Teknisten haavoittuvuuksien hallinta terveydenhuollon organisaatiossa

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus
syksy, 2023

Tuomo Oksanen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutus Tiivistelmä

Tekijä Tuomo Oksanen Vuosi 2023

Työn nimi Teknisten haavoittuvuuksien hallinta terveydenhuollon organisaatiossa

Ohjaaja Ismo Turve

TIIVISTELMÄ

Opinnäytetyön tutkimuksen tarkoituksena oli selvittää, kuinka saadaan tunnistettua terveydenhuollon organisaation tietojärjestelmissä olevat tekniset haavoittuvuudet sekä miten havaittuihin haavoittuvuuksiin reagoidaan ja kuinka ne hoidetaan asianmukaisesti. Opinnäytetyön toimeksiantaja oli Etelä-Pohjanmaan hyvinvointialue.

Opinnäytetyöni teoreettinen viitekehys koostuu suurimmalta osin ISO 27001 Tietoturvallisuuden hallintajärjestelmät ja ISO 27002 Tietoturvallisuuden hallintakeinot -standardien ohjeistuksista ja määrityksistä. Opinnäytetyö toteutettiin toiminnallisena. Tutkimusaineisto kerättiin työpaikalla toteutetuilla ryhmäkeskustelutyyppisillä usealla työpajalla, joissa hyödynnettiin työmenetelminä mm. ryhmäkeskustelua ja visualisointia. Aineiston muodostamisessa ja analysoinnissa hyödynnettiin dokumenttianalyysiä.

Johtopäätöksenä voidaankin todeta, että tutkimuskysymyksiin vastaaminen onnistui kaiken kaikkiaan hyvin. Työpajojen tuotoksena saimme luotua organisaatiolle soveltuvan (liite 2) teknisten haavoittuvuuksien hallintaprosessin. Tuotos mukailee osittain organisaatiossa jo käytössä olevia prosesseja ja toimintamalleja. Organisaatiosta saaduissa palautteissa todettiin työpajojen olleen hyvä tapa prosessin suunnittelussa. Työpajojen toteuttamista pidettiin tärkeänä, joissa oli alustus ja johdatus teorialla aiheeseen, joka auttoi osallistujia saamaan tietoa työpajoissa tapahtuvaan prosessin suunnittelun ja toteutuksen tueksi. Organisaatio piti aihetta tärkeänä ja oli tyytyväinen kehittämistyön tuloksiin.

Avainsanat tietoturva, kyberturva, tekninen haavoittuvuus

Sivut 62 sivua ja liitteitä 2 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology Abstract

Author Tuomo Oksanen Year 2023

Subject Management of technical vulnerabilities in the health care organization

Supervisor Ismo Turve

ABSTRACT

The purpose of the thesis was to sort out how to identify technical vulnerabilities in healthcare organization's information systems and how to respond identified vulnerabilities and how they are handled in the appropriate manner. The thesis was commissioned by South Ostrobothnia wellbeing services county.

The theoretical framework of this thesis consists mostly of ISO 27001 Information management systems and ISO 27002 Information controls standards related instructions and definitions. The thesis was conducted as functional. The research materials were collected using group type discussion workshops, where utilized work methods were group discussions and visualization. Creating and analyzing the thesis materials were analyzed using document analysis method.

Overall, the research questions were all well answered. As a result of the workshops, were succeeded to create the technical vulnerabilities management process in appendix 2, which is suitable to organization. As a word suitable means that the product partly adapts processes and operations models that organization already have in use. The feedback from the organization was that workshops were a good way to plan the process and the way that workshops were implemented, theory at first in the meetings, because the participants managed to get the necessary information to go ahead of the planning and execution of the process. The organization understood the importance of this topic and were pleased with the results of the development.

Keywords information security, cyber security, technical vulnerability

Pages 56 pages and appendices 2 pages

Sanasto

CVE	Common Vulnerabilities and Exposures, haavoittuvuuksien julkinen yksilöintimalli
CVSS	Common Vulnerability Scoring System, FIRST:in avoin viitekehyksen menettely haavoittuvuuksien vakavuusluokitteluun
DVM	Defender Vulnerability Management, Microsoftin riskipohjainen automatisoitu haavoittuvuuksien tunnistusjärjestelmä
ISMS	Information Security Management System, Tietoturvallisuuden hallintajärjestelmä
ISO	International Organization for Standardization, kansainvälinen standardointijärjestö
IEC	International Electrotechnical Commission, kansainvälinen sähköalan standardointijärjestö
IOC	Indicator of Compromise, digitaalinen jälki, joka kertoo päätelaitteen tai tietoverkon olleen tietomurron kohteena
PTJ	Potilastietojärjestelmä, sosiaali- tai terveydenhuollon järjestelmä, jolla ylläpidetään ja käsitellään potilas- tai asiakastietoja.
Assets	Omaisuuserä, joka viittaa kaikkeen organisaation omistamaan, joita hyödynnetään yrityksen toimintoihin (esim. ohjelmistot, järjestelmät, tietokannat, laitteet, tietotekniset laitteet, henkilöstö, tilat).

Sisällys

Kuvat, kuviot ja taulukot

Liitteet

1 Johdanto

Erityisesti tänä päivänä haitallisten kybertoimien lisääntyessä tietoverkoissa, tietoturvallisuuden uhkat korostuvat organisaatioiden päivittäisessä toiminnassa. Tietojärjestelmien ja laitteiden heikkoudet eli haavoittuvuudet voivat pahimmillaan mahdollistaa haitallisille kybertoimijoille pääsyn organisaation tärkeään tieto-omaisuuteen ja pahimmillaan vaarantaa koko organisaation toiminnan. Mahdollinen tietomurto voi lisäksi aiheuttaa suuren mainehaitan ja epäluottamusta kansalaisten sekä yhteistyökumppanien parissa, kuten kävi vuonna 2020 paljastuneessa Vastaamon laajassa tietomurrossa.

Teknisten haavoittuvuuksien ajantasaisella, suunnitelmallisella ja järjestelmällisellä hallinnalla voidaan osaltaan auttaa organisaatiota suojautumaan näitä uhkia vastaan sekä turvata päivittäinen toiminta. Haavoittuvuuksien hallinnalla tarkoitetaan haavoittuvuuksien systemaattista tunnistamista, arviointia ja haavoittuvuuksien poistamista organisaation tietoteknisestä ympäristöstä esim. paikkaamalla haavoittuvuus tuoreella ohjelmistoversiolla, jossa haavoittuvuus on korjattu. Teknisten haavoittuvuuksien hallinnassa lisäksi määritetään toimet, jotka voidaan tehdä haavoittuvuuksien haitallisten vaikutuksen minimoimiseksi eli lievennetään haavoittuvuuden hyväksikäytön uhkaa.

Tämä toiminnallisen tutkimuksen menetelmän mukainen opinnäytetyö käsittelee teknisten haavoittuvuuksien hallintaa organisaatiossa ISO 27001 -standardin mukaisesti. Toimeksiantona sovittiin, että toteutan organisaatioon teknisten haavoittuvuuksien hallintaprosessin ISO 27001 Tietoturvallisuuden hallintajärjestelmät standardin mukaisena. Työssä tutkitaan tietoturvallisuuden ISO 27000 tuoteperheen standardeja, jotka esittelevät mm. tietoturvallisuuden hallintajärjestelmien vaatimukset, hallintakeinot ja riskien hallintaa. Lisäksi työssä tutkitaan ja pyritään hyödyntämään olemassa olevia haavoittuvuuksien hallintaprosesseja ja käytänteitä. Työssä tuodaan esiin tietoturvallisuuteen ja haavoittuvuuksien hallintaan liittyvää teoriaa, termejä sekä käsitteitä. Työ rajataan ISO 27001 -standardin liite A luvun 8.8 mukaan teknisten haavoittuvuuksien hallintaan. Opinnäytetyön tuloksena syntyy organisaatiolla teknisten haavoittuvuuksien hallintaprosessi, jota voidaan systemaattisesti ja toistuvasti toteuttaa.

Työssäni pyritään vastaamaan seuraaviin kysymyksiin:

- Kuinka teknisten haavoittuvuuksien hallinta toteutetaan ISO 27001 -standardin mukaisesti?
- Millä työtavoilla saamme toteutettua ISO 27001 -standardin mukaisen teknisten haavoittuvuuksien hallintaprosessin?
- Miten saamme toteutettua organisaatiolle toimivan ISO 27001 -standardin mukaisen teknisten haavoittuvuuksien hallintaprosessin?

2 Tietoturvallisuus

Kirjassaan Kimmo Rousku kuvaa, että puhuessamme tietoturvasta, sillä tarkoitetaan tiedon saatavuuden, eheyden sekä luottamuksellisuuden turvaamista. Saatavuudella tarkoitetaan, että tietoa tarvitsevien henkilöiden tulee saada tiedot tietojärjestelmästä tai palvelusta sovitun SLA:n (Service level agreement) vasteajan puitteissa. Tänä päivänä digitaalisten palveluiden oletetaan olevan käytössä käytännössä koko ajan eli palveluiden tulisi olla saatavilla melkein 100 % vasteella. Saatavuuteen vaikuttavat haitallisesti erilaiset viiveet tietoverkoissa, kuten kyberhyökkäys DoS (Denial of Service). DoS eli palvelunestohyökkäys hidastaa esim. kohteena olevaa verkkosivujen tarjoamaa palvelinta, koska palvelimelle johdetaan eri puolilta niin suuri määrä tietoliikennettä, että palveluista tulee käytännössä toimimattomia ja se näkyy suoraan käyttäjille sivuston toimimattomuutena. (Rousku, 2014, ss. 47–50)

Luottamuksellisuudella tarkoitetaan, että salattuihin ja tietoluokiteltuihin tietoihin pääsevät käsiksi vain tietoon valtuutetut ja tiedon pysyvän turvassa eikä tiedot esimerkiksi tahattomasti vuoda julkiseen internettiin. Luottamuksellisuus hoidetaan yleensä käyttöoikeuksien hallinnalla eli oikeudet annetaan vain siihen tietoon, joihin on tarve töiden vuoksi päästä. Luottamuksellisuus saattaa rikkoutua tilanteessa, jossa työntekijän käyttäjätunnukset joutuvat hakkerin käsiin ja kaapattua tunnusta hyödynnetään organisaatioon liittyvään tietomurtoon. (Rousku, 2014, ss. 47–50)

