Sosiaali- ja terveysalan tietoturvavaatimusten kartoitus ja valmistautuminen NIS2-direktiivin soveltamiseen

Jonathan Berts

2025 Laurea

Laurea-ammattikorkeakoulu

Sosiaali- ja terveysalan tietoturvavaatimusten kartoitus ja valmistautuminen NIS2-direktiivin soveltamiseen

Jonathan Berts
Tietojenkäsittely, kyberturvallisuus
Opinnäytetyö
Toukokuu 2025

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tietojenkäsittelyn koulutusohjelma, kyberturvallisuus

Tradenomi (AMK)

Jonathan Berts

Sosiaali- ja terveysalan tietoturvavaatimusten kartoitus ja valmistautuminen NIS2-direktiivin soveltamiseen

Vuosi 2025 Sivumäärä 58

Euroopan unionin NIS2-direktiivi on ollut voimassa jo muutaman vuoden ajan, mutta helmikuuhun 2025 mennessä Suomi ei ole vielä saattanut sitä osaksi kansallista lainsäädäntöä. Tämä opinnäytetyö tarkastelee erään julkisen sosiaali- ja terveysalan organisaation toimia sen valmistautuessa tuleviin lainsäädännöllisiin vaatimuksiin kehittämällä kattavan tietoturvallisuuden hallintajärjestelmän (ISMS, Information Security Management System). Opinnäytetyö on toteutettu päiväkirjamuotoisena raporttina kahdeksan viikon seurantajakson ajalta. Luottamuksellisuussyistä toimeksiantaja on anonymisoitu.

Päiväkirjamuotoisen raportoinnin lisäksi opinnäytetyöhön sisältyy visuaalinen käsitekartta sosiaali- ja terveysalalle soveltuvista keskeisistä laeista, asetuksista ja vaatimuksista. Käsitekartta sisältää myös valikoituja kansallisia ja kansainvälisiä standardeja ja viitekehyksiä, kuten ISO/IEC 27000 -sarjan standardit ja CIS:n tietoturvakontrollit, jotka tukevat vahvan tietoturvallisuuden hallintajärjestelmän rakentamista ja jatkuvaa kehittämistä.

Seurantajakson loppuun mennessä ISMS-toteutushanke on vielä käynnissä. ISMS-toteutushankkeen tehokkaan etenemisen varmistamiseksi tunnistettiin keskeisiä kehittämiskohteita. Huomionarvoista on, että jakson loppupuolella NIS2-direktiivin toimeenpaneva kansallinen lainsäädäntö hyväksyttiin, mikä lisäsi organisaation velvoitetta noudattaa uusia sääntelyvaatimuksia.

Visuaalinen koonti sosiaali- ja terveysalan erityisvaatimuksista ja tukityökaluista voi myös toimia käytännöllisenä perehdytysmateriaalina organisaation tietohallintoyksikköön tuleville uusille ICT-asiantuntijoille.

Asiasanat: SOTE, Sosiaali- ja terveys, NIS2, ISMS, tietoturva

Laurea University of Applied Sciences **Abstract**

Degree Programme in Business Information Technology

Bachelor of Business Administration

Jonathan Berts

Mapping of information security requirements in the social and healthcare sector and preparing for the implementation of the NIS2 directive

Year 2025 Pages 58

The European Union's NIS2 Directive has been in force for several years; however, as of February 2025, Finland has yet to enact the corresponding national legislation. This thesis examines the efforts of a public social and healthcare organization to prepare for the forthcoming legal requirements by developing a comprehensive Information Security Management System (ISMS). The study is structured as a diary-based report covering an eight-week observation period. For reasons of confidentiality, the commissioning organization has been anonymized.

In addition to the diary-based documentation, the thesis includes a visual concept map of the key laws, regulations, and requirements applicable to the social and healthcare sector. The concept map also integrates selected national and international standards, frameworks, and benchmarks, such as the ISO/IEC 27000 series and the CIS Controls, that provide a foundation for building and continuously improving a robust ISMS.

By the end of the observation period, the ISMS implementation project was still ongoing. Key areas requiring further development to ensure the effective advancement of the ISMS implementation project were identified. Notably, near the end of the observation period, the Finnish legislation transposing the NIS2 Directive was approved, thereby intensifying the organization's obligation to comply with the new legislative requirements.

The visual mapping of the social and healthcare sector-specific requirements and relevant tools may also serve as a practical onboarding aid for new ICT professionals within the organization's information security unit.

Keywords: SOTE, Social and healthcare, NIS2, ISMS, Information security

Sisällys

1 Johdanto

NIS2-direktiivi on velvoittanut organisaatiot ja valtiot koko EU:ssa ottamaan kyberturvallisuuden aiempaa vakavammin. Kyse ei ole vain teknisten suojausten parantamisesta, vaan myös johtamisvastuusta, riskienhallinnasta ja jatkuvuuden turvaamisesta. Jokainen EU-maa on velvoitettu saattamaan direktiivi osaksi kansallista lainsäädäntöään, mikä tarkoittaa, että sääntelyn käytännön toteutus ja valvonta vaihtelevat maittain. Julkisella sektorilla varsinkin sosiaali- ja terveydenhuollon toimialat ovat tiukan valvonnan alaisina, sillä ne kuuluvat NIS2-direktiivin mukaan olennaisiin tahoihin kriittisillä aloilla ja käsittelevät sekä säilyttävät suuria määriä arkaluonteisia tietoja.

Tämän opinnäytetyön tavoitteena on edistää yhden Suomen suurimmista työnantajista tietoturvan hallintajärjestelmää (ISMS) hyödyntämällä ISO/IEC 27001- ja 27002-standardeja sekä soveltuvin osin muita kriteeristöjä tai viitekehyksiä. Standardien avulla arvioidaan ja kehitetään organisaation turvallisuustoimenpiteitä rakenteellisesti sekä varmistetaan niiden vaatimustenmukaisuus EU:n NIS2-kyberturvallisuusdirektiivin näkökulmasta. Lisäksi organisaatiota valmistellaan näin tulevaan Suomen lainsäädäntöön liittyen NIS2-direktiiviin.

NIS2-direktiivin vaatimukset eivät kuitenkaan ole ainoita velvoitteita, jotka kohdistuvat sosiaali- ja terveydenhuollon toimialalle. Opinnäytetyön toinen tavoite on kartoittaa ja selkeyttää, mitkä tietoturvavaatimukset koskevat sosiaali- ja terveydenhuollon toimialaa sekä millaisia työkaluja ja dokumentteja on tarjolla niiden soveltamisen tueksi niin kansallisella kuin kansainväliselläkin tasolla.

Opinnäytetyö on päiväkirjamuotoinen ja sen toteutusaika on kahdeksan viikon jakso keväällä 2025, tarkemmin 24.2.2025–18.4.2025. Pääteksti on jaettu alalukuihin, joista kukin edustaa yhtä viikkoa ja alkaa tavoitesuunnitelmalla sekä päättyy yhteenvetoon viikon saavutuksista. Tietoturvasyistä tämä opinnäytetyö on tarkoituksella kirjoitettu siten, että toimeksiantajaan liittyviä tietoja ei voida tunnistaa, ja vain muutama sovellus mainitaan nimeltä.

Toimeksiantajana toimii kaupungin sosiaali- ja terveyspalveluiden (SOTE) tietohallinnon alainen yksikkö, jossa toimii myös toimialan tietoturvatiimi. Organisaation ja sen tietoturvan hallintajärjestelmän hankkeen laajuuden vuoksi tämä opinnäytetyö on rajattu SOTE-toimialaa koskeviin velvoitteisiin ja vaatimuksiin. Painopiste on SOTEn ISMS:n aliprojektien kehittämisessä, mutta kaikki ajanjakson aikana suoritetut tehtävät, jotka liittyvät ISMS:n toteutushankkeeseen, on dokumentoitu. Tavoitteena on rakentaa lisää vankkoja peruskiviä, joiden pohjalta voidaan kehittää entistä vahvempi ISMS-järjestelmä.

ChatGPT 4o:ta on käytetty opinnäytetyön kieliasun tarkasteluun. Keskeiset käsitteet on selitetty taulukossa 1.

Käsite	Selite
CIS, Center for Internet Security	Voittoa tavoittelematon organisaatio, joka kehittää parhaita käytäntöjä, ohjeistuksia ja työkaluja organisaatioiden kyberturvallisuuden parantamiseksi.
CSIRT, computer security incident response team	Tietoturvaloukkauksiin reagoiva ja niitä tutkiva yksikkö, tämän opinnäytetyön kontekstissa EU:n jäsenmaiden kansallisella tasolla.
CSOC, Cyber Security Operations Center	Organisaatiokohtainen kyberturvallisuuden valvontakeskus, joka vastaa organisaation tietoturvatapahtumien jatkuvasta seurannasta, analysoinnista ja niihin reagoimisesta.
GAP analysis, suom. Puute- tai Kuiluanalyysi	Analyysi, jossa vertaillaan nykytilan ja tavoitetilan välistä eroa, jotta voidaan tunnistaa kehityskohteet ja parannettavat alueet organisaation toiminnassa.
In-house-yhtiö	Osakeyhtiömuotoinen toimija, joka on valtion, kunnan tai kuntayhtymän omistama ja niiden määräysvallassa. Tällaiselta yhtiöltä tehtävät hankinnat voidaan toteuttaa ilman hankintalain edellyttämää kilpailutusta.
ISO/IEC 27000 standardiperhe	Ryhmä kansainvälisen tietoturvanhallinnan standardeja, jotka tarjoavat ohjeistuksia ja vaatimuksia tietoturvan hallintajärjestelmien suunnitteluun, toteutukseen ja jatkuvaan parantamiseen.
ISMS, Information security management system, suom. Tietoturvan hallintajärjestelmä	Järjestelmällinen lähestymistapa tietoturvan hallintaan, jonka tarkoituksena on

	suojata organisaation tiedot riskeiltä ja varmistaa niiden luottamuksellisuus, eheys ja saatavuus.
MCSB, Microsoft Cloud Security Benchmark	Microsoftin kehittämä kyberturvallisuuden viitekehys, joka tarjoaa parhaita käytäntöjä ja suosituksia pilvipalveluiden turvallisuuden parantamiseksi.
NIS2-direktiivi (engl. Network and Information Security Directive)	Euroopan unionin kyberturvallisuusdirektiivi, joka velvoittaa keskeisiä toimijoita parantamaan kyberturvallisuuttaan ja raportointikäytäntöjään.
NIST, National Institute of Standards and Technology	Yhdysvaltain liittovaltion standardointi- ja teknologiainstituutti, joka kehittää ja edistää standardeja, mittaustekniikoita ja parhaita käytäntöjä muun muassa teknologian, tietoturvan ja innovaatioiden tukemiseksi.
NIST Cybersecurity Framework (CSF) 2.0	NISTin kehittämä viitekehys, joka auttaa organisaatioita hallitsemaan ja parantamaan kyberturvallisuuttaan järjestelmällisesti ja riskiperusteisesti.
NIST SP 800-53	NISTin laatima tietoturvakontrollien kokoelma, joka tarjoaa kattavat suositukset liittovaltion tietojärjestelmien ja organisaatioiden suojaamiseen.
RACI	Vastuujen määrittelymalli, joka selkeyttää roolit ja vastuut projektin tai prosessin eri vaiheissa ja sisältää neljä roolia: Responsible (vastuullinen), Accountable (vastuussa), Consulted (kuultu) ja Informed (tietoinen).
SaaS palvelu	Pilvipalvelumalli, jossa ohjelmistot tarjotaan käyttäjille internetin kautta tilausperusteisesti ilman, että käyttäjän tarvitsee huolehtia ohjelmiston asennuksesta tai ylläpidosta.

SIEM	Tietoturvaratkaisu, joka kerää, analysoi ja korreloi tietoturvatapahtumia ja lokitietoja organisaation ympäristössä, auttaen havaitsemaan mahdollisia uhkia ja reagoida niihin
SOAR	Tietoturvaratkaisu, joka yhdistää orkestroinnin, automaation ja reagoinnin, jotta organisaatiot voivat tehokkaasti hallita ja vastata tietoturvauhkiin.
SOTE, Sosiaali- ja Terveydenhuollon toimiala	Kaupungin SOTE kattaa kansalaisten sosiaalipalvelut ja terveydenhuollon palvelut sekä niiden järjestämisen ja rahoittamisen.
Splunk	Analytiikka- ja lokinhallintatyökalu, joka kerää, indeksoi ja visualisoi suuria määriä kone- ja liikenneaineistoa, auttaen organisaatioita havaitsemaan ja ratkaisemaan tietoturvaongelmia sekä parantamaan operatiivista tehokkuutta. Splunk tarjoaa muun muassa SIEM- ja SOAR-ratkaisuja.

Taulukko 1 Keskeiset käsitteet

2 Nykytilanne

Tässä luvussa selitän oman työkuvani ja taustani sekä organisaation SOTE-toimialan nykytilanteen NIS2-direktiivin näkökulmasta. Toimialan sidosryhmiä on osittain avattu, mutta jotta organisaatio pysyy mahdollisimman hyvin anonymisoituna eikä tiettyjä palveluntarjoajia paljastuisi, en käsittele niitä tarkemmin. Viranomaiset ja muut organisaatiot, jotka koskevat kaikkia SOTE-toimialoja, on kuitenkin mainittu nimeltään.

2.1 Oma työ ja osaaminen

Taustaltani olen sairaanhoitaja, ja aloitin kyberturvallisuusopintoni syksyllä 2022. Opinnäytetyön kirjoittamisen alkaessa minulla on 13 kuukauden kokemus toimialan tietohallintoyksikön sovelluspalvelujen alayksikössä ICT-asiantuntijana. Suurin osa työstäni keskittyy järjestelmiin, joita käytin sairaanhoitajana. Työrooliini kuuluu erilaisten järjestelmien käyttäjähallinta ja ylläpito, asiakastuki, palautekäsittely, sekä identiteetin- ja pääsynhallinta (IAM) eri

työkalujen avulla, esimerkiksi Active Directory (AD). Olen myös käyttänyt puolet työajastani tietoturvatiimin tehtäviin viime syksystä lähtien, noin neljä kuukautta. Näihin tehtäviin kuuluu pääasiassa ISMS-toteutushankkeen aliprojektit, asiakastuki ja -neuvonta tietoturvaan liittyen, sekä uusien tai päivitettyjen sovellusten tietosuojan vaikutuksenarvioihin (TSVA) osallistuminen.

Työn monimutkaisuuden ja monivivahteisuuden takia tarvitaan ongelmanratkaisukykyä ja loogista ajattelua ja usein myös teknistä osaamista, erityisesti järjestelmien ja hallintakeinojen ymmärrystä. Tehtävien priorisointi ja järjestäminen ovat myös tärkeitä, koska usein aikataulu on hyvin tiukka. Vuorovaikutustaidot ovat ehdottomasti myös tärkeät, sillä tehdään melko tiivistä yhteistyötä eri toimijoiden ja asiakkaiden kanssa; empatia on erityisen tärkeää asiakaspalvelussa. Itsensä ohjaaminen ja tiedonhankinta ovat myös tärkeitä, sillä joskus on osattava löytää ratkaisuja itsenäisesti.

Vaikka olen melko tuore IT-alalla, taustalla on vahva kiinnostus tietotekniikkaan, jonka ansiosta pystyn suorittamaan nykyiset työtehtävät melko itsenäisesti. Tietoturvaan liittyvät asiat ovat kuitenkin vaativampia sekä ajoittain hyvin yksityiskohtaisia ja näissä työtehtävissä tarvitsen tukea sekä ohjausta. Omana tavoitteena on keskittyä enemmän tietoturvaan liittyviin tehtäviin lähitulevaisuudessa ja kehittää omaa osaamista myös vapaa-ajalla. Painopiste tulee olemaan riskinhallinnassa ja myös teknisessä osaamisessa, varsinkin päätelaite- ja verkkoturvallisuudessa.

2.2 Vuorovaikutustaidot

Työssäni vuorovaikutustaidot ovat melko keskeisiä. Tiimin ja yksikön sisällä tehdään tiivistä yhteistyötä, ja selkeä kommunikaatio on hyvin tärkeää. Asiakastuessa empatia on olennainen osa, joka tulee suhteellisen luonnollisesti itselleni, erityisesti hoitoalan taustan ansiosta. Työ ei ole tietenkään ilman haasteita, ja silloin kun tunteet käyvät kuumana, olipa kyseessä asiakkaan tai palveluntarjoajan kanssa käytävä keskustelu, on tärkeää pysyä asiallisena ja pysyä aiheessa.

Omien vuorovaikutustaitojeni osalta olen huomannut, että usein olen taipuvainen puhumaan ensin ja ajattelemaan vasta myöhemmin, vaikka olisi suotavampaa toisin päin. Tämä on ollut aktiivisessa työskentelyssäni kehityskohteena siitä asti, kun aloitin nykyisessä työpaikassani. Tietohallinnassa ja varsinkin tietoturvallisuusaiheissa on tärkeää olla selkeä ja ytimekäs viestinnässä ja pyrkiä olemaan mahdollisimman perusteellinen liioittelematta. Haluaisin kuitenkin kuvitella, että vuorovaikutustaitojeni vahvuuksia ovat oma-aloitteisuus, aktiivisuus ja uteliaisuus sekä tiimityöskentelytaito.

Liittyen sidosryhmien kanssa kommunikaatioon, niin sähköposti taitaa olla tärkein viestintäkanava, joka on kaikilla käytössä. Sisäisesti käytetään Microsoft Teams-sovellusta ahkerasti, niin

pika-viestintätoimintona kuin kokousten pitämiseen. Mikäli on jatkuva projekti tai muuten tärkeä asia käsiteltävänä, Teams-kokous on tavallisin tapa koota osallistujat ulkopuolisista sidosryhmistä mukaan. In-house-yhtiön kanssa kommunikoidaan taas pääasiassa tekemällä tikettejä organisaation service deskille.

2.3 Toimialan nykytilanne NIS2-direktiivin näkökulmasta

Yksi organisaation suurimmista projekteista liittyen tietoturvaan on ISMS-toteutushanke, jolla pyrimme saamaan entistä ennen parempaa ja tehokkaampaa tietoturvahallintaa. Toimivalla ISMS-järjestelmällä halutaan turvata tietovarannot ja helpottaa riskienhallintaa ISO/IEC 27001 ja 27002-standardeilla. Tähän liittyy tietoturvariskien hallintaprosessi, hallintokeinojen kypsyysarviointi, jonka perusteella voidaan löytää kriittisimmät kehityskohteet, ja keskitetty häiriöhallinta, joka liittyy myös NIS2-direktiivin vaatimuksiin liittyen tapahtumaraportointiin.

Jokaisella aliprojektilla on omat haasteet ja suurin haaste tällä hetkellä on todennäköisesti kommunikaatio. Vaikka tietovarannot ja muut digitaaliset resurssit olisivat hyvin turvattu, niin toimialalta puuttuu osittain selkeää dokumentaatiota siitä, miten tietovarannot ja prosessit ovat turvattu. Tähän liittyy myös se problematiikka, että monet palvelut on ulkoistettu palveluntarjoajille ja he ovat velvoitettuja jakamaan tietoa ainoastaan sopimuksen puitteissa.

Myös keskitetty häiriöhallinta on näin hyvin haasteellista, koska palveluntarjoajat hoitavat pitkälti oman tietoturvansa eivätkä välttämättä raportoi kuin suurista tietoturvatapahtumista organisaatiolle. Tavoitteena olisi saada informaatio kulkemaan järkevästi ja tehokkaasti niille, jotka hyötyvät tästä tiedosta tai tarvitsevat sitä päätöksentekoon. Tämä on myös tärkeää NIS2-direktiivin artiklan 23 raportointivaatimusten kannalta, jossa velvoitetaan organisaatiot raportoimaan merkittävistä tietoturvapoikkeamista 24 tunnin sisällä ja laatimaan 72 tunnin sisällä kattavan raportin tapahtumasta. (Direktiivi 2022/2555/EU.)

2.4 Sidosryhmät

Sidosryhmiä on runsaasti, sekä sisäisiä että ulkoisia. Organisaatio on erittäin suuri ja sen toimialoja johtaa organisaation kanslia, josta määrätään organisaatiokohtaiset linjaukset. Koko organisaation laitteiden hallinta ja ylläpito on keskitetty in-house-yhtiöön, ja käytössä olevien sovellusten hallinto ja ylläpito kuuluvat toimialoille. Sovelluksia on yli sata, joilla on omat palveluntarjoajat ja asiakastukea. Sosiaali-, terveystoimiala, SOTE, on myös palveluntarjoaja ja asiakkaat ovat käytännössä kaikki kunnan asukkaat, eli palveluiden käyttäjät. Toimialan tietohallinto on palveluntuottaja ja toimii tukena tietohallintaan liittyvissä asioissa toimialan muille työntekijöille. Koska organisaatio toimii julkisella sektorilla niin kaupunginhallitus vastaa, että organisaatio täyttää tietosuojalainsäädännön mukaiset velvoitteet ja valvoo velvoitteiden toteutumista.

Sosiaali-, terveys- ja pelastustoimialan ulkoisiin sidosryhmiin kuuluu vielä viranomaiset, joka valvovat tai ovat muuten tekemisissä kansalaisten sosiaali-, terveys- ja pelastuspalveluiden kanssa. Näihin kuuluu Digi- ja väestötietovirasto DVV, Sisäministeriön pelastusosasto SMPEI, Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira, Terveyden ja Hyvinvoinnin laitos THL, Tietosuojavaltuutetun toimisto TSV, ja Traficomin Kyberturvallisuuskeskus.

Monet palvelimet ja LAN- sekä WAN-verkot ovat ulkoistettu ja niiden tietoturvahallinta on pääosin palvelutarjoajien vastuulla, toisaalta toimialan tietyt sisäiset verkot ja miten tietoturva toteutuu päätepisteissä, on in-house-yhtiön vastuulla. Sovellusten ja SaaS-palvelujen tietoturva on palveluntarjoajien vastuulla, mutta sovellusten tietoturvallinen käyttö on taas toimialan vastuulla.

2.5 Kehittäminen ja opinnäytetyön tavoitteet

Optimointi ja tehostaminen ovat lähellä sydäntäni, joten pohdinta siitä, kuinka prosesseja voidaan tehostaa ja resursseja säästää, on usein mielessäni työtehtäviä suorittaessani. ISMS-toteutushanke ylipäätänsä on valtava projekti, mutta tavoitteeni on kuitenkin edistää siihen liittyvää aliprojektia merkittävällä tavalla tämän seurantajakson aikana. Yleistavoitteena on kartoittaa toimialaan kohdistuvia tietoturvavaatimuksia sekä valmistautua NIS2-direktiivin vaatimuksiin, jonka lainsäädäntö olisi pitänyt olla valmiina jo viime syksynä, eli aikataulu on hyvin kiireellinen.

Tämän perusteella ja ottaen huomioon, että yritän työstää melko itsenäisesti joitain osia tietyistä alaprojekteista, niin keskityn tässä seurantajaksossa muutamiin ISO/IEC 27001:2023 A-liitteessä mainittuihin hallintakeinojen kypsyysarviointeihin. Niiden perusteella voidaan luoda puute-/kuiluanalyysit (eng. GAP-analysis) ja nostaa huomioitavat riskit esille. Kypsyysarviointien lisäksi nostan tässä opinnäytetyössä esille ISMS-toteutushankkeen näkökulmasta kiinnostavia tai muuten tärkeitä tietoturvaan liittyviä ongelmia ja tehtävänantoja, jotka tulevat seurantajakson aikana esille.

3 Päiväkirjaraportointi

Tässä luvussa esitellään opinnäytetyön ydin: päiväkirjaraportti. Jokainen alaluku edustaa yhtä työviikkoa. Alaluku alkaa viikon suunnitelmalla ja päättyy viikon analyysiin. Näiden väliin sijoittuvat työpäivät, joista jokaisella on oma alaotsikkonsa muodossa ”viikonpäivä päivämäärä”. Viikon analyysissä on koottu ja tarkasteltu viikon aikana kertynyttä materiaalia alaotsikon ”Viikkoanalyysi” alle. Alaotsikoiden suuren määrän vuoksi niitä ei ole numeroitu; ainoastaan uudet viikot on numeroitu.

Osa työpäivien kuvauksista on hyvin lyhyitä, koska jouduin priorisoimaan sovelluspalvelujen tehtäviä, kuten häiriötikettejä ja käyttöoikeuksien hallintaa, tietoturvaan liittyvien tehtävien edelle.

3.1 Viikko 1

Ensimmäisen viikon tavoitteeni ovat yksinkertaiset, mutta käytännössä melko haastavat: tutustua ISMS-hankkeeseen ja selvittää, missä vaiheessa kukin aliprojekti on. Käytännössä tämä tarkoittaa projektin hahmottamista, konkreettisten tavoitteiden ymmärtämistä ja miten tavoitteet aiotaan saavuttaa, hahmottamaan mitä on jo tehty ja mitkä haasteet on tunnistettu. NIS2-direktiivin vaatimusten läpikäynti on myös olennaista ISMS-toteutushankkeen tavoitteiden hahmottamiseksi. Avuksi on myös ISO/IEC 27001:2023 (jäljempänä ISO 27001) A-liitteen hallintakeinot, jonka perusteella voidaan pilkota ISMS-projektin aliprojekteihin ja tavoitteeni olisi edistää muutama näistä aliprojekteista merkittävästi seuraavien kahdeksan viikon aikana.

Viime syksynä valtiovarainministeriö julkaisi uudet pilvipalvelulinjaukset, ja organisaatiollamme on tavoitteena hyödyntää julkipilvipalveluita, noudattaen standardisoituja tietoturvan hallintokeinoja. Tietoturvapäällikkö suositteli jo aiemmin, että tutustuisin Microsoft Cloud Security Benchmarkiin (MCSB), joka tarjoaa suositeltuja parhaita käytäntöjä ja ohjeita monipilviympäristöjen tietoturvan parantamiseen. Tavoitteena on ehtiä ainakin tutustumaan Microsoftin omaan materiaaliin tähän liittyen.

Maanantai 24.2.2025

Aloitin päiväkirjan toteutusjakson ensimmäisenä maanantaina käymällä läpi omien työtehtävieni tilanteen, koska prioriteetti on kuitenkin häiriötiketeissä ja muussa asiakaspalvelussa. Tämän jälkeen halusin saada selkeän kuvan siitä, mitä NIS2-direktiivissä oikeasti vaaditaan ja näin myös siitä, mitä vaatimuksia tulevassa Suomen lainsäädännössä tulee olemaan organisaatioiden tietoturvaan liittyen. NIS2-direktiiviin liittyvä lainsäädäntö olisi pitänyt olla valmiina jokaisessa EU:n jäsenmaassa lokakuuhun 2024 mennessä, mutta Suomi ei ole vielä soveltanut lainsäädäntöä tähän liittyen (European Commission 2025).

NIS2-direktiivin velvoitteet ovat hyvin oleellisia SOTE-toimialalle, koska direktiivi kohdistuu 2 artiklan mukaan muun muassa keskisuuriin terveysalan toimijoihin tai minkä tahansa kokoisiin julkisiin toimijoihin, joiden palvelujen estyminen aiheuttaisi merkittäviä seurauksia yleiselle turvallisuudelle tai terveydelle. Tämän lisäksi toimiala luokitellaan 3 artiklan mukaisesti keskeiseksi ja tärkeäksi toimijaksi, mutta jäsenvaltion on kuitenkin määritettävä tämä erikseen. (Direktiivi 2022/2555/EU.)

SOTE-toimialalla toimivien organisaatioiden tulisi 23 artiklan mukaan raportoida merkittävistä tietoturvapoikkeamista nimetylle CSIRT-toimijalle sekä ilmoittaa mahdollisista turvatoimenpiteistä asiakkaille, joita toimialan palveluihin kohdistuvat merkittävät kyberuhkat koskevat (Direktiivi 2022/2555/EU). Ensimmäinen ilmoitus on tehtävä 24 tunnin kuluessa merkittävän tietoturvapoikkeaman havaitsemisesta, jatkoilmoitus lisätiedoilla 72 tunnin kuluessa ja tilanteen päätyttyä loppuraportti. Merkittävä tietoturvapoikkeama määritellään tapahtumaksi, joka on aiheuttanut tai voi aiheuttaa vakavan toimintahäiriön, taloudellista tappiota tai huomattavaa aineellista tai aineetonta vahinkoa. (Traficom – Kyberturvallisuuskeskus 2025a.)

Vaikka NIS2-direktiivin edellyttävä lainsäädäntö ei ole vielä valmis, Suomi on kuitenkin soveltanut ensimmäisen NIS-direktiivin vaatimuksia lainsäädäntöön. Vuonna 2017 Liikenne- ja Viestintäministeriön julkaisemassa NIS-direktiiviin liittyvässä loppuraportissa ”Verkko- ja tietoturvadirektiivi” ehdotettiin Viestintävirastoa Suomen CSIRT-toimijaksi (Liikenne- ja viestintäministeriö 2017). Viestintäviraston Traficomin Kyberturvallisuuskeskus oli jo toiminut Suomen kansallisena CERT-yksikkönä (engl. Cybersecurity Emergency Response Team), ja heidän lakisääteiset tehtävänsä liittyivät vahvasti tuleviin NIS-direktiivin CSIRT-tehtäviin (Traficom – Kyberturvallisuuskeskus 2024). Näin ollen oli luonnollista integroida myös tulevat tehtävät heidän toimintaansa.

Kyberturvallisuuskeskus on laatinut dokumentin erittäin kriittisistä toimialoista, joihin terveysala kuuluu. Sosiaali-, terveystoimialalla on huomattavasti enemmän kuin 250 työntekijää, joten toimialamme luokitellaan suureksi toimijaksi ja sen perusteella keskeiseksi toimijaksi. Vaikka NIS2-direktiivin lainsäädäntö ei ole vielä valmis, toimialamme tulee raportoida merkittävistä tietoturvapoikkeamista NIS-direktiivin lainsäädännön perusteella CSIRT-toimijalle. Suomessa eri toimialoilla on kuitenkin omat valvontaviranomaisensa, ja tietoturvapoikkeaman ilmoittaminen Kyberturvallisuuskeskukselle on vapaaehtoista. Terveydenhuollon osalta valvontaviranomaisena toimii Valvira, jolle toimialamme on velvollinen raportoimaan merkittävistä tietoturvapoikkeamista. (Traficom – Kyberturvallisuuskeskus 2025b.)

Jäsenmaiden organisaatiot ovat NIS2-direktiivin 21 artiklan mukaan velvoitettuja toteuttamaan ja ylläpitämään teknisiä, operatiivisia ja organisatorisia hallintatoimenpiteitä kyberuhkien haitallisten vaikutusten ehkäisemiseksi tai minimoimiseksi. Tämä edellyttää ajantasaista kyberturvallisuuden riskienhallinnan toimintamallia, jonka perusteella otetaan käyttöön tarvittavat hallintatoimenpiteet. Toimintamallin tulisi kattaa vähintään kymmenen keskeistä kohtaa, jotka mainitaan artiklassa: riskianalyysi, tietoturvapoikkeamien käsittely, toiminnan jatkuvuuden hallinta, toimitusketjun turvallisuus, verkko- ja tietojärjestelmien turvallisuus, hallintatoimenpiteiden auditointi, kyberturvallisuuskoulutus, kryptografian toimintaperiaatteet, henkilöstöturvallisuus, ja lisäturvatoimien käyttöönotto. (Direktiivi 2022/2555/EU.)

Tiistai 25.2.2025

Työpäivä alkoi jälleen kriittisten työtehtävien ongelmien ratkomisella ja oman työn tilannekatsauksella. Näiden tehtävien suorittamisen jälkeen keskityin ISMS-toteutushankkeen statuksen hahmottamiseen. Tietoturvapäällikkö on jatkuvasti päivittänyt varsin kattavaa dokumentaatiota, joten yleiskuvan saaminen oli melko helppoa. Valtaosa alkuselvityksistä ja laajuuden määrittämisestä on jo tehty, joten voimme keskittyä olennaisiin aliprojekteihin. Tällä hetkellä on kolme keskeistä osa-aluetta: tietoturvapoikkeamien ja -häiriöiden hallinta, tietoturvariskien hallintaprosessi ja tietoturvariskien hallintakeinot.

Tietoturvapoikkeamien ja -häiriöiden hallintaan liittyy esimerkiksi toipumissuunnitelmapohjan ja kriittisyysluokittelutyökalun (Business Impact Analysis, BIA) kehittäminen, jonka avulla voimme luokitella järjestelmien ja laitteiden kriittisyysluokat, ja kehittää keskitettyä tietoturvakeskusta (engl. Cloud Security Operations Centre, CSOC).

Tietoturvariskien hallintaprosessi on pitkälti käynnissä ja in-house-yhtiöllä on tässä keskeisin rooli. Vaatimusmäärittelyt tulevat kuitenkin organisaation eri toimialoilta, mikä edellyttää tiivistä yhteistyötä. Itse olen lähinnä vain tietoinen aliprojektin etenemisestä, mutta en ole osallistunut siihen aktiivisesti.

Tietoturvariskien hallintakeinot liittyvät suoraan ISO 27001-standardin A-liitteen hallintakeinoihin (Suomen Standardisoimisliitto SFS 2023a). Tällä hetkellä olen mukana kahdessa aliprojektissa, jotka koskevat hallintakeinoja 6.7 Etätyöskentely ja 8.1 Käyttäjien päätelaitteet. Pyrimme pitämään kerran viikossa tietoturvatiimin jäsenten kanssa ISMS-statuspalaverin, jossa käymme läpi eri aliprojektien tilanteet. Hallintakeinoja on yhteensä 93, ja ne ovat jaettu neljään kategoriaan: organisaatioon liittyvät, henkilöstöön liittyvät, fyysiset hallintakeinot, ja teknologiset hallintakeinot. Kypsyysarvioinnit näiden osalta ovat vielä hyvin alustavia; toistaiseksi vain noin 4 % on tehty. Suurimmat haasteet ovat olleet kommunikaatio eri sidosryhmien kanssa sekä vaikeus löytää johdon hyväksymiä dokumentteja, joissa on tarkasti määritelty hallintakeinojen toteutus toimialalla.

ISO 27001-standardin hallintakeinojen kypsyysarvioinnin ja sopeuttamisen lisäksi selvitämme parhaillaan Microsoft Cloud Security Benchmarkin (MCSB) mahdollista hyödyntämistä. Esimerkiksi standardin hallintakeino 5.23 Pilvipalvelujen tietoturvallisuus käsittelee pilvipalveluiden tietoturvaa, mutta MCSB:n avulla voisimme mahdollisesti täsmentää julkipilvipalveluiden käytön tietoturvallisuutta merkittävästi.

Keskiviikko 26.2.2025

Tänään tietoturvatiimin tikettijonoon ilmoitettiin mahdollinen tietoturvapoikkeama, joka liittyi riskiin potilastietojen vuotamisesta tietyssä sovelluksessa. Testasin itse sovelluksen toimivuutta testiympäristössä ja totesin, että riski voisi olla todellinen, mikäli tuotantoympäristön sovellus toimii samalla tavalla. Selvitystyöhön kului useita tunteja, sillä ilmoittaja oli

havainnut mahdollisen tietoturvapoikkeaman, mutta ei osannut kuvata ongelmaa teknisellä tasolla. Jouduin siis selvittämään itse tarkemmin, mistä tilanteessa oli kyse. Lopulta tein tarvittavat selvityspyynnöt järjestelmätoimittajalle sekä ylläpitäjälle.

Tämä tapaus osoitti jälleen, että tietoturvapoikkeamien ilmoittamiselle ja käsittelylle ei ole riittävän selkeää prosessia. Ilmoittaja oli tehnyt viisi eri tikettiä eri tahoille samasta asiasta, mutta eri selityksillä. Yksi näistä ohjattiin tietoturvatiimille, ja muut tiketit suljettiin kommentilla, että asiaa käsitellään tietoturvatiimin tiketin kautta. Oletin itse, että toinen taho ottaa tiketin vastuulleen, ja suljin tietoturvatiimin tiketin viitaten tähän. Kyseinen taho kuitenkin sulki myöhemmin myös oman tikettinsä perustelulla, että asiaa hoidetaan tietoturvatiimin kautta. Kommunikaatio ei siis toiminut riittävän hyvin, ja eri tahot joutuivat itse etsimään tiketit, jotka liittyivät samaan asiaan, sekä selvittämään tilanteen etenemisen. Suurin vastuu tästä ongelmasta oli ilmoittajalla, sillä ohjeistuksen mukaan samasta asiasta tulee tehdä vain yksi tiketti, johon lisätään tarvittaessa lisätietoja.

Tietoturvatiimillä on parhaillaan suunnittelussa tietoturvapoikkeamien ilmoituslomake, joka olisi täytettävissä rakenteellisesti mahdollisimman tarkasti. Tämä helpottaisi tarvittaessa oikean palveluntarjoajan konsultointia sekä tiketin ohjaamista oikealle taholle. Toteutus vaatii yhteistyötä in-house-yhtiön kanssa, ja olemme tiedustelleet mahdollisuutta kehittää lomaketta yhdessä heidän kanssaan. Pyyntö on kuitenkin ollut avoinna helmikuun alusta lähtien ilman edistystä.

Usein tietoturvapoikkeamailmoitukset eivät saavu tietoturvan tikettijonoon, vaan ne välittyvät muita kanavia pitkin, kuten esimerkiksi sähköpostitse tietoturvapäällikölle, käytäväkeskustelujen yhteydessä, tai tietoturva-asiantuntijan henkilökohtaiseen puhelimeen. Sama haaste koskee myös tietoturvaan liittyviä neuvontapyyntöjä, jotka saapuvat monia eri reittejä pitkin, mikä vaikeuttaa niiden keskitettyä ja rakenteellista käsittelyä. Tavoitteena on kehittää prosessi, joka selkeyttää sekä tietoturvapoikkeamien että neuvontapyyntöjen hallintaa.

Torstai 27.2

Torstaisin alayksikkömme pitää viikkopalaverin, jossa käsitellään ajankohtaisia asioita sovelluspalveluihin liittyen sekä käydään läpi kollegoiden työtilanteet. Samanaikaisesti tietoturvatiimi pitää oman viikkopalaverinsa, mutta tällä hetkellä prioriteettini on sovelluspalveluyksikön tehtävissä, joten osallistun pääasiassa sovelluspalvelutiimin palaveriin. Tietoturvatiimi tekee kuitenkin tiivistä yhteistyötä yksikössä toimivien tiimien kanssa. Yksi ISMS:n aliprojekteista, joka liittyy vahvasti sovelluspalveluihin, on tietojärjestelmien vastuuhenkilöroolien määrittäminen. Tavoitteena on selkeyttää tehtävien delegointia, kehittää sovelluskohtaisia ohjeita ja koulutuksia sekä kartoittaa sovellusten omaisuuseriä.

Muutamia muita keskeisiä asioita tähän liittyen ovat järjestelmien sekä omaisuuserien tai tietovarantojen kriittisyysluokittelu. Sen avulla voidaan tarkemmin ja tietoturvallisemmin määrittää, ketkä saavat käsitellä omaisuuseriä, milloin ja miten niitä käsitellään, sekä miten ne säilytetään ja turvataan. Tämä edellyttää kuitenkin, että tietojärjestelmien vastuuhenkilöroolit ovat riittävän selkeät, jotta oikea ammattilainen voi aloittaa omaisuuserien ja tietovarantojen tunnistamisen sekä listaamisen.

Loppupäivä kului pääasiassa sovelluspalvelujen tehtävien parissa sekä tietohallinnon kuukausiinfossa, jossa käytiin läpi tietohallinnon yksiköiden tilannekatsaukset ja muita ajankohtaisia asioita. Infossa tuli myös esille loppusuoralla oleva mielenkiintoinen laaja projekti: asiakas- ja potilastietojen tietoalusta. Sen avulla toimialan tietojohtaminen ja tilastopalvelut voivat tehdä parempia päätöksiä sekä kehittää entistä tehokkaampia sosiaali-, terveyspalveluja. Tietoalustan tietoturva otetaan erittäin vakavasti, mutta en ole itse mukana kyseisessä projektissa tällä hetkellä.

Perjantai 28.2

Tänään kävin tarkemmin läpi ISO 27001 A-liitteen hallintakeinot ja niiden aliprojektien tilan toimialallamme. Apuna käytin myös ISO/IEC 27002:2022-standardia (jäljempänä ISO 27002), jossa jokaisesta hallintakeinosta on määritelty tarkoitus, ohjeistus ja mahdolliset lisätiedot (Suomen Standardisoimisliitto SFS 2023b). Hallintakeino 6.7 Etätyöskentely on ollut vastuullani, ja sen kypsyysarviointi sekä kuiluanalyysi ovat valmiina. Hallintakeino 8.1 Käyttäjien päätelaitteet on myös työn alla, mutta se on huomattavasti laajempi ja edellyttää tietoa useilta eri tahoilta. Tässä aliprojektissa kommunikaatio ja dokumenttien löytäminen ovat jälleen osoittautuneet haasteellisiksi, vaikka päätelaitteiden tietoturva vaikuttaa olevan hyvällä tasolla.

Koska kypsyysarviointeja on tehty tähän mennessä vain vähän ja pystyn edistämään joitakin niistä melko itsenäisesti, päätin keskittyä ensisijaisesti teknologisiin hallintakeinoihin. Käymistäni hallintakeinoista suljin alustavasti pois seuraavat: 8.4 Pääsy lähdekoodiin, 8.8 Teknisten haavoittuvuuksien hallinta, 8.14 Tietojenkäsittelypalvelujen vikasietoisuus, sekä kaikki ohjelmointiin, kehittämiseen ja sovelluksiin liittyvät hallintakeinot (8.25–8.34). Poissulkemisen syinä olivat joko näiden aiheiden luottamuksellisuus tai laajuus, sillä opinnäytetyöni on julkinen ja sen seurantajakso on vain kahdeksan viikkoa.

Muiden teknologisten hallintakeinojen kypsyysarvioinnit pystyn ainakin aloittamaan ja joitakin jopa työstämään aktiivisesti itsenäisesti. Myös tietyt organisaatioon ja henkilöstöön liittyvät hallintakeinot vaikuttavat hyviltä kandidaateilta, mutta monet niistä edellyttävät ISMS-toteutushankkeen aliprojektien etenemistä ennen kuin niitä voidaan arvioida tarkemmin.

Viikkoanalyysi

Muun työn ohella minulla on ollut melko haastavaa varata aikaa ja perehtyä kunnolla ISMS-toteutushankkeen tilanteeseen sekä tutustua kaikkiin standardeihin ja viitekehyksiin, joiden avulla kehitetään perusteellinen tietoturvan hallintajärjestelmä. Myös yleiskuvan muodostaminen kaikista SOTE-toimialan tietoturvaa koskevista määräyksistä, laeista ja vaatimuksista on ollut varsin haastavaa, joten sen hahmottaminen jatkuu edelleen ensi viikolla. Olen kuitenkin tässä vaiheessa saanut riittävän hyvän yleiskuvan toimialamme ISMS-toteutushankkeesta ja sen aliprojekteista, jotta voin ensi viikon aikana alkaa edistää itsenäisesti tiettyjä aliprojekteja.

3.2 Viikko 2

Tällä viikolla pyrin keskustelemaan ja sopimaan in-house-yhtiön kanssa, millä tavalla voisimme mahdollisimman sujuvasti edistää ISO 27001:n teknologisten hallintakeinojen kypsyysarviointeja. Prioriteettina on löytää sopivan keskustelukanavan sekä vastuuhenkilöitä jokaiseen valittuun hallintakeinoon. Tämän lisäksi tietohallinnon sisältä on löydettävä vastuuhenkilöt, jotka osaavat vastata hallintakeinoihin liittyviin kysymyksiin. Monet organisaatioon liittyvien hallintakeinojen kypsyysarvioinnit voidaan myös aloittaa, mikäli kommunikaatio lähtee sujumaan toivotetulla tavalla.

Tämän lisäksi tavoitteeni on lisätä ymmärrystäni THL:n vaatimuksista SOTEn palvelunantajiin liittyen sekä asiakastietolaista ja sen tietoturvavaatimuksista. Kolmantena prioriteettinani on hahmottaa, miten MCSB:tä voidaan hyödyntää toimialan ISMS-toteutuksessa ja sen perusteella myös tutustua mahdollisiin NIST 800-53:n ja CIS:n kontrolleihin, johon viitataan MCSB:ssä.

Maanantai 3.3

Toinen seurantaviikko lähti normaalilla tavalla käyntiin käsittelemällä kriittisimmät työtehtävät, jotka liittyvät sovelluspalveluihin. Lähetin kuitenkin in-house-yhtiön asiakkuuspäällikölle sähköpostiviestin, jossa tiedustelin, millä tavalla voisimme edetä kypsyysarviointien kanssa. Sain vastauksen, että voin hänen kauttaan pyytää aiheen tai hallintakeinon perusteella vastuuhenkilön. Toisaalta ei ole täysin selvää, mikä tarkalleen kuuluu in-house-yhtiön vastuulle, joten kysyin vielä, onko heillä käytössä vastuumatriisi, esimerkiksi RACI-muodossa, jotta voisin muodostaa kysymykseni sen mukaisesti. Ainoa vastuumatriisi, jonka olen löytänyt, on vuodelta 2021, eikä se liity suoraan in-house-yhtiön toimintaan, vaan sen edeltäjän toimintaan.

Viime viikolla suunnittelin, että voisin edistää suhteellisen monet hallintakeinot samaan aikaan ja päätin silloin edistää teknologisten hallintakeinot, pois lukien muutamia, jotka vaikuttivat liian laajalta tähän opinnäytetyön seurantajakson katsoen. Tänään kuitenkin ajattelen, jos aloittaisin prosessi hieman hallitsevammin, ja keskittyisin ensimmäiseksi korkeintaan kolmeen eri teknologisten hallintakeinoihin. Näin ajatellen, päätin valita 8.7 Haittaohjelmilta suojautuminen, 8.13 Tietojen varmuuskopiointi ja 8.17 Kellojen synkronointi. Valinnat

perustuvat asetettuihin prioriteetteihin ja tietoturvapäällikön ehdotuksiin. Kellojen synkronointi valitsin kolmanneksi, koska olen itse havainnut, että kaikki laitteiden kellot eivät ole synkronoineet ja tämä on käsittääkseni aika perusteellinen vaatimus esimerkiksi keskitetyssä häiriöhallinnassa.

Sosiaali- ja terveysministeriö (STM) on myös pyytänyt toimialalta erilliset vastaukset DVV:n digiturvallisuuden kokonaispalveluun liittyviin kysymyksiin, joihin aloimme vastaamaan yhdessä tietoturvatiimin kanssa. Kysymykset oli pitkälti muotoiltu niin, että jos suurin osa ISO 27001-hallintakeinojen kypsyysarvioinneista olisi ollut valmiina, meillä olisi ollut useisiin kysymyksiin vastaukset valmiina. Kysymykset liittyvät kuitenkin myös tietosuojaan, johtamiseen sekä tilastoihin, kuten henkilötyövuosiin ja kustannuksiin, joten meidän täytyy vielä konsultoida tarvittavat tahot ja jatkaa vastausten laatimista myöhempänä ajankohtana.

Tiistai 4.3

Suurin osa työpäivästä meni sovelluspalvelujen työtehtäviin, enkä ole saanut vastausta in-house-yhtiön vastuumatriisista. Tietoturvatiimin jonoon on kuitenkin reititetty suhteellisen kiinnostavan tiketin. Käyttäjä ilmoittaa, että hän ei pysty ladata Visual Studio Codeen tiettyä lisäosaa. Tämä on sinänsä kiinnostava, koska tietoturvatiimin puolelta emme tienneet, että Visual Studio Code on asennettu tai käytössä missään SOTEn koneella. Lisäksi tiketti oli tehty keskellä perjantain ja lauantain välisenä yönä, mikä herätti taas epäilyä väärinkäytöstä. Toisaalta tämä voi olla ihan sovittu ja luvallista käyttöä, mutta varmistetaan kuitenkin taustatiedot ensimmäisenä.

Keskiviikko 5.3

En ole vielä saanut vastausta vastuumatriisin käyttöön in-house-yhtiön asiakaspäälliköltä, joten laadin yleiset kysymyslistat liittyen hallintakeinoihin 8.7 Haittaohjelmilta suojautuminen, 8.13 Tietojen varmuuskopiointi ja 8.17 Kellojen synkronointi". Lähetin nämä asiakkuuspäällikölle siinä toiveessa, että hän voisi ohjata minut alustavasti ainakin oikeisiin vastuuhenkilöihin. Kysymyslistat perustuvat vahvasti ISO 27002 standardin suomenkielisen version hallintokohtaisten sisältöön.

Torstai 6.3

Torstai alkoi tuttuun tapaan alayksikön viikkopalaverilla, jossa kävimme läpi kollegojen työtilanne ja sovelluksiin liittyvät tiedotettavat asiat. Tänä yönä oli havaittu suhteellisen laaja häiriö tärkeässä järjestelmässä ja jotkut kollegat olivat jo varhain aamulla alkaneet korjaamaan ammattilaisten käyttöoikeuksia, jotka olivat automatisoidun päivityksen myötä lakanneet toimimasta. Koko työpäivä meni tämän tilanteen hallinnoimiseksi sekä käyttöoikeuksien korjaamiseksi.

Perjantai 7.3

Torstaina alkanutta häiriötilanne oli palveluntarjoajan mukaan saatu korjattu, mutta edelleen tuli tikettejä liittyen samaan problematiikkaan, joten häiriötilanteen hallinta jatkui vielä tänään. Tilanne on suhteellisen hyvin hallittu iltapäivän alussa ja pystyin keskittymään muuhun työhön. En saanut tänäänkään vastausta asiakaspäälliköltä, suunnitelmana kuitenkin on jatkaa kysymyslistojen laatimista, jotta saisimme kypsyysarvioinnit edistettyä. Tavoitteena myös etsiä toimialan sisältä vastuuhenkilöitä valittuihin hallintakeinoihin, mutta käsittääkseni päävastuu on kuitenkin in-house-yhtiöllä kyseessä olevissa hallintakeinoissa; ilman vastuumatriisia en tosiaan voi olettaa mitään.

Selvittelin THL:n vaatimuksia, jotka kohdistuvat toimialan tietoturvaan ja tietojärjestelmiin, erityisesti määräyksiä 3/2024, 4/2024 ja 5/2024. Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (jäljempänä asiakastietolaki) 77 ja 78 § velvoittavat asiakas- tai potilastietojen käsittelijän palvelunantajan laatimaan tietoturvasuunnitelman, josta tulee ilmetä, miten lain vaatimukset varmistetaan ja toteutetaan. THL:n määräyksessä 3/2024 on tarkennettu vaatimuksia, jotka muistuttavat NIS2-direktiivin velvoitteita. Määräyksessä suositellaan kuitenkin suoraan hyödyntämään ISO/IEC 27000-standardiperheen standardeja toimivan tietoturvallisuuden hallintajärjestelmän rakentamisessa, kun taas NIS2-direktiivissä viitataan kansainvälisten standardien käyttöön yleisellä tasolla, mutta ei suoraan suositella tiettyä standardia. (Terveyden ja hyvinvoinnin laitos 2024a, 6–7.)

Tietoturvasuunnitelmasta tulee käsitellä menettelyt virhe- ja ongelmatilanteissa sekä miten turvataan palveluiden jatkuvuus. Tietojärjestelmien käyttöohjeet ja kuvaukset, sekä pääsynhallinta, tunnistautuminen, käytön seuranta sekä käyttövaltuuksien hallintaa tulee olla dokumentoituna. Tämän lisäksi velvoitetaan, että tietoturvasuunnitelmassa on dokumentaatio fyysisestä turvallisuudesta, laitehallinnasta, ja verkkopalvelujen tietoturvallisesta käytöstä sekä Kanta-palvelujen tietoturvakäytännöistä. Ei mitään kuitenkaan toimisi, jollei henkilökunnalla on tarpeeksi hyvä koulutusta ja osaamista, joten koulutuksen ja kehittämisen tärkeys on myös panostettu. (Terveyden ja hyvinvoinnin laitos 2024a, 8–9.)

THL:n määräyksessä 4/2024 käsitellään tietojärjestelmien ja hyvinvointisovellusten luokittelua ja sertifiointia. Yksinkertaistettu tämä tarkoittaa, että jokainen tietojärjestelmä, jossa käsitellään asiakas- tai potilastietoja, on sertifioitava määräyksen 5/2024 ja sen liitteiden vaatimusten mukaisesti. Asiakastietolain 79 § mukaan on jaoteltava tietojärjestelmä joko luokkaan A tai B, mutta lain mukaan THL:llä on myös oikeus antaa määräyksiä näistä luokista. Määräyksessä käytetään luokat A1, A2, A3, ja B, josta vain B-luokan tietojärjestelmiä ei tarvitse sertifiointia. A1, A2 ja A3 -luokat ovat eritelty käyttötarkoituksen, käsiteltyjen tietojen luonteen ja laajuuden perusteella, ja A3 on näistä kriittisin luokka ja riskitaso on oletusarvoisesti korkea. A3-luokan tietojärjestelmiin kuuluu kaikki Kanta-palveluihin liittyvät, joissa

käsitellään laajasti hoidollisia tai palvelujen sisältöön liittyviä asiakastietoja. Kaikki A-luokan tietojärjestelmät tulee olla rekisteröitynä Valviran ylläpitämässä rekisterissä, mikä edellyttää sertifiointia ja kirjallisen selvitys määräys 5/2024 vaatimusten täyttämisestä. (Terveyden ja hyvinvoinnin laitos 2024b, 6–9.)

Sain myös selville, että toimialamme tulee myös häiriötilanteessa tehdä Palvelujärjestelmän ja Varautumisen Tilannekuvajärjestelmäilmoitus PAVAT, jossa raportoidaan tilannekuvatiedot häiriötilanteesta Etelä-Suomen Tilannekeskukselle. Häiriötilanne tässä yhteydessä liittyy myös muihin kuin kyberuhkien häiriötilanteisiin, mutta NIS2-direktiivin ”merkittävä tietoturvapoikkeama” luokitellaan tässä kontekstissa myös häiriötilanteeksi. Hyvinvointialueiden ja sosiaali- ja terveyspalvelujärjestelmän perustamisen myötä on tehty sopimukset hyvinvointialueiden välisestä yhteistyöstä, jossa on sovittu muun muassa häiriötilanteiden ja poikkeusolojen varautumisesta ja PAVAT-tilannekuva on osa tätä.

Organisaatiomme on osa Etelä-Suomen yhteistyöaluetta, jossa HUS-yhtymän Valmiuskeskus toimii alueen valmiuskeskuksena. Heidän tehtäviinsä kuuluu toimia yhteyspisteenä häiriötilanteissa sekä käsitellä yhteistyöalueen PAVAT-ilmoituksia. (Etelä-Suomen yhteistyöalueen yhteistyösopimus 2024, 28.) Tulevaisuudessa on tarkoitus tarjota myös muille yhteistyöalueille mahdollisuus liittyä PAVAT-järjestelmään (Croell, Hetemaa, Knape, Leipälä, Louet-Lehtoniemi, Ridanpää, Suomela, Syrjänen & Syrjä 2023, 10).

Viikkoanalyysi

Seurantajakson toinen viikko oli omistettu suureksi osaksi sovelluspalvelujen tehtäviin, varsinkin torstaina alkaneen häiriötilanteen vuoksi. Tänä viikkona yritin saavuttaa toimiva viestintäkanava in-house-yhtiön kanssa liittyen ISO 27001 standardin hallintakeinojen kypsyysarviointiin, mutta kommunikaatio on jälleen todettu haastavaksi. In-house-yhtiön asiakaspäällikkö ei ole vielä perjantai iltapäivänä palannut minun kysymyksiini.

Aloitin kuitenkin tällä viikolla kysymyslistojen laatimisen muutamalle hallintakeinolle ja aion luoda lisää tulevalla viikolla. THL:n määräyksen 4/2024 asiakas- tai potilastietojen käsittelevän tietojärjestelmän luokittelu voi olla hyödyllinen myös tietojärjestelmien kriittisyysluokittelussa, joka on yksi ISO 27001-standardin teknologiapohjaisista hallintakeinoista ja mahdollinen aliprojektikandidaatti ensi viikolle. Tällä viikolla en ehtinyt vielä käydä läpi MCSB:tä tarkemmin, mutta ensi viikon hallintakeinon valinnan perusteella voisin tutustua myös MCSB:n suosituksiin ja toimenpiteisiin liittyen valittuihin hallintakeinoihin.

Olen taas vähän enemmän tietoinen siitä, mitä SOTE-toimialalta ja toimivalta ISMS-järjestelmältä vaaditaan. Toimialan tietoturvaan ja tietosuojaan kohdistuvat asiakastietolain ja THL:n määräysten vaatimukset alkavat olla suhteellisen selkeät minulle ja sen perusteella myös ISMS-toteutushankkeen perusteet sekä tarkoitus. Toisaalta toimialaan liittyy paljon muita

lakeja, suurin osa tietosuojaan, mikä taas menee tämän opinnäytetyön laajuuden viereen, joten en suunnittele käsittelemään tässä seurantajaksossa enempää lakia jollei ole pakollista mahdollisen aiheen eteen.

Uutena informaationa minulle tuli myös PAVAT-järjestelmä ja yhteistyöalueiden sopimukset. PAVAT-ilmoituksen tekeminen ja kenen vastuulla se on loppujen lopuksi on vielä kuitenkin epäselvä minulle. Satuin myös huomaamaan, että hallituksen esitys (57/2024) NIS2-direktiivi koskevaan lainsäädäntöön on mennyt ensimmäisen käsittelyn läpi 5.3.

3.3 Viikko 3

Tänä viikkona prioriteetti on valittujen hallintakeinojen kypsyysarvioiden edistämisessä sekä miten niissä voidaan mahdollisesti hyödyntää MCSB:n suositukset ja turvallisuustoimenpiteet. Näiden perusteella laajennan mahdollisesti kysymyslistat. Otan vähintään yksi hallintakeino lisää käsiteltäväksi ja luon siitä kysymyslistan. Aion myös ottaa selvää, pystyykö joku toimialan tietohallinnossa ottamaan kantaa hallintakeinojen liittyviin kysymyslistoihin. Tavoitteena on myös aloittaa luomaan jonkinlaista visuaalista karttaa, josta tulisi ilmi toimialamme kohdistuvia vaatimuksia, lakeja, standardeja sekä miten ne liittyvät toisiin. Kolmantena prioriteettina tutustun Julkriin ja Katakriin, Valtiovarainministeriön julkistama arviointikriteeristö sekä ulkoministeriön auditointityökalu vastaavasti, jotka ovat hyödynnetty toimialan sisällä.

In-house-yhtiön kanssa kommunikointiin liittyen en koe tällä hetkellä, että pystyisin minun asemassani vaikuttamaan paljon. Yhteistyö on ollut käsittääkseni pitkään haasteellinen, molempien puolten mielestä. Olisi kuitenkin luontevana ja suositeltavana kehittämään yhteistyö- ja kommunikaatiotavat, enkä ole ihan varma, miksi tämä ei ole korkeampi prioriteetti organisaatiossa.

Maanantai 10.3

Maanantai aamu alkoi tietojärjestelmän tilannekatsauspalaverilla, missä käsiteltiin torstaina alkanut häiriö. Tämä on sinänsä kiinnostava tapaus, koska kyseessä oli laaja häiriö, josta palveluntuottaja aloitti Major incident management-prosessin (MIM). Käytännössä MIMissä tulisi olla keskitetty häiriöhallinta johon sidosryhmät osallistuvat laajuuden ja tarpeen mukaan. Viime viikon tapauksessa nähtiin kuitenkin, että prosessi ei toimi kovin hyvin ainakaan meidän näkökulmastamme, kun me tietojärjestelmän pääkäyttäjät eivät saaneet mitään muuta informaatiota tilanteesta, kuin SOTEn muut ammattilaiset saivat palvelutuottajan lähettämä häiriötiedotteen kautta. Tietohallinnon MIM-manageri ei myöskään saanut kutsua mihinkään tilannepalaveriin tai tietoa mistään häiriötilanteeseen liittyen.

Tilanteesta selvittiin kuitenkin suhteellisen hyvin lähinnä siksi, että pari pääkäyttäjä alkoivat selvittää millä tavalla pystymme ratkaisemaan häiriötilanteeseen liittyvät

käyttöoikeusongelmat ilman palvelutuottajan ohjeistusta tai apua, ja ohjeistivat selvityksensä perusteella muut pääkäyttäjät. Myös SOTEn esihenkilöt saivat informaatiota meiltä, miten he voivat mahdollisesti ratkaista käyttöoikeusongelmia heidän työkaluillaan. Tänään toisen tahon, ei siis palveluntarjoajan, kanavan kautta tuli tiedotteen, joka selitti mitä on tapahtunut ja että ongelma on nyt ratkaistu, mutta ei sen tarkempaa mistä se johtui. Edelleen tulee kuitenkin häiriötikettejä liittyen samaan problematiikkaan.

Tarkoitus on käydä läpi sisäisesti, mitä me teemme tulevaisuudessa samankaltaisessa häiriötilanteessa, sekä palveluntuottajan kanssa selvittää, miten voisimme sujuvammin saada informaatiota häiriötilanteesta ja mitä vastuita kelläkin on MIM-prosessissa. Tähän liittyen organisaatiossa pitäisi olla selkeämmät jatkuvuussuunnitelmat, toipumissuunnitelmat ja vaikutusanalyysit, ei pelkästään liittyen kyseessä oleva tietojärjestelmään, vaan toimialalaajuisesti. Toisaalta palveluntuottajalla on omat versiot näistä ja toimivat sisäisesti eri tavalla kuin meidän organisaatiomme, mutta on kiinnostavaa seurata, mitä jatkotoimenpiteitä tulee käyttöön meidän toimialamme tämän häiriötilanteen jälkeen.

Hallintakeinojen kypsyysarvioinnin liittyen, in-house-yhtiön asiakaspäällikkö ei ole vielä palannut kysymyksiini. Liittyen tietoturvatiimin viime viikon tiistaina tullutta häiriötiketti Visual Studio Coden lisäosan asentamisesta, emme ole vielä saaneet vastauksia lisätietokysymyksiin tai uutta informaatiota.

Aloitin tänään selvittää, miten voisimme hyödyntää Microsoft Cloud Security Benchmark (MCSB) hallintakeinojen kypsyysarvioinnissa. MCSB tarjoaa kattava ohjeistus ja suositusten kokoelma pilvipalveluiden turvallisuuden parantamiseksi. MCSB:n kontrollit viittaavat suoraan Center for Internet Securityn (CIS) ja NIST SP 800-53 kontrolleihin, sekä Payment Card Industry Data Security Standard (PCI-DSS) kontrolleihin, mikäli ne ovat sovellettavissa. Tärkein työkalu vaikuttaa oleva Microsoft Defender for Cloud, johon MCSB:ssä viitataan usein. Kontrollit ovat sovellettavissa Azure-pilvipalvelujen lisäksi myös Amazon Web Servicen ja Google Cloud Platformin palveluihin, mutta on selkeästi panostettu Microsoftin omaan Azure ohjeistukseen eniten.

Vaikka MCSB viittaa lähinnä julkipilvipalvelujen tietoturvallisuuden parantamiseksi ja ylläpitämiseksi, niin kategoriat ja listatut kontrollit kytkeytyvät myös useisiin ISO 27001-standardin A-liitteen hallintakeinoihin. Valitsemaisiini hallintakeinoihini kytkeytyvät ainakin osittain MCSB:ssä oleviin kontrolleihin ja niihin löytyy näin myös CIS:n sekä NIST SP 800-53 kontrolleja. Taulukossa 2 on listattu hallintakeinot sekä vastaavat kontrollit. Käytetty versiot ovat MCSB version 1, CIS version 8 ja NIST SP 800-53 revision 5.

ISO/IEC 27001:2022	MCSB v1	CIS v8	NIST SP 800-53 r5
8.7 Haittaohjelmilta suojautuminen	Endpoint security	10.1 - Deploy and maintain anti-malware software 10.2 - Configure automatic anti-malware signature updates 13.7 - Deploy a host-based intrusion prevention solution	SC-3: Security function isolation SI-2: Flaw remediation SI-3: Malicious code protection SI-16 Memory protection
8.13 Tietojen varmuuskopiointi	Backup and recovery	11.2 - Perform Automated Backups 11.3 - Protect Recovery Data 11.5 - Test Data Recovery	CP-2: Contingency plan CP-4: Contingency plan testing CP-6: Alternate storage site CP-9: Information system backup
8.17 Kellojen synkronointi	Logging and threat detection	8.4 - Standardize time synchronization	AU-8: Time stamps

Taulukko 2 Hallintakeinojen ja kontrollien kytkökset

Tarkoituksena on jatkaa tutustuminen CIS:n ja NIST SP 800-53 kontrolleihin huomenna.

Tiistai 11.3

Seuraavana aamuna olin saanut in-house-yhtiön asiakaspäälliköltä viestin, jossa oli määritetty vastuuhenkilöt hallintakeinoihin liittyviin kysymyksiin, mutta vastuumatriisia ei ollut mainittu. Kun olen saanut vastuuhenkilöiden vastaukset ja kannanotot, teen kypsyysarvioinnin ja voin toivon mukaan antaa suosituksia heille jatkotoimenpiteistä, joilla saataisiin tavoittelemamme kypsyysaste.

Tänä aamuna tuli myös kiinnostava tiketti liittyen laajempaan käyttöoikeuksiin liittyvään ongelmaan, joka koskee vain tietyt käyttäjät tietyssä ulkoistetussa terveyspalvelussa, mutta ei kuitenkaan yksikkölaajuisesti ja vain osa tietystä tietojärjestelmästä ei toimi. Selvitin toisen

asiantuntijan kanssa tilanne ja todettiin, että aikoinaan oli tehty tilapäisratkaisu liittyen, miten käyttäjien tiedot synkkaavat pilvipalveluihin. Käyttäjien tiedot eivät saaneet synkata täydellisesti päällekkäisyyden takia ja tietyille ammattilaisille oli luotu oma ryhmä, jonka ryhmäkäytäntö oli estää Azureen synkattavia tietoja. Käyttäjät eivät näin päässeet kirjautumaan sisään tiettyihin palveluihin, jotka tarkistivat Microsoft Entra ID:n kautta tietyt tiedot, koska heidän tietonsa eivät olleet kerta kaikkeaan replikoituneet sinne. Koska kyse oli ulkoistetun palvelun henkilökuntaa, heidän tietonsa tarkistetaan pelkästään Azure-palvelujen kautta. Poistettiin käyttäjiltä ryhmän, minkä jälkeen ongelma korjaantui.

Yllä oleva tapaus olisi voitu estää toimivalla identiteetin hallinnalla, joka löytyy myös hallintakeinona ISO 27001 -standardissa. Ammattilaisille oli erikseen laadittu oma yhteyshenkilöprofiili työprofiilin lisäksi, eikä tietty ammattilainen ollut siksi sidottu yhteen identiteettiin. Pääsyoikeudet eivät olleet mitenkään seurannassa tai varsinaisesti kenenkään vastuulla, mikä teki koko asia hankalampi taas, kun kyse on ulkoistettu palvelu ja vastuiden jako on epäselvä.

Aloitin CIS:n kontrollien tutustumista sovelluspalvelujen tehtävien jälkeen. Tuorein versio CIS Controls-dokumentaatiosta on 8.1, joka julkaistiin vuonna 2024. Näiden kontrollien laatija on Center for Internet Security itse, joka on yhteisölähtöinen, voittoa tavoittelematon organisaatio, ja heidän tavoitteensa on auttaa luomaan turvallisemman kyberympäristön ihmisille, yrityksille ja hallituksille. Dokumentaatio kontrolleista on mielestäni helppo lukea ja ymmärtää; jokaisen kontrollin tarkoitus, kriittisyys, työkaluja ja suojaustoimenpiteitä ovat selkeästi listattu ja selitetty. (Center for Internet Security 2025.)

Uutena CIS Controls versiossa 8 on implementation groups, suom. implementointiryhmät. Ryhmiä on kolme, IG1, IG2 ja IG3, jotka voidaan yksinkertaistettuna jakaa seuraavasti:

- IG1: Pienet ja keskikokoiset yritykset, jolla on rajatusti IT- ja kyberturvallisuusasiantuntemusta, ja rajoitettu sietokyky käyttökatkoksiin
- IG2: Yritykset, joilla on IT-hallinnasta ja -suojauksesta vastuussa olevaa henkilökuntaa, ja käsittelevät usein arkaluonteista asiakas- tai yritystietoa
- IG3: Yritykset, jotka työllistävät IT- ja kyberturvallisuuteen erikoistunutta henkilökuntaa, ja onnistuneita kyberhyökkäyksiä voivat aiheuttaa merkittävää haittaa kansanterveydelle

IG2 sisältää IG1:een suunnatut kontrollit ja vastaavasti IG3 sisältää IG2:n kontrollit, ja näin ollen jokaisella suojaustoimenpiteelle on määritetty vähintään yksi implementointiryhmä. Vaativimmat ja erikoistuneimmat suojaustoimenpiteet ovat suunnattu IG3:n ryhmän yrityksiin, joilla on resursseja implementoida ja seurata niitä, kun taas pienemmät yritykset voivat keskittyä IG1:n ryhmän perussuojaustoimenpiteisiin. (Center for Internet Security 2024, 4-7.)

Dokumentissa on myös listattu erityyppisiä omaisuuseriä, kuten laitteita, tietoa, käyttäjiä ja ohjelmia. Jokainen suojaustoimenpide on liitetty omaisuuskategoriaan sekä lisäksi kartoitettu yhden NISTin Cybersecurity Frameworkin (CSF) kuudesta toiminnasta mukaan. CSF on viitekehys, jonka tarkoitus on auttaa organisaatioita hallinnoida ja kehittää niiden kyberturvallisuus. CSF:n kuusi keskeistä toimintaa koskien riskejä ovat: govern, identify, protect, detect, respond ja recover; jotka ovat vastaavasti suomeksi: hallita, tunnistus, suojautuminen, havaitseminen, vastaaminen ja palautuminen. (The NIST Cybersecurity Framework (CSF) 2.0 2024, 3-4.)

Organisaatiomme käsittelee päivittäin suuria määriä arkaluontoista tietoa ja työllistää IT- ja kyberturvallisuuteen erikoistunutta henkilökuntaa. Onnistuneella kyberhyökkäyksellä voisi olla merkittäviä seurauksia kansanterveydelle. Näiden tietojen perusteella organisaatiomme, ja jopa pelkkä toimialamme, voidaan luokitella IG3:n ryhmään. CIS Controls-dokumentissa todetaan, että tämän luokan organisaatioilla on usein myös henkilökuntaa, joka on erikoistunut esimerkiksi penetraatiotestaukseen ja sovellusturvallisuuteen. Koska nämä palvelut ovat meillä pääosin ulkoistettuja, emme voi toteuttaa vaativimpia CIS-kontrolleja tehokkaasti ilman tiivistä yhteistyötä palveluntarjoajien kanssa.

CIS controls-dokumentin listaukset suojaustoimenpiteistä eivät ole valmiina käyttöön otettavaksi semmoisena, vaan implementoijan täytyy hyödyntää asiantuntijaisuutta, kokemusta ja muuta dokumentaatiota, jonka perusteella voidaan organisaatiokohtaisesti muokata suojaustoimenpiteet sopivaksi. Kirjoittajat kannustavat myös tunnistamaan, että kyse ei ole pelkästään listan läpikäymisestä, mutta se voi toimia erinomaisena lähtökohtana identifioimaan puutteita ja kehittämään yrityksen kyberturvallisuutta. (Center for Internet Security 2024, 4.)

Keskiviikko 12.3

In-house-yhtiön asiantuntija oli lähettänyt vastauksen minun pyyntööni koskien hallintakeinojen kypsyysarviointia. Vastauksessa toivottiin, että toimialan tietoturvakatselmointi tulisi ensimmäiseksi tehdä sisäisesti ja koostaa ympäristöön koskevia kysymyksiä heille vastattavaksi. Tämä on ihan ymmärrettävää, koska samoista aiheista tulee heille kysymyksiä monelta eri tahoilta. Asiantuntija vetosi myös siihen. että kaupunginkanslian vetoisessa tietoturvajohtamisen muutoshankkeessa tullaan käsittelemään perusteellisesti nämä asiat yhdessä in-house-yhtiön kanssa, joten tässä vaiheessa on hankalampaa käydä läpi hallintakeinojen kypsyysarviointia toimialakohtaisesti. Argumentoin, että jos saisimme tässä vaiheessa jo perusteelliset tiedot tietoturvatilanteesta, niin voisimme aloittaa kuiluanalyysejä ja riskienarviointia ajoissa. Lähetin vastaukseni, jossa selitin tilanteemme vielä ja viittasin siihen, että lähettämäni kysymyslistoissa olen pyrkinyt pysyä heille kuuluvissa asioissa, mikä on toisaalta vaikea arvioida ilman selkeä vastuumatriisia.

Tänään kävimme myös läpi 6.3 tapahtunutta häiriötilanteen tietojärjestelmän palvelutarjoajan edustajan kanssa. MIM-prosessissa oli toimittu ohjeiden mukaisesti heidän puoleltansa, mutta laajennettu informaatio tilanteesta ei ollut kuitenkaan tullut meille pääkäyttäjille asti. Palveluntarjoajalle toimitettujen ohjeiden mukaan heidän pitää olla yhteydessä in-house-yhtiöön ja tietohallinnon MIM-manageriin, jotka eivät olleet kuitenkaan jatkoinformoineet meitä järjestelmän pääkäyttäjiä tilanteesta. Palvelutarjoajan muiden asiakkaiden kanssa oli pidetty MIM-tilannekokous, mutta organisaatiostamme ei ollut kukaan osallistunut.

Tapahtumasta voimme oppia paljon. Vaikka kyse ei ollut ulkoisesta tai sisäisestä uhkasta, joka olisi tarkoituksellisesti halunnut häiritä palveluita, voimme käyttää NISTin CSF. Palveluntarjoaja oli itse havainnut ongelman ja tunnistanut ainakin osittain ketkä häiriö koskee, sekä pysäyttäneet häiriön edistystä. Tämän jälkeen alkoi palauttamiseen liittyviä toimenpiteitä. Meidän organisaatiomme puolelta emme pystyneet tunnistamaan tarkkaan ketkä häiriö koski, mutta havaittiin häiriötilanteen saamamme häiriötiedotteen sekä tulevien häiriötikettien perusteella. Pyrimme omilla resursseilla vastaamaan ja ratkaisemaan ongelmat; tässä tilanteessa emme olisi kuitenkaan pystyneet ratkaisemaan ongelman juurisyy tai pysäyttää sen ilman palveluntarjoajan apua. Hallintaosuus oli ainakin meidän puoleltamme suhteellisen heikko häiriötilanteen aikana ja täydelliseen toipumiseen kestää aikaa.

Pystymme kuitenkin jälkikäteen analysoida tilanteen edistäminen ja missä onnistuimme tai epäonnistuimme. Varsinkin oma MIM-prosessimme vaatisi perusteellinen läpikäynti ja prosessin kehittäminen, jotta tulevaisuudessa pystyisimme toimimaan sujuvammin yhteistyössä mahdollisien sidosryhmien kanssa ja tehokkaammin jakaa tietoa sekä toimia niiden perusteella. Tietohallinnon johdolla on vastuu kehittää yhteistyössä MIM-prosessia, mutta asiantuntijamme, jotka toimivat keskeisesti häiriötilanteessa, voivat antaa arvokasta tietoa ja konkreettisia ehdotuksia. Tarkoitus on jatkaa ensi viikon aikana prosessin kehittämistä ja uudelleen hahmottamista.

Torstai 13.3

Alayksikön viikkopalaverissa kävimme 6.3 tapahtuneesta häiriötilanteesta johtuvia oheisongelmia läpi sekä missä vaiheessa niiden käsittely on. Kävimme myös alustavasti läpi, miten voisimme myötävaikuttaa MIM-prosessin kehittämiseen. Lisäksi kävimme tuttuun tapaan läpi tiimiläisten työtilanne ja mahdollisia sovelluskohtaisia ongelmia. Viikkokokouksen ja lounaan jälkeen pidettiin lähiesihenkilön kanssa kehityskeskustelua, joten ei jäänyt paljon aikaa muihin kuin sovelluspalveluihin liittyviin työtehtäviin.

Iltapäivällä tein alustavan katsauksen yhden asiakastietojen kyselyjärjestelmän väärinkäytön seurantaan, eli käytännössä siihen, millä perusteella väärinkäyttöä voidaan havaita ja miten voisimme mahdollisesti automatisoida käyttöoikeuksien väärinkäytön havainnointia. Toimin itse vastuukäyttäjänä kyseisessä järjestelmässä ja meillä on velvollisuus seurata järjestelmän

käyttäjien käyttöä. Järjestelmässä käyttäjä pystyy hakemaan asiakkaan tai potilaan tiettyjä tietoja, ja käyttöoikeuksien laajuus riippuu työtehtävästä sekä yksiköstä, jossa käyttäjä työskentelee.

Väärinkäytön havainnointi on kuitenkin melko haasteellista, koska vastuukäyttäjinä emme pysty selvittää, onko tietyllä käyttäjällä oikeus nähdä tietyn asiakkaan tai potilaan tiedot tai onko käyttäjä hakenut enemmän tietoja kuin tarpeellista kyseisestä asiakkaasta tai potilaasta. Järjestelmään on lisätty käyttäjille täytettävä lisäkenttä haun perustelemiseksi, ja lokeista pystytään näkemään, mitkä ovat haettujen tietojen kategoria ja mikä käyttäjä on hakenut niitä. Kynnys pyytää näitä tietoja sekä se, kuka saa lukea lokit, ovat ainakin minulle vielä epäselviä.

Vastuukäyttäjinä pystymme tuottamaan käyttäjän tai yksikön kohtaisia käyttötilastoja ja näin ollen väärinkäytön havainnointi vastuukäyttäjien puolesta perustuisi pitkälti hakumäärien arviointiin, eli pitäisi jollain tavalla analysoida, ovatko haun tarkoitus ja hakumäärä normaalien rajojen sisällä tietylle käyttäjälle tai käyttäjäryhmälle. Toinen mahdollisuus on tarkastaa, että käyttäjät käyttävät järjestelmän vain työaikana; työajan ulkopuolella haetut tiedot saattavat viitata siihen, että käyttäjän tili on kaapattu tai muuten vaarantunut. Tarkoitus on ensi viikolla käydä järjestelmän muiden vastuukäyttäjien kanssa läpi analyysini tilanteesta.

Perjantai 14.3

Perjantain kunniaksi minulla oli mahdollisuus osallistua päivän mittaisen työpajaan, liittyen tietoturvapoikkeamien hallinnan prosessi. Työpaja pidettiin tietoturvatiimin, tietoturvakonsulttifirman edustajien ja alayksiköiden lähiesihenkilöiden kesken. En ole aikaisemmin osallistunut aiheeseen liittyneihin palavereihin, joten osallistuin lähinnä kuunteluoppilaana. Tietoturvapoikkeamien hallinnan prosessin kuvaus ja toimialakohtainen dokumentaatio on pitkälti valmis ja työpaja oli koottuna lähinnä dokumentin yhteiseksi läpikäymiseksi. Tavoite on kehittää ja implementoida keskitettyä prosessia, jolla saataisiin tietoturvapoikkeamat tehokkaasti ja asiallisesti käsitelty.

Prosessin teoreettisena pohjana toimii ISO/IEC 27035-standardi, joka ohjeistaa tehokkaaseen tietoturvapoikkeamien hallintaprosessin luomiseksi. Standardin tavoitteet ovat prevent, detect, react, recover, sekä analyse and document; suomeksi vastaavasti: estää, havaita, reagoida, toipua, sekä analysoida ja dokumentoida, ja näin ollen muistuttavat CSF:n keskeisistä toiminnoista. Kyseessä oleva standardi on uusi minulle ja arvostan, että löytyy ISO/IEC-standardikirjastosta dokumentaatiota kyseiseen aiheeseen.

Sain myös vastauksen in-house-yhtiön asiantuntijalta liittyen hallintakeinojen kypsyysarviointeihin. Vastauksen perusteella yhtiön toimintaa peilataan useamman standardin ja parhaiden käytänteiden kautta, myös ISO 27001-standardin. He keskittyvät myös NIS2-direktiivin

vaatimusten täyttämiseen. Vastuumatriisin teko on ehdotettu, kun vastuiden jako on vielä epäselvä. Relevantin kohde vastauksessa oli kuitenkin se, että hän oli suostuvainen osallistumaan palaveriin toimialamme tietoturvatiimin kanssa ja keskustella aiheesta.

Tämän perusteella tiedustelen ensi viikolla tietoturvapäälliköltä, miten kannattaa tässä edetä. Tässä vaiheessa alkaa omasta mielestä tuntua siltä, että emme tulee saamaan relevanttia dokumentaatiota tai informaatiota in-house-yhtiöltä millään muualla tavalla kuin se, että edistetään yhdessä tietoturvajohtamisen muutoshanke, ja näin ollen meidän kannattaa keskittyä muihin aliprojekteihin toistaiseksi.

Viikkoanalyysi

Hallintakeinojen kypsyysarviointi ei ole edistynyt merkittävästi tälläkään viikolla, eikä myöskään ole ollut edistystä tietoturvatiimin jonossa olevaan häiriötikettiin liittyen VSC:hen. Edellisen viikon häiriötilanteesta on keskusteltu ahkerasti, ja olemme alayksikön puolesta valmiita myötävaikuttamaan MIM-prosessin kehittämisessä. Kuitenkin yksikön päälliköllä on päävastuu meidän puoleltamme, ja virallinen aloite on käsittääkseni tultava häneltä. Palveluntarjoajan puolelta päävastuu prosessin kehittämisestä ja ylläpidosta on heidän kehittämispäälliköllänsä.

Perjantain työpaja oli hyvin kiinnostava, vaikka en ollut perehtynyt aiheeseen. Aliprojekti on yksi suurimmista toimialan ISMS-toteutushankkeessa ja näin ollen hyvin tärkeä. En kuitenkaan tällä hetkellä pysty varaamaan työaikaa siihen tai ISO/IEC 27035-standardiin tutustumiseen. Toisaalta arvioin, että voi olla hyödyllisempää tutustua kyseiseen standardiin mieluummin kuin esimerkiksi NISTin CSF:n tietoturvapoikkeamien hallinnan osuuteen, koska toimialamme tietoturvatiimi on jo keskittymässä ISO/IEC 27000-sarjan standardeihin. CSF:stä löytyy myös riskienhallintaosuus, jolla on vastaavaa dokumentaatiota ISO/IEC 27005-standardissa.

Tutustuin tällä viikolla myös MCSB:n kautta CIS Controls-dokumentaatioon, josta olin hyvin vaikuttunut sen helppokäyttöisyydestä ja selkeydestä. Kontrollien perusteella on tärkeää alustavasti kartoittaa yrityksen omaisuuserät ja niiden tyypit. Tämä taitaa olla toinen suuri ongelma organisaatiossamme, jossa on valtava määrä laitteita ja muita omaisuuseriä, mutta ei vaikuta olevan tehokasta prosessia niiden seurannalle, vaikka niistä on olemassa listauksia. Palavereissa liittyen hallintakeinoon 8.1 Käyttäjien päätelaitteet on myös keskusteltu toisesta ongelmasta, eli siitä, että päätelaitteet ja muut omaisuuserät eivät ole selkeästi kriittisyysluokiteltuja vielä. Julkriin tai Katakriin en ehtinyt tutustua vielä, mutta sain tietoa, että nämä vaativat päivitystä, joten en priorisoi näiden kriteeristöihin tutustumista.

3.4 Viikko 4

Kolmen ensimmäisen seurantaviikon perusteella on todettava, että nykyisellä lähestymistavalla en saa edistettyä minkään hallintakeinon kypsyysarviointia. Tavoitteeni tälle viikolle on

keskustella tietoturvatiimin ja erityisesti tietoturvapäällikön kanssa siitä, miten voisimme edistää hallintakeinojen kypsyysarviointia ja tarkemmin, mitä minä voin tehdä niiden edistämiseksi. Myös lähestymistapaani hallintakeinojen valintaan on muutettava, esimerkiksi omaisuuseriin liittyvät hallintakeinot ovat priorisoitava. Omaisuuserien luokittelu ja tunnistaminen vaikuttaisi olevan jokaisen toimialan oma vastuu, mutta ainakin laitteiden hallinta, ylläpito ja turvaaminen ovat pitkälti in-house-yhtiön vastuulla.

In-house-yhtiön asiantuntijan vastausten perusteella vaikuttaa siltä, että tietoturvaan liittyvät muutokset ja kehitystyö tapahtuvat kaupunkikanslian vetämän tietoturvajohtamisen muutoshankkeen myötä, eikä näin ollen todennäköisesti tule muutoksia tämän opinnäytetyön seurantaviikkojen aikana. Käyn siksi uudelleen läpi hallintakeinot ja pyrin keskittymään pelkästään sellaisiin, joita voidaan ainakin osittain edistää sisäisesti toimialalla. En ole vielä ehtinyt tutustua NIST SP 800-53 -dokumentaatioon, joten pyrin tekemään sen tällä viikolla.

Tällä viikolla haluan myös priorisoida viime viikon alussa mainitun visuaalisen kartan luomisen. Toimialakohtaisia standardeja, vaatimuksia ja lakeja alkaa kasaantua siinä määrin, että kokonaisuuden hahmottaminen ilman työkalua on yhä vaikeampaa. Toinen prioriteetti on viime viikon torstaina mainittuun sovellukseen liittyen järjestettävä palaveri vastuukäyttäjien kanssa, jossa käymme yhdessä läpi, miten voisimme edistää väärinkäytön havainnointia ja mahdollisesti sen automatisointia.

Maanantai 17.3

Aloitin viikon käymällä läpi keskeneräiset tehtäväni sovelluspalvelupuolella sekä tikettijonot. Tietoturvatiimin jonoon 4. maaliskuuta saapunutta tikettiä, joka liittyy Visual Studio Coden lisäosan asentamiseen, ei ole vielä käsitelty loppuun, koska tekijä ei ole vastannut lisätietokysymyksiin. Tavallisessa tapauksessa häiriötiketti suljettaisiin, jos käyttäjä ei reagoi lisätietopyyntöihin viikon kuluessa, mutta koska tässä voi olla kyse tietoturvapoikkeamasta, tikettiä ei ole vielä suljettu.

Tapa, jolla tämän mahdollisen tietoturvapoikkeaman käsittely hoidetaan, ei ole kovin tehokas tai hallittu, eikä riskin omistaja ole selkeästi määritelty. Tässä tapauksessa kyse on kuitenkin yksittäisestä käyttäjästä, joka on itse ilmoittanut ongelmasta liittyen järjestelmään, joka ei tietojemme mukaan kuulu organisaation käytössä oleviin järjestelmiin. Tapauksella ei siis ole korkeaa prioriteettia. Suurin huoli kuitenkin on, että työkoneelle on mahdollisesti asennettu sovellus, joka ei kuulu järjestelmäsalkkuun. Koska minulla ei ole pääsyä järjestelmäsalkkuun, joutuisin konsultoimaan muita asiantuntijoita, mutta kyseinen häiriötiketti on kuitenkin nyt toisen asiantuntijan hoidossa.

Kävimme tietoturvapäällikön kanssa alustavasti lyhyen keskustelun hallintakeinojen kypsyysarvioinneista sekä in-house-yhtiön kanssa tehtävän yhteistyön haasteista. Käytössämme on

riskienhallintajärjestelmä, johon merkitään tunnistetut riskit, niiden omistajat sekä korjaavat toimenpiteet. Jokaiselle hallintakeinolle on tehty oma kohde, jotta kypsyystasoa ja mahdollisia parannustoimenpiteitä voidaan arvioida erikseen. Toistaiseksi kypsyystaso arvioidaan saatavilla olevan dokumentaation perusteella.

Koska osaan arvioinneista ei ole saatu pyydettyä dokumentaatiota, niille on jouduttu merkitsemään matala kypsyystaso, vaikka ne olisivatkin käytännössä toteutettu hyvällä tasolla. Osa hallintakeinojen kypsyysarvioinneista on vielä aloittamatta, joten yritän löytää sellaisen hallintakeinon, jonka arviointia voisin edistää suhteellisen itsenäisesti.

Vaikka osa hallintakeinojen kypsyystasoista ei ole toivotulla tasolla, NIS2-direktiivin vaatimukset voidaan silti täyttää. ISO 27001-standardin hallintakeinojen kattavuus on laajempi kuin NIS2-direktiivin 21 artiklan kymmenen keskeistä vaatimusta. Tämän vuoksi voimme priorisoida tiettyjä hallintakeinoja ja keskittyä niiden kehittämiseen tulevaa lainsäädäntöä varten. Priorisoitujen hallintakeinojen kypsyysarvioinnit on tehty ainakin alustavasti, ja niihin liittyviä korjaavia toimenpiteitä on jo merkitty riskienhallintajärjestelmään. Tietoturvapäällikkö on järjestänyt palavereita riskien omistajien kanssa näistä.

Tiistai 18.3

Olin varannut täksi päiväksi palaverin vastuukäyttäjien kanssa liittyen viime torstaina esiteltyyn asiakastietojen kyselyjärjestelmän väärinkäytön havainnointiin. Kävimme läpi tilanteen ja analyysini ja pohdimme tämän perusteella mahdollisia ratkaisuja. Loimme lisää tilastoja järjestelmän käytöstä ja analysoimme niiden perusteella parhaat tavat havaita väärinkäyttöä. Tietoturvasyistä en avaa tässä opinnäytetyössä analyysimme tarkempia yksityiskohtia.

Järjestelmän toiminnasta heräsi muutamia kysymyksiä, joten lähetimme järjestelmätoimittajan edustajalle kysymyslistan. Kysymyksemme liittyivät lokien hallintaan sekä siihen, mihin lokeihin meillä on oikeuksia vastuukäyttäjinä. Olimme myös kiinnostuneita siitä, miten muut organisaatiot ovat toteuttaneet valvontaa, ja tiedustelimme, onko järjestelmätoimittajalla tietoa heidän ratkaisuistaan. Väärinkäytösepäilyt tulisi raportoida myös järjestelmätoimittajalle, mutta halusimme selkeyttä siihen, miten prosessi tulisi käytännössä toteuttaa.

Loput työajasta kului sovelluspalveluihin liittyviin tehtäviin sekä tietoturvatiimin jonoon tulleiden tikettien käsittelyyn, jotka olivat pääasiassa neuvontapyyntöjä.

Keskiviikko 19.3

Keskiviikko käynnistyi kuukausittaisella yksikkökokouksella, jossa kävimme läpi alayksiköiden työtilannetta. Tietojohtaminen ja tilastopalvelut -yksikön edustajat esittelivät myös tulevaa tietojohtamisen toimintamallia. Esityksessä en huomannut mainintaa tietoturvallisuuden toteuttamisesta, mutta siinä korostettiin tavoitteena olevan tietojen saatavuuden ja

luotettavuuden parantaminen, jotka ovat osa tietoturvan kolmea peruspilaria: luottamuksellisuus, eheys ja saatavuus.

Esityksestä tuli mieleeni in-house-yhtiön asiantuntijan aiemmin mainitsema tietoturvajohtamisen muutoshanke 2025–2028, ja pohdin, miten nämä liittyvät toisiinsa, voisiko esimerkiksi tuleva toimintamalli olla osa muutoshanketta. In-house-yhtiön asiantuntija oli luvannut vielä palata kysymyslistoihini, mutta oli myös ehdottanut palaveria viime viestissään. Aloitin alustavat taustatyöt mahdollista palaveria varten kokoamalla omia kysymyksiä, erityisesti siitä, miten tietojohtamisen muutoshanke liittyy ISO 27001-standardin hallintakeinojen kypsyysarviointeihin. Lisäksi pohdin jälleen, miten voisimme edistää yhteistyötä heidän kanssaan.

Aloitin tänään myös tietojen kokoamisen visuaaliseen karttaan SOTE-toimialaan liittyvistä laeista, määräyksistä ja vaatimuksista sekä siitä, mitä standardeja ja kriteeristöjä voimme soveltaa prosessien kehittämisessä. Alustavasti keräsin ISO/IEC 27000-standardiperheen standardit, THL:n määräykset, EU-direktiivit, kansalliset kriteeristöt kuten Julkri, Katakri ja Pitukri, sekä asiakastietolain ja vuoden 2016 NIS-direktiiviin liittyvää lainsäädäntöä, kuten tietosuojalaki ja laki julkisen hallinnon tiedonhallinnasta. Tarkoituksena on laatia lyhyet selitykset jokaiselle kohteelle ja yhdistää eri elementit visuaalisesti.

Tänään sain myös hyvin kattavan vastauksen asiakastietojen kyselyjärjestelmään liittyen. Varasin ensi viikoksi toisen palaverin vastuukäyttäjien kanssa, ja ennen sitä käyn perusteellisesti läpi järjestelmätoimittajan edustajan vastauksen.

Torstai 20.3

Osallistun poikkeuksellisesti tänään tietoturvatiimin viikkopalaveriin, koska sovelluspalvelun viikkopalaveri korvataan tämän viikon perjantaina kehittämisiltapäivällä. Agendalla on tällä hetkellä ISMS:n vuosikellon kehittäminen, joka odottaa johdon kommentointia ja hyväksyntää. Vuosikellossa on merkitty kvartaaleittain tai kuukausittain, mitkä asiat tulisi tarkistaa ja tarvittaessa päivittää, muun muassa riskijärjestelmään nostetut riskit. Kävimme myös läpi vakavimmat tietoturvapoikkeamat ja -häiriöt.

Tietosuojan vaikutustenarvioinnin (TSVA) prosessia tulisi kehittää tietoturvatiimin asiantuntijoiden näkökulmasta. Tällä hetkellä tietoturvatiimin asiantuntija osallistuu lähes jokaiseen TSVA-palaveriin liittyen eri järjestelmiin, vaikka suurin osa käsitellyistä asioista liittyy tietosuojaan, eikä suoraan tietoturvaan. Tavoitteena on tehostaa tietoturvatiimin osuutta ja luoda mahdollisimman varhaisessa vaiheessa tietoturvan kypsyys- ja riskiarviointi, kun tietyn järjestelmän TSVA käynnistetään.

Tämän palaverin ansiosta minulle selkeni myös MCSB:n (Microsoft Cloud Security Benchmark) tärkeys ja miksi meidän kannattaa huomioida kyseinen viitekehys. Muutama järjestelmää on

siirtymässä Azuren julkipilvipalveluihin ja jotkut järjestelmät ovat jo siirtynyt, joten Microsoftin kehittämä viitekehys on kullanarvoinen näiden järjestelmien ylläpidossa ja hallintakeinojen kehittämisessä. Pyrin tutustumaan mahdollisimman pian myös NIST SP 800-53 -hallintakeinoihin, joihin on CIS:n hallintakeinojen lisäksi viitattu laajasti MCSB-viitekehyksessä.

Kahden viikon päästä tietoturvatiimin agendalla on osallistuminen muutamaan suun terveydenhuoltoon liittyvään projektiin, muun muassa uuden järjestelmän käyttöönottoon ja uusien laitteiden kilpailutukseen. Tiistaina 1.4. ja keskiviikkona 2.4. järjestetään kuuden palvelutarjoajan intraoraaliskannereiden esittelyt, joihin ilmoittauduin osallistuvani. Skannerit ovat suunniteltu hampaiden skannaamiseen ja tuottavat digitaalisia 3D-skannauksia.

Perjantai 21.3

Tämän viikon perjantain aamupäivä kului sovelluspalvelujen tehtävissä, ja iltapäivällä järjestettiin sovelluspalvelujen alayksikön kehittämisiltapäivä. Tämän vuoksi en ehtinyt edistää tietoturvatiimin asioita.

Viikkoanalyysi

Vaikka toimialamme panostaa ISO 27001-standardin mukaisuuteen, ei ole välttämätöntä täyttää jokaisen hallintakeinon kypsyystavoitetta, jos ensisijaisena tavoitteena on täyttää NIS2-direktiivin vaatimukset. Tätä tietoa tulisi hyödyntää mahdollisimman paljon, varsinkin kun meillä on ollut suuria kommunikaatiohaasteita tietyn sidosryhmän kanssa hallintakeinojen kypsyysarvioinneissa, eikä ole tehokkaasti pystytty luoda analyysi nykytilanteesta. Tieto vaikuttaa myös visuaaliseni kartoitukseni luomiseen.

MCSB ja sen jäsennelty lähestymistapa hallintakeinojen toteuttamiseen julkipilviympäristössä on tullut tutuksi minulle viime viikkojen aikana. En ole kuitenkaan mukana missään projektissa tai käsittelen mitään sovellusta, jonka toteutus olisi esimerkiksi Azuren julkipilvessä, joten en ole pystynyt konkreettisesti nähdä, miten MCSB:n listatut hallintakeinot ovat toteutettu.

Asiakastietojen kyselyjärjestelmän väärinkäytön havainnointia tulee myös kehittää ja mahdollisesti automatisoida. Ensi viikolla pidämme aiheesta palaverin, jossa käymme läpi järjestelmätoimittajalta saamamme tiedot.

3.5 Viikko 5

Seurantajakson puolessavälissä en ole vieläkään edistänyt mitään hallintakeinon kypsyysarviointia. Aion tänä viikkona analysoida ja konkretisoida, mitkä NIS2-direktiivin 21 artiklan vaatimukset kohtaavat mihinkin ISO 27001-standardin hallintakeinoihin. Analyysini perusteella käyn

läpi riskijärjestelmäämme merkatut kypsyysarvioinnit ja niiden kypsyystasot sekä mahdolliset puutteet.

In-house-yhtiön asiantuntijan ja meidän tietoturvatiimimme keskeistä palaveria ei ole vielä suunniteltu, mutta näennäisesti emme pysty järjestää palaveria kaikilla tietoturvatiimin jäsenillä lyhyen ajan sisällä. Pyrin kuitenkin tänä viikkona laatimaan pohjaa mahdolliseen palaveriin, jotta saisimme siitä maksimaalista hyötyä.

Maanantai 24.3

Sovelluspalvelujen tehtävien suorittamisen jälkeen kävin tutkimaan VSC:hen liittyvä tietoturvatiketti. Tämä oli automaattisesti suljettu järjestelmän toimesta, koska käyttäjä ei ollut vastannut lisätietopyyntöihin, emmekä näin saatu ikinä selvää mihin tarkoitukseen hän käytti kyseistä ohjelmaa. Sain kuitenkin selvitetty, että se on in-house-yhtiön vastuulla määritellä ja rajoittaa mitkä sovellukset käyttäjä pystyy asentaa mihinkin laitteeseen. Organisaatiossa on käytössä sovelluskeskus, jonka kautta pystyy asentamaan sallitut sovellukset. Periaatteessa käyttäjä ei pysty asentaa kuin näitä, mutta ilmeisesti on jonkinlaisia poikkeuksia, mikä tuo mukanaan riskin, joka pitäisi arvioida. Epäilen, että emme tule saamaan listaa näistä poikkeuksista pyydättäessämme.

Iltapäivällä pidimme tietosuojan asiantuntijoiden ja erityissuunnittelijoiden kanssa suunnittelupalaverin. Aiheena oli tutkimuslupahakemuksen kehittäminen. Tietoturvatiimimme oli kutsuttu mukaan, jotta saataisiin myös tietoturvanäkökulma huomioitu hakemuksessa. Hakemuksen lomake on hyvin kattava tietosuojan näkökulmasta jo, mutta siinä ei ollut vielä huomioitu tietoturvaa. Lomakkeessa oli muutamia avointa kysymystä, joten ehdotuksemme oli, että tietoturvaan liittyvä kysymys olisi myös avoin ja osittain ohjeistettu. Hakijan tulisi vastata esimerkiksi siihen, että mitkä tallennusvälineitä tai pilvipalveluita hän käyttää tutkimukseen, millä sovelluksilla hän käsittelee tutkimusdatansa ja onko käytössä koulun, työn tai omat laitteet. Seuraava kokous on kuukauden päästä, ja ennen sitä lomakkeen suunnittelijat haluaisivat vielä konsultoida tietoturvatiimiä, joten odotetaan yhteydenottoa.

Tiistai 25.3

Suurin osa tästä päivästä meni sovelluspalvelujen tehtäviin. Tänään oli myös tarkoitus käydä läpi muiden vastuukäyttäjien kanssa, minkälainen prosessi haluaisimme kehittää asiakastietojen kyselyjärjestelmän mahdollisen väärinkäytön seurantaa. Kaikilla ei ollut mahdollisuutta osallistua, joten palaveri siirtyy ensi viikolle.

Aloitin iltapäivällä kartoittamaan, mitkä NIS2-direktiivin vaatimukset kohdistuvat mihin ISO 27001-standardin hallintakeinoihin. Kävin alustavasti läpi otsikkokohtaisesti vaatimukset sekä hallintakeinot, ja tässä vaiheessa mietin, että joku on varmasti tehnyt tätä ennen minua.

Käyttämällä selaimessa hakukonetta, löysin hakusanoilla ”NIS2”, ”ISO 27001” ja ”mapping” (suom. kartoitus) monta sivustoa, jossa on listattuna ja kartoitettuna direktiivin vaatimusten ja standardin hallintakeinojen suhdetta. Nämä ovat suurin osin samanlaiset, mutta poikkeamia löytyy. Listaukset ovat tietoturvayrittäjän tai -yritysten luomia, eikä vaikuta olla olemassa virallista kartoitusta tehtyä, esimerkiksi EU:n puolelta. Listaukset ovat melko pitkiä, enkä näin ollen liitä mikään niistä tähän dokumenttiin.

Kävin näiden läpi toimialamme riskijärjestelmään merkatut kypsyysarvioinnit ja huomasin muutamaa aloittamatta kypsyysarviointia, jotka kohdistuvat NIS2-direktiivin vaatimuksiin. Nämä ovat kuitenkin semmoisella tasolla, etten itse pysty näitä edistämään itsenäisesti, enkä mainitse näitä hallintakeinoja tässä opinnäytetyössä tietoturvasyistä.

Keskiviikko 26.3

Keskiviikkona pidimme tietoturvatiimin kanssa pitkästä aikaa ISMS-toteutushankkeen statuspalaveri, jossa pyrimme käydä läpi missä vaiheessa kukin ISMS-toteutushankkeen aliprojektien ja minkälaisia edistyksiä tai tehtäviä on huomioitava. Tietoturvapoikkeamien keskitetty hallinta-aliprojekti edistyy hitaasti mutta varmasti. Käytössämme on Splunkin sovellus, jonka avulla pystymme jäsentämään ja normalisoida sovellus- tai järjestelmälokeja, jotta pystyisimme havaitsemaan väärinkäyttöä tai kyberuhkia (Kidd 2024).

Tässä kapasiteetissa puhutaan System Information and Event Management -ratkaisusta (SIEM), joka pystyy kerätä dataa hyvin laajasta valikoimasta laitteista ja sovelluksista sekä korreloida eri tapahtumat esimerkiksi ajan perusteella (Kidd 2025). SIEM-ratkaisun voidaan tehostaa Security Orchestration, Automation and Response -ratkaisun (SOAR) avulla. Kun SIEM-ratkaisussa nousee hälytyksiä, SOAR-ratkaisun voi automaattisesti vastaa näihin ja tehdä automatisoituja toimenpiteitä, sen sijaan, että ammattilainen kävisi manuaalisesti läpi hälytykset (Kidd 2023).

Tärkeimmät järjestelmät keräävät jo lokeja, jotka voimme pyytää tarvittaessa palveluntarjoajalta. Ongelma on lähinnä se, että meillä ei ole keskitettyä automatisoitua tapa seurata tietoturvapoikkeamat, vaan joudumme pyytämään erikseen lokeja ja syöttää ne Splunkiin. Mitä vaan lokitieto on yleensä valtava jopa lyhyestä ajasta, mutta pystymme melko tehokkaasti kohdistaa lokihakuja, jos on tiedossa mitä tietoa halutaan tietystä järjestelmästä ja esimerkiksi tietystä käyttäjästä. Työ on kuitenkin manuaalista, eikä pystytään vielä automaattisesti havaita tietoturvapoikkeamat tietyissä järjestelmissä.

Haluamme myös kehittää erillinen tikettijono tietoturvatiimille, johon voidaan ohjata käyttäjien havaittua tietoturvapoikkeamiin liittyvät tiketit. Teimme alustava tiedustelupyynnön tästä in-house-yhtiölle helmikuun alussa, mutta asia ei ole edistynyt. Tavoite olisi, että saisimme manuaalisesti luotuja tietoturvapoikkeamahavaintoja keskitetty yhteen paikkaan, josta olisi helpompi seurata ja käsitellä niitä. Tällä hetkellä havainnot tulevat esimerkiksi

tietoturvapäällikölle sähköpostitse tai puhelimitse esille, tai yleisellä palvelupyynnöllä tiketti-järjestelmään.

Agendalla olisi ollut paljon muutakin, mutta aika loppui kesken ja siirrettiin seuraavaan palaveriin, liittyen tietoturvapoikkeamien hallintaan. Mukana oli tietoturvatiimin lisäksi ulkoisen sidosryhmän tietoturvakonsultit, jonka kanssa kehitetään prosesseja. Kävimme tänään läpi konsulttien luoma prosessikaava MIM-prosessista, jonka prioriteetti oli noussut 6.3 tapahtuneen häiriötilanteen myötä. Tällä hetkellä ei ole selkeästi dokumentoitu, mitkä roolit ovat vastuussa mistäkin asiasta MIM-häiriötilanteessa, eikä prosessia ole organisaation puolesta kuvattua. Ehdotetusta prosessikaavasta tulee selkeästi esille MIM-prosessin eri vaiheet ja tukidokumentaation tarkoitus on tuoda selkeästi esille mitä on kenenkin vastuulla sekä minkälaisia vastuuhenkilöitä tulisi määritellä. Dokumentaatio on vielä kesken ja pidetään seuraava palaveri muutaman viikon päästä.

Torstai 27.3

Torstaipäivä meni kokonaan sovelluspalvelujen viikkopalaverissa ja tehtävissä.

Perjantai 28.3

Tänään nousi puheeksi sovelluspalveluissa oleva ongelma, liittyen tietojärjestelmän lokeihin. Terveysasemalla oli havaittu mahdollista väärinkäyttöä, ja tietosuojan asiantuntijat olivat tilanneet tietyn ammattilaisen käyttölokit ylihoitajalle. Vaikka lokitiedot olivat jäsennelty ja karsittu mahdollisimman paljon, rivejä oli kuitenkin kymmeniä tuhansia, koska lokit menivät kaksi vuotta taaksepäin. Tällä hetkellä ei ole dokumentoitua tai kuvattua automatisoitua prosessia, jonka avulla voisimme analysoida käyttölokit; ainut tapa on käydä manuaalisesti läpi niitä, esimerkiksi Splunkin avulla. Sen lisäksi tämä olisi ylihoitajan vastuulla käydä läpi, eli ammattilainen, jolla ei välttämättä ole kokemusta tai koulutusta tähän tehtävään.

Kävimme alustavasti läpi, miten voisimme helpottaa ylihoitajan työtä ja mitä työkalu voisimme käyttää. Tietoturvapäällikkö suositteli myös Splunkin käyttö, jonka erän toiminallisuuden on nimenomaan lokien normalisointia, eikä sovellus tallenna tietoja julkipilvipalveluihin. Pidetään maanantaina palaveri Splunk-asiantuntijan kanssa ja käymme tarkemmin läpi mitkä tiedot halutaan lokeista.

Tietoturvapäällikön ja sovelluspalvelujen vastaava asiantuntijan kanssa kävimme läpi riskijärjestelmään merkatut kriittisimmät riskit ja miten voisimme edistää niiden riskienhallinta. Jälleen on todettava, että dokumentaatiota ja standardisoituja prosesseja ovat suurin puute organisaatiossa ja tuovat näin ollen suurimmat riskit, ainakin teoriassa. Tietoturvapoikkeamien automatisoidun havainnointiin halutaan hyödyntää Splunk-sovellusta enemmän ja käymme

ensi viikolla läpi Splunk-asiantuntijan kanssa, miten voisimme normalisoida ja luoda haluamamme hälytyksiä potilastietojärjestelmästä tulleista lokeista.

Viikkoanalyysi

Tässä vaiheessa seurantajaksoa voin varmuudella todentaa, että ilman sujuvaa yhteistyötä in-house-yhtiön kanssa, en pysty edistämään mitään hallintakeinon kypsyysarviointia merkittävällä tavalla. Esimerkiksi oli myös tietoturvapäällikölle luvattu jo ajat sitten, että hänelle lähetetään dokumentaatiota liittyen varmuuskopiointiin tai ylipäätänsä informaatio siitä, miten se on toteutettu organisaatiossa, eikä ole saanut mitään siihen liittyen. Pidetään mahdollisesti palaveri hallintakeinojen kypsyysarviointien yleiskuvasta in-house-yhtiön edustajien kanssa, mutta emme aktiivisesti edistä sitä meidän puoleltamme tällä hetkellä; yhteistyökuvan muutokset ja muutosaloitteen on tultava kaupungin kanslian tasolta. Tietoturvapäällikkö on ollut yhteydessä myös tästä asiasta jo ajat sitten kaupungin kansliaan useampaan kertaan.

Viime viikon perjantaista lähtien olen saanut osallistua tietoturvapoikkeamien hallinnan aliprojektiin liittyviin palavereihin ja olen saanut yleiskuvan aliprojektin haasteista ja tarpeista. Tässä aliprojektissa olemme myös riippuvaisia in-house-yhtiön ja sen hallinnoimista järjestelmistä, mutta voimme silti toimialaisesti implementoida omia prosessia ja valvontaa. Aliprojekti on tullut kaupungin kanslian tasolta, joten in-house-yhtiö on käsittääkseni aktiivisesti mukana työstämässä keskitetty CSOC-palvelua organisaatioon. Toimialakohtaisesti on kuitenkin implementoitava järjestelmien lokien automatisoitua valvontaa esimerkiksi Splunk-järjestelmään ja konfiguroimaan sääntöjä ja hälytyksiä tarpeemme mukaan.

Tällä viikolla kaikilla asiakastietojen kyselyjärjestelmän vastuukäyttäjillä ei ollut mahdollisuutta osallistua väärinkäytön havainnointipalaveriin, eikä seuraavalla viikolla, joten lykkäsimme sen kahden viikon päähän. Tässä vaiheessa on tärkeää, että kaikki ovat tietoisia siitä, miten tilanne kehittyy, varsinkin kun meitä on määrällisesti melko vähän. Toisaalta tästäkin järjestelmästä voidaan pyytää lokeja ja myös itse ladata käyttötilastot CSV-tiedostoon, joten voisimme mahdollisesti hyödyntää Splunkia myös tässä. Tästä syystä olisi hyödyllistä keskustella myös Splunk-asiantuntijan kanssa aiheesta, ennen kuin pidämme vastuukäyttäjien kanssa palaverin.

3.6 Viikko 6

Tuleva viikko on hyvin pitkälti jo suunniteltu työn puolelta. Maanantaiksi on suunniteltu sovelluspalvelujen tehtävien lisäksi palaveri Splunk-asiantuntijan kanssa liittyen lokien hallintaan. Tiistai ja keskiviikko menevät kokonaisuudessaan intraoraaliskannereiden esityksissä kilpailutusta varten. Torstai on myös täysin varattuna sovelluspalvelujen tehtäviin ja viikkopalaveriin, paitsi iltapäivällä osallistun ensimmäiseni TSVA:n alkupalaveriin moneen kuukauteen. Perjantaina on myös toisesta järjestelmästä TSVA:n alkupalaveri ja sovelluspalvelujen

tehtävien lisäksi olen varannut pari tuntia intraoraaliskannereiden yhteenvedon tekemiseksi. Näin ollen ei ole tälläkään viikolla aikaa kehittää asiakastietojen kyselyjärjestelmän väärinkäytön havainnointiprosessia vastuukäyttäjien kanssa. Jos jää ylimääräistä aikaa, niin käytän sitä todennäköisesti Splunk-järjestelmän perehtymiseen.

Maanantai 31.3

Iltapäivällä kävimme läpi sovelluspalvelujen asiantuntijoiden ja Splunk-asiantuntijan kanssa, miten voimme ohjeistaa ja mahdollisesti helpottaa lokien lukeminen ja tulkitseminen muille ammattilaisille. Kyseinen loki on itsessään vajaa 70 000 riviä ja yksi rivi sisältää aikaleima, tapahtuman selite, ammattilaisen tunniste, potilaan perustiedot sekä mahdolliset erityislisäykset, muun muassa erityisen syyn vahvistaminen.

Erityisen syyn vahvistaminen-kenttä on sinänsä tärkeä tässä tapauksessa, koska tämä kenttä on täytettävä vain, jos järjestelmä havaitsee, että ammattilaisella ei ole suoraa hoitosuhdetta tiettyyn potilaan kanssa. Sen perusteella voimme suodattaa lokia hyvin tehokkaasti ja nähdä vain niiden potilaiden nimet, johon on käytetty erityisen syyn vahvistaminen. Tämä ei kuitenkaan automaattisesti tuo näkyvyyttä siihen, mitä tietoja ammattilainen on hakenut, vaan on merkattava ylös aikaleima ja potilaan nimi ja käyttää etsi-toimintaa ilman suodatinta.

Olimme tässä vaiheessa kuitenkin saaneet ensiapuratkaisu siihen, miten ylihoitaja voisi tässä tapauksessa lähteä ratkomaan väärinkäytön tunnistaminen, suodattamalla erityisen syyn vahvistamisen tapahtumat. Kävimme alustavasti läpi myös, miten voisimme tulevaisuudessa automatisoida tätä prosessia ja helpottaa väärinkäytön havainnointi Splunkin avulla. Splunk-asiantuntija konsultoi vielä palveluntarjoajaa, miten voisimme implementoida lokit tehokkaasti Splunkiin.

Tiistai 1.4

Intraoraaliskannereiden esittelylle on varattu aikaa koko täksi päiväksi sekä huomiseksi. Yhteensä on kuusi palveluntarjoajaa, josta kolme esittää tuotteensa tänään. Organisaatiomme puolelta osallistuu suhteellisen iso määrä asiantuntijaa. Kliiniseltä puolelta osallistuvat ylihammaslääkäri, apulaisylihoitaja, hankinnoista vastaava suuhygienisti ja hankinnoista vastaava hammaslääkäri. Tietohallinnon yksiköstä osallistuvat seuraavasti: tekniseltä puolelta johtava asiantuntija sekä kaksi tietoliikenteen ICT-asiantuntijaa, digitaalisen kehittämisen yksiköstä kaksi asiantuntijaa, ja tietoturvan puolesta osallistuu tietoturva-asiantuntija sekä minä.

Tietoturvan näkökulmasta keskeistä olisi saada hahmotusta, miten datavirrat liikkuvat, miten käyttäjänhallinta on toteutettu ja onko laitteisiin liittyvä sovellus tietoturvallinen. Yllättävin

asia oli nähdä, miten suuria eroja voi olla toteutustavoissa eri palveluntarjoajilla. Avaan kaikkien esittelyt huomisen kirjauksissa, jotta olisi käytännöllisempää verrata ja listata niitä.

Keskiviikko 2.4

Esittelyt jatkuivat tänään ja organisaation puolelta osallistumme samalla kokoonpanolla kuin eilen.

Jokainen intraoraalinen skanneri käyttää eri sovellus, mutta datavirrat olivat suhteellisen samankaltaisia. Keskeistä tässä on, että jokainen laite käyttää WiFiä jollain tavalla. Skannerit toimivat niin, että ne ottavat jokaisessa sekunnissa kymmeniä korkealaatuisia digitaalisia kuvia eri kulmista ja näin ollen yksi skanneri vaatisi vähintään 50mbit/s yhteys WiFin kautta.

Yhden palvelutarjoajan tapa siirtää dataa oli ainutlaatuisin kaikista: laite lähettää tiedot suoraan palvelutarjoajan pilvipalveluun, ilman mitään välilaitetta. Ainakin tämä on tulevaisuuden tavoite, koska nyt palvelutarjoajan mukaan joutuu kuitenkin käyttää ”purskutin”, joka pystyy tehokkaammin ja luotettavammin siirtää tarvittavat datamäärät. Toiset toteutustavat käyttävät kaikki jonkinlainen USB-laite, joka yhdistää skanneri ja tietokone, joko WiFi 6:lla tai WiFi Directillä.

Koska suurin osa skannereista yhdistyvät suoraan tietokoneeseen, vaikka se on langaton yhteys, niin luokitellaan kokonaisuus lääkinnälliseksi laitteeksi, tai vähintään lääkinnälliseksi lisälaitteeksi, EU:n Medical Device Regulation-asetuksen, MDR, mukaan (Asetus 2017/745/EU). Vaikka MDR-asetus on hyvin olennainen direktiivi SOTE-toimialalle, niin se ei suoranaan käsitä tietoturvaa, joten en avaa aihetta tässä opinnäytetyössä. Pyysimme kaikilta esittelijöiltä teknistä dokumentaatiota käytetystä laitteistosta ja datavirtakaavioita.

Sovellusten käyttäjähallintaa on myös toteutettu hyvin erillä tavailla. Jossain sovelluksissa määritellään pääkäyttäjä, joka hallinnoi organisaation käyttöoikeudet joko sovelluksen kautta tai palvelutarjoajan kautta. Toisen sovelluksen käyttäjähallinta on integroitu suoraan Windowsin Active Directoryyn ja on näin suoraan palvelun käyttäjän vastuulla hallinnoimaan.

Muutamassa sovelluksessa käyttäjätili on laitekohtainen, eikä henkilökohtainen, eikä näin ollen täyttää tietosuojavaatimuksia. Esimerkiksi ei pystytä varmuudella sanoa lokien perusteella, kuka ammattilainen on katsonut mitä tietoja, jos on käytössä laitekohtainen yhteiskäyttötili. Näin ollen lokitus ja käyttäjähallinta eivät täytä asiakastietolain (703/2023) tai EU:n yleinen tietosuoja-asetus GPDR:n vaatimuksia (Asetus 2016/679/EU). Vaikka tietosuoja ja tietoturva tukevat toisiaan, en avaa tässä opinnäytetyössä GDPR-asetusta.

THL:n määräyksen 4/2024 mukainen sovelluksen luokittelu on tehty vain kahdelle kuudesta sovelluksesta. Luokitellut järjestelmät löytyvät Valviran Astori-rekisteristä, mikä tarkoittaa, että ne täyttävät asiakastietolain ja toisiolain vaatimukset (Valvira 2025a). Rekisteristä löytyy

myös sovelluskohtaisia huomioita, jotka liittyvät käyttöönottoon ja tietoturvaan. Molemmat kyseiset sovellukset ovat B-luokkaa, mikä tarkoittaa, että ne eivät ole yhteydessä suoraan Kanta-palveluihin, eivätkä edellytä tietoturvallisuuden arviointia tai tietoturvallisuustodistusta. Asiakastietolain (703/2023) mukaan sovellus, jossa käsitellään asiakas- tai potilastietoja, on oltava luokiteltu ja rekisteröity, jos halutaan ottaa sitä käyttöön SOTE-toimialalla.

Torstai 3.4

Suurin osa torstaipäivästä kului suunnitellusti sovelluspalvelujen viikkopalaverissa ja siihen liittyvissä tehtävissä, mutta iltapäivällä osallistuin pitkästä aikaa tietosuojan vaikutustenarviointiin (TSVA). TSVA:n tarkoituksena on kartoittaa uuden sovelluksen tai lisäyksen riskejä, jotka liittyvät asiakas- tai potilastietojen tietosuojaan. Arvioinnin yhteydessä käsitellään myös sovelluksen teknistä toteutusta ja tarkistetaan, miten tietoturva on toteutettu ja varmistettu.

Kyseinen TSVA koskee lisäys toiseen sovellukseen, josta on jo tehty TSVA, joten melko paljon taustatietoa on jo dokumentoitu ja voidaan viitata siihen. Uutena sovelluksessa on uusi tapa ottaa yhteyttä asiakkaaseen tai potilaaseen, ja arvioidaan, tuleeko uusia riskejä tässä toteutuksessa. Tänään ei päästy kuitenkaan tietoturvan tekniseen osuuteen, jatketaan seuraavan viikon palaverissa.

Perjantai 4.4

Aloitin perjantaipäivän laatimalla pohjan intraoraaliskannereiden kartoitusta ja yhteenvedon laatimista varten. Tarkoituksena on arvioida jokaisen skannerin ja sen käyttämän sovelluksen osalta tietoturvallisuuteen liittyviä huolia. Tietoturvan, tietosuojan ja asiakastietolain (703/2023) näkökulmasta neljä kuudesta vaihtoehdosta eivät ole edes kilpailutuksessa varteenotettavia, koska niiden sovelluksissa käsitellään asiakas- tai potilastietoja, mutta sovellukset eivät ole luokiteltu Astori-rekisteriin. Keskityn näin ollen erityisesti kahteen vaihtoehtoon, joiden sovellukset on asianmukaisesti luokiteltu, mutta täytän kartoituspohjan kaikkien skannereiden osalta mahdollisimman kattavan vertailun varten.

Tänään alkoi toinen TSVA, myös liittyen lisäykseen järjestelmäsalkussa olevaan sovellukseen. Palaveriin osallistuivat yhdeksän ammattilaista eri yksiköistä ja palveluntarjoajien puolelta. Vaikka palaveri kesti kaksi tuntia, emme päässeet käsittelemään lisäyksen teknistä toteutusta sen tarkempaa. Sovelluksen palveluntarjoajan puolelta ei ollut teknistä asiantuntijaa paikalla, eikä ollut myöskään muuta teknistä dokumentaatiota kuin datavirtakaavio, missä oli piirretty laite, josta osoittaa nuoli sovellukseen. Ensi viikkona TSVA jatkuu.

Viikkoanalyysi

Mennyttä viikko oli suurin osin omistettu intraoraaliskannereiden kilpailutukseen. Henkilökohtaisesti pidin esittelyt ja skannereiden sovellusten toteutustavat kiinnostavina, ja oli antoisaa

analysoida jotain konkreetista, johon oli monta vertailukohdetta. Jatkan vielä ensi viikkona kartoitusta ja yhteenvedon luomista omasta puolesta ensi viikkona.

Skannereiden esittelyjen ja sovelluspalvelujen tehtävien ohessa suurin osa työajasta meni TSVA:ihin, jonka prosessin tehokkuus epäilen, että kaipaa tehostamista ja kehittämistä. Tästä on ollut ainakin tietoturvatiimin puolesta jo puhetta, että tietoturva-asiantuntijan ei tarvitsisi osallistua jokaiseen TSVA-palaveriin, koska suurin osa käsitellyistä aiheista liittyvät tietosuojaan.

Splunkin käyttötarkoitus ja käytännöllisyys ovat mielestäni tällä hetkellä kiinnostavimpia aiheita tietoturvapoikkeamien hallinnan aliprojektiin liittyen. Toimiva SIEM-ratkaisu tarjoaa vankan pohjan tietoturvapoikkeamien havainnointiin, ja SOAR-ratkaisun avulla voidaan jopa automatisoida reaktiot näihin tietoturvapoikkeamiin. En ehtinyt perehtyä Splunkiin tämän viikon aikana tarkemmin, mutta mieleeni tuli, että sovellusta voisi mahdollisesti hyödyntää asiakastietojen kyselyjärjestelmän väärinkäytön havainnointiin. Aion selvittää ensi viikolla, olisiko integraatio tämän järjestelmän kanssa mahdollinen.

3.7 Viikko 7

Tämän viikon ensimmäinen prioriteetti on saada valmiiksi intraoraaliskannereiden kartoitus ja lähettää dokumentti muiden asiantuntijoiden täytettäväksi ja kommentoitavaksi. Näin voimme tarvittaessa lähettää lisätietopyynnöt toimittajille ennen kilpailutuksen etenemistä. Toinen prioriteetti on selvittää, onko mahdollista integroida asiakastietojen kyselyjärjestelmän käyttötilastot Splunkiin. Pidämme myös jatkopalaverin Splunkin asiantuntijan kanssa liittyen 31. maaliskuuta käsitellyn tietojärjestelmän lokitietoihin ja mahdollisen väärinkäytön havainnointiin. Kolmantena prioriteettina on osallistua tietoturvan näkökulmasta viikoittaisiin tietosuojan vaikutusten arviointipalavereihin (TSVA), joissa arvioidaan uusien sovellusten vaikutuksia asiakas- ja potilastietojen suojaan.

Maanantai 7.4

Viikko alkoi sovelluspalvelujen tehtävien parissa ja päättyi kahden tunnin TSVA-palaveriin. Valitettavasti palaverissa ei vieläkään päästy käsittelemään tietoturvan näkökulmaa.

Tiistai 8.4

Seuraavana päivänä tietoturva-asiantuntija otti yhteyttä minuun liittyen käytyihin TSVA:ihin. Toimialan tietoturvatiimi on itse kehittänyt dokumenttipohjan sovelluksen tietoturvan kypsyysarvioinnista, ja täytimme yhdessä kypsyysarviointia mahdollisimman kattavasti saadun dokumentaation perusteella eilisen TSVA:han liittyvästä sovelluksesta. Dokumenttipohja perustuu vahvasti THL:n määräys 3/2024 vaatimuksiin ja tarkoitus on puoliautomaattisesti nostaa

sovellukseen liittyviä riskejä, jos määräyksen vaatimukset eivät täydy. Listaus on pitkä ja jatketaan vielä huomenna.

Loput työpäivästä meni intraoraaliskannereiden pohjan muokkaamisessa ja täyttämisessä. Pohjassa on kategorisoituna esimerkiksi käyttäjähallinta, datavirrat, tekniset tiedot ja muut asiat liittyen tietoturvaan ja skannereiden tekniseen toteutukseen. Tämä on ensimmäinen kertaa, kun osallistun mihinkään laitteen kilpailutukseen ja mieleen nousi muutamaa kehityskohdetta. Esittelyt olivat suurin osin hyvin vapaamuotoisia, jollain toimittajalla oli enemmän strukturoitu esittely valmiina, kun taas toisella oli dialogiperustuva lähestymistapaa.

Itsellä olisi kannattanut olla melko strukturoitu pohja valmiina, jonka perusteella olisi kysytty olennaiset kysymykset tietoturvaan liittyen. Valmiina olevat strukturoidut kysymykset tai tietopyynnöt olisivat myös olleet hyödyllisiä lähettää palveluntarjoajalle esittelyjen jälkeen; nyt pyysimme teknistä dokumentaatioita, viittaamatta sen tarkempaan mihinkään. Meillä ei ollut myöskään yhteistä yhteenvetopohjaa, minkä takia loin pohjan itse. Tämä pohja ei kuitenkaan perustuu mihinkään standardiin tai kriteeristöön, mutta tulevaisuutta varten voisimme kehittää ainakin tietoturvan puolesta omaa pohjaa laitteiden tai sovellusten kilpailutusta varten.

Keskiviikko 9.4

Tänään pidin sovitusti lyhyempi työpäivä henkilökohtaisen tapaamisen vuoksi. Ehdin kuitenkin sovelluspalvelujen tehtävien lisäksi osallistua tietoturvapoikkeamahallinnan projektin palaveriin. Palaverissa ei kuitenkaan käsitellyt muita asioita kuin tietoturvapoikkeamahallinnan dokumentin hiominen, joka lähti johdolle hyväksyttäväksi.

Torstai 10.4

Viikkopalaverin ja sovelluspalvelujen tehtävien lisäksi en ehtinyt osallistumaan muuhun kuin viime viikon torstaina alkaneen TSVA:n jatkopalaveriin. Palaverissa pyrittiin keskittymään tekniseen toteutukseen ja tietoturvaan liittyviin asioihin. Palvelutarjoajan mukaan kaikki on kunnossa, eivätkä pysty lähettämään mitään dokumentaatiota liittyen laitteisiin, koska kaikki tiedot ovat salassa pidettäviä. Näissä tapauksissa kannattaa kuitenkin merkitä ylös riskin, että emme voi takaa tietoturvallista toteutusta, jos dokumentaatiota toteutuksesta ei saada. Riskin omistajan on päätettävä, onko palveluntarjoaja tarpeeksi luotettava ja joko hyväksyä riski tai ei. Kävimme myös loput kohteet TSVA:sta läpi ja saimme arvio valmiiksi kuitattavaksi riskin omistajille.

Perjantai 11.4

Perjantain kunniaksi pidimme pitkästä aikaa palaverin liittyen hallintakeinoon 8.1 Käyttäjien päätelaitteet. Tällä hetkellä organisaatiossa ei ole selkeä päätelaitteiden kriittisyysluokittelua, mikä vaikeuttaa huomattavasti priorisointia häiriötilanteissa. Teoreettisesti katsoen, jos

suuri määrä päätelaitteita lakkaa toimimasta samaan aikaan, kaikki ovat tällä hetkellä yhtä kriittiset ja tulisi saada toimimaan mahdollisin nopeasti. Käytännössä tämä ei ole mahdollista, jollei ole aina valmiina valtavan määrä resursseja ja henkilöstöä mahdollista laajaa häiriötilannetta varten. Päätelaitteiden kriittisyysluokittelulla voimme helpommin priorisoida tärkeimpien päätelaitteiden korjaus ja jättää vähemmän kriittiset laitteet myöhemmäksi korjattavaksi.

Kriittisyysluokittelu ei tarvitse olla kovin monimutkainen tai syventävä, eikä tarvitse luokitella tiettyjen ammattiryhmien käyttämiä päätelaitteita erikseen. Lähestymistapamme on luoda kriittisyysluokat, johon kohdataan esimerkiksi oheispäätelaitteet tai tiettyjen ammattiryhmien käyttämät päätelaitteet. Käytämme perustasoinen 5x5 riskimatriisin pohjana, jossa erotellaan riskit vakavuuden ja todennäköisyyden perusteella, mutta vähennetään ruutujen määrä yhdeksään, eli 3x3. Näin ollen häiriötilanteissa priorisoitavat päätelaitteet ovat niitä, joiden toimimattomuus todennäköisemmin aiheuttavat merkittäviä vahinkoja ja jotka ovat esimerkiksi todennäköisimmät kohteet kyberhyökkäyksessä. Toisesta päädystä löytyy päätelaitteet, jonka toimimattomuus ei aiheuta huomioitavaa vahinkoa, eikä vaikuta lähes ollenkaan palvelujen saatavuuteen.

Luokittelussa käytämme yhdistelmää kirjaimista A–C sekä numeroista 1–3. Kirjaimet kuvaavat riskin vakavuutta: A-luokka tarkoittaa kriittistä, B-luokka kohtalaista ja C-luokka vähämerkityksellistä riskiä. Numerot puolestaan kuvaavat riskin todennäköisyyttä: 1-luokka tarkoittaa lähes varmaa ja tapahtuu vuosittain, 2-luokka tapahtuu todennäköistä muutaman vuoden sisällä ja 3-luokka on erittäin epätodennäköistä tapausta. Jotta saisimme alustavan käsityksen siitä, minkälaiset laitteet kuuluisivat mihinkin luokkaan, listasimme mahdollisimman monta eri laitetta ja ryhmittelimme ne kriittisyyden mukaan. Näille ryhmille määritimme alustavat arvot seuraaville jatkuvuudenhallinnan tunnusluvuille:

- Recovery Point Objective (RPO): varmuuskopioinnin tiheys
- Recovery Time Objective (RTO): palvelun tai laitteen palautumisaika
- Maximum Tolerable Period of Disruption (MTPD): johdon määrittämä maksimaalinen aika, jonka häiriö voi kestää ennen kuin se on kriittinen

Nämä käsitteet ja muut jatkuvuudenhallintaan liittyvät asiat on määritelty standardissa ISO/IEC 27031:2011, josta on odotettavissa uusi versio vuoden 2025 aikana. Taulukosta 3 löytyy esimerkki luokittelumatriisista, jossa tärkeimmät päätelaiteluokat on merkitty punaisella, toiseksi tärkeimmät keltaisella ja vähiten kriittiset vihreällä. Esimerkissä C1 on merkitty keltaisella, koska häiriön tai riskin todennäköisyys on arvioitu hyvin korkeaksi. Vastaavasti B3 on merkitty vihreällä, koska todennäköisyys on arvioitu hyvin matalaksi. Ennakoivat toimenpiteet, kuten perusteellisempi testaus, kohdistetaan ensisijaisesti kriittisimpiin luokkiin.

	Vakavuus (A-C)		
Todennäköisyys (1–3)	A1	B1	C1
	A2	B2	C2
	A3	B3	C3

Taulukko 3 Kriittisyysluokittelu-matriisi 3x3

Iltapäivällä pidimme palaverin tietojärjestelmän lokien viemisestä Splunkiin. Toimialan tämän hetken tavoite on pystyä tehokkaammin havainnoida järjestelmän väärinkäyttöä, esimerkiksi potilastietojen urkkimista. Lokit voitaisiin viedä Splunkiin päivittäin ja pystyisimme oikealla sääntöjen konfiguraatiolla nähdä hälytykset epäilystä väärinkäytöstä ja puuttua niihin ajoissa. Tällä hetkellä saamme lokit vain pyydättäessä, eikä niiden analysointi ole mitenkään automatisoitu. Loimme palveluntarjoajalle toiminallinen muutospyyntö, joka lähti ICT-palvelupäällikölle hyväksyttäväksi.

Viikkoanalyysi

Pitkän tauon jälkeen olen osallistunut taas muutamaan TSVA-palaveriin ja jälleen todennut, että varatut resurssit käytetään suhteellisen epätehokkaasti. Vaihtoehto olisi, että dokumentaatio tulevasta sovelluksesta tai laitteesta pystyttäisiin jakaa ajoissa osallistujille, jotta kaikilla olisi mahdollisuus perehtyä sovelluksen toimivuuteen ja toteutukseen. Toisaalta on vaikea perehtyä dokumentaatioon, jos palveluntarjoaja ei suostu antaa mitään dokumentaatiota, mikä sinänsä voidaan katsoa ongelmalliseksi, koska riskienomistajan tulisi luottaa sokeasti palveluntarjoajaan. On ymmärrettävää, että palveluntarjoaja ei voi lähettää salassa pidettäviä dokumentteja, mutta edes jonkinlainen yleinen kaavio siitä, miten tiedot liikkuvat ja esimerkiksi millä protokollalla tai salaustekniikalla tiedot ovat salattu, olisi hyvin tervetullut.

Splunkin tärkeys SIEM-ratkaisuna on tullut yhä selvemmäksi ja olen pohdiskellut, miksi siihen ei ole satsattu enemmän. Suurimpana syynä voisin kuvitella, on rahaa ja resurssien käyttöä. Organisaatio ei ole voittoa-tavoitteleva yritys, eikä organisaatiolla ole esimerkiksi tuotteisiin liittyviä yrityssalaisuuksia. Tärkeimmät tiedot, jotka käsitellään organisaatiossa, on todennäköisesti asiakas- tai potilastietoja, josta ei saa suoraan rahallista hyötyä muualla tavalla kuin esimerkiksi kiristämisellä.

Asiakas- tai potilastietojen leviämisellä voi kuitenkin olla vakavia seurauksia yhteiskunnalle, kuten nähtiin psykoterapiakeskus Vastaamon tietovuodossa, jonka seurauksena osa uhreista teki itsemurhan (STT 2024). Vaikka tietoturvan tehostaminen ei tuo organisaatiolle suoraa

rahallista hyötyä, olisi tärkeää mielestäni, ja todennäköisesti monen muunkin mielestä, että asiakas- ja potilastietojen suojaamiseen osoitetaan riittävästi resursseja.

Viikko päättyi kuitenkin positiivisessa mielessä, kun saimme vihdoin ainakin osittain edistetty ISO 27001-standardiin liittyvä hallintakeinoa 8.15 Lokikirjaukset ja viety eteenpäin kehitysehdotus potilastietojen lokien seurannasta.

3.8 Viikko 8

Viimeinen seurantaviikko on edessä, ja tavoitteena on viimeistellä aiemmin mainittu visuaalinen kartta SOTE-toimialaan kohdistuvista vaatimuksista, määräyksistä ja tukidokumenteista, kuten kriteeristöistä ja standardeista. Toinen tavoite, jota emme välttämättä ehdi saavuttaa tämän viikon aikana, on tuoda asiakastietojen kyselyjärjestelmän käyttötilastot Splunkiin ja konfiguroida alustavat hälytyssäännöt, jotta voisimme havaita väärinkäytöksiä entistä tehokkaammin. Seuraan myös mielenkiinnolla, miten tietojärjestelmän lokituksen hallinta etenee, vaikka en usko, että sen osalta tapahtuu merkittäviä edistyksiä tällä viikolla.

Maanantai 14.4

Huomenna olisi taas TSVA-palaveri tarjolla, liittyen eri sovellukseen kuin viime viikon TSVA:t. Tämän TSVA:n varten olemme saaneet teknistä dokumentaatiota sovelluksesta palveluntarjoajalta, joten käytin tänään aikaa dokumentaatioon perehtymiseen. Dokumentaatio on ymmärrettävästi salassa pidettävä, varsinkin kilpailijoilta, ja toteutus on kuvattu melko yleisellä tasolla. Tämä on kuitenkin riittävä meille, kun dokumentaatiosta tulee selville, että palveluntarjoaja käyttää moderni salaustekniikkaa, datavirrat ja tietojen säilyttämisestä on tarpeeksi tietoa, ja tietokannat sijaitsevat EU/ETA-alueella. Dokumentaatiosta nousi kuitenkin yksi tekninen huoli esille liittyen SMS-viestintään, joka nostan huomisen TSVA-palaverissa esille. Loput työpäivästä meni sovelluspalvelujen tehtävien nimessä.

Tiistai 15.4

Huomasin tänään, että NIS2-direktiiviin liittyvä lainsäädäntö on vihdoin hyväksytty Suomen eduskunnassa. Viikko sitten, kyberturvallisuuslaki (124/2025) tuli voimaan, joka asettaa tiukemmat vaatimukset organisaatioihin liittyen kyberuhkien riskienhallintaan, valvontaan ja tietoturvapoikkeamien raportointiin. Lain myötä on myös selkeytetty, mitkä kansalliset organisaatiot ja toimijat ovat NIS2-direktiivin riskienhallinta- ja raportointivelvoitteiden alla.

Terveydenhuollon tarjoajia valvova viranomainen Valvira (2025b) on listannut kyberturvallisuuslakiin liittyvät konkreettiset toimenpiteet ja niiden määräpäivät. Kyberturvallisuuslaki koskee jokaista hyvinvointialuetta ja terveydenhuollon organisaatiota, joka työllistää yli 50 henkilöä tai jonka liikevaihto on yli 50 miljoonaa euroa vuodessa. Näillä toimijoilla on velvollisuus ilmoittautua Valviran toimijaluetteloon 8.5. mennessä, eli kuukauden kuluessa lain

voimaantulopäivästä. Vaikka soveltamisala tässä kontekstissa on SOTE-palvelut, kattaa kyberturvallisuuslaki ja sen velvoitteet koko organisaation toiminnan, ei pelkästään SOTE-toimialaa. Jokaisella toimijalla on oltava 8.7. mennessä laadittu toimintamalli, joka sisältää kyberturvallisuuteen liittyvän riskienhallinnan.

Velvoitteiden valvomisessa Valviralla (2025b) on myös oikeus suorittaa ennakollista valvontaa, kuten fyysisiä tarkastuskäyntejä tai asiakirjapohjaista tarkastamista, tai velvoittaa toimija teettämään turvallisuusauditointia. Kyberturvallisuuslain velvoitteista laiminlyönti voi johtaa varoitukseen, velvoittavaan määräykseen tai seuraamusmaksuehdotukseen, josta päättää Traficomin yhteyteen perustettava seuraamusmaksulautakunta. Seuraamusmaksu keskeiselle toimijalle on enimmäkseen 10 000 000 euroa tai 2 prosenttia kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi, eli merkittävä summa joka tapauksessa (Traficom – Kyberturvallisuuskeskus 2025a).

Iltapäivä oli suunnitellusti varattu TSVA-palaverille, joka sujui hyvin, koska paikalla olivat kaikki tarvittavat osapuolet ja olimme ehtineet perehtyä sovelluksen toimintaan ja tekniseen toteutukseen etukäteen. Palaverissa nostimme esiin arvioitavia riskejä sekä laadimme konkreettisia lisätietopyyntöjä palveluntarjoajalle. Palveluntarjoajan edustaja pystyi vastaamaan osaan kysymyksistä heti, ja loput hän selvittää seuraavaan kertaan mennessä, muun muassa minun nostama SMS-viestintään liittyvä riski. Palaveri oli mielestäni onnistunut, mikä oli pitkälti kaikkien osallistujien hyvän valmistautumisen ansiota. Vielä on paljon arvioitavaa, mutta suunta on erittäin hyvä.

Viime viikon TSVA-palaverissa olisin kaivannut samanlaista toimintatapaa, ja lisäksi selkeämpää johtajaa, joka olisi pystynyt ohjaamaan keskustelua tarvittaessa tai ainakin tiennyt, kehen ottaa yhteyttä eri asioissa. Henkilökohtaisesti koen, että kaikki TSVA:t voitaisiin luokitella projekteiksi, ja näin ollen niillä tulisi olla selkeä projektipäällikkö, joka johtaa kokonaisuutta eteenpäin ja delegoi tehtävät selkeästi.

Keskiviikko 16.4

Aamu alkoi poikkeavan suuren määrän häiriötiketeillä, jotka liittyivät samanlaiseen problematiikkaan kuin 6.3 tapahtunutta häiriötä. Selvitimme asiaa palveluntarjoajan kanssa samalla kuin ratkaisimme häiriötikettien kirjautumisongelmat. Syy kirjautumisongelmiin oli automatisoitu eräajo, joka oli passivoitu 6.3 häiriötilanteen jälkeen, mutta otettu taas tänä aamuna käyttöön. Automatiikka toimii nyt niin kuin pitääkin ja käyttöoikeuksien passivoiminen johtui aiemmin asetetuista eräpäivistä, eikä vaatinut toimenpiteitä meiltä tai palveluntarjoajan puolelta. Suurin osa aamupäivästä meni kuitenkin tämän tilanteen seurantaan, jonka jälkeen osallistuin myös kahden tunnin yksikkökokoukseen.

Ehdin iltapäivällä perehtyä vanhaan valmistettuun TSVA-dokumenttiin, jonka arvioitu sovellus hyödyntää julkipilvipalvelua ja TSVA:han oli hyödynnetty MCSB:n viitekehys. Viitekehys oli omasta mielestä hyödynnetty varsin tehokkaasti. Hallintakeinot oli käyty läpi ja täytetty saadun teknisen dokumentaation perusteella. Tämän perusteella oli pystytty nostaa hyvin konkreettiset kysymykset järjestelmätoimittajalle, joka oli vastannut kirjallisesti melko kattavasti jokaiseen esitettyyn kysymykseen. Viitekehys tulee todennäköisesti olemaan käytännöllinen työkalu tulevaisuudessa, varsinkin kun ainakin henkilökohtaisesti tuntuu siltä, että yhä enemmän sovelluksia siirtyy johonkuhun suureen julkipilvipalveluun, kuten Microsoftin Azure, Google Cloud Platform tai Amazon Web Services.

Torstai 17.4

Sovelluspalvelujen viikkopalaverin ja tehtävien jälkeen pidimme palaverin tietojärjestelmien vastuuhenkilöroolien dokumentaation hiomista varten. Vastuuroolit ovat jo alustavasti mukana SOTEn tietoturvasuunnitelmassa, mutta suunnitelma on päivitettävä säännöllisin väliajoin. Tietoturvasuunnitelma on THL:n määräyksen 3/2024 velvoitteisiin perustuva dokumentti, jota on käsitelty tässä opinnäytetyössä luvussa 4.2, alaotsikon ”Perjantai 7.3” alla.

Uudet roolit ovat pitkälti valmiina, mutta dokumentaatio vaatii tarkkaa läpikäyntiä, jotta teksti olisi riittävän selkeä eikä roolien välillä esiintyisi ristiriitaisuuksia. Vastuuhenkilörooleja on yhteensä seitsemän, verrattuna voimassa olevan tietoturvasuunnitelman neljään rooliin. Ne liittyvät pääkäyttäjyyteen, sopimushallintaan sekä toiminnan ja toimittajan vastuisiin. Yksi rooli voi kuitenkin jakautua useammalle vastuuhenkilölle, tai yhdellä henkilöllä voi olla useita rooleja, riippuen tietojärjestelmän laajuudesta.

Tietojärjestelmien vastuuhenkilöroolien määrittämisen myötä voimme luoda tietojärjestelmäkohtaisesti selkeämmät ohjeet esimerkiksi käyttäjähallintaan, riskien hallintaan, haavoittuvuuden seurantaan ja tietoturvapoikkeamien hallintaan. Seuraava askel olisi päivittää tietoturvasuunnitelman osa omaisuuserien tunnistamisesta ja määrittämisestä, eli tietoturvan näkökulmasta selkeämmin listata mitä halutaan turvata tietojärjestelmiin liittyen, esimerkiksi palvelimet tai potilastiedot.

Perjantai 18.4

Opinnäytetyön seurantajakson viimeinen perjantai on pitkäperjantai, eli pääsiäisen ensimmäinen pyhäpäivä. Vapaapäivän käytin visuaalisen kartan valmistamista varten. Avaan visuaalisen kartan sisältö ja selitteet seuraavassa luvussa.

Viikkoanalyysi

Suomen lainsäädäntö liittyen EU:n NIS2-direktiiviin on viimein hyväksytty eduskunnassa ja sen myötä kyberturvallisuuslaki ja sen velvoitteet ovat astuneet voimaan. Organisaatiomme pitää

laatia organisaatiolaajuinen kyberturvallisuuden riskienhallinta toimintamalli viimeistään 8.7. mennessä. Traficom on tähän liittyen luonut 139-sivuinen suositus valvoville viranomaisille, joka myös toimijat voivat hyödyntää toimintamallin laatimisessa (Traficom 2025).

Tänäkään viikkona en ehtinyt edistää asiakastietojen kyselyjärjestelmän väärinkäytön havainnoinnin automatisaatiota. Tässä tilanteessa huomaa, että tällaiset pikkuprojektit ilman selkeää määräpäivää jäävät helposti tekemättä, varsinkin, kun on jatkuvasti meneillään isompia projekteja, joilla on määräpäivät ja korkeampi prioriteetti. Kehityskohde löytyy selkeästi minusta ja työni suunnittelusta. Selkeä, itseohjautuva suunnitelma, jossa otetaan huomioon kaikki käynnissä olevat tehtävät, auttaisi tällaisia pienempiä projekteja saamaan enemmän huomiota.

4 SOTE-toimialalle kohdistuvat tietoturvavaatimukset ja niiden soveltamista tukevien työkalujen visuaalinen kartoitus

Seurantajakson aikana olen koonnut kaikki huomaamani SOTE-sektorille soveltuvat lait, vaatimukset, määräykset ja velvoitteet, jotka liittyvät tietoturvaan ja osittain myös tietosuojaan. Lisäksi olen koonnut työkalut, kuten kansainväliset standardit, viitekehykset ja muut hallintakeinot, jotka tukevat organisaation pyrkimyksiä parantaa tietoturvatasoaan. Olen laatinut visuaalisen käsitekartan, jossa olen pyrkinyt esittämään, mitkä näistä vaatimuksista ja työkaluista ovat keskeisimpiä SOTE-sektorin tietoturvan kehittämisessä.

Käsitekartta on jaettu kahteen osaan, valkoisella ja mustalla taustalla. Valkoisella taustalla ovat kaikki kansalliset osatekijät, kun taas mustalla taustalla sijaitsevat ei-kansalliset osatekijät. Kukin laatikko edustaa esimerkiksi yhtä lakia tai kriteeristön osaa riippuen sen taustaväristä. Monista laatikoista lähtee myös nuoli, joka osoittaa toiseen laatikkoon, mikä tarkoittaa, että esimerkiksi tietty laki tai EU-direktiivi on otettu huomioon kriteeristön tai velvoitteiden laatimisessa. Käsitekartan nimi on "SOTE tietoturva- ja tietosuojavaatimukset ja niiden soveltamista tukevat työkalut", ja se löytyy liitteestä 1. Taulukossa 4 on selitetty käsitekartan laatikoiden värit ja niiden sisältö.

Väri	Selite
Tummansininen (valkoisella taustalla)	Visuaalisen kartan otsikko: **SOTE Tietoturva- ja tietosuojavaatimukset ja niiden soveltamista tukevat työkalut**

Vaaleansininen	Suomalaiset lait. Käsitekartassa on merkitty vain tietoturvaa koskevat lait, lisää SOTE-toimialalle soveltuvat lait on listattu liitteessä 2.
Vihreä	Tietoturvaan liittyvät kansalliset kriteeristöt ja mallit. • Kybermittari on Traficomin Kyberturvallisuuskeskuksen kehittämä malli, joka on avoimesti saatavilla ja tukee kyberturvallisuuden arviointia sekä pitkäjänteistä kehittämistä. Malli pohjautuu NIST CSF:ään sekä U.S. Department of Energy Cybersecurity Capability Maturity Model, C2M2. (Traficom – Kyberturvallisuuskeskus 2020a, 4.) • Katakri, kansallinen turvallisuus auditointikriteeristö, on viranomaisten tietoturva-auditointityökalu, jota käytetään arvioimaan organisaation kykyä suojata kansallista tai kansainvälistä salassa pidettävää tietoa. Kriteeristössä on huomioitu seuraavat lait ja EUn päätös: o Laki julkisen hallinnon tiedonhallinnasta "Tiedonhallintalaki" 906/2019 o Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019 o Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 1406/2011 o Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004 o Turvallisuusselvityslaki 726/2014 o EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä 2013/488/EU. (Kansallinen turvallisuusviranomainen 2020, 5–7.) • PiTuKri, Pilvipalveluiden turvallisuuden arviointikriteeristö, on Traficomin laatima kriteeristö, jonka tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa. Kriteeristön laatimisessa on huomioitu: o BSI:n pilviturvallisuuskriteeristö o CSA-pilviturvallisuusyhteisön suojausmatriisi o ISO 27015- ja ISO 27016-standardit

	○ Katakri-kriteeristö (Traficom – Kyberturvallisuuskeskus 2020b, 3.) • Julkri, julkisen hallinnon tietoturvallisuuden arviointikriteeristö, on tiedonhallintalautakunnan suositus julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä. Sitä voidaan hyödyntää tiedonhallintalain, turvallisuusluokitteluasetuksen sekä osin tietosuoja-asetuksen mukaisesti asetettujen tietoturvavaatimusten täyttymisen arvioinnissa. Kriteeristön laatimisessa on huomioitu: ○ Laki julkisen hallinnon tiedonhallinnasta "Tiedonhallintalaki" 906/2019 ○ Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019 ○ Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 1406/2011 ○ Tietosuojalaki 1050/2018 ○ GDPR, EU:n yleinen tietosuoja-asetus EU 2016/679 ○ Katakri ○ PiTuKri. (Valtiovarainministeriö 2023, 7–11.)
Oranssi	THL:n määräykset, jotka perustuvat asiakastietolain 79–88 § (703/2023).
Keltainen	Tahot, joille tehdään ilmoitus merkittävästä poikkeamasta: • NIS2-häiriöilmoitus tehdään kyberturvallisuuslain (124/2025) mukaisesti Suomen CSIRT-yksikölle Traficomille. • PAVAT-ilmoitus tehdään Etelä-Suomen sosiaali- ja terveydenhuollon valmiuskeskuksen Tilannekeskukselle. Lait, jotka ovat sopimuksen taustana: ○ Laki sosiaali- ja terveydenhuollon järjestämisestä 612/2021 ○ Sosiaali- ja terveydenhuollon häiriötilanteisiin 308/2023 ○ Valmiuslaki 1552/2011 ○ Hyvinvointialueista annetun lain 611/2021.

	(Etelä-Suomen yhteistyöalueen yhteistyösopimuksen 2024, 2;21;28.)
Sininen (mustalla taustalla)	EU direktiivit ja asetukset • GDPR-asetus EU 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta. Myös Euroopan unionin yleinen tietosuoja-asetus, jonka tarkoitus on vahvistaa yksilön oikeuksia henkilötietojen suojaan ja yhtenäistää tietosuojakäytännöt koko EU-alueella. • NIS-direktiivi EU 2016/1148, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa. Direktiivi on Euroopan unionin ensimmäinen verkko- ja tietojärjestelmien turvallisuusdirektiivi, jonka tavoitteena oli parantaa jäsenvaltioiden digitaalista häiriönsietokykyä ja vahvistaa kriittisten palveluiden kyberturvallisuutta. • MDR-asetus EU 2017/745 lääkinnällisistä laitteista, joka korvasi aiemman lääkinnällisiä laitteita koskevan direktiivin (MDD) ja toi mukanaan merkittäviä muutoksia lääkinnällisten laitteiden turvallisuuteen, laatuun ja markkinoille pääsyyn liittyen. • NIS2-direktiivi EU 2022/2555, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa. Tämä direktiivi korvasi aiemman NIS1-direktiivin. Sen tavoitteena on parantaa EU:n kyberturvallisuuden tasoa entistä kattavammin ja yhdenmukaisemmin eri jäsenmaissa. • CER-direktiivi EU 2022/2557, kriittisten toimijoiden häiriönsietokyvystä. Yleiseen turvallisuuteen liittyvä direktiivi, joka tähtää kriittisten toimijoiden resilienssin eli toimintakyvyn parantamiseen häiriötilanteissa. Se täydentää kyberturvallisuuteen keskittyvää NIS2-direktiiviä, mutta keskittyy erityisesti fyysisiin riskeihin, kuten luonnonkatastrofeihin, pandemioihin, sabotointiin ja teknisiin vikoihin.
Liila	Kansainväliset standardit, viitekehykset ja muut työkalut. • BSI:n pilviturvallisuuskriteeristö, joka on Saksan Bundesamt für Sicherheit in der Informationstechnik laatima kriteeristö C5 - Cloud Computing Compliance Criteria Catalogue

	• Center of Internet Security Controls, joka on joukko parhaita käytäntöjä ja suosituksia, joiden tarkoituksena on auttaa organisaatioita parantamaan kyberturvallisuuttaan. • CSA-pilviturvallisuusyhteisön suojausmatriisi, eli Cloud Security Alliancen laatima viitekehys Cloud Controls Matrix (CCM) • ISO/IEC 27000-standardiperhe, varsinkin: o 27001 – Tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset o 27002 – Tietoturvallisuuden hallintajärjestelmän hallintakeinojen määrittäminen ja toteuttaminen o 27003 – Ohjeistaa ISMS:n käyttöönottoa o 27005 – Ohjeita tietoturvariskien hallintaan o 27009 – Selittää, miten ISO/IEC 27001- ja 27002-standardeja voidaan mukauttaa eri toimialoille. o 27017 - Tietoturvakontrollit pilvipalveluille o 27035 - Kattaa tietoturvapoikkeamien hallinnan, mukaan lukien suunnittelu, havaitseminen ja reagointi. (Suomen Standardisoimisliitto SFS 2020, 23-29.) • Microsoft Cloud Security Benchmark, MCSB, on Microsoftin kehittämä turvallisuusviitekehys, joka tarjoaa suosituksia ja parhaita käytäntöjä Microsoftin pilvipalveluiden, kuten Azure-ympäristön, suojaamiseen. • NIST Cybersecurity Framework, NISTin kehittämä viitekehys, joka auttaa organisaatioita hallitsemaan ja parantamaan kyberturvallisuuttaan järjestelmällisesti ja riskiperusteisesti. • NIST SP 800-53, NISTin laatima tietoturvakontrollien kokoelma, joka tarjoaa kattavat suositukset liittovaltion tietojärjestelmien ja organisaatioiden suojaamiseen.

Taulukko 4 SOTE Tietoturva- ja tietosuojavaatimukset ja niiden soveltamista tukevat työkalut, visuaalisen käsitekartan (liite 1) selitteet

Käsitekartta voi olla hyödyllinen SOTE-toimialan tietoturva-asiantuntijan työssä tai uuden asiantuntijan perehdytyksessä. Itse sain aikoinaan perehdytyksen yhteydessä tietoa tietoturvatiimistä sekä asiantuntijoiden että päällikön työkuvista, mutta kokonaisuuden hahmottaminen oli haastavaa. Käsitekarttaan kokoamani materiaali koostuu pitkälti dokumenteista ja asioista, joista jokaisen SOTE-toimialan tietoturva-asiantuntijan tulisi vähintään pintatasolla olla tietoinen.

5 Yhteenveto

Seurantajakson aikana olen havainnut muutaman kehityskohteen, joita voimme tietohallinnon yksikössä mahdollisesti kehittää. MIM-prosessin selkeyttäminen ja kehittäminen olisi mielestäni melko korkea prioriteetti, varsinkin vastuuhenkilöiden ja heidän rooliensa selkeyttäminen. Kommunikaatio eri osapuolien välillä on koettu melko huonoksi MIM-häiriön aikana. MIM-prosessin kehittämisessä voisi ainakin tietoturvapoikkeamien hallintaprosessi toimia tukena, sillä siinä määritellään tietoturvahäiriöihin liittyvän MIM-prosessin vaiheet ja eri vastuut.

Toinen selkeä kehityskohde omasta näkökulmastani on TSVA-prosessi, jonka sisältöä ja vastuita olisi syytä selkeyttää muillekin osallistujille kuin tietosuojan asiantuntijoille. Erityisesti tietoturva-asiantuntijan rooli on monin paikoin epäselvä, erityisesti tilanteissa, joissa palveluntarjoaja ei suostu toimittamaan sovelluksesta tai siihen mahdollisesti liittyvästä laitteesta mitään dokumentaatiota. Myös muiden vastuuhenkilöiden, ja erityisesti prosessin johtajan, vastuut ovat epäselvät. Tietosuojan vaikutustenarvioinnin tekemisen peruste on kuitenkin selkeä ja erittäin tärkeä: tarkoituksena on selvittää, mitä henkilötietoja sovelluksessa käsitellään ja miten näiden tietojen suojaaminen toteutetaan.

Organisaation SOTE-toimialan ISMS-toteutushanke edistyy hitaasti mutta varmasti. Päädyin seurantajakson alussa keskittymään ISO 27001-standardin A-liitteen hallintakeinojen kypsyysarviointeihin, mutta kommunikaatio-ongelmat in-house-yhtiön kanssa osoittautuivat suuremmaksi haasteeksi kuin alun perin ajattelin. Opinnäytetyön toteuttaminen päiväkirjamaisena raportointina ja sen tiukka aikataulu ei myöskään näin ollen osoittautunut kaikilta osin tarkoituksenmukaisimmaksi lähestymistavaksi. Tietoturvapäällikön ja tietohallintoyksikön muiden asiantuntijoiden kanssa olemme kuitenkin pystyneet edistämään joidenkin hallintakeinojen toteutusta, kuten 8.1. Käyttäjien päätelaitteet ja 8.15 Lokikirjaukset.

Minulle on seurantajakson aikana ainakin käynyt selväksi, kuinka valtava määrä dokumentaatiota liittyy tietoturvaan ja erityisesti tietosuojaan sosiaali- ja terveydenhuollossa. Jotta ymmärtäisin paremmin, miten eri muuttujat ja osa-alueet liittyvät toisiinsa, loin visuaalisen kartoituksen kokoamalla yhteen keskeisimmät lait, asetukset ja vaatimukset, jotka sosiaali- ja terveydenhuollon toimialan tulee täyttää tietoturvan näkökulmasta, sekä työkalut, jotka tukevat näiden velvoitteiden toteuttamista.

Toimeksiantajalle tämä visuaalinen kartta (liite 1) ja siihen liittyvä tukidokumentaatio voivat toimia pohjana toimialamme tietohallinnon tietoturva-asiantuntijoiden perehdyttämiselle. Vaikka lakien tulkinta ja soveltaminen on pääosin tietosuojan asiantuntijoiden vastuulla, itseäni kiinnostaa nähdä, mistä eri sosiaali- ja terveydenhuollon velvoitteet perustuvat.

Lähteet

Sähköiset

Asetus 2016/679/EU. Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). 27 päivänä huhtikuuta. Viitattu 7.4.2025. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32016R0679&qid=1744040767174

Asetus 2017/745/EU. Euroopan parlamentin ja neuvoston asetus lääkinnällisistä laitteista, direktiivin 2001/83/ey, asetuksen (ey) n:o 178/2002 ja asetuksen (ey) n:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ety ja 93/42/ety kumoamisesta. 5 päivänä huhtikuuta 2017. Viitattu 7.4.2025. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32017R0745

Center for Internet Security 2024. CIS Critical Security Controls, Version 8.1.

Center for Internet Security 2025. About us. Viitattu 2.4.2025. https://www.cisecurity.org/about-us

Croell, K., Hetemaa, T., Knape, N., Leipälä, J., Louet-Lehtoniemi, T., Ridanpää, H., Suomela, T., Syrjänen, T. & Syrjä, V. 2023. Sosiaali- ja terveyden- huollon järjestäminen yhteistyöalueilla. Viitattu 2.4.2025. https://www.julkari.fi/bitstream/handle/10024/147854/PT2023_045_YTA-raportti_30112023%20korjattu_s.pdf?sequence=4&isAllowed=y

Direktiivi 2022/2555/EU. Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi). 14 päivänä joulukuuta 2022. Viitattu 2.4.2025. https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fi

Etelä-Suomen yhteistyöalueen yhteistyösopimus 2024. Viitattu 2.4.2025. https://ahjojulkaisu.hel.fi/68754BE7-7C71-CC9D-9743-92706CD00000.pdf

European Commission 2025. NIS2 Directive: new rules on cybersecurity of network and information systems. Viitattu 2.4.2025. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Hallituksen esitys 57/2024 vp. Viitattu 7.3.2025. https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_57+2024.aspx

Kansallinen turvallisuusviranomainen 2020. Katakri 2020. Viitattu 25.4.2025. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Kidd, C 2023. SOAR: Security Orchestration, Automation & Response. Viitattu 12.4.2025. https://www.splunk.com/en_us/blog/learn/soar-security-orchestration-automation-response.html

Kidd, C. 2024. What Is Splunk & What Does It Do? A Splunk Intro. Viitattu 12.4.2025. https://www.splunk.com/en_us/blog/learn/what-splunk-does.html

Kidd, C. 2025. SIEM: Security Information & Event Management Explained. Viitattu 12.4.2025. https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html

Kyberturvallisuuslaki 124/2025. Viitattu 23.4.2025. https://finlex.fi/fi/lainsaadanto/saadoskokoelma/2025/124

Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023. Viitattu 2.4.2025. https://www.finlex.fi/fi/lainsaadanto/saadoskokoelma/2023/703

Liikenne- ja viestintäministeriö 2017. Verkko- ja tietoturvadirektiivi Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti. Viitattu 2.4.2025. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79770/LVM_09_2017_Verkko_%20ja_tietoturvadirektiivi.pdf?sequence=1&isAllowed=y

Sosiaali- ja terveysministeriö 2025. Sosiaali- ja terveyspalveluja koskeva lainsäädäntö. Viitattu 26.4. https://stm.fi/sotepalvelut/lainsaadanto

STT 2024. Vastaamo-uhrien juristi: Ihmisiä on päätynyt itsemurhaan tietomurron ja kiristyksen takia. Helsingin Sanomat. Viitattu 15.4.2025. https://www.hs.fi/suomi/art-2000010265660.html

Suomen Standardisoimisliitto SFS 2020. SFS-EN ISO/IEC 27000:2020 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto.

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

Suomen Standardisoimisliitto SFS 2023b. SFS-EN ISO/IEC 27002:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot.

Terveyden ja hyvinvoinnin laitos 2024a. Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista. Viitattu 2.4.2025. https://thl.fi/documents/155392151/190361269/THL_Maarays_3_2024_Tietoturvasuunnitelmaan_sisallytettavista_sevityksista_ja_vaatimuksista.pdf/9123733d-c1ae-09f5-e05d-a33894441c6c/THL_Maarays_3_2024_Tietoturvasuunnitelmaan_sisallytettavista_sevityksista_ja_vaatimuksista.pdf?t=1708438054468

Terveyden ja hyvinvoinnin laitos 2024b. Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista. Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista. Viitattu 2.4.2025. https://thl.fi/documents/155392151/190361269/THL-Maarays4-2024_Sosiaali-ja_terveydenhuollon_tietojarjestelmien_ja_hyvinvointisovellusten_luokittelusta_ja_sertifioinnista.pdf/c2c4ce1b-540e-0f0d-490e-468ca5975165/THL-Maarays4-2024_Sosiaali-ja_terveydenhuollon_tietojarjestelmien_ja_hyvinvointisovellusten_luokittelusta_ja_sertifioinnista.pdf?t=1714978021090

The NIST Cybersecurity Framework (CSF) 2.0 2024. Viitattu 2.4.2025. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Traficom – Kyberturvallisuuskeskus 2020a. Kybermittari - Kansallinen kyberturvallisuuden arviointimalli – Käyttöohje. Viitattu 25.4.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_Käyttöohje_V1.pdf

Traficom – Kyberturvallisuuskeskus 2020b. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Viitattu 25.4.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Traficom 2025. Liikenne- ja viestintävirasto Traficomin suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä. Viitattu 23.4.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Suositus%20NIS-valvoville%20viranomaisille%20kyberturvallisuuden%20riskienhallinnan%20toimenpiteistä.pdf

Traficom – Kyberturvallisuuskeskus 2024. RFC 2350. Viitattu 2.4.2025. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/cert/rfc-2350

Traficom – Kyberturvallisuuskeskus 2025a. Tärkeää tietoa Euroopan unionin kyberturvallisuusdirektiivistä (NIS2). Viitattu 2.4.2025. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi/tarkeaa-tietoa

Traficom – Kyberturvallisuuskeskus 2025b. Ilmoita tietoturvapoikkeamasta (NIS-ilmoitusvelvollisuus). Viitattu 2.4.2025. https://www.kyberturvallisuuskeskus.fi/fi/asioi-kanssamme/ilmoita-tietoturvapoikkeamasta-nis-ilmoitusvelvollisuus

Valvira 2025a. Asiakastietolain ja toisiolain mukainen rekisteri Astori. Viitattu 7.4.2025. https://valvira.fi/sosiaali-ja-terveydenhuolto/astori-rekisteri

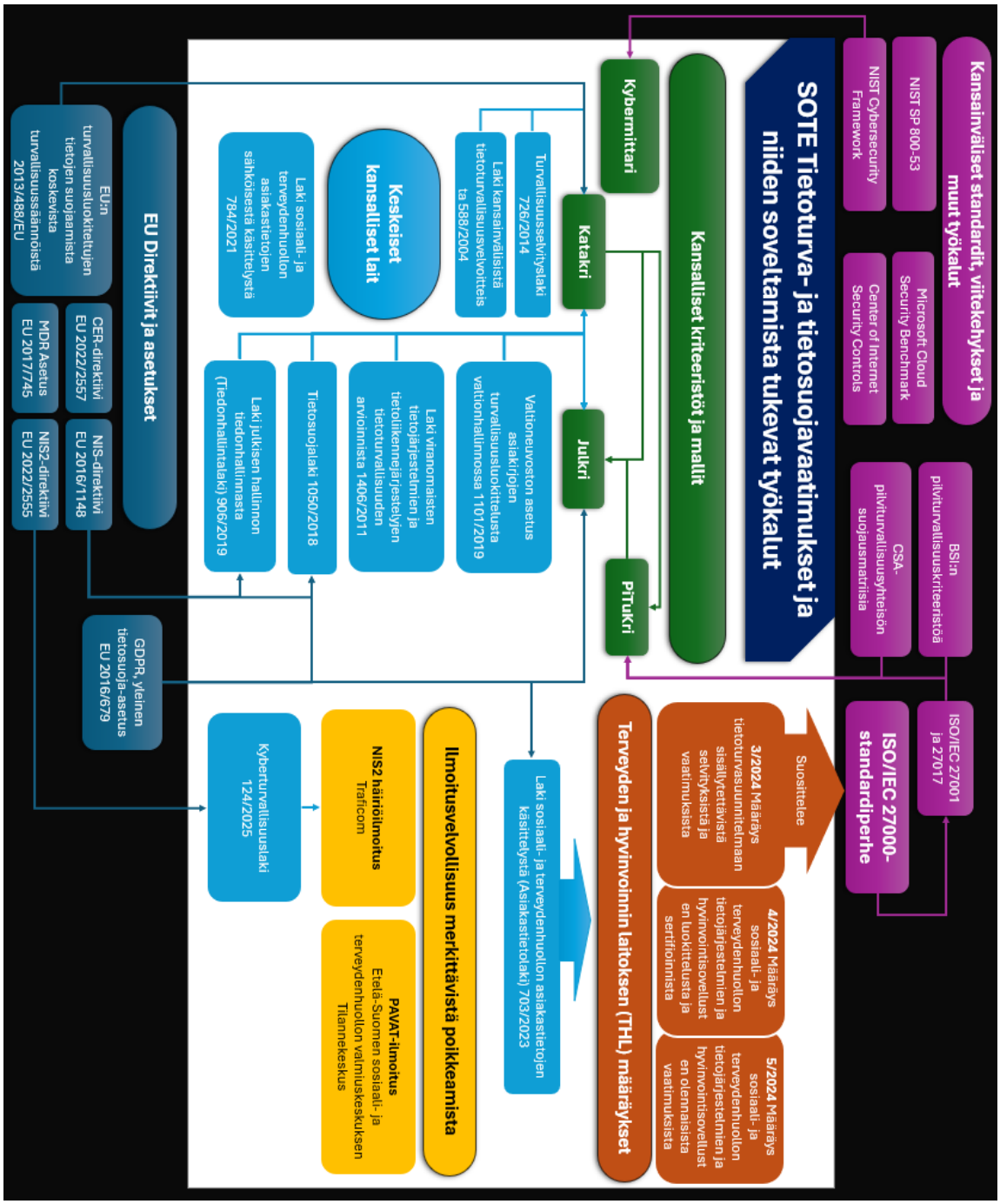
Valvira 2025b. Kyberturvallisuuslaki (NIS2). Viitattu 23.4.2025. https://valvira.fi/sosiaali-ja-terveydenhuolto/kyberturvallisuuslaki

Tämän tekstin kieliasun muokkaamisessa on hyödynnetty ChatGPT 4o:ta.

Taulukot

Liitteet

Liite 1: SOTE Tietoturva- ja tietosuojavaatimukset ja niiden soveltamista tukevat työkalut, käsitekartta



Liite 2: SOTE-toimialan koskevat lait

Tietosuojalaki (1050/2018)
Laki viranomaisten toiminnan julkisuudesta (621/1999)
Laki julkisen hallinnon tiedonhallinnasta (906/2019)
Laki sähköisen viestinnän palveluista (917/2014)
Rikoslaki (39/1889) 38 § Tieto- ja viestintärikoksista
Arkistolaki (831/1994)
Työsopimuslaki (55/2001)
Vahingonkorvauslaki (41/1974)
Laki yksityisyyden suojasta työelämässä (759/2004)
Laki kunnan ja hyvinvointialueen viranhaltijasta (2003/304)
Laki hyvinvointialueesta (611/2021)
Laki sosiaali- ja terveydenhuollon järjestämisestä (612/2021)
Laki pelastustoimen järjestämisestä (613/2021)
Laki sosiaali- ja terveydenhuollon sekä pelastustoimen järjestämisestä Uudellamaalla (615/2021)
Terveydenhuoltolaki (1326/2010)
Laki terveydenhuollon ammattihenkilöistä (559/1994)
Laki sosiaalihuollon ammattihenkilöistä (817/2015)
Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (94/2022)
Sosiaali- ja terveysministeriön asetus käyttöoikeudesta asiakastietoon (825/2022)
Laki sosiaalihuollon asiakasasiakirjoista (254/2015)
Laki sähköisestä lääkemääräyksestä (61/2007)
Laki potilaan asemasta ja oikeuksista (785/1992)
Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021)
Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019)
Laki eräistä EU-direktiiveissä säädetyistä lääkinnällisistä laitteista (629/2010)
Laki lääkinnällisistä laitteista (719/2021)
Oppilas- ja opiskelijahuoltolaki (1287/2013)
Laki kuntouttavasta työtoiminnasta (189/2001)
Suomen perustuslaki (731/1999)
Sosiaalihuoltolaki (1301/2014)
Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
Lastensuojelulaki (417/2007)
Laki kehitysvammaisten erityishuollosta (519/1977)
Vammaispalvelulaki (673/2023)
Laki omaishoidon tuesta (937/2005)
Perhehoitolaki (263/2015)
Laki ikääntyneen väestön toimintakyvyn tukemisesta sekä iäkkäiden sosiaali- ja terveyspalveluista (980/2012)
Laki toimeentulotuesta (1412/1997)
Vanhemmuuslaki (775/2022)
Laki lapsen elatuksesta (704/1975)
Laki lapsen huollosta ja tapaamisoikeudesta (361/1983)
Adoptiolaki (22/2012)
Avioliittolaki (234/1929)
Työterveyshuoltolaki (1383/2001)
Laki hedelmöityshoidoista (1237/2006)
Tartuntatautilaki (1227/2016)
Laki rajat ylittävästä terveydenhuollosta (1201/2013)
Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023)
(Sosiaali- ja terveysministeriö 2025.)