Tietoturvan hallinnointi sekä jatkuva kehitys yksityisellä terveydenhuollon alalla

Sara Väisänen

2024 Laurea

Laurea-ammattikorkeakoulu

Tietoturvan hallinnointi sekä jatkuva kehitys yksityisellä terveydenhuollon alalla

Sara Väisänen

Tietojenkäsittely

Opinnäytetyö

Joulukuu, 2024

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tietojenkäsittelyn koulutusohjelma, kyberturvallisuus

Tradenomi (AMK)

Sara Väisänen

Tietoturvan hallinnointi sekä jatkuva kehitys yksityisellä terveydenhuollon alalla

Vuosi 2024 Sivumäärä 41

Tässä päiväkirjamuotoisessa opinnäytetyössä seurattiin kahdeksan viikon ajan hallinnollisen tietoturvan työtehtäviä suomalaisessa yksityisen terveydenhuollon yrityksessä. Opinnäytetyössä kuvattiin päivittäistä työskentelyä sekä pohdittiin tietoturvatietoisuuteen vaikuttavia näkökulmia. Työn tavoitteena oli havainnoida ison tietoturvakoulutusprojektin uudistamistyöhön liittyviä seikkoja sekä seurata tietoturvan hallintajärjestelmän kehitystyötä. Kahdeksan viikon seurantajakso sijoittui aikavälille 16.9.2024-10.11.2024.

Päivittäistä työskentelyä kuvattiin päiväkirjamuotoisesti sekä analysoitiin mietteitä työstä, joita tuettiin lähdemateriaalein. Tietoperustana tässä työssä käytettiin alan kirjallisuutta, tutkimusartikkeleita, lainsäädäntöä sekä alan lehtien julkaisuja. Työssä käytettiin toimintatutkimuksen menetelmiä.

Kaikkia työn tavoitteita ei saavutettu, mutta tärkeimpinä tuloksina olivat riskienhallinnan sitominen päivittäiseen työhön etenkin isoa projektia aloittaessa sekä asiantuntijataitojen kehittyminen. Lopputuotoksena oli havainnot tietoturvakoulutuksen sisällöstä ja kuinka sisällön hiominen voi edesauttaa tietoturvataitoja myös työsuhteen ulkopuolella.

Asiasanat: Tietoturva, projektinhallinta, jatkuva kehitys

Laurea University of Applied Sciences **Abstract**

Degree Programme in Business Information Technology, Cyber Security

Bachelor's degree

Sara Väisänen

Information security management and continuous improvement in private healthcare

Year 2024 Pages 41

This thesis follows the work of an administrative information security specialist in a Finnish private healthcare company for eight weeks. The diary-based thesis describes everyday work in detail and consideration was given to aspects that affect information security awareness. The purpose of this thesis was to observe what aspects affect the development of an information security education project and to follow the development of an information security management system. This thesis was written over an eight-week period from 16.9.2024 to 10.11.2024.

Everyday work was described on a day-to-day basis and thoughts were analyzed weekly and these were supported by sources. The knowledge base in this thesis report was derived from information security literature, research articles and relevant legislation. Action research methods were used in this thesis.

All the goals were not met, but the most important findings related to risk management practices and how to connect these in everyday work especially when working on a big project and the development of professional expertise. The final output was observations about the content of information security training and how perfecting the content can advance skills of information security outside of work.

Keywords: Information security, project management, continuous improvement

Sisällys

1 Johdanto

Tietoturvassa jatkuva kehitys on tärkeässä osassa, jotta koko ajan muuttuvaan uhkakenttään voidaan vastata. Jatkuvaa kehitystä voidaan tehdä hallinnollisin sekä teknisin keinoin ja tässä opinnäytetyössä tarkastellaan tietoturvan kehitystä yksityisessä terveydenhuollossa hallinnollisesta näkökulmasta.

Tietoturvatietoisuus sekä -kouluttaminen on osana hallinnollista tietoturvaa. Opinnäytetyön toimeksiantaja on havainnut tietoturvan sekä tietosuojan koulutusohjelman uudistamisen olevan ajankohtaista, sillä nykyinen koulutusmalli on kerran työsuhteen alussa suoritettava eikä aiheeseen palata johdonmukaisesti työsuhteen aikana. Tämän päiväkirjamuotoisen opinnäytetyön tavoitteena on havainnoida ison tietoturvakoulutusprojektin uudistamistyöhön liittyviä seikkoja sekä kuvata tietoturvan hallintajärjestelmän kehitystä kohti ISO27001 sertifiointia, jotta raportointijakson lopussa hallintajärjestelmä olisi riittävän kypsä läpäisemään sertifioinnin ensimmäisen vaiheen.

Opinnäytetyö toteutetaan päiväkirjamuotoisena syksyllä 2024. Raportointijakson aikana kuvaan työtehtäviäni päiväkohtaisesti sekä tuotan viikoittaiset analyysit, jossa syvennytään aiheeseen. Kahdeksan viikon raportointijakso on aikavälillä 16.9.2024-10.11.2024.

Toimeksiantaja odottaa saavansa tämän kehittämistyön tuloksena terveydenhuollon ammattilaisten tietoturvatietoisuuden tason nostoa. Henkilökohtaisena tavoitteenani on oman ammatillisen kehittymisen seuranta, kuinka asiantuntijuuteen kasvu on edistynyt työn aikana.

Opinnäytetyön teon aikana tuli ilmi, että tietoturvan sekä tietosuojan koulutusohjelman tekoa joudutaan viivästyttämään, mutta tietoturvan hallintajärjestelmän kehitystyö jatkui aktiivisena koko opinnäytetyön teon ajan.

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantaja on suomalainen yksityisen terveydenhuollonalan yritys, joka työllistää 33 000 henkilöä Suomessa, Virossa, Ruotsissa sekä Saksassa. Yrityksen digitaaliset palvelut pitää sisällään sovelluskehityksen sekä IT:n. IT:n alaisuuteen kuuluu useita eri tiimejä, jotka vastaavat jatkuvista palveluista muun muassa tietoturvasta, digitaalisesta arkkitehtuurista sekä loppukäyttäjäpalveluista.

1.2 Keskeiset käsitteet

Confluence – Atlassian yhtiön kehittämä yhteisöllisen sisällöntuotannon väline. Käytännössä yrityksen sisäinen työtila, jossa dokumentoidaan yrityksen sisäisiä projekteja, käytäntöjä sekä hallinnoidaan tiimien omia dokumentteja.

Jira – Atlassianin kehittämä projektinhallintatyökalu.

Workday – HR-järjestelmä, toimii myös yrityksen verkkokoulutusmateriaalin alustana.

Sprint – Kehitysjakso, joka voi olla viikosta neljään viikkoa pitkä

ISO27001 - Kansainvälinen standardi tietoturvan hallintaan

Tietoturvan hallintajärjestelmä - Kattava lähestymistapa organisaation jatkuvan tietoturvan varmistamiseen

NIS2 – Euroopan Unionin kyberturvallisuusdirektiivi

2 Nykytilanne

2.1 Nykyinen työ ja oma osaaminen

Toimin nykyisessä työssäni Junior Information Security Specialistin roolissa (nuorempi tietoturva-asiantuntija). Työni koostuu hallinnollisen tietoturvan tehtävistä.

Opinnäytetyötä aloittaessa työkokemusta on IT-alalta kertynyt noin vuoden ajan. Olen nykyisessä työssäni tukiroolissa kehittämässä digitaalisille palveluille tietoturvan hallintajärjestelmää, joka tähtää ISO27001 sertifiointiin. Työtehtäviini sisältyy myös ohjeistusten tekoa, myynniltä tulevien tukilomakkeiden käsittelyä, jossa tiedustellaan yrityksen tietoturvakäytännöistä ja hieman fyysisen turvallisuuden asioita, josta minulla on kokemusta edellisestä ammatistani. Työ hallintajärjestelmän parissa pitää sisällään ISO27001 standardin vaatimusten toteuttamista sekä jo olemassa olevan dokumentaation etsimistä. Työssäni teen myös muiden tiimien kanssa yhteistyötä. Työskennellessäni tietoturvan hallintajärjestelmän parissa, olen huomannut, kuinka tärkeää on ymmärtää myös teknisiä ratkaisuja. Itselläni on ymmärrystä ylätasolla, mutta haluaisin syvemmin osata myös teknistä puolta. Oma osaamiseni teknisen tietoturvan alueella on kehityskohteenani ja olenkin työni ohessa oppinut jo monia asioita.

Työssä onnistuakseni, olen tarvinnut tukea sekä ohjausta, jota olen saanut. Uutena minulle on tullut työn asiantuntijarooli. Edellisessä työelämässä työn suorittaminen on ollut mekaanista,

joten asiantuntijuuteen opettelu on ollut hetkittäin haastavaa, mutta minulla on ollut esihenkilön tuki alusta asti ja olen saanut luvan kanssa myös opetella uuden roolin käytäntöjä.

Saamani kokemus riskienhallinnasta, tiedon suojaamisen prosesseista, säädösten ja lakien tuntemuksesta sekä tietoturvakulttuurin kehittämisestä on suurimmilta osin sovellettavissa myös tulevaan tietoturvan sekä tietosuojan koulutusohjelmaan.

2.2 Sidosryhmät

Työssäni sidosryhmiä on sekä sisäisiä että ulkoisia. Tulevan projektini sisäisiin sidosryhmiin kuuluu tietoturvatiimi, tietosuojatiimi, hallinnollinen ylilääkäri, verkkopedagogi sekä suurimpana sidosryhmänä henkilöstö, jolle koulutus tullaan jalkauttamaan. Tietoturvan hallintajärjestelmän laajuutena on yrityksen digitaaliset palvelut, joten tässä kontekstissa tärkeimpänä sidosryhmänä on digitaaliset palvelut kokonaisuudessaan.

Ulkoisiin sidosryhmiin kuuluu kumppaniyritys, jonka kanssa tietoturvan sekä tietosuojan koulutusohjelma rakennetaan.

2.3 Vuorovaikutus

Oman tiimini vuorovaikutus tapahtuu pääsääntöisesti Slack- viestintäsovelluksessa ja viikoittain pidettävässä Teams etäkokouksessa, jossa käydään tiimin jäsenten käynnissä olevat työtehtävät sekä seuraavan sprintin tulevat tehtävät. Koko tiimin yhteisiä tapaamisia on yhdestä-kahteen kertaa vuodessa. Työssäni tietoturvan sekä tietosuojan koulutusohjelman aikana vuorovaikutus tapahtuu pääsääntöisesti Teamsin välityksellä etäkokouksina.

Haasteena omalle vuorovaikutukselleni koen oman luonteen ujouden, jolloin en tuo omia ajatuksiani esille ellen koe tietäväni aiheesta niin paljon kuin itse haluaisin. Huomaan palaverien aikana, etten kysy asioita, jotka eivät ole täysin selviä itselleni, vaan koitan mieluimmin itsenäisesti asian ensin selvittää ja vasta sitten kysyn. Esihenkilöni kanssa pidämme joka toinen viikko kahvihetken, johon yleensä kasaan kahden viikon ajalta kiireettömiä asioita, jotka ovat jääneet askarruttamaan. Pyrin aktiivisesti pois tästä toimintamallista, mutta koen häiritseväni toisten työntekoa, jos kysyn kiireettömiä asioita Slackissä. Koen myös sähköisen viestimisen ajoittain hankalana, itselleni luontevampaa on hoitaa asioita kasvotusten taikka puhelimitse.

2.4 Kehittäminen

Tämän päiväkirjamuotoisen opinnäytetyön aikana, tulen kehittämään yhteistyössä sidosryhmien kanssa tietoturvan sekä tietosuojan koulutusohjelmaa. Kumppaniksi valitun yrityksen kanssa tehdään pitkäaikaista yhteistyötä. Projektin ollessa laaja, se on jaettu eri vaiheisiin. Ensimmäisessä vaiheessa koulutus tehdään sekä jalkautetaan terveydenhuollon henkilöstölle, toisessa vaiheessa tukipalveluille (laskutus, viestintä, markkinointi) ja kolmannessa vaiheessa

koulutus jalkautetaan digitaalisille palveluille. Näiden vaiheiden jälkeen koulutusohjelman jatkokehitys alkaa, jolloin jokainen vaihe pistetään pienempään kokonaisuuteen, jolloin roolijaottelu alkaa syventyä. Opinnäytetyön aikana keskitytään ensimmäiseen vaiheeseen. Aion tässä työssä käyttää toimintatutkimuksen menetelmiä. Toimintatutkimus on tapa tehdä tutkimusta siten, että siitä on käytännön hyötyä ja sen avulla pyritään aktiivisesti muuttamaan sosiaalisia käytäntöjä (Heikkinen & Kaukko 2023, 7). Toimintatutkimus etenee syklisenä kokonaisuutena, johon kuuluu suunnittelu, toteutus, havainnointi sekä reflektointi. (Heikkinen & Kaukko 2023, 73–74.). Syklinen kokonaisuus toimii tässä projektissa, sillä havainnointivaiheessa keräämme palautetta koulutuksesta koeryhmältä, joka myös tukee toimintatutkimuksen menetelmien käyttöä, koska saamme osallistuttaa henkilöstön edustajia vaikuttamaan heille tarkoitettuun koulutukseen. Saadun palautteen perusteella, voimme palata suunnittelun pariin, josta edelleen toteutukseen kuten syklisessä prosessissa, samalla reflektoiden kuinka käytäntöjä voidaan parantaa.

Tietoturvan sekä tietosuojan koulutusohjelman lisäksi, työhöni kuuluu tietoturvan hallintajärjestelmään liittyvää kehitystyötä tiiviisti kollegani kanssa.

3 Yrityksen tietoturvatietoisuus

Tietoturvaa ei pystytä takaamaan vain teknologian avulla, vaan onnistunut tietoturvakulttuuri nojaa kolmeen asiaan; ihmiset, prosessit ja teknologia. Teknologialla pystyy turvaamaan monia eri asioita, mutta arjen päivittäiset toimet kuten yrityksen laitteista huolehtiminen, salasanoista huolehtiminen sekä yrityksen tietoturvapolitiikkojen ja –ohjeistusten noudattaminen, ei ole niitä asioita joihin teknologisin keinoin pystytään vaikuttamaan. (Herath, Rao 2009, 154–165). Kouluttamisen keinoin, pystytään varmistumaan siitä, että ihmiset tietävät, kuinka heidän tulisi toimia tietoturvaan liittyvien asioiden kanssa ja näin ollen parantaa yrityksen tietoturvatietoisuutta. Tietoturvan sekä tietosuojan koulutusohjelma tulee olemaan rooliperustainen. Rooliperustaisuus tarkoittaa sitä, että jokaisella roolilla on oma koulutuksensa, jonka sisältö on räätälöity juuri siihen työrooliin mitä työntekijä suorittaa (Merrit ym. 2024, 53). Tietoturvasta huolehtiminen nähdään usein vain tietoturvatiimin tai IT työntekijöiden vastuuna, vaikka todellisuudessa tietoturvasta huolehtiminen on kaikkien vastuulla, työtehtävästä riippumatta (Gardner, Thomas 2014, 56). Sitomalla koulutus omaan rooliin, voi tuoda henkilöstölle tunteen, että heidän tekemisellään on väliä, kun mietitään tietoturvallisuutta. Asiat, jotka tuntuvat kaukaisilta, eivät kosketa samalla tavalla kuin sellaiset, jotka ovat tekemisessä läsnä.

Yrityksen tietoturvatietoisuutta ei ole mitattu. Esihenkilömme käy toisinaan esittelemässä yrityksen sisällä tietoturvatiimiä ja meidän tekemistämme, jolla yritetään parantaa tietoturvatietoisuutta. Yrityksessä on käytössä sähköpostin tietoturvakoulutus, joka pelillisin keinoin

opettaa tunnistamaan kalastelusähköposteja sekä työsuhteen alussa suoritettava tietoturvan sekä tietosuojan koulutus. Sähköpostin tietoturvakoulutus ei ole niin aktiivisessa käytössä, kun haluaisimme sen olevan ja tässä on tunnistettu tarve sen markkinoimiselle. Tietoturvan hallintajärjestelmässä yhtenä suorituskykymittarina on tietoisuus sekä osallistuminen tietoturvakoulutuksiin, joten tulevaisuudessa kun saamme hallintajärjestelmän pyörimään osana arkea, pystymme seuraamaan osallistumista koulutuksiin.

4 Päiväkirjaraportointi

4.1 Viikko 1

Tämän viikon tavoitteena, on kerrata jo tehdyt suunnitelmat tietoturvan ja tietosuojan koulutusohjelmasta sekä sopia kuinka jatkamme projektin kanssa.

Maanantai 16.9

Projektin suunnittelu on aloitettu noin puoli vuotta ennen päiväkirjaraportoinnin alkua, joten maanantain tavoitteena oli kerrata jo tehdyt suunnitelmat, sillä tänään oli projektiin liittyvä palaveri. Kyseisen palaverin tarkoituksena oli varmistaa, että olemme kumppaniyrityksen kanssa edelleen yhtä mieltä koulutuksen jaottelusta, koulutuksen kestosta sekä toimitustavasta. Edellinen tapaaminen on ollut projektin suunnittelun alussa keväällä.

Koulutuksen kesto on ollut keskustelunaiheena projektia aloittaessa. Koulutuksen ollessa suunnattu terveydenhuollon ammattilaisille, sen kesto ei voi olla liian pitkä, jotta sen suorittaminen ei veisi heidän pääasialliselta työltään liikaa aikaa eikä häiritse terveyspalveluita. Koulutuksen on oltava myös mahdollista keskeyttää, jos suorittajataholle tulee kiireisempi työtehtävä. Kestoksi on sovittu 15–20 minuuttia.

Koulutus toimitetaan verkkokoulutuksena, joka suoritetaan toimeksiantajan HR järjestelmä Workdayssa. Koulutus tulee olemaan pakollinen kaikille, joten suoritusten määrän seuraaminen järjestelmässä on tärkeää ja kyseinen alusta mahdollistaa sen. Suurin osa myös muista koulutuksista on keskitetty kyseiselle alustalle.

Palaverissa saimme todettua, että olemme yhdessä linjassa projektin suhteen ja seuraavaksi järjestämme työpajan 25.9. Työpaja tarkoittaa järjestelyä, jossa ryhmä ihmisiä oppii, hankkii uutta tietoa toisiltaan, harjoittaa luovaa ongelmanratkaisua tiettyyn aihealueeseen liittyen (Ørngreen, Levinsen 2017, 71). Työpajassa saamme yhdessä kasvotusten käsiteltyä aihetta kokonaisvaltaisesti, koska työpajan kesto tulee olemaan pidempi kuin yksittäinen palaveri.

Tiistai 17.9

Jirassa ylläpidämme projektien ja tehtävien statusta. Työkalun tavoitteena on, että jokaisesta työtehtävästä olisi tiketti, jotta töiden statusta saataisi seurattua. Yhteistyötä tehdään paljon eri tiimien kesken ja kyseinen työkalu helpottaa ajan tasalla pysymistä. Edellispäivän tapaamisen perusteella päivitin omaa tikettiäni vastaamaan tämänhetkistä statusta kommentoimalla tikettiin tehdyt päätökset sekä luomalla uuden alatehtävän ensi viikon työpajalle.

Pidimme tiimin kanssa viikkopalaverin, jossa jokainen sai tuotua esiin tekemiään töitä sprintin ajalta, joka on ollut viikon mittainen. Tiimistäni kaksi jäsentä on myös mukana tietoturvakoulutusprojektissa, joten he tiesivätkin jo edellispäivän palaverin sisällön, mutta sain kerrottua myös muille tiimin jäsenille missä mennään tämän projektin osalta.

Keskiviikko 18.9

Minulla oli tänään toiseen projektiin liittyviä työtehtäviä, joten en kerennyt paneutua tietoturvan sekä tietosuojan koulutusohjelman projektiin lainkaan.

Torstai 19.9

Tein projektille alustavan suunnitelman keväällä, jossa kuvasin projektin etenemisen vaiheita. Suunnitelma ei ollut enää ajantasainen, sillä keväällä kuvaamassani suunnitelmassa projektia olisi päästy jo aloittamaan sekä koulutusta jalkauttamaan. En osannut keväällä suhteuttaa projektin laajuutta sekä siihen vaadittavaa aikaa, joten otin työn alle suunnitelman päivittämisen.

Projektin elinkaari voidaan nähdä nelijakoisena, johon sisältyy valmistelu, suunnittelu, toteutus sekä päättäminen (Mäntyneva 2016, 16). Valmistelua sekä suunnittelua on tehty keväästä asti, mutta kuten on projekteissa tapana, suunnitelmat voi muuttua.

Tuotan suunnitteludokumentin Confluenceen, tiimin työtilaan, jotta sen etenemistä voi kirjallisesti päivittää helposti saatavissa olevaan muotoon. Projektisuunnitelmille ei ole erillistä pohjaa, jonka perusteella sen voisi rakentaa, joten minulla on aika vapaat kädet siitä, mitä sinne tulisi kirjata. Koen tämän hieman haastavana, sillä en koe olevani riittävän ammattitaitoinen itse päättämään mikä on relevanttia tietoa ja mikä ei.

Päätin aloittaa dokumentin nykytilan läpikäynnillä, listasin asiat, joita käydään läpi tämänhetkisessä koulutuksessa. Koen, että näin saan seuraavaan kohtaan perusteltua, miksi koulutus tarvitsee uudistaa.

Perjantai 20.9

Jatkoin suunnitelman päivittämistä. Edellispäivän jälkeen minulla oli nykytilan läpikäynti ja seuraavaksi päätin lisätä tulevaisuuden tilan, jossa haluaisimme koulutuksen kanssa olla.

Tavoitteet koulutukselle ovat rooliperustaisuus sekä jatkuva kehitys muuttuvan uhkakentän mukaan. Rooliperustaisessa koulutuksessa sisältö on räätälöity työroolin mukaisesti, sairaanhoitaja ei hyödy koulutuksesta, joka on liian tekninen ja sovelluskehittäjä ei hyödy koulutuksesta, jos se on liian ylätasolla oleva. Projektin ensimmäisessä vaiheessa roolien tunnistaminen tuskin tuottaa hankaluuksia, mutta se on otettava huomioon projektin edetessä muihin vaiheisiin. Pohdin pitkään, listaisinko ensimmäisen vaiheen työroolit suunnitelmaan, mutta lopulta päätin jättää ne kirjaamatta.

Viikkoanalyysi 1

Ensimmäisellä viikolla ei vielä päästy itse työn suorittamiseen, vaan keskityin enemmän valmisteleviin toimenpiteisiin. Vaikka suunnitelmat vielä voi muuttua, koen että alustavan suunnitelman päivittäminen oli tärkeä osa projektia. Katsellessani keväällä tekemääni suunnitelmaa projektille, ymmärsin että alustava aikataulu, jonka tein ei ollut lainkaan realistinen. Ensimmäisessä suunnitelmassa olin jakanut projektin samanlaisiin osiin, miten se on nyt jaettu mutta olin asettanut aikataulutavoitteeksi, että toisen vuosikvartaalin aikana koulutus olisi jo jalkautettu terveydenhuollon henkilökunnalle. Nyt eletään kolmannen vuosikvartaalin loppupuolta ja projektia ollaan vasta käynnistämässä. Olisin toivonut keväällä palautetta epärealistisesta aikatauluhahmotelmastani, mutta oman ammatillisen kehittymisen kannalta koen, että on hyvä, kun itse huomasin asian.

Pohtiessani viikon aikana tekemääni työtä, mietin tietoturvakulttuuria yrityksessämme. Tietoturvakulttuurin kehittäminen on tärkeä osa tietoturvatietoisuutta, jotta yrityksen tärkeimmät voimavarat pysyvät suojattuina. Koulutuksen sisällön tulisi luoda tunne, että jokainen työntekijä on tärkeässä osassa yrityksen riskienhallintaa. (Merrit ym. 2024, 7.) Nykyinen koulutus ei tarjoa kovinkaan paljon tarttumapintaa työhön, jota suoritetaan, joten aihe voi jäädä etäiseksi. Koska tämänhetkinen koulutus on ollut käytössä useamman vuoden, voi olla hankalaa muuttaa työntekijöiden asennetta ja suhtautumista tietoturvaan.

4.2 Viikko 2

Viikon tavoitteenani on päästä etenemään projektissa ja tavata yhteistyökumppanimme edustajat. Itselleni ei ole kovin luontevaa palaverissa esittää asioita, vaikka tuntisin aiheen, joten aion myös harjoittaa esitystaitoja, kun pidämme yhteisen työpajan keskiviikkona.

Maanantai 23.9

Yrityksellä on käytössä sähköpostin tietoturvakoulutus, joka pelillisin keinoin kouluttaa sähköpostiin liittyvistä uhista. Sähköpostin tietoturvakoulutus on lisäosa, joka saadaan työntekijöiden sähköpostiin liitettyä ja se lähettää epäsäännöllisesti harjoitusposteja, jotka ovat kuten oikeita tietojenkalastelusähköposteja ja työntekijän tehtävänä on tunnistaa ja raportoida ne.

Lisäosa mahdollistaa myös oikeiden tietojenkalastelusähköpostien raportoimisen tietoturvatiimille. Tämä edesauttaa yritystä saamaan oikeanlaista kuvaa uhkakentästä, kun työntekijät raportoivat heihin kohdistuneista kalasteluyrityksistä eivätkä vain poista tulleita sähköposteja raportoimatta kenellekään. ENISA:n (2024, 7) raportin mukaan, vuoden 2024 ensisijaisten tietoturvauhkien joukossa on sosiaalinen manipulointi, johon tietojenkalastelu myös liitetään.

Tietoturvan sekä tietosuojan koulutusohjelman sisällöntuotanto tulee pääosin kumppaniyritykseltä, mutta aiomme sisällyttää siihen sähköpostin tietoturvakoulutuksen pakolliseksi osuudeksi. Sähköpostin tietoturvakoulutus on yrityksen kokoon nähden todella harvalla käytössä ja useista eri markkinointiyrityksistä huolimatta, käyttäjämäärää ei olla saatu kasvatettua. Toimme tämän ajatuksen esiin lisäosan palveluntarjoajan kanssa, ja he lähtivät mukaan toteuttamaan integraatiota Workdayhin.

Tiistai 24.9

Minulla oli toiseen projektiin liittyviä palavereja lähes koko päivä, joten en kerennyt suorittaa tietosuojan ja tietoturvan koulutusohjelmaan liittyen mitään.

Keskiviikko 25.9

Pidimme tänään työpajan yhdessä kumppaniyrityksen edustajien sekä yrityksemme tietosuojajohtajan kanssa. Aloitimme käymällä läpi nykyistä koulutusta, sen puutteita sekä hyviä puolia. Koulutuksen hyvänä asiana on sen interaktiivisuus, ettei koulutusta pysty suorittamaan ilman, että käyttäjä avaa huomiolaatikoita sekä se, että koulutuksen pystyy keskeyttämään ja jatkamaan kun tilanne sallii. Nämä asiat aiomme sisällyttää tulevaankin koulutukseen, sillä terveydenhuollon ammattilaisilla työ on hektistä ja voi tulla tilanteita, joissa heille ilmaantuu tärkeämpi työtehtävä. Saimme rutkasti ajatuksia kumppaniyrityksen edustajilta, kuinka heidän näkökulmastaan koulutusta voisimme toteuttaa. Keskustellessamme odotuksista, joita koulutuksen suhteen voi olla, tietosuojajohtajamme toi esiin erinomaisen ajatuksen siitä, että myös yrityksen asiakkaat vaativat korkealaatuista palvelua, joten voidaan myös ajatella, että emme pelkästään yrityksenä vaadi työntekijöitä kouluttautumaan, vaan myös meidän asiakkaamme vaatii korkeatasoista palvelua.

Koulutuksen sisältö tulee sisältämään konkreettisia toimia, joita voidaan toteuttaa tietoturvan parantamiseksi, tämä ei ainoastaan palvele yritystä, vaan yritämme suhteuttaa toimet siten, että myös henkilöstön yksityiselämässä he voisivat hyötyä toimista. Koulutuksessa tuomme esiin rikollisen näkökulman, miksi rikolliset kiinnostuvat jostakin työntekijästä ja mitkä ovat ne keinot, joilla he toimivat. Liian teknisiin kuvauksiin emme mene, vaan koitamme herätellä henkilöstöä näkemään asia sellaisesta näkökulmasta, josta harvemmin puhutaan.

Työpaja oli rento, saimme kaikki esittää omia mielipiteitä aiheeseen liittyen ja saimme luontevasti keskustellen suunnittelua tehtyä. Sovimme seuraavan palaverin marraskuun alkuun, sillä se oli ainut ajankohta, joka kaikille sopi. Joudumme priorisoimaan tietoturvan hallintajärjestelmän projektia, sillä sisäiset auditoinnit ovat alkaneet ja ne vievät niin paljon aikaa, ettei ole järkevää samanaikaisesti tehdä täysipainoisesti kahta projektia. Tietoturvan sekä tietosuojan koulutusohjelman kehitystyö pysyy käynnissä, mutta jää hieman taka-alalle.

Työpajan päätteeksi sovimme, että yhteydenpitoon käytämme yrityksen Slack- viestintäsovellusta. Joudun jättämään seuraavalle päivälle heidän kutsumisensa meidän ympäristöömme.

Torstai 26.9

Tänään aloitin päivän kirjaamalla Jira-tiketille eilisen päivän työpajan sisällön ja tein uuden tiketin kumppaniyrityksen kutsumisesta meidän Slack- ympäristöön. En kirjannut koko työpajan sisältöä Jiraan, vain pääpiirteet, jotta esihenkilömme näkee nopealla vilkaisulla missä mennään projektin kanssa.

En ollut varma kuinka ulkopuolisia kutsutaan meidän Slack- ympäristöön, joten hain Confluencesta ohjeet. Löysin kirjallisen ohjeistuksen ja varmistin kollegaltani, että tehdäänkö se sillä tavalla, sillä hän on aikaisemmin tehnyt ulkopuolisille kanavia. Hän muisteli, että yritys olisi jo ollut kutsuttuna meidän ympäristöömme, mutta tarkemmin katsottuaan hän löysi, että se oli irrotettu meidän ympäristöstämme. Hän neuvoi tekemään tiketin sisäisten palvelukanavien kautta, jotta toisen tiimin jäsen voisi kutsua kumppaniyrityksen edustajat Slackiin. Sisäisiä tukipyyntöjä varten on oma tikettijärjestelmänsä, jossa kaikki yrityksen edustajat voivat tehdä tukipyyntöjä, jotka menevät sille taholle kuka niissä voi avustaa. Yrityksessämme on oma tiimi tunnuksien hallinnointiin ja siitä tiimistä sain tukihenkilön avustamaan. Päivän päätteeksi yrityksen edustajat olivat meidän ulkoisella Slack kanavalla ja sain lisättyä itse kanavalle kollegani, esihenkilöni sekä tietosuojajohtajan.

Perjantai 27.9

Yrityksessämme on kehitetty tietoturvan hallintajärjestelmää 2023 toukokuusta lähtien ja olen itse ollut mukana kehitystyössä helmikuusta 2024 lähtien. Tietoturvan hallintajärjestelmä on riskiperustainen lähestyminen tietoturvaan, joka ottaa huomioon ihmiset, teknologian sekä prosessit. Tietoturvan hallintajärjestelmä sisältää politiikkoja, toimintatapoja sekä kontrolleja, joilla pyritään turvaamaan tiedon eheys, luotettavuus sekä saatavuus. (Kosling, 2024.) Tietoturvan hallintajärjestelmän sisäiset auditoinnit ovat käynnissä, ja koska olen ollut tiiviisti mukana hallintajärjestelmän teossa, olen myös mukana auditoinneissa. Sisäisessä auditoinnissa on tarkoituksena selvittää hallintajärjestelmän tila, puolueettoman tahon toimesta onko hallintajärjestelmä riittävän kypsä sertifiointiauditointiin. Meillä on kumppaniyritys suorittamassa sisäistä auditointia, koska yrityksen sisäisesti meillä ei ole osaajaa

suorittamaan sitä, joka ei olisi ollut kehittämässä hallintajärjestelmää. Kumppaniyritykselle on avattu pääsy hallintajärjestelmään sekä tarvittaviin dokumentteihin, joita auditoijat ovat tarkastelleet. Lisäksi auditoijat haastattelevat asiantuntijoita, jotta saadaan selville, noudatetaanko hallintajärjestelmän käytäntöjä todellisuudessa kuten ne ovat kuvattu. Tänään on vuorossa toimitusketjun sekä henkilöstön tietoturvatietoisuuden haastattelut.

Tietoturvan hallintajärjestelmä on tehty digitaalisille palveluille, joten koko yrityksen toimintoja ei ole otettu huomioon tässä hallintajärjestelmässä. Tämä osoittautui hieman haasteelliseksi, sillä hankintaan liittyvät asiat ovat rajauksen ulkopuolella, sillä hankintatiimi ei ole osa digitaalisia palveluita.

Henkilöstön tietoturvatietoisuuden haastattelussa oli paikalla kolme asiantuntijaa eri toiminnoista digitaalisista palveluista, joten saimme riittävän otannan siitä, kuinka tietoturva näkyy heidän työssään. Auditoinnissa haastattelun keinoin kävimme läpi, kuinka asiantuntijoiden mielestä tietoturvatietoisuutta on koulutettu. Olemme kollegani kanssa painottaneet asiantuntijoille, että sisäisen auditoinnin tarkoituksena on löytää kehitettävää yrityksen toiminnoista ja prosesseista, ei syyllisiä mistään kohtaan. Sisäiset auditoinnit voidaan nähdä oppimistilaisuutena, missä voisimme tehdä asiat paremmin. Onneksi asiantuntijat ovat tätä kuunnelleet ja sainkin ylös kehitysehdotuksia.

Kehitysehdotukset kirjasin projektin Jira-tiketille, jotta ne eivät unohdu. Tämä auttaa meitä myös sertifiointiauditoinnin jälkeen, koska hallintajärjestelmän keskiössä on jatkuva kehitys ja prosessien sekä toimintatapojen kehittäminen parempaan ja toimivampaan suuntaan.

Viikkoanalyysi 2

Kumppaniyrityksen kanssa pidimme keskiviikkona työpajan, josta saimme valtavasti eri näkökulmia, miten voimme koulutusta toteuttaa. Koulutuksen ollessa suunnattu aikuisille, opettamiskeinotkin pitää olla suhteutettuja aikuisille. Aikuisten oppimista voisi kuvailla ongelmakeskeisenä. Aikuiset haluavat oppia lisää, jotta voivat ratkaista jonkin ilmenneen ongelman. (Merriam, Bierema 2014, 65). Koulutus, joka tuo esiin rikollisen näkökulman tietoturvassa voi auttaa tässä, sillä aiomme tuoda ilmi, miksi jokin henkilö asemastaan riippumatta on kiinnostava verkkorikollisille. Tämä on ongelma, joka tuodaan esille ja koulutuksessa annamme ratkaisuja, kuinka suojautua työelämässä, mutta myös yksityiselämässä.

Toisella raportointiviikolla tuli ilmi, että joudumme priorisoimaan tietoturvan hallintajärjestelmän projektia, sillä se pitää sisällään useita auditointeja, jotka on jo aikataulutettu lokakuulle ja on havaittu monia asioita, joita tarvitsee vielä kehittää ennen sertifiointiauditointien alkamista. En osannut odottaa tätä, mutta ymmärrän projektin tärkeyden, joten joudun mukauttamaan omaa toimintaani töissä sen mukaiseksi. Tietoturvan hallintajärjestelmän projektiin arvioisin kuluvan työaikaa kahdesta kolmeen päivää viikossa lokakuun puoliväliin asti,

sillä sisäisiä auditointihaastatteluja on vielä jäljellä ja auditoinnin tulokset käydään läpi erillisessä tilaisuudessa. Koska sisäiset auditoinnit sekä työ tietoturvan hallintajärjestelmän parissa kuuluvat olennaisena osana työhöni, raportoin niistä päiväkohtaisesti myös.

Havaitsin oman asemani koulutusprojektissa hieman epäselväksi. Olemme tästä käyneet keskusteluja esihenkilöni kanssa keväällä, että toimisin projektin koordinoivana tahona, mutta projektin käynnistyttyä olen huomannut, että asia onkin jäänyt itselleni epäselväksi. Oma heikkouteni on, että koen häpeän tunnetta, kun en ole aiemmin asiaa osannut pohtia tällä tavoin ja joudun jälkikäteen kysellä ja palata aiheeseen. Työntekijän on ymmärrettävä oma roolinsa ja tämän lisäksi ymmärrettävä roolinsa osana yhteistä työtä (Mönkkönen, Roos 2010, 146). Tämä on tullut esille vasta asiantuntijatyössä, kuinka tärkeä on osata oma rooli ja tietää mitä se pitää sisällään. Edellisestä kokemuksestani työelämässä ei ole hyötyä tässä kontekstissa, sillä työtä suoritettiin hyvin mekaanisesti ja ohjeistukset sekä toimintamallit tulivat esihenkilöiltä. Koen, että epäselvyyksiä on jäänyt osittain siksi, etten ole osannut allokoida riittävästi aikaa itse projektin suorittamiseen liittyvien asioiden pohtimiseen, olen enemmänkin keskittynyt pohtimaan sisällöllisesti mitä olisi hyödyllisintä kouluttaa henkilöstölle.

4.3 Viikko 3

Edellisellä viikolla haasteeksi nousi oma asemani tietoturvan sekä tietosuojan koulutusohjelmassa, joten viikon tavoitteenani on käydä esihenkilöni kanssa keskustelua aiheeseen liittyen ja pyytää ohjausta. Tietoturvan hallintajärjestelmän sisäiset auditoinnit jatkuvat, ja tavoitteenani on osallistua niihin sekä havainnoida itse kehitysehdotuksia proaktiivisesti.

Maanantai 30.9

Viikko alkoi rauhallisesti, käymme maanantaisin läpi kollegani kanssa mitä tulemme viikon aikana tekemään liittyen tietoturvan hallintajärjestelmän projektiin. Projektissa on noussut useita kehitysehdotuksia ja minulla on työn alla hankintaketjuun liittyviä uudistuksia. Lokakuussa 2024 voimaan astuva NIS2 direktiivi, asettaa vaatimuksia kyberturvallisuuden riskienhallintaan, johon myös toimitusketjut kuuluvat (Traficom 2024). Olemme kerran käyneet hankintatiimin kanssa läpi mitä tietoturvaan liittyviä vaatimuksia haluaisimme lisätä heidän prosessiinsa, ja minulla on työn alla ollut vaatimuskohtien avaaminen, mitä tarkoitamme milläkin vaatimuksella. Pyysin kollegaltani kommentteja tekemääni dokumenttiin ja sain palautteeksi, että se on oikein toimiva tähän kontekstiin.

Kaikki hankinnat eivät mene keskitetysti oman tiiminsä kautta, vaan pienempiä hankintoja kuten lisenssit ohjelmistoon menevät IT:n sisällä oman prosessin kautta. Haluamme myös tähän prosessiin tuoda tietoturvaa mukaan. Päiväni kuluikin siinä, kun koitin sopia eri tiimien kanssa palavereja aiheisiin liittyen.

Tiistai 1.10

Sisäiset auditoinnit jatkuivat sovelluskehityksen teemalla. Ennen auditointia tarkastin suunnitelman, jonka saimme kumppaniyritykseltä ja kertaan päivän agendan sekä siihen liittyvät kohdat hallintajärjestelmästä. Itselleni sovelluskehityksen toiminta ja tekniset asiat ovat haastavia, joten koin tärkeäksi valmistautua tapaamiseen kertaamalla jo dokumentoituja materiaaleja. Auditoijat haastattelivat sovelluskehityksen vetäjiä, kuinka heidän käytännön työssään tietoturva otetaan huomioon.

Sisäisen auditoinnin jälkeen oli tietoturvatiimin viikkopalaveri. Palaverissa olikin iso määrä yleisiä asioita käsiteltävänä, sillä edellisviikon viikkopalaveri jouduttiin perumaan. Projektien lisäksi Jirassa on myös tikettejä pienemmille tehtäville, jotka sijoitetaan sprintille sitä mukaa kun niitä tulee ilmi. Pyrimme siihen, että suurin osa työstä, jota tehdään, olisi tiketti. Itselläni oli pienempi tehtävä, joka olin suorittanut ja merkinnyt valmiiksi, joten tiketti poistui sprintiltä, kun se suljettiin. Auki jääneet tiketit siirretään seuraavalle sprintille.

Viikkopalaverin jälkeen olin pyytänyt palaveria esihenkilöni kanssa toiseen asiaan liittyen, mutta koska kummallakaan ei ollut kiirettä sen asian käsittelyn jälkeen, toin esille omat haasteeni ja kysymykseni liittyen tietoturvan sekä tietosuojan koulutusprojektiin. Sain esihenkilöltäni ohjausta mitä kaipasin. Olin myös huolissani onko oma dokumentaationi ollut riittävä ja tarvitsisiko siihen lisätä jotakin. Esihenkilöni mielestä dokumentaatio on hyvällä tasolla, mutta voisin lisätä projektisivulle vielä keneltä voi kysyä lisätietoja. Ehdotin myös, että sulkisin aiemman Jira tiketin aiheesta, sillä se oli suunnitteluvaiheelle ja tekisin uuden tiketin itse projektille. Esihenkilöni piti tätä hyvänä ajatuksena ja neuvoi, että kannattaa kirjata sulkukommentti nykyiselle tiketille, joka kuvaisi, että suunnitelma on valmis ja siirrytään toteutusvaiheeseen. Uudelle Jira tiketille linkittäisin Confluencesta löytyvän suunnitelman.

Keskiviikko 2.10

Tänään oli vuorossa hallintajärjestelmän sisäinen auditointi arkkitehtuurista sekä verkkojen toiminnasta. Koitin valmistautua auditointiin käymällä läpi hallintajärjestelmää, mutta en koe, että minulla on riittävä ymmärrys yrityksen verkkoarkkitehtuurista. Se on selvästi puute itselläni, mutta myöskään tämänhetkinen työni ei vaadi kovin laajaa ymmärrystä asiasta. Kaikki asiantuntijat, joita olimme pyytäneet paikalle, pääsivät kertomaan, kuinka yrityksessä asiat tehdään, joten ei onneksi tarvinnut huolehtia siitä, etteikö haastattelussa kysymyksiin saataisi vastauksia.

Lähtökohtaisesti yritän keskittyä yhteen asiaan kerrallaan, kun teen töitä, mutta auditoinnin aikana mieleeni tuli, etten ollut lähettänyt kalenterikutsua marraskuun alkuun, kun otamme kumppaniyrityksen kanssa tietoturvan sekä tietosuojan koulutusohjelman seuraavan palaverin. Laitoin yhteiselle Slack- kanavallemme tiedustelua, otammeko samankaltaisen työpajan

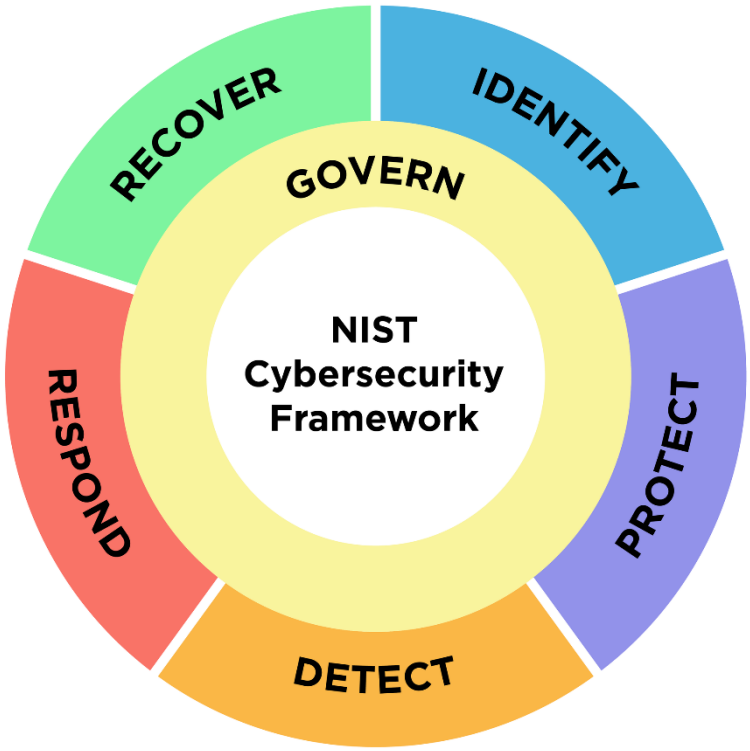
kuten aikaisemmin vai lyhyemmän tapaamisen, tätä emme sopineet edellisellä kerralla. En saanut päivän aikana vastausta kysymykselleni, joten joudun palaamaan siihen aiheeseen, kun saan kumppaniyrityksen edustajilta vastauksen.

Torstai 3.10

Keskityin tänään tietoturvan sekä tietosuojan koulutusohjelman dokumentaatioon. Sain aamulla vastauksen kumppaniyrityksen edustajalta eiliseen tiedusteluuni. Pidämme seuraavan tapaamisen myös työpajana. Sain laitettua kaikille työpajaan saapuville kalenterikutsut.

Aiemmin viikolla keskustellessani esihenkilöni kanssa, nousi esille, että voisin päivittää projektin Jira dokumentaatiota, sillä aikaisempi tiketti on ollut suunnitelman teolle. Laitoin sulkukommentin kyseiseen tikettiin ja merkitsin sen valmiiksi. Käytämme dokumentaatiossa NIST Cybersecurity viitekehystä. NIST Cybersecurity viitekehys on ohjeistuksia, joita organisaatiot voivat noudattaa ymmärtääkseen ja parantaakseen kyberturvallisuuteen liittyviä riskejä (NIST Cybersecurity Framework 2.0 2024, 1). Viitekehys on jaettu kuuteen toimintoon (kuvio 1), josta niitä voidaan jakaa kategorioittain. Tietoturvan sekä tietosuojan koulutusohjelma menee viitekehyksessä toiminnon Protect- alle ja Awareness and Training-alakategoriaan. Jirassa on paljon tikettejä, joita käsitellään ja kun ne ovat jaettu niiden toimintojen alle, mihin ne viitekehyksen mukaan kuuluvat, helpottaa tämä työn määrän kanssa.

Lisäsin tiketille lyhyen kuvauksen työstä ja linkitin Confluence sivun, jossa projekti on dokumentoituna. Vielä minulla ei ollut lisätä kovin montaa alatehtävää tiketille, vain seuraava työpaja, mutta työn edetessä alatikettejä tulee varmasti luotua enemmänkin.



Kuvio 1: NIST Cybersecurity Framework diagram (National Institute of standards and technology 2024)

Perjantai 4.10

Koitin jo alkuviikosta sopia palaveria hankintatiimin kanssa, jotta pääsisimme esittelemään tarkemmin NIS2 kyberturvallisuusdirektiivin tuomia vaatimuksia. Sain aamusta vastauksen tiedusteluilleni, ja saimme sovittua läpikäynnin lokakuun puoleenväliin. Laitoin kollegalleni viestiä aiheesta, jotta hän ei ihmettele, kun sähköpostiin tulee kalenterikutsu toisen tiimin viikkopalaveriin.

Yrityksessämme koitetaan mahdollisuuksien mukaan jakaa iloisia asioita kaikkien kanssa, joten muutaman kuukauden välein on tapahtuma, jossa eri tiimien edustajia tulee lyhyesti esittelemään, mitä heidän tiimissä tehdään tai jos jotakin uutta on otettu käyttöön, demoamaan sitä. Tämä tapahtuma oli tänään ja oli virkistävää saada katsaus siihen, mitä muilla on tapahtunut lähiaikoina. Itse en ole kyseisessä tapahtumassa käynyt esittelemässä mitään, mutta luulen, että kun tietoturvan sekä tietosuojan projekti etenee ja saamme jalkautettua ensimmäisen koulutuksen, saattaa tulla kutsu esittelemään sitä. Mutta se menee varmasti vasta ensi vuoden puolelle.

Viikkoanalyysi 3

Koin helpottavaksi, kun sain esihenkilölle tuotua ilmi omia haasteitani ja sain positiivista palautetta tähänastisesta työstäni. Olen kuitenkin tietoturvan alalla ihan urani alkuvaiheessa, joten koen tärkeäksi saada palautetta, jotta pystyn jatkossakin tekemään asiat oikein. Esihenkilöni muistutti minua myös olemaan armollinen itselleni ja muistamaan, että myöskään valmistumisen jälkeen en välttämättä ole valmis, vaan ala pitää sisällään jatkuvaa oppimista.

Toisinaan asiantuntijatyössä koen haasteita ison kuvan hahmottamisessa sekä yksin työskentelyssä. Aikaisemmassa työhistoriassani työ on ollut nopeatempoista ja työssä hyvin suoriutuminen tarkoitti sitä, kuinka paljon on päivän aikana saanut aikaiseksi. Asiantuntijuudessa asia on lähes päinvastainen, asioita suunnitellaan tarkasti ja palaverienkin saaminen voi kestää koko viikon. Pitäisi osata tarkastella kokonaisuutta, eikä pelkästään yksittäisiä työtehtäviä. Koen sen turhauttavaksi, mutta se on myös osittain uuteen rooliin opettelemisen kipuilua. Esihenkilöni kertoi tästä jo keväällä hyvän esimerkin; koitimme pohtia, kuinka saamme kasvatettua sähköpostin tietoturvakoulutuksen käyttäjämäärää, minä keksin sen, että se sidottaisi tietoturvan sekä tietosuojan koulutusohjelmaan. Tämä havainto on säästänyt useiden tuntien työtä, jossa koitetaan pohtia uusia markkinointikeinoja.

Olen havainnut, että tekemällä kirjallisen listauksen töistä, joita olen viikon aikana suorittanut, olen saanut itseltäni turhautumisen tunnetta pois. Konkreettisesti työn jäljen näkeminen auttaa hahmottamaan isoa kuvaa, missä yksittäisen päivän määrällinen työsuorite ei ole sen takeena oletko hyvä työntekijä vai et.

Yksin työskentelyyn on ollut vaikea opetella, kun aikaisemmassa työhistoriassa olen tehnyt työtä, joka vaatii työpisteellä olemista, kollegoiden kanssa. Asiantuntijatyössä asetelma on täysin päinvastainen, työn luonne mahdollistaa sen, että työtä voi tehdä milloin tahansa ja työn paikkasidonnaisuus on vähentynyt (Ahtela 2016, 9). Olen ottanut tavoitteekseni käydä viikoittain toimistolla, jotta työ ei tuntuisi niin yksinäiseltä.

4.4 Viikko 4

Tällä viikolla on yksi sisäinen auditointi tietoturvan hallintajärjestelmään liittyen, tavoitteenani on tarkastella toimistomme tiloissa, kuinka fyysisen turvan kontrollit täyttyvät, jotta auditoijan kysyessä jotain, osaisin itse vastata suoraan. Tavoitteenani on myös saada esitysmateriaalia tuotettua ensi viikon hankintapalaveriin.

Maanantai 7.10

Kävimme kollegani kanssa joka maanantaisen palaverimme, jonka aikana keskustelimme, mitä töitä tämän viikon aikana saamme edistettyä. Toisinaan palaverissa keskustelunaiheet vaihtelevat projektista toiseen ja koen, että olen monessakin asiassa saanut häneltä arvokasta oppia. Itselläni on työn alla hankintaan liittyvät turvallisuusvaatimukset. Pidämme tulevana

perjantaina palaverin toisen tiimin edustajien kanssa, kuinka saisimme tietoturvaa tuotua heidän prosesseihinsa. Tähän liittyen koitimme keksiä, miten muotoilisimme vaatimukset, jotta toiselle tiimille ei tulisi kohtuuttomasti lisää työkuormaa, mutta siten, että saisimme myös vastauksia tietoturvan tasosta, kun pienempää softaa ollaan hankkimassa. Keskustelimme myös tiketistä, jonka esihenkilömme oli hänelle osoittanut. On tullut ilmi, että yrityksen tietoturvaohjeistuksia olisi syytä parantaa laitteiden hyväksytyn käytön osalta. Olemme keskustelleet tietoturvaohjeistusten selkiyttämisestä, osana tietoturvan sekä tietosuojan koulutusohjelmaa, sillä aiomme koulutukseen sisällyttää osion, jossa kerrotaan mistä ajantasaiset ohjeistukset löytyvät. Ohjeiden parantamisen myötä aihe nousi jälleen esiin.

Suurin osa ohjeistuksista on Sharepointissa, josta yrityksen työntekijät pääsevät niitä lukemaan. Aloitamme päivitykset yleisistä tietoturvan sekä tietosuojan ohjeistuksista, sillä se sivu on linkattu myös moneen muuhun paikkaan. Aloitin tarkastamalla minkä tiesin olevan vanhentunutta tietoa, ja korjasin ne. Tiketillä, jonka esihenkilömme oli kollegani osoittanut, oli kuvaus mitä ainakin tarvitsisi kirjata, joten jatkoin pohtimalla, kuinka ne olisi hyvä kirjoittaa ohjeistuksiin.

Tiistai 8.10

Tänään keskityin esitysmateriaalin tekoon seuraavan viikon hankintapalaveria varten. Tarkoituksena on esitellä mitä vaatimuksia haluaisimme tuoda tietoturvan näkökulmasta ja miksi. Lokakuussa voimaan astuva NIS2 direktiivi sekä ISO27001 sertifiointi toimii pohjana vaatimuksille.

Euroopan Unionin kyberturvallisuusdirektiivi (EU) 2022/2555 eli NIS2 korvaa aiemmin vuonna 2016 voimaantulleen NIS direktiivin. Direktiivin tavoitteena on vahvistaa EU:n ja jäsenvaltioiden kyberturvallisuutta kriittisillä toimialoilla. Kyberturvallisuusdirektiivi on ollut voimassa joulukuusta 2022 lähtien ja se on saatettava osaksi kansallista lainsäädäntöä 17.10.2024 mennessä. (Valtioneuvosto 2024.)

Kyberturvallisuusdirektiivin (EU 2022/2555) 21 artikla kuvaa kyberturvallisuusriskien hallintatoimenpiteitä, joita jäsenvaltioiden keskeiset ja tärkeät toimijat tulevat noudattamaan. Toimitusketjun turvallisuus on osana hallintatoimenpiteitä. Kollegani on tehnyt listauksen vaatimuskohdista, jotka täyttävät vaatimukset ja joita haluamme alihankkijoiden sekä yhteistyökumppaneiden noudattavan tietoturvatoiminnassaan ja minä olen avannut vaatimuskohdat siten, että ne ovat selitettynä auki, mitä tarkoitamme kyseisellä kohdalla. Tämä on erityisen tärkeää siksi, että emme ole jokaisessa hankinnassa mukana niin tiiviisti ja haluamme, että myös hankinnassa ymmärretään mitä tullaan vaatimaan, jos heille esitetään kysymyksiä. Hankalinta materiaalin teossa oli kuvaus direktiivistä ja mietin pitkään, kuinka pystyisin lyhyesti kuvaamaan mistä on kyse, menemättä liian paljon yksityiskohtiin. Tapanani on innostua ja

selittää joskus turhankin syvällisesti asioista, kun pitäisi osata tiiviisti kuvata käsillä olevaa asiaa. Sain päivän aikana materiaalin tehtyä.

Keskiviikko 9.10

Jatkoin tänään pohtimista, miten tietoturvaohjetta laitteiden hyväksytyn käytön osalta kannattaisi parantaa. Ohjeistuksen tulisi olla senkaltainen, jotta henkilöt, jotka eivät ymmärrä tietoturvaa kovin syvällisesti, ymmärtäisivät mitä sillä tarkoitetaan (Taylor, Alexander, Finch & Sutton 2013, 12). Kyseessä ei ole politiikkatason dokumentti, joten ohjeistukseen voi lisätä esimerkkejä, jotka voisivat havainnollistaa minkälaisia ohjelmistoja esimerkiksi ei saa asentaa työnantajan tarjoamille laitteille. Nykyisessä ohjeistuksessa sanotaan, ettei mitään tulisi asentaa ilman tietohallinnon ohjeistusta, itse pidän tätä yksiselitteisenä ohjeistuksena, joten oli hankalaa muotoilla lause uudelleen, jotta siihen saisi sisällytettyä esimerkkejä.

Lisäksi listasin omia ajatuksia, mihin ohjeisiin voisimme lisätä linkit sivulle, jotta se palvelee mahdollisimman kattavasti niitä, joille ohjeet tehdään.

Torstai 10.10

Tänään keskityin pohtimaan, miten voisimme tuoda tietoturvaa pienempiin softahankintoihin, keskustelimme maanantaina tästä kollegani kanssa ja jatkoin asian työstämistä. Nykyisellään on kysymyslista, johon käyttäjän tulee vastata, jos hän haluaa jonkin softan tai lisenssin käyttöönsä mitä ei vielä ole. Tietosuojan osalta datan sijainti on kysymyslistalla, mutta tietoturvan osalta haluamme tuoda lisäyksiä. Hankaluutena on ollut keksiä sellaiset vaatimukset, jotka mukailisivat ISO27001 sekä NIS2, menemättä liian yksityiskohtaisuuksiin, sillä käyttäjän on itse löydettävä vastaukset ja tuotava ne ilmi tilauslomakkeella. Kollegani maanantaina toi ilmi, että voisimme johonkin kohtaan tuoda myös riskikulman, syntyykö softan käytöstä riskiä, jos palveluntarjoajalla tapahtuu tietomurto. Kasasin omat ajatukseni Confluence sivulle, jotta meillä olisi huomenna pidettävässä palaverissa näyttää, mitkä ovat ne mitä olemme tuomassa mukaan prosessiin.

Perjantai 11.10

Tietoturvan hallintajärjestelmän sisäiset auditoinnit jatkuivat tänään fyysisellä auditoinnilla toimistolla. Aloitimme tarkastelemalla hallintajärjestelmää ja käymällä läpi toimistojen turvallisuusohjeistuksia. Saimme tämän keskustelun aikana monia kehityskohteita nostettua itsellemme.

Jatkoimme auditointia kävelemällä toimiston tilat läpi, sekä esittelemällä kuinka fyysinen tietoturvallisuus näkyy toimistossamme. Itselläni on vahva tausta fyysisen turvallisuuden parista, joten tämä aihealue oli itselleni kovin tuttu ja pystyinkin kertomaan, kuinka käytännössä toimimme varmistaaksemme fyysisen turvallisuuden toimistossa.

Auditoinnin jälkeen, oli palaveri toisen tiimin edustajien kanssa, tietoturvalisäyksistä softan hankkimisprosessiin. Palaveri oli kaikille mieluisa ja toisen tiimin edustaja saikin palaverin aikana tehtyä pyytämämme muutokset. Olin itse huolissani lisäisikö meidän vaatimuksemme heidän työkuormaansa, mutta heillä oli myös intressinä prosessin parantaminen sekä se, että turvattomia hankintoja ei tehtäisi.

Palaverin jälkeen käytin aikaa Jirassa tikettejä päivitellen. Lisäsin kommentit muutoksista, joita olimme tehneet, jotta asiasta olisi dokumentaatiota projektin tiketillä sekä suljin tiketin valmiina. Aamupäivällä auditoinnin aikana nousi kehitysehdotuksia, joita olin kirjannut itselleni ylös. Pidämme hallintajärjestelmän projektin Jirassa omaa tikettiä kehityskohteille, joten kirjasin sinne kaiken ja lisäsin lyhyet kuvaukset, mitä sillä haetaan.

Viikkoanalyysi 4

Tämä viikko oli pitkälti suunnittelutyötä, mutta koen että pääsin tavoitteeseeni, jotka asetin itselleni viikon alussa.

Olemme jo pitkään suunnitelleet ja pohtineet kuinka saisimme tuotua tietoturvaa myös hankintoihin, ja siksi olin erityisen innoissani perjantain tapahtumista, kun suunnittelemani tietoturvalisäykset otettiin heti käyttöön ja toinen tiimi piti niitä hyvinä lisäyksinä. Ensi viikolla on vielä toinen tapaaminen aiheeseen liittyen, mutta eri tiimin kanssa. Vaikka hankintakulma on vain yksi osa-alue tietoturvan hallintajärjestelmää, koen, että olen saanut paljon edistettyä tietoturvallisuutta. Pyysin itse, että saisin edistää hankintaan liittyviä tietoturvalisäyksiä, sillä aihe kiinnosti itseäni ja tiesin, että myös lainsäädäntö on ottamassa aiheeseen kantaa NIS2 direktiivin muodossa.

Alanvaihtajana minulla on aikaisemmasta työhistoriasta kokemusta sekä tietoa. Olen nähnyt haasteellisena fyysisen turvallisuuden kokemuksen hyödyntämisen tietoturvallisuuteen. Itsearviointi korostuu osaamisen tunnistamisessa, vaikka se tuottaa selvän haasteen paitsi omatoimisesti tunnistaa, mitkä kaikki voi olla relevanttia ja arvokasta osaamista, mutta myös vaikeuden sanoittaa sitä tavalla, jonka työnantajat tunnistavat (Rahikainen ym. 2024, 151). Olen aikaisemmin pohtinut, kuinka voisin hyödyntää aikaisempaa osaamistani, mutta fyysinen toimistoauditointi oli konkreettinen esimerkki, kuinka sain tuotua aikaisemman työhistorian osaamista nykyiseen ammattiini. Pystyin tuomaan ilmi, mitkä asiat on turvallisuuden kannalta hyvin hoidettu ja missä on parantamisen varaa. Olen aikaisemmin tehnyt fyysisen turvallisuuden GAP- analyysiä nykyiselle työnantajalleni, joten olen myös pystynyt tuottamaan esimerkkejä, kuinka voisimme parantaa realistisesti turvallisuuden tasoa. Mitä enemmän opin tietoturvasta ja sen hallinnoinnista, sen paremmin pystyn näkemään yhtymäkohtia fyysiseen turvallisuuteen ja sitä kautta tuomaan omaa osaamistani paremmin esiin.

4.5 Viikko 5

Tämän viikon tavoitteenani on saada viimein päätökseen hankintaprosessiin liittyvät uudistukset sekä jatkaa ohjeistusten parantamista, joka nousi aiheeksi edellisellä viikolla.

Maanantai 14.10

Tietoturvan hallintajärjestelmän joka maanantainen palaveri kollegani kanssa oli myös tänään ja esille nousi muutamia kehityskohteita, joita voisimme alkaa edistämään. Kollegallani on työnohjauksellinen rooli, mitä tulee minun tekemisiini tietoturvan hallintajärjestelmän parissa, tämä on ollut mielestäni hyvä ratkaisu, sillä projekti on hänen ja minun osaamiseni ei ole vielä sillä tasolla, että olisin pystynyt itsenäisesti hyppäämään projektiin keväällä mukaan ilman ohjausta ja apua. Mutta projektin edetessä, minulle on annettu enemmän vastuuta ja saankin aika lailla itse päättää mitä kehityskohteita aion itse alkaa edistämään. Edellisessä fyysisessä auditoinnissa nousi laitteiden käytöstä poistamisen yhteydessä puute, otin tämän asian itselleni hoitaakseni sekä muutamia ohjeistuksiin liittyviä asioita.

Tänään oli viimeinen sisäinen auditointipäivä ja auditointi suoritettiin yhdellä toimipisteellä. Toimipisteeltä on tarkoitus muuttaa ensi vuoden alussa, mutta tämä oli erinomainen hetki kerätä ajatuksia, mitä uudella toimipisteellä voitaisi paremmin ottaa huomioon liittyen fyysiseen tietoturvallisuuteen. Tosin sellaisia kehityskohteita missä tietoturvatiimi pystyisi avustamaan, ei noussut kovin paljoa.

Esihenkilöni myös tiedusteli, olisinko halukas pitämään uudelle työntekijälle pienen esittelyn fyysisen turvan kehityskohteista, joita nousi esille edellisviikon auditoinnissa. Koin tämän mielekkääksi ja olin heti mukana.

Tiistai 15.10

Tänään oli tietoturvan hallintajärjestelmään liittyen johdon katselmus. Johdon katselmus on ISO27001 sertifioinnin vaatimuksena, ja tarkoituksena on tarkastella säännöllisesti hallintajärjestelmä ja arvioida sen soveltuvuutta sekä tarkoituksenmukaisuutta (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2023, 15). Johdon katselmuksissa myös tarkastellaan muutokset, joita hallintajärjestelmään on tehty. Tämä oli ensimmäinen johdon katselmus ja nyt oli tarkoituksena hyväksyttää hallintajärjestelmä ja sen sisältämät politiikat johdolla sekä tarkastella millä tavalla hallintajärjestelmää tullaan pyörittämään ja kuinka se saataisi sidottua osaksi arkea sekä perustyöntekoa.

Pääosin hallintajärjestelmä hyväksyttiin sellaisenaan, mutta tarkennuksia riskienhallintaan pyydettiin ja tästä aiomme ottaa työn alle aktiivisen tiedottamisen, kuinka riskienhallintaa tulisi tehdä ja kuinka kaikilla riskeillä tulisi olla omistaja. Riskienhallintaa tulisi tehdä johdonmukaisesti sekä kirjata ylös havaitut riskit sekä tehdä niille toimenpiteet. Työkaluna tässä

käytämme myös Jiraa, jotta riskienhallinta olisi helposti toteutettavissa, eikä tarvitse käyttää erillistä työkalua. Vuosi sitten on pidetty riskityöpajoja, jossa suurimmaksi osaksi kaikille tiimeille on esitelty kuinka riskienhallintaa kannattaisi tehdä.

Johdon katselmuksen lisäksi pidimme viikkopalaverin, jossa kävimme läpi viikon aikana tehtyjä töitä sekä tarkastelimme sprintin tikettejä. Pohdimme, pitäisikö tietoturvan hallintajärjestelmän tiketit tuoda osaksi sprinttejä, mutta päätimme että tämä on todennäköisesti seuraavan vuoden asioita, sillä tulevana vuonna keskitymme hallintajärjestelmän pyörittämiseen.

Keskiviikko 16.10

Tänään pidimme palaverin hankinnan kanssa, jossa esittelimme NIS2 tuomat velvoitteet toimitusketjujen hallintaan. Saimme palaverissa sovittua, että näitä vaatimuksia aletaan soveltamaan jo tällä viikolla, kun kyberturvallisuuslain pitäisi astua Suomessa voimaan. Palaverissa nousi ilmi, että miten toimitaan silloin, kun toimija ei täytä vaatimuksia. Tällöin voi nousta riski, jonka käsittelyyn on oma politiikkansa. Lisäsin esitysmateriaaliin tämän kohdan ja toimitin sen koko toiselle tiimille, jotta heilläkin on materiaalia, kun vaatimuksia aletaan lisäämään sopimuksiin.

Torstai 17.10

Keskityin tämän päivän ohjeiden päivittämiseen, jonka aloitimme edellisellä viikolla. Koitin jo aikaisemmin muotoilla laitteiden hyväksytyn käytön kohtaa ja tänään päätin tehdä sen kokonaan uudestaan, siten, että jokaiselle laitetyypille tulee oma alaotsikkonsa, jotta sellaiset henkilöt, jotka haluavat löytää ohjeistusta vain johonkin tiettyyn laitteeseen liittyen, löytävät sen helpommin.

Keräsin Sharepointista ohjeistuksia ja tarkastin mitä niihin on kirjattu, jotta ohje on linjassa muiden ohjeistusten kanssa. Kahdesta ohjeistuksesta löytyi ristiriitaisuuksia keskenään, laitoin nämä uuteen ohjeeseen, mutta lisäsin kommentin sen kappaleen kohdalle, jotta muistamme käydä keskustelua, kuinka asia halutaan linjata.

Tiedustelin kollegaltani, kuinka vapaat kädet ohjeen tekoon on, jotta tiedän missä raameissa pysyä. Ohjetta ei oteta käyttöön, ilman tietoturvan sekä tietosuojan ohjausryhmän tarkastusta ja hyväksyntää, joten toistaiseksi on hyvinkin vapaat kädet päivityksiin.

Halusin erityisesti lisätä toimitilaturvallisuutta käsittelevään kohtaan maininnan, että henkilökortteja tulisi käyttää, kun ollaan fyysisesti toimipisteillä. Olen huomannut, että kuvallisten henkilökorttien käyttö ei ole kovin suosittua yrityksessä, vaikka se olisi hyvä tapa edistää toimitilaturvallisuutta, kun heti pystyy näkemään, onko kyseessä henkilökunnan jäsen vai joku ulkopuolinen. Hallinnon puolella käyttö on lisääntynyt, kun yhdistimme kuvallisen henkilökortin sekä kulkuavaimen, mutta silti henkilöstö ei kovin mieluusti niitä käytä. Itse pidän tätä

kummallisena, sillä oman työhistoriani aikana, olen aina joutunut käyttämään henkilökorttia ja se lisää toimitilaturvallisuutta. Lisäksi kun on paljon työntekijöitä, niin helposti näkisi kenen kanssa juttelee.

Perjantai 18.10

Itseäni kiinnostaa kovasti tekemäni työn lainsäädännön velvoitteet, ja siksi aloitin päiväni tarkastamalla, olisiko NIS2 direktiivistä tullut lisää tietoa. Kyberturvallisuuslain olisi pitänyt astua kansalliseen lainsäädäntöön tänään. Vielä ei ollut tullut päivitettyä tilannetietoa.

Saimme tänään myös tietoturvan hallintajärjestelmän sisäisen auditoinnin raportin. Käymme seuraavalla viikolla auditoijien kanssa yhdessä läpi raporttia, mutta oli mielenkiintoista jo ennakkoon nähdä mitkä asiat nostettiin puutteiksi ja mitkä kehitysehdotuksiksi. Osan puutteista olimme jo kirjanneet itse kehityskohteiksi ja ottaneet työn alle, jotta sertifiointiauditoinnissa saamme näytettyä, että hallintajärjestelmää jatkuvasti kehitetään. On myös helpompi auditoinnin raportin kanssa osoittaa eri tiimeille, mitä asioita tulisi kehittää, kuin että lähtisi pyytämään muutoksia ihan kylmiltään, vaikka yleisesti ottaen yrityksessä koitetaan jatkuvasti kehittää toimintaa ja prosesseja.

Viikkoanalyysi 5

Tällä viikolla tuli päätökseen hankintaan liittyvät tietoturvavaatimukset. Itselleni tämä oli merkityksellinen virstanpylväs, sillä suurimmaksi osaksi ne olivat minulla työn alla ja palaverissa esitin vaatimukset, toki kollegani tuki täydentämällä aihealueita, jotka eivät ole itselleni niin tuttuja. Aikaisemmin hankinta ja tietoturva ei ole tehnyt kovinkaan paljoa yhteistyötä ja koin, että yhdessä pitämämme palaveri toi tietoturvaa taas hieman enemmän näkyvämmäksi osaksi ja saimme tuotua tietoturvaa lähemmäs arjen työntekoa.

Riskienhallinta nousi monissa keskusteluissa esille kuluneella viikolla. Riski yleisesti tarkoittaa epävarmuuden ja mahdollisten negatiivisten seurausten yhdistelmää. Riskienhallinnan tarkoitus on tunnistaa, analysoida, arvioida sekä käsitellä, eli kokonaisvaltaisesti hallita riskejä. (Juvonen, Koskensyrjä, Kuhanen, Kämppi & Talala 2023, 3–19). Tietoturvan rooli riskienhallinnassa on tärkeä osa yrityksen kokonaisvaltaista riskienhallintaa, sillä kasvavissa määrin yritykset käyttävät erilaisia teknologisia tietojärjestelmiä (NIST Managing Information Security Risk 2011, 2–3). Tietoturvavaatimukset, joita haluamme saada mukaan hankintoihin, ovat osa riskienhallintaa. On tarve selvittää, onko mahdollinen yhteistyökumppani varautunut mahdollisiin häiriötilanteisiin tai kouluttavatko ne henkilöstöään tietoturvallisuudesta. Jos yhteistyökumppaniksi valittaisi jokin sellainen taho, joka ei kouluta henkilöstöään tietoturvallisuuden osalta, se voisi olla mahdollinen riski. Vaatimalla yhteistyökumppaneilta henkilöstön kouluttamista, häiriötilanteisiin varautumista sekä erilaisia tietoturvakäytäntöjä, voimme varmistua, että kumppani on myös tietoturvallinen. Tässä yhteydessä meidän täytyy myös tarkastella

omaa toimintaa, sillä terveydenhuollonalan toimijana myös meidän toimintaamme liittyy riskejä.

Riskien tunnistaminen on verrattain helppoa, mutta niitä pitäisi myös käsitellä sekä seurata. Seuranta edellyttää systemaattista toimintatapaa, jonka mukaisesti riskejä kartoitetaan säännöllisesti (Juvonen ym. 2023, 23). Koen, että riskienhallinta ei ole vielä täysin integroitunut päivittäisiin toimintatapoihin, riskejä on tunnistettu ja suurimmaksi osaksi niillä on omistaja, mutta niiden käsittely on jäänyt hieman taka-alalle. Tämä voi johtua asiantuntijoiden kiireisestä työstä, mutta osittain varmasti tiedon puutteesta. Toivomme, että kun alamme muistuttamaan säännöllisesti riskien omistajia, saamme myös edistettyä riskien käsittelyä.

4.6 Viikko 6

Tämän viikon tavoitteena, on saada purettua tietoturvan hallintajärjestelmän auditointiraporttia ja tehdä kaikista havaituista asioista omat tiketit sekä sivut Confluenceen. Pidämme myös raportin purkutilaisuuden, jossa käymme läpi yhdessä auditoijien kanssa suoritettua sisäistä auditointia.

Maanantai 21.10

Saimme edellisen viikon perjantaina auditointiraportin tietoturvan hallintajärjestelmän sisäisestä auditoinnista. Kävin sitä jo perjantaina lävitse, mutta tänään kollegani kanssa keskustelimme mitkä ovat seuraavat tehtävät siihen liittyen. Raportissa oli kirjattuna puutteet (non-conformities) sekä kehitysehdotukset (opportunities for improvement). Puutteet tarkoittavat sitä, että implementoinnissa tai käytännöissä on jotakin sellaista, joka ei täysin vastaa sertifioinnin vaatimuksia ja se tulisi tällöin korjata. Kehitysehdotukset olivat sellaisia, että implementointi vastaa sertifioinnin vaatimuksia, mutta kehitysehdotus voisi parantaa käytäntöjä.

Aikomuksena on siirtää havaitut puutteet sekä kehitysehdotukset Confluenceen sekä Jiraan, jotta korjaukset, joita teemme, tulee myös dokumentoitua. Pyysin kollegaltani, voisinko ottaa suurimman osan havaintojen siirroista itselleni, koska raportoinnissa on myös kirjattava korjaavat toimet. Koin, että olisi hyödyllistä oman oppimiseni kannalta pohtia korjaavia toimia usean havainnon kohdalla. Tämä kävi kollegalleni.

Osa havainnoista, oli sen kaltaisia, että ne vaativat toisilta tiimeiltä joko lisää ohjeistusten tekoa tai muuta muokkausta. Laitoinkin toisen tiimin edustajalle tiedon auditointiraportista ja kerroin, että voisi olla ihan hyvä ottaa asia työn alle, ennen seuraavaa auditointia. Tiedustelin myös, olisiko toisen tiimin edustaja halukas tulemaan auditointiraportin purkutilaisuuteen, hän oli, joten laitoin hänelle myös kalenterikutsun.

Puutteiden luokittelu oli jaettu kahteen kategoriaan, merkittävä sekä vähäinen. Suurimmaksi osaksi puutteet oli luokiteltu vähäisiksi, mutta joukkoon oli päätynyt myös yksi merkittävä.

Olemme aikaisemminkin keskustelleet kollegani kanssa, kuinka merkittävien puutteiden kanssa toimitaan, jotta saamme tarpeeksi hyvin näytettyä seuraavassa auditoinnissa, että edistämme ja jatkuvasti kehitämme hallintajärjestelmää, mutta kyseinen puute oli luonnoltaan sen kaltainen, että sen korjaaminen vaatii useamman tiimin työpanosta ja on isotöinen, joten tästä kysyin kuinka sen kanssa kannattaisi toimia. Sovimme, että kirjaamme sen ylös kuten muutkin puutteet, mutta sen korjaamiseksi todennäköisesti tarvitsemme esihenkilömme apua.

Tiistai 22.10

Jatkoin tänään auditoinnin puutteiden kirjaamista Confluenceen sekä Jiraan. Auditointiraporttiin jokaisen havainnon kohdalle oli kirjattu suositellut toimet, mutta joidenkin puutteiden kanssa minulla meni hyvin paljon aikaa sovittaa suositellut toimet meidän yrityksemme kontekstiin. Sellaisten puutteiden kohdalla, josta en ollut varma, päätin säästää seuraavalle päivälle, kun pidämme auditointiraportin läpikäynnin auditoijien kanssa, jotta saamme varmat vastaukset ja kirjattua korjaavat toimet oikein.

Pidimme myös viikkopalaverin, jossa tarkasteltiin menneen viikon työtehtäviä. Meidän tiimillämme on sprintit olleet aiemmin viikon mittaisia, mutta ne on vaihdettu kahden viikon mittaisiksi, jotta työtahtimme olisi samassa linjassa muiden digipalveluiden tiimien kanssa, joten tikettejä emme tällä kertaa tarkastelleet. Käymme viikkopalaverin lopussa läpi, onko menneeltä viikolta joitakin kohokohtia tai haasteita ja sainkin tuotua kohokohdaksi sen, että hankintaan liittyvät vaatimukset on saatu vietyä eteenpäin.

Keskiviikko 23.10

Pidimme tänään tietoturvan hallintajärjestelmän auditoijien kanssa raportin läpikäynnin. Paikalle saimme myös toisten tiimien esihenkilöitä, jotta he saisivat myös käsityksen, mitä heidän tarvitsisi prosesseissaan kehittää. Merkittävä puute liittyi laitteiston sijoitteluun ja tästä olisin itse toivonut, että keskustelua syntyisi, tai edes palaverin sopimista oikeiden henkilöiden kesken, mutta keskustelua ei tullut. Aihe on monimutkainen ja koen hieman, että sen hoitamista saatetaan vältellä. Tuskin tahallisesti, mutta ainakin sen kannalta, että kenen vastuulle se kuuluu.

Itselleni jäi epäselväksi osa puutteista, kun edellispäivänä aloitin siirron Confluenceen sekä Jiraan, mutta kun kävimme yhdessä lävitse kaikki puutteet, niin sain selvyyden niihinkin.

Muutoin päivän aikana jatkoin puutteiden kirjaamista ja koitin pohtia, kuinka niitä voisimme kehittää, jotta kontrollit olisivat sertifioinnin kanssa linjassa.

Torstai 24.10

Sain tänään kirjattua kaikki puutteet itsellemme Confluenceen sekä Jira tiketeiksi ja aloitin kehitysehdotusten kirjaamisen. Kirjaamme kollegani kanssa kehitysehdotukset, siten, että kirjaamme löydöksen ID-numeron otsikon perään, jotta ne tunnistettaisi olevan kehityskohteita, eivätkä niin kriittisiä toteuttaa kuin puutteet. Osa kehitysehdotuksista oli toistensa kanssa samankaltaisia, ja nämä yhdistettiin yhdelle tiketille. Pääosin samankaltaisuudet liittyivät tietoisuuteen tai kouluttamiseen.

Kollegani teki muutoksia poikkeamanhallintaohjeistukseen ja pyysi minulta kommentteja, olisiko minulla jotakin lisättävää. Pääosin muutokset liittyivät NIS2 direktiivin vaatimuksiin ilmoituksista. Kyberturvallisuusdirektiivin (EU 2022/2555) mukaisesti, toimijan täytyy tehdä ennakkovaroitus merkittävästä poikkeamasta 24 kuluessa kun toimija tulee tietoiseksi merkittävästä poikkeamasta sekä poikkeamailmoitus 72 tunnin kuluessa siitä, kun toimija tulee tietoiseksi merkittävästä poikkeamasta. Lopullinen raportti tulisi toimittaa kuukauden sisällä valvovalle viranomaiselle. Lisäsin kommentiksi, että voisi olla hyvä selkiyttää mikä taho ilmoitukset tekee, kun merkittävä poikkeama tapahtuu.

Esihenkilöni muutama viikko aikaisemmin tiedusteli, pitäisinkö uudelle työntekijälle katsauksen fyysisen turvallisuuden asioista, mitä nousi esille tietoturvallisuuden hallintajärjestelmään liittyen. Nyt kun olimme saaneet loppuraportin, niin ajattelin, että olisi hyvä saada palaveri sovittua ja saimmekin sovittua ensi viikolle katsauksen.

Perjantai 25.10

Jatkoin tänään kehitysehdotusten kirjaamista Jiraan. Osaan kehitysehdotuksista minulla oli ajatuksia, kuinka voisimme niitä toteuttaa ja kirjasin ne itselleni ylös. Ensi viikolla lähdemme kollegani ja esihenkilömme kanssa Cyber Security Nordic tapahtumaan Messukeskukseen. En ole aikaisemmin käynyt messuilla, jotka liittyisivät kyberturvallisuuteen, joten olen innoissani päästessäni tapahtumaan kuuntelemaan ajankohtaisia aiheita kyberturvallisuudesta.

Viikkoanalyysi 6

Asettamani tavoitteet tälle viikolle täyttyivät lähes kokonaan. Kaikki kehitysehdotuksia en kerennyt kirjaamaan, sillä käytin niiden, kuten puutteidenkin kanssa, paljon aikaa pohtimiseen sekä korjaavien toimenpiteiden ideoimiseen. Puutteiden kanssa suositellut korjaavat toimenpiteet ovat olleet suoraviivaisia, mutta todennäköisesti tulee vaatimaan muidenkin tiimien osallistumista. Se voi olla haaste, sillä kuluvalla viikolla havaitsimme, että turvallisuuskulttuuri yleisesti ei ole kovin hyvällä tasolla. Turvallisuutta, oli se sitten fyysinen tai tekninen, pidetään osin enemmän työtä haittaavana osana, kuin positiivisena ja hyvänä asiana. Toki enemmän on huomiossa ne, jotka kritisoivat turvallisuuteen liittyviä asioita kuin ne, jotka eivät sano mitään, mutta suhtautuvat vakavasti turvallisuuteen.

Tässä asiassa varmasti tietoturvallisuuden koulutusohjelma tulee olemaan merkityksellinen, kun mahdollisia uhkia tuodaan helpommin ymmärrettävästi esille, ei kukaan huolehdi asiasta, jota ei edes tiedä olevan. Uhan vähättely on myös mahdollista. Uhan vähättely on reaktio, jossa tunnustetaan ongelma tai uhka, mutta pyritään vähentämään sen aiheuttamaa stressiä. Uhkaa voidaan vähätellä, jos asiaa ei täysin ymmärrä ja tätä aukkoa ymmärryksessä voidaan paikata kouluttamisella ja tietoisuuskampanjoilla. (Thompson, McGill & Narula 2024).

Vaikka suuri osa työajastani on mennyt tietoturvan hallintajärjestelmän ja sen projektin aihealueissa, olen koittanut suunnitella myös tietoturvallisuuden koulutusohjelmaa. Kun tarkoituksena on kehittää rooliperustainen tietoturvakoulutus, pitää ottaa huomioon myös turvallinen kehittäminen, tietoturvan tuonti koodaamiseen. Tämä aihe nousi esille kuluvalla viikolla. Tähän olemme pohtineet muutamaa eri vaihtoehtoa, joko samankaltainen kuin kaikille muillekin, Workdayssa käytävä jatkuva koulutus taikka erillinen oma koulutuspolkunsa koodaajille, joka olisi jollakin muulla alustalla, kuin Workdayssa. Sovellusten ollessa kriittinen osa liiketoimintaa, yrityksen täytyy ymmärtää senhetkiset uhat ja riskit (Timbó 2023). Yrityksessämme tehdään turvallista kehitystä ja tietoturva on osa koodaamista, mutta siinä aihealueessa korostuu koulutuksen sisältö, että se on mahdollisimman ajantasaista.

Koen, että oma asiantuntijuuteni on kehittynyt tämän syksyn aikana. Tämä nousi erityisesti mieleen torstaina, kun kollegani teki muutoksia poikkeamanhallintaohjeistukseen ja pyysi minulta kommentteja siihen liittyen. Alkukeväästä kun tulin mukaan tähän tietoturvan hallintajärjestelmän projektiin, en kokenut, että olisin riittävän ammattitaitoinen tarkastelemaan muiden tekemiä asioita ja lisäämään niihin omia kommenttejani. Saamalla palautetta tekemästäni työstä on antanut lisää itsevarmuutta omaan tekemiseeni. Jatkuva, kannustava palaute tukee käsitystä siitä, minkälainen ihminen on työntekijänä ja kasvattaa motivaatiota oppia ja kehittyä (Sarkkinen 2017). Saamani palaute on ollut hyvää ja kun saan kommentin, että lisäykseni on ollut hyvä ajatus, on se tuonut varmuutta omaan tekemiseeni enkä koe olevani niin arka sanomaan omia mielipiteitäni ja ajatuksiani. Palautteen ei toki aina pidä olla hyvää, mutta kun se kerrotaan rakentavasti ja hyvillä tarkoitusperillä, on se edesauttanut omaa oppimistani.

4.7 Viikko 7

Viikon tavoitteena on saada ISO27001 sertifiointiauditoinnin ensimmäinen vaihe käytyä lävitse. Osallistumme myös Cyber Security Nordiciin tulevalla viikolla, joten tavoitteena on päästä kuulemaan ajankohtaisia aiheita kyberturvallisuudesta.

Maanantai 28.10

Tällä viikolla perjantaina on ISO27001 sertifiointiauditoinnin ensimmäinen vaihe. Kävimme kollegani kanssa palaverissa lävitse, että keskitymme tämän viikon osalta hallintajärjestelmän

viimeisiin tarkastuksiin, että kaikki linkit sekä muut tekstit ovat ajantasaisia sekä lisäämme pieniä parannuksia. Tällä viikolla normaaleja työpäiviä ei olekaan kovin montaa, joten tavoitteena olikin saada tänään käytyä lävitse kontrollit.

Päivän aikana esihenkilömme laittoi tiimimme Slack kanavalle viestin, että hallinnon toimitilojen osalta fyysisen turvallisuuden tietoisuutta olisi tarve parantaa pienen koulutustilaisuuden muodossa marraskuussa. On ilmennyt, että fyysinen turvallisuus nähdään taakkana, joka hankaloittaa työtehtäviä. Tästä kirjaamme tiketin ja otamme työn alle koulutustilaisuuden järjestämisen.

Tiistai 29.10

Tänään oli ensimmäinen Cyber Security Nordic messupäivä Messukeskuksessa. Tapahtuma on kyberturvallisuuden ammattilaisille suunnattu tapahtuma, jossa paikalla on alan osaajia sekä palveluiden edustajia. Tapahtumassa oli myös esityksiä eri yritysten edustajilta. (Cyber Security Nordic 2024).

Itselleni mieleenpainuvin esitys oli päivän lopussa ja se käsitteli tietoturvatietoisuutta sekä turvallisuuskulttuuria. Tietoturvapolitiikat ja ohjeistukset voidaan nähdä nopeusrajoituksena tyhjällä tiellä. Se nähdään, mutta siinä hetkessä tehdään valinta, noudatetaanko nopeusrajoitusta ja kohteeseen päästään hitaammin vai kun on kiire, painetaanko kaasua tyhjällä tiellä ja päästään kohteeseen nopeammin, nopeusrajoituksesta välittämättä. Asiaa ratkaistaan teillä nopeuskameroilla, jotka pakottavat, ainakin hetkellisesti, noudattamaan nopeusrajoitusta. Samankaltaista valvontaa tai tässä tapauksessa muistutusta kannattaisi harkita turvallisuudenkin kanssa, pidetään asia pinnalla, ettei unohtuisi, että sääntöjä kuuluisi noudattaa, mutta myös mielessä pitäen sen, että ihmisluontoa on hankala muuttaa. Ihminen kun luonnostaan haluaa tehdä asioita helpoimmalla mahdollisella tavalla. (Luoma 2014).

Mielestäni vertauskuva oli erinomainen, itse pidän esimerkeistä sekä koen oppivani paremmin niiden kautta. Viestinnän merkitys tietoturvatietoisuudessa sekä turvallisuuskulttuurissa on erittäin tärkeä, pidetään turvallisuusasiat pinnalla, jotta ne eivät unohtuisi. Tällä hetkellä yrityksessämme olisi parantamisen varaa tietoturvatietoisuuden kanssa, sitä ei markkinoida tai viestitä niin paljoa, kuin varmasti olisi tarvetta.

Keskiviikko 30.10

Tänään oli lyhyempi messupäivä ja keskityimme enemmän esitysten kuuntelemiseen, kuin messualueella katselemiseen. Huomasin, että tämänkaltaisessa tilaisuudessa pitäisi osata verkostoitua ja käydä keskustelemassa eri ihmisten kanssa. Tämä on itselleni hyvin vaikeaa, koska en koe osaavani aloittaa sellaista keskustelua ihmisten kanssa, joita en tunne. Tämä on

ehdottomasti sellainen aihealue, jossa minun tarvitsee petrata, mutta se varmasti helpottaa, kun on enemmän työvuosia alla tällä alalla.

Torstai 31.10

Huomenna on tietoturvan hallintajärjestelmän sertifointiauditoinnin ensimmäinen vaihe, joten kävimme tänään läpi hallintajärjestelmää yhdessä kollegani ja esihenkilöni kanssa. Keskustelimme yleisesti auditointiprosessista sekä siitä, miten asiat esitellään auditoijille. Minä ja esihenkilöni käymme läpi standardin lisäys A:n mukaiset kontrollit ja kollegani käy lävitse standardin klausuulit. Saimme palaverin aikana hyvin käytyä läpi seuraavan päivän kulun.

Pidimme myös viikkopalaverin, joka jouduttiin siirtämään tälle päivälle, koska olimme tiistaina Cyber Security Nordicissa.

Olin myös sopinut tälle päivälle palaverin liittyen fyysisen turvallisuuden aihealueeseen uudelle työntekijällemme, joka tulee ottamaan vastuulleen Digitaalisten palveluiden toimistot. Olin iloinen, että läpikäynnissä asiat otettiin vakavasti ja myös hänelle tuli mieleen asioita, mihin hän pystyy myös kiinnittämään huomiota. Tämä toi lisää varmistusta siihen, että aktiivisella tiedottamisella varmasti saamme vaikutettua turvallisuuskulttuuriin yleisesti.

Sain myös Slack viestin tietoturvakyselystä, jonka hoidin keväällä. Kyselyyn tarvittiin lisäselvitystä. Kerroin ottavani kyselyn ensi viikolla työn alle, sillä koko perjantai menisi auditoinnissa.

Perjantai 1.11

Tänään oli tietoturvan hallintajärjestelmän sertifiointiauditoinnin ensimmäinen vaihe. Ensimmäisessä vaiheessa katsotaan, olemmeko sillä tasolla, että voimme siirtyä toiseen vaiheeseen. Kävimme aloituspalaverin, jossa esittelykierros ja keskustelimme yleisesti prosessista. Tässä auditoinnissa kirjataan ylös huolenaiheet, jotka eivät suoraan ole poikkeamia mutta voivat auditoinnin toisessa vaiheessa nousta esiin poikkeamina.

Juuri ennen auditoinnin alkamista, aloituspalaverin aikana sain sähköpostin tietoturvan sekä tietosuojan koulutusohjelman kumppaniltamme, että joudumme perumaan seuraavan maanantain koulutussuunnittelupalaverin. En kerennyt tähän paneutua, sillä koko loppupäivä meni auditoinnin parissa.

Auditointi oli hyvin pitkälti sitä, että kävimme kohta kohdalta lävitse toteutusta ja auditoija esitti tarkentavia kysymyksiä. Olin itse jännittänyt sitä, osaanko riittävän tarkasti kertoa aihealueista, mutta kun kävimme keskustelua, sain omasta mielestäni todella hyvin tuotua asiat ilmi. Ruokatauon aikana esihenkilömme kehui toimintaani auditoinnissa tiimimme yhteisellä Slack kanavalla, mikä toi lisää varmuutta omaan osaamiseeni. Olin erittäin iloinen, että

monen kuukauden työpanos on tuottanut sen tuloksen, että omaa tietämystäni ja osaamistani kehuttiin, hyvinkin vuolaasti.

Päivän lopuksi pidimme yhteisen loppupalaverin ja auditoijat nostivat havaitsemansa huolenaiheet. Aiheet olivat odotettuja, mikään niistä ei yllättänyt. Saamme auditoijilta loppuraportin, jonka pohjalta lähdemme toteuttamaan muutoksia ennen auditoinnin seuraavaa vaihetta.

Viikkoanalyysi 7

Tämä viikko oli hyvin hektinen ja paljon tapahtui viikon aikana. Itselleni uutta on se, että työnantaja tukee työntekijöiden osaamisen kehittämistä, esimerkkinä kuluvalla viikolla ollut Cyber Security Nordic. Tätä ei ole aikaisemmassa työelämässäni ollut, ja tuntuu hyvinkin motivoivalta, että työnantaja näkee työntekijät voimavarana yrityksessä ja tukee kehittymistä ja oppimista. Jatkuva kehittyminen auttaa innovoimaan uutta, tarkastelemaan asioita toisesta näkökulmasta (Rumage 2024). Edellisessä työelämässäni sääntöjen ja ohjeistuksien noudattamista valvottiin sekä myös sanktioitiin, jos oli toiminut ohjeiden vastaisesti ja tämä ajattelutapa on itselläni edelleen hyvin pinttyneesti. Tiistain esityksen jälkeen pohdin, että varmasti motivoinnin kautta saa parempia tuloksia kuin sillä, että henkilöstö pelotellaan noudattamaan ohjeistuksia. Parempi olisi saada henkilöstö ymmärtämään ohjeistusten taustat ja ymmärryksen kautta noudattamaan annettuja ohjeistuksia.

Perjantaina saamani sähköposti tietoturvan sekä tietosuojan koulutusohjelman kumppanilta, että joudumme perumaan maanantaille sopimamme koulutussuunnittelun palaverin, turhautti kovasti. Perumisen syynä oli sopimustekniset asiat. Tätä koulutusprojektia on suunniteltu alustavasti jo helmikuussa, ja vieläkään marraskuussa emme ole saaneet konkreettisesti asiaa edistettyä. Projekti on todella iso ja tämän kokoluokan koulutusuudistusta ei ole yrityksessämme tehty, mutta aihe on kuitenkin tärkeä ja projekti on yksi niistä asioista, joiden takia minut on yritykseen palkattu. En osannut lainkaan varautua siihen, että sopimukselliset asiat eivät olleetkaan kunnossa ja jouduimme perumaan. Perjantaina kerkesin kertoa tämän esihenkilölleni, hän oli myös saanut aiheesta ilmoituksen. Itselleni tuli sellainen tunne, että projektia ei edes haluttaisi edistää, esihenkilöni vakuutti, että kyllä sitä tullaan edistämään. Tulevalla viikolla keskustelua varmasti tarvitsee jatkaa, että kuinka voimme edetä asian suhteen, jos sopimusteknisiin asioihin emme saa selvyyttä. Elämme kuitenkin vuoden loppupuolta ja joulukuussa suurin osa kehitystyöstä lakkaa joulutauon vuoksi, voi hyvin olla, että vasta tammikuun puolella pääsemme jatkamaan projektia täysimittaisesti. En tietenkään tiedä, mitkä asiat ovat vaikuttaneet siihen, että edistäminen jouduttiin keskeyttämään, eikä rooliini kuulukaan kaikkea tietää.

Perjantain auditointi tuotti paljon onnistumisen tunteita, oli helpottavaa kuulla, että tietoturvan hallintajärjestelmä on riittävän kypsä, jotta voimme edetä auditoinnin seuraavaan

vaiheeseen. Toisessa vaiheessa pyydämme mukaan myös muita asiantuntijoita, jotta auditointi olisi mahdollisimman kokonaisvaltainen.

Viikko piti sisällään paljon onnistumisia mutta myös hieman pettymystä, mutta sellaista asiantuntijatyö on.

4.8 Viikko 8

Tämän viikon tavoitteena on selvittää, missä mennään tietoturvan ja tietosuojan koulutusohjelman kanssa.

Maanantai 4.11

Aloitin päivän käymällä lävitse materiaalia tietoturvakyselystä, jonka olin saanut tehtyä keväällä. Asiakas oli halunnut lisäselvitystä antamiimme vastauksiin. Olin edeltävällä viikolla pyytänyt, että esihenkilöni katsoisi kyselyä kanssani lävitse ja käymme huomenna asiasta palaverin, mutta kävin läpi kohtia ja pohdin, kuinka kirjaisimme lisäselvitykset.

Pidimme myös kollegani kanssa maanantaipalaverin. Kävimme lävitse perjantain auditointia, siitä jääneitä kysymyksiä ja ajatuksia. Kerroin, että olin jännittänyt auditointia hurjasti ja olin kovin tyytyväinen, kun sain kaiken kerrottua. Pohdimme myös yhdessä, kuinka etenisimme tietoturvan koulutusohjelman kanssa nyt kun se peruttiin edellisellä viikolla. Kollegani heitti ajatuksen ilmoille, että meidän varmasti tarvitsisi tehdä varasuunnitelma, kuinka voisimme edistää asiaa, vaikka projekti kumppanin kanssa olisi hetkellisesti katkolla. Kirjasin projektin Jira-tiketille tämänhetkisen tilanteen sekä lisäsin alitiketin varasuunnitelmalle. Koulutuspuolta olisi tärkeä edistää, sillä koulutuksiin osallistuminen on yhtenä suorituskykymittarina tietoturvan hallintajärjestelmässä sekä yksi huolenaiheista auditoinnissa.

Loppupäivän jatkoin tietoturvakyselyn parissa.

Tiistai 5.11

Pidimme esihenkilöni kanssa palaverin tietoturvakyselystä, johon toivottiin lisäselvitystä edellisellä viikolla. Tietoturvakysely on mahdollisen asiakkaan lähettämä, samankaltainen kuin listaus tietoturvavaatimuksista, joita aikaisemmin veimme oman yrityksemme hankintaprosessiin mukaan. Saimme keskusteltua lävitse, kuinka sitä kannattaisi lähestyä.

Viikkopalaverissa saimme tietää, että koulutusprojektista on haluttu lisää tietoa ylempien tahojen puolesta ja tulevana perjantaina asiasta käydään keskusteluja. Toimme esihenkilöllemme tietoon, että aloitamme kollegani kanssa varasuunnitelman teon, jotta saisimme jotenkin edistettyä koulutuspuolta ennen ensi vuotta. Henkilöstön kouluttaminen on kirjattu yhdeksi toimenpiteeksi vastuullisuusraporttiin, joten koko projektia ei voida hylätä.

Keskustelimme myös, voiko tulla tilanne, jossa koulutus halutaan toteuttaa itse. Se on epätodennäköistä, että siihen mentäisiin, mutta mahdollista. Mutta itse koko koulutusuudistuksen tekeminen ilman kumppania nykyisillä resursseillamme on liki mahdotonta, edes ensi vuoden aikana. Pidimme kesällä palaverin, jossa oli mukana ylempien tahojen edustajia ja kyseisessä palaverissa koulutusuudistusta pidettiin hyvinkin tarpeellisena ja projektille annettiin vihreää valoa. Itseäni turhauttaa tämänkaltainen edestakainen asioiden pallotteleminen, mutta itselläni ei ole kokemusta korporaatiomaailman hankaluuksista.

Keskiviikko 6.11

Aloittelin tänään alustavaa varasuunnitelmaa koulutusprojektille. Alkuperäisessä suunnitelmassa kumppaniyrityksen kanssa, oli tarkoituksena lähettää henkilöstölle kysely liittyen tietoturvatietoisuuteen. Pohdimme maanantaina kollegani kanssa, että se on varmasti hyödyllinen aloituskohta myös meillä, jotta saisimme proaktiivisesti vietyä asiaa eteenpäin. Pohdin, mitä kyselyyn voisi tulla, jotta saisimme henkilöstön mielipiteet mahdollisimman hyvin kerättyä.

Päivän lopuksi hankintatiimin edustaja lähestyi sähköpostitse ja tiedusteli, voisimmeko antaa tietoturvan mielipidettä järjestelmään, jota olemme hankkimassa. Vastaus haluttiin vielä saman päivän aikana. Tiedustelin kollegaltani, lukiko hän kyseistä sähköpostia, hän olikin ottanut asian jo työn alle.

Torstai 7.11

Kuten aiemmin jo todettu, meillä on tapana pitää kahden viikon välein esihenkilöni kanssa palaveri ja keskustella viimeisen kahden viikon ajan tapahtumista ja palaverin aikana on myös mahdollista nostaa mahdollisia ongelmakohtia esiin, joko työntekijän tai esihenkilön puolelta. Näitä palavereja on jouduttu perumaan syksyn aikana aika paljon, ja tänään oli ensimmäinen kerta kahteen kuukauteen, kun kerkesimme pitää juttutuokion. Sain paljon positiivista palautetta jälleen viimeperjantaisesta auditoinnista, joka edelleen on yksi syksyn ammatillisista kohokohdista itselläni. Sain myös nostettua itseäni vaivaavia asioita esille ja kävimme niistä myös keskustelua.

Meillä on tarkoituksena kollegani kanssa tehdä pienimuotoinen koulutus fyysisestä turvallisuudesta toiselle tiimille, ja tätä varten tiedustelin sen tiimin henkilöltä, voisinko nähdä heidän olemassa olevat ohjeistuksensa liittyen aiheeseen, jotta meidän koulutuksemme sisältö olisi linjassa nykyisten ohjeistusten kanssa. Hän sanoi selvittävänsä ja palaavansa aiheeseen.

Perjantai 8.11

Tänään saimme tiedon, että tietoturvan koulutusprojekti on hyväksytty ylemmillä tahoilla ja pääsemme jatkamaan sen toteutusta, tosin alkuperäisestä aikataulusta myöhässä.

Esihenkilömme käy tulevalla viikolla kumppaniyrityksen kanssa asiat läpi ja toivottavasti pääsisimme tämän kuun aikana konkreettisesti tekemään asian eteen jotakin.

Viikkoanalyysi 8

Saimme viikon lopuksi tiedon, että voimme jatkaa tietoturvan sekä tietosuojan koulutusohjelmaa, vaikkakin projektin suunniteltu aikataulu ei pitänyt. Itseäni turhautti kovasti projektin viivästyminen ja kerroinkin tästä esihenkilölleni, joka ymmärsi turhautumisen. Olen keskustellut koulutusprojektista kollegani kanssa, joka mielestäni hyvin sanoikin, että isoilla projekteilla on tapana viivästyä suunnitellusta aikataulusta, ja se kannattaa ottaa huomioon suunnitteluvaiheessa. Itselleni tämä on ollut hyvä muistutus, en ymmärtänyt, että tämänkaltaisessa organisaatiossa asiat voivat viivästyä, kun suunnitelmien täytyy kulkea muualtakin, kuin oman tiimimme esihenkilön kautta. Alkuperäinen suunnitelma ei ehkä ollut epäonnistunut, mutta enemmän epärealistinen ja tästä osaan jatkossa ottaa opikseni ja suunnitella paremmin.

Viikolla hankintatiimi lähestyi tiedustelulla järjestelmästä, johon haluttiin tietoturvatiimin näkemystä, onko se turvallinen. Vaikka vastaukset haluttiin aika tiukalla aikataululla, päivän loppuun mennessä, olin tyytyväinen, että viimekuussa käymämme palaveri on edesauttanut sitä, että matalalla kynnyksellä otetaan yhteyttä tietoturvatiimiin ja tiedustellaan meidän näkemystämme. Ollessamme lokakuun lopussa Cyber Security Nordicissa, kuuntelimme esityksen, jossa korostettiin turvallisuuden olevan tiimilaji. Turvallisuutta ei voi rakentaa yksin, vaan siihen tarvitaan useiden tiimien yhteistyötä. Yhdellä tiimillä ei voi olla osaamista kaikesta, vaan tarvitaan myös muiden ammattitaitoa tuoda ne oman työnsä osa-alueet esiin ja yhdessä suunnitella turvallisempaa kulttuuria. (Kidman 2024). Tässä koen, että olemme onnistuneet ja jatkamme yhteistyön rakentamista myös muidenkin tiimien kanssa, kuten olemme jo suunnittelemassa fyysisen turvallisuuden koulutusta toiselle tiimille. Siitä koulutuksesta varmasti saamme aluksi risuja, sillä olemme huomanneet sen tiimin sisällä olevan vastustusta, koska turvallisuuteen liittyvät asiat koetaan hankaloittavan tarpeettomasti työtehtävien hoitamista. Mutta tiedämme heidän esihenkilönsä olevan sitoutunut turvallisuuden edistämiseen ja ylläpitämiseen, joten se varmasti toimii myös meidän eduksemme. Johdon asenteella on iso vaikutus henkilöstönkin suhtautumisessa turvallisuuskulttuuriin (URM 2022).

5 Yhteenveto ja pohdinta

Päiväkirjamuotoisessa opinnäytetyössä kirjasin kahdeksan viikon ajan työpäivieni sisältöä sekä analysoin mennyttä viikkoa. Opinnäytetyön alussa itselläni oli kuvitelma mitkä ovat omat kehityskohteeni, mutta työn edetessä ymmärsin, että viikoittainen analysointi sekä työviikon asioiden äärelle pysähtyminen avasi paljon enemmän omista kehityskohteistani, mutta myös

vahvuuksistani. Itselleni arvokas havainto on ollut se, etten tiedä mitä en tiedä. Tarkoittaen, etten ole edes tunnistanut kaikkea mitä en tiedä, jotta voisin kysyä niistä.

5.1 Tavoitteiden täyttyminen

Opinnäytetyön tavoitteeksi oli havainnoida ison tietoturvakoulutusprojektin uudistamistyöhön liittyviä seikkoja, kuinka iso projekti lähtee käyntiin kumppaniyrityksen kanssa sekä kuvata tietoturvan hallintajärjestelmän kehitystyötä kohti ISO27001 sertifioinnin ensimmäistä vaihetta. Tietoturvan sekä tietosuojan koulutusohjelman osalta tavoitteeseen ei päästy kahdesta syystä. Ensimmäisenä syynä oli tietoturvan hallintajärjestelmän sertifiointiprosessi, joka on laaja ja paljon työtä vaativa kokonaisuus ja se vei lokakuussa suurimman osan työajastani, joten emme voineet tehdä kahta isoa projektia samanaikaisesti. Itse luulin, että se olisi voinut olla mahdollista, mutta en myöskään ollut koskaan ollut osana sertifiointiprosessia, joten en pystynyt realistisesti kuvittelemaan sitä työmäärää, joten loppujen lopuksi olin tyytyväinen, kun ensimmäisen yhteisen palaverin jälkeen kumppaniyrityksen kanssa sovimme, että jatkamme marraskuussa. Toisena syynä oli sopimustekniset hankaluudet, jotka tulivat ilmi marraskuussa. Oli erittäin turhauttavaa kuulla, ettemme pystyneet marraskuun alussa pysymään aikataulussa, vaan jouduimme perumaan seuraavan tapaamisen. Turhautuminen johtui siitä, että tietoturvan sekä tietosuojan koulutusohjelma olisi ollut minun projektinani, vaikka mukana tietysti olisi ollut kumppaniyritys, muita asiantuntijoita sekä kollegani tiimistäni. Kyseessä olisi ollut ensimmäinen projekti, jota koordinoin ja olisin halunnut päästä tekemään ja osoittamaan itselleni, olevani kykenevä tähän työhön.

Tietoturvan hallintajärjestelmän kehitys kohti sisäistä auditointia ja päiväkirjaraportoinnin toiseksi viimeisellä viikolla läpikäyty sertifiointiauditoinnin ensimmäinen vaihe, oli onnistunut. Vaikka on vielä paljon asioita, joita hallintajärjestelmän puitteissa tarvitsee kehittää, onnistuimme tavoitteissa ja hallintajärjestelmä on riittävän kypsä sertifiointiauditoinnin toiseen vaiheeseen.

Opinnäytetyössä henkilökohtaisena tavoitteena oli seurata omien asiantuntijataitojen kehittymistä raportointijakson aikana. Viikkoanalyysien aikana, pohdin paljon omaa osaamistani ja miksi koitan kovasti itselleni todistaa olevani sopiva työhön, vaikka saamani palaute osoittaa, että teen työni hyvin. Osittain varmasti sen vuoksi, että edellisessä ammatissani olin ollut pitkään ja siinä työssä en tarvinnut apua keneltäkään, toisin kuin nyt. Olen ollut asiantuntijatyössä yli vuoden, ja kaipaan vielä monissa asioissa apua kollegoilta sekä esihenkilöltäni. Esihenkilöni on sanonut minulle, että itselleen täytyy antaa armoa eikä oppiminen koskaan lopu, tämä on ollut erinomainen neuvo. Viikkoanalyyseissä olen joutunut pohtimaan viikolla tapahtuneita asioita ja se on näyttänyt, että lyhyeenkin viikkoon voi mahtua paljon onnistumisia. Opinnäytetyön tekemisen aikana osaamiseni on kehittynyt, sillä olen pystynyt havaitsemaan omia kehityskohteitani paremmin sekä pohtimaan asioita useasta eri näkökulmasta.

5.2 Jatkokehitys

Opinnäytetyötä tehdessäni laajensin omaa tietoperustaani ja tutustuin alan kirjallisuuteen viikoittain. Ymmärsin, että vaikka asia ei olisi täysin verrannollinen omaan työnkuvaani, voisin pohtia, saisinko sovellettua saamaani tietoa nykyiseen työhön. Kirjallisuudesta saamani näkökulmat tietoturvan kouluttamiseen sekä kouluttamiseen yleisesti, on avannut omaa näkökantaani valtavasti. Olen ymmärtänyt, että kouluttamisessa ei pidä olla vain yhtä mallia, vaan suhteuttaa koulutusta yleisön mukaan sekä sisällön hiominen sellaiseksi, että se palvelisi myös työsuhteen ulkopuolella, tarjoten tietoa myös muihin elämän osa-alueisiin.

Olen oppinut paljon riskienhallinnasta ja kuinka se on sidoksissa tietoturvaan. Työ tietoturvan sekä tietosuojan koulutusohjelman parissa jatkuu, täysipainoisesti todennäköisesti tammikuussa 2025. Kyseisen projektin kannalta olisi hyvä dokumentoida siihen liittyvät riskit, joita tuli myös ilmi opinnäytetyön aikana.

Opinnäytetyön alussa pohdin omaa teknistä osaamistani, joka ei ole niin hyvää kuin haluaisin sen olevan. Tietoturvan hallintajärjestelmän ensimmäisen vaiheen sertifioinnissa, osasin kertoa ylätasolla teknisemmistäkin asioista, joka oli osoitus itselleni, että ymmärrän enemmän mitä olen itse kuvitellut. Tekninen tietoturva on laaja osa-alue ja täysin en varmasti koskaan pääse siihen sisälle, haluaisin silti osata enemmän ja tässä aion itseäni kehittää.

Työstäni saama palaute on ollut hyvä osoitus, että teen työni hyvin ja laadukkaasti. Olen pitkään noudattanut ajatusmallia, että kuuntelemalla oppii enemmän kuin puhumalla, mutta opinnäytetyön aikana havaitsin, että olisi itselleni hyödyllisempää tuoda enemmän omia ajatuksiani esille ja joskus mennä oman mukavuusalueensa ulkopuolelle. Ei ole heikkoutta myöntää, että jotakin asiaa ei tiedä, vaan se on osoitus siitä, että vaikka ei tiedä, on halukas oppimaan.

Lähteet

Painetut

Gardner, B. & Thomas, V. 2014. Building an Information Security Awareness Program. USA: Elsevier.

Heikkinen, H. & Kaukko, M. 2023. Toimintatutkimus – Käytännön opas. Tampere: Vastapaino.

ISO/IEC27001:2022. 2023. Suomen Standardisoimisliitto SFS.

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Kämppi, P. & Talala, T. 2023. Yrityksen riskienhallinta. 3. painos. Aalto University Executive Education.

Merriam, B. S. & Bierema, L. 2014. Adult learning – Linking theory and practice. USA: Jossey-Bass

Mäntyneva, M. 2016. Hallittu projekti. Viro: Printon.

Mönkkönen, K. & Roos, S. 2010. Työyhteisötaidot. 2. painos. Helsinki: Unipress

Taylor, A., Alexander, D., Finch, A. & Sutton, D. 2013. Information Security Management Principles. 2. painos. Britannia: BSC Learning and Development.

Sähköiset

Ahtela, J. 2016. Työaika, tietotyö ja tulevaisuus: esimerkkinä ohjelmistoala. Työ-ja elinkeinoministeriön julkaisuja 34/2016. Viitattu 5.10.2024. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75601/TEMrap_34_2016_netti.pdf;jsessionid=90F5E92276D3D883D8CABD5AE98373B4?sequence=1

Cyber Security Nordic. 2024. Viitattu 29.10.2024. https://cybersecuritynordic.messukeskus.com/

ENISA Threat Landscape 2024. The European Union Agency for Cybersecurity ENISA. Viitattu 23.9.2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 NIS2 direktiivi. Viitattu 8.10.2024 sekä 25.10. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FIN&toc=OJ%3AL%3A2022%3A333%3AFULL

Herath, T. & Rao. H.R. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 47 (2), 154-165. Viitattu 12.11.2024. https://www.sciencedirect.com/science/article/abs/pii/S0167923609000530?via%3Dihub

Kosling, K. 2024. What is an Information Security Management System (ISMS)?. IT Governance. Viitattu 1.12.2024. https://www.itgovernanceusa.com/blog/what-exactly-is-an-information-security-management-system-isms-2

Merrit, M., Hansche, S., Ellis, B., Sanchez-Cherry, K., Snyder & J., Walden, D. 2024. Building a Cybersecurity and Privacy Learning program, NIST SP 800-50r1. National Institute of Standards and Technology. Viitattu 21.9.2024. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf

National Institute of Standards and Technology 2011. Managing Information Security Risk. NIST Special Publication 800-39. Viitattu 18.10.2024. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf

National Institute of Standards and Technology 2024. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. Viitattu 3.10.2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Rahikainen, E.S., Rautiainen, A., Tiensuu, I., Paavola, J-M., Ulander, M., Sjöblom, M., af Hällström, C & Jousilahti, J. 2024. Osaamisen tunnistamisen hyvät käytännöt. Tietoyhteiskunnan kehittämiskeskus TIEKE ry. Viitattu 13.10.2024. https://tieke.fi/wp-content/uploads/2024/03/Osaamisen-tunnistamisen-hyva%CC%88tka%CC%88yta%CC%88nno%CC%88t_loppuraportti.pdf

Rumage, J. 2024. What Is Continuous Learning and Why Is It Important?. BuiltIn. Viitattu 3.11.2024. https://builtin.com/articles/continuous-learning

Sarkkinen, M. 2017. Palaute on työelämän pienin suuri asia. Työterveyslaitos. Viitattu 26.10.2024. https://www.ttl.fi/tyopiste/palaute-on-tyoelaman-pienin-suuri-asia

Thompson, N., McGill, T. & Narula, N. 2024. "No point worrying" – The role of threat devaluation in information security behavior. Computers and Security 143. Viitattu 12.11.2024. https://www.sciencedirect.com/science/article/pii/S0167404824001998?via%3Dihub

Timbó, R. 2023. Security in Software Development. Revelo. Viitattu 27.10.2024. https://www.revelo.com/blog/security-in-software-development

Traficom, 2024. Tärkeää tietoa Euroopan Unionin Kyberturvallisuusdirektiivistä. Viitattu 30.9.2024. Https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tarkeaa-tietoa-euroopan-unionin-kyberturvallisuusdirektiivista#67853-0

URM Consulting. 2022. How do you gain top management commitment?. Viitattu 10.11.2024. https://www.urmconsulting.com/blog/how-do-you-gain-top-management-commitment

Valtioneuvosto 2024. Kyberturvallisuusdirektiivin kansallinen täytäntöönpano etenee: Hallitus esittää uutta kyberturvallisuuslakia. Viitattu 8.10.2024. https://valtioneuvosto.fi/-//1410829/kyberturvallisuusdirektiivin-kansallinen-taytantoonpano-etenee-hallitus-esittaa-uutta-kyberturvallisuuslakia

Ørngreen, R., & Levinsen, K. T. 2017. Workshops as a Research Methodology. Electronic Journal of E-Learning, 15(1), 70–81. Viitattu 16.9.2024. https://vbn.aau.dk/ws/portalfiles/portal/257686207/_rngreen_Levinsen_Workshop_as_a_Research_methodology_ejel_volume15_issue1_article569.pdf

Julkaisemattomat

Kidman, Å. 2024. What is needed to ensure a secure future and why – security as a team sport!. Esitys. Cyber Security Nordic. Helsinki.

Luoma, I. 2024. Beyond Awareness: Transforming Your Organization’s Security Culture. Esitys. Cyber Security Nordic. Helsinki.

Kuviot