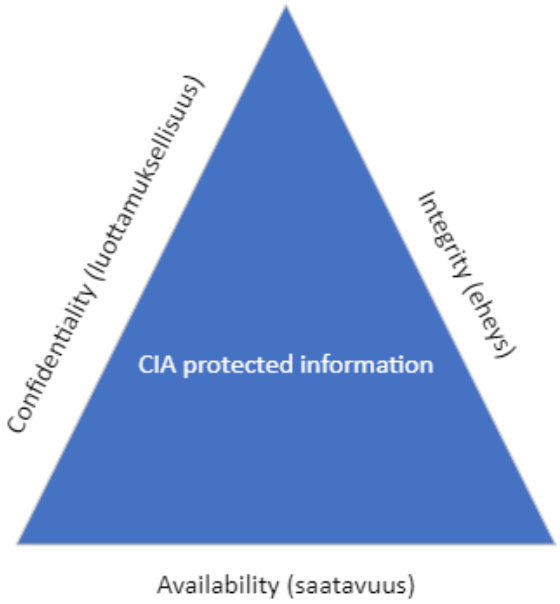
Eheydellä taas tarkoitetaan, että tietoa ei tahattomasti muuteta ja tietoa saa käsitellä sekä muuttaa vain tietoihin oikeutetut. Tietomurron tapahtuessa tiedon muuttumattomuuden varmistuttaessa, tulee varmistaa, että varmuuskopioista on aina alkuperäinen palautettavissa. (Rousku, 2014, ss. 47–50)

2.1 CIA Triad

Tietoturvallisuuden käytäntöjä ohjaamaan on toteutettu CIA Triad -malli. CIA Triad (CIA kolmikko) kuvastaa tietoturvan kolmea tärkeintä osa-aluetta eli C=confidentiality (luottamuksellisuus), I=integrity (eheys) ja A=availability (saatavuus). Kyseisestä mallista saatetaan välillä käyttää myös lyhennettä AIC. Syy AIC-lyhenteeseen on, koska CIA saatetaan

yhdistää tunnettuun USA:n tiedustelupalveluun eli Central Intelligence Agencyyn (CIA). Jos CIA Triadin kuvion sivustan yksikin sivusta ei ole kunnossa tai puuttuu, niin tällöin voidaan todeta keskiössä olevan tietoturvallisuuden olevan puutteellinen. Organisaatiota voi helpottaa ymmärtämään CIA Triadin toimintamalli mieltämällä luottamuksellisuuden, eheyden ja saatavuuden toisiinsa liitoksissa oleviin kokonaisuuksiin. Kuvio 1 sisältää CIA Triadin. (Chai, 2023)

Kuvio 1. Tietoturvallisuuden CIA Triad (mukaillen Chai, 2023)



2.2 Tietoturvallisuus ja informaatioteknologian suojaaminen ja erot

Usein sekoitetaan mitä tarkoitetaan informaatioteknologian suojauksella ja tietoturvallisuudella. Informaatioteknologialla tai kyberturvallisuudella pyritään estämään elektronisen tiedon hakkeroimista tai tiedon vaarantumista. Informaatioteknologialla suojattaviin omaisuuseriin kuuluvat tietokoneet, palvelimet, tallennusjärjestelmät, tietoverkot, mobiililaitteet ja IoT (internet of things) laitteet. (Dataguard, 2022)

Tietoturvallisuudella taas pyritään suojaamaan arvokasta tieto-omaisuutta sijainnista riippumatta. Toisin sanoen tietoturvallisuuden tärkein tehtävä on siis tiedon luottamuksellisuuden, eheyden ja saatavuuden turvaaminen. Lisäksi tietoturvallisuus eroaa

informaatioteknologiasta, koska siihen kuuluu informaatioteknologian lisäksi fyysinen turvallisuus. (Dataguard, 2022)

2.3 Tietoturva vs. tietosuoja

Tietoturva ja tietosuoja kulkevatkin rinta rinnan, jossa molemmat ovat tärkeitä elementtejä tietoturvallisuudessa. Kuten useamman kerran onkin jo mainittu niin tietoturvallisuuden tärkein tehtävä on turvata tietojen eheys, luottamuksellisuus ja saatavuus. Tietoturvallisuus käsittää niin tekniset ja fyysiset suojauskeinot kuin hallinnollisetkin ohjeistukset sekä politiikat. (Fortra, 2021)

Tietoturvallisuudella pyritään suojaamaan organisaation tietotekninen ympäristö luvattomilta pääsyiltä tai haittaohjelmilta ja tietoturva ottaa huomioon niin henkilöt kuin ohjelmistot. Lisäksi tietoa suojataan teknisesti eri menetelmillä ja erilaisilla hallinnollisilla käytänteillä sekä ohjeistuksilla. (Intellfence, 2021)

Se miten tietosuoja eroaa tietoturvasta, tietosuoja määrittää kuinka henkilötietoja käytetään, tallennetaan, hallitaan, jaetaan ja ylläpidetään. Tietosuojaus käytännössä kertoo henkilön yksilöivien henkilötietojen ylläpidosta. Henkilötietojen käsittelyn säätelyllä ei yksistään ole kovin hyvää suojausta ilman tietoturvallisuuden tuomia menettelyjä mm. tiedon teknistä suojausta. (Fortra, 2021)

Henkilötietoa on kaikki se tieto, jolla voidaan yhdistää tiettyyn henkilöön suoraan tai välillisesti yhdistämälle eri tietoja toisiinsa. Henkilö voidaan tunnistaa esim. nimellä, osoitteella tai auton rekisterinumerolla. Henkilötietoja suojataan tietosuoja-asetuksella. Tietojen tallennusmuodolla ei ole väliä, joten tietosuoja-asetus kattaa sähköisen kuin paperisen muodon. Tietosuojalainsäädännön piiriin ei kuulu sellainen toiminta, jossa yksityinen henkilö esim. pitää osoitekirjaa tai sosiaaliseen verkostoitumiseen sekä tietoja ei käytetä ammatillisessa tai kaupallisessa toiminnassa. (Tietosuojavaltuutetun toimisto, n.d.-a)

Suomessa tietosuojaan liittyviä asioita valvoo viranomaisen statuksella tietosuojavaltuutetun toimisto. Tietosuojavaltuutetun toimisto on kansallinen toimija, jonka tehtävänä on mm. valvoa tietosuojalainsäädännön toteuttamista (Tietosuojavaltuutetun toimisto, n.d.-b).

Euroopassa henkilötietojen käsittelyä vahvasti ohjaa EU:n yleinen tietosuoja-asetus GDPR (General Data Protection Regulation), joka antaakin henkilölle laajat oikeudet omiin tietoihinsa. GDPR tuli voimaan kaikkiin EU-maihin vuonna 2018. (Tietosuojavaltuutetun toimisto, n.d.-c)

3 Kyberturvallisuus

Limnell ym. (2014) kuvaavat kyberturvallisuutta kirjassaan seuraavasti: On olemassa fyysinen maailma, joka muodostuu atomeista. Atomeista koostuva maailma on kiinteästi havaittava ja kosketeltava, kuten auto tai tietokone. Atomien rinnalla on ihmisen luoma biteistä koostuva maailma. Kyber-termillä bittien maailmassa tarkoitetaan sitä mitä et voi nähdä tai koskea. Toisin sanoen bittien maailmaa ovat mm. tietoverkot, internet ja sosiaalisen media. Kyber-sana taas tulee kreikan kielestä, joka on tarkemmin lyhenne sanasta kybereo. Kybereo-sanalla tarkoitetaan ohjaamista, opastamista sekä hallintaa. Kyber-termi onkin enemmän kuin yleisluontoinen sana, joka kuvastaa digitaalista ympäristöä. Kyber-sanan jälkimmäinen sana määrittää sen kontekstin tarkemmin, kuten kyberturvallisuus tai kybermaailma. (Limnéll ym., s. 29)

Kyberturvallisuuden rajat monesti hämärtyvät ja usein keskusteluissa esiintyy epäselvyyttä siitä, että onko kyberturvallisuus sama asia kuin tietoturvallisuus, verkkoturvallisuus tai tietokoneisiin liittyvää turvallisuus. Käsitteitä aiheeseen liittyen on tuhottoman paljon, joten ei kannata asiaa liikaa vatvoa. Toisin sanoen kyber-sanana siis kuvastaa biteistä koostuva maailma. (Limnéll ym., s. 30)

Bittien maailman ja atomien fyysisen maailman yhteen sitoutuminen tuo ihmisille paljon hyvää erilaisten digitaalisten palveluiden muodossa, joka myös tarkoittaa bittien maailmassa tapahtuvien ongelmien seurauksien näkyvän suoraan käyttäjille. Digitaalisten palveluiden toimivuutta, jossa haitalliset toimijat kohdistavat vihamielisiä toimintoja esim. pankkijärjestelmään, pyritään suojaamaan kyberturvallisuudella. Erilaiset laitteet ovat nykyään yhä enenemissä määrin internettiin kytkettyjä, jolloin kyberturvallisuus korostuu myös kansalaisten arjessa. Tänä päivänä sähkö- ja energialaitosten ollessa tietoverkon kautta ohjattavia, piilee niissä myös isoja riskejä, kuten kyberhyökkäyksellä aiheutetut laajat sähkökatkot ja ongelmat kiinteistöjen lämmönjakelussa. Nyt ja tulevaisuudessa olemme koko ajan enemmän ja enemmän riippuvaisia kybermaailman palveluista ja siitä on tullut olennainen osa meidän arkeamme. Yleisesti kehitettävä asia on se, että emme kuitenkaan täysin ymmärrä kybermaailman näkymätöntä toimintaa. (Limnéll ym., ss. 31–34)

Puhuttaessa kyberturvallisuudesta, tulee erityisesti keskittää huomio viimeiseen sanaan eli turvallisuuteen. Turvallisuus on tila, johon tulisi pyrkiä tekemällä erilaisia parantavia toimenpiteitä. Turvallisuuden parantamisen vastavoimana onkin erilaiset uhat. Uhkia löytyy monenlaisia, joiden oikeanlainen arviointi on erityisen tärkeää. Uhkia lajitellessa voi olla hyödyllistä jakaa uhat kolmeen erilliseen kategoriaan: kohde (mitä turvataan), uhat (miltä turvataan) ja keinot (miten turvataan). Kyberturvallisuus koskettaa meitä jokaista, jonka takia kyberturvan perehdyttäminen ja tietoisuuden lisääminen on asia, jota tulee yleisesti tavoitella. (Limnéll ym., 2014, ss. 34–38)

3.1 Tietoturvauhka

Enisa (Euroopan Unionin kyberturvallisuusvirasto) julkaisee vuosittaista raporttia siitä minkälainen uhkamaisema kuluneena vuonna ollut. Enisan uhkamaisemaraportti sisältää tunnistetut tärkeimmät uhat, uhkiin liittyvät trendit ja uhkatekijät. Lisäksi raportti esittelee käytetyt hyökkäystekniikat sekä vaikutus ja motivaatioanalyysit. Raportissa esitellään myös erilaisia lievennyskeinoja eli tapoja, kuinka uhkien haitallisia vaikutuksia voidaan pienentää. (Enisa, 2022)

Enisan vuoden 2022 Threat Landscape uhkaraportin mukaan, yleisimmät uhat ovat:

- Ransomware (kiristyshaittaohjelma)
- Malware (haittaohjelma)
- Social Engineering threats (sosiaalisen hakkeroinnin uhat)
- Threats against data (uhka liittyen tietoon)
- Threat against availability: Denial if Service (uhka liittyen saatavuuteen, palvelunestohyökkäys)
- Threat against availability: Internet threats (uhka liittyen saatavuuteen, internetin uhat)
- Disinformation – misinformation (väärän tiedon tahallinen levittäminen, väärän tai väärinjohdattelevan tiedon levittäminen)
- Supply-chain attacks (toimitusketjuhyökkäys)

(Enisa, 2022)

Kyberturvallisuuden uhat voidaankin määritellä siten, että ne ovat yleensä yksilöiden tekemiä haitallisia toimia, joissa on tarkoituksena varastaa tietoa, vahingoittaa tai lamauttaa tietojärjestelmiä. (Imperva, n.d.)

Kyberturvallisuuteen liittyy useita uhkia, ohessa muutamia yleisimpiä kategorioita

- haittaohjelma (malware)
- sosiaalinen hakkerointi (social engineering)
- palvelunestohyökkäys (DoS)
- väliintulohyökkäys (man in the middle)
- SQL-injektiot

(Imperva, n.d.)

Kyberturvallisuuden uhkien lähteitä on useita. Lähteistä lukuiset eri ryhmittymät ovat yhdistetty valtiollisiin toimijoihin ja osa jopa terroristiryhmittymiin. Lisäksi kyberturvallisuuden uhkia muodostavat myös yksittäiset hakkerit, yrityksen sisäiset työntekijät tai joskus jopa järjestelmien toimittajat. Haitallisiin toimiin käytetään usein hyödyksi mm. jo olemassa olevia käyttöoikeuksia. (Imperva, n.d.)

3.2 Uhkatekijät

Uhkatekijät (threat actor) tai voidaan käyttää myös termiä haitalliset toimijat. Haitalliset toimijat voivat olla yksittäisiä henkilöitä tai laajempia ryhmittymiä. Haitalliset toimijat pyrkivät hyväksikäyttämään tietoteknisten ympäristöjen erilaisia heikkouksia. Yleensä haitalliset toimet kohdistetaan yksittäisiä tahoja tai organisaatioita vastaan. Uhkatekijät eli haitalliset toimijat yleensä yhdistetään kyberrikollisuuteen ja melko usein haitalliset toimet ovat kiristyshaittaohjelmia eli ransomwarea. Haitallisiin toimijoihin voidaan mieltää hakkerit, organisaatioiden sisäiset toimijat, terroristit tai jopa internetin trollit. Internetin trollit ovat tahoja, jotka tarkoituksellisesti yrittävät internetissä ärsyttää ihmisiä ja kylvää ristiriitaa eri foorumeilla. (Crowdstrike, 2023.-d)

Haitalliset toimijat valitsevat yleensä kohteensa satunnaisesti ja pyrkivät hyödyntämään haavoittuvuuksia yksittäisten henkilöiden sijasta. Haavoittuvuuksien hyväksikäytöllä pyritään

mahdollistamaan laajoja automatisoituja hyökkäyksiä ja leviämään verkosta toiseen. Laajojen ja suurivaikutteisten kyberhyökkäysten tarkoituksena on saada aiheutettua mahdollisimman suurta haittaa. (Crowdstrike, 2023.-d)

3.3 Riski (sis. riskienhallinta)

Uhka ja riski ovat eri asioita. Uhkaa voidaan torjua, mutta riski on mukana kaikessa toiminnassa. Riskillä kuvataan tapahtumaa, jossa on odotus jonkin huonon asian tapahtumisesta. Riskin mahdollisuus ja vaikutus ilmenee ajan kuluessa eri lailla sekä riski voi olla hyvä tai huono. Riskien estämisen sijaan niitä voidaan koittaa väistää eri menetelmiä käyttäen, kuten estäminen, merkitseminen, pienentämällä vaikutusten mahdollisuutta ja siirtämällä niitä. Riskien kanssa voidaan myös totutella tulla toimeen. Organisaatiossa riskeistä on hyvä olla tietoinen ja siihen auttaa riskien analysointi, jossa voi hyödyntää mm. todennäköisyyslaskelmaa. Todennäköisyyslaskemalla pyritään tunnistamaan haitalliset riskit ja miettimään riskin tapahtuessa sen vaikutuksia. Yhtenä vaihtoehtona riski voidaan hahmottaa ja laskea rahallisena arvona omaisuuteen, jolloin arvoina käytetään uhkaa ja uhkan tapahtumisen tuloa. Joskus voi olla, että uhkan tapahtumisen todennäköisyyttä ei saada määritettyä, jolloin riskiä ei saada määritettyä. Riskin määrittämättä jääminen saattaa aiheuttaa sen, että kohdistetaan toimet joko ali- tai ylimitoitetusti. (Limnéll ym., 2014, s. 108)

Riskien käsittelyä ajateltaessa, riskienhallintaprosessi kuuluu siihen olennaisesti. Riskienhallinta on oiva työkalu, jossa riskit pyritään arvioimaan ja havaitsemaan. Lisäksi riskienhallinta auttaa organisaatioita suunnittelemaan ja ottamaan käyttöön eri riskienhallinnan menetelmiä. (Limnéll ym., 2014, s. 109)

3.4 Haavoittuvuus

Informaatiotekniikassa haavoittuvuudella tarkoitetaan heikkoutta, jossa tekijä voi mahdollisesti hyödyntää sitä vaikuttamalla itse järjestelmän toimintaan. Haavoittuvuus ilmenee, kun heikkous löytyy järjestelmästä ja tekijällä tulee olla pääsy sekä mahdollisuus hyödyntää kyseistä heikkoutta. Lisäksi tekijän tulee olla teknisesti osaava ja tekijällä tulee olla taito hyväksikäyttää (exploit) olemassa olevaa heikkoutta. (Limnéll ym., 2014, s. 110)

Järjestelmissä voi olla myös heikkouksia, jotka ovat ns. ominaisuuksia. Kyseisiä järjestelmän normaaliin toimintaan tarkoitettuja ominaisuuksia manipuloimalla voi hyökkääjä päästä sisään järjestelmään. Haavoittuvuus voi liittyä myös ns. käyttäjän tekemään virheeseen, jossa esim. järjestelmän ylläpitäjä tekee varomattoman muutoksen tahattomasti. Kyseistä käyttäjän konfiguraatiovirhettä hyökkääjä hyödyntää päästäkseen järjestelmään. (National Cyber Security Centre, 2015)

Huomautuksena voisi mainita siitä, kun usein mainitaan vain pelkästään haavoittuvuus eikä määritellä erikseen, että onko haavoittuvuus tekninen. ISO27002:2013 standardiasiakirja käyttää haavoittuvuuksista mainittaessa termiä tekninen haavoittuvuus vain erottaakseen haavoittuvuuden yleisluontoisemmasta riskien hallinnan konseptista. (SFS ISO29147:2020, s.6)

3.5 Haittaohjelmat

Enisan 2022 vuoden uhkaraportin mukaan edelleen yleinen haittaohjelmatyyppi on kiristyshaittaohjelma eli tuttavallisemmin ransomware (Enisa, 2022). Kiristyshaittaohjelman toiminta on karkeasti sellainen, jossa hyökkääjä lukitsee omalla salausavaimellaan käyttäjän tietokoneella olevat tiedostot ja vaatii rahaa vastineeksi siitä, että tiedot saadaan takaisin käyttöön. Yleensä hyökkääjä ilmoittaa, että maksun jälkeen uhri saa avaimen tiedostojen salauksen purkuun ja työskentelyä voidaan jatkaa normaalisti. Aina ei ole takeita, että maksun jälkeen uhri saisi salauksen purkavan avaimen. Toki, jos hyökkääjä ei antaisi salauksen purkavaa avainta maksun saadessaan, miksi kukaan enää maksaisi kiristäjälle.

Yhtenä keinona levittää kiristyshaittaohjelmaa on tapa, jossa hyödynnetään käyttöjärjestelmässä olevia haavoittuvuuksia. Kasperskyn kansainvälinen tutkimus ja analysointitiimi (GReAT) tunnistikin vuonna 2023 Windows-käyttöjärjestelmässä olleen CVE-2023-28252 nollapäivä-haavoittuvuuden (zero-day vulnerability) todistetusti hyväksikäytetyn kiristyshaittaohjelman levityksessä. Kyseisen kiristyshaittaohjelman leviämistä edisti tekninen haavoittuvuus, joka mahdollisti käyttöoikeuksien korottamisen. (Kaspersky, 2023.-b)

Myös madot hyödyntävät käyttöjärjestelmässä olevia haavoittuvuuksia. Kun laite esim. tietokone onnistutaan tartuttamaan madolla, madot leviävät kohdelaitteesta organisaation muihin tietoliikenneverkkoihin ja sitä kautta muihin laitteisiin monistamalla itseään. Matotartunnan avulla haitallinen toimija voi käynnistää DDoS-hyökkäyksiä (keskitetty palvelunesto), varastaa arkaluontoista tietoa tai toteuttaa lunnasvaatimushyökkäyksiä. (Baker, 2023)

Internet-selaimen haavoittuvuuksia voidaan hyödyntää asettamalla verkkosivulle skripti tai saastunut tiedosto. Henkilön vieraillessa sivustolla selaimen haavoittuvuutta hyödynnetään, jotta skripti tai saastunut tiedosto saadaan ladattua tietokoneelle ja samalla suoritetaan. (Kaspersky, n.d.-a)

4 Terveydenhuollon tietojärjestelmät ja teknologiat

Suomessa Valvira on sosiaali- ja terveysalan lupa- ja valvontavirasto, jonka tehtäviin kuuluu sosiaalihuollossa dokumentoitavien asiakastietojen ja terveydenhuollossa dokumentoitavien potilastietojen kehittäminen ja seuraaminen sekä toimiminen valvovan viranomaisen roolissa. Valvira jaottelee sosiaali- ja terveydenhuollon järjestelmät seuraavasti:

- apteekkijärjestelmät
- Kanta-palvelut
- asiakastietojen välityspalvelut
- reseptijärjestelmät
- terveydenhuollon potilastietojärjestelmät
- sosiaalihuollon asiakastietojärjestelmät

(Valvira, n.d.)

Terveydenhuollon tietojärjestelmät koostuvat paikallisista, alueellisista ja kansallisista järjestelmistä. Paikalliset ja alueelliset järjestelmät ovat ns. operatiivisen käytön järjestelmiä, joita ammattilainen käyttää päivittäisessä työssään. Kansalliset palvelut ovat ns. tietovarantoja, joihin tietoa talletetaan keskitetysti. Kansallisten palveluiden tietovarannoista tietoa käytetään maanlaajuisesti. (Vuorinen, 2019, s. 14)

Esimerkkinä paikallisesta järjestelmästä on potilastietojärjestelmä (PTJ). Ammattilainen käyttää potilastietojärjestelmää päivittäisessä työssään saadakseen työnsä tueksi tarvittavat potilas- tai asiakastiedot. Potilastietojärjestelmällä hallitaan ja ylläpidetään potilaaseen liittyviä olennaisia tietoja. Kanta- ja koodistopalvelu kuuluvat olennaisiin kansallisiin palveluihin. Kanta-palvelu on ns. yhteiskäyttöpalvelu eli se palvelee sosiaali- ja terveydenhuollon ammattihenkilöitä, että kaikkia Suomen kansalaisia. Kanta-palvelut sisältää esimerkiksi oheiset palvelut:

- potilastiedon arkisto
- sähköinen lääkemääräys
- potilaan mahdollisuus seurata omia tietojaan internetin kautta (Oma-kanta)

(Vuorinen, 2019, s. 14)

Kansallinen arkkitehtuuri hyödyntää yhteistä keskeistä tallennussijaintia. Kyseiseen tallennussijaintiin alueelliset ja paikalliset potilastietojärjestelmät tallettavat olennaiset tiedot potilaasta. Potilaan tiedot ovat liitettävissä alueelliseen Kanta-palveluun, jos potilas ei ole tietojen luovutusta erikseen kieltänyt. Oman rekisterinpitäjän tiedot ovat näkyvissä alueellisessa järjestelmässä vaikka Kanta-palvelun yhteys puuttuisikin. Jotta organisaatio voisi tietojärjestelmänsä Kanta-palveluihin liittää, tulee sitä ennen tietojärjestelmän läpäistä sertifiointiprosessi. Tietojärjestelmän sertifiointiprosessi sisältää mm. tietoturvallisuuden auditoinnin. (Vuorinen, 2019, s. 15)

Kansallisten järjestelmien saatavuuteen ja tietoturvallisuuteen panostetaan melkoisesti erilaisilla toimilla, kuten suojaamalla tietoliikenneyhteyksiä ja panostamalla järjestelmien valvontaan. Kansallisessa järjestelmässä hyödynnetään verkon pilkkomista eli segmentointi, joka tarkoittaa, että verkot ovat omia erillisiä lohkojaan. Pienille toimijoille voi muodostua haasteeksi käyttää erinäisiä palveluita esim. Omakanta-palvelua suoraan internetin yli, koska se on altis internetin häiriöille. Omakanta-palvelu ei ole niin kriittinen, jolloin isoa vahinkoa ei tapahdu vaikka pääsy hetkellisesti estyisi. Internetissä eli julkisessa verkossa olevat palvelut ovatkin usein haluttuja kohteita erilaisille haitallisille toimille juurikin niiden näkyvyyden takia. On hyvä tiedostaa myös, että arkaluontoisia tietoja voi tulla julkisiksi, kun terveydenhuollon asiakkaat käsittelevät tietoja omilla käytössä olevilla järjestelmillään ja välineillään. (Vuorinen, 2019, s. 15)

Kyseisiin järjestelmiin ilmenneet haitalliset toimet on toteutettu enimmäkseen julkisen verkon puolelta tai ovat kohdistuneet paikallisiin järjestelmiin, joka on aiheuttanut sen, että kansalliset palvelut ovat usein säästyneet häiriöiltä. Ulkoapäin tulevilla haitallisilla kybertoimilla on rasitettu Oma-kanta palveluiden toimintaa ja haitattu julkisen verkon kautta toimivien palvelunantajien toiminnanharjoittamista. Yleisin hyökkäystyyppi on ollut palvelunestohyökkäys Kanta-palveluihin, jolla on pyritty vaikuttamaan palvelun toimintaan heikentävästi tai on isketty muihin verkon kriittisiin palveluihin, kuten Väestörekisterikeskuksen toimittamia palveluita kohden. (Vuorinen, 2019, s. 15)

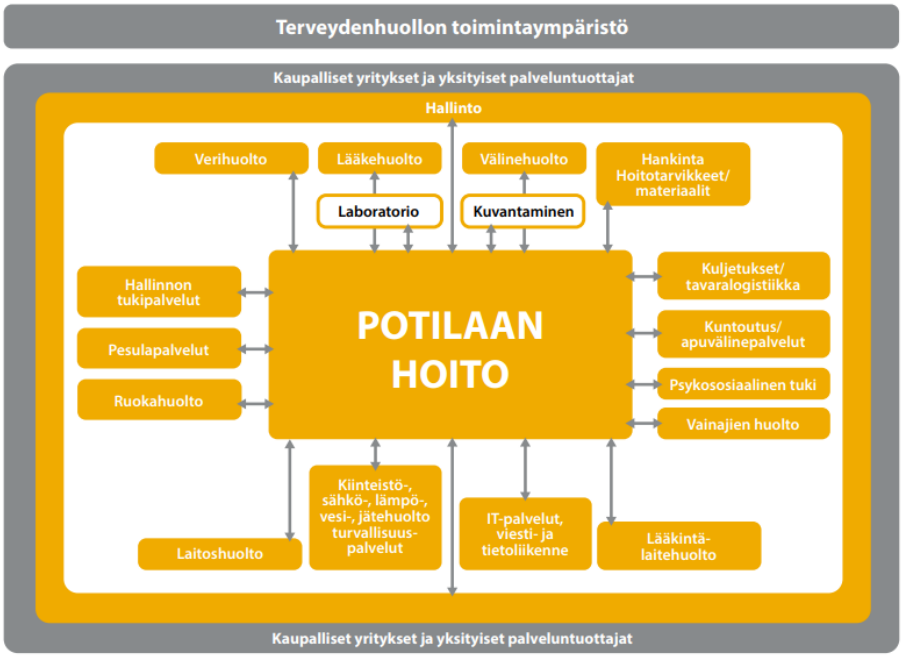
Yksi eniten tietojärjestelmiä käyttäviä kohteita on sairaala. Erinäisiä tietoturvariskejä kasvattaa suoraan internettiin kytketyt (IoT) laitteet. Ison riskin tietoturvamielessä

muodostavat sairaalassa olevat lukuisat lääkinnälliset laitteet. Lääkinnälliset laitteet ovat yhteydessä muihin laitteisiin ja verkkoihin, jotka ovat taas useimmiten yhteydessä suoraan internettiin. Suuri syy IoT-laitteiden yleistymiseen on teknologian huima kehitys ja ihmisten kyky sekä halu käyttää laitteita, joilla voi esim. itse seurata omaa terveydentilaa. Ylimääräistä haastetta aiheuttaa se, kun lääkinnällisissä laitteissa tietoturvavaatimuksia ei huomioida tarpeeksi ja laitteiden käyttöönoton hyväksyntäkriteeristössä asia saattaa jäädä tunnistamatta. Kokonaisuudessa tulee ottaa huomioon, että nykyajan ja tulevien älykkäiden järjestelmien käyttö ei enää rajoitu vain sairaalan sisälle vaan tulee tiedostetaa kaikki mahdolliset toimintaympäristöt. (Vuorinen, 2019, s. 15)

Sairaalaympäristössä on käytössä suuri määrä erilaisia tukevia palveluita, jotka liittyvät potilaan hoitoon. Hoidon edellytyksenä on hoidon jatkuvuuden turvaaminen häiriötilanteiden sattuessa. Sairaalan tietotekniseen ympäristöön sisältyy ns. perinteistä laitteistoa, joita käytetään toimistotyössä. Häiriöt esim. maksuliikenteessä voivat pahimmillaan estää henkilöstön palkkojen maksua ja vaikuttaa erilaisten potilaslaskutuksien käsittelyihin. (Vuorinen, 2019, s. 16)

Kuvio 2 sisältää visualisoinnin terveydenhuollon tyypillisestä toimintaympäristöstä, jossa potilas on kaiken keskiössä ja mukaan ovat linkattuina laboratorio- ja kuvantamispalvelut.

Kuvio 2. Terveydenhuollon toimintaympäristö (Vuorinen, 2019, s. 16)



Ohessa listattuna asioita, joita tulee terveydenhuollon kyberturvallisuusympäristössä on hyvä ottaa huomioon potilaan tietosuojan lisäksi:

- **Etähoidon mahdollistavat järjestelmät**, jotka mahdollista potilaan terveydentilan seurannan. Järjestelmää voidaan hyödyntää myös esim. lääkkeen annostelussa.
- **Verkkokytkentäiset lääkinnälliset laitteet**, joita ovat mm. kannettavat päätelaitteet tai päälle puettavaa älyteknologiaa, jopa robotit avustamassa toimenpiteitä.
- **Erilaiset potilaan identifioimiseen tarkoitetut järjestelmät**, kuten älykkäät rannekkeet.
- **Sairaalan tietoverkkoihin liitettävät verkkolaitteet**, jotka mahdollistavat etälaitteiden liittymisen organisaation tietotekniseen ympäristöön
- **Kannettavat älykkäät laitteet**, kuten mobiilaitteet ja niiden sisältämät sovellukset, jotka sisältävät tietoja potilaasta.
- **Kliiniset tietojärjestelmät**, joita hyödynnetään potilaan hoidon toteuttamisessa ja seurannassa.
- **Kiinteistöautomaatio,** joka sisältää esim. sairaalan älykkäitä toimintoja liittyen niin lukitukseen, kuten hoitoinstrumenttien sterilointiin.

(Vuorinen, 2019, s. 14)

4.1 Tietoturvallisuus terveydenhuollossa

Suomessa, terveydenhuollon tietojärjestelmien tietoturvallisuutta säädellään luokittelemalla tietojärjestelmät A- ja B-luokkaan. A-luokan tietojärjestelmille on vaatimuksena tietoturvallisuuden auditointi, jossa auditoinnin toteuttaminen kuuluu Traficomin hyväksymille kumppaneille. A-luokan tietojärjestelmistä koostetaan raportti ja auditoinnista saa ns. virallisen tietoturvallisuuden todistuksen. Tietoturvallisuuden todistus on kerrallaan voimassa kolme vuotta ja voimassaolon aikaa voi jatkaa maksimissaan kolme vuotta, jonka jälkeen auditointi tulee suorittaa uudelleen. Tietojärjestelmän tuottaja saa itse valita auditoivan tahon, mutta se tulee valita Traficomin määrittämästä listauksesta. Traficomin hyväksymiä tietoturvallisuuden arviointilaitoksia ovat mm. Nixu Certification Oy ja KPMG IT Sertifiointi Oy. (Valvira, n.d.-a)

A-luokka jakautuu A1, A2 ja A3 alaluokkiin. Kaikkiin näihin kuuluu vähintään tietoturvallisuuden arviointi auditoimalla, josta hyväksynnän jälkeen myönnetään tietoturvallisuustodistus. Mainituista alaluokista A3 on se, jossa on eniten vaatimuksia. A3-luokka käsittää mm. Kanta-palveluita hyödyntävät terveydenhuollon potilaskertomusjärjestelmät. (Valvira, n.d.-b)

B-luokan tietojärjestelmiltä ei edellytetä tietoturvallisuuden auditointia. B-luokan tietojärjestelmän tuottajan on huolehdittava, että järjestelmä on niiden vaatimuksien mukainen kuin siltä edellytetään. Terveyden- ja hyvinvointilaitokselta löytyy Excel-dokumentti nimeltä Terveyden ja hyvinvoinnin laitoksen Asiakas- ja potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset -profiilissa, jossa listataan asiat, joita minimissään B-luokan tietojärjestelmältä edellytetään ennen rekisteröintiä. B-luokan tietojärjestelmän virallisen arviointilaitoksen auditoinnin voi tehdä niin halutessaan. (Valvira, n.d.)

4.2 Tietoturvauhkat ja tekniset haavoittuvuudet terveydenhuollossa

Terveydenhuolto saattaa olla erityisen houkutteleva kohde haitallisille toimijoille, koska terveydenhuollon esim. sairaalan tietotekninen ympäristö sisältää paljon erinäisiä verkkoon kytkettyjä laitteita ja laitteet saattavat keskustella useiden muiden laitteiden kanssa. Kyseiset laitteet lisäksi ovat usein yhteydessä internettiin. Terveydenhuollossa on käytössä lukuisia laitteita, verkkoja, järjestelmiä ja sovelluksia, jonka takia haavoittuvuuksien hallinta on melko haastavaa laajassa organisaatiossa. Osaltaan haastetta lisää asiakkaiden itsehoidossa käyttämät terveydenhuollon järjestelmät, esim. verensokerin seurannassa tietoa ladataan kädessä olevasta sensorista älypuhelimeen asennetun sovelluksen kautta, josta tieto siirretään internetin yli järjestelmän tietokantaan.

Kyberturvallisuuskeskuksen Terveydenhuoltoalan kyberuhkia-nimisen dokumentin mukaan terveydenhoitoala sisältää useita haasteita ja uhkia, jotka kohdistuvat tietojenkäsittelyn vaatimuksiin, jossa pyritään turvaamaan potilaan tietojen eheys ja saatavuus. On olennaista hoidon kannalta, että potilastiedoissa ovat oikeat arvot eivätkä ne matkalla muutu itsekseen tai tahallisesti sekä tietojen tulee olla niihin oikeutettujen henkilöiden tarvittaessa saatavilla. Eheys korostuu, koska hoidon kannalta on tärkeää, että potilastiedot ovat juuri ne ammattilaisen kirjaukset eikä järjestelmä jonkin virhetoiminnon takia muuta tietoja tai luvattomasti joku pääse niitä muuttamaan. (Kyberturvallisuuskeskus, n.d.-g)

Saatavuus korostuu esim. kriittisessä hoitotilanteessa, jossa potilaan tietojen näkyvyys voi olla elämän ja kuoleman asia. Luottamuksellisuudella huolehditaan, että tiedot ovat vain niiden käyttöön, joilla on oikeudet kyseiseen tietoon esim. potilaan hoidon kannalta. Yleisesti potilastietojen suojaus estää henkilötietojen hyödyntämisen rikollisessa tarkoituksessa. Rikollisessa mielessä toisen tietoja voidaan yrittää hyödyntää esiintymällä toisena henkilönä, joka on identiteettivarkaus. Rakennuksien osalta kiinteistöautomaatio ja sen suojaaminen kyberhyökkäyksiltä korostuu, koska älykkäiden rakennuksien myötä toiminnot ovat enemmän tietoverkon yli tavoitettavissa. Kiinteistöautomaation toimimattomuus voi suoraan vaikuttaa potilaan hoitoon sairaalassa. (Kyberturvallisuuskeskus, n.d.-g)

Hoitoyksikköjen keskittyessä ensi sijassa potilaan hoitoon saattaa kyberturva-asiat jäädä taka-alalle. Lääketieteellisten tekniikoiden tavoin kyberturvallisuus olisikin syytä huomioida yhtä tärkeänä asiana potilaan hoidon kannalta. Kyberturvan tietoutta ja osaamista tulisikin kehittää eri yksiköissä sekä korostaa kyberriskien tärkeyden huomioimista päivittäisessä toiminnassa, jota voisi edes auttaa asian vieminen johdon suuntaan. (Kyberturvallisuuskeskus, n.d.-g)

Vuosina 2016–2018 käytetyimpiä haittaohjelmia oli ollut kiristysvaatimushaittaohjelma ns. ransomwarea, joissa kohteen esim. tietokoneen tiedostot salataan hyökkääjän toimesta niin, että käyttäjä ei pysty niitä enää käyttämään ja salauksen purkavaa avainta kaupataan tiettyä korvausta vastaan. Kyseinen toimi voi olla organisaatiolle erittäin kiusallinen ja laajasti toimintaa haittaavaa, koska kiristyshaittaohjelma pyrkii leviämään kaikkialle, jonne sillä on kirjoitusoikeus. Pahimmillaan salataan kaikki tiedostot varmuuskopioita myöden ja palautuminen voi olla vaikeaa ja rahallinen menetys on yleensä suuri sekä toipuminen häiriöistä aiheuttaa suuria kustannuksia. (Vuorinen, 2019, s. 18)

Terveydenhuoltoon isosti, erityisesti sairaalaympäristöihin kohdistunut laaja ransomware-hyökkäys oli nimeltään WannaCry. WannaCry oli erityisen tehokas leviämään ja aiheuttikin vuonna 2017 haasteita ja ongelmia kansainvälisesti, laajasti eri toimialoilla. Suomessa, Turun yliopisto joutui kokemaan WannaCry:n, kun sitä löydettiin heidän kuvantamiseensa liittyviltä työasemilta. (Vuorinen, 2019, s. 19)

Yksi merkittävä laitteiden ja järjestelmien suorituskykyä heikentävä menetelmä on virtuaalivaluuttojen louhinta. Virtuaalivaluuttojen louhinta mahdollistetaan saastuttamalla laitteet haittaohjelmalla. (Vuorinen, 2019, s. 19)

Lisäksi koko ajan kasvussa olevat sähköpostin välityksellä tapahtuva tietojenkalastelu yleistyy. Yleisin tapa on, jossa vastaanottajalle lähetetään sähköposti, jossa on linkki aidon näköiselle Microsoft-tilin kirjautumissivulle. Kun henkilö menee tietojenkalastelusivustolle ja antaa organisaatiossa käytössä olevan käyttäjätunnuksensa ja salasanansa haitalliselle sivustolle, sillä haitallinen toimija saa kaksivaiheisen tunnistautumisen puuttuessa käyttäjän sähköpostin haltuunsa ja voi käyttää sitä uusissa haitallisissa toimissa mm. laskutuspetoksiin. (Vuorinen, 2019, s. 19)

Lääkinnällisiin laitteisiin liittyy useita uhkia. Yksi mainittava uhka on lääkinnällisiin laitteiden ylläpitoon liittyvät laitteiden toimittajien etäyhteydet. Valmistaja ottaa etäyhteyksiä kriittisiin lääkinnällisiin laitteisiin. Valmistaja tarvitsee etäyhteyksiä laitteiden konfigurointiin, vian selvitykseen ja laitteen toiminnan seuraamiseen. Toki etäkäyttö auttaa toimittajia takaamaan, että laitteet toimivat oikein ja halutulla tavalla. Ongelmana kuitenkin on, että organisaatio joutuu antamaan toimittajille pääsyjä organisaation sisäverkkoon. Kun toimittaja päästetään organisaation sisäverkkoon, olisi samalla hyvä huomioida millä tasolla tietoturva on laitteen toimittajan tietoteknisessä ympäristössä. Tietojärjestelmien prosesseissa suositellaan hyödynnettävän standardin mukaista esim. ITIL-viitekehystä (Information Technology Infrastructure Library). ITIL-viitekehystä voi käyttää hyväksi lääkinnällisten laitteiden tietoverkkoja mietittäessä. (Vuorinen, 2019, s. 19)

Lääkinnälliset laitteet sisältävät ohjelmistoja, kun taas ohjelmistot usein sisältävät eri asteisia haavoittuvuuksia. Vastuu ohjelmistojen haavoittuvuuksien korjauksista on usein lääkinnällisen laitteen toimittajalla. Jos valmistaja joutuisi korjaamaan laitteen ohjelmistossa olevan haavoittuvuuden, haavoittuvuus korjattaisiin uudella päivitetyllä ohjelmistoversiolla. Uuden ohjelmistoversion käyttöönotto aiheuttaisi valmistajalle lisätyötä, koska ohjelmiston vaatimuksenmukaisuus tulee todentaa uudelleen, joka on yksi syy miksi korjaukset ovat hitaita. Laitteiden käyttäjä todennäköisesti joutuisi myös mukaan ohjelmistoversion päivitykseen. (Vuorinen, 2019, ss. 19-20)

Ohessa lueteltuna terveydenhuollon toimintaympäristöön liittyviä tulevaisuuden kyberuhkia:

- Tietoverkkoon kytketty lääkintälaite hakkeroidaan, jossa haasteena erityisesti kotona yleistyvät käytettävät laitteet ja järjestelmät
- RFID-tunnisteesta tehdään duplikaatti haitallisisen toimijan toimesta (esim. tiloihin kulkuoikeus)
- Kyberhyökkäys pilvipalveluun, joissa tuotetaan esim. potilastietojärjestelmäpalvelua
- Ihmisten aikaan saamat virheelliset konfiguroinnit tai muuten tietoturvattomaan toimintaan liittyvät ongelmat, joka voi johtua mm. henkilön puutteellisesta osaamisesta
- Erilaiset järjestelmähäiriöt, jotka liittyvät IT-infraan mm. verkkolaitteen toimimattomuus

- Pilvipalvelun tai laitteen tuottajan taholta johtuvat erinäiset toimitusketjuun liittyvät ongelmat

(Vuorinen, 2019, s. 20)

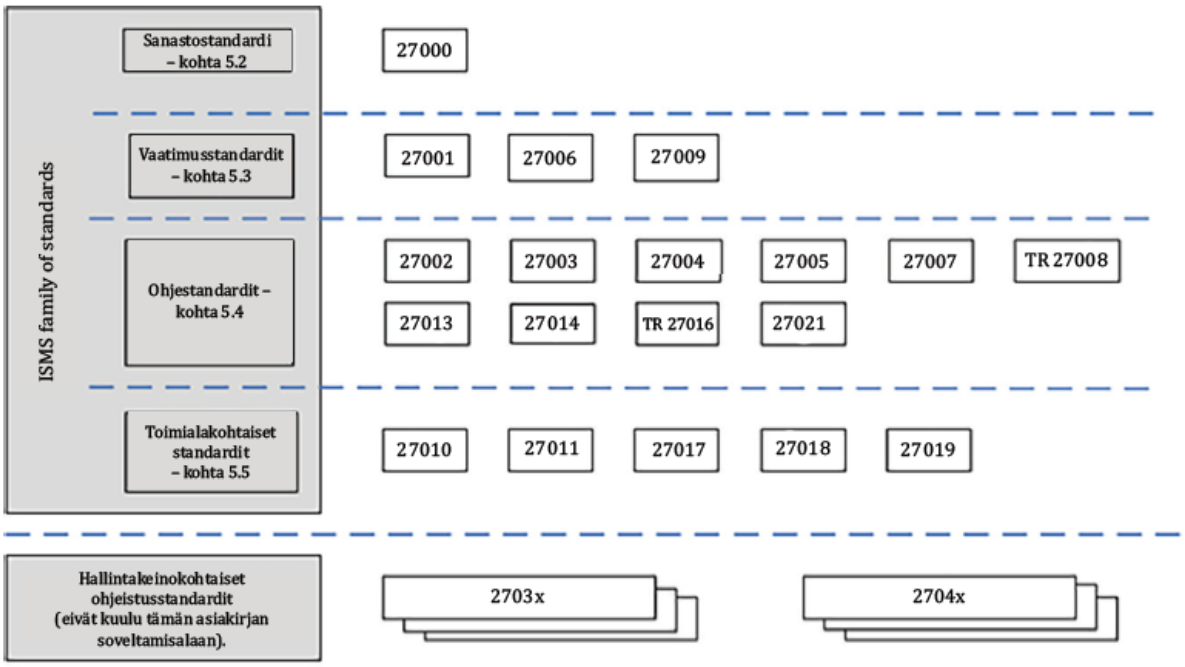
5 Tietoturvallisuuden hallintajärjestelmien standardisarja ISO 27000

ISO 27001 -standardi koostuu useasta erillisestä standardista. ISO 27001 tunnetaan myös ISO 27000 tuoteperheenä, joka on kokoelma parhaita tietoturvakäytäntöjä, joilla organisaatio pystyy kehittämään tietoturvallisuuttaan. ISO 27000 -standardisarja koostuu useista eri tietoturvallisuuden hallintajärjestelmien standardeista. ISO 27000 -standardit ohjaavat ja auttavat organisaatioita kehittämään sekä ylläpitämään tietoturvallisuuttaan. Kyseiset standardit auttavat kehittämään ja ylläpitämään tietoturvaa, koska niissä esitetään tietoturvallisuuden hallintajärjestelmien vaatimukset eli parhaat käytännöt. ISO 27000 tuoteperhe käsittää kaiken kaikkiaan 46 eri standardia, joista ISO 27000 informatiivisesti esittelee muita standardeja ja avaa niihin liittyviä termejä sekä määrityksiä. (Irwin, 2020)

Tietoturvallisuuden hallintajärjestelmä käsittää uhkien hallinnan ja hallintakeinot. Uhkien hallinta ja hallintakeinot sisältää tietoturvallisuuden kolme tärkeää osa-aluetta ihmiset, prosessit ja teknologian. (Irwin, 2020)

Kuva 1 sisältää Tietoturvallisuuden hallintajärjestelmän standardisarjan toisiinsa linkittyvät suhteet.

Kuva 1. Tietoturvallisuuden hallintajärjestelmästandardisarjan keskinäiset suhteet (SFS ISO27000:2020, s. 24)



5.1 Tietoturvallisuuden hallintajärjestelmä ISO 27001

Tietoturvallisuuden hallintajärjestelmä (Information Security Management System, ISMS) on malli, jolla yritykset ja organisaatiot pyrkivät suojaamaan tärkeimpiä omaisuuseriään (assets), joista tieto-omaisuus on yksi tärkeimpiä suojattavia. Tietoturvallisuuden hallintajärjestelmä on olennainen osa ISO 27001 -standardia, sillä ISO 27001 -standardi ohjaa ja määrittää tietoturvallisuuden hallintajärjestelmän ylläpitoa ja kehitystä. Tietoturvallisuuden hallintajärjestelmää hyödyntämällä, organisaation tulee arvioitua riskit ja varmistettua samalla tietojen riittävän suojaustason. Tietoturvallisuuden hallintajärjestelmän olemassaoloa tukee mm. kyberrikollisuuden lisääntyminen ja suuret kustannukset tietomurroissa. Lisääntynyt automaatio, jotka usein sisältävät ohjelmistoja eli koodia, ovatkin haluttuja kohteita rikollisille ja koodien sisältämät lukuisat eri haavoittuvuudet muodostavat suuren riskin. Kansainvälisesti monilla aloilla, kuten terveysala, tietoturvallisuuden hallintajärjestelmä onkin edellytyksenä mm. markkinoille pääsyyn ja saadakseen yhteistyökumppaneita. (Dataguard, 2022)

ISO 27001 -standardi määrittelee kuinka organisaatio luo, toteuttaa ja ylläpitää tietoturvallisuuden hallintajärjestelmää. Asiakirjassa esitellään jatkuvaa parantamista koskevat vaatimukset. Organisaation luomaan ja toteuttamaan tietoturvallisuuden hallintajärjestelmään vaikuttavat mm. organisaation tarpeet ja tavoitteet. (SFS-EN ISO 27001:2022, s. 5)

Koko tietoturvallisuuden hallintajärjestelmän luomisella on tarkoitus suojella tiedon eheyttä, luotettavuutta ja saatavuutta. Tietoturvallisuuden hallintajärjestelmän olennaisena osana hyödynnetään riskien arviointia, joka tehdään osana riskienhallintaprosessia. Mainituilla toimilla on myös osaltaan tarkoitus vahvistaa sidosryhmien luottamusta riskien hallintaan ja tietojen oikeaoppiseen tietoturvalliseen käsittelyyn. On myös erittäin tärkeää, että tietoturvallisuuden hallintajärjestelmää hyödynnetään organisaation prosesseja mietittäessä ja yhdistetään johtamiseen sekä hallintarakenteeseen. (SFS-EN ISO 27001:2022, s. 5)

ISO 27001 -standardiasiakirjan vaatimukset ovat sopivat kaikenkokoisiin organisaatioihin. Vaatimusten soveltuvuus ei rajaa pois tiettyä tyyppiä tai ota kantaa organisaation luonteeseen. Taulukko 1 sisältää kappaleittain tietoturvallisuuden hallintajärjestelmän osa-

alueet, jotka tulee ottaa tarkasteluun. Organisaation sitoutuminen ISO 27001 -standardin asiakirjan käytänteisiin ja ohjeistuksiin tarkoittaa, että organisaation tulee ottaa huomioon kaikki vaatimukset luvuista 4–10. (SFS-EN ISO 27001:2022, s. 6)

Taulukko 1. ISO 27001 luvut 4–10: (SFS-EN ISO 27001:2022, s. 6–14)

luku 4	Organisaation toimintaympäristö
luku 5	Johtajuus
luku 6	Suunnittelu
luku 7	Tukitoiminnot
luku 8	Toiminta
luku 9	Suorituskyvyn arviointi
luku 10	Parantaminen

ISO 27001 -standardiasiakirjan lopussa on liite A, joka sisältää ns. tarkistuslistan eri hallintakeinoista. Kyseiset hallintakeinot tulisi huomioida otettaessa käyttöön tietoturvallisuuden hallintajärjestelmää. Liite A:n listaus ei sisällä kaikkia hallintakeinoja vaan tarvittaessa organisaatio voi käyttää muitakin standardin ulkopuolisia hallintakeinoja tai luoda kokonaan omansa. Lisäksi liite A:n hallintakeinoja tulisi käyttää yhdessä tietoturvariskien käsittelyä määritettäessä, jotta varmasti kaikkiin tietoturvariskeihin löytyy tarvittavat hallintakeinot. (SFS-EN ISO 27001:2022, s. 9)

5.2 Tietoturvallisuuden hallintakeinot ISO 27002 (Information security controls, ISC)

Hallintakeinojen tarkoitus on varmistaa, että organisaatiolla on riittävä suojaustaso tietojen luottamuksellisuuden, eheyden ja saatavuuden turvaamiseen. Hallintakeinoilla pyritään määrittämään ja toteuttamaan tietojen riittävä suojaustaso, ei siis pyritä täydellisyyteen. ISO 27002 -standardiasiakirjassa kuvatuilla tietoturvallisuuden hallintakeinojen toimenpiteillä, voidaan riskiä muuttaa tai säilyttää. Tietoturvapolitiikalla toteutuu riskin säilyminen, mutta tietoturvapolitiikan mukaan toimimalla voidaan vaikuttaa itse riskiin tekemällä muutos. Hallintakeinot voidaankin jaotella organisaatio, henkilöstö, fyysinen ja teknologia kohtaisiin osa-alueisiin. (SFS-EN ISO 27002:2022, s. 8)

ISO 27002 -standardiasiakirja määrittää kuinka tietoturvallisuuden hallintakeinoja otetaan käyttöön niin, että ne ovat ISO 27001 tietoturvallisuuden hallintajärjestelmän mukaiset.

Hallintakeinot ovat sellaiset, että niitä suunnitellessa otetaan huomioon kaikki tiedossa olevat tietoturvariskit. Toisin sanoen jokaiseen tunnistettuun tietoturvariskiin tulisi olla hallintakeino, jolla riskiä voidaan hallita, ehkäistä tai pienentää. ISO 27002 on ns. viiteasiakirja verraten ISO 27001 -standardiin. ISO 27001 -standardiasiakirjaa voidaan käyttää pelkästään ohjeena, kun yrityksessä halutaan ylipäätään hyödyntää tietoturvallisuuden hallintakeinoja, tuolloin hallintakeinot tulisi olla yleisesti hyväksyttyjä. (SFS-EN ISO 27002:2022, s. 7)

ISO 27002 -standardia voidaan hyödyntää toimiala- tai organisaatiokohtaisesti tietoturvallisuuden hallintaan liittyvien ohjeiden kehittämistä. Tietoturvallisuuden hallinnan ohjeiden kehittämisessä tulisi huomioida toimialan ja organisaation spesifin ympäristön tarpeet riskiperäisesti. Jos halutaan hyödyntää ISO 27002 -standardiasiakirjan ulkoisia hallintakeinoja, niitä voidaan luoda riskien arvioinnin kautta. (SFS-EN ISO 27002:2022, s. 7)

Käyttämällä standardin toimintaperiaatteita, sääntöjä, erilaisia prosesseja, mukaan lukien erilaiset tavat menetellä, organisaatiot huomioiden ja hyödynnetään ohjelmisto- ja laitetoimintoja, saadaan muodostettua tietoturvallinen toiminta. Mainitut asiat määrittävät, että organisaatio täyttäisi velvoitteensa liittyen turvallisuuteen ja organisaation toimintaan. Lisäksi hallintakeinoja tulisi arvioida, kehittää ja seurata. Hallintakeinoja tulisi myös toistuvasti katselmoida ja yrittää parantaa. (SFS-EN ISO 27002:2022, s. 7)

Koska teknologialla toteutettava turvallisuus on rajallista, tulisi organisaation saavuttaakseen halutun ja tarpeeksi hyvän tietoturvallisuuden tason ottaa mukaan koko organisaatio panostamaan aiheeseen. Tietoturvallisuutta tulee tukea osana hallinnollisia malleja ja organisaatiokohtaisilla prosesseilla. Toimivien ja olennaisten hallintakeinojen tunnistaminen vaatii huolellista riskien huomiointia ja käsittelyä. (SFS-EN ISO 27002:2022, s. 7)

6 Haavoittuvuuksien hallinta

Haavoittuvuuksien hallinta on toistuva prosessi, jossa arvioidaan, tunnistetaan, raportoidaan ja poistetaan haavoittuvuuksia eri päätelaitteilta, palvelimilta, verkon laitteista, sovelluksista, palveluista sekä järjestelmistä. Yleensä toimesta vastuussa oleva tiimi käynnistää toimet haavoittuvuuksien tunnistamiseksi ja paikkausten varmistamiseksi. Haavoittuvuuksien tunnistamisessa ja paikkausten varmistamisessa hyödynnetään yleensä jotain työkalua, kuten haavoittuvuusskannausohjelmistoa. (Crowdstrike, 2022.-a)

Haavoittuvuuksien tunnistamisen jälkeen käynnistetään erinäiset prosessit, jossa haavoittuvuudet arvioidaan priorisoidusti ja käynnistetään toimet paikkausten tai poistamisen toimet. Jos itse haavoittuvuutta ei saada muuten poistettua (remediate) tai paikattua (patched), tuolloin yhtenä keinona voidaan käyttää haavoittuvuuden vaikutusten minimoimista (mitigate). (Crowdstrike, 2022.-a)

Toimivassa haavoittuvuuden hallintaprosessissa hyödynnetään useista eri lähteistä saatavilla olevaa uhkatietoa. Organisaation tietoteknologia ja yrityksen toiminnot ovat asioita, joita voidaan hyödyntää riskien priorisoinnissa. Onnistuneessa haavoittuvuuden hallintaprosessissa on erittäin tärkeää, että haavoittuvuudet otetaan työn alle pikaisesti. (Crowdstrike, 2022.-a)

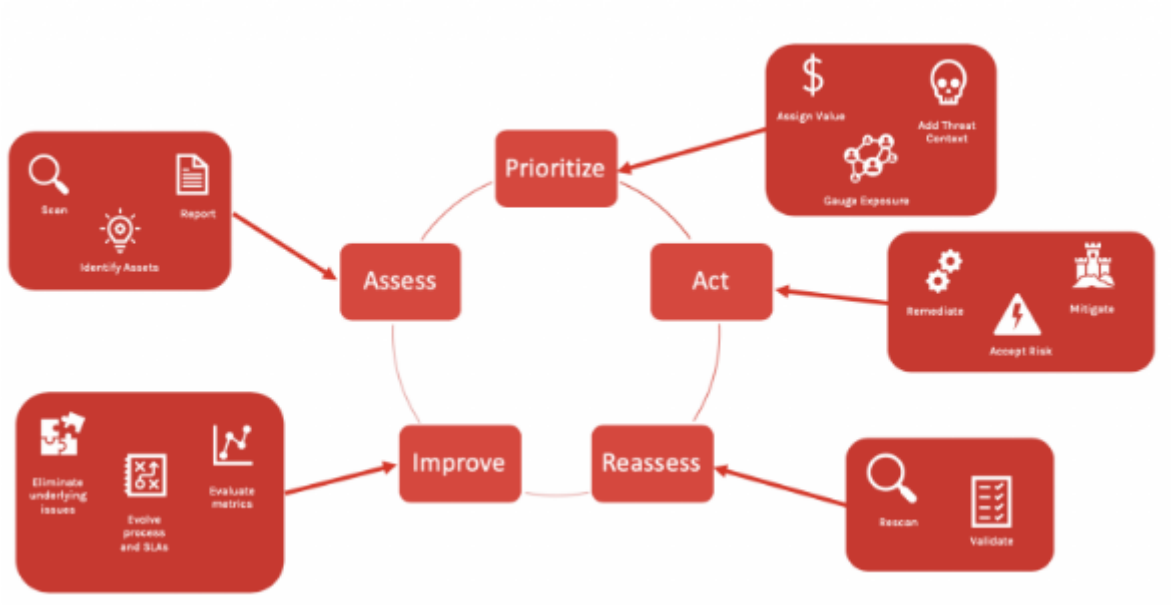
Haavoittuvuuksien hallinta tulee toteuttaa organisaatiossa riskiperusteisesti ja priorisoidusti. Eli mitä suurempi riski organisaatiolle, jolloin korkeimmalle priorisoiduista omaisuuseristä (assets), tulisi haavoittuvuudet ottaa työn alle ensi sijassa. (Souppaya & Scarfone, 2022)

Monilla eri tahoilla on omat haavoittuvuuksien hallinnan mallinsa, kuten Crowdstrike (Crowdstrike, -b), Rapid7 (Rapid 7, n.d.-a) ja Gartner (Barros, A., 2019). Kyseiset mallit ovat pääosin samankaltaisia eli samat tavoitteet ja asiat sekä vaiheet toistuvat, haavoittuvuuksien tunnistaminen, arviointi ja käsittely.

6.1 Haavoittuvuuksien hallinnan esimerkki Crowdstrike

Kyseisessä kappaleessa kuvataan esimerkkinä Crowstriken haavoittuvuuden hallinnan sykli (vulnerability management cycle). Kuvio 3 sisältää Crowdstriken visualisoinnin heidän haavoittuvuuksien hallinnan viitekehyksestä.

Kuvio 3. Crowdstrike Vulnerability Management Lifecycle (Crowdstrike, -b)



Ensimmäisessä vaiheessa arvioidaan (assess) ja tunnistetaan omaisuuserät (assets), joihin haavoittuvuuden arviointia kohdennetaan. Arviointivaiheessa tunnistetut haavoittuvuudet analysoidaan ja niistä luodaan raportti jatkotoimia varten. Tämä vaihe sisältää haavoittuvuuksien skannauksen. (Crowdstrike, -b)

Toinen vaihe, priorisointi (prioritize) koostuu haavoittuvuuksien määrittelemisestä arvon, vaikuttavuuden ja uhkasisällön perusteella. Haavoittuvuus priorisoidaan käsiteltäväksi aiemmin tunnistettujen kriittisien omaisuuserien perusteella. Priorisoituihin omaisuuseräluettelon objekteihin tulee lisätä tietoa siitä, kuinka laajan riskin kyseinen haavoittuvuus muodostaa organisaatiolle. Toisen vaiheen viimeisessä stepissä lisätään uhkatietoa haavoittuvuusraporttiin. Uhkatiedon keräämisessä kannattaa hyödyntää olemassa olevia järjestelmiä, joista uhkatieto löytyy valmiina. Organisaation laajaa henkilöstön osaamista kannattaa myös hyödyntää. (Crowdstrike, -b)

Kolmas vaihe Crowdstriken haavoittuvuuden hallinnassa on toiminta (act). Tässä vaiheessa hyödynnetään toisen vaiheen priorisoinnissa syntynyttä tietoa. Havaitut riskit voidaan joutua hyväksymään. Riskien hyväksyminen voi olla järkevää ei-kriittisten omaisuuserien tapauksissa, erityisesti riskin tai uhan olevan pieni vaikuttavuudeltaan verraten organisaatioon. Haavoittuvuuden hyväksikäytön riskin tai uhan ollessa suuri ja kyseinen omaisuuserä on kriittinen, haavoittuvuus tulee korjata ensi sijassa. Jos haavoittuvuutta ei voida korjata, haavoittuvuuteen voidaan määrittää hallintakeino, jolla rajoitetaan haavoittuvuuden hyväksikäytön mahdollisuutta. (Crowdstrike, -b)

Neljännessä vaiheessa, joka on uudelleenarvioinnin vaihe (reassess) varmistetaan toimien vaikuttavuus. Toisin sanoen tarkistetaan haavoittuvuuksien korjausten tai hallintakeinojen toimivuus ja samalla todennetaan, ettei toimet ole aiheuttaneet uusia haavoittuvuuksia. (Crowdstrike, -b)

Viidennessä ja viimeisessä vaiheessa kehitetään (improve) koko haavoittuvuuden hallinnan sykliä. Jotta haavoittuvuuden hallinnan syklistä saadaan kehittyvä, toimiva ja löydetään heikkoudet, tulee prosessia itsessään toistuvasti arvioida. Ennalta reagoiva ja aktiivisesti ajan tasalla oleva haavoittuvuuden hallinta tekee organisaatiosta vaikean kohteen haitallisille toimijoille. (Crowdstrike, -b)

6.2 Riskiperusteinen haavoittuvuuksien hallinta

Riskiperusteinen haavoittuvuuksien hallinta perustuu kyberturvallisuuden malliin, jossa pyritään tunnistamaan organisaatiolla suurimman riskin muodostavat haavoittuvuudet. Riskipohjaisen haavoittuvuuksien hallinnan mallia tukevat kasvaneet määrät päätelaitteissa sekä lisääntynyt tietoteknisten järjestelmien monimutkaisuus. Tietoteknisen ympäristön monimutkaisuuden ja päätelaitteiden kasvun lisäksi organisaatioiden muiden tärkeiden tehtävien muutokset, kuten pilvipalveluiden kasvu sekä muut mahdolliset muutostyöt järjestelmissä työllistävät it-henkilöstöä. Riskipohjainen haavoittuvuuksien hallinnan malli voi helpottaa henkilöstön kuormaa näissä tilanteissa, jossa tehtäviä joudutaan kiireiden takia priorisoimaan. (Crowdstrike, 2021.-c)

Riskipohjaisen haavoittuvuuksien hallinnan mallissa hyödynnetään priorisointia. Toisin sanoen tunnistetaan haavoittuvuudet, jonka jälkeen priorisoidaan haavoittuvuudet kiireellisyysjärjestykseen. Kiireellisyysjärjestyksen kärkeen käsiteltäväksi otetaan organisaation toiminnalle isoimman uhan muodostavat haavoittuvuudet. (Crowdstrike, 2021.-c)

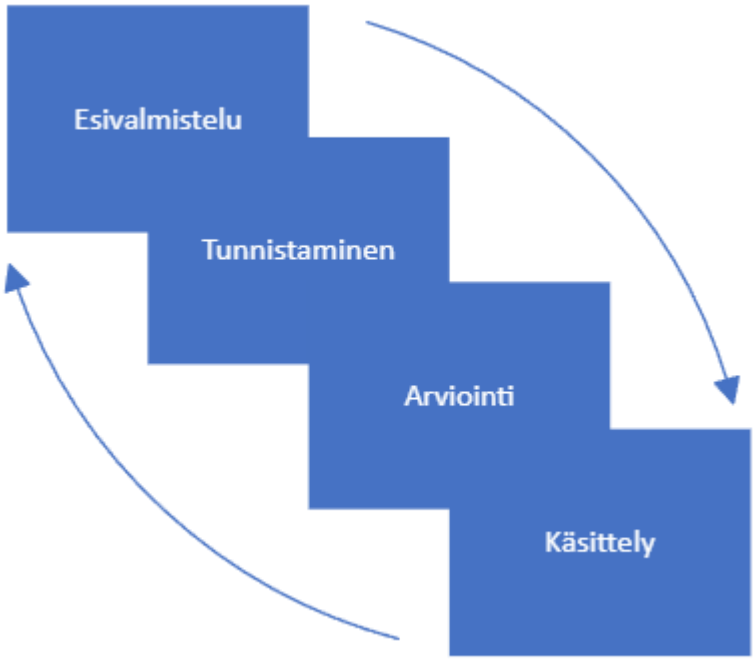
Microsoftin Defender Vulnerability Management (haavoittuvuuksien hallinta) on järjestelmä, joka tekee automaattisesti riskipohjaista älykästä priorisointia organisaation ympäristöstä. Defender Vulnerability Management (DVM) käyttää Microsoftin laajaa uhkatietokantaa, murtautumisen todennäköisyyksiä ja laitteiden arviointeja haavoittuvuuksien priorisoinnissa organisaation tietoteknisestä ympäristöstä. Defender Vulnerability Management -järjestelmä keskittyy havaitsemaan ja nostamaan esiin haavoittuvuuksia organisaation tietoteknisestä ympäristöstä verraten niitä maailmalla nousussa olevia uhkiin, joita jo käytännössä hyödynnetään hyökkäyksissä. (O'Sullivan ym., 2023)

7 Teknisten haavoittuvuuksien hallinta ISO 27002 –standardin mukaisesti

ISO 27002 -standardiasiakirjassa määritellään muiden 113 kpl hallintakeinojen lisäksi alaluvussa 8.8 teknisten haavoittuvuuksien hallinnan hallintakeino. Teknisten haavoittuvuuksien hallintakeino määrittää, että organisaation olisi hankittava käytössä olevista tietojärjestelmien teknisistä haavoittuvuuksista tietoa. Organisaation tulisi arvioida riskit, joille organisaatio on mahdollisesti altistunut ja arvioida riskit haavoittuvuuksiin verraten. Organisaatiosta löytyneisiin riskeihin tulisi reagoida oikeanlaisilla keinoilla ja menetelmillä. Kyseisten menetelmien tarkoitus on suojata organisaatiota estämällä haavoittuvuuksien hyödyntäminen haitallisessa tarkoituksessa. (SFS-EN ISO 27002:2022, s. 102)

Tämän opinnäytetyön alaluvut 11.1–11.4 on jaoteltuna kirjoittajan hahmottelemana mukaillen standardin ISO 27002 8.8 Teknisten haavoittuvuuksien hallintaosiota, josta myös kuvio 4 kertoo. Eli 11.1 osiossa kerrotaan teknisten haavoittuvuuksien hallintaprosessin esivalmisteluista. Esivalmisteluvaihe sisältää mm. prosessin vastuiden ja roolien määrittämisen. Alaluvut 11.2–11.4 sisältävät haavoittuvuuksien tunnistamisen, haavoittuvuuksien arvioinnin ja haavoittuvuuksien käsittelyn vaiheet. Kuvio 4 sisältää visualisoituna ISO 27002 teknisten haavoittuvuuksien hallintakeinon menettelyjen eri vaiheet, jossa esivalmistelut tehdään ensimmäisellä kerralla ja muuten toistetaan vaiheita tunnistamisesta käsittelyyn.

Kuvio 4. Teknisten haavoittuvuuksien hallinnan vaiheet



7.1 Esivalmistelu

Menestyksellisen ISO 27002:n mukaisen teknisten haavoittuvuuksien hallinnan (hallintakeino) määrittäminen, kehittäminen ja ylläpitäminen edellyttää, että organisaatiossa määritetään vastuut ja roolit seuraaviin osa-alueisiin:

- Haavoittuvuuksien seuranta
- Haavoittuvuusriskien arviointi
- Päivittäminen
- Omaisuuserien seuranta
- Mahdolliset koordinointivastuut

(SFS-EN ISO 27002:2022, s. 102)

Lisäksi organisaatiolta tulisi löytyä omaisuuserien luettelo, jossa on tarkasti määritetty ohjelmiston versiot, toimittaja, nimi, versionumerot ja ohjelman mahdollinen käyttö. Lisäksi ohjelman käytöstä tulisi ilmetä resurssit, minne ohjelmaa on asennettu ja kuka on vastuussa ohjelmistosta. (SFS-EN ISO 27002:2022, s. 102)

7.2 Teknisten haavoittuvuuksien tunnistaminen

Teknisten haavoittuvuuksien tunnistamista sujuvoittamaan organisaatiolta tulisi löytyä tarkka luettelo eri omaisuuseristä. Omaisuuseräluetteloa hyödyntämällä organisaatio pystyy tekemään toimivaa teknisten haavoittuvuuksien hallintaa, kun siitä tunnistetaan esim. ohjelmisto, ohjelmiston palvelin ja vastuuhenkilö. (SFS-EN ISO 27002:2022, s. 102)

Organisaation ohjelmistoista ja muista teknologioista tulisi tunnistaa omaisuuseräluetteloon verraten tietolähteet, joilla haavoittuvuudet löydetään ja tunnistetaan. Hyväksi todettuja tietolähteitä voidaan hyödyntää löytämään ajankohtaista tietoa haavoittuvuuksista. Kyseisiä tietolähteiden luetteloita olisi hyvä päivittää sitä mukaa, kun uusia tietolähteitä löytyy. Tietolähteiden päivityksessä tietojen tulisi perustua omaisuuseräluettelon ajanmukaisuuteen. (SFS-EN ISO 27002:2022, s. 102)

Tietojärjestelmien ja koko niiden arkkitehtuurin osalta toimittajien tulisi määrittää ja ylläpitää haavoittuvuuksista dokumentaatiota sekä toimittaja huomioi kuinka haavoittuvuuksia käsitellään ja miten tietoa haavoittuvuuksista julkaistaan. Sopimuksissa voidaan edellyttää toimittajalta lisävastuita. (SFS-EN ISO 27002:2022, s. 102)

Organisaation tulisi tehdä käyttämiin teknologioihinsa säännöllisiä haavoittuvuusskannauksia. Kyseisillä haavoittuvuuksien skannauksilla voidaan tunnistaa tietojärjestelmissä olevat haavoittuvuudet ja varmistetaan haavoittuvuuksien korjaamisen onnistuneisuus. (SFS-EN ISO 27002:2022, s. 102)

Osaavien henkilöiden tulisi tehdä organisaatiossa toistuvia tunkeutumisen testauksia (penetration testing). Tunkeutumistestien tulisi olla hyvin ennalta suunniteltuja ja niiden tulee olla helposti toistettavia. Samaisten henkilöiden tulisi tehdä haavoittuvuuksien arviointia, joilla tuetaan varsinaista haavoittuvuuksien tunnistamista. Kyseisiä menetelmiä toteuttaessa tulisi olla erityisen huolellinen, koska niistä voi aiheutua merkittävää haittaa organisaation toiminnalle. (SFS-EN ISO 27002:2022, s. 102)

Organisaation tulisi seurata kolmannen osapuolen valmistamien kirjastojen ja lähdekoodeja haavoittuvuuksien varalta. Kolmannen osapuolen valmistamien kirjastojen ja lähdekoodien

seurannassa organisaatio voi hyödyntää turvallisen ohjelmoinnin hallintakeinoa (8.28). (SFS-EN ISO 27002:2022, s. 102)

Hallintakeino myös ohjaa, että organisaation tulisi ottaa käyttöön toimintamalli ja taidot haavoittuvuuksien havaitsemiseen omissa tuotoksissaan ja palveluissaan sekä niiden tulisi kattaa myös ulkopuoliset elementit. Samalla olisi luotava tavat haavoittuvuusraporttien vastaanottamiselle, koskien niin sisäisiä kuin ulkoisia tietolähteitä. Organisaatiolla tulisi olla olemassa ulkopuolelta tulevia ilmoituksia varten julkinen paikka, jonne ulkopuoliset tahot voivat ilmoittaa haavoittuvuuksiin liittyvistä ongelmista ja havainnoista. (SFS-EN ISO 27002:2022, s. 102)

Organisaation tulisi lisäksi laatia raportoinnin osalta mallit, kuinka tietoa kirjataan. Raportointia sujuvoittamaan tulisi laatia verkkopohjaiset lomakepohjat. Haavoittuvuuksien osalta tulisi harjoittaa seurantaa eri uhkatietojen lähteistä, jonne ajantasaista tietoa haavoittuvuuksista julkistetaan. Organisaatiolle voisi lisäksi olla hyötyä muodostaa julkinen bug bounty -ohjelma, jonne voidaan julkisesti raportoida ohjelmistoista tai palveluista löytyneistä haavoittuvuuksista. Bug bounty antaa esim. hakkereille mahdollisuuden yleensä jonkinlaista palkkiota vastaan raportoida organisaatiolle löytämistään haavoittuvuuksista suoraan. Bug bounty -menettely auttaa organisaatiota korjaamaan löydetyt haavoittuvuudet ennen kuin jotkut haitalliset tahot ne löytävät. Suositeltavaa myös on, että organisaatio jakaa tietoa eri luotettavien toimijoiden ja tahojen kanssa. (SFS-EN ISO 27002:2022, s. 103)

7.2.1 Haavoittuvuusskannaus

Haavoittuvuusskannaus toteutetaan esim. tietokoneelle asennettavalla haavoittuvuusskanneriohjