. motivaatio (engl. motivation; mikä motivoi uhkaajaa tekemään hyökkäyksen) ja 4. tilaisuus (engl. opportunity; tilaisuus, jonka uhkaaja saa, jotta voi suorittaa hyökkäyksen) (Risk management 2023, 2). NCSC:n suositteleman varmennussuunnitelman (engl. assurance plan) käyttöönotolla varmistetaan, että suojattavat asiat ovat oikeasti suojattuina, ja että turvallisuuskontrollit toimivat sekä yksittäisinä että yhdessä odotetusti. Suunnitelmassa kerätään tietoa kontrollien suunnittelusta, toteuttamisesta, testaamisesta sekä ihmisiltä ja prosesseista. Varmennussuunnitelmaan liittyvä varmennusmalli puolestaan kuvaa sitä, että riskien hallintakeinot ovat sekä sopivia että tehokkaita. Mallissa sisäinen, ulkoinen, käyttöönottoon liittyvä ja operatiivinen varmennus ovat kytkeytyneitä toisiinsa. Näiden avulla voi osoittaa päättäjille, että palvelu on riittävän turvallinen. Esimerkiksi haavoittuvuuksien hallinta tuo sekä sisäistä että operatiivista varmennusta, ja turvallisuusvaatimukset sekä sisäistä että ulkoista varmennusta. Ulkopuolella sijaitseva pilvipalvelu ei ole kokonaan omissa käsissä, joten sen riittävät varmennuskeinot tulee pohtia eri tavalla kuin oman palvelun varmennuskeinot. (Risk management 2023, 6, 12.)

Limnéll ja muut (2014) toteavat, että täydellistä turvallisuutta ei ole, eikä sitä koskaan voida saavuttaa. Koska uhkia ja epävarmuutta on aina, eikä kaikkea voida turvata, täytyy asiat priorisoida. Mihin halutaan kohdistaa turvatoimia eniten? On mietittävä, miltä turvataan (uhat), mitä turvataan (kohde) ja miten turvataan (keinot). Organisaatioiden on otettava käyttöön vahvoja tietoturvatoimenpiteitä, koska kyberrikollisten taidot ovat kasvaneet, volyymit lisääntyneet ja pysäyttäminen vaikeutunut. Kalastelu- ja sosiaalisen manipuloinnin hyökkäykset, kiristyshaittaohjelmat, sisäiset uhat, kehittyneet jatkuvat uhat (APT:t) sekä pilvipalveluiden, mobiililaitteiden ja tekoälyn turvallisuushaasteet voivat vaarantaa organisaation turvallisuutta ja johtaa taloudellisiin menetyksiin ja maineen vahingoittumiseen. (Limnéll ym. 2014, 28, 37; Death 2023.)

Mahdollisuudet tuntuvat usein unohtuvan kyberturvallisuudesta puhuttaessa. Keskitytään uhkiin ja niiden torjumiseen, vaikka mahdollisuuksia innovointiin ja kehittämiseen on. Jos haluaa menestyä, tarvitsee molempia: sekä turvallisuuden varmistamista, että mahdollisuuksien hyödyntämistä.

Limnéll ja muut (2014) käyttävät käsitettä ”kybermahdollisuus”. Kybermahdollisuuksia toteutettaessa käytetään usein uusia liiketoimintamalleja ja tekniikoita, jolloin työntekijöiltä tarvitaan uudenlaista osaamista ja vanhojen toimintatapojen muuttamista. (Limnéll ym. 2014, 85, 91 & 202.)

Riskienhallinta, riskienhallintatyökalut ja organisaation tietoturvatason arviointi

Tietoturvariskien hallinnassa tärkeimmäksi nousivat CIA-triadi (ks. tarkemmin kuvio 2) ja ISO 27000 -perheen standardit (ks. standardeista tarkemmin luvusta 3.3.1). Tietoturvariskit arvioidaan ISO 27001 -standardin mukaan CIA-triadin eli tiedon luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta. Standardin tärkeimmät osat ovat tietoturvariskien arviointi ja niiden käsittely. Nämä muodostavat ISMS:n eli tietoturvallisuuden hallintajärjestelmän perustan. Sekä tietoturvallisuuden hallintajärjestelmää että riskien arviointimenetelmiä on jatkuvasti parannettava, jotta ne pysyvät ajankohtaisina ja tehokkaina suhteessa muuttuvaan riskiympäristöön. (Calder 2023; Death 2023.)

Organisaatioiden on ensin tunnistettava kriittisimmät tietonsa ja järjestelmänsä, jotta voidaan varmistua tiedon CIA-triadin toteutumisesta (Death 2023). Omaisuuserät tulee siis ensin kartoittaa, jotta voi löytää niihin liittyviä haavoittuvuuksia tai uhkia, jotka voisivat puolestaan hyödyntää niissä olevia heikkouksia. Omistajilla on tästä paras tieto, koska he tuntevat omaisuuksien haavoittuvuudet parhaiten. Haavoittuvuuksien tunnistaminen auttaa tunnistamaan mahdollisia riskejä. Riskeistä täytyy olla tietoinen, jotta voi käsitellä niitä. Toisaalta pitää pystyä jatkuvasti ja tehokkaasti arvioimaan, mikä on kunkin riskin senhetkinen taso, mitä riskejä pitää hallita ja missä määrin. ISO 27001 -standardi edellyttää, että tietoturvariskien arviointiprosessi "on määriteltävä ja toteutettava". (Calder 2023.)

Tunnistamisen jälkeen analysoidaan riskien todennäköisyys ja vaikutus, määritetään riskitaso ja arvioidaan se suhteessa riskin hyväksymiskriteereihin. Riskienarviointiprosessissa on oltava yhdenmukaiset riskin hyväksymiskriteerit sekä kriteerit tietoturvariskien arvioinnin suorittamiselle. Jokaiselle riskille on oltava omistaja eli henkilö, joka on vastuussa omaisuudesta, toiminnasta tai tehtävästä johon riski liittyy, tai henkilö, joka vastaa riskin hallinnasta. Prosessissa on varmistettava, että arvioinnit tuottavat johdonmukaisia, päteviä ja vertailukelpoisia tuloksia. Koko prosessi on dokumentoitava ja dokumentit säilytettävä. (Calder 2023.)

Kun riski on tunnistettu, edellyttää ISO 27001 -standardi kontrollien eli hallintakeinojen määrittämistä riskin hallitsemiseksi. Hallintakeino tarkoittaa toimenpidettä, jolla pyritään vähentämään riskitasoa, esimerkiksi palomuurin asentaminen. Luettelo hallintakeinoista on standardin liitteessä A. Tarkempi kuvaus jokaisesta hallintakeinosta on ISO 27002 -standardissa. Tietoturvan hallintajärjestelmää varten on analysoitava kaikki 93 liitteen A hallintakeinoa ja arvioitava yksitellen, mitkä niistä otetaan käyttöön ja mitkä jätetään perustellusti pois. Toki voi käyttää myös muita, esim. NIST SP 800-53:n mukaisia kontrollilistauksia. Kontrollit tulee ottaa käyttöön järkevästi ja suhteellisesti: niiden tulee olla järkeviä ja tarpeellisia, ja sellaisia, että niillä voi oikeasti hallita kyseistä riskiä. Kun kontrollit on valittu, tehdään riskienhallintasuunnitelma, jossa toimenpiteet, vastuut ja priorisointi näiden toteuttamiselle on kuvattu. Riskin omistajien on hyväksyttävä omat toimenpiteensä ja kontrollit sekä mahdollinen jäännösriski riskin käsittelyn jälkeen. Koko prosessi on jälleen dokumentoitava ja dokumentit säilytettävä. (Calder 2023; Death 2023; Risk management 2023, 12.)

Riskienhallinnan onnistuminen organisaatiossa vaatii Ilmosen, Kallion, Koskisen ja Rajamäen (2016) mukaan sitä, että riskienhallinta on tullut osaksi normaalia toimintaa ja johtamista. Tavoitteen eteen pitää tehdä paljon töitä. Aluksi tarvitaan riskikuva eli tieto siitä, millaisia ovat organisaation merkittävimmät riskit. Lisäksi pitää ymmärtää, mikä on riskinkantokyky, eli kestetäänkö jonkin tehtävän päätöksen johdosta siitä mahdollisesti aiheutuva riski. Kokonaisuuden hallitsemiseksi riskien riippuvuudet toisistaan on tunnistettava. Riskienhallinnan standardeja voi käyttää soveltuvin osin riskienhallintatyön tukena, koska ne edistävät yhteisen sanaston ja toimintamallien luomista. (Ilmonen ym. 2016, 5, 10, 17, 35.)

Riskienhallinta on Ilmosen ja muiden (2016, 18) määritelmän mukaan ”käytettyjen resurssien, pääomien ja kustannusten optimoimista suhteessa tavoiteltaviin hyötyihin.” Riskienhallinnan vieminen organisaation perusprosesseihin välittyy yleensä myös sen ulkopuolelle, ja antaa hyvän vaikutelman. Maine alan laadukkaana toimijana nousee. Pelkkä huomiointi ei tietenkään riitä, vaan tarvitaan systemaattista ja tavoitteellista riskienhallintaa, joka kasvattaa yleistä riskitietoisuutta. Ilmonen ja muut (2016, 41) toteavat, että ”Riskitietoisuuden kasvaessa riskienhallinnasta tulee vähitellen olennainen osa yrityksen kulttuuria ja tapaa tehdä yrityksessä töitä. Lopulta riskienhallinnasta tulee olennainen osa jokaisen työntekijän jokaista työtehtävää. Tällöin voidaan puhua erittäin kehittyneestä riskienhallintakulttuurista.”

Riskienhallinnan käyttöönottamisen alkuvaiheessa kannattaa pyrkiä perusasioiden kuntoon saattamiseen. Kun riskienhallinta saadaan osaksi vuosisuunnittelua ja prosessit ja raportointimenettelyt käyntiin, ei tule kuitenkaan luulla, että asia on nyt kunnossa. Riskienhallinnan pääpaino ei ole johtajille tehtävissä kauniissa raporteissa, vaan nimenomaan riskien hallinnassa. Tunnistaminen ja analysointi mahdollistavat ensinnäkin riskien priorisoinnin ja toiseksi hallintakeinoihin liittyvän päätöksenteon. Riskien hallinta oikeastaan alkaa toden teolla vasta silloin, kun hallintakeinoja mietitään. (Ilmonen ym. 2016, 46.)

Tietoturvatietoisuus ja henkilöstön osaaminen

Kun mietitään, miten tietoturvaa saadaan käytännössä toteutettua organisaatiossa, nousevat työntekijät tärkeään asemaan. Tarvitaan tietoturvapolitiikka, joka on dokumenttina saatavilla sekä organisaation työntekijöille että sidosryhmille (Calder 2023). On tärkeää, että organisaatioon kehittyy turvallisuus- ja tietoturvakulttuuri. Tämän edistämiseksi täytyy olla paljon viestintää ja koulutusta. Työntekijöiden on saatava riittävästi tietoa ja työkaluja sen toteuttamiseksi. Työntekijöiden ja organisaation yhteisvastuuta ja sitoutumista tietoturvaan on vahvistettava. (Death 2023.)

Puhutaan myös riskienhallintakulttuurista. Riskienhallintakulttuuri tarkoittaa sitä suhtautumistapaa, jolla työntekijät ja johto suhtautuvat riskienhallintaan. Jos kulttuuri ei ole suotuisa, ei riskienhallinnan toteutuminen onnistu. Riskienhallinta on yleensä hyvin käytännönläheistä toimintaa, ja se tapahtuu operatiivisella tasolla. Ilmonen ja muut toteavatkin, että ”Riskienhallinta on aivan liian keskeinen osa johtamista ja aivan liian tärkeää organisaation olemassaololle, jotta sitä kannattaisi tehdä miltään osin puolivillaisesti (Ilmonen ym. 2016, 89).” Työntekijöiden ei voi antaa ajatella, että heidän ei tarvitse miettiä riskejä, koska riskienhallintapäällikkö tuntee riskit. Todellisuudessa jokainen työntekijä toteuttaa riskienhallintaa jo vaikkapa noudattamalla ohjeita ja puuttumalla epäkohtiin. (Ilmonen ym. 2016, 29, 54, 88-89, 222.)

Turvallisuuskulttuuri, tietoturvakulttuuri ja riskienhallintakulttuuri pyrkivät suojelemaan organisaation resursseja ja toimintaa. Niissä pyritään luomaan yhtenäinen ajattelutapa ja toimintatapoja, mutta eri näkökulmista. Viestintä ja koulutus ovat keskeisessä asemassa. Johto määrittää tavoitteet ja toimintatavat, mutta jokaisen vastuulla on toimia niiden mukaisesti. Organisaation johto voi viestinnällään ja esimerkillään edistää näiden kulttuurien läpiviemistä. Tärkeää käytännön läpi-

viennissä on, että asialla on johdon tuki, ohjeistukset ovat toimintakelpoisia, työntekijät perehdytetään ja he ymmärtävät esimerkiksi riskienhallinnan tuottaman lisäarvon organisaatiolle. (Death 2023; Ilmonen ym. 2016, 66.)

Tietoturvan osalta Järvinen (2022) nostaa työntekijän näkökulmasta esiin mukavuuden. Mukavuus kertaa turvallisuus on vakio, eli kun toista kasvatetaan, toinen pienenee. Sellaista järjestelmää, joka on sekä mukava käyttää että turvallinen, on vaikea tehdä. Kyse onkin kompromissin löytämisestä: mikä on tietoturvan kannalta hyväksyttävissä, mutta ei kuitenkaan estä työntekoa. Tähän auttaa, kun työntekijät ymmärtävät, miksi rajoitukset ovat olemassa. (Järvinen 2022, 32-33.)

Tietoturvariskienhallinnan ja uhkamallinnuksen hybridimalli

Haji, Qing ja Soler Costa (2019) kehittivät tutkimuksessaan tietoturvaan hybridimallia, joka yhdisti hallinnollisen ja teknisen lähestymistavan riskienarvioinnissa uhkamallinnuksen avulla. Hybridimallilla pystyttiin osoittamaan, että yhdistämällä osia molemmista saadaan kattavampi lähestymistapa tietoturvariskien arviointiin. Kuviossa 1 on esitetty hybridimallin vaiheet. (Haji ym. 2019, 101-102, 104.)

Kuvio 1. Tietoturvariskienhallinnan ja uhkamallinnuksen hybridimalli (Haji ym. 2019, 102, muokattu)

1. Hybridimallin ensimmäinen vaihe on liiketoiminnan kohdentaminen. Siinä kehitetään tietoturvariskienhallinnan ja tiedon luokittelun politiikat, määritellään riskien arvioinnin laajuus ja suojaustoimenpiteet, riskien hyväksyttävä taso sekä mittaristot ja viestintästrategia. Tavoitteena on yhteensovittaa liiketoiminnan tarpeet ja tietoturvatoimenpiteet.
2. Omaisuuden profilointivaiheessa tunnistetaan ja luokitellaan omaisuus sekä määritellään sen omistaja. Omaisuuden pilkkomisella määritetään palvelun komponentit, joissa voi olla heikkouksia. Näillä toimenpiteillä saadaan syvällistä tietoa kyseisen omaisuuden tärkeydestä ja sen vaikutuksesta kriittisiin toimintoihin.
3. Haavoittuvuuksien löytämisvaiheessa käytetään usein automaattisia työkaluja tai manuaalisia prosesseja heikkouksien paljastamiseen. Haavoittuvuuslistaa on tärkeä mukauttaa olemassa olevan tiedon perusteella.
4. Uhka-analyysivaihe sisältää uhkaprofiloinnin, uhkaskenaarion muodostamisen ja uhkapuun tekemisen. Näillä vaiheilla tuotetaan tarvittavaa tietoa riskin rakentamisen vaiheeseen ja mahdollistetaan saman uhkaskenaarion toistaminen muilla vastaavilla komponenteilla.
5. Riskin laskemisvaihe voidaan mallin mukaan tehdä joko kvalitatiivisesti tai kvantitatiivisesti (esim. mittaamalla riskin rahallista arvoa). Tällä saadaan tietoa riskin arvioimiseksi ja päätöksenteon tueksi.
6. Kontrolliaukkoanalyysissa tarkastellaan olemassa olevia kontrolleja (hallintakeinoja), uusien kontrollien määrittämisen tarvetta sekä kontrollien aukkojen tunnistamista. Ensinnä selvitetään, ovatko olemassa olevat kontrollit riittäviä ja miten niitä voidaan parantaa tai täydentää hyväksyttävän riskitason saavuttamiseksi. Analyysi auttaa myös suunnittelemaan uusia kontrolleja ja parantamaan riskienhallintaa.
7. Riskin käsittelyvaiheessa suunnitellaan hyväksymättömien riskien käsittelyn yksityiskohdat ja optimoidaan toteutus ja sen kustannus–hyötysuhde. Uusien kontrollien toteuttaminen voi esimerkiksi tarvita taloudellista panostusta. Kun riskienhallinnasta nousee tarpeita kontrolleille, nostetaan riskien käsittelysuunnitelmat päätöksentekijöiden tietoon, jotta he puolestaan voivat hyväksyä lieventämistoimenpiteet riskin hyväksyttävän tason saavuttamiseksi. (Haji ym. 2019, 102-104.)

3.1.2 Aiemmat opinnäytetyöt

Tiedonhaun perusteella löytyi 20 aiheeseen liittyvää opinnäytetyötä. Vaikka kaikissa käsiteltiin tietoturvaa, tarkastelutavat ja painotukset vaihtelivat. Yksikään näistä töistä ei käsitellyt tarkalleen samaa aihetta, eli uhka-riskimallinnuksen itsepalvelumallia. Tämä opinnäytetyö tuo siten esiin näkökulman, jota ei ole käsitelty aiemmissa opinnäytetöissä, ja tarjoaa uudenlaisen lisän tietoturvaa sekä uhka- ja riskimallinnuksia koskevaan keskusteluun.

Tietoturvaan liittyvät strategiat ja johtaminen

Rivan (2021) opinnäytetyössä käsiteltiin johdon roolia tietosuojan toteuttamisessa. Tietoturva oli opinnäytetyössä sivuosassa. Useiden samaa aihetta sivuavien politiikkojen ylläpito niin, etteivät ne

sisällä toisiinsa nähden ristiriitaisia tietoja, on tärkeää. On oltava selkeä vastuuhenkilö, yhteisvastuullisuus ei toimi. Heinonen (2020) selvitti tietoturvan strategista johtamista sekä itse tietoturvastrategian rakentamista suomalaisissa suuryrityksissä. Merkityksellisen tietoturvastrategian elementtejä olivat, että se on konkreettisia tuloksia aikaansaava, ymmärrettävä, liiketoimintalähtöinen ja sitouttava ja vastuuttava (Heinonen 2020, 90).

Uhkamallinnus ja tekniset analyysit

Uhkamallinnuksia ja teknisiä analyyseja tutkivat Jansson (2021), Luoma (2023) ja Stenbäck (2020). Näissä töissä käytettiin erilaisia uhkamallinnusmenetelmiä, kuten STRIDE ja DREAD, ja keskityttiin järjestelmien tietoturvariskien tunnistamiseen ja arviointiin teknisellä tasolla. Jansson (2021) hyödynsi uhkamallinnusta tehdessään uhkien tunnistamismenetelmä STRIDEa, Microsoftin uhkamallinnustyökalua ja laski uhkien toteutumistodennäköisyyden DREAD-arviointimenetelmällä. Luoman (2023) työssä tehtiin strateginen uhkamallinnus sekä synteesi siitä, miten hyökkääjä voisi hyökätä organisaatiota vastaan. Tälle synteesille sitten tehtiin riskiarviointi sekä riskien lieventämis- ja vähentämistoimet. Itse strateginen uhkamallinnus oli työstä salattu, joten siihen ei päässyt konkreettisesti tutustumaan. Stenbäck (2020) tutki tietoturvanäkökulmaa vaatimusmäärittelyn ja järjestelmäsuunnittelun osana.

Riskienhallinta, riskienhallintatyökalut ja organisaation tietoturvatason arviointi

Riskienhallinnan sekä organisaatioiden tietoturvatason arviointi ja tähän liittyvien kehitysehdotusten tekeminen olivat Partasen (2020), Väänäsen (2021), Yli-Hietasen (2021), Baxterin (2021), Hytösen (2022), Stamatioun (2022), Jakimovan (2022) ja Virtaniemen (2023) opinnäytetöiden aiheina. Nämä työt keskittyivät riskienhallinnan nykytilan kartoittamiseen ja kehittämiseen, usein ISO 27001 tai ISO 31000 -standardien pohjalta. Väänäsen (2021) opinnäytetyössä tehtiin ISO 27001 -standardin mukainen puuteanalyysi yritykselle ja Yli-Hietasen (2021) opinnäytetyössä arvioitiin IT-alan yrityksen tietoturvan nykytilaa samaan standardiin verraten. ISO 27001 liite A:n vaatimukset oli käännetty suoraan kysymysmuotoon, ja tietoturvan tilaa käytiin läpi näiden kysymysten perusteella. Yrityksellä oli aikomus hankkia ISO 27001 -sertifiointi, joten opinnäytetyö osoitti konkreettisesti, mitkä asiat ovat jo kunnossa ja missä on vielä kehitettävää.

Baxterin (2021) opinnäytetyössä selvitettiin valtioneuvoston kanslian riskienhallinnan nykytilaa teemahaastatteluilla ja kyselyllä ja tavoitteena oli tätä kautta kehittää valtioneuvoston kanslian tietoturvallisuuden riskienhallintaa. Osaltaan opinnäytetyössä näkyi samoja elementtejä eli tietoturvatietoisuuden lisäämistä sekä vastuiden jakamista organisaatioon kuin tässä opinnäytetyössä. Baxter ei kuitenkaan käsitellyt konkreettista uhkien- ja riskienhallintaa. Baxterin (2021, 12) mukaan riskienhallinnan tulee olla organisaation kaikkiin osa-alueisiin ulottuvaa, eikä tietoturvaa ja riskienhallintaa tule eristää toisistaan. Hytösen (2021) yamk-opinnäytetyössä luotiin kokonaisvaltainen riskienhallinnan viitekehys ammattikorkeakouluympäristöön ja kerättiin toiminnan keskeisiä riskejä. Tietoturvauhkien ja -riskien tunnistamista ei työssä suoraan käsitelty. Stamatiou (2022) arvioi Rego Riskienhallinnan työkalun soveltuvuutta kohdeorganisaation käyttöön. Virtaniemen (2023) työssä selvitettiin riskienhallinnan tilaa ja Partasen (2020) työssä riskienhallinnan kypsyysastetta.

Jakimova (2022) perehtyi riskienhallintatyöpajojen kehittämiseen. Riskienhallintaprosessissa oli tunnistettu puutteita: esimerkiksi kokonaiskuvaa järjestelmistä ja niiden riskienhallinnan vaiheista ei ollut. Riskien käsittelyssäkin oli puutteita eikä vastuutahoja oltu nimetty. Kehittämisehdotuksena olivat mm. riskityöpajojen jälkeen tehtävien toimenpiteiden määrittely ja niiden vastuuttaminen sekä toimenpiteiden seuranta ja raportointi. Tuloksissa on havaittavissa samankaltaisuuksia uhka-riskimallinnukseen: uhka-riskimallinnusten aiemmassa tilassakaan ei ollut kokonaiskuvaa palvelujen riskienhallinnan vaiheista, ja riskien käsittelyssä ja vastuutahojen nimeämisessä sekä toimenpiteiden seurannassa oli puutteita. Uhka-riskimallinnuksen itsepalvelumallissa pyrittiin huomioimaan, että kokonaiskuva saadaan, ja vastuutahot sekä toimenpiteet saadaan sekä nimettyä, näkyviin että seurantaan. (Jakimova 2022, 23, 26-27.)

Tietoturvatietoisuus ja henkilöstön osaaminen

Häkkisen (2022), Selinin (2022), Heinosen (2022), Kälviäisen (2023), Walleniuksen (2023), Ylisen (2023) ja Lavrenzin (2024) opinnäytetöissä keskityttiin työntekijöiden tai opiskelijoiden tietoturvatietoisuuden kartoittamiseen ja tietoturvaosaamisen parantamiseen. Töissä selvitettiin kyselyjen ja haastattelujen avulla työntekijöiden tietoturvaosaamisen tasoa ja kehitettiin tulosten perusteella kohdeorganisaation tietoturvallisuuden tasoa tai tietoturvakulttuuria. Esimerkiksi Lavrenzin (2024) opinnäytetyössä laadittiin tietoturvaopas, jota työntekijä voi käyttää toimialasta riippumatta. Opas

on hyvä yleisopas esimerkiksi sellaisille yrityksille, joissa ei muuten juurikaan ole tietoturvakoulutusta. Lavrenzin (2024, 21) mukaan se ei kuitenkaan ”välttämättä tarjoa uutta tietoa henkilöille, jotka ovat saaneet tietoturvakoulutusta aiemmin tai työskentelevät it-alalla”. Heinosen (2022) opinnäytetyössä tietoturva-aihetta käsiteltiin työntekijän ja hänen osaamisensa sekä työntekijästä aiheutuvien tietoturvauhkien ja -riskien kautta.

3.1.3 Kirjallisuuskatsauksen yhteenveto

Tietoturvaan liittyvät strategiat ja johtaminen

Vahva ydinviesti on, että onnistumisen edellytyksenä on johdon sitoutuminen. Johtajien on asetettava selkeät tavoitteet ja politiikat sekä määriteltävä roolit, vastuut ja resurssit. Politiikkojen toteuttamiskelpoisuus ja laatu ovat avainasemassa. Tietoturvallisuuden parantamiseen liittyvään muutokseen tarvitaan avointa vuoropuhelua sidosryhmien kanssa, tasapainoa tietoturvallisuuden ja käytettävyyden välillä, sekä yhteistyön ja yhteisymmärryksen edistämistä. Muutosprosessi koostuu eri vaiheista, ja organisaatiokulttuuri vaikuttaa muutoksen onnistumiseen. Työntekijöiden osaamisen kasvattaminen ja viestintä (sisältäen myös onnistumisista viestimisen) ovat tärkeitä. Työntekijöiden on tunnistettava oma roolinsa ja toimintansa tärkeys tietoturvallisuustavoitteiden saavuttamisessa. (Calder 2023; Nair & Geershma 2023; Death 2023; Salminen 2022, 26-27, 129.)

Tietoturvaan liittyvät strategiat ja tietoturvan johtaminen liittyvät tämän opinnäytetyön aiheeseen eli uhka-riskimallinnuksen itsepalvelumalliin välillisesti tuoden sille nk. selkänojaa. On tärkeää huomioida Heinosen (2020, 90) mainitsemat merkityksellisen tietoturvastrategian elementit: konkreettisia tuloksia aikaansaava, ymmärrettävä, liiketoimintalähtöinen, sitouttava ja vastuuttava. Tällä tavoin saadaan tietoturvaa ja riskienhallintaa integroitua toimeksiantajan strategiseen johtamiseen. Johdon sitoutumisella ja viestinnällä on itsepalvelumallin käyttöönoton läpiviemisessä suuri rooli. Merkitys ja sen ymmärtäminen on olennaista: miksi tätä tehdään?

Uhkamallinnus ja tekniset analyysit

Uhkien arviointiin ja analysointiin on tarjolla runsaasti eri menetelmiä, joista osa soveltuu myös uhka-riskimallinnuksen itsepalvelumalliin. NCSC (Risk Management 2023) esitteli uhkien arvioinnin apuvälineeksi neljää osa-aluetta: kyvykkyys, aikomus, motivaatio ja tilaisuus. Lisäksi olisi hyvä tehdä varmennussuunnitelma (Risk Management 2023). Strateginen uhkamallinnus toi Luoman

(2023, tiivistelmä) mukaan yhden, yhteisen ja organisaatiotasoisen lähtökohdan uhkamallinnustyölle. Kaikilla oli käytössä sama uhkamalli, jota vasten riskejä arvioitiin. Tämän vuoksi eri järjestelmissä tehtävät riskiarviot olivat tasalaatuisempia. Harmillisesti malli itsessään oli opinnäytetyöstä salattu. Siitä olisi voinut olla konkreettista apua uhka-riskimallinnuksen itsepalvelumallin kehittämisessä. (Luoma 2023, tiivistelmä, 39-43.)

Täydellistä turvallisuutta ei voida ikinä saavuttaa, joten on tärkeää priorisoida toimenpiteitä ja keskittyä tärkeimpiin uhkiin ja kohteisiin. Tietoturvallisuuden parantaminen on yksi tärkeä askel, jota uhka-riskimallinnuksen itsepalvelumalli toteuttaa. Uudet liiketoimintamallit ja teknologiat voivat tarjota myös mahdollisuuksia. Näiden toteuttaminen vaatii uutta osaamista ja toimintatapojen kehittämistä. (Risk management 2023; Limnéll ym. 2014; Death 2023.)

Riskienhallinta, riskienhallintatyökalut ja organisaation tietoturvatason arviointi

Tietoturvariskienhallinnassa keskeisiä tekijöitä ovat CIA-triadi ja ISO 27000 -standardiperhe, jotka ohjaavat riskien arviointia ja käsittelyä. Organisaation on ensin tunnistettava kriittisimmät omaisuutensa ja arvioitava riskit niiden haavoittuvuuksien ja uhkien perusteella. Riskien arvioinnin jälkeen analysoidaan riskien todennäköisyys ja vaikutus, määritetään riskitaso ja valitaan tehokkaat hallintakeinot. Riskin omistaja vastaa riskin hallinnasta. Koko prosessi on dokumentoitava. (Calder 2023; Death 2023.)

Riskienhallinnan onnistuminen edellyttää sen integroimista osaksi organisaation päivittäistä toimintaa. Hyvin toteutettu riskienhallinta parantaa organisaation mainetta ja kehittää riskitietoisuutta, kun se tulee osaksi jokaisen työntekijän työtehtäviä. Tietoturvauhkia ja -riskejä käsittelevän uhka-riskimallinnuksen itsepalvelumallin kehittäminen tässä opinnäytetyössä ei ole yksi yhteen toimeksiantajan koko riskienhallinnan kehittämisen kanssa, mutta siihen pätevät pitkälti samat periaatteet. Kuten minkä tahansa muunkin riskienhallinnan osalta, standardeja on hyvä käyttää yhteisen termistön löytämiseksi. Tavoitteena on saada itsepalvelumalli osaksi päivittäistä toimintaa kasvattamalla yleistä tietoturvatietoisuutta. (Ilmonen ym. 2016, 35, 41; Calder 2023; Death 2023.)

Riskienhallinnan kypsyystason ja organisaation tietoturvatason arviointi jäävät tässä opinnäytetyössä kehitettävän itsepalvelumallin ulkopuolelle, koska ne koskettavat koko organisaatiota. Esimerkiksi riskienhallinnan kypsyystason arviointi olisi varmasti hyödyllinen toimeksiantajalle. Siinä

tulisi huomioida muukin kuin tietoturvaan liittyvä riskienhallinta. Hytönen (2021) käytti omaa riskienhallinnan viitekehystään rakentaessaan COSO ERM-viitekehystä ja ISO 31000 -standardia, jotka toimeksiantajallakin ovat käytössä. Kuten Hytönen (2021, 7) toteaa, käyttöönotettu viitekehys voi pitkällä aikavälillä lisätä mm. organisaation riskitietoisuutta. Uhka-riskimallinnuksen itsepalvelumalliin ei voitu rajauksen vuoksi hankkia erillistä työkalua, jonka käyttöönottoa sitten olisi voitu seurata, kuten esimerkiksi Stamatioun (2022) työssä. Vaikka aiemmat opinnäytetyöt liittyivätkin aiheeseen vain osittain, voi uhka-riskimallinnuksen itsepalvelumallissa hyödyntää niiden huomioita esimerkiksi käyttöönottovaiheeseen liittyen. Lisäksi on mahdollista seurata esimerkiksi Jiran riskirekisterin käytön lisääntymistä palveluissa aiempaan verrattuna, vaikka erillistä ulkopuolista työkalua ei olekaan hankittu.

Tietoturvatietoisuus ja henkilöstön osaaminen

Työntekijöiden rooli tietoturvan toteutuksessa on keskeinen. Tietoturvapolitiikan on siksi oltava selkeästi saatavilla, tietoturvariskienhallinnan menettelyjen tiedossa, ja viestinnän ja koulutuksen on oltava jatkuvaa ja työkalujen oltava toimivia. Näin edistetään organisaation turvallisuus-, riskienhallinta- ja tietoturvakulttuuria. Vaikka kulttuurin tila, tietoturvatietoisuus ja henkilöstön osaaminen näissä asioissa eivät ole tämän opinnäytetyön varsinaisia painopisteitä, on niihin kiinnitetty paljon huomiota. Pyrkimyksenä on, että uhka-riskimallinnuksen itsepalvelumalli edistää hyvää tietoturva- ja riskienhallintakulttuuria näiden tutkimusten, opinnäytetöiden ja teosten ajatuksia omaksuen. (Calder 2023; Death 2023; Heinonen 2022; Järvinen 2022, 32-33.)

Hybridimalli

Hajin ja muiden (2019) kehittämä hybridimalli muistutti toimeksiantajan uhka-riskimallinnusta. Toimeksiantajan perustelu uhkamallinnuksen ja riskimallinnuksen yhdistämiselle oli ajankäytöllinen, eikä uhka-riskimallinnuksen aiempi toteutus pohjaudu Hajin ja muiden hybridimalliin. Hybridimallissa on kuitenkin tunnistettavissa samoja elementtejä kuin tässä opinnäytetyössä kehitetyssä uhka-riskimallinnuksen itsepalvelumallissa ja pyrkimys on sama, eli yhdistämällä uhka- ja riskimallinnuksen elementtejä yhteen malliin, saadaan kattavampi lähestymistapa tietoturvariskien arviointiin. (Haji ym. 2019, 102-104.)

3.2 Keskeiset käsitteet ja niiden suhteet

3.2.1 Tietoturva ja tietoturvallisuus

Käsitteitä tietoturva ja tietoturvallisuus käytetään synonyymeina. Tietoturvan eli tietoturvallisuuden määritelmä Kyberturvallisuuden sanastossa (2018) on, että se tarkoittaa järjestelyjä, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuus tarkoittaa sitä, että kukaan sivullinen ei pääse käsiksi tietoihin. Eheys tarkoittaa sitä, että tieto on yhtäpitävää alkuperäisen tiedon kanssa, eli se ei ole muuttunut. Saatavuudella tarkoitetaan, että tieto on käytettävissä haluttuna aikana. (Kyberturvallisuuden sanasto 2018, 15.)

NISTin (n.d.) käyttämässä määritelmässä tietoturva tarkoittaa tietojen ja tietojärjestelmien suojaamista luvattomalta pääsyltä, käytöltä, paljastamiselta, häirinnältä, muokkaamiselta tai tuhoamiselta, jotta voidaan varmistaa niiden luottamuksellisuus, eheys ja saatavuus. Toisin sanoen tiedon luottamuksellisuus, eheys ja saatavuus ovat tietoturvallisuuden avainasiat. Tietoa suojataan haittavaikutuksia, kuten luvatonta pääsyä, paljastamista tai tuhoamista, vastaan. (NIST CSRC n.d..)

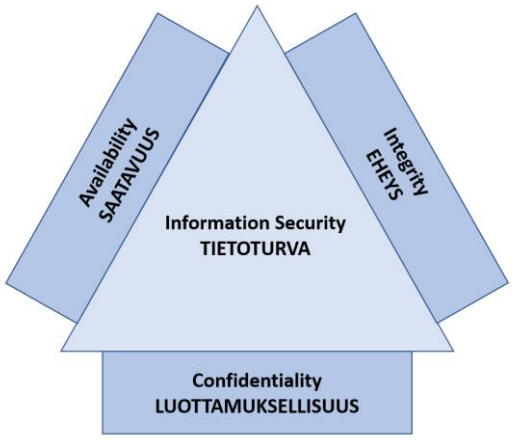
Tiedon luottamuksellisuuden, eheyden ja saatavuuden lisäksi on nostettu esiin pääsynvalvonta, todentaminen ja kiistämättömyys. Pääsynvalvonnalla tarkoitetaan sen varmistamista, että ainoastaan valtuutetuilla käyttäjillä on oikeus päästä tietojärjestelmään. Todentaminen tarkoittaa puolestaan sitä, miten valtuutettu käyttäjä voi todentaa käyttöoikeutensa (esim. käyttäjätunnus ja salasana, sähköinen avainkortti). Kiistämättömyys tarkoittaa sitä, että järjestelmää käyttävän henkilön tiedot sekä hänen tekemänsä toimenpiteet voidaan luotettavasti tunnistaa ja tallentaa, eli niistä jää lokitiedostot. Pääsynvalvonnan, todentamisen ja kiistämättömyyden huomioiminen laajentavat tietoturvan ajattelumallia. (Häkkinen 2022, 11.)

Tietoturvallisuus on toimeksiantajan määritelmän mukaan tietoaineistojen luottamuksellisuuden, eheyden ja saatavuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Uhka-riskimallinnuksen itsepalvelumalli on tarkoitettu nimenomaisesti tietoturvaan liittyvien uhkien ja riskien tunnistamiseen, arviointiin ja analysointiin. Tässä opinnäytetyössä tietoturvan käsitteenä käytetään seuraavassa luvussa esitettävää CIA-triadia, jota ei laajenneta suoraan esimerkiksi tunnistamisen, todentamisen ja kiistämättömyyden periaatteilla, vaikka näitä asioita uhka-riskimallinnuksessa nostetaankin esille. Tämä johtuu siitä, että mallin ensiaskelissa pyritään helppoon

omaksuttavuuteen. CIA-triadi on niin tunnettu ja ymmärrettävä, että sen käyttö sellaisenaan on aluksi vähemmän uutta omaksumista vaativaa ja kuvio on visuaalisesti helppo muistaa.

3.2.2 CIA-triadi

CIA-triadi on tietoturvan ytimessä (Death 2023). Se määrittelee tietoturvan perusperiaatteet ja ohjaa toimenpiteiden toteutusta tietojen ja tietojärjestelmien suojaamiseksi. ”C” tulee englannin kielen termistä confidentiality eli luottamuksellisuus, ”I” termistä integrity eli eheys ja ”A” termistä availability eli saatavuus. Kuviossa 2 on esitetty nämä CIA-triadin osa-alueet. Järvinen (2022) toteaa että luottamuksellisuus on käytännössäkin helppo ymmärtää. Esimerkiksi työnantajan palkanmaksutietojen suojaaminen niin, etteivät ulkopuoliset pääse niihin käsiksi, on luottamuksellisuuden periaatteen toteuttamista. Luottamuksellisuuden periaatteen toteuttaminen voi välillä olla vaikeaa. Miten saat esimerkiksi työntekijän olemaan paljastamatta yrityssalaisuuksia huijarille tai suojattua laitteet ja verkot niin, ettei kukaan pääse niihin oikeudettomasti käsiksi? Eheys tarkoittaa Järvisen (2022) mukaan sitä, että tiedot ovat loogisesti oikein, ja kaikki niihin tehdyt muutokset ovat sellaisia, joissa käyttäjällä on ollut oikeus muutoksia tehdä. Tieto ei siis ole päässyt vääristymään kenenkään pahantahtoisen hyökkääjän toimesta. Eheyden toteuttamista on esimerkiksi se, että tietokantaan pääsee tekemään muokkauksia vain pääkäyttäjän oikeuksilla, ei pelkillä peruskäyttäjän oikeuksilla. Saatavuuden periaate tarkoittaa, että tiedon tulee olla saatavilla silloin, kun käyttäjä sitä tarvitsee. Tämän periaatteen toteutumista varmistetaan erilaisin teknisin keinoin. (Death 2023; Järvinen 2022, 13-15.)



Kuvio 2. CIA-triadi (Death 2023, muokattu)

CIA-triadia täydennetään usein mm. kiistämättömyyden (engl. non-repudiation), tunnistautumisen ja todentamisen (engl. authentication), vastuullisuuden (engl. accountability) ja auditoitavuuden (engl. auditability) periaatteilla. Näiden näkökulmien huomioiminen auttaa organisaatioita torjumaan tietoturvauhkia kattavammin. Esimerkiksi kiistämättömyys varmistaa, että kukaan ei voi kieltää tehneensä jotain toimenpidettä. Pystytään todentamaan, onko henkilö tosiasiassa esimerkiksi lähettänyt viestin tai hyväksynyt jotain tehtäväksi. (Srivathshav 2020; Security and Privacy Controls for Information Systems and Organizations 2020, 409.)

3.2.3 Tietoturvariskienhallinnan elementit

Uhka-riskimallinnusta ei voi tehdä, jos ei tiedä, mitä riski ja uhka tarkoittavat. On hyvä huomioida, ettei uhka itsessään aiheuta riskiä, vaan tarvitaan myös kolmas tekijä, haavoittuvuus. Lisäksi siihen, miten uhka toteutuu, vaikuttavat hyökkäysvektori ja hyökkäyspinta-ala. Tässä luvussa käsitellään näiden käsitteiden määritelmiä sekä suhdetta toisiinsa.

Uhka ja tietoturvauhka

Uhka on ISO 27000 -standardin mukaan mahdollinen syy epätoivottuun tapahtumaan, josta voi seurata haittaa järjestelmälle tai organisaatiolle (SFS-EN ISO/IEC 27000:2020, 15). Ilmosen ja muiden (2016, 226) määritelmän mukaan uhka tarkoittaa tiettyyn, turvattavaan kohteeseen kohdistuvan vahingon tai häviön mahdollisuutta. Uhka-riskimallinnuksen itsepalvelumallissa mietitään uhkia nimenomaisesti tietoturvan osalta. Tietoturvauhka on Kyberturvallisuuden sanaston (2018, 25) mukaan ”mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu tietoturvaan ja toteutuessaan vaarantaa sen”. Limnéll ja muut määrittelevät uhan muodostuvan vastapuolen kyvystä ja aikomuksesta tehdä jokin vahingollinen tai epämieluisa teko tilanteessa, jossa se on mahdollista (Limnéll ym. 2014, 245). Yhdistyneen kuningaskunnan NCSC tarkastelee uhkia neljän osa-alueen kautta: kyvykkyys (uhkaajan kyvykkyys tehdä hyökkäys), aikomus (mitä uhkaaja aikoo saavuttaa), motivaatio (mikä motivoi uhkaajaa tekemään hyökkäyksen) ja tilaisuus (tilaisuus, jonka uhkaaja saa, jotta voi suorittaa hyökkäyksen). Nämä osa-alueet vaikuttavat siihen, miten uhka arvioidaan. (Risk management 2023, 2.) Toimeksiantajan määritelmä uhalle on, että se on mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku. Uhka-riskimallinnuksen itsepalvelumallissa tätä syvennettiin niin, että uhka kohdistuu nimenomaan tietoturvaan, eli tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen.

Riski ja tietoturvariski

Riski on määritelty sekä ISO 31000 -standardissa (SFS-ISO 31000:2018, 6) että Kyberturvallisuuden sanastossa (2018, 12) epävarmuuden vaikutukseksi tavoitteisiin. Vaikutus voi olla myönteinen, kielteinen tai molempia. Riski ilmaistaan tavallisesti riskin lähteiden, mahdollisten tapahtumien, niiden seurausten ja niiden todennäköisyyden yhdistelmänä. (SFS-ISO 31000:2018, 6.) NISTin (n.d.) määritelmässä todetaan, että riski on määritelmä sille, kuinka suuressa määrin taho on uhattuna mahdollisen olosuhteen tai tapahtuman vuoksi. Tarkasteltavana ovat haitalliset vaikutukset, jotka syntyisivät, jos tämä toteutuisi, sekä tapahtuman toteutumisen todennäköisyys. (NIST CSRC n.d..) Tietoturvariski on määritelty ISO 27000 -standardissa epävarmuuden vaikutukseksi tietoturvatavoitteisiin. Siinä on mahdollisuus, että uhka hyödyntää haavoittuvuutta ja siten aiheuttaa vahinkoa organisaatiolle. (SFS-EN ISO/IEC 27000:2020, 13.)

Euroopan unionin verkko- ja tietoturvadirektiivissä (NIS2) riski on määritelty poikkeaman aiheuttamien menetysten tai häiriöiden mahdollisuudeksi. Riski on menetysten tai häiriön suuruuden ja poikkeaman toteutumisen todennäköisyyden yhdistelmä. (Direktiivi 2022/2555/EU, 112, artikla 6.) Riski ilmenee tällä tavoin. Se, miten riski syntyy, vaatii vierelleen uhan ja haavoittuvuuden käsitteet (Death 2023). Riskin syntymisen pohtiminen on tärkeää, koska se auttaa tunnistamaan riskin ja sen mahdolliset vaikutukset selkeämmin. Tsohou, Karyda ja Kokolakis (2015) tutkivat kognitiivisia ja kulttuurillisia vinoumia tietoturvakäytäntöjen noudattamiseen liittyen. Riskejä pitää arvioida monipuolisesti, jotta tehtävien johtopäätösten päättely- ja tulkintavirheiden (nk. kognitiivisen vinouman) vaikutus vähenee. (Tsohou ym. 2015, 134-136, 139.)

Toimeksiantaja lähtee siitä näkökulmasta, että pelkällä riskikäsitetasolla operoitaessa johtopäätökset ovat alttiita päättely- ja tulkintavirheille. Tämän vuoksi tarvitaan tietoa nimenomaan siitä, miten riski syntyy. Riski on uhka x haavoittuvuus, eli jos toinen on 0, on myös tulos 0 eli riskiä ei ole. Uhkien ja haavoittuvuuksien tunnistamisen kautta riskeihin tulee syvempi ymmärrys, ja tiedostetaan paremmin, miten ja miksi riski syntyy. Toimeksiantajan mukaan riskistä puhutaan silloin, kun haavoittuvuus eli heikkous ja sitä mahdollisesti hyväksikäyttävä uhka ovat olemassa yhtä aikaa. (Katso uhan, haavoittuvuuden ja riskin käsitteiden yhteenliittymisestä tarkemmin tämän luvun alakohdasta Tietoturvariskienhallinnan elementtien suhde toisiinsa.)

Uhka-riskimallinnuksen itsepalvelumallissa on tärkeää tunnistaa uhkia ja haavoittuvuuksia, joista tietoturvariskejä voi aiheutua. Riskin on mainittu lyhyesti olevan tavoitteisiin vaikuttava epävarmuustekijä. Koska kyse on itsepalvelumallista, jota käyttävät muut kuin tietoturva-asiantuntijat, ei ole tarvetta lähteä syventämään käsitettä teoreettisesti enempää kuin toimeksiantaja on määritellyt. On tiedossa, että tässä vaiheessa kaikille ei ole tuttua miettiä riskejä, joilla voi olla myönteisiä vaikutuksia. Tämä johtunee pitkälti siitä, että yleiskielessä sanan ”riski” merkitys on kielteinen (Kyberturvallisuuden sanasto 2018, 12).

Riskit jaotellaan yleensä strategisiin, operatiivisiin ja taloudellisiin riskeihin. Strategiset riskit liittyvät organisaation pitkän aikavälin tavoitteisiin, operatiiviset puolestaan päivittäisiin toimintoihin. Taloudelliset riskit liittyvät rahaan. Tietoturvallisuuteen liittyvät riskit kohdistuvat tiedon saatavuuteen, luottamuksellisuuteen ja eheyteen. (Ilmonen ym. 2016, 77-81.) Riski voi kuulua myös useampaan ”lajiin” esimerkiksi olla sekä strateginen että taloudellinen. Toimeksiantaja jaottelee riskit strategisiin, operatiivisiin ja taktisiin riskeihin. Uhka-riskimallinnuksen itsepalvelumallissa käytetään toimeksiantajan jaottelua.

Haavoittuvuus eli heikkous

Haavoittuvuus on määritelty Kyberturvallisuuden sanastossa (2018) alttiudeksi tietoturvaan kohdistuville uhkille. Se on heikkous, joka mahdollistaa sen, että vahinko toteutuu. Sitä voidaan myös käyttää vahingon aiheuttamisessa. Haavoittuvuuksia eli heikkouksia voi löytyä niin tietojärjestelmistä, prosesseista kuin ihmisen toiminnastakin. Ilmosen ja muiden (2016) määritelmän mukaan haavoittuvuus tarkoittaa alttiutta turvallisuutta uhkaaville tekijöille. Haavoittuvuudessa on kyse suojattavan kohteen heikkoudesta, jota yksi tai useampi uhka voi käyttää hyväkseen. NISTin (n.d.) määritelmän mukaan haavoittuvuus on heikkous tietojärjestelmässä, turvallisuusmenettelyissä, sisäisissä kontrolleissa tai toteutuksessa. Tämä heikkous voi altistaa järjestelmän hyökkäykselle tai uhan aktivoitumiselle. NIS2 -direktiivissä haavoittuvuudella tarkoitetaan esimerkiksi palvelun heikkoutta, alttiutta tai vikaa, jota kyberuhka voi hyödyntää. (Kyberturvallisuuden sanasto 2018, 15; Ilmonen ym. 2016, 218; NIST CSRC n.d.; Direktiivi 2022/2555/EU, 112, artikla 6.)

Toimeksiantajan määritelmän mukaan haavoittuvuus on puute, vika tai toimintatapa, joka altistaa yhdessä uhan kanssa potentiaaliselle riskille. Uhka-riskimallinnuksen itsepalvelumallissa mietitään haavoittuvuuksien tunnistamista aiempaa syvällisemmin, koska halutaan, että haavoittuvuuksiin

kiinnitetään huomiota riskien ymmärtämiseksi paremmin. Haavoittuvuuksien tunnistaminen auttaa hyökkäysvektorien tunnistamisessa.

Hyökkäysvektori

Hyökkäysvektorin käsitteestä ei ole varsinaista tieteellistä käsitemäärittelyä, mutta se on hyvin tunnettu käsite kyberturvallisuuden piirissä. Hyökkäysvektori on se tapa, jolla hyökkääjä hyökkäyksensä toteuttaa. Se on konkreettinen menetelmä tai reitti, jota hyökkääjä käyttää haavoittuvuutta hyödyntääkseen. Hyökkääjä voi tämän reitin kautta päästä esimerkiksi käsiksi verkkopalvelimeen ja asentaa sinne haittaohjelman. (Shacklett n.d..) Toimeksiantajalla ei ole yleistä määritelmää hyökkäysvektorille. Uhka-riskimallinnuksen itsepalvelumallissa hyökkäysvektoria ei käsitteenä tuoda esiin, mutta sen tunnistamista edesautetaan kysymyksillä.

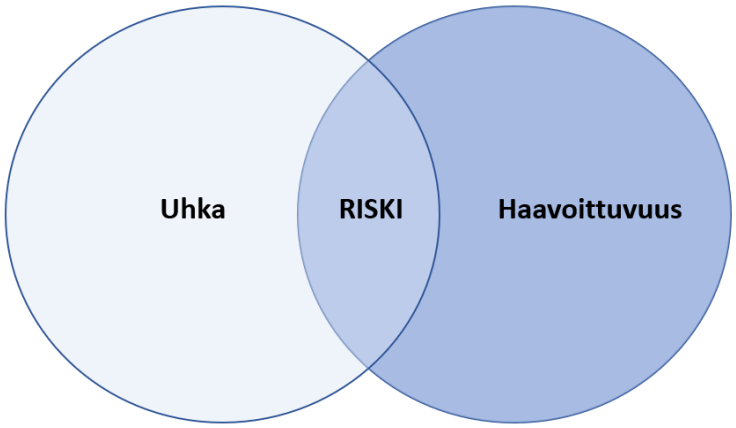
Hyökkäyspinta-ala

Hyökkäyspinta-ala on joukko sisäänpääsykohtia, joka sijaitsee järjestelmän, sen osan tai ympäristön rajalla, jossa hyökkääjä voi yrittää tunkeutua sisään, vaikuttaa toimintaan tai varastaa tietoja järjestelmästä, sen osasta tai ympäristöstä (Security and Privacy Controls for Information Systems and Organizations 2020, 395). Toimeksiantajalla ei ole yleistä määrittelyä hyökkäyspinta-alalle. Uhka-riskimallinnuksen itsepalvelumallissa hyökkäyspinta-alan käsitettä ei tuoda esiin, mutta se on mukana mallin taustalla.

Tietoturvariskienhallinnan elementtien suhde toisiinsa

Uhka, riski, haavoittuvuus, hyökkäysvektori ja hyökkäyspinta-ala ovat kaikki keskeisiä käsitteitä tietoturvassa, ja ne liittyvät toisiinsa muodostaen kokonaisuuden, jonka ymmärtäminen auttaa suojaamaan palveluja paremmin. Kuviossa 3 näkyy, miten uhka, riski ja haavoittuvuus liittyvät toisiinsa. Varsinaisen riskin määritelmän lisäksi uhka-riskimallinnuksen itsepalvelumallissa halutaan käsitellä riskin syntymistä. Uhan ja haavoittuvuuden tulee olla yhtä aikaa voimassa. Jos ne eivät ole yhtä aikaa voimassa, ei ole myöskään riskiä. Uhka ilman haavoittuvuutta ei aiheuta riskiä, kuten ei myöskään haavoittuvuus ilman uhkaa. Riskipotentiaali ilmenee vain, kun uhat ja haavoittuvuudet yhdistyvät. (Death 2023; Field 2023.) Kun uhka ja haavoittuvuus tunnistetaan, päästään kiinni riskin juurisyihin. Haavoittuvuus altistaa palvelun uhille. Riski voi syntyä, jos uhka toteutuu. Mitä

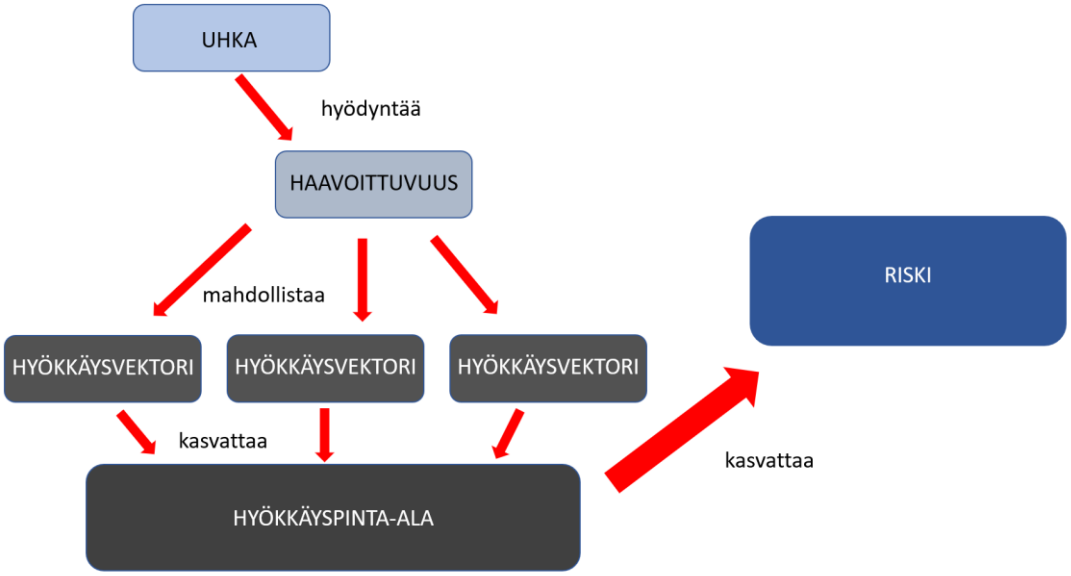
enemmän haavoittuvuuksia on, sitä enemmän on mahdollisia uhkia ja sitä suurempi on riski. (Cobb 2023; Calder 2023.)



Kuvio 3. Uhan, riskin ja haavoittuvuuden suhde toimeksiantajalla

Käytännön esimerkkinä toimii avoin kotiovi. Olet lähtenyt kauppaan ja jättänyt oven auki. Haavoittuvuus eli alttius päästää murtovaras sisään on olemassa. Jos asut yksin muutoin autiolla saarella ja lähtösi jälkeen nousee myrsky, ei murtovaras pääse saarelle koska sää on surkea. Näin ollen uhkaa ei ole. Silloin ei ole myöskään riskiä asuntomurrosta. Jos taas kerrot sosiaalisessa mediassa kauppareissustasi ja sää on mainio, murtovaras ottaa veneen ja lähtee keikalle. Tällöin sekä haavoittuvuus että uhka ovat olemassa, joten myös riski on olemassa. Uhka-riskimallinnuksen itsepalvelumallissa mietitään sekä uhkia että haavoittuvuuksia. Näiden yhdistelmästä aiheutuvia tietoturvariskejä sitten tunnistetaan ja käsitellään.

Uhka-riskimallinnuksen itsepalvelumallissa halutaan tunnistaa yhteydet uhan, haavoittuvuuden, riskin sekä hyökkäysvektorin ja hyökkäyspinta-alan välillä. Kuviossa 4 on esitetty näiden käsitteiden suhde. Uhka hyödyntää haavoittuvuutta. Haavoittuvuus mahdollistaa uhkan toteutumisen tiettyä reittiä (hyökkäysvektori). Mitä useampia haavoittuvuuksia ja/tai hyökkäysvektoreita on, sitä enemmän on hyökkäyspinta-alaa eli niitä paikkoja, missä uhka voi kohdistua palveluun. Mitä suurempi hyökkäyspinta-ala, sitä suurempi riski. Riski on seurausta näistä kaikista. Hyökkäyksen onnistuminen riippuu siitä, kuinka hyvin tai paljon uhka voi hyödyntää palvelun haavoittuvuuksia käytettävissä olevien hyökkäysvektorien kautta.



Kuvio 4. Uhka hyödyntää haavoittuvuuksia hyökkäysvektoreiden kautta, ja laajempi hyökkäyspinta-ala kasvattaa riskiä.

Käytännön esimerkkiä avoimesta ovesta voi täydentää hyökkäysvektorin ja hyökkäyspinta-alan käsitteillä. Jos olisit sulkenut ja lukinnut oven, mutta jättänyt ikkunan auki ja kellarin oven lukitsematta, olisi oven lukitsemisesta huolimatta kaksi hyökkäysvektoria olemassa. Jokainen reitti talon sisään on tässä hyökkäysvektori. Mitä enemmän näitä on, sitä suurempi on hyökkäyspinta-ala. Murtovarkaalle tämä vaikuttaa jo suorastaan tervetulokutsulta, eli riski asuntomurrolle on suuri.

3.2.4 Uhka-riskimallinnus

NISTin määritelmän mukaan uhkamallinnus on riskien arviointimenetelmä, joka mallintaa sekä hyökkäys- että puolustusnäkökulmia loogiselle entiteetille, kuten tiedolle, sovellukselle, isäntäjärjestelmälle, järjestelmälle tai ympäristölle (Security and Privacy Controls for Information Systems and Organizations 2020, 422). Uhkamallinnuksessa keskitytään uhkiin, joita tiettyyn tahoon voi kohdistua. Riskien arvioinnilla saadaan tietoa, kuinka todennäköisesti uhka voi vaarantaa omaisuuden, ja mitä vaikutuksia sillä olisi (Cobb 2023).

Uhka-riskimallinnus on toimeksiantajan tapa yhdistää tietoturvauhkien ja tietoturvariskien mallinnus- ja käsittelyprosessit (tietoturvauhkien ja -riskien tunnistaminen, analysointi ja käsittely).

Uhka-riskimallinnuksella on pyritty tiiviiseen ja resursseja säästävään ohjeistamiseen ja toimintaan. Tätä toimintatapaa käyttäen ei ole tarvinnut tehdä ensin uhkamallinnusta ja sen jälkeen ehkä osittain päällekkäistä riskimallinnusta, vaan on tehty molemmat samanaikaisesti. Tällaisena yhdistelmämallina uhka-riskimallinnuksen käyttö on toimeksiantajalla vakiintunut.

3.3 Viitekehykset

3.3.1 ISO-standardit

ISO ja IEC muodostavat maailmanlaajuisen järjestelmän, joka on erikoistunut standardisointiin (SFS-EN ISO/IEC 27001:2023, 5). Standardeissa annetaan ohjeita, joita voidaan soveltaa organisaatioon ja sen toimintaympäristöön soveltuvalla tavalla (SFS-ISO 31000:2018, 6). ISO-standardit eivät ole pakottavia, mutta niitä käytetään laajasti niiden tarjoamien yleisesti hyväksyttyjen käytäntöjen, luotettavuuden, kansainvälisen yhteensopivuuden, keskeisten riskienhallinta- ja tietoturvallisuusnäkökulmien sekä sertifioinnin ja niiden noudattamisella saavutettavan kilpailuedun vuoksi. Standardien noudattamisen ja varsinkin sertifioinnin katsotaan olevan tae organisaation laadusta ja halusta noudattaa asianmukaisia tietoturvaperiaatteita (SFS-EN ISO/IEC 27000:2020, 18).

ISO 31000

ISO 31000 -standardi sisältää ohjeita riskienhallintaan. Siinä kuvataan riskienhallinnan periaatteet, puitteet ja prosessi. Riskienhallinnan tarkoituksena on arvon luominen ja säilyttäminen, organisaation suorituskyvyn parantaminen sekä innovoinnin ja tavoitteiden saavuttamisen tukeminen. Riskienhallinta auttaa organisaatiota saavuttamaan tavoitteensa ja tekemään tietoon perustuvia päätöksiä. Riskienhallinta kuuluu osaksi kaikkia organisaation toimintoja, myös johtamiseen. Standardi korostaa ylimmän johdon johtajuutta ja sitä, että riskienhallinta sisällytetään organisaation johtamisjärjestelmään. (SFS-ISO 31000:2018, 4-5, 7.) Riskienhallinnan viitekehys ja riskienhallinnan prosessi ovat kaksi eri asiaa, jotka tukevat toisiaan. Pelkkä viitekehys eli yksittäisten riskien tunnistamis- ja hallintaprosessi ei hyödytä, jos sitä tukemassa ei ole strategisia politiikkoja ja johtamistoimia. (Field 2023.)

Riskienhallinnan toistuvuus on tärkeää. Kun koko ajan kertyy uutta kokemusta, tietoa ja tehdään analyyseja eri asioista, voidaan prosessia, toimintoja sekä hallintakeinoja uudistaa ja kehittää. Riskienhallintaa itseäänkin kehitetään jatkuvasti. Jotta riskienhallinta olisi vaikuttavaa, sen tulee olla

a) sisällytetty organisaation johtamisjärjestelmään, b) jäsennelty ja kattava, c) räätälöity, d) sidosryhmät mukaan ottava, e) dynaaminen, f) parhaaseen saatavilla olevaan tietoon perustuvaa, g) inhimilliset ja kulttuuriset tekijät huomioivaa sekä h) jatkuvasti kehittyvää. Toimeksiantaja noudattaa ISO 31000:n vaatimuksia riskienhallinnassa. (SFS-ISO 31000:2018, 4, 8-9.)

ISO 27000 -perhe

ISO 27000 -standardisarjasta puhutaan perheenä, joka käsittelee tietoturvallisuuden hallintajärjestelmiä (ISMS) ja niihin liittyviä osa-alueita. Organisaatio voi poimia ISO 27000 -perheen 50 standardin joukosta itselleen ja toimialalleen sopivat tietoturvastandardit. Perheen keskeiset standardit ovat ISO 27000, ISO 27001 ja ISO 27002. Näillä organisaatio voi toteuttaa ISO 27001 -standardin mukaisen tietoturvallisuuden hallintajärjestelmän. ISO 27001:tä käytetään myös sertifioinnin perustana. Loput standardit tarjoavat lisäohjeita tietoturvallisuuden hallintajärjestelmän osa-alueista tai lisävaatimuksia, jotka laajentavat hallintajärjestelmän kattamaan tiettyjä aihealueita. (Calder 2023; Nair & Greeshma 2023.)

ISO 27000 tarjoaa yleiskuvan tietoturvallisuuden hallintajärjestelmän (ISMS) toiminnasta, keskeisten termien määritelmät sekä perusperiaatteet. ISMS on tärkeä organisaation tietoturvallisuudelle, koska tieto ja siihen liittyvät järjestelmät ja prosessit ovat kriittistä liiketoimintaomaisuutta. Tietoturvallisuuden toteuttaminen puolestaan edellyttää riskienhallintaa. Voidakseen luoda ISMS:n ja parantaa sitä organisaation täytyy 1. tunnistaa tieto-omaisuus ja tietoturvavaatimukset, 2. arvioida ja käsitellä tietoturvariskit, 3. valita ja toteuttaa riskien hallintakeinot sekä 4. seurata hallintakeinojen vaikuttavuutta ja ylläpitää ja parantaa ISMS:ää. (SFS-EN ISO/IEC 27000:2020, 18-21.)

ISO 27001 on perheen selkäranka (Nair & Greeshma 2023). Se määrittelee tietoturvallisuuden hallintajärjestelmän vaatimukset ja luettelon keskeisistä tietoturvakontrolleista. Tietoturvallisuuden hallintajärjestelmän käyttöönotto on organisaation oma, strateginen päätös. Sen pyrkimyksenä on suojata tiedon luottamuksellisuutta, eheyttä ja saatavuutta riskienhallintaprosessin avulla. Osaltaan se vahvistaa sidosryhmien luottamusta riskienhallinnan asianmukaisuuteen. Liite A sisältää luettelon keskeisistä tietoturvakontrolleista, jotka ovat sovellettavissa jokaiseen organisaatioon. Tietoturvakontrolleja eli hallintakeinoja on 93 kappaletta. ISO 27002 antaa yksityiskohtaiset ohjeet näihin liittyen. Hallintakeinot on jaettu neljään hallintakeinosarjaan ja laajennettu kohdissa A.5–

A.8. Jokaiselle hallintakeinolle on useita attribuutteja, esim. tyyppi (ehkäisevä, havaitseva tai korjaava) ja tietoturvan osa-alue, johon se liittyy (hallintotapa ja ekosysteemi, suojaaminen, puolustus tai kriisinkestävyys). Näiden attribuuttien kautta hallintakeinoja on mahdollista tarkastella ja järjestää. ISO 27001:n toteuttaminen ei ole mahdollista ilman ISO 27002:a, ja ilman ISO 27001:n tarjoamaa johtamiskehystä ISO 27002:sta tulisi vain irrallinen toimenpide, jolla ei olisi merkittävää vaikutusta organisaation tietoturvaan. (Calder 2023; SFS-EN ISO/IEC 27001:2023, 6; SFS-EN ISO/IEC 27002:2022, 17-18; Nair & Greeshma 2023.)

ISO 27005 puolestaan keskittyy riskien arviointiin ja hallintaan. Tietoturvariskien arviointiprosessin vaiheet ovat 1. riskien tunnistaminen, 2. riskianalyysi ja 3. riskien merkityksen arviointi. Organisaation tulee varmistaa, että tietoturvariskien kohdalla toimintamalli ja periaatteet ovat samanlaiset kuin muiden riskien kohdalla, jotta ei synny kahta erillistä riskisaareketta vaan riskejä voidaan tarkastella tarvittaessa myös yhdessä. (ISO/IEC 27005:2022:fi, 21.) ISO 27005 on linjassa muiden standardien, kuten ISO 27001:n ja ISO 31000:n, kanssa, jotka tarjoavat kattavan kehyksen tietoturvallisuuden hallintaan ja yleiseen riskienhallintaan (Nair & Greeshma 2023).

ISO 27000 -perhe tarjoaa myös toimialakohtaisia tietoturvastandardeja, jotka on räätälöity eri alojen erityistarpeisiin. Toimialakohtaisia standardeja on tehty mm. terveydenhuoltoon, pilvipalveluihin ja energia-alalle. Esimerkiksi standardi ISO 27799 sääntelee terveydenhuollon tiedonhallintaa ISO 27002 -standardin avulla, standardi ISO 27017 pilvipalveluiden turvallisuusvaatimuksia ja standardi ISO 27019 energiainfrastruktuurin tietoturvaa (SFS-EN ISO 27799:2016, 1; SFS-EN ISO/IEC 27017:2021:en, 1; ISO/IEC 27019:2017, 1). Yksi uhka-riskimallinnuksen itsepalvelumallin kehittämisen vaatimus oli, että se mahdollisuuksien mukaan noudattaa ISO 27000 -perheen standardeja.

3.3.2 NIS2 -direktiivi

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa eli NIS2 -direktiivi (Network and Information Systems Directive 2) astui voimaan 18.10.2024. Direktiivillä haluttiin vahvistaa EU:n yhteistä kyberturvallisuuden tasoa sekä kansallista kyberturvallisuuden tasoa. Direktiivin soveltamisalaa laajennettiin aiempaan NIS1 -direktiiviin verrattuna, joten se kattaa nyt enemmän toimialoja ja organisaatioita. (Direktiivi 2022/2555/EU, 80-81, 142, artiklat 1, 2, 42.)

NIS2 -direktiivillä on annettu yhteiskunnan kriittisille sektoreille vähimmäisvaatimustaso erilaisista toimenpiteistä, joilla kyberturvallisuusriskejä hallitaan. Lisäksi tuli raportointivelvoite merkittävistä poikkeamista sekä valvontavelvoitteita. Direktiivillä haluttiin edistää entistä enemmän EU-maiden välistä yhteistyötä ja tiedonvaihtoa kyberuhkien torjumiseksi ja kyberturvallisuuden parantamiseksi. (Direktiivi 2022/2555/EU, 92, 99-100, 105, 111, artiklat 5, 14-17, 21, 23, 32, 33.)

Suomessa Traficom on tehnyt direktiivin toimeenpanoa varten suositusluonnoksen. Se perustuu tulevaan kyberturvallisuuden riskienhallinnasta annettuun lakiin ja julkisen hallinnon tiedonhallinnasta annettuun lakiin (906/2019, nk. tiedonhallintalaki) tehtäviin muutoksiin. Suositusta on tarkoitus käyttää apuvälineenä, ei tyhjentävänä listana. Suositusluonnoksessa kerrotaan toteutusesimerkki kuhunkin vaatimukseen liittyen, se, miten vaatimuksenmukaisuuden voi todentaa, perustelut sekä viitteet eli standardit ja viitekehykset, joihin tämä perustuu. Traficom kirjoittaa suosituksen lopulliseen muotoonsa, kun lait on vahvistettu eduskunnassa. Tämän opinnäytetyön kirjoitusvaiheessa lopullista suositusta ei oltu vielä julkaistu. (Traficom/18410/09.00.02/2023, 4, 10-11.)

Suositusluonnoksen luku 11 Perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi oli tähän opinnäytetyöhön liittyen tärkein. Sen toimenpiteet perustuvat NIS2 -direktiivin 21 artiklan 2 kohdan osittaiseen g alakohtaan. ”Tämän alakohdan kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 11 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 11 kohdassa.” Luku 11 koostuu kolmestatoista perustason tietoturvakäytännöstä, jotka ovat:

1. *Toimija on ohjeistanut perustason tietoturvakäytännöt henkilöstölle, alihankkijoille ja muille kumppaneille.*
2. *Toimija on tunnistanut kriittisimmän omaisuutensa.*
3. *Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä.*
4. *Toimija on erottanut kriittiset ja haavoittuvat viestintäverkot ja tietojärjestelmät muista ympäristöistä.*
5. *Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä haitallisia ja luvattomia ohjelmistoja vastaan.*
6. *Toimija on järjestänyt tunnistautumisen sisäisiin ja ulkoisiin palveluihinsa ja laitteisiinsa turvallisesti.*
7. *Toimija on erottanut järjestelmiensä pääkäyttäjätunnukset ja korotettujen oikeuksien tunnukset muista tunnuksista.*

8. *Toimija on varmistanut, että sen luottamuksellista tietoa käsitellään turvallisesti.*
9. *Toimija on huolehtinut, että sen järjestelmiä päivitetään säännöllisesti ja kriittiset päivitykset asennetaan viivytyksettä.*
10. *Toimija on huolehtinut, että sen palvelut ja laitteet on turvallisesti konfiguroitu.*
11. *Toimija on huolehtinut, että sen kriittiset palvelut ja tieto-omaisuus on varmuuskopioitu.*
12. *Toimija on varautunut, miten sen toiminta voidaan ylläpitää vakavissa poikkeamissa.*
13. *Toimijalla on käytössään kriittisten toimintojen tapahtumakirjaus (loki). (Traficom/18410/09.00.02/2023, 98-114.)*

Toimeksiantaja kuuluu NIS2 -direktiivin piiriin, ja se on varmistanut, että täyttää vaatimukset perustason tietoturvakäytännöille. Toimeenpanon tukimateriaalina toimivat mm. Liikenne- ja viestintävirasto Traficomin suositusluonnos sekä siinä viitatut ISO 27002:n vaatimukset.

3.3.3 Threat Modeling Manifesto ja Threat Modeling Capabilities

Uhkamallinnus on järjestelmän kuvausten analysointia, jonka tarkoituksena on tuoda esiin turvallisuuteen ja yksityisyyteen liittyviä huolenaiheita. Uhkamallinnuksen perusperiaatteet ovat lausuttuna Threat Modeling Manifestossa, jonka on kehittänyt joukko alan asiantuntijoita. Se on tarkoituksella yksinkertaistettu, jotta se olisi helppo omaksua käyttöön. Neljä uhkamallinnuksen pääkysymystä ovat vapaasti suomennettuina:

1. Minkä parissa työskentelemme?
2. Mikä voi mennä vikaan?
3. Mitä aiomme tehdä asialle?
4. Teimmekö riittävän hyvää työtä?

Alussa siis tunnistetaan, minkä parissa työskennellään ja mikä voi mennä vikaan. Uhkamallinnuksen tuloksena syntyy uhkia. Uhat antavat tietoa päätöksenteon tueksi. Threat Modeling Manifeston (2020) periaatteiden mukaan uhkamallinnusta kannattaa tehdä varhaisilla ja usein toistuvilla analyyseillä. Uhkamallinnusta tulee toteuttaa organisaation kehityskäytäntöjen mukaisesti samalla syklillä. Tulokset ovat merkityksellisiä silloin, kun ne tuovat arvoa sidosryhmille. Dialogin kautta luodaan yhteistä ymmärrystä ja tuotetaan arvoa, ja dokumentoinnilla tallennetaan yhteinen ymmärrys sekä saadaan mitattavaa tietoa asioista. (Threat Modeling Manifesto 2020.)

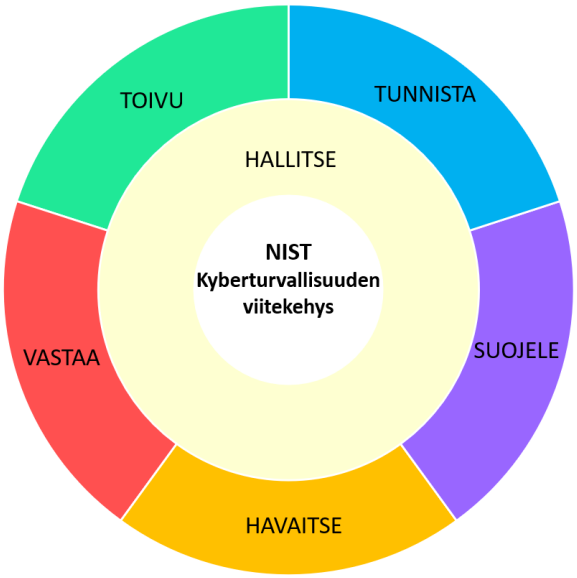
Tärkeimpiä muistettavia asioita prosessissa ovat: Jokainen pystyy tekemään tämän. Ongelman analysointi ei riitä: etsitään käytännöllisiä ja oleellisia ratkaisuja. Älä kadota kokonaiskuvaa, koska osat voivat olla toisistaan riippuvaisia, äläkä keskity liikaa hyökkääjiin, omaisuuksiin tai tekniikoihin. Täydelliseksi hiotun raportin sijaan voi tehdä useita, koska ei ole olemassa yhtä täydellistä näkökulmaa, ja lisäesitykset voivat valaista erilaisia ongelmia. (Threat Modeling Manifesto 2020.) Threat Modeling Manifesto on yksinkertainen ja järkevä, joten sitä on helppo käyttää. Esimerkiksi NCSC (Risk management 2023, 14) käyttää riskienhallinnassaan Threat Modeling Manifeston periaatteita, ja niitä voidaan käyttää myös uhka-riskimallinnuksen itsepalvelumallissa.

Threat Modeling Manifeston jälkeen on julkaistu uhkamallinnuskyvykkyyksiin keskittyvä Threat Modeling Capabilities. Siinä määritellään uhkamallinnuksen kyvykkyyksien luettelo, jonka osia käyttöönottamalla organisaation uhkamallinnusohjelma, konkreettisten uhkamallinnusten tekeminen sekä niiden laatu paranevat. Kyvykkyydet on järjestetty seitsemään prosessialueeseen: strategia, koulutus, uhkamallien luominen, toiminta uhkamallien perusteella, viestintä, mittaus ja ohjelmahallinta. Jokaisella prosessialueella on erilaisia kyvykkyyksiä, jotka toimivat käytännön askeleina kohti parempaa uhkamallinnusohjelmaa. Riskienhallinta liittyy näistä prosessialueista suoraan ainakin toimintaan uhkamallien perusteella sekä mittaukseen. Toiminta uhkamallien perusteella -prosessialueella tiimit käyttävät uhkamallinnusta ymmärtääkseen ja määrittääkseen riskejä asianmukaisesti. Organisaatio voi käyttää riskiprofiilinsa mukauttamisessa uhkamallinnusta tai erillistä riskienhallintaprosessia, johon saadaan tietoja uhkamallinnuksen kautta. Mittauksen prosessialueella organisaatio voi hyötyä uhkamallinnuksista saaden niistä mittareita riskien ymmärtämiseksi, mittaamiseksi ja riskienhallinnan täydentämiseksi. (Threat Modeling Capabilities, 2023.)

3.3.4 NIST CSF kyberturvallisuuden viitekehys

NIST CSF kyberturvallisuuden viitekehys (engl. Cyber Security Framework) auttaa organisaatioita ymmärtämään ja käsittelemään kyberturvallisuusriskejään (uhat, haavoittuvuudet, vaikutukset) ja vähentämään niitä räätälöidyillä toimenpiteillä. Viitekehys hyödyntää olemassa olevia standardeja, ohjeita ja parhaita käytäntöjä, ja se antaa yhteisen kielen kyberriskien hallinnalle. CSF on laajalti hyväksytty alan standardi. (The NIST Cybersecurity Framework (CSF) 2.0 2024, iv; Nair & Greeshma 2023.)

CSF:n toimintoja on tarkoitus käyttää rinnakkain. Kuviossa 5 on esitetty kyberturvallisuuden viitekehyksen toiminnot. Toimenpiteitä, jotka tukevat hallintaa (engl. govern), tunnistamista (engl. identify), suojelemista (engl. protect) ja havaitsemista (engl. detect), tulisi toteuttaa jatkuvasti. Niiden toimenpiteiden, jotka tukevat vastaamista (engl. respond) ja toipumista (engl. recover), tulisi puolestaan olla valmiina jatkuvasti ja aktivoitua, kun kyberturvallisuuspoikkeamia ilmenee. Kaikilla toiminnoilla on keskeinen rooli kyberturvallisuuspoikkeamien hallinnassa. Nämä toiminnot auttavat estämään poikkeamia, valmistautumaan niihin sekä havaitsemaan ja hallitsemaan niitä. CSF:n periaatteet ovat laajemman tason periaatteita kyberuhkiin liittyen, ja niiden hyödyntämistä uhka-riskimallinnuksen itsepalvelumallissa ei suoraan tarvita. Toipumisen ja vastaamisen toiminnot ovat toimeksiantajalla joka tapauksessa uhka-riskimallinnuksesta erillään. (The NIST Cybersecurity Framework (CSF) 2.0 2024, 5.)



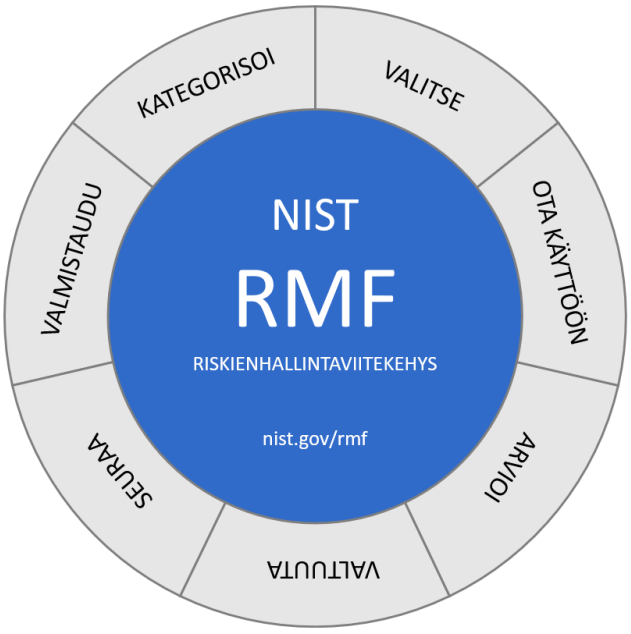
Kuvio 5. NIST CSF kyberturvallisuuden viitekehyksen toiminnot (The NIST Cybersecurity Framework (CSF) 2.0 2024, 5, muokattu)

3.3.5 NIST RMF riskienhallintaviitekehys

NIST RMF riskienhallintaviitekehys (engl. Risk Management Framework) yhdistää turvallisuus- ja riskienhallintakeinot järjestelmäkehityksen elinkaareen. Viitekehys sisältää seitsemänvaiheisen prosessin, jota voi käyttää tietoturva- ja tietosuojariskien hallintaan. Uusimmassa RMF-julkaisussa riskienhallintaviitekehystä on päivitetty yhdenmukaisemmaksi kyberturvallisuuden viitekehyksen

kanssa. Näitä kahta viitekehystä voi siis nyt hyödyntää toisiaan täydentävästi. (Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy 2018, vi.)

RMF:n seitsemän vaihetta ovat valmistautuminen (engl. prepare), kategorisointi (engl. categorize), valitseminen (engl. select), käyttöönotto (engl. implement), arviointi (engl. assess), valtuutus (engl. authorize) ja seuranta (engl. monitor). Nämä on esitetty kuviossa 6. Ensin valmistaudutaan riskienhallintaan. Tämän jälkeen kategorisoidaan eli luokitellaan järjestelmä ja siinä käsitellyt tiedot sekä valitaan NIST SP 800-53:n mukaisia kontrolleja järjestelmän suojaukseen riskiarvioinnin perusteella. Kontrollit toteutetaan ja tämän jälkeen arvioidaan, tuottavatko kontrollit haluttuja tuloksia. Toimivaltainen esihenkilö tekee riskiperusteisen päätöksen järjestelmän käyttöluvan myöntämisestä, minkä jälkeen jatkuvasti seurataan kontrollien käyttöönottoa sekä järjestelmään kohdistuvia riskejä. Kontrollidokumentti on yli 400-sivuinen teos, jonka tuntemista läpikotaisin ei uhka-riskimallinnuksen itsepalvelumallin käyttäjiltä voi odottaa, vaan tietoturvariskien hallintakeinot ja niiden seuranta täytyy tehdä muilla keinoin. (NIST Risk Management Framework RMF n.d.; Security and Privacy Controls for Information Systems and Organizations 2020.)



Kuvio 6. NIST RMF riskienhallintaviitekehys (NIST Risk Management Framework n.d.)

3.3.6 NIST tietokeskeinen uhkamallinnus

NIST on julkaissut tietokeskeisen uhkamallinnusmenetelmän (engl. Data-Centric Threat Modeling). Tietokeskeistä uhkamallinnusta voi käyttää tietoturvariskien hallintaan ja niiden vähentämiseen sekä turvallisuustarpeiden huomioimiseen ja tiedon luottamuksellisuuden, eheyden ja saatavuuden suojaamiseen. Uhkamallinnus suositellaan tehtäväksi sekä kehitysprosessin alussa että myöhemmin toistuvasti. Tietokeskeinen uhkamallinnus mahdollistaa kunkin palvelun erityisten turvallisuustarpeiden huomioimisen pelkkien yleisten parhaiden käytäntöjen sijaan. Yleisesti tietoturva-ammattilaiset, järjestelmänvalvojat ja muut turvallisuudesta vastaavat tahot ovat keskittyneet suojaamaan järjestelmiä. Tiedon suojaaminen on jäänyt vähemmälle, ja haasteena onkin, miten suojataan tietty tietokokonaisuus. (Souppaya & Scarfone 2016, 2, 9-10.)

Tietokeskeinen uhkamallinnus sisältää neljä vaihetta:

1. Tunnista ja kuvaa järjestelmä ja kiinnostava data: Ensimmäisessä vaiheessa on tärkeää tunnistaa, miten tieto liikkuu järjestelmässä auktorisoitujen sijaintien välillä. Tätä tietoa peilataan turvallisuustavoitteisiin (tiedon luottamuksellisuus, eheys ja saatavuus). Vaiheessa tunnistetaan myös henkilöt ja prosessit, jotka pääsevät käsiksi tietoon tavalla, joka voi vaikuttaa turvallisuustavoitteisiin.
2. Tunnista ja valitse uhkavektorit, jotka sisällytetään malliin: Toisessa vaiheessa tunnistetaan potentiaaliset hyökkäysvektorit ts. reitit/menetelmät, joilla hyökkääjä pääsee järjestelmään. Hyökkäysvektori voi vaikuttaa negatiivisesti turvallisuustavoitteisiin eli uhata tiedon luottamuksellisuutta, eheyttä ja/tai saatavuutta tiedon jossain säilytys- tai muokkauskohdassa.
3. Kuvaa turvallisuuskontrollit uhkavektorien lieventämiseksi: Kolmannessa vaiheessa tunnistetaan ja dokumentoidaan turvallisuuskontrollimuutokset (esim. nykyisten kontrollien tiukentaminen tai konfigurointimuutokset), jotka auttavat lieventämään hyökkäysvektoriin liittyvää riskiä ja ovat kohtuudella toteutettavissa. Jokaisen tällaisen muutoksen osalta tehdään vielä arvio sen tehokkuudesta ja mahdollisista negatiivisistakin vaikutuksista (esim. kustannukset, vaikutukset käytettävyyteen tai suorituskykyyn).
4. Analysoi uhkamalli: Neljännessä vaiheessa analysoidaan kaikki aiemmin luetellut asiat, jotka siis muodostavat uhkamallin. Jokaisen turvallisuuskontrollivaihtoehdon tehokkuus ja vaikuttavuus valittuja hyökkäysvektoreita vastaan arvioidaan. Analysointivaiheen haaste tulee siitä, miten nämä kaikki osatekijät yhdistetään. Painotetaanko kustannuksia, käytettävyyttä, toimenpiteen tehokkuutta, ja mitä näistä painotetaan minkäkin hyökkäysvektorin kohdalla. (Souppaya & Scarfone 2016, 11-16.)

Nämä vaiheet vertautuvat Threat Modeling Manifeston (2020) neljän kysymyksen viitekehykseen: mitä olemme tekemässä, mikä voi mennä pieleen, mitä aiomme tehdä asialle sekä teimmekö tar-

peeksi hyvää työtä. Molemmissa lähestymistavoissa on samat vaiheet: järjestelmän ymmärtäminen, uhkien tunnistaminen, kontrollien suunnittelu ja tehokkuuden arviointi. Siinä missä Threat Modeling Manifesto on yleisempi uhkamallinnuksen lähestymistapa, keskittyy tietokeskeinen uhkamallinnus erityisesti tietonäkökulmaan. Tietokeskeisessä uhkamallinnuksessa on uhkavektorien luokittelun ja listaamisen jälkeen kuusikriteerinen pisteytys, jonka jälkeen vielä arvioidaan kontrollien tehokkuutta hyökkäysvektoreittain. Menetelmä on tämän vuoksi liian monimutkainen uhka-riskimallinnuksen itsepalvelumallin käyttöön. (Threat Modeling Manifesto 2020.)

3.3.7 OWASP Threat Dragon ja Microsoftin uhkamallinnustyökalu

Open Worldwide Application Security Project (OWASP) on voittoa tavoittelematon säätiö, joka työskentelee ohjelmistojen tietoturvan parantamiseksi. OWASPilla on muutamia uhkamallinnustyökaluja, joista yksi on OWASP Threat Dragon. Se noudattaa Threat Modeling Manifeston arvoja ja periaatteita ja sitä voidaan käyttää uhkien dokumentointiin ja niiden lieventämisratkaisujen määrittämiseen. Threat Dragon tukee STRIDE, LINDDUN, CIA, DIE ja PLOT4ai -menetelmiä, tarjoaa mallinnuskaavioita ja sisältää sääntömoottorin, joka automaattisesti luo uhkia ja niiden lieventämisratkaisuja. Threat Dragon tarjoaa kiinnostavan ja yksinkertaisen menetelmän uhkien mallintamiseen, mutta koko uhka-riskimallinnuksen tarpeisiin se ei vastaa. (OWASP Threat Dragon 2024.)

Microsoftin uhkamallinnustyökalu (engl. Microsoft Threat Modeling Tool) on ilmainen ja käyttäjäystävällinen. Se on osa Microsoftin turvallisen kehityksen elinkaarta (engl. Microsoft Security Development Lifecycle). Työkalu on suunniteltu niin, että käyttäjä ei tarvitse syvällistä tietoturvaosaamista, joten uhkamallinnuksen tekeminen on helppoa. Työkalu käyttää STRIDEa. Kuten OWASPin Threat Dragonissa, on Microsoftin uhkamallinnustyökalussakin uhkien luomiseen ja analysointiin liittyvää automaatiota. (Microsoft Threat Modeling Tool threats 2022.) Sovelluskehittäjien on työkalun avulla mahdollista tehdä ohjelmistolleen tietoturvasuunnitelma ja jakaa tietoa. Tämä tukee ketterää tietoturvallisen kehittämisen syklin toteutusta. (Jansson 2021, 46.)

3.3.8 Riskienhallinnan viitekehysten ja menetelmien vertailu

Lambrinoudakis, Gritzalis, Xenakis, Katsikas, Karyda, Tsochou, Papadatos, Rantos, Pavlosoglou, Gasparinatos, Pantazis ja Zacharis (2022) ovat kirjoittaneet ENISA:n eli Euroopan unionin kyberturvallisuusviraston raportissa erilaisista riskienhallinnan viitekehyksistä ja menetelmistä sekä niiden

yhteensopivuudesta toistensa kanssa. He ovat esitelleet ja arvioineet kattavasti kolmekymmentä viitekehystä, joiden joukossa ovat tässäkin opinnäytetyössä mainitut ISO 27005, NIST 800-sarjan viitekehykset, COSO-ERM, johon toimeksiantajan riskienhallinta osaltaan perustuu, mutta näiden lisäksi myös monia muita, kuten OCTAVE eri muunnoksineen, ISACA RISK IT FRAMEWORK, IRAM2, ETSI TVRA, MONARC, MEHARI CORAS ja FAIR. Keskeisten kehyksen tai menetelmän ominaisuuksien kautta tehtiin analyysia niiden yhteensopivuudesta. Yhteensopivuuteen vaikuttavat mm. käytetty standardi (ISO, NIST), lähestymistapa (omaisuuseriin perustuva, skenaarioihin perustuva), riskien arvioinnin laatu (määrällinen, laadullinen, puolimäärällinen), käytettävät kirjastot (esim. uhkakirjastot), kieli ja riskin laskentatapa. Jos joku menetelmä käyttää tiettyä uhkakirjastoa, sitä voi olla vaikea sopeuttaa toiseen menetelmään, jossa on eri uhkakirjasto. (Lambrinoudakis ym. 2022, 4, 31.)

Esimerkiksi ISO 27005 ja NIST SP 800-37 ovat molemmat riskienhallintakehyksiä, jotka voidaan organisaation käytössä yhdistää tietoturvariskienhallinnan tehostamiseksi. Niissä molemmissa on samantyyppisiä vaiheita, kuten riskien tunnistaminen, arviointi, käsittely ja seuranta. Lähestymistavat ovat erilaisia, ja kumpikin viittaa eri standardeihin, mutta näitä viitekehyksiä yhdistämällä voisi saavuttaa kattavamman riskienhallinnan tason ja siten parantaa tietoturvaa. MEHARI on yhteensopiva ISO-standardien kanssa, mutta sitä puolestaan ei voisi yhdistää kätevästi meillä Suomessa näihin viitekehyksiin, koska se on saatavilla vain ranskaksi. (Lambrinoudakis ym. 2022, 8-9, 20, 31.)

3.4 Uhkamallinnus- ja riskienhallintamenetelmät

Uhkamallinnus- ja riskienhallintamenetelmät ovat keskeisiä apuvälineitä tietoturvauhkiin varautumisessa. Organisaatio voi niiden avulla ennakoida, tunnistaa ja hallita siihen kohdistuvia tietoturvauhkia ja -riskejä. Eri menetelmät tarjoavat kukin oman, systemaattisen tapansa kartoittaa ja analysoida tietoturvauhkia ja -riskejä. Niillä pyritään tunnistamaan esimerkiksi järjestelmän heikkoja kohtia, jotka voivat olla alttiina hyökkäyksille, tai arvioimaan, kuinka hyökkääjä käyttäisi haavoittuvuutta hyväkseen. Menetelmien avulla organisaatio saa kattavan kuvan tietoturvariskeistään ja voi siten kohdistaa resurssejaan tehokkaammin riskienhallintaan ja tietoturvahyökkäysten estämiseen.

STRIDE

STRIDE-malli luotiin alun perin Microsoftilla sen oman uhkamallinnustyökalun osaksi. STRIDE toimii ikään kuin muistitekniikkana eri turvallisuusuhkatyypeille. Se kattaa kuusi uhkakategoriaa, jotka vaikuttavat laitteen tai sovelluksen turvallisuuteen:

- Identiteetin huijaaminen (engl. Spoofing Identity)
- Datan peukalointi (engl. Tampering with Data)
- Vastuun kiistäminen (engl. Repudiation)
- Tietovuoto (engl. Information Disclosure)
- Palvelunestohyökkäys (engl. Denial of Service, DoS)
- Oikeuksien (käyttövaltuuksien) laajentaminen (engl. Elevation of Privilege). (Microsoft Threat Modeling Tool threats 2022; Kirtley 2023.)

PASTA

PASTA (Process for Attack Simulation and Threat Analysis) on yhdysvaltalaisen VerSprite -yrityksen kehittämä riskikeskeinen uhkamallinnusmenetelmä, joka keskittyy uhkien ja haavoittuvuuksien arvioimiseen ja priorisointiin hyökkäyssimulaatioiden avulla. PASTA on riskikeskeinen lähestymistapa, jossa arvioidaan uhkia suhteessa niiden oletettuun vaikutukseen liiketoiminnalle. PASTAssa on hyökkääjän näkökulma, sillä siinä keskitytään hyökkäyssimulaatioihin. Uhkien arvioinnissa käytetään todennäköisyyskerrointa. Todennäköisyyskerroin perustuu hyökkäyssimulaatioihin, joilla mallinnetaan ja analysoidaan todellisia uhkia ja niiden vaikutuksia. Kerroin antaa mitattavaa tietoa siitä, mihin turvallisuustoimenpiteitä kannattaa kohdistaa. PASTAn luvataan olevan helppo integroitava ohjelmistokehityksen elinkaareen, sekä systemaattisuudessaan vähemmän työläs kuin jotkut muut uhkamallit. (UV 2023; What is Threat Modeling? 2024.)

PASTAn seitsemän vaihetta ovat:

1. Valmistautuminen (engl. preparation): määritellään uhkamallin tavoitteet ja laajuus
2. Sovelluksen palastelu (engl. application decomposition): ymmärretään arkkitehtuuri, komponentit ja tiedon kulku
3. Uhka-analyysi (engl. threat analysis): tunnistetaan mahdolliset uhat eri tekniikoilla
4. Haavoittuvuusanalyysi (engl. vulnerability analysis): tutkitaan järjestelmän heikkouksia, joita voitaisiin hyödyntää
5. Hyökkäysten kartoittaminen (engl. attack enumeration): kartoitetaan mahdolliset hyökkäykset tunnistettujen uhkien ja haavoittuvuuksien perusteella

6. Riski- ja vaikutusanalyysi (engl. risk and impact analysis): arvioidaan jokaisen uhan vaikutus ja todennäköisyys
7. Vastatoimenpideanalyysi (engl. countermeasure analysis): kehitetään strategioita riskin vähentämiseksi tai poistamiseksi. (What is Threat Modeling? 2024.)

DREAD

DREAD on Microsoftin kehittämä apuväline uhkien riskienarviointiin. Sillä pisteytetään riskien suuruutta viiden kategorian avulla:

- Vahinko (engl. damage): kuinka paljon kokonaisvahinkoa tai vaikutusta uhka voi aiheuttaa
- Toistettavuus (engl. reproducibility): kuinka helposti hyökkäys voidaan tehdä uudelleen tai toistaa
- Hyödynnettävyys (engl. exploitability): kuinka todennäköisesti tai helposti heikkoutta tai uhkaa voidaan hyödyntää
- Käyttäjävaikutus (engl. affected users): niiden (loppu)käyttäjien lukumäärä, joihin uhan hyödyntäminen vaikuttaisi
- Havaittavuus (engl. discoverability): kuinka todennäköisesti hyökkääjä löytää uhan tai haavoittuvuuden järjestelmästä sitä hyödyntääkseen. (Kirtley 2023.)

Kaikille osa-alueille annetaan arvosanat, joiden perusteella sitten lasketaan riskin kokonaisvaikutus. Nykyisin DREAD ei ole enää Microsoftin käytössä, koska annettujen arvosanojen katsottiin olevan subjektiivisia arvioijien näkemyksistä riippuen. (Kirtley 2023.)

CVSS

CVSS (engl. Common Vulnerability Scoring System) on maailmanlaajuisesti käytetty ja standardisoitu uhkien pisteytysjärjestelmä, jota käytetään tunnistettuihin haavoittuvuuksiin. Sen on kehittänyt NIST (National Institute of Standards and Technology) ja sitä ylläpitää FIRST (Forum of Incident Response and Security Teams). CVSS:n antamat pisteet ja tiedot auttavat tietoturvaa ylläpitäviä henkilöitä arvioimaan uhkia, tunnistamaan vaikutuksia, priorisoimaan korjauspäivityksiä ja tunnistamaan keinoja suojata omaa järjestelmäänsä. Näin he pystyvät arvioimaan ja priorisoimaan haavoittuvuutta oman hallintaprosessinsa mukaisesti. (Common Vulnerability Scoring System SIG n.d..)

Hyökkäyspuut

Hyökkäyspuut (engl. attack trees) ovat diagrammeja. Niissä kuvataan, millä eri tavoin asiat voivat mennä pieleen (esim. mitä hyökkäyksiä voi tapahtua), ja mistä syistä tämä johtuu. Hyökkäyspuulla on tehokasta tehdä juurisyyanalyysia (engl. root cause analysis, RCA). Siinä käytetään hierarkkista esitystapaa, joka kuvaa vaiheita onnistuneen hyökkäyksen toteuttamiseksi. Jokainen vaihe vaatii, että edellinen on suoritettu. Hyökkäyksen toteuttaminen vaatii, että kaikki vaatimukset puun alimmista osista huipulle asti on täytetty. Hyökkäyspuun kautta huomataan, miten monia hyökkäystapoja on, ja miten paljon ja millaisia vaiheita hyökkäykseen liittyy. Kun hyökkäyspuu on tehty, päästään itse asiaan, eli käännetään asia hyökkäyspuuhun liittyvän kyberturvallisuusriskin arvioinniksi: mistä riski tulee, mitä heikkouksia järjestelmässä on, ja miten riskiä vähennetään? (Risk management 2023, 13.)

Riskienhallintamenetelmät

Erilaisten uhkamallinnusmenetelmien lisäksi on olemassa erilaisia riskienhallintamenetelmiä. Niitä ovat mm. Hazop-analyysi (engl. Hazard and Operability Study, HAZOP), vaarojen arviointi ja kriittiset hallintapisteet (engl. Hazard Analysis and Critical Control Points, HACCP), liiketoimintavaikutusten analysointi (engl. Business Impact Analysis, BIA), juurisyyanalyysi (engl. Root Cause Analysis, RCA), kustannushyötyanalyysi (engl. Cost-Benefit Analysis, CBA), vikapuuanalyysi (engl. Fault Tree Analysis, FTA), todennäköisyyksien päivittämiseen tarkoitettu Bayes, riskin arvonalaisuus (engl. Value at Risk, VAR), ryhmäpäätöksentekomenetelmä Delphi ja graafinen turvallisuusriskien mallinnusmenetelmä CORAS. (Ilmonen ym. 2016, 115.)

3.5 Muut työkalut

Katakri

Katakri on kansallinen turvallisuusauditointikriteeristö, jonka on julkaissut Kansallinen turvallisuusviranomainen, NSA (National Security Authority). Se on viranomaisten käyttöön tarkoitettu arviointityökalu, jolla voidaan arvioida organisaation turvallisuusjärjestelyjen tilaa sekä viranomaisten tietojärjestelmien turvallisuutta. Katakria käytetään, kun halutaan varmistua, että viranomaisen

salassa pidettävät tiedot on suojattu voimassa olevan lainsäädännön ja Suomea sitovien kansainvälisten tietoturvallisuusvelvoitteiden mukaisesti. (Katakri – tietoturvallisuuden auditointityökalu viranomaisille n.d., Katakri 2020 2020, 5.)

PiTuKri

PiTuKri on turvallisuuden arviointikriteeristö, jonka on julkaissut Liikenne- ja viestintävirasto Traficomin alainen Kyberturvallisuuskeskus. Se on viranomaisten käyttöön tarkoitettu arviointityökalu, jonka tavoitteena on edistää viranomaisten salassapidettävän tiedon turvallisuutta tilanteissa, joissa tietoa käsitellään pilvipalveluissa (Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) 2020, 3). PiTuKria käytetään sekä pilvipalveluiden turvallisuuden arvioinnissa, että myös omaehtoisen turvallisuustyön tukena. (Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) 2020, 3-4.)

3.6 Uhkamallinnuksen ja riskimallinnuksen kaupalliset työkalut

Uhkamallinnukseen ja riskimallinnukseen on saatavilla sekä kotimaisia että ulkomaisia kaupallisia valmistyökaluja. Kuten jo aiemmin todettiin, tämän opinnäytetyön rajauksena oli, että uhka-riskimallinnus täytyy tehdä toimeksiantajan nykyisiä työkaluja hyödyntäen. Jos toimeksiantaja haluaa myöhemmin kehittää uhka-riskimallinnusta tuomalla siihen esimerkiksi käyttöliittymän ja riskirekisterin, täytyy tehdä erikseen kattava kartoitus tarjolla olevista tuotteista hyvine ja huonoine puolineen luonnollisesti myös tietoturvanäkökulma huomioiden. Tarjolla on mm. tällaisia työkaluja:

- Arter on suomalainen yritys, joka tarjoaa tuotteita laadun- ja jatkuvuudenhallintaan, kokonaisarkkitehtuuriin sekä prosessien kehittämiseen. ARC-ohjelmisto on kokonaisarkkitehtuurin visualisointityökalu, jolla voi hallita myös tietoturvaa. IMS-ohjelmistolla puolestaan voi hoitaa yrityksen riskienhallinnan. Arterin avulla voi rakentaa tietoturvallisuuden hallintamallin. (Todennetusti toimivia ratkaisuja 2024.)
- Digiturvamalli käyttää pohjana Microsoft Teamsia. Siinä valitaan tärkeimmät vaatimuskehikot, esim. ISO 27001, ja tämän mukaan täytetään, millä tasolla nykyiset toimintamallit ovat. Digiturvamalliin voi liittää dokumentaatiota ja hoitaa sillä tietoturvariskien riskienhallinnan. Riskienhallinnan osalta tietoturvariskien tunnistamista voi osaltaan automatisoida (viitekehyksiin viitaten), saada yhdenmukaisen toimintatavan ohjeineen riskienhallintaan, sekä linkittää riskien käsittelyn ISMS:ään. Digiturvamallista saa myös riskirekisterin. (Kohti parempaa ja sertifioitua digiturvaa n.d..)
- Granitella on tarjolla tietoturvaohjelma, jolla saadaan kyber- ja tietoturvariskit osaksi päätöksentekoa. Granitella voi yhdenmukaistaa riskiohjelman tavoitteet ja tietoturva-

riskit, tunnistaa mm. haavoittuvuudet sekä ylläpitää ajantasaista riskirekisteriä ja raportoida kehityksestä eteenpäin. Myös haluamiaan standardeja, esim. ISO 27001:stä, voi soveltaa. (Riskienhallinta n.d..)

- Hyperproof on tuote, johon riskienhallinnan voi keskittää. Siinä on mukana riskirekisteri. Riskien arvioinnin voi vakioida ja asettaa oman organisaation tarpeiden mukaiseksi. Riskirekisterissä voi yhdistää hallintakeinot riskeihin ja käyttää koontinäyttöjä ja raportteja. Riskitilanteen muutokset voi nähdä siitä jopa reaaliajassa. (Innovative Compliance Operations Platform - Hyperproof 2024.)
- Parapet on palvelu, joka koordinoi yrityksen politiikat, säännöt ja menettelytavat ja ylläpitää turvallisuusriskien hallintaa mm. automaattisilla raporteilla ja valvomalla kriittisiä riskejä reaaliaikaisesti. Riskit voi tunnistaa esim. ISO-standardin kautta, ja hälytykset luvataan sekä ulkoisista että sisäisistä uhista ja riskeistä. (IT Risk Management 2020.)
- Rego Riskienhallintajärjestelmä sisältää riskiarvioinnit ja -analyysit, riskirekisterin, jäännösriskien reaaliaikaisen seurannan, toimenpiderekisterin ja muistutustoimintoja, muokattavan riskiarviointimallin ja muita ominaisuuksia. (Rego Riskienhallinta 2024).

3.7 Riskienhallinta, riskien arviointi, riskien käsittely ja jatkuva parantaminen

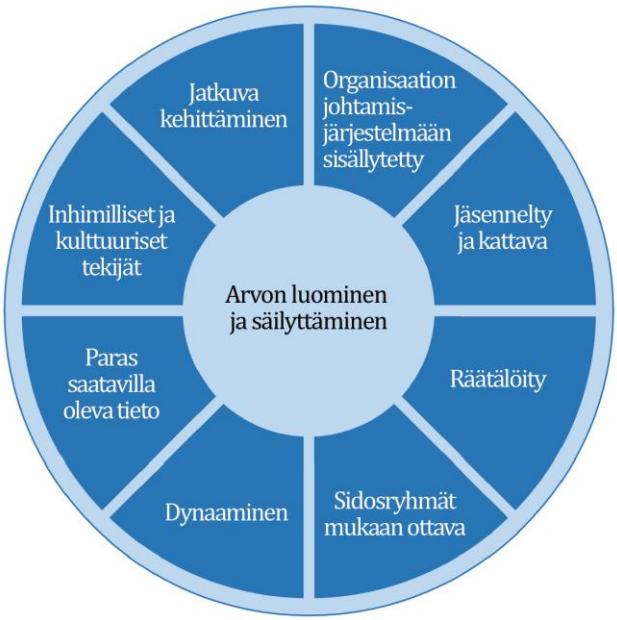
3.7.1 Riskienhallinta

Riskienhallinta ei vain suojaa organisaatiota riskeiltä, vaan se myös parantaa organisaation kykyä luoda ja säilyttää arvoa. Riskienhallinnan avulla suorituskyky paranee ja sillä voidaan tukea sekä innovointia että tavoitteiden saavuttamista. Tietoturvariskien hallinta, kuten muutkaan riskienhallinnan alueet, ei ole tarkkaa tiedettä. Se perustuu organisaatioiden strategisesta suunnittelusta, valvonnasta, hallinnasta ja päivittäisestä toiminnasta vastuussa olevien henkilöiden ja ryhmien asiantuntija-arvioihin. Riskienhallinnan tavoitteena on kehittää riittäviä ja asianmukaisia toimenpiteitä, jotka varmistavat organisaation toimintojen suojaamisen. (ISO 31000:2018, 7; Managing Information Security Risk - Organization, Mission, and Information System View 2011, 1.)

Jotta riskienhallintaan sitoudutaan pitkäaikaisesti, on johdon määriteltävä selkeä riskienhallintapolitiikka ja riskienhallinnan tavoitteet. Joka organisaatiotasolle integroitu riskienhallinta mahdollistaa sen, että resurssit keskitetään riskeihin, jotka vaikuttavat organisaation tavoitteiden saavuttamiseen. Riskienhallinnan avulla suojataan omaisuutta, varmistetaan toiminnan jatkuvuus sekä tehdään parempia päätöksiä. Riskienhallintaa on arvioitava säännöllisesti ja sitä pitää kehittää. (Nair & Greeshma 2023.)

ISO 31000:2018 Riskienhallinta

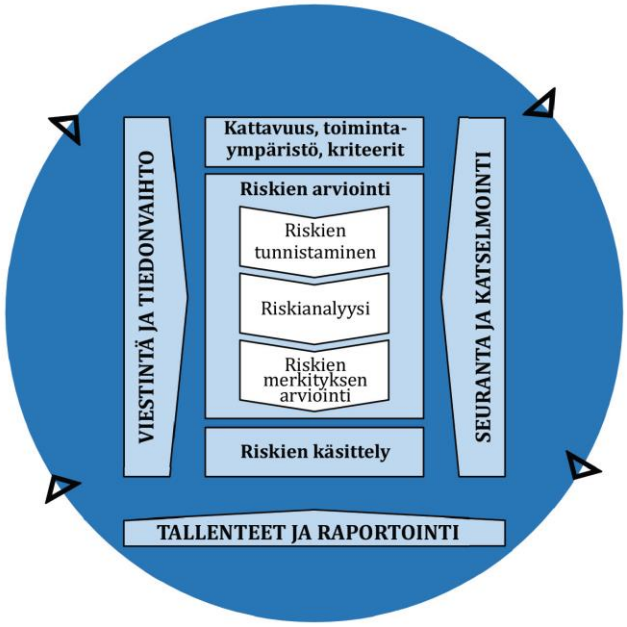
ISO-standardi 31000 määrittelee riskienhallinnan ohjeet. Se kattaa kaikki organisaation riskityypit (taloudelliset, toiminnalliset, strategiset yms.) eikä sen käyttö ole toimialariippuvaista. Onnistuneeseen riskienhallintaan tarvitaan standardin mukaan kuvion 7 mukaisia tekijöitä. Riskienhallinnalle tarvitaan puitteet - riskienhallinnan sisällyttäminen organisaation johtamisjärjestelmään ja sen suunnittelu, toteuttaminen, arviointi ja kehittäminen koko organisaatiossa. Riskienhallinnan keskiössä on arvon luominen ja säilyttäminen. Jotta riskienhallinta toimii ja voi onnistua, sen on oltava organisaation johtamisjärjestelmään sisällytetty, jäsennelty ja kattava ja räätälöity. Sidosryhmät on huomioitava. Dynaaminen tarkoittaa reagointia muutoksiin oikea-aikaisesti. Riskienhallinnan tulee perustua parhaaseen saatavilla olevaan tietoon ja sen on huomioitava inhimilliset ja kulttuurilliset tekijät. Riskienhallintaa on kehitettävä jatkuvasti. (ISO 31000:2018, 8-9.)



Kuvio 7. Riskienhallinnan periaatteet (ISO 31000:2018, 8)

Riskienhallinnan prosessi on esitelty kuviossa 8. Riskienhallintastrategialla määritellään mukaisesti kattavuus, toimintaympäristö ja kriteerit. Riskit arvioidaan menettelyllä, johon kuuluvat riskien tunnistaminen, riskianalyysi ja riskin merkityksen arviointi. Tämän jälkeen riskit käsitellään. Seurannalla ja katselmoinnilla tavoitellaan laadun ja tulosten varmistamista sekä niiden parantamista.

Riskienhallintaprosessi sekä sen tulokset dokumentoidaan ja raportoidaan. Viestintä ja tiedonvaihto auttavat lisäämään sidosryhmien tietoa ja ymmärrystä riskeistä sekä saamaan sidosryhmiltä päätöksentekoa tukevaa palautetta ja tietoa. (ISO 31000:2018, 14-20.)



Kuvio 8. Riskienhallintaprosessi (ISO 31000:2018, 14)

NIST Riskienhallinnan ohje ja ISACA Risk IT process framework

NISTin riskienhallinnan ohje NIST SP 800-39 sisältää ohjeita riskienhallinnan strategiseen suunnitteluun ja operatiiviseen toimintaan. Ohje on tarkoitettu Yhdysvaltojen liittovaltion hallinnon käyttöön, mutta sitä käytetään ympäri maailman. Se on yhdenmukaistettu ISO-standardien 31000, 31010, 27001 ja 27005 kanssa. Ohjeessa käydään läpi riskienhallinnan rakenne (integrointi johtamis- ja päätöksentekoprosesseihin), riskien arviointi sekä riskienhallinnan käyttöönotto ja seuranta. Sen painopiste on kyberturvallisuusriskeissä ja tietojen suojaamisessa. (Managing Information Security Risk - Organization, Mission, and Information System View 2011, 4.)

ISACA:n kehittämä Risk IT on viitekehys IT-riskien hallintaan ja ohjaukseen. Keskeiset periaatteet viitekehyksessä ovat yhteys liiketoiminnan tavoitteisiin, yhteensovittaminen koko yrityksen riskienhallinnan kanssa, kustannusten ja hyötyjen tasapaino, avoin viestintä, johtamisen tuki sekä jatkuvuus. Viitekehys jakautuu kolmeen osaan: riskien hallinnointi (engl. risk governance), riskien arviointi (engl. risk evaluation) ja riskin käsittely (engl. risk response). ISACA Risk IT keskittyy

tietotekniikan ja tietojärjestelmien riskienhallintaan sekä näihin liittyviin liiketoimintariskeihin. Se painottaa eniten liiketoiminnan tavoitteiden huomioimista ja kustannusten ja hyötyjen tasapainoa. (ITIL® Continual Service Improvement 2011, 192-193.)

Yhteenveto riskienhallinnan standardeista ja viitekehyksistä

Sekä NIST SP 800-39 eli NISTin riskienhallinnan ohje, ISO 31000 -standardi Riskienhallinta, että ISACA Risk IT -viitekehys tarjoavat kehikon riskienhallintaprosessille. Kaikki kolme standardia/viitekehystä korostavat jatkuvan, jäsennellyn ja systemaattisen riskienhallintaprosessin merkitystä. Riskien tunnistaminen, arviointi, hallinta ja seuranta ovat keskeisiä elementtejä näissä kaikissa. Riskienhallintaa pidetään strategisena prosessina, joka vaatii johdon sitoutumista. Se tulee sitoa organisaation tavoitteisiin ja päätöksentekoon. Riskienhallintaprosessia tulee parantaa jatkuvasti, eikä riskienhallinta koskaan ole kertaluontoinen prosessi. Riskienhallinta luo perustan riskien arvioinnille ja analysoinnille varmistaen, että riskit arvioidaan oikealla tavalla suhteessa organisaation tavoitteisiin ja sietokykyyn. Toimeksiantajalla riskienhallinta perustuu ISO 31000 -standardiin, joka on näistä laajin ja yleisin. Riskienhallinnan toimintamallit ovat toimeksiantajalla valmiiksi olemassa, joten uhka-riskimallinnuksen itsepalvelumallissa toimitaan näiden toimintamallien sisällä.

3.7.2 Riskien arviointi

Riskien arviointi on kokonaisprosessi, joka kattaa riskien tunnistamisen, riskianalyysin ja riskien merkityksen arvioinnin (ISO/IEC 27005:2022:fi, 9). Tietoturvariskien arviointiprosessi tehdään kuten muidenkin riskien arviointiprosessi: se koostuu riskien tunnistamisesta, riskianalyysista ja riskien merkityksen arvioimisesta (ISO/IEC 27005:2022:fi, 21, vrt. kuvio 8). Riskien arvioinnin alkuvaiheessa määritellään riskien hyväksymiskriteerit (SFS-EN ISO/IEC 27001:2023, 10). Riskin hyväksyminen tarkoittaa tietoista päätöstä ottaa tietty riski (ISO/IEC 27005:2022:fi, 11). Riskien hyväksymiskriteerit määrittävät, millä ehdoilla ja tasolla organisaatio on valmis hyväksymään tietyn riskin ilman lisätoimenpiteitä. Hyväksymiskriteerit liittyvät läheisesti organisaation riskinsietokykyyn ja -haluun, eli siihen, kuinka suuria riskejä se on valmis ottamaan suhteessa tavoitteisiinsa, resursseihinsa ja toimintaympäristöönsä. Jos riski kasvaa hyväksyttävän rajan yli, tarvitaan toimenpiteitä. (Guide for Conducting Risk Assessments 2012, 2.)

NIST SP 800-30 riskien arviointiopas ”Guide for Conducting Risk Assessments” ohjeistaa, kuinka riskien arviointi suoritetaan. Ohjeistus on osa NISTin laajempaa kehystä, joka on suunnattu erityisesti tietoturva- ja riskienhallintaprosessien kehittämiseen ja ylläpitoon, eli se siis voidaan integroida NIST RMF:n kanssa. Oppaassa kerrotaan, kuinka valmistautua riskien arviointiin, miten riskien arviointi suoritetaan, miten tuloksista viestitään, sekä miten riskien arviointia ylläpidetään. Oppaassa myös muistutetaan, että riskienarvioinnit eivät ole tarkkoja mittausvälineitä vaan ne heijastelevat esimerkiksi käytettyjä menetelmiä ja työkaluja, niiden perusteena toimivan tiedon laatua ja luotettavuutta, arviointitulosten tulkintaa sekä arviointia suorittavien henkilöiden taitoja ja asiantuntemusta. (Guide for Conducting Risk Assessments 2012, ix, 2, 5, 20.)

Riskien arviointi voi olla määrällistä, laadullista tai puolimäärällistä (Guide for Conducting Risk Assessments 2012, 14). Uhka-riskimallinnuksen itsepalvelumallissa riskejä arvioidaan toimeksiantajan riskien arviointimatriisin perusteella. Siinä on neljä arvoa vaikutukselle ja neljä todennäköisyydelle. Arvoille on myös sanalliset kuvailut sekä lisätulkintaohjeita, mutta niitä ei tietoturvasyistä avata tässä opinnäytetyössä. Sanallisilla kuvauksilla varmistetaan arviointien yhdenmukaisuutta. Toimeksiantajan riskien arviointi on puolimäärällinen. Arvioinnissa käytetään sekä numeerista pisteytystä (1–4) että sanallista kuvausta, mutta pisteytys ei perustu tarkkoihin laskelmiin tai mittaustietoihin, vaan se antaa viitteellisen arvion. Riskin suuruus lasketaan todennäköisyys x vaikutus.

Riskien tunnistaminen

Riskien tunnistamisprosessissa löydetään, havaitaan ja kuvataan riskit. Tunnistamisen kannalta olennaista on, että saatavilla on olennaista, asianmukaista ja ajantasaista tietoa. Sama määrittely koskee tietoturvariskejä ISO 27005 -standardissa. (SFS-ISO 31000:2018, 16; ISO/IEC 27005:2022:fi, 21.) Riskin tunnistamiseen liittyy monenlaisia vaikuttavia tekijöitä sekä tapahtumien ja niiden seurausten sekä uhkien tunnistamista. Tunnistamisen voi aloittaa esimerkiksi uhkakartoituksella. Riskien ja uhkien tunnistaminen on vasta alkua, sitten alkaa varsinainen työ, vaikkakin tunnistamisvaiheen kattavuus ja onnistuminen ovatkin koko riskienhallintaprosessin kriittisimpiä kohtia. (Ilmonen ym. 2016, 109.)

Riskianalyysi

Riskianalyysilla tavoitellaan ymmärrystä riskin luonteesta, ominaisuuksista sekä riskitasosta. Yhdellä tapahtumalla voi olla useita syitä ja seurauksia, minkä lisäksi se voi vaikuttaa useisiin tavoitteisiin. Kaikki ei siis aina ole yksiselitteistä ja selkeää, kun riskejä analysoidaan. Riskianalyysissa on huomioitava mm. tapahtumien ja seurausten todennäköisyys, seurausten luonne ja suuruus, monimutkaisuus, liittymäpinnat ja nykyisten hallintakeinojen vaikuttavuus. Riskianalyysilla tuotetaan syvempää ymmärrystä päätöksentekoa varten. (SFS-ISO 31000:2018, 17; ISO/IEC 27005:2022:fi, 21.)

Riskien analysointia voi tehdä uhkakeskeisesti (engl. threat-oriented approach), omaisuus/vaikutuskeskeisesti (engl. asset/impact -oriented approach) tai haavoittuvuuskeskeisesti (engl. vulnerability-oriented approach). Jokainen analyysimenetelmä huomioi samat riskitekijät ja sisältää saman joukon arviointitoimintoja, mutta eri järjestyksessä. Tarkastelutapa voi vaikuttaa tuloksiin, ja jotkin riskit voivat jäädä huomaamatta. Siksi riskien tunnistaminen useammasta näkökulmasta (esim. yhdistämällä uhkakeskeinen lähestymistapa omaisuus/vaikutuskeskeiseen lähestymistapaan) voi parantaa analyysin tarkkuutta ja tehokkuutta. Uhka-riskimallinnuksen itsepalvelumallissa on yhdistetty elementtejä näistä kaikista. Kysymysluettelossa on tunnistettu aihealueita, joiden kautta uhkia voi muodostua (esim. inhimilliset virheet). Omaisuuskeskeinen lähestymistapa on käytössä, koska ennen varsinaisen uhka-riskimallinnuksen aloittamista tehdään omaisuuksien kartoitus ja sen myötä saadaan lisää ymmärrystä omaisuuden vaarantumisen merkityksestä. Kysymysluettelossa on tunnistettu palvelujen ja prosessien heikkoja kohtia, jotta haavoittuvuudetkin saadaan mukaan. Elementtejä yhdistämällä pyritään saamaan analysoinnista tarkempaa, kattavampaa ja tehokkaampaa. (Guide for Conducting Risk Assessments 2012, 15.)

Riskien merkityksen arviointi

Riskien merkityksen arviointi tukee päätöksentekoa. Siinä määritetään riskianalyysin tuloksia riskikriteereihin vertaamalla, ovatko riski tai sen merkittävyys hyväksyttävissä olevia vai tarvitaanko lisätoimenpiteitä. Päätöksissä on huomioitava toimintaympäristö sekä todelliset ja havaitut seuraukset ulkoisille ja sisäisille sidosryhmille. (SFS-ISO 31000:2018, 18; ISO/IEC 27005:2022:fi, 21.)

3.7.3 Riskien käsittely

Kun riskit on löydetty, analysoitu ja arvioitu, on tärkein vielä jäljellä: niiden käsittely. Se voi tarkoittaa mm. seuraavia vaihtoehtoja:

- riskin vähentäminen: tehdään toimenpiteitä, että riski ei toteudu niin usein tai sen seuraukset eivät ole niin vakavia
- riskin hyväksyminen: päätetään tietoisesti hyväksyä riski
- riskin torjuminen: ei tehdä riskin aiheuttavaa toimintaa tai lopetetaan se
- riskin ottaminen tai lisääminen: halutaan ottaa riski, jotta voidaan hyödyntää joku mahdollisuus
- riskin lähteen poistaminen: esimerkiksi poistetaan joku ohjelma käytöstä kokonaan
- riskin jakaminen tai siirtäminen: esimerkiksi sopimuksella kumppanin kanssa tai vakuutuksella. (SFS-ISO 31000:2018, 18.)

Riskien käsittelyprosessissa mietitään ja valitaan riskin käsittelyvaihtoehdot. Tämän jälkeen suunnitellaan ja toteutetaan toimenpiteet, arvioidaan vaikuttavuus sekä se, onko jäljelle jäänyt riski hyväksyttävällä tasolla. Kaikkia riskejä on käytännössä mahdotonta poistaa, vaikka tehtäisiin mitä toimenpiteitä. Mikäli jäännösriski on edelleen liian suuri, pitää riskiä käsitellä edelleen. ISO 27005 -standardissa tietoturvariskien hallintakeinot noudattavat samaa linjaa ISO 31000 -standardin kanssa ja täsmentävät ISO 27001 -standardissa kerrottuja asioita. Sopivat hallintakeinot valitaan tunnistettujen riskien vähentämiseksi tai hallitsemiseksi. Tietoturvariskien osalta tulee huomioida eri vaihtoehdot, mm. tietoturvakontrollien käyttöönotto tai joidenkin riskien hyväksyminen tietoisen päätöksen perusteella. (SFS-ISO 31000:2018, 18; Calder 2023; Nair & Greeshma 2023.)

Seuranta on avainasemassa riskienhallinnan prosessin ja riskien arvioinnin prosessin lisäksi myös riskien käsittelyprosessissa. Seurannalla varmistetaan, että riskien käsittely on vaikuttavaa, tehokasta ja kustannustehokasta. Prosessilla täytyy saada tietoa, jolla parannetaan tulevia riskien arviointeja. On pystyttävä analysoimaan häiriöitä, muutoksia, onnistumisia ja epäonnistumisia sekä oppimaan niistä, ja havaittava toimintaympäristön muutoksia, jotka voivat muuttaa joko riskejä, riskikriteerejä tai riskien priorisointia. Lisäksi on tunnistettava uusia riskejä. (ISO/IEC 27005:2022:fi, 42.) Seurannalla pyritään jatkuvaan parantamiseen, jotta riskien arviointiprosessi pysyy dynaamisena ja tehokkaana, mahdollistaa tarvittavien muutosten tekemisen ja tukee organisaation kykyä hallita riskejä tehokkaasti. (Calder 2023.)

3.7.4 Jatkuva parantaminen

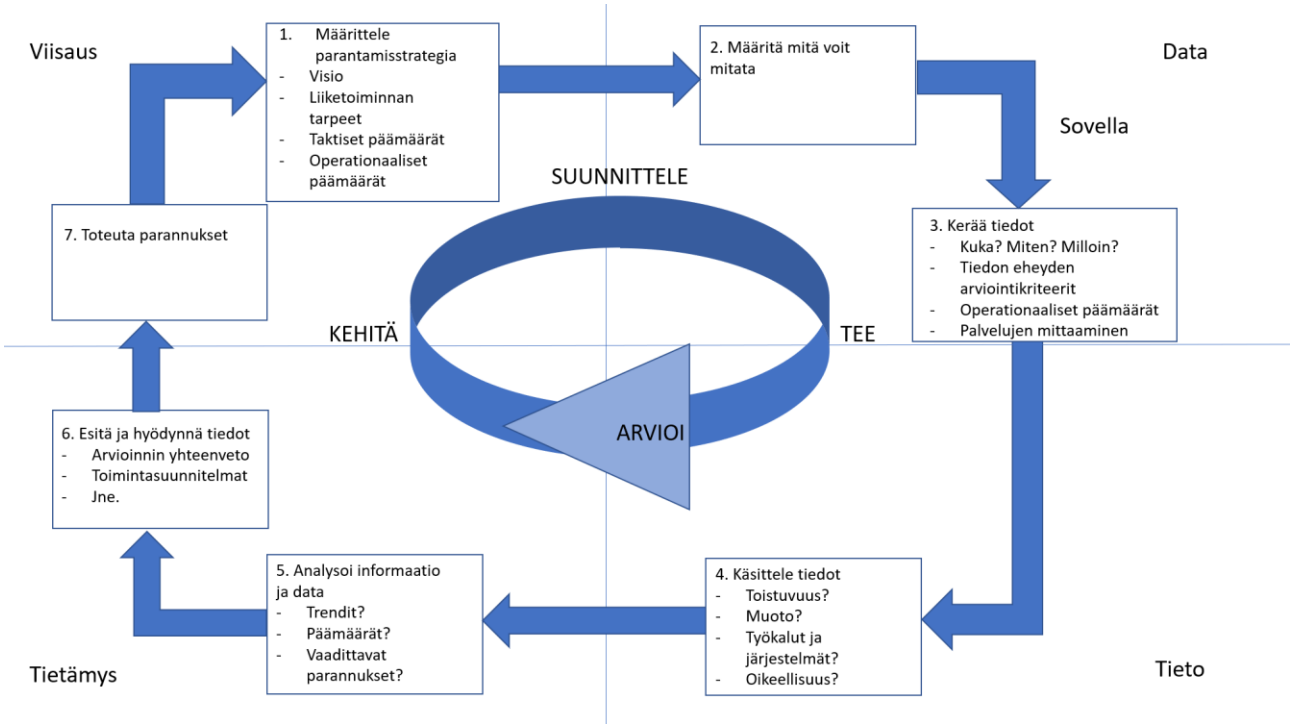
PDCA (engl. Plan, Do, Check, Act) -malli on jatkuvan parantamisen menetelmä, jota sen yksinkertaisuuden ja helpon lähestymistavan vuoksi pidetään edelleen yhtenä parhaista jatkuvan parantamisen menetelmistä. Ensin muutos suunnitellaan (engl. Plan), tämän jälkeen muutos tehdään (engl. Do). Tekemisen jälkeen arvioidaan (engl. Check) muutosta ja sen tehokkuutta, ja kehitetään toimintaa (engl. Act) saadun tiedon perusteella. Tämän jälkeen jälleen suunnitellaan muutos (engl. Plan) ja kehän kiertäminen jatkuu. (Calder 2023.)

ISO 31000 -standardissa ei suoraan todeta, että se noudattaa PDCA-mallia, mutta Periaatteet -luvussa on viittaus jatkuvaan kehittämiseen, ja riskienhallinnan puitteet on esitetty PDCA:n kaltaisena ympyrämallina, jossa ovat suunnittelu, tekeminen, arviointi ja kehittäminen sekä näiden lisäksi organisaation johtamisjärjestelmään sisällyttäminen. Asioita ei siis vain seurata, vaan niistä opitaan, ja opitut asiat otetaan osaksi toimintaa. PDCA-mallilla riskien käsittely ei ole yksittäisten teknisten päätösten tekemistä siiloissa, vaan se kannustaa jatkuvaan liiketoiminnan parantamiseen ja tukee jatkuvaa suunnittelu- ja kehitysprosessia. (SFS-ISO 31000:2018, 4, 8-9; Field 2023.)

ISO 27001:ssä ei ole ollut PDCA-malliin viittausta vuoden 2005 jälkeen. PDCA-malli on yksi monista jatkuvan parantamisen menetelmistä, eikä standardi edellytä sen käyttöä – ainoastaan, että organisaatio parantaa jatkuvasti tietoturvallisuuden hallintajärjestelmäänsä. (Calder 2023.) Jos kuitenkin haluaa ajatella ISO 27001:stä PDCA-mallin kautta, voisi ajatella lukujen 4-7 olevan suunnitteluvaihe. Silloin tunnistetaan mahdollisuus ja suunnitellaan muutos. Luku 8 Toiminta vastaa tekemisvaihetta. Luku 9 Suorituskyvyn arviointi vastaa arviointivaihetta, jossa arvioidaan ja analysoidaan tuloksia sekä tunnistetaan, mitä on opittu. Luku 10 Parantaminen vastaa toiminnan kehittämisvaihetta, jossa toimitaan sen mukaan, mitä arviointivaiheessa opittiin. (Nair & Greeshma 2023.)

PDCA-malli ei ole ainut jatkuvan parantamisen malli. Yksi PDCA:n haastavista menetelmistä on seitsemän vaiheen parantamisprosessi (engl. seven-step improvement process). Molemmat ovat osa jatkuvaa palvelun parantamista (engl. Continual Service Improvement, CSI). Sykli integroidaan tiedonhallinnan DIKW-rakenteeseen (engl. Data-to-Information-to-Knowledge-to-Wisdom, data – tieto – tietämys – viisaus). PDCA-syklin ja seitsemän vaiheen parantamisprosessin integrointi etenee kuvion 9 mukaan seuraavasti: Suunnittele -vaiheessa vaihe 1) määrittele parantamisstrategia

ja 2) määritä mitä voit mitata, Tee -vaiheessa 3) kerää tiedot ja 4) käsittele tiedot, Arvioi -vaiheessa 5) analysoi informaatio ja data ja 6) esitä ja hyödynnä tiedot, sekä Kehitä -vaiheessa 7) toteuta parannukset. Seitsemän vaiheen parantamisprosessin tavoitteet ovat liiketoimintatavoitteita tukevia ja parantamisella pyritään mittauskelpoisuuteen, kustannusten säästöön, palvelun laadun säilymiseen sekä jatkuvaan arviointiin ja toiminnan mukauttamiseen. Prosessi kattaa palvelujen, prosessien, kumppanien ja teknologian arvioinnin koko niiden elinkaaren ajan. Prosessissa varmistetaan liiketoimintatavoitteiden saavuttaminen seuraamalla ja analysoimalla palvelujen toimittamista. Se mahdollistaa jatkuvan arvioinnin ja parantaa asiakaspalvelua liiketoimintatarpeiden mukaan. (ITIL® Continual Service Improvement 2011, 47-48.)



Kuvio 9. Seitsemän vaiheen parantamisprosessi (ITIL® Continual Service Improvement 2011, 40, muokattu)

4 Uhka-riskimallinnuksen itsepalvelumallin rakentaminen

Tässä luvussa käsitellään uhka-riskimallinnuksen itsepalvelumallin rakentamisen keskeisiä vaiheita ja sen sisältöä. Aluksi tarkastellaan aiemmin käytettyä mallia ja siihen liittyen havaittuja kehitystarpeita. Tämän jälkeen esitellään itsepalvelumalliin sisällytetyt keskeiset periaatteet, jotka ohjaavat

mallin toimintaa. Luvun lopussa kuvataan itsepalvelumallin sisältöä, sen käytännön toteutusvaiheita sekä viimeistelty prosessi, joka mahdollistaa uhka-riskimallinnuksen tehokkaamman ja käyttäjäystävällisemmän hallinnan.

4.1 Uhka-riskimallinnuksen aiempi toteutustapa

Toimeksiantajan uhka-riskimallinnus toimi aiemmin tietoturva-asiantuntijavetoisesti. Kun palvelua oltiin rakentamassa, kuului suunnitteluvaiheeseen uhka-riskimallinnuksen tekeminen. Uhka-riskimallinnuksesta tehtiin tilaus, ja tietoturvayksikkö käsitteli tilauksen. Asiakkaaseen eli palveluun otettiin yhteyttä ja sovittiin kolmesta erillisestä uhka-riskimallinnustyöpajasta. Työpajoissa olivat mukana palvelun tuoteomistaja ja tiimin jäsenet sekä tietoturva-asiantuntija tai kaksi. Ensimmäinen työpaja liittyi uhkien tunnistamiseen ja uhkien luokitteluun. Toisessa työpajassa arvioitiin uhkien todennäköisyys ja vaikutus eli se, minkä tasoisen riskin uhka muodostaa. Kolmannessa työpajassa käsiteltiin riskit, eli päätettiin riskien omistajat, riskienhallintakeinot, toteutusaikataulut ja valvontavastuut. Tämän vaiheen lopputuloksena saatiin kokonaisnäkemys riskeistä, niiden tasosta, käsittelytoimenpiteistä, vastuista ja aikataulusta. Sisältö perustui pitkälti nykyisellään jo vanhentuneeseen VAHTI-ohjeeseen vuodelta 2017 (Rousku 2017). Materiaaleihin oli linkitetty ISO 27005 -standardi, STRIDE, OWASP, DREAD ja Microsoft SDL Threat Modeling, joita pystyi halutessaan käyttämään apuvälineenä. Excel-dokumentti oli kuvion 10 mukaisesti nk. tyhjä, eli siinä oli annettu esimerkki mutta ei muuta ohjausta. Aluksi tunnistettiin uhat ja sen jälkeen riskit ja niiden merkitys. Kuvio 10 esitetyn osan lisäksi Excel-dokumentissa oli otsikot ja tarkemmat sarakkeet riskien käsittelylle, seurannalle ja arvioinnille.

Uhkien tunnistaminen						Riskien tunnistaminen			Riskin merkityksen arviointi			
Riskin tunniste	Riskiluokka		Uhka (kuvaava nimi)	Syyt ja tekijät uhkan taustalla - miksi uhka voi toteutua?	Seurauksia uhkan toteutumisesta - mitä voi tapahtua?	Todennäköisyys		Vaikutus	Riskin suuruus (T x V)		Toimenpidetarpeet riskin käsittelylle (vakavuus/sietokyky	
	3	Luonnonvoimat	Koronavirustartunta.	Laivassa paljon ihmisiä (viruksen mahdollisia kantajia), hyvät bufeet (tartuntalähde), hupelissa huono käsihygienia.	Tartunnalla voi olla vakavia seurauksia erityisesti riskiryhmäläisille.		Ei arvioitu		Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu
		Täytä arvo 1-6					Ei arvioitu		Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu
		Täytä arvo 1-6					Ei arvioitu		Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu
		Täytä arvo 1-6					Ei arvioitu		Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu

Kuvio 10. Osa toimeksiantajan aiemmasta uhka-riskimallinnuksen Excel-dokumentista

Työpajojen jälkeen tietoturvayksikkö kokosi tästä isosta Excel-dokumentista aineiston ja tuotti tarvittavan raportoinnin. Asiakas eli palvelu sai valmiin raportin ja tallensi sen haluamaansa paikkaan, esimerkiksi Confluencen tai intranetin työtilaan tai verkkolevylle. Uhka-riskimallinnus oli kertaluontoinen, eikä tietoturvauhkien ja -riskien käsittelyä tämän jälkeen seurattu. Tietoturvayksikkö toimi sparraajana, ja tietoturvauhkien ja -riskien käsittely jäi palvelun vastuulle.

4.2 Uhka-riskimallinnuksen kehittäminen kohti itsepalvelumallia

Aiemman uhka-riskimallinnuksen kehittämistä tarvittiin, koska havaittiin, ettei se nykytilanteessa toiminut parhaalla mahdollisella tavalla. Tietoturva-asiantuntijoiden resurssit olivat uhka-riskimallinnusten työpajoihin riittämättömät ja jonot muodostuivat pitkiksi. Asiakas eli palvelu ei saanut uhka-riskimallinnusta välttämättä juuri silloin, kun olisi tarvinnut, koska tietoturva-asiantuntijoiden kalenterit olivat täynnä. Uhka-riskimallinnukseen haluttiin itsepalvelumalli niin, että se on käytössä 24/7 ilman erillistä tilausta aina, kun asiakas tarvitsee. Pitkällä aikavälillä ajateltiin, että suurin osa kaikista uhka-riskimallinnuksista tultaisiin tekemään itsepalveluna. Vain tietyissä erityisissä tilanteissa uhka-riskimallinnus tultaisiin tekemään osin tai täysin yhteistyössä tietoturvayksikön kanssa. Tietoturva-asiantuntijoiden työpanosta piti myös saada kohdistettua toimeksiantajalle kaikista kriittisimpiin asioihin.

Aiemman uhka-riskimallinnuksen yksi puute oli, että se oli useimmiten kertaluontoinen. Siitä ei myöskään jäänyt tulokseksi kuin täytetty Excel-dokumentti, jonka aiheuttamista mahdollisista jatkotoimenpiteistä tai myöhemmistä uusista tietoturvariskien arvioinneista ei ollut tietoa. Riskejä ei viety toimeksiantajan linjauksesta huolimatta aina Jiraan eikä seurantaa tehty. Koska tietoturvauhat ja -riskit eivät ole olemassa vain palvelun suunnitteluvaiheessa, haluttiin, että uhka-riskimallinnuksen itsepalvelumallista tehtäisiin sellainen, että sen voisi tehdä toistuvasti. Nähtiin, että palvelut voisivat hyödyntää uhka-riskimallinnuksen itsepalvelumallia säännöllisesti. Kun uhka-riskimallinnus toteutettaisiin näkyvästi eli esimerkiksi tunnisteen avulla, voisi itsepalvelumallien käyttöä seurata hakemalla niitä työtiloista. Yhdenmukaisella riskien Tietoturva-merkinnällä saataisiin valtakunnallista näkyvyyttä riskien lukumäärään, aiheisiin jne. Haluttiin, että uhka-riskimallinnuksen toteuttamisia olisi helpompi seurata ja mittaroida.

Tuoteomistajille ja tiimeille ei tietoturva-asiantuntijavetoisista työpajoista välttämättä kertynyt paljoa osaamista, ja osin ajateltiin myös, että tietoturva-asiantuntija tulee ja kertoo uhat ja riskit.

Uhka-riskimallinnuksen kehittämisessä haluttiin, että palvelut ottavat enemmän vastuuta omasta tietoturvastaan ja sen kehittämisestä. Haluttiin, että uhka-riskimallinnuksia toistuvasti tekemällä palvelut ensinnäkin kiinnittävät huomiota tietoturvauhkiin ja -riskeihin, ja toisaalta oppivat ottamaan niitä huomioon aina, kun palvelua kehitetään ja koko elinkaaren ajan. Lisäksi palvelujen omaa osaamista tietoturvauhista ja riskeistä haluttiin kasvattaa. Tietoturva-ajattelun haluttiin lisääntyvän ja palvelun tietoturvallisuuden kasvavan. Uhka-riskimallinnuksen itsepalvelumallin kehittäminen nähtiin niin tärkeäksi, että se oli osa toimeksiantajan riskienhallinnan kehittämistä kehitysportfolio 2024:n mukaisesti (portfolio epic Uhka-riskimallinnuksen itsepalvelun mahdollistaminen).

Tässä opinnäytetyössä perehdyttiin systemaattisen kirjallisuuskatsauksen avulla teorioihin, tutkimuksiin ja standardeihin, tietoturvan viitekehyksiin sekä riski- ja uhkamallinnusmenetelmiin ja työkaluihin. Toimeksiantajalta tuli mallille joitain vaatimuksia. Taustahaastattelut toivat arvokasta kehittämiseen tarvittavaa tietoa, ja toimeksiantajan sisäiset materiaalit puolestaan tukea ja taustoitusta. Näiden kaikkien kokonaisuudesta alkoi muodostua hahmotelma siitä, mitä elementtejä uhka-riskimallinnuksen itsepalvelumallissa tulisi olla, jotta se olisi hyvä käyttää ja täyttäisi sille asetetut tavoitteet ja vaatimukset. Tietoturvayksikön johtoryhmälle pidettiin itsepalvelumallin kehittämisen etenemisestä säännöllisiä katsauksia, joissa keskusteltiin malliin kytköksissä olevista prosesseista ja menettelyistä, sovittiin etenemissuunnasta ja lisättiin vaatimuksiin NIS2:n sisällyttäminen malliin. Näissä katsauksissa saatiin ylläpidettyä avointa ja hedelmällistä vuoropuhelua, mikä varmasti paransi uhka-riskimallinnuksen itsepalvelumallin laatua ja toimivuutta.

4.3 Uhka-riskimallinnuksen itsepalvelumallin periaatteelliset lähtökohdat

Uhka-riskimallinnuksen itsepalvelumallin lähtökohdiksi tulivat suoraan esimerkiksi toimeksiantajan turvallisuuden strategiset linjaukset ja riskienhallinnan perusperiaatteet. Näiden lisäksi lähtökohdiksi valittiin useita tietoturvaan ja riskienhallintaan liittyviä viitekehyksiä ja malleja. Näitä yhdisteltiin tietoturvauhkien ja -riskienhallinnan tehostamiseksi. Viitekehykset ja mallit valittiin huolellisesti siten, että ne sopivat toimeksiantajan asemaan, vastasivat toimeksiantajan tarpeita ja tukivat uhka-riskimallinnuksen itsepalvelumallin tarkoitusta, ollen samalla keskenään yhteensopivia. Nämä harkitut ja perustellut periaatteelliset lähtökohdat sisällytettiin malliin, joka suunniteltiin käyttäjäystävälliseksi ja helposti omaksuttavaksi. Itsepalvelumallin käyttö ei siten edellyttänyt syvällistä ymmärrystä lähtökohdiksi valituista viitekehyksistä tai malleista.

Threat Modeling Manifesto

Threat Modeling Manifesto (2020) sopi hyvin uhka-riskimallinnuksen itsepalvelumallin taustalle, koska se on yksinkertainen, lyhyt ja helposti ymmärrettävä. Sen periaatteisiin kuuluvat mm. toistuvuus, lisäarvon tuottaminen ja dokumentaatio. Threat Modeling Manifeston neljä avainkysymystä tulivat huomioiduiksi vaivattomasti.

1. Minkä parissa työskentelemme? Uhka-riskimallinnuksen itsepalvelumallissa tämä tuli esiin aloitusvaiheessa, jossa tehdään omaisuuksien arviointi. Siinä nimenomaisesti haluttiin kartoittaa, mitä osia palvelussa on, mihin se on kytkeytynyt, ja mihin suuntaan ja mitä tietoa liikkuu.
2. Mikä voi mennä vikaan? Uhka-riskimallinnuksen itsepalvelumallin kysymyksillä ohjattiin käyttäjiä arvioimaan, missä kohtaa omaisuuksien välillä liikkuvan tiedon suhteen voisi olla tietoturvauhkia tai -riskejä. Tarkoituksena oli tunnistaa tilanteita, joissa joku voi mennä vikaan.
3. Mitä aiomme tehdä asialle? Kun uhka-riskimallinnuksen itsepalvelumallissa oli tunnistettu tietoturvariski, se kuului tämän jälkeen analysoida, arvioida ja tehdä sille lieventämis- tai vähentämistoimenpiteitä.
4. Teemmekö riittävän hyvää työtä? Uhka-riskimallinnuksen itsepalvelumallin toimintatavassa siirryttiin kertaluontoisesta prosessista jatkuvaan toimintaan. Riskeille määriteltiin omistajat ja käsittelylle asetettiin määräajat, mikä mahdollisti riskien hallintakeinojen etenemisen arvioinnin. Kun lisäksi uhka-riskimallinnusta päivitettiin säännöllisesti, pystyttiin arvioimaan, olivatko toimenpiteet olleet riittäviä vai vaatiko asia lisätoimia. Tämä mahdollisti jatkuvan arvioinnin ja parantamisen. (Threat Modeling Manifesto 2020.)

ISO 31000 -standardi ja ISO 27000 -standardiperhe

Uhka-riskimallinnuksen itsepalvelumallin lähtökohtana olivat ISO-standardit eli ISO 31000 ja ISO 27000, ISO 27001, ISO 27002 ja ISO 27005. ISO 31000 on riskienhallinnan periaatteisiin ja toteuttamiseen liittyvä standardi, joka toimeksiantajan riskienhallinnan pohjana, joten se luonnollisesti otettiin myös uhka-riskimallinnuksen pohjaksi. Uhka-riskimallinnuksen itsepalvelumalli sisällytettiin standardin vaikuttavan riskienhallinnan periaatteiden mukaisesti organisaation johtamisjärjestelmään, se oli jäsennelty ja kattava sekä räätälöity palveluita varten. Siinä pyrittiin myös siihen, että käytetään parasta saatavilla olevaa tietoa ja palvelun tekijöiden ja omistajien osaamista. Itsepalvelumallissa huomioitiin riskien liittyminen muihin palveluihin sekä sidosryhmäyhteistyö mm. tietoturvayksikön kanssa. Toistettavuudella pyrittiin dynaamisuuteen eli siihen, että uhka-riskimallinnusten avulla muutoksiin voitiin reagoida jatkuvasti ja oikea-aikaisesti. Uhka-riskimallinnuksen

kehittämisessä ja käyttäjien tukemisessa huomioitiin inhimilliset ja kulttuurilliset tekijät sekä sitouduttiin parantamaan mallia jatkuvasti (ks. tarkemmin Kuvio 7). Riskin tunnistamisen, analysoinnin ja arvioinnin vaiheet noudattivat ISO 31000:n sisältöä.

ISO 27000 -standardista otettiin itsepalvelumallin pohjaksi tietoturvaan liittyviä termejä sekä tietoturvallisuuden hallintajärjestelmän asioita siltä osin kuin ne liittyivät tietoturvariskien arviointiin. Uhka-riskimallinnuksen itsepalvelumalli oli tarkoitettu tehtäväksi kuten ISO 27001 -standardin kohdassa 8.2 todetaan: ”suunnitelluin aikavälein tai kun merkittäviä muutoksia ehdotetaan tai kun tällaisia muutoksia tapahtuu (SFS-EN ISO/IEC 27001:2023, 14)”. ISO 27001 -standardin A-liitteen 93 hallintakeinoa (SFS-EN ISO/IEC 27001:2023, 17-24) käytiin läpi yksityiskohtaisesti, ja niistä jokaisen kohdalla tehtiin harkinta, sisällytetäänkö hallintakeino uhka-riskimallinnuksen itsepalvelumallin kysymyksiin. Hallintakeinojen sisällyttämisellä haluttiin lisätä toimeksiantajan ISO 27001 -standardinmukaisuutta. Hallintakeinoista 34 kappaletta voitiin sisällyttää kysymyksiin. Loput hallintakeinoista olivat sellaisia, joihin toimeksiantajalla oli erillinen ohjeistus tai joihin uhka-riskimallinnuksen itsepalvelumallin käyttäjä ei voinut vaikuttaa. Uhka-riskimallinnuksen itsepalvelumalli tehtiin ensivaiheessa palvelujen käyttöön. Tällainen palvelusta vastaava itsepalvelumallin käyttäjä ei ole suoraan vastuullinen esimerkiksi siitä, miten sähkökaapelointi on missäkin toimistossa suoritettu, minkä vuoksi hallintakeinoa 7.12 Kaapeloinnin turvallisuus (SFS-EN ISO/IEC 27001:2023, 21) ei otettu mukaan kysymyksiin. Periaatteena oli, että mallista saadaan ymmärrettävä ja helppokäyttöinen, eikä käyttäjä turhaudu sellaisiin kysymyksiin, joille hän ei voi tehdä mitään. ISO 27001 -standardin dokumentoinnin vaatimukseen (SFS-EN ISO/IEC 27001:2023, 11-14) vastattiin sillä, että jokainen uhka-riskimallinnus tuli säilyttää palvelun työtilassa päivämäärällä erotettuna. Näin pystyttiin tarvittaessa palaamaan aiemmin tehtyyn uhka-riskimallinnukseen ja voitiin todeta, mitä asioita ja toimenpiteitä missäkin vaiheessa on tehty.

ISO 27002 -standardi, joka täydensi ISO 27001 A-liitteen hallintakeinoja, käytiin läpi kursorisesti, mutta sen tarkempi soveltaminen jätettiin uhka-riskimallinnuksen jatkokehitykseen. Hallintakeinojen tarkennukset suhteessa A-liitteen hallintakeinoluetteloon läpikäymällä varmistuttiin kuitenkin siitä, että uhka-riskimallinnuksen itsepalvelumallin kysymykset eivät ole ristiriidassa myöskään ISO 27002:n kanssa. ISO 27005 -standardista uhka-riskimallinnuksen itsepalvelumallin pohjaksi otettiin tietoturvariskienhallintaan liittyviä termejä, sekä katsottiin, että itsepalvelumalli noudattaa tietoturvariskien arviointiprosessia.

NIS2

NIS2 -direktiivin perustason tietoturvakäytännöt sisällytettiin uhka-riskimallinnuksen itsepalvelumalliin siltä osin, kuin ne olivat käyttäjille perusteltuja. Traficomin suositusluonnoksen 13 perustason tietoturvakäytännöstä 12 oli sellaisia, joiden elementtejä itsepalvelumalliin pystyttiin sisällyttämään. Esimerkiksi viestintäverkkojen erottelu tapahtuu palvelun ulkopuolella, eikä itsepalvelumallin käyttäjillä ole siihen vaikutusvaltaa. Tästä syystä kyseinen aihe jätettiin kysymysten ulkopuolelle. (Traficom/18410/09.00.02/2023, 98-114.)

STRIDE

STRIDEssä on nostettu esiin erilaisia käytännön näkökulmia tietoturvauhkiin, joten se sisällytettiin uhka-riskimallinnuksen itsepalvelumalliin. STRIDEn osa-alueiden avulla itsepalvelumallissa tunnistettiin mahdollisia hyökkäysvektoreita. Tämä kirjoitettiin käyttäjille tavanomaisten kysymysten muotoon, esimerkiksi: ”Missä palvelun osissa hyökkääjä voisi saada korkeammat käyttöoikeudet, mikä antaisi hänelle pääsyn arkaluontoisiin tietoihin tai järjestelmän hallintaan?” Tällaisten kysymysten perusteella käyttäjät miettivät, onko heillä tietoturvariskiä tähän liittyen. Uhka-riskimallinnuksen taustamateriaaleihin tehtiin lyhyt yhteenveto siitä, mitä STRIDE pitää sisällään. Kysymyksissä huomioitiin jokainen STRIDEn osa-alue ja näiden kysymysten yhteyteen lisättiin linkki STRIDE-yhteenvetoon.

Katakri

Uhka-riskimallinnuksen itsepalvelumalli noudatti soveltuvin osin Katakrin (Katakri - Tietoturvallisuuden auditointityökalu viranomaisille n.d., 11) vaatimusta T-03 Tietoturvallisuusriskien hallinta. Vaatimuksena oli, että ”organisaatio on arvioinut olennaiset turvallisuusluokiteltuihin tietoihin kohdistuvat riskit ja mitoittanut tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti”. Ensin itsepalvelumallin omaisuuksien arvioinnissa tunnistettiin palvelun käsittelemät tiedot ja niiden suojausluokat (vrt. Katakrin turvallisuusluokittelu) sekä tietojen kulkusuunnat omaisuuksien välillä. Tämän jälkeen tehtiin varsinainen uhka-riskimallinnus. Katakrin mukaisesti tietoturvallisuusriskien hallinta on ”järjestelmällistä, koordinoitua ja jatkuvaa toimintaa, jonka avulla tunnistetaan, analysoidaan, arvioidaan, käsitellään ja seurataan tietoturvallisuusriskejä”. Tätä kaikkea uhka-riskimallinnuksen itsepalvelumallilla tehtiin. Tietoturvallisuusriskien hallinta uhka-riskimallinnuksen avulla oli osa organisaation toimintaa ja se yhdistettiin muihin riskienhallinnan prosesseihin. Tavoitteena

oli varmistaa, että silloin kun kyse oli palvelussa käsiteltävistä turvallisuusluokitelluista tiedoista, tehtiin niiden suojaamiseksi riittäviä toimenpiteitä. (Katakri - Tietoturvallisuuden auditointityökalu viranomaisille n.d., 11.)

NIST SP 800-30

Uhka-riskimallinnuksen itsepalvelumallissa hyödynnettiin riskien arvioinnissa sekä uhkakeskeistä, omaisuuskeskeistä että haavoittuvuuskeskeistä näkökulmaa (Guide for Conducting Risk Assessments 2012, 15). Itsepalvelumallissa tehtiin ennen aloittamista omaisuuksien arviointi, jossa saatiin ymmärrystä omaisuuksien arvosta sekä siitä, mitä seurauksia ko. omaisuuksien vaarantumisesta olisi. Kysymysluettelossa oli sekä uhkakeskeisiä että haavoittuvuuskeskeisiä aiheita. Eri uhkia läpikäymällä arvioitiin tietoturvauhkia, joita nämä uhat aiheuttavat. Eri haavoittuvuuksia läpikäymällä arvioitiin tietoturvauhkia, joille nämä haavoittuvuudet palvelun altistavat. Kun näitä eri lähestymistapoja yhdisteltiin, voitiin tunnistaa ulkoiset ja sisäiset uhat, organisaation arvokkaimmat omaisuudet sekä haavoittuvimmat alueet. Tämä auttoi priorisoimaan riskejä. Riski, että jotain merkittäviä riskejä jäisi huomioimatta, pieneni, kun näkökulmien kattavuus oli parempi. Riskienhallinnasta tuli tehokkaampaa ja paremmin kohdennettua, kun tietoa saatiin eri näkökulmista.

Riskimatriisi

Uhka-riskimallinnuksen itsepalvelumallissa riskien suuruuden laskennassa käytettiin kuvion 11 mukaista riskipisteytystä. Riskin suuruus laskettiin yksinkertaisesti todennäköisyys x vaikutus. Itsepalvelumalliin ei haluttu monimutkaista laskukaavaa, jotta se ei veisi huomiota pääasialta. Todennäköisyyden arvot olivat asteikolla lähes varma (4), todennäköinen (3), mahdollinen (2) ja epätodennäköinen (1). Vaikutuksen arvot olivat kriittinen (4), merkittävä (3), kohtalainen (2) ja vähäinen/ei vaikuta (1).

Todennäköisyyden arvot	
4	Lähes varma
3	Todennäköinen
2	Mahdollinen
1	Epätodennäköinen

Vaikutuksen arvot	
4	Kriittinen
3	Merkittävä
2	Kohtalainen
1	Vähäinen / ei vaikuta

Kuvio 11. Toimeksiantajan riskimatriisi

Toimeksiantaja on määritellyt kullekin tietoturvariskin todennäköisyyden ja vaikutuksen arvolle tarkemman sisällön, jota ei kuitenkaan voida tässä opinnäytetyössä tietoturvasyistä tarkemmin avata. Tarkemmassa sisällössä on avattu erilaisia parametreja, joiden avulla arviointia tehdään. Tämä toimi riskien arvioinnin yhdenmukaistajana.

4.4 Uhka-riskimallinnuksen itsepalvelumallin sisältö

Uhka-riskimallinnuksen itsepalvelumallin rakentamisessa tunnistettiin tarve sekä varsinaisen itsepalvelumallin luomiselle että tukimateriaaleille kuten termipankille ja koulutusmateriaaleille. Uhka-riskimallinnuksen käyttäjät eivät olleet tietoturva-asiantuntijoita, joten aiemmin tietoturva-asiantuntijan heille hahmottamat tietoturvariskin, uhan yms. käsitteet tuli tuoda helposti käyttäjän omaksuttaviksi. Myöskään riskienhallintaprosessi osa-alueineen ei välttämättä ollut käyttäjille tuttu, joten itsepalvelumalliin tehtiin selkeä rakenne, jota seuraamalla prosessin läpivienti onnistui itsenäisesti.

Itsepalvelumalliin kuului omaisuuksien tunnistaminen, johon sisältyi kytkösten tunnistaminen muihin palveluihin. Tätä kautta pystyttiin kohdentamaan käyttäjien fokusta oman palvelun ja sen liittymäpintojen tietoturvauhkiin ja -riskeihin. Itsepalvelumallia käyttäessä tuli myös tietää, tarvitseeko palvelun ottaa yhteyttä tietoturvayksikköön uhka-riskimallinnuksen tekemisestä vai ei. Tätä varten tehtiin etenemispolut. Itsepalvelumallin käyttämistä varten tarvittiin lisäksi ohjeistusta ja koulutusmateriaalit, sekä työkalujen eli Confluencen ja Jiran käytön ohjeet. Lisäksi julkaistiin termipankki ja UKK (usein kysytyt kysymykset) sekä itsepalvelumallin käyttöesimerkki. Uhka-riskimallinnuksen itsepalvelumallin haluttiin olevan käyttäjälle helposti lähestyttävä ja kiinnostava, jotta käyttäjä ryhtyisi tekemään sitä mielellään uudelleenkin.

Käyttäjätestaus

Uhka-riskimallinnuksen itsepalvelumallin melko hiottua toteutusta testattiin käyttäjillä 27.8.-16.9.2024. Toimeksiantaja kartoitti halukkaita testaajia, joille käyttäjätestaus sopi annetussa aikataulussa. Käyttäjille annettiin lyhyt ohjeistus Confluencessa uhka-riskimallinnuksen itsepalvelumallin käytöstä ja pyyntö antaa kommentteja ja kehittämisehdotuksia vapaamuotoisesti. Itsepalvelumallia tarkasteli kahdeksan palvelua. Taulukossa 3 on esitetty, miten palvelut käyttivät itsepalvelumalliluonnosta käyttäjätestausaikana tai sen jälkeen.

Taulukko 3. Itsepalvelumallin käytön jakauma käyttäjätestauksessa

Uhka-riskimallinnuksen itsepalvelumallin käyttö käyttäjätestauksessa	Lukumäärä
Käytetty (varsinaisen käyttäjätestausajan jälkeen)	1
Otetaan käyttöön myöhemmin käyttäjätestausajan jälkeen	5
Tarvitsee enemmän tukea alkuvaiheessa	1
Katsoo ettei malli sovellu omaan tarkoitukseen	1
Yhteensä	**8**

Saatujen kommenttien mukaan kokonaisuus vaikutti lupaavalta ja siltä, että se madaltaa kynnystä aloittaa tietoturvariskien arviointia. Valmiiden kysymysten lista vaikutti kattavalta. Kehittämisehdotuksia tuli mm. työmääräarvion antamiseen sekä sen selkeyttämiseen, mistä saa apua matalalla kynnyksellä. Yksi palvelu ehti konkreettisesti käyttää itsepalvelumallia ennen opinnäytetyön valmistumista, vaikkakin varsinaisen käyttäjätestausajan jälkeen. Palvelu piti mallia monipuolisena ja kattavana sekä isona parannuksena aiempaan Exceliin nähden. Jatkokehitysehdotuksena ehdotettiin interaktiivisuuden rakentamista, eli jos vastaa tiettyyn kysymykseen tietyllä tavalla, se avaisi lisäkysymyksiä tai sulkisi niitä annetun vastauksen mukaisesti. Viisi palvelua ei pystynyt toteuttamaan itsepalvelumallia annetussa ajassa, vaan ne tekevät sen myöhemmin tänä vuonna. Yksi palvelu totesi, ettei malli sovellu heille. Toinen palvelu puolestaan katsoi, että he tarvitsevat alkuvaiheessa enemmän tietoturva-asiantuntijan tukea uhka-riskimallinnukseen.

Käyttäjätestauksen testaajien etsimisen ja heidän ohjeistamisensa toteutti konkreettisesti toimeksiantaja, joten opinnäytetyön kirjoittajalla ei ollut siihen enempää vaikutusmahdollisuuksia. Käyttäjätestaus jäi harmillisen puutteelliseksi, vaikka saadut kommentit olivatkin tärkeitä ja hyödynnettävissä nyt tai tulevaisuudessa. Yksi käyttäjätestauksen ulkopuolella ollut taho kysyi toimeksiantajan kautta mallin perehdytystä jo etukäteisesti. Tämä annettiin, ja he kokivat itsepalvelumallin jo luonnoksenakin niin hyödylliseksi, että ottivat sen käyttöön.

Asiantuntijoiden kommenttikierros

Käyttäjätestauksen jälkeen järjestettiin vielä tietoturva- ja riskienhallinnan asiantuntijoiden kommenttikierros 14.10.-2.11.2024. Viisi asiantuntijaa toimitti kommentteja ja kehittämisehdotuksia,

joiden jakaantuminen aiheittain on esitetty taulukossa 4. Kommentit ja kehittämisehdotukset olivat hyödyllisiä sisällön kattavuuden ja osin käyttäjänkin näkökulmasta.

Taulukko 4. Asiantuntijoiden kommentit

Kommentin aihe	Kommentteja (kpl)
Ehdotus, joka voidaan toteuttaa	**6**
Ehdotus, joka voidaan toteuttaa osittain	**1**
Ehdotus, jota ei toteuteta	**2**
Tulevaisuuden jatkokehittämisehdotus	**2**
Tekniset muutokset johtuen 15.10.2024 riskimatriisin muutoksista	**5**
Linkkivinkit käyttäjälle	**4**
Yleinen kehuva palaute	**2**
Yhteensä	**22**

Itsepalvelumallin käyttäjät ja vastuuhenkilö

Uhka-riskimallinnuksen käyttäjiä olivat ensivaiheessa palvelut. Perusajatuksena oli, että uhka-riskimallinnuksen tekoon osallistuisivat palvelun tuoteomistaja, tiimi sekä arkkitehti ja mahdollisesti palvelupäällikkö. Tuoteomistaja tekisi mallin käyttöön liittyvät esivalmistelut, selvittäisi etenemispolun ja huolehtisi uhka-riskimallinnuksen läpiviemisestä. Arkkitehti ja tiimiläiset puolestaan ovat tuoteomistajan lisäksi palvelun parhaita asiantuntijoita, ja kaikkien panosta uhka-riskimallinnukseen tarvittiin. Vastuu uhka-riskimallinnuksesta olisi tuoteomistajalla koko palvelun elinkaaren ajan. Itsepalvelumalli sopi osittain muillekin käyttäjille, esimerkiksi organisaation ulkopuolelta hankittavien palvelujen omistajille. Itsepalvelumallin kysymykset olivat pääsääntöisesti käyttökelpoisia heillekin, mutta mallista puuttuivat kysymykset, jotka liittyvät nimenomaisesti hankittavien palvelujen tietoturvauhkiin ja -riskeihin.

Itsepalvelumallin prosessi

Uhka-riskimallinnuksen itsepalvelumallin tekeminen aloitettiin ensimmäisellä kerralla tutustumalla Confluencesta itsepalvelumallin taustamateriaaleihin, termipankkiin sekä usein kysyttyihin kysymyksiin. Materiaalien avulla käyttäjälle syntyi kokonaisnäkemys, mitä hän on tekemässä, miten ja miksi. Aluksi käyttäjä perehtyi uhka-riskimallinnuksen toimintatavan muutokseen ja uuden toimintatavan perusteisiin. Materiaaleissa esitettiin keskeiset käsitteet kuten tietoturva, CIA-triadi, uhka,

riski ja haavoittuvuus. Tämän jälkeen käytiin läpi etenemispolut ja prosessit. Omaisuuksien arviointi, riskien tunnistaminen sekä riskien analysointi ja arviointi käytiin läpi yksityiskohtaisesti. Käyttäjälle tarjottiin Jiran ja Confluencen ohjeistusta itsepalvelumallin käyttöön liittyen. Keskeiset käsitteet löytyivät termipankista. Usein kysytyt kysymykset tehtiin, jotta mieleen nouseviin kysymyksiin löytyisi helposti vastauksia. Esimerkkitapauksesta pystyi katsomaan, miten tiedot merkitään itsepalvelumalliin ja Jiraan.

Käyttäjän (tai heidän edustajansa) tuli tarkistaa, mikä etenemispolku sopii heille. Uhka-riskimallinnuksen itsepalvelumallia pystyivät toki täyttämään kaikki palvelut, mutta itsepalvelumallin tekemisen jälkeinen käsittely jakautui kolmeen etenemispolkuun. Etenemispolkujen luokittelun teki toimeksiantaja. Polut erosivat toisistaan sen osalta, miten tietoturvayksikkö oli mukana uhka-riskimallinnuksessa. Suurin osa kuului etenemispolulle, jossa palvelu pystyi tekemään täysin itsenäisesti uhka-riskimallinnuksen itsepalvelumallin kautta. Tietoturvayksikköä ei tarvittu tällä etenemispolulla lainkaan mukaan.

Kun taustatiedot oli hankittu tai ne olivat muuten hallussa, siirryttiin omaisuuksien arviointiin. Tässä muodostettiin kokonaiskuva siitä, mitä omaisuuksia palvelulla on, ja mitä tietoa ja mihin suuntaan omaisuuksien välillä liikkuu, sekä missä ovat sen rajapinnat muihin palveluihin. Huomioitavana olivat muun muassa systeemin arkkitehtuuri, tietojen kulkeminen paikasta toiseen ja riippuvuudet. Omaisuuksien arvioinnissa ei listattu kaikkia omaisuuksia (esim. ihmiset, laitteet jne.), koska se olisi tehnyt omaisuuksien arvioinnista liian korostetun. Näitä omaisuuksia käsiteltiin itsepalvelumallin kysymyksissä eli ne kuitenkin huomioitiin. Omaisuuksien arvioinnilla saatiin fokusoitua käyttäjien keskittymistä oman palvelunsa tietoturvauhkiin ja -riskeihin. Aihe olisi mennyt liian laajaksi, jos käyttäjät olisivat lähteneet ajattelemaan koko organisaation kaikkia tietoturvauhkia ja -riskejä. Ohjeistuksessa kuitenkin huomioitiin, että käyttäjät saattavat tunnistaa rajapinnalta toisen palvelun tietoturvauhkia tai -riskejä. Omaisuuksien arviointi muodosti perustan tehokkaalle ja oikein suunnatulle uhka-riskimallinnukselle.

Kun fokus oli kunnossa, siirryttiin varsinaiseen asiaan eli uhka-riskimallinnukseen. Käyttäjät olivat kopioineet Confluenceen mallipohjat omaan työtilaansa ja heidät ohjeistettiin ottamaan käyttöön Jiran riskirekisteri. Uhka-riskimallinnuksen koostesivulle täytettiin palvelun sekä uhka-riskimallin-

nuksen perustietoja, tiedon suojausluokka sekä palvelun liiketoimintakriittisyys. Uhka-riskimallinnus oli muotoiltu aiheittain pohdittaviksi kysymysluetteloiksi. Kysymykset oli jaoteltu neljään aihealueeseen:

1. Organisaatioon liittyvät (sis. myös operatiiviset)
   - Organisaatioon liittyvät tietoturvauhat ja -riskit
   - Operatiiviset tietoturvauhat ja -riskit
2. Ihmisiin liittyvät
3. Fyysiset
4. Teknologiaan liittyvät
   - Pääsy tietoihin
   - Pääsy dokumentaatioon
   - Pääsy lähdekoodiin
   - Ylläpito-oikeudet
   - Todentaminen
   - Kapasiteetinhallinta
   - Teknisten haavoittuvuuksien hallinta
   - Konfiguraationhallinta
   - Tietojen poistaminen
   - Ympäristöt
   - Testaus
   - Lokit
   - Muut teknologiaan liittyvät asiat.

Aihealuejaottelu mukaili ISO 27001 A-liitteen tietoturvallisuuden hallintakeinojen jakoa organisaatioon liittyviin, henkilöstöön liittyviin, fyysisiin ja teknologisiin hallintakeinoihin (SFS-EN ISO/IEC 27001:2023, 17-24). Ihmisiin liittyvissä tietoturvariskeissä otettiin huomioon henkilöstön lisäksi ulkopuoliset ihmiset. Aihealueiden alla oli yksi tai useampia aiheita (esimerkiksi pääsy lähdekoodiin), sekä aina kohta omille lisäyksille.

Confluence-pohjissa oli käyttäjille tukena kuvat CIA-triadista sekä uhan, riskin ja haavoittuvuuden suhteesta (ks. kuviot 2 ja 3). Näillä haluttiin parantaa käyttäjien fokuksen säilymistä nimenomaan tietoturvaan liittyvissä uhissa ja riskeissä. Tämän opinnäytetyön kuvista poiketen kuvat sovitettiin toimeksiantajan värimaailmaan. Kuvat näkyivät usealla sivulla sekä materiaaleissa että itse uhka-riskimallinnuksessa, jotta niihin oli helppo palata ainakin alkuvaiheessa, kun termit tai asiat eivät vielä olleet kaikilla käyttäjillä täysin omaksuttuja.

Itsepalvelumallissa esitettiin kysymyksiä, jotka johdattelivat käyttäjiä pohtimaan kuhunkin aiheeseen liittyviä oman palvelun tietoturvauhkia ja -riskejä. Kysymyksissä kiinnitettiin huomiota uhkien

ja haavoittuvuuksien tunnistamiseen sekä riskien monipuoliseen pohdintaan. Kuviossa 12 on ensimmäinen osa yhdestä aihealueen kysymyksestä, pääsystä lähdekoodiin. Ajatuksena oli, että aihetta ei tarvitse miettiä pelkän otsikon perusteella, vaan Pohdittavaa -sarakkeessa annettiin apukysymyksiä pohdinnalle. Käyttäjille tarjottiin linkit ISO 27001 -standardin A-liitteen hallintakeinoon, NIS2 -direktiivin Traficomin suositukseen perustason tietoturvakäytännöistä, STRIDEen ja toimeksiantajan tarvittaviin materiaaleihin, jos ne liittyivät kysymyksessä olevaan aiheeseen. Direktiivejä ja standardin hallintakeinoja ei ollut välttämätöntä lukea, vaan käyttö sujui hyvin ilmankin. Toimeksiantajan materiaalilinkit veivät esimerkiksi arkkitehtuurilinjauksiin tai muihin aineistoihin, joista pystyi tarkistamaan, onko näitä noudatettu. Vastaus-sarakkeessa muistutettiin uhan, haavoittuvuuden ja riskin tunnistamisesta. Aiheiden alla oli aina myös kohtia, joihin pystyi lisäämään uusia aiheita, jotka ovat ko. palvelulle ominaisia, mutta puuttuivat luettelosta. Luettelo ei ollut tyhjentävä ja tämä todettiin myös ohjeistuksessa.

PÄÄSY LÄHDEKOODIIN	Pohdittavaa	Linkit	Vastaus
Pääsy lähdekoodiin	Ketkä pääsevät lukemaan (lukuoikeus) tai muokkaamaan (kirjoitusoikeus) lähdekoodia? Entä ketkä ja millä oikeuksilla pääsevät kehittämistyökaluihin? Entä ohjelmistokirjastoihin? Miten näitä hallitaan ja miten lähdekoodi on suojattu? Aiheutuuko lähdekoodiin pääsystä järjestelmässänne/palvelussanne tietoturvauhkia tai -riskejä?	Hallintakeino Lähdekoodien, kehittämistyökalujen ja ohjelmistokirjastojen luku- ja kirjoitusoikeuksia on hallittava asianmukaisesti. (SFS-EN ISO/IEC 27001:2023 Liite A 8.4) A.8.4 Pääsy lähdekoodiin	Miksi uhka voi toteutua, ts. missä voi olla haavoittuvuus? Löytyykö uhka? Löytyykö haavoittuvuus? Jos molemmat löytyvät, on kyseessä riski. Miten hyökkääjä voisi tässä tilanteessa hyödyntää haavoittuvuutta? Mistä riskin huomaa? Mistä voi tunnistaa riskin kertymistä? **Kirjoita vastaus tähän.** **Kirjoita myös perustelu asialle.** ☐ EI TUNNISTETTUA RISKIÄ ☐ RISKI TUNNISTETTU Maalaa tämä ruutu punaisella taustavärillä, jos uhka tai riski on tunnistettu (ja poista tämä teksti).

Kuvio 12. Pääsy lähdekoodiin -aihe uhka-riskimallinnuksen itsepalvelumallissa

Jos riski aiheessa tunnistettiin, merkittiin tieto kysymyksen kohdalle, ja joko jatkettiin kaikkien kysymysten läpikäyntiä ja palattiin tunnistettuihin riskeihin myöhemmin, tai analysoitiin ja arvioitiin riski saman tien ja vasta sen jälkeen siirryttiin seuraavaan kysymykseen. Riskin tietoja merkittiin sekä Confluencen lomakkeelle, että osin Jiraan. Mallipohja ohjasi täyttämään Jiraa niin, että sen kaikkien laatikoiden kysymyksiin tuli saman tien vastattua oikealla tavalla. Jos riskiä ei tunnistettu, merkittiin tämä tieto kysymyksen kohdalle ja siirryttiin seuraavaan kysymykseen. Silloin Jiraan ei tarvinnut tehdä mitään merkintää.

Kysymysten periaatteena oli varmistaa, että niiden avulla saatiin paljon kattavampi lopputulos tietoturvauhkien ja -riskien arvioinnista kuin silloin, jos käyttäjät olisivat täyttäneet aiempaa lähes tyhjää Excel-mallinnusta itsenäisesti. Monilla käyttäjillä ei ollut syvällistä kokemusta tietoturvan vaatimuksista, joten itsepalvelumallissa näin ei oletettukaan. Itsepalvelumallin aihealueiden ja kysymysten avulla käyttäjiä autettiin saavuttamaan hyvän kokonaiskuva palvelunsa tietoturvauhista ja -riskeistä. Mallipohjalla pyrittiin varmistamaan, että mahdollisten tietoturvariskien eri aihealueet tulivat kattavasti huomioiduiksi. Käytettyyn termistöön kiinnitettiin myös huomiota. Käyttäjien haluttiin esimerkiksi tunnistavan hyökkäysvektoreita, mutta koska hyökkäysvektori on ammattitermi eikä käyttäjien arkikieltä, sitä ei käytetty uhka-riskimallinnuksessa. Sen sijaan kysyttiin, miten hyökkääjä voisi tässä tilanteessa hyödyntää haavoittuvuutta.

Käyttäjät saivat käyttää itsepalvelumallia sillä tavoin, minkä kokivat järkevimmäksi. Malli ei säädellyt toteuttamistapaa. Käyttäjät pystyivät käymään kysymykset läpi rivi riviltä, eli yksi aihe kerrallaan. Jos riski tunnistettiin, se voitiin analysoida ja arvioida heti. Toinen vaihtoehto oli ensin käydä läpi kaikki aiheet ja tunnistaa sieltä riskit, ja tämän jälkeen suorittaa analysointi- ja arviointikierros. Riskien todennäköisyyden ja vaikutuksen arviointiin annettiin apuvälineeksi toimeksiantajan riskimatriisi tarkempine sisältöineen. Materiaalissa oli tämän lisäksi nostettu esiin asioita, joita todennäköisyyden ja vaikutuksen kohdalla voi tarkastella. Todennäköisyyden osalta voi miettiä mm. hyökkääjää, puolustautumista, haavoittuvuuksia, aiempia hyökkäyksiä ja trendejä, toimintaympäristöä ja kumuloituvia riskejä. Vaikutuksen osalta voi pohtia mm. tiedon luonnetta ja arvoa, liiketoimintaa, lainsäädännöllisiä asioita, sidosryhmiä, toipumista ja pitkäaikaisvaikutuksia.

Koska malli oli aina saatavilla ja käyttäjien omassa työtilassa, sitä pystyi tekemään tarpeen mukaan joko yhdellä tai useammalla kertaa. Kun uhka-riskimallinnus oli itsepalvelumallin avulla tehty ja dokumentoitu ja tietoturvariskit laitettu Jiraan, asioiden käsittely jatkui Jiraan laitettujen, vastuutettujen ja aikataulutettujen riskien kautta. Näin pyrittiin varmistamaan, että tietoturvariskit ensinnäkin saadaan vastuullisille henkilöille hoidettavaksi, ja toiseksi aikataulutettiin seurantaa toimenpiteiden toteutumisen seuraamiseksi.

Tietoturvayksikön tukipalvelu toimi nopean avun kanavana, jos käyttäjä ei ollut varma mihin etenemispolkuun heidän palvelunsa kuuluu, tai itsepalvelumallia käyttäessä heräsi joku muu kysymys. Itsepalvelu-etenemispolulla ei ollut tarvetta konsultoida tietoturvayksikköä millään lailla, jos asian sai hoidettua itsenäisesti. Yhdellä etenemispoluista tietoturvayksikkö konsultoi lyhyesti tehtyä itsepalvelumallia, ja yhdellä puolestaan itsepalvelumallin jälkeiset toimenpiteet toteutettiin tiiviissä yhteistyössä tietoturvayksikön ja palvelun kesken. Etenemispolkujen tarkempi kriteeristö on jätetty tässä tietoturvasyistä kertomatta. Käyttäjille tehtiin myös kuvat kunkin etenemispolun prosessista. Kuviossa 13 on esitetty itsepalvelumallin etenemispolku. Siinä tietoturvayksikköön ei tarvitse välttämättä olla lainkaan yhteydessä, vaan prosessi hoidetaan kokonaan itsenäisesti.

Kuvio 13. Uhka-riskimallinnuksen etenemispolku itsepalvelumallissa

Itsepalvelumallilla tehtävä uhka-riskimallinnusta päivitettiin koko palvelun elinkaaren ajan: joko kerran vuodessa tai aiemmin, jos palveluun tuli merkittäviä muutoksia. Omaisuuksien arviointia päivitettiin tarvittaessa tai ainakin tarkistettiin sen ajantasaisuus. Koostesivu tuli päivittää joka kerta mallinnusta tehtäessä, jotta sen tiedot säilyivät ajan tasalla. Uhka-riskimallinnuksia tuli siis käyttäjien työtilaan useita. Nämä erotettiin toisistaan päivämäärällä. Aiemmat mallinnukset vaadittiin säilyttämään dokumentointivaatimuksen vuoksi. Tietoturvariskien tietoja päivitettiin tai luotiin uusia riskejä, ja tarkistettiin samalla toimenpiteiden onnistuminen. Uhka-riskimallinnukseen liittyvät sivut merkittiin tunnisteella, jonka kautta niitä pystyy organisaatiotasolla hakemaan.

Inhimilliset tekijät

Sekä tietoturvaan liittyvien käsitteiden että riskimatriisin määrittelyillä pyrittiin siihen, että riskien arviointi ja analysointi saataisiin tehtyä mahdollisimman yhdenmukaisesti. Tunnistamis- ja arviointivaiheeseen liittyy kuitenkin paljon psykologisia tekijöitä, jotka voivat inhimillisistä syistä aiheuttaa tiettyjen asioiden ylikorostumista. Aloitteleva käyttäjä voi korostaa liikaa esimerkiksi riskin todennäköisyyttä tai vaikutusta, kun kokeneempi käyttäjä huomioi molempia tasapuolisesti, jolloin päästään parempaan arvioon. Ilmonen ja muut (2016) viittaavat Drottz-Sjöbergin (1991) tutkimukseen, jossa käsitellään kaksikymmentä erilaista kognitiivista vinoumaa riskienhallinnassa. Tutkimuksesta on esimerkiksi ilmennyt, että riski, joka on jo toteutunut aiemmin, koetaan suuremmaksi kuin riski, josta ei ole kokemusta. Riski, jota käsitellään paljon julkisuudessa, koetaan suuremmaksi kuin riski, jota ei käsitellä julkisuudessa. Riski, joka kohdistuu muihin kuin käyttäjään itseensä, koetaan suuremmaksi kuin riski, joka kohdistuu käyttäjään. Uhka-riskimallinnuksen itsepalvelumallissa tunnistettiin inhimillisten tekijöiden vaikutus ja tästä kirjoitettiin ohjeistukseen. Varsinkin itsepalvelumallin käyttämisen alkuvaiheessa on seurattava uhka-riskimallinnusten laatua ja tarjottava tukea arviointiin käyttäjien sitä pyytäessä. Tietoturvatietoisuuden kasvattaminen ja riskienhallinnan prosessien omaksuminen eivät tapahdu hetkessä, mutta ajattelua aletaan ohjata tähän suuntaan. Uhka-riskimallinnuksen itsepalvelumallissa lähdetään siitä, että tietoturva on jokaisen vastuulla oleva asia, ja jokainen voi siihen omalla toiminnallaan vaikuttaa. Tietoturva ei ole lisäosa, vaan osa jokapäiväistä toimintaa. (Ilmonen ym. 2016, 90-93.)

Riskien käsittely ja hallinnointi

Uhka-riskimallinnuksen itsepalvelumallilla tunnistettiin tietoturvauhkia ja -riskejä, sekä analysoitiin ja arvioitiin ne. Rinnakkaisena toimenpiteenä tietoturvariskit vietiin Jiraan sieltä kautta käsiteltäviksi. Riskille asetettiin vastuuhenkilö ja seuranta-aika. Riskin vastuuhenkilöksi tuli tilanteen mukaan joko tuoteomistaja tai palvelupäällikkö, eli henkilö, joka vastaa liiketoiminnastakin. Toimeksiantajalla oli ohjeistus siitä, milloin riskin hallintakeinot pitää päättää tai toteuttaa esimerkiksi johtoryhmätasolla. Riskien hallintakeinot eli ne toimenpiteet, joilla riskiä konkreettisesti esimerkiksi vähennettiin, toteutettiin mallista erillään mutta kuitenkin olennaisesti malliin kytkeytyen. Uhka-riskimallinnukseen ja Jiran tietoturvariskille tehtyjen kirjausten perusteella saatiin hyvät taustatiedot hallintakeinoista päättämiseksi ja niiden toteuttamiseksi. Uhka-riskimallinnuksen seuraavassa päivityksessä tarkasteltiin, miten hallintakeinot ovat konkreettisesti edenneet ja onko niillä ollut haluttua vaikutusta, sekä tehtiin tarvittavia muokkauksia. (Ilmonen ym. 2016, 62, 113, 130-134.)

5 Tulokset

Tässä luvussa esitellään uhka-riskimallinnuksen itsepalvelumalliin liittyen valmistuneet materiaalit sekä analysoidaan, kuinka hyvin niillä vastattiin asetettuihin vaatimuksiin. Lisäksi tarkastellaan itsepalvelumalliin liitettyjä keskeisiä mittareita ja liittymäpintoja, jotka varmistavat seurannan ja kehittämisen tarpeita. Luvun lopuksi keskitytään niihin tekijöihin, joita on hyvä huomioida opinnäytetyön jälkeen tapahtuvassa varsinaisessa käyttöönottoprosessissa.

5.1 Uhka-riskimallinnuksen itsepalvelumallin materiaalit

Uhka-riskimallinnuksen itsepalvelumalli valmistui 22.11.2024, ja siihen kuuluvat seuraavat asiat käyttäjille:

- Uhka-riskimallinnustyökalu
- Uhka-riskimallinnuksen toimintatavan muutoksen ja perusteiden ohjeistus
- Etenemispolkujen ja prosessien ohjeistus
- Omaisuuksien arvioinnin ohjeistus
- Riskien tunnistamisen ohjeistus
- Riskien analysoinnin ja arvioinnin ohjeistus
- Jiran käytön ohjeistus
- Confluencen käytön ohjeistus

- Usein kysytyt kysymykset (UKK)
- Termipankki
- Esimerkkitapaus.

Toimeksiantajalle kuuluvat materiaalit:

- Itsepalvelumallin lähtökohdat
- Itsepalvelumallin liittymäpinnat organisaation sisäisiin asiakokonaisuuksiin
- Itsepalvelumallin kysymysten pääversio
- Käyttöönottosuunnitelma
- Viestintäsuunnitelma
- Koulutusmateriaalirungot
- Itsepalvelumallin kehittämisehdotukset.

Yllä mainitut asiat on luovutettu toimeksiantajalle käyttöönottoa varten. Materiaalit sisältävät käyttäjille varsinaisen uhka-riskimallinnustyökalun, sekä sen käyttöön liittyvän ohjeistuksen. Käyttäjille kerrotaan ensin toimintatavan muutoksesta ja perusteista, ja sen jälkeen jokaisesta uhka-riskimallinnuksen osa-alueesta sekä kokonaisprosessista. Työkalujen eli Jiran ja Confluencen osalta on mukana ohjeistus uhka-riskimallinnuksen näkökulmasta. Materiaaleissa on UKK-sivu sekä termipankki ja esimerkki, jossa käydään läpi eri toiminnot ja periaatteet kuvitteellisen Kynä-palvelun avulla. Toimeksiantajalle tarkoitetuissa materiaaleissa on esitelty tarkemmin itsepalvelumallin taustalla olevat periaatteet ja vaatimukset, ja käyty kohta kohdalta läpi mm. NIS2 vaatimukset ja ISO 27001 -standardin A-liitteen hallintakeinot perustellen, mitä ja miksi on tai ei ole otettu mukaan. Lisäksi on käyty yksityiskohtaisesti läpi ISO 27001 -standardin osalta, miten sen vaatimuksiin on vastattu uhka-riskimallinnuksen itsepalvelumallissa. Toimeksiantajalle on koottu organisaation sisäiset liittymäpinnat uhka-riskimallinnukseen liittyen. Kysymysten pääversio sisältää kysymykset, joita kehittämällä itsepalvelumallista voi tehdä seuraavia versioita. Itsepalvelumallin käyttöönottosuunnitelma, viestintäsuunnitelma ja koulutusmateriaalirungot on valmisteltu niin pitkälle kuin opinnäytetyön kirjoittajan on ollut mahdollista toimivaltansa puitteissa tehdä. Viimeisenä toimeksiantajalle on mukana itsepalvelumallin jatkokehittämisehdotuksia, joita ei tässä ensimmäisessä itsepalvelumallin versiossa pystytty perustelluista syistä huomioimaan.

5.2 Uhka-riskimallinnuksen itsepalvelumallille asetettuihin vaatimuksiin vastaaminen

Uhka-riskimallinnuksen itsepalvelumallin kehittämisen tavoitteena oli, että tietoturva-asiantuntijoiden resursseja on saatava vapautettua muuhun käyttöön. Uhka-riskimallinnusta oli pystyttävä tekemään silloin kun käyttäjä itse tarvitsee, 24/7 -ajatuksella. Pitkän tähtäimen tavoite oli, että suuri osa uhka-riskimallinnuksista voitaisiin tehdä itsepalveluna. Käyttöönoton jälkeen voidaan todeta, minkä verran tietoturva-asiantuntijoiden aikaa saadaan vapautettua, mutta oletus on, että työajan säästöä tulee. Malli on saatavilla Confluence-työtilassa ja mallipohjat ovat sieltä vapaasti kopioitavissa aina, kun käyttäjä niitä tarvitsee. Jonotusta tietoturva-asiantuntijan vapaaseen aikaan ei enää tarvita. Tehty itsepalvelumalli mahdollistaa sen, että suurin osa palveluista voi tehdä uhka-riskimallinnuksen täysin itsenäisesti. Tietoturvayksikön kanssa yhteistyötä tarvitsevat käyttäjät saavat palvelunsa nopeammin, kun kaikille ei enää tarvita tietoturvayksikön järjestämiä työpajasarjoja. Itsepalvelumallista on tehty käyttäjäystävällinen ja kysymykset on pyritty pitämään selkeinä. Näin mallinnuksen tekeminen itsessään on helppoa, ja käyttäjät pystyvät keskittymään mallinnuspohjan sijaan itse asiaan.

Toisena tavoitteena oli, että uhka-riskimallinnus ei olisi enää kertaluontoinen, vaan sitä tehtäisiin säännöllisesti. Lisäksi haluttiin, että uhka-riskimallinnuksista pystyisi tekemään seurantaa, kun aiemmin tietoa jatkotoimista ei saatu lainkaan. Toivottiin myös mittareita ja uhka-riskimallinnuksen sisällyttäminen vuosikelloon. Itsepalvelumalli on rakennettu sille periaatteelle, että sitä voidaan tehdä useasti. Mallipohjaa voi kopioida vapaasti. Omassa työtilassa tehdyt uhka-riskimallinnukset erotetaan toisistaan päivämäärällä. Työtilan sivuille lisätyillä tunnisteilla saadaan haettua kaikista työtiloista kaikki tehdyt uhka-riskimallinnukset. Jiran tietoturvariskien käytön aktivoimisella saadaan riskejä näkyviin, ja niistä saadaan muodostettua organisaatiotasoisia näkymiä. Kun uhka-riskimallinnus liitetään vuosikelloon, voi sen käyttöönottoprosenteista asettaa mittarin. Laadullistenkin mittarien kehittäminen on mahdollista esimerkiksi tehtyjä kirjauksia läpikäymällä. Myöhemmin voi seurata mallinnusten päivitystahtia.

Kolmantena tavoitteena oli uhka-riskimallinnuksen käyttäjien oman tietoturvaosaamisen tason parantaminen ja se, että palvelu ottaisi vastuuta omasta tietoturvastaan. Tämän lisäksi haluttiin elinkaariajattelua eli sitä, että uhka-riskimallinnuksen teko ei ole vain kertaluontoinen suunnitteluvaiheen tehtävä – eiväthän tietoturvauhat ja -riskit mihinkään häviä. Haluttiin, että riskit sekä

huomioitaisiin että dokumentoitaisiin aiempaa paremmin. Itsepalvelumallin vaikutus käyttäjien tietoturvaosaamisen syventämiseen näkyy käyttöönoton jälkeen. Lähtökohta on, että käyttäjien ei tarvitse tunnistaa viitekehyksiä, standardeja tai malleja, vaan ne on uitettu kysymysten sisään. Käyttäjä voi halutessaan katsoa linkeistä lisätietoja aiheeseen liittyen. Yleinen tieto siitä, mitä tietoturva on, ja mitä ovat uhka, riski ja haavoittuvuus, on itsepalvelumallin peruslähtökohta. Jos nämä käsitteet eivät ole aiemmin tuttuja, ne tulevat materiaaleissa ja mallissa tutuiksi. Riskien nostaminen Jiraan ja sitä kautta riskien käsittely tulevat itsepalvelumallin kautta aiempaa järjestelmällisemmin ja kattavammin käyttöön. Itsepalvelumallin kysymyksissä on pyritty siihen, että palveluun liittyviä tietoturvauhkien ja -riskien osa-alueita on käsitelty niissä monipuolisesti. Käyttäjien tietoturva-ajattelu lisääntyy, kun he miettivät oman palveluaan näiden aihealueiden kautta. Uhka-riskimallinnuksen itsepalvelumalli mahdollistaa uuden mallinnuksen tekemisen milloin vain, kun tarve tai yleinen päivitysajankohta tulee. Käyttöönotossa tulee huomioida sen korostaminen, että kyse on nyt jatkuvasta, järjestelmän elinkaaren ajan käytössä olevasta toiminnasta. Mitä enemmän työtä tietoturvauhkien ja -riskien parissa tehdään, sen paremmaksi kasvaa palvelun tietoturvallisuus. Tätä kautta myös toimeksiantajan tietoturvallisuuden taso kohoaa. Tietoturvayksikkö pystyy itsepalvelumallia päivittämällä nostamaan uusia riskinäkökulmia organisaation tarkasteltaviksi, jolloin malli säilyy ajankohtaisena muuttuvassa maailmassa.

5.3 Uhka-riskimallinnuksen itsepalvelumallin mittarit ja liittymäpinnat

Aiemmassa uhka-riskimallinnuksessa seurantaa ei toteutettu lainkaan. Ei ollut tietoa, mitä palvelut tekivät tietoturvariskeilleen työpajojen jälkeen, vai tekivätkö mitään. Uhka-riskimallinnuksen itsepalvelumallissa pyrittiin siihen, että sitä voi ylipäänsä mitata ja seurantaa voi tehdä. Itsepalvelumallissa voitiin saada työtilojen tunnisteiden avulla tietoa siitä, kuinka moni palvelu on ottanut uhka-riskimallinnuksen käyttöön, sekä myöhemmin käydä katsomassa, kuinka monta mallinnusta kukin palvelu on tehnyt. Palvelun tekemien uhka-riskimallinnusten kirjausten laadusta pystyi tekemään seurantaa. Jiraan luotujen tietoturvariskien lukumäärää ja sisältöä pystyttiin seuraamaan. Johtoryhmä pystyi asettamaan tavoitteen, että x prosenttia palveluista on ottanut uhka-riskimallinnuksen käyttöön ensimmäisenä käyttöönottovuotena. Uhka-riskimallinnuksen itsepalvelumalli liittyi osaksi organisaation riskienhallintaa. Se kuului osaksi IT-järjestelmädokumentaatiota ja hyödynsi uhkapankkia.

Tulevaisuudessa mittareiden kehittämisessä päästään parempaan automaatioasteeseen, jos uhka-riskimallinnusta varten hankitaan tai kehitetään järjestelmä, jolla on oma tietokanta. Tuolloin tietoja saadaan käsiteltyä tietokantahauilla. Nyt Jira toimii riskirekisterinä. Jos uhka-riskimallinnuksen viimeisin tekopäivä vietäisiin organisaation palvelunhallintavälineeseen, olisi tieto helpommin saatavilla. Tämä vaatii välineeseen teknisen muutoksen. Kirjaaminen IT-järjestelmädokumentaation osaksi helpottaa asiaa jo jonkin verran. Määrällisiä mittareita uhka-riskimallinnukselle voivat olla muun muassa käyttöönoton aste, käyttökertojen määrä, käyttäjäkohtainen aktiivisuus (kuinka moni palvelu käyttää mallia säännöllisesti) sekä pelkän itsepalvelumallin käyttäjien suhde tietoturvayksikön tukemiin käyttäjiin. Lisäksi voisi mitata tukipyyntöjen määrää, koulutukseen käytettyä aikaa ja tietoturva-asiantuntijoiden ajansäästöä. Pidemmällä aikavälillä nähdään myös riskitason muutos, jota on tärkeää seurata. Laadullisia mittareita saisi helposti käyttäjätyytyväisyyttä ja tietoturvayksikön tukipalvelun onnistumista tutkimalla.

Uhka-riskimallinnuksen itsepalvelumalli voi tulevaisuudessa tarjota paljon tietoa eri tarkoituksiin. Kun palveluista alkaa kertyä mallinnustietoa, ja niiden tietoturvariskejä alkaa tulla myös Jiraan, voidaan tietoja hyödyntää luonnollisesti itsepalvelumallin kehittämisessä, mutta myös valvonnan parantamiseen (esimerkiksi käyttötapaukset, valvonnan painopisteet), jatkuvuudenhallinnan kehittämiseen ja yleisesti tietoturva-asioiden painopisteiden määrittelyyn sekä esimerkiksi uhkapankin kehittämiseen. Tietoa voi kuljettaa myös toiseen suuntaan itsepalvelumallin kehittämiseksi.

5.4 Uhka-riskimallinnuksen itsepalvelumallin käyttöönotto

Uhka-riskimallinnuksen itsepalvelumallin käyttöönotto tehdään tässä opinnäytetyössä valmistellun materiaalin avulla tulevan vuoden alussa. Käyttöönottoa varten tarvitaan uhka-riskimallinnuksen itsepalvelumallin virallinen kytkentä koko organisaation riskienhallintaan ja vuosikelloon, sekä johdon päätökset asiaan liittyen (käyttöönotto, päivittämissykli, vastuiden määrittely ym.). Malli on sulautettava osaksi olemassa olevia prosesseja, jotta sen käytöstä tulee luontevaa. Käyttöönottoa varten on tehty käyttöönottosuunnitelma sekä viestintäsuunnitelma. Vastuu käyttöönotosta on toimeksiantajan tietoturvayksiköllä.

Tietoturvariskien tunnistaminen uhka-riskimallinnuksen itsepalvelumallin avulla auttaa toimeksiantajaa riskien torjumisessa sekä ohjaamaan resursseja ja päätöksiä tietoon perustuen. Tämä voi vähentää kustannuksia sekä konkreettisia riskien toteutumisesta aiheutuvia vahinkoja, ja parantaa

toimeksiantajan reagointikykyä. Johdon tuen ja sitoutumisen merkitystä käyttöönoton onnistumiselle ei voi liikaa korostaa. Käyttöönottosuunnitelmassa on huomioitu se, että tarvittavat päätökset ja kytkökset tehdään, sekä se, että vastuuhenkilöt uhka-riskimallinnukselle sekä riskeille löytyvät. Uhka-riskimallinnuksen itsepalvelumallin käyttöönotto edistää omalta osaltaan toimeksiantajan riskienhallinta- sekä tietoturvakulttuurin kehittymistä. Kehittymisen takaamiseksi johdon on sitouduttava mallin läpiviemiseen sekä näytettävä esimerkkiä. Tässä olisi hyvä kohta ottaa riskienhallintaa järjestelmällisemmin johtamisen tueksi ja osaksi johtamisen prosessia. Uhka-riskimallinnusten tekemisen koordinointi on tärkeää, jotta riskien laatu ja määrä ei muodostu hallitsemattomaksi (Hytönen 2021, 24).

Toinen yhtä tärkeä rooli käyttöönoton onnistumisessa on käyttäjillä. Heille annettavien toiminta-ohjeiden on oltava käyttökelpoisia ja heidät on perehdytettävä, jotta he ymmärtävät itsepalvelumallin merkityksen ja sen tuoman lisäarvon palvelulleen. Itsepalvelumallia on tämän vuoksi käsiteltävä laajasti ennen käyttöönottoa palvelujen sekä tuoteomistajien ja johdon kanssa. Myös suoraan käyttäjille tehtyä viestintää tarvitaan. Hyvällä viestinnällä saadaan itsepalvelumalli jollain tapaa tutuksi jo ennen kuin se otetaan konkreettisesti käyttöön. Viestintä ei lopu itsepalvelumallin käyttöönottoon, vaan sitä tulee tehdä jatkuvasti nostaen esiin konkreettisia onnistumisia, jotka puolestaan rohkaisevat muita käyttäjiä. Hyvä viestintä auttaa pitämään aihetta eli tietoturvauhkia ja -riskejä esillä, ja luo positiivisen ilmapiirin, jossa käyttäjät pystyvät antamaan palautetta ja ehdotuksia mallin kehittämiseksi. Lisäksi tarvitaan yhteistä keskustelua sekä riskienhallintaosaamisen kehittämistä.

Uhka-riskimallinnuksen itsepalvelumallin käyttöönottovaiheessa tarvitaan hetkellisesti hieman isompi panostus tukikanavaan, koska alussa kysymyksiä voi luonnollisesti tulla enemmän. Käyttäjille tulee aiempaan elämään verrattuna enemmän työtä, koska uhka-riskimallinnus tehtiin aiemmin vain yhden kerran. Johdon tuki varmistaa, että resurssit tähän työhön saadaan ja työn merkitys ymmärretään. Itsepalvelumallin esittely- ja koulutustilaisuuksien kautta tulee varmistaa, että malli tuntuu käyttäjille helposti lähestyttävältä ja arkipäiväiseltä. Näin itsepalvelumallin käyttämisen aloittamisen kynnys madaltuu. Jos käyttäjä ei saa riittävää tukea tai aikaa tehdä tätä työtä, jää tietoturvariskejä tunnistamatta. Tunnistamatonta riskiä ei voi hallita (Hytönen 2021, 13).

6 Opinnäytetyön arviointi ja johtopäätökset

Tässä luvussa tarkastellaan, miten opinnäytetyö vastaa asetettuihin kehittämiskysymyksiin ja miten hyvin työ täyttää luotettavuuden, validiteetin ja eettisyyden vaatimukset. Lisäksi analysoidaan toteutuksen onnistumista ja saavutettuja tuloksia vertaamalla niitä teoreettiseen viitekehykseen. Lopuksi pohditaan tulosten sovellettavuutta käytännön tilanteissa ja niiden hyödyntämismahdollisuuksia.

6.1 Kehittämiskysymyksiin vastaaminen

Kehittämiskysymykset tässä opinnäytetyössä olivat:

1. Millainen on toimeksiantajan tarpeita palveleva uhka-riskimallinnuksen itsepalvelumalli?
2. Millaisia tukiprosesseja ja ohjeistuksia on rakennettava, jotta palvelu voi käyttää itsepalvelumallia?
3. Mitä tarvitaan, jotta uhka-riskimallinnuksen tekeminen muuttuu pysyväksi osaksi palvelun toimintaa?

Toimeksiantajan tarpeita palvelevan uhka-riskimallinnuksen itsepalvelumallin sisältörunko muodostui teoriapohjan kautta perehtymällä kirjallisuuteen, standardeihin sekä viitekehyksiin. Taustahaastattelujen ja säännöllisten yhteispalaverien kautta tuli esiin toimeksiantajan tarpeita ja ehdotuksia malliin liittyen. Itsepalvelumallista tuli aina käytettävissä oleva, eikä sen käyttöön tarvitse opetella uusia työkaluja. Mallin käyttäjältä ei vaadita syvällistä tietoturvan tai riskienhallinnan asiantuntemusta. Itsepalvelumalli, sen ohjeistus sekä koulutusmateriaalit on rakennettu käyttäjää ajatellen. Itsepalvelumalli sopii ensivaiheessa palveluille, mutta muutkin voivat käyttää sitä soveltuvin osin, ja mallissa on tilaa myös omille aihealueille. Itsepalvelumallin käyttöä voi mittaroida ja seurata.

Jotta palvelu pystyy käyttämään itsepalvelumallia, on mallin itsensä oltava käyttäjäystävällinen. Erilaiset tietoturvavaatimukset ja turvallisuusnäkökulmat on sulautettu aihealueisiin niin, että aihealueet läpikäymällä saa monipuolisen ja kattavan kuvan palvelun tietoturvallisuuden tilasta. Käyttäjille tarjotaan monipuoliset tukimateriaalit ja ohjeistukset mallin käyttöön ja käytöstä heräävii kysymyksiin. Jotta itsepalvelumallia voidaan käyttää tehokkaasti, auttavat ohjeet käyttäjiä mal-

linnuksen jokaisessa vaiheessa. Prosessi on sanoitettu ymmärrettävästi. Tuki toimii matalalla kynnyksellä ja käyttäjät tietävät, miten tukea saa. Koulutusmateriaalit ja UKK sekä termipankki tukevat käyttäjää tarvittaessa. Käytännön esimerkin kautta näkee konkreettisesti, miten mallia ja Jiraa täytetään. Mallin käytöstä kerätään palautetta ja kokemuksia. Kun käyttöönotosta on kulunut jonkin aikaa eli uhka-riskimallinnusta on tehty itsepalvelumallin kautta jo paljon, kerätään tietoa sekä määrästä että laadusta mallin kehittämistä varten.

Jotta uhka-riskimallinnuksen itsepalvelumallin tekeminen muuttuu pysyväksi osaksi palvelun toimintaa, vaaditaan ensin johdon tekemät päätökset asiaan liittyen. Johdon on osoitettava tekemiseen resurssit ja varmistettava, että uhka-riskimallinnusta tehdään säännöllisesti ja johdonmukaisesti. On tärkeää integroida uhka-riskimallinnuksen itsepalvelumallin tekeminen olemassa oleviin kehittämisprosesseihin. Itsepalvelumallia tulee kehittää jatkuvasti käyttäjien toiveita ja ehdotuksia huomioiden. Käyttäjiä tulee kouluttaa myös käyttöönoton jälkeen. Uhka-riskimallinnusten seuranta ja niistä raportointi auttavat osoittamaan itsepalvelumallin käytön toteutumista, sen tuomia hyötyjä sekä kehittämistarpeita.

Kehittämiskysymykset olivat aiheeseen liittyviä ja johdonmukaisia, ja niihin saatiin opinnäytetyössä vastaukset. Kehittämiskysymykset auttoivat suuntaamaan itsepalvelumallin kehittämistyötä. Tutkimuksellinen kehittämistoiminta tuki menetelmänä uhka-riskimallinnuksen monipuolista tarkastelua ja tiedon tuottamista siihen liittyen.

6.2 Opinnäytetyön luotettavuus, validiteetti ja eettisyys

Luotettavuuden arviointi tutkimuksellisessa kehittämistyössä on erilaista kuin tutkimuksessa. Luotettavuutta voi tarkastella esimerkiksi vakuuttavuuden ja johdonmukaisuuden käsitteiden avulla. Toikko ja Rantanen (2009) viittaavat Lincolnin ja Cuban (1985) määrittelyihin. Vakuuttavuus (engl. conformability) perustuu uskottavuuteen ja johdonmukaisuuteen. Johdonmukaisuus (engl. dependability) puolestaan syntyy siitä, että aineisto kerätään ja analysoidaan huolellisesti ja läpinäkyvästi. Lisäksi analyysivaiheen epävarmuustekijät ja johtopäätöksiä heikentävät osatekijät tuodaan ilmi. Luotettavuutta lisäävänä nähdään myös aineiston kyllääntyminen. (Toikko & Rantanen 2009, 123-124.)

Luotettavuuteen on tässä opinnäytetyössä pyritty sillä, että asiat on kerrottu rehellisesti ja johdonmukaisesti. Aineisto on kerätty systemaattisen tiedonhaun menetelmällä, ja toimeksiantajan materiaalit on tarkasteltu kattavasti. Systemaattisella tiedonhaulla on haettu teoriatietoa laajoilla hauilla eri lähteistä, ja aineisto on valittu tarkasti ja kriittisesti pohtien sekä lähteiden laatua korostaen. Systemaattisella tiedonhaulla on saavutettu kyllääntyminen, eli piste, jossa uusien tietojen kerääminen ei tuo enää esiin uusia teemoja, näkökulmia tai ideoita ilmiöstä. Kerätty aineisto katsotaan tuolloin riittävän laajaksi ja monipuoliseksi. Syvemmän tiedon saamiseksi toimeksiantajan asiantuntijoille on tehty taustahaastatteluja. Toimeksiantajan vaatimuksia on noudatettu ja asioita säännöllisesti läpi toimeksiantajan kanssa. Vaatimusten sisältöä on tarkennettu yhteistyössä työn edetessä. Opinnäytetyön vaiheet, menetelmät ja tulokset on toteutettu ja dokumentoitu huolellisesti ja systemaattisesti sekä kuvattu avoimesti.

Validiteetti tarkoittaa pätevyyttä eli sitä, kuinka hyvin tutkimus heijastaa tutkimaansa ilmiötä, ja kuinka luotettavia ja totuudenmukaisia sen tulokset ovat. Tutkimuksellisessa kehittämistyössä validiteetin sijaan tärkeämpää on kehittämistulosten käyttökelpoisuus eli se, että kehittämisprosessin seurauksena syntyneet tulokset ovat hyödynnettävissä. Kehittämistoiminnalta jää puuttumaan merkitys, jos sen tuloksena ei synny mitään käyttökelpoista. Toikko ja Rantanen (2009) viittaavat Alasoinin (2006) näkemykseen, jossa tuodaan esiin toisen asteen geneerisiä tuloksia eli sellaisia tuloksia, joilla on merkitystä sekä yksittäisen organisaation kannalta, mutta myös laajemmin. (Toikko & Rantanen 2009, 125-126, 159.)

Toimeksiantajan mukaan opinnäytetyön kirjoittaja on paneutunut aiheeseen perusteellisesti ja hyödyntänyt aktiivisesti sekä kirjallisuutta että kokeneiden asiantuntijoiden näkemyksiä. Opinnäytetyön aikana kirjoittajan ammatillinen osaaminen kasvoi toimeksiantajan mukaan huomattavasti ja kirjoittajalla on kyky hahmottaa monimutkaisia kokonaisuuksia sekä tuottaa johdonmukaista ja perusteltua tekstiä. Teksti olisi voinut kuitenkin olla viimeistellympää kielenhuollon näkökulmasta. Toimeksiantaja arvosti erityisesti systemaattisen tiedonhakumallin onnistunutta käyttöä ja teoreettisen viitekehyksen kattavaa käsittelyä. Toimeksiantaja katsoi, että teoriaosiossa olisi voinut perehtyä Open Access -aineistojen lisäksi myös lisensoituihin, vertaisarvioituihin akateemisiin tutkimuksiin, mikä olisi mahdollisesti syventänyt analyysia.

Eettisyys opinnäytetyössä on pyritty varmistamaan monin tavoin. Opinnäytetyössä on noudatettu Tutkimuseettisen neuvottelukunnan (TENK) eettisiä ohjeita ja hyvää tieteellistä käytäntöä (Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa 2023), ammattikorkeakoulujen opinnäytetöiden eettisiä suosituksia (Ammattikorkeakoulujen opinnäytetöiden eettiset suositukset 2020), ja Jyväskylän ammattikorkeakoulun raportointiohjeita (Liukko & Perttula 2021). Tutkimuslupa haettiin ja saatiin toimeksiantajalta. Projektisuunnitelma ja tutkimuslupahakemus hyväksyttiin toimeksiantajan johtoryhmässä. Opinnäytetyön hyväksyi toimeksiantajan puolesta uhka-riskimallinnuksen tuoteomistaja, ja asia esiteltiin tietoturvayksikön johtotiimille. Opinnäytetyössä ei käsitelty asiakkaiden tietoja, joten muita lupia tai erillistä eettistä arviointia ei tarvittu. Kaikki materiaali on tarkistettu yhdessä toimeksiantajan kanssa ennen sen sisällyttämistä opinnäytetyöhön.

Taustahaastattelujen kohteita eli toimeksiantajan asiantuntijoita ei nimetä eli he pysyvät tässä opinnäytetyössä anonyymeina. Asiantuntijoille kerrottiin käsiteltävät aiheet ja haastattelun tarkoitus ennakkoon ja kysyttiin suostumus haastatteluun. Kaikki suostuivat haastatteluihin mielellään. Jokaisen haastateltavan kanssa keskusteltiin vielä haastattelun aluksi tapaamisen tarkoituksesta sekä siitä, että haastatteluja ei nauhoiteta eikä ketään siteerata nimellä. Haastatteluista tehtiin käsin muistiinpanot, joita käytettiin aiheesta saatujen tietojen syventämiseen sekä kehittämisideoina. Myös käyttäjätestaukseen liittyvät sekä asiantuntijoiden mallista antamat kommentit kirjattiin ylös anonyymeina.

Opinnäytetyön ja itsepalvelumallin edistymistä käytiin säännöllisesti läpi sekä toimeksiantajan nimeämän opinnäytetyön ohjaajan että toimeksiantavan yksikön johtoryhmän kanssa. Heillä oli mahdollisuus antaa palautetta ja kehittämisehdotuksia koko prosessin ajan, ja esitettyjä näkökohtia ja uusia vaatimuksia sisällytettiin mallin kehittämistyöhön. Opinnäytetyö liittyi toimeksiantajan tietoturvauhkien ja -riskienhallintaan, joten toimeksiantajan materiaalit säilytettiin vain toimeksiantajan verkkolevyllä, eikä niitä siirretty tietoturvasyistä henkilökohtaiselle tietokoneelle missään vaiheessa. Kuten toimeksiantajan kanssa sovittiin, toimeksiantajan materiaaleja ei käytetty tarkemmin opinnäytetyössä lähdeaineistona, eikä niiden sisältöä avattu enempää kuin on tarpeen. Tämä linjaus tehtiin sen vuoksi, ettei opinnäytetyöstä tarvitsisi ryhtyä salaamaan osia, vaan se pystyttiin julkaisemaan kokonaan julkisena.

Opinnäytetyön kirjoittaja on työssä toimeksiantajalla, tosin eri yksikössä kuin minne opinnäytetyö on tehty. Opinnäytetyön aihe oli toimeksiantajan tilaustyö, mutta aihe-ehdotuksia oli kymmenkunta, ja kirjoittaja sai valita aiheen niiden joukosta. Aihe oli toimeksiantajalle tärkeä, koska heillä itsellään ei ollut resurssia kehittää uhka-riskimallinnusta, ja itsepalvelumallille asetettiin suuria toiveita myös resurssiensäästömielessä, vaikka muitakin tavoitteita toki oli. Kirjoittaja piti kuitenkin enemmän näkökulmansa muissa tavoitteissa: tärkeää oli saada hyvä, käyttökelpoinen ja ymmärrettävä malli, jolla palvelut voivat itse tehdä uhka-riskimallinnusta. Opinnäytetyön kirjoittajalle tärkeitä periaatteita olivat kertaluontoisuudesta jatkuvuuteen -periaate sekä se, että palveluilla itsellään on paras tieto omista tietoturvauhistaan ja -riskeistään. Kirjoittajalle tärkeä pitkän tähtäimen tavoite oli tietoturvallisuuden tason parantaminen, joka todellistuu, kun itsepalvelumallia käytetään säännöllisesti, tietoturvauhkia ja -riskejä tunnistetaan ja niitä käsitellään.

Eri yksikössä työskentelyn vuoksi tietynlaisen objektiivisuuden säilyttäminen oli helpompaa, kuin silloin, jos kirjoittaja olisi työskennellyt yksikössä, jonka työtilanteeseen tehty malli suoraan vaikuttaa. Kirjoittaja tiedosti sen, että kehittämistoiminnassa voi olla vaarana liian positiivisen kuvan antaminen kehittämistoiminnasta tai toimeksiantajan miellyttäminen kirjoittamalla korostaen positiivisia seikkoja (Toikko & Rantanen 2009, 128). Uhka-riskimallinnuksen itsepalvelumallin kehittämisprosessi on pyritty raportoimaan mahdollisimman tarkasti, jotta lukija saa kattavan kokonaiskuvan prosessin etenemisestä. Tulokset on raportoitu rehellisesti ja läpinäkyvästi nostaen esille myös ei-suotuisia seikkoja ja parannusehdotuksia.

6.3 Toteutuksen arviointi

Opinnäytetyöhön tutkimusmenetelmäksi valittu tutkimuksellinen kehittämistoiminta sopi tämän opinnäytetyön toteuttamiseen. Oli olemassa käytännön ongelma, ja tietoa tuotettiin käytännön toimintaympäristössä. Toteuttamisessa hyödynnettiin tutkimuksellista logiikkaa. Ongelmanratkaisun lisäksi tuotettiin tietoa myös laajempaan keskusteluun. Opinnäytetyössä hyödynnettiin kehitysprojektimaista tavoitteiden määrittelyä, prosessia ja tulosten arviointia. Valittu menetelmä toimi suunnitellusti. (Tuomi & Latvala 2022; Toikko & Rantanen 2009, 156-157.)

Systemaattisella tiedonhaulla opinnäytetyöhön saatiin kattava ja objektiivinen lähdeaineisto. Toimeksiantajalta saatiin käyttöön tarvittavat materiaalit, ja taustahaastattelut toivat paljon eri näkö-

kulmia uhka-riskimallinnuksen kehittämiseen. Aineiston keruuseen liittyen ei ollut ongelmia. Opinnäytetyön tekemisprosessi sujui hyvin, vaikka omaksuttava tietomäärä oli suuri. Opinnäytetyön toteuttamiseen oli riittävästi aikaa, ja se valmistui jopa etuajassa aikataulusta. Työssä pystyttiin etenemään alussa asetettujen jaksokohtaisten tavoitteiden mukaisesti. Tekemistä auttoi, että uhka-riskimallinnuksen kehittämiselle oli Jirassa Portfolio Epic, jonka alle pystyi tekemään tietoturvayksikön nimissä Jira-tiketit eli hallitsemaan ja järjestämään työtä paremmin kuin ilman Jiraa. Toimeksiantajan kanssa oli hyvä tehdä yhteistyötä.

Toikko ja Rantanen (2009) ovat nostaneet esiin kehittäjään kohdistuvat moninaiset odotukset. Organisaatio odottaa jotain, pyritään tuloksiin ja toisaalta tutkimuksellisuuden näkökulmasta vaaditaan rehellisyyttä ja kriittisyyttä. Lisäksi on huomioitava asiakkaat. Mallin rakentaminen tehtiin toimeksiantajan yhteisten riskienhallinnan puitteiden sisällä ja tiettyjä vaatimuksia noudattaen. Tämän lisäksi asiantuntijoiden taustahaastatteluissa ja kommenteissa nousi ehdotuksia, ja käyttäjänäkökulma oli huomioitava. Tämä tarkoitti esimerkiksi sitä, että joitain tietoturvamielessä täsmällisiä termejä jätettiin käyttämättä ja jotain kysymystä tietyllä tavalla syventämättä, jotta malli säilyi helposti ymmärrettävänä ja lähestyttävänä. Valintatilanteissa pyrittiin käyttäjälle parhaimpaan ratkaisuun asiapitoisuutta unohtamatta. Ratkaisut löytyivät yllättävän hyvin. (Toikko & Rantanen 2009, 129.)

Opinnäytetyöhön olisi voinut jälkikäteen ajatellen nostaa vielä enemmän käyttäjänäkökulmaa. Varsinainen käyttäjätestaus jäi tuloksiltaan laihaksi, eikä tietoturvayksikön resurssien vähyyden vuoksi ollut järkevää teettää tätä uudelleen. Käyttäjänäkökulmaa pyrittiin kuitenkin huomioimaan opinnäytetyössä taustahaastattelujen ja materiaaleista kerätyn tiedon sekä teoreettisten lähteiden perusteella. Opinnäytetyön kirjoittaja on tehnyt pitkän työuran ohjaus- ja koulutustehtävissä, mistä oli apua materiaalien työstämisessä käyttäjäystävällisiksi. Mallin kehittämiseen saadut asiantuntijakommentit olivat tärkeitä sisällön kattavuuden näkökulmasta.

6.4 Tulosten arviointi

6.4.1 Odotetut tulokset

Opinnäytetyön tulokseksi odotettiin konkreettista uhka-riskimallinnustyökalua, johon on liitetty itsepalvelumallin käyttöön liittyvät ohjeet, prosessit ja koulutusmateriaalit. Lisäksi odotettiin, että

uhka-riskimallinnuksesta saadaan toistuva ja pysyvä käytäntö, ja että käyttäjien osaamista ja ymmärrystä palvelunsa tietoturvan tasosta pystyttäisiin syventämään. Tulokset ovat odotettuja, eli opinnäytetyössä luotiin uudenlainen uhka-riskimallinnuksen itsepalvelutyökalu tukimateriaaleineen. Uhka-riskimallinnuksen itsepalvelumalli mahdollistaa toistuvan käytön mallin kehittämisen huomioiden. Sekä itsepalvelumalli että materiaalit syventävät käyttäjien osaamista ja ymmärrystä palvelunsa tietoturvan tasosta ja sen tietoturvauhista ja -riskeistä. Mitä enemmän mallia käytetään, sen paremmin asiat tulevat tutuksi ja mallia kehitettäessä voidaan sen sisältöä myös syventää.

6.4.2 Tulosten vertaaminen teoreettiseen viitekehykseen

Tietoturvaan liittyvät strategiat ja johtaminen

Uhka-riskimallinnuksen itsepalvelumallin kehittämisen ja käyttöönoton suunnittelun yhteydessä ilmeni runsaasti yhtäläisyyksiä aiempaan tutkimukseen. Ydinviesti on sama, eli johdon täytyy sitoutua, jotta voidaan onnistua. Käyttöönotossa ja sen jälkeen tarvitaan selkeät tavoitteet, linjaukset ja resurssit, jotta uhka-riskimallinnuksen tekemiselle käytännössä on mahdollisuus. Tarvitaan ymmärrystä muutosprosessista, koska kyseessä on käyttäjille muutos entiseen toimintamalliin. On oltava selkeä ja innostava muutosvisio ja käyttäjien kanssa on saavutettava yhteinen ymmärrys tavoitteista ja toimenpiteistä. Käyttäjien on tärkeää ymmärtää oma roolinsa ja heidän tekemiensä uhka-riskimallinnusten merkitys kokonaisuudessa, sekä lisätä omaa osaamistaan tietoturvauhkien ja -riskien osalta. Uhka-riskimallinnuksen itsepalvelumallilla ja sen tukimateriaaleilla pyritään vahvistamaan ymmärrystä kokonaisuudesta ja työn merkityksestä sekä käyttäjien tietoturvaosaamista. Johdon rooli ja muutoksen toteuttaminen puolestaan kuuluvat käyttöönoton vaiheisiin.

Uhkamallinnus ja tekniset analyysit

Aiemmissa tutkimuksissa uhkamallinnusta pidettiin tärkeänä muuttuvassa maailmassa, jossa uhat vain lisääntyvät. Toimeksiantajakin on tunnistanut tämän, ja siksi uhka-riskimallinnuksen itsepalvelumallia lähdettiin kehittämään. Uhka-riskimallinnuksessa ei menty käyttäjänäkökulman vuoksi kaikista syvimpiin teknisiin uhka-analyyseihin, mutta haluttiin ylipäänsä lisätä uhkatietoisuutta ja ymmärrystä uhkien suhteesta riskeihin. Itsepalvelumalliin sisällytettiin mm. STRIDE, koska se oli käyttäjäystävällinen ja ymmärrettävä uhkien tunnistamismalli. Omaisuuksien arvioinnilla sekä

uhka-riskimallinnuksella pyrittiin toteuttamaan Limnéllin ja muiden (2014, 37) esille nostamat perusasiat: miltä turvataan (uhat ts. tietoturvauhat), mitä turvataan (kohde ts. omaisuudet) ja miten turvataan (hallintakeinot). Uhka-riskimallinnuksen itsepalvelumallia käyttämällä ja tunnistetuille riskeille toimenpiteitä tekemällä organisaation tietoturvallisuuden taso paranee.

Riskienhallinta, riskienhallintatyökalut ja organisaation tietoturvatason arviointi

Aiemmissa tutkimuksissa nostettiin tietoturvan riskienhallintaan liittyen tärkeimmiksi CIA-triadi sekä kriittisten tietojen ja järjestelmien tunnistaminen. Kuten Calder (2023) painotti, paras tieto on järjestelmien omistajilla, koska he tuntevat omaisuudet parhaiten. Tämän vuoksi uhka-riskimallinnuksen itsepalvelumallissa vastuu on siirretty tietoturvayksiköltä palvelujen omistajille. Riskien tunnistaminen, analysointi ja arviointi noudattavat uhka-riskimallinnuksen itsepalvelumallissa ISO-standardeja. Sen sijaan että olisi käännetty ISO 27001 A-liitteen hallintakeinot kysymysmuotoon kuten Yli-Hietasella (2021), tehtiin uhka-riskimallinnuksen itsepalvelumalliin pohdittavaksi kysymyksiä ja esimerkkejä, joiden kautta hallintakeinot saatiin käsiteltyä. Itsepalvelumallista jätettiin pois ne hallintakeinot, joihin mallin käyttäjät eivät pystyneet vaikuttamaan. Näin itsepalvelumallista saatiin käyttäjäystävällisempi eikä sen käyttö vaatinut ISO-standardien osaamista.

Riskienhallinnan onnistuminen organisaatiossa vaatii Ilmosen ja muiden (2016, 41) mukaan sitä, että riskienhallinta tulee osaksi normaalia toimintaa ja johtamista. Tämän saavuttamiseksi pitää työskennellä ahkerasti. Kun organisaation riskitietoisuus kasvaa, siitä tulee vähitellen uusi normaali tapa tehdä töitä. Riskienhallinnan tilan ja kypsyystason tai organisaation tietoturvatason arviointi eivät kuuluneet tämän opinnäytetyön piiriin, mutta tuovat mielenkiintoisia jatkotutkimusmahdollisuuksia koko organisaatiota ajatellen.

Tietoturvatietoisuus ja henkilöstön osaaminen

Organisaation turvallisuus-, riskienhallinta- ja tietoturvakulttuurien syntymiseen liittyvinä seikkoina nostettiin aiemmissa tutkimuksissa esille sekä käyttökelpoiset että helposti saatavilla olevat ohjeistukset ja politiikat, että varsinkin työntekijöiden rooli. Deathin (2023) mukaan tarvitaan sekä viestintää että koulutusta, mutta etenkin tietoa ja työkaluja työntekijöille, jotta tietoturvakulttuuri voi syntyä. Uhka-riskimallinnuksen itsepalvelumallin tavoitteena oli tehdä helposti käytettävä ja löydettävä sekä monipuolinen työkalu, jonka lisäksi tulee tietoa tietoturvaan ja riskienhallintaan

liittyvistä asioista. Näin voidaan tavoitella tietoturva- ja riskienhallintakulttuurien edistämistä sekä tietoturvatietoisuuden nousua.

Hybridimalli

Hajin ja muiden hybridimalli (Haji ym. 2019) oli ainut malli, joka aiemmissa tutkimuksissa muistutti toimeksiantajan uhka-riskimallinnusta. Muita tutkimuksia ei tällaiseen uhkamallinnuksen ja riskimallinnuksen yhdistelmään liittyen löytynyt, joten toimeksiantajan malli on joko melko harvinainen tai sellaisesta ei ole tehty aiemmin juurikaan tutkimusta. Hajin ja muiden luoman hybridimallin mukaisesti muokattu uhka-riskimallinnuksen itsepalvelumalli voisi tuottaa lisää tietoa käyttäjien avuksi esimerkiksi uhkaskenaarioihin ja uhkaprofiileihin sekä haavoittuvuuksien löytämiseen ja uhka-analyysien tekemiseen. Tällaista itsepalvelumallin rikastamista voisi tehdä, kun uhka-riskimallinnuksista saadaan kerättyä dataa tähän pohjaksi. Se auttaisi käyttäjiä tulevien uhka-riskimallinnusten teossa. Kaikilta osin uhka-riskimallinnuksen itsepalvelumallia ei ole syytä muokata niin syvälliseksi kuin hybridimallia, koska silloin malli ei olisi riittävän käytännönläheinen ja vaatisi liian paljon resursseja.

Kaiken kaikkiaan tulokset olivat johdonmukaisia aiempiin tutkimuksiin verraten. Opinnäytetyöstä saadut tulokset olivat odotettuja. Aiemmin ei ole juurikaan tutkittu uhka-riskimallinnuksen kaltaisia hybridimalleja, eikä varsinkaan tällaisesta itsepalvelumallista ollut tutkimusta. Kaupallisissakaan työkaluissa ei uhka- ja riskimallinnuksen suoraan yhdistävää vastaavaa tuotetta ollut tarjolla. Uutta uhka-riskimallinnuksen itsepalvelumallissa aiempaan uhka-riskimallinnukseen verrattuna on itsepalvelukonsepti, mallin sulauttaminen eri viitekehyksiin ja vahvempi käytännönläheisyyteen pyrkiminen.

6.4.3 Tulosten hyödynnettävyys

Opinnäytetyössä kehitetty uhka-riskimallinnuksen itsepalvelumalli on toimeksiantajan käytettävissä ja sen käyttö on vapaasti laajennettavissa. Itsepalvelumallille on luotu prosessit, toimintaohjeet ja mallipohjat. Malli joustaa palvelun mukaan ja skaalautuu tarvittaessa muihinkin tarpeisiin, varsinkin jos siihen tehdään lisäosia eli kysymyspatteristoja tietyistä aihealueista. Uhka-riskimallinnuksen itsepalvelumalli tarjoaa kattavan ja tehokkaan lähestymistavan tietoturvariskien hallintaan. Itsepalvelumallin avulla voidaan tunnistaa, arvioida ja hallita tietoturvariskejä systemaattisesti,

mikä parantaa tietoturvallisuuden tasoa koko organisaatiossa. Vaikka itsepalvelumalli onkin vain "pisara meressä" alati kasvavien kyberuhkien maailmassa, se on tärkeä toimeksiantajalle, tämän tieto-omaisuudelle ja tietoturvallisuudelle.

Uhka-riskimallinnuksen itsepalvelumalli on suunniteltu käyttäjäystävälliseksi, eli sen käyttäjän ei tarvitse olla tietoturvan syväasiantuntija. Malli auttaa käyttäjiä apukysymyksin ja ohjaten oikeaan toimintatapaan. Kun käyttäjä noudattaa mallin ohjeistusta, hän tulee automaattisesti kattaneeksi koko tietoturvariskienhallinnan prosessin ilman, että valintoja tarvitsee erikseen pohtia. Mallin looginen rakenne varmistaa, että kaikki olennaiset riskinhallinnan toimenpiteet ja vaiheet toteutuvat. Tukimateriaalit on kirjoitettu helposti lähestyttäviksi ja konkreettista uhka-riskimallinnuksen tekemistä ja siihen liittyviä kysymyksiä ajatellen. Confluence ja Jira työkaluina ovat jo yleisesti omaksuttuja, joten niiden käyttämisen opiskelusta ei aiheudu lisävaivaa.

Uhka-riskimallinnuksen itsepalvelumalli soveltuu hyvin myös organisaation ulkopuoliseen käyttöön, sillä se ei ole sidonnainen tiettyyn organisaatioon. Mallin käyttöön ei vaikuta se, minkä organisaation ja minkä nimikkeinen henkilö mallia täyttää, vaan se, tunnistaako hän palvelussaan tietoturvauhkia tai -riskejä esimerkiksi pääsynhallinnan aihealueella. Malli on helposti muokattavissa erilaisiin toimintaympäristöihin ja tarvittaessa myös eri työkaluille. Erilaisten uhka-riskimallinnuksen lisäosien rakentamista voisi toteuttaa esimerkiksi organisaatioiden välisenä yhteistyönä.

7 Kehittämisehdotukset ja jatkotutkimusaiheet

Tämän opinnäytetyön tehtävänä oli rakentaa uhka-riskimallinnuksen itsepalvelumalli siihen liittyvine toimintatapoineen ja materiaaleineen. Itsepalvelumallin käyttöönotto ja sen varsinainen käyttövaihe jäivät opinnäytetyön ulkopuolelle. Tässä luvussa käydään ensin läpi kehittämisehdotuksia, jotka voisivat parantaa itsepalvelumallia, kun tietoa käyttöönoton jälkeen on saatavilla enemmän. Sen jälkeen esitellään jatkotutkimusaiheita, jotka voisivat syventää ymmärrystä ja tarjota uusia näkökulmia opinnäytetyön aiheeseen.

7.1 Kehittämisehdotukset

Uhka-riskimallinnuksen itsepalvelumallia kehitettäessä tärkeintä olisi käyttäjänäkökulman huomioiminen. Mallia voisi kehittää käyttäjiltä ja tietoturva-asiantuntijoilta kerättyjen tietojen ja havaintojen perusteella. Toimeksiantajan palvelumuotoilun asiantuntijat voisivat antaa käytettävyysasiantuntemustaan itsepalvelumallin kehittämiseen. Itsepalvelumallin riskien käsittelyn Konkreettiset toimenpiteet -osioon voisi kehittää aihealuekohtaisia esimerkkejä: mitä hallintakeinoja juuri tähän tilanteeseen voisi esimerkiksi olla. Uhka-riskimallinnuksen itsepalvelumallin kehittäminen liittyy jatkuvan parantamisen ajatukseen, joka on esitetty mm. ISO 31000 -standardissa ja seitsemän vaiheen parantamisprosessissa. Seitsemän vaiheen parantamisprosessi olisi hyvä ottaa käyttöön tässä vaiheessa. (SFS-ISO 31000:2018, 8; ITIL® Continual Service Improvement 2011, 40.)

Itsepalvelumalli tehtiin ensivaiheessa palvelujen käyttöön. Mallia voisi laajentaa myös muille yleisille käyttäjäryhmille, esimerkiksi ulkopuolelta hankittaviin palveluihin tai pilvipalveluihin. Mittareita olisi seurattava, kehitettävä ja parannettava, kun uhka-riskimallinnukseen liittyvää tietoa alkaa konkreettisesti palveluilta kertyä. Samalla pystyttäisiin asettamaan tavoitteita, esimerkiksi tyytyväisten käyttäjien lukumäärä, uhka-riskimallinnusten käyttöönoton kattavuus tai uhka-riskimallinnuksen päivityksen tehneiden osuus.

Palvelut tuottavat itsepalvelumallin kautta tärkeitä huomioita tietoturvauhista ja -riskeistä. Uhkapankki voi kerätä tietoa uhka-riskimallinnuksessa löytyvistä riskeistä itselleen, ja rikastaa omaa sisältöään. Tietoa voisi jatkossa hyödyntää myös valvonnassa, jossa voitaisiin miettiä sopivia valvontakeinoja itsepalvelumallin kautta nousseille riskeille. Uhka-riskimallinnus voi tuottamisen lisäksi vastaanottaa tietoa, eli esimerkiksi uhkapankin ja valvonnan tiedoilla voi syventää tietoa tiettyjen aihealueiden kysymysten kohdalla. Uhkamallinnuskyvykkyyksien vahvistamiseen toimeksiantaja voisi käyttää uhkamallinnuskyvykkyyksien prosessialueita (Threat Modeling Capabilities 2023). Tietojen käsittely on alussa melko manuaalista, joten toimeksiantaja voisi pohtia uhka-riskitietokannan tekemistä tai hankkimista. Tietokannasta tulisi olla linkitys esimerkiksi uhkapankkiin, valvontaan ja muihin tarpeellisiin palveluihin.

Kun uhka-riskimallinnuksen itsepalvelumalli nyt otetaan käyttöön, olisi hyvä lisätä tietoturvariskeihin liittyvää tiedottamista. Käyttäjille tulisi näyttää konkreettisin esimerkein uhka-riskimallinnusten itsepalvelumallin käytön vaikutuksia eli tietoturvatilanteen parantumista, riskien vähentymistä

tai riskitason madaltumista. Näin käyttäjät kokisivat, että heidän toiminnallaan on merkitystä ja haluaisivat tehdä jatkossakin töitä tämän tavoitteen eteen. Käyttäjät eivät ole pysyvä, lukittu ihmisjoukko, vaan sekä tiimit, tehtävät että muut muutokset aiheuttavat käyttäjien siirtymistä paikasta toiseen, poistumista, uusien tulemista yms. Olisi varmistettava, että uhka-riskimallinnusta tekevien osaaminen pysyy ajan tasalla koko ajan, ja että käyttäjät saisivat tarvittavaa tukea mallin tekemiseen.

Markkinoilla on uhka- ja riskimallinnuksiin tarkoitettuja tuotteita, mutta ei tällaista varsinaista yhdistelmää. Sellainen on kuitenkin varmasti rakennettavissa. Toimeksiantaja voi selvittää, onko tällainen tietokantapohjainen uhka-riskimallinnustyökalu mahdollista toteuttaa omana työnä, tai löytyisikö markkinoilta mallia, jolla jatkossa voisi toimia. Tämä edellyttää kilpailutusmenettelyn lisäksi huolellista kartoitustyötä, räätälöintiä organisaatiolle sopivaksi sekä tuotteiden itsensä tarkkaa arvioimista tietoturvanäkökulmasta.

Uhka-riskimallinnuksen itsepalvelumallilla tunnistettujen riskien hallintakeinojen priorisoinnin tulisi olla käyttäjille näkyvää. Selkeästi viestityn priorisoinnin avulla resurssit saataisiin keskittymään merkittävimpiin uhkiin. Sekä käyttäjien että johdon tulisi saada heille sopivaa tietoa hallintakeinoista. Uhka-riskimallinnuksista nousseita tietoja voitaisiin myös käyttää johdon päätöksenteon tukena, jolloin joitain haasteita voidaan tunnistaa jopa ennakkoon ja rakentaa entistä parempia hallintakeinoja.

7.2 Jatkotutkimusaiheet

Jatkotutkimuksissa voitaisiin tarkastella laajemmin käyttäjänäkökulmaa, erityisesti käyttäjätyytyväisyyttä, mallin käytettävyyttä ja käyttöastetta. Voisi esimerkiksi tutkia, kuinka tyytyväisiä käyttäjät ovat itsepalvelumalliin ja millaisia asenteita mallia kohtaan on. Käyttäjäkokemusta voisi syventää tutkimalla, koetaanko itsepalvelumalli helppokäyttöiseksi ja mielekkääksi sekä seuraamalla, miten käyttäjät konkreettisesti hyödyntävät mallia eli tekemällä käytettävyystestausta. Olisi tärkeää selvittää, kuinka riittävä tukipalveluiden saatavuus vaikuttaa käyttäjäkokemukseen. Käyttöasteen seuranta antaisi tietoa siitä, miten itsepalvelumallin käyttö yleistyy ja tavoittaako se kaikki, joiden tulisi itsepalvelumallia käyttää.

Itsepalvelumallia voisi jatkotutkimuksissa vertailla aiempaan, tietoturva-asiantuntijavetoiseen uhka-riskimallinnukseen. Olisi tärkeää selvittää, onko itsepalvelumalli yhtä tehokas ja laadukas riskien tunnistamisessa ja hallinnassa kuin asiantuntijavetoinen prosessi. Toinen mahdollinen jatkotutkimusaihe laatuun liittyen olisi uudet innovaatiot: voisi tutkia, tuottaako itsepalvelumallin käyttäminen uusia, innovatiivisia riskienhallinnan lähestymistapoja ja mahdollisuuksia riskienhallinnan kehittämisessä.

Jatkotutkimusaiheena toimintaympäristöön liittyen olisi kiinnostava nähdä, kuinka uhka-riskimallinnuksen jatkuva ja laajamittainen käyttö tuo tietoa päätöksenteon tueksi, ja miten toimeksiantaja hyödyntää tätä tietoa. Lisäksi voisi tutkia, miten itsepalvelumallin käyttö on myöhemmin vaikuttanut tietoturva-asiantuntijoiden työnkuvaan ja vastuunjakoon. Jatkossa voisi analysoida, onko tehokkuus parantunut, kun käyttäjät tarvitsevat vähemmän tietoturva-asiantuntijoiden apua, ja tuoko tämä säästöjä ja millä aikavälillä. Mielenkiintoinen tutkimusaihe olisi myös organisaatioiden välisten yhteistyömahdollisuuksien selvittämisessä: soveltuisiko itsepalvelumalli muidenkin organisaatioiden käyttöön ja löytyisikö yhteistyömahdollisuuksia mallin kattavuuden laajentamiseksi.

Jatkotutkimuksissa voisi tarkastella, onko tietoturvallisuuden taso organisaatiossa parantunut, kun itsepalvelumallia käyttämällä tietoturvauhkia ja -riskejä tunnistetaan säännöllisesti, ja niille määritellään ja toteutetaan hallintakeinoja. Olisi lisäksi kiinnostavaa, että jatkossa selvitettäisiin organisaation tietoturvakulttuurin nykytila sekä asetettaisiin päämäärä, mitä kohti halutaan suunnata. Kuten Selinin (2022) työssä, toimeksiantaja voisi selvittää, kuinka motivoituneita työntekijät olivat oppimaan tietoturvallisuudesta, kuinka tietoturvallisesti he toimivat, sekä kuinka organisaatio voi tukea heitä tietoturvallisemmassa työskentelyssä. Riskienhallinnan tilaa ja kypsyysastetta koko organisaatiossa voisi myös selvittää, kuten mm. Partanen (2020), Baxter (2021) ja Virtaniemi (2023) ovat tehneet.

Lähteet

Ammattikorkeakoulujen opinnäytetöiden eettiset suositukset. 2020. Ammattikorkeakoulujen rehtorineuvosto Arene ry. Viitattu 2.7.2024. https://www.arene.fi/wp-content/uploads/Raportit/2020/AMMATTIKORKEAKOULUJEN%20OPINN%C3%84YTET%C3%96IDEN%20EETTISET%20SUOSITUKSET%202020.pdf?_t=1578480382.

Baxter, A. 2021. Tietoturvallisuuden riskienhallinnan kehittäminen valtioneuvoston kansliassa. Opinnäytetyö, AMK. Laurea-ammattikorkeakoulu, tradenomi (amk), turvallisuus ja riskienhallinta. Viitattu 26.5.2024 https://urn.fi/URN:NBN:fi:amk-2021052110300.

Calder, Alan. 2023. ISO 27001/ISO 27002 - A guide to information security management systems. United Kingdom: IT Governance Publishing. Viitattu 2.5.2024. https://learning.oreilly.com/library/view/iso-27001-iso-27002/9781787784956/, O'Reilly.

Cobb, M. 2023. Risk assessment vs. threat modelling: What's the difference? Artikkeli TehcTarget -sivustolla. Julkaistu 15.6.2023. Viitattu 8.4.2024. https://www.techtarget.com/searchsecurity/tip/Risk-assessment-vs-threat-modeling-Whats-the-difference.

Common Vulnerability Scoring System. N.d. CVSS-luokittelun sivusto. Viitattu 27.7.2024. https://www.first.org/cvss/.

Death, Darren. 2023. Information Security Handbook. Second Edition. United Kingdom: Pact Publishing. Viitattu 2.5.2024. https://learning.oreilly.com/library/view/information-security-handbook/9781837632701/, O´Reilly.

Direktiivi 2022/2555/EU. Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa. Euroopan unionin virallinen lehti 27.12.2022. Viitattu 30.8.2024. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32022L2555.

Field, Alan. 2023. Risk Management and ISO 31000 - A pocket guide. United Kingdom: IT Governance Publishing. Viitattu 2.5.2024. https://learning.oreilly.com/library/view/risk-management-and/9781787784178/, O´Reilly.

Guide for Conducting Risk Assessments. 2012. NIST Special Publication 800-30. Revision 1. Julkaistu syyskuussa 2012. Viitattu 8.8.2024. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Haji, S., Qinq, T. & Soler Costa, R. 2019. A Hybrid Model for Information Security Risk Assessment. International Journal of Advanced Trends in Computer Science and Engineering, 8(1.1), 2019, 100 – 106. Viitattu 8.4.2024. https://www.researchgate.net/profile/Qing-Tan-5/publication/333426720_A_Hybrid_Model_for_Information_Security_Risk_Assessment/links/5f263917458515b729fb42d9/A-Hybrid-Model-for-Information-Security-Risk-Assessment.pdf.

Heinonen, H. 2020. Strategian merkitys tietoturvan johtamisessa. Opinnäytetyö, ylempi AMK. Jyväskylän ammattikorkeakoulu, tekniikan ja liikenteen ala, teknologiaosaamisen johtamisen tutkinto-ohjelma. Viitattu 14.6.2024. https://urn.fi/URN:NBN:fi:amk-2020060417173.

Heinonen, T. 2022. Miten työntekijän tulisi hallita tietoturvallisuuttaan? Opinnäytetyö, AMK. Haaga-Helia ammattikorkeakoulu, tietojenkäsittelyn koulutusohjelma. Viitattu 22.6.2024. https://urn.fi/URN:NBN:fi:amk-2022060214493.

Hytönen, E. 2021. Kokonaisvaltaisen riskienhallinnan viitekehys ammattikorkeakoulussa. Opinnäytetyö, ylempi AMK. Laurea-ammattikorkeakoulu, tradenomi, tulevaisuuden johtaminen ja asiakaslähtöinen palveluliiketoiminta. Viitattu 22.6.2024. https://urn.fi/URN:NBN:fi:amk-202101311732.

Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. 2023. Tutkimuseettinen neuvottelukunta TENK. Tutkimuseettisen neuvottelukunnan HTK-ohje 2023. Tutkimuseettisen neuvottelukunnan julkaisuja 2/2023. Viitattu 2.7.2024. https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf.

Häkkinen, R. 2022. Henkilöstön käsityksiä Oulun poliisilaitoksen tietoturvallisuudesta. Opinnäytetyö, AMK. Centria-ammattikorkeakoulu, liiketalous. Viitattu 25.5.2024. https://urn.fi/URN:NBN:fi:amk-202205047235.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2016. Johda riskejä. Käytännön opas yrityksen riskienhallintaan. Toinen laitos. Finanssi- ja vakuutuskustannus FINVA. Turenki: Hansaprint.

Innovative Compliance Operations Platform - Hyperproof. 2024. Hyperproof-tuotteen etusivu. Viitattu 3.6.2024. https://hyperproof.io/product/.

ISO/IEC 27005:2022:fi. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Ohjeita tietoturvariskien hallintaan. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 28.10.2022. Viitattu 12.4.2024. https://janet.finna.fi/, SFS Online.

ISO/IEC 27019:2017. Information technology — Security techniques — Information security controls for the energy utility industry. Edition 1. Vahvistettu lokakuussa 2017. Viitattu 23.8.2024. https://www.iso.org/standard/68091.html.

IT Risk Management. 2020. Parapet IT Risk Management -tuotteen etusivu. Viitattu 27.5.2024. https://parapet.com/Solutions/IT-Risk-Management.

ITIL® Continual Service Improvement. 2011. 2011 edition. London: TSO. Viitattu 8.8.2024. https://www.kornev-online.net/ITIL/05%20-%20ITIL%20V3%202011%20Continual%20Service%20Improvement%20CSI.pdf.

Jakimova, A. 2022. Tietojärjestelmien riskityöpajojen kehittäminen valtioneuvoston kansliassa. Opinnäytetyö, AMK. Laurea-ammattikorkeakoulu, tradenomi (amk), turvallisuus ja riskienhallinta. Viitattu 24.6.2024. https://urn.fi/URN:NBN:fi:amk-2022120326130.

Jansson, K. 2021. Cybersecurity Threat Modeling on Medical Devices. Opinnäytetyö, AMK. Metropolia-ammattikorkeakoulu, tieto- ja viestintätekniikka. Viitattu 7.6.2024. https://urn.fi/URN:NBN:fi:amk-2021111720495.

Järvinen, P. 2022. Yrityksen tietoturvaopas. Meedia Zone Oü: Kauppakamari.

Kansallinen riskiarvio 2023. 2023. Sisäministeriö. Sisäministeriön julkaisuja 2023:4. Helsinki. Viitattu 14.6.2024. http://urn.fi/URN:ISBN:978-952-324-602-7.

Katakri – tietoturvallisuuden auditointityökalu viranomaisille. N.d. Kansallisen turvallisuusviranomaisen (NSA) internetsivu. Viitattu 26.5.2024. https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille.

Katakri 2020. 2020. Tietoturvallisuuden auditointityökalu viranomaisille. Kansallisen turvallisuusviranomaisen (NSA) julkaisu. Traficomin julkaisusarja. Viitattu 26.5.2024. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246.

Kirtley, N. 2023. DREAD Threat Modeling. Julkaistu 25.9.2023. Viitattu 29.7.2024. https://threatmodeling.com/dread-threat-modeling/.

Kohti parempaa ja sertifioitua digiturvaa. N.d. Digiturvamallin etusivu. Viitattu 26.5.2024. www.digiturvamalli.fi.

Kyberturvallisuuden sanasto. 2018. Turvallisuuskomitea. Sanastokeskus TSK. TSK 52. Helsinki. Viitattu 14.6.2024. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf.

Kälviäinen, I. 2023. Opiskelijoiden tietoturvaosaamisen taso ja kehittämistarve ammattioppilaitoksessa X. Opinnäytetyö, ylempi AMK. Laurea-ammattikorkeakoulu, turvallisuusjohtaminen. Viitattu 8.6.2024. https://urn.fi/URN:NBN:fi:amk-2023061323762.

Lambrinoudakis, C., Gritzalis, S., Xenakis, C., Katsikas, S., Karyda, M., Tsochou, A., Papadatos, K., Rantos, K., Pavlosoglou, Y., Gasparinatos, S., Pantazis, A., Zacharis, A. 2022. Compendium of Risk Management Frameworks with Potential Interoperability. Supplement to the Interoperable EU Risk Management Framework Report. The European Union Agency for Cybersecurity, ENISA. Julkaistu tammikuussa 2022. Viitattu 30.8.2024. https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks.

Lavrenz, S. 2024. Yritysten tietoturvallisuus henkilökunnan näkökulmasta: Tietoturvaopas henkilöstölle. Opinnäytetyö, AMK. Haaga-Helia ammattikorkeakoulu, tradenomi (amk). Viitattu 24.6.2024. https://urn.fi/URN:NBN:fi:amk-202402112785.

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Saarijärven Offset Oy: Docendo.

Liukko, S. & Perttula, S. 2021. Opinnäytetyön raportointi. Jyväskylä: Jyväskylän ammattikorkeakoulu. Viitattu 16.3.2024. https://help.jamk.fi/raportointi/.

Luoma, I. 2023. Strategic Threat Modelling. Opinnäytetyö, ylempi AMK. Metropolia ammattikorkeakoulu, Master of Engineering, Information Technology. Viitattu 24.6.2024. https://urn.fi/URN:NBN:fi:amk-202401111300.

Managing Information Security Risk - Organization, Mission, and Information System View. 2011. NIST Special Publication 800-39. Julkaistu maaliskuussa 2011. Viitattu 8.8.2024. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

Microsoft Threat Modeling Tool threats. 2022. Artikkeli. Julkaistu 25.8.2022. Viitattu 25.7.2024. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

Nair, A. & Greeshma, M. R. 2023. Mastering Information Security Compliance Management. United Kingdom: Packt Publishing. Viitattu 2.5.2024. https://learning.oreilly.com/library/view/mastering-information-security/9781803231174/, O´Reilly.

Nieles, M., Dempsey, K. & Yan Pillitteri, V. 2017. An Introduction to Information Security. NIST National Institute of Standards and Technology. Viitattu 16.3.2024. https://doi.org/10.6028/NIST.SP.800-12r1.

NIST CSRC. N.d. Glossary. The National Institute of Standards and Technology (NIST) Computer Security Resource Center. Teknisten termien sanasto NISTin sivustolla. Viitattu 16.3.2024. https://csrc.nist.gov/glossary.

NIST Risk Management Framework RMF. N.d. NISTin riskienhallintaviitekehyksen aloitussivu. Viitattu 23.7.2024. https://csrc.nist.gov/Projects/risk-management.

OWASP Threat Dragon. 2024. OWASPin Threat Dragon -uhkamallinnustyökalun verkkosivut. Viitattu 9.4.2024. https://owasp.org/www-project-threat-dragon/.

Paananen, R., Soikkeli, M., Starck, M., Aro, M., Kuusisto, T. Rusila, T. & Tuulensuu, T. 2024. Suomen kyberturvallisuusstrategia 2024-2035. Valtioneuvoston kanslian julkaisusarja 2024:11. Helsinki. Julkaistu 10.10.2024. Viitattu 19.10.2024. http://urn.fi/URN:ISBN:978-952-383-376-0.

Partanen, A. 2020. Riskienhallinnan kypsyydenarviointi: case: sisäministeriön hallinnonala. Opinnäytetyö, ylempi AMK. Laurea-ammattikorkeakoulu, turvallisuusjohtaminen. Viitattu 9.6.2024. https://urn.fi/URN:NBN:fi:amk-2020122229858.

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). 2020. Traficomin julkaisuja 13/2020. Kyberturvallisuuskeskus. Liikenne- ja viestintävirasto Traficom. Versio 1.1. Viitattu 13.7.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf.

Prisma - Transparent Reporting of Systematic Reviews and Meta-Analyses. 2024. Prisma 2020 statementin etusivu. Viitattu 18.3.2024. https://www.prisma-statement.org.

Rego Riskienhallinta. 2024. Rego Riskienhallinta -tuotteen etusivu. Viitattu 27.5.2024. https://www.qreform.com/rego/riskienhallinta.

Risk management. 2023. Yhdistyneiden Kuningaskuntien National Cyber Security Centren riskienhallintaopas. Julkaistu 23.6.2023. Versio 2.0. Viitattu 11.8.2024. https://www.ncsc.gov.uk/collection/risk-management.

Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy. 2018. NIST Special Publication 800-37. Revision 2. Julkaistu lokakuussa 2018. Viitattu 4.8.2024. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

Riskienhallinta. N.d. Graniten riskienhallinnan tuotteen etusivu. Viitattu 27.5.2024. https://granite.fi/ratkaisut/riskienhallinta/.

Riva, U. 2021. Tietosuojan johtaminen Organisaation johdon rooli tietosuojan toteuttamisessa. Opinnäytetyö, ylempi AMK. LAB-ammattikorkeakoulu, tradenomi (YAMK), uudistava johtaminen. Viitattu 26.5.2024. https://urn.fi/URN:NBN:fi:amk-2021092017885.

Rousku, K. 2017. VAHTI – ohje riskienhallintaan. Julkaisun on toimittanut Kimmo Rousku. Valtiovarainministeriön julkaisuja 22/2017. Helsinki: Valtiovarainministeriö, Julkisen hallinnon ICT. Viitattu 24.8.2024. http://urn.fi/URN:ISBN:978-952-251-862-0.

Salminen, J. 2022. Muutoksen johtaminen. Matkaopas organisaation muutosmatkalle. Birk. Helsinki: Grano.

Security and Privacy Controls for Information Systems and Organizations. 2020. NIST Special Publication 800-53. Revision 5. Julkaistu lokakuussa 2020. Viitattu 6.8.2024. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Selin, M. 2022. Tietoturvakulttuurin kartoittaminen organisaatiossa X. Opinnäytetyö, AMK. Laurea-ammattikorkeakoulu, tradenomi (amk), turvallisuus ja riskienhallinta. Viitattu 24.6.2024. https://urn.fi/URN:NBN:fi:amk-2022122131249.

SFS-EN ISO 27799:2016. Terveydenhuollon tietotekniikka. Tiedonhallinta terveydenhuollossa standardin ISO/IEC 27002 avulla. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 19.8.2016. Viitattu 23.8.2024. https://janet.finna.fi/, SFS Online.

SFS-EN ISO/IEC 27000:2020. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Helsinki: Suomen standardisoimisliitto SFS. Vahvistettu 28.2.2020. Viitattu 12.4.2024. https://janet.finna.fi/, SFS Online.

SFS-EN ISO/IEC 27001:23. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 4.8.2023. Viitattu 12.4.2024. https://janet.finna.fi/, SFS Online.

SFS-EN ISO/IEC 27002:2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 18.11.2022. Viitattu 21.4.2024. https://janet.finna.fi/, SFS Online.

SFS-EN ISO/IEC 27017:2021:en. Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015). Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 29.1.2021. Viitattu 23.8.2024. https://janet.finna.fi/, SFS Online.

SFS-ISO 31000:2018. Riskienhallinta. Ohjeet. Helsinki: Suomen standardisoimisliitto SFS. Vahvistettu 23.2.2018. Viitattu 12.4.2024. https://janet.finna.fi/, SFS Online.

Shacklett, M. E. N.d. Definition attack vector. TechTarget -sivuston artikkeli. Viitattu 3.9.2024. https://www.techtarget.com/searchsecurity/definition/attack-vector.

Souppaya, M. & Scarfone, K. 2016. Guide to Data-Centric System Threat Modeling. Draft NIST Special Publication 800-154. Julkaistu maaliskuussa 2016. Viitattu 23.7.2024. https://csrc.nist.gov/files/pubs/sp/800/154/ipd/docs/sp800_154_draft.pdf.

Srivathsav, R. 2020. A little more than the CIA Triad! Blogikirjoitus Medium-sivustolla. Julkaistu 15.10.2020. Viitattu 23.8.2024. https://medium.com/coinmonks/a-little-more-than-the-cia-triad-6c54d6263083.

Stamatiou, A. 2022. Rego-riskienhallinnan työkalun käyttöönotto virastojen riskienhallinnan arviointiin. Opinnäytetyö, AMK. Laurea-ammattikorkeakoulu, tradenomi (amk), turvallisuus ja riskienhallinta. Viitattu 8.6.2024. https://urn.fi/URN:NBN:fi:amk-2022051810129.

Stenbäck, M. 2020. Tietoturvan näkökulma vaatimusmäärittelyssä ja järjestelmäsuunnittelussa. Opinnäytetyö, ylempi AMK. Tampereen ammattikorkeakoulu, tietojärjestelmäosaamisen koulutus YAMK. Viitattu 24.6.2024. https://urn.fi/URN:NBN:fi:amk-2020113025145.

The NIST Cybersecurity Framework (CSF) 2.0. 2024. NIST CSWP 29. Julkaistu 26.2.2024. Viitattu 4.8.2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

Threat Modeling Capabilities. 2023. Julkilausuma uhkamallinnuskyvykkyyksistä. Viitattu 20.10.2024. https://www.threatmodelingmanifesto.org/capabilities/.

Threat Modeling Manifesto. 2020. Julkilausuma uhkamallinnuksen perusperiaatteista. Viitattu 24.6.2024. https://www.threatmodelingmanifesto.org/.

Todennetusti toimivia ratkaisuja. 2024. Arter Oy:n tuotteiden etusivu. Viitattu 26.5.2024. www.arter.fi.

Toikko, T. & Rantanen, T. 2009. Tutkimuksellinen kehittämistoiminta. Tampere: Tampereen yliopistopaino - Juvenes Print. 3. korjattu painos. Viitattu 12.4.2024. https://urn.fi/URN:ISBN:978-951-44-7732-4.

Traficom/18410/09.00.02/2023. Liikenne- ja viestintävirasto Traficomin suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä. Luonnos. Viitattu 30.8.2024. https://www.lausuntopalvelu.fi/FI/Proposal/DownloadProposalAttachment?proposalId=ebc51269-712e-4115-b137-b0b2a710dac4&attachmentId=22133.

Tsohou, A., Karyda, M., & Kokolakis, S. 2015. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. Computers & Security, 52, 128-141. Viitattu 8.9.2024. https://doi.org/10.1016/j.cose.2015.04.006.

Tuomi, S. & Latvala, E. 2022. Opinnäytetyön ohjaajan käsikirja. Jyväskylä: Jyväskylän ammattikorkeakoulu. Viitattu 15.3.2024. https://help.jamk.fi/opinnaytetyon-ohjaus/.

UV, Tony. 2023. What is the PASTA Threat Model? Artikkeli VerSpriten sivustolla. Julkaistu 29.6.2023. Viitattu 25.7.2024. https://versprite.com/blog/impact-and-probability-in-threat-modeling/.

Virtaniemi, S. 2023. Sisäministeriön riskienhallinnan kehittäminen. Opinnäytetyö, ylempi AMK. Laurea-ammattikorkeakoulu, turvallisuusjohtaminen. Viitattu 8.6.2024. https://urn.fi/URN:NBN:fi:amk-2023102327855.

Väänänen, K. 2021. ISO/IEC 27001 mukainen puuteanalyysi Keski-Suomen alueen yritykselle. Opinnäytetyö, AMK. Jyväskylän ammattikorkeakoulu, tieto- ja viestintätekniikka. Viitattu 25.5.2024. https://urn.fi/URN:NBN:fi:amk-2021112922283.

Wallenius, H. 2023. Henkilöstön tietoturvatietoisuuden vahvistaminen. Opinnäytetyö, AMK. Laurea-ammattikorkeakoulu, tradenomi (amk), turvallisuus ja riskienhallinta. Viitattu 25.5.2024. https://urn.fi/URN:NBN:fi:amk-202302132342.

What is Threat Modeling? 2024. Artikkeli VerSpriten sivustolla. Viitattu 29.7.2024. https://versprite.com/security-resources/what-is-threat-modeling/.

Yli-Hietanen, K. 2021. ISO/IEC 27001 -standardin sertifiointiin valmistautuminen IT-alan yrityksessä. Opinnäytetyö, AMK. Satakunnan ammattikorkeakoulu, tuotantotalouden tutkinto-ohjelma. Viitattu 8.6.2024. https://urn.fi/URN:NBN:fi:amk-202105077576.

Ylinen, P. 2023. Porvoon kaupunginkirjaston tietoturvakartoitus. Opinnäytetyö, AMK. Kaakkois-Suomen ammattikorkeakoulu, tekniikan ammattikorkeakoulututkinto, kyberturvallisuus. Viitattu 25.5.2024. https://urn.fi/URN:NBN:fi:amk-2023053015845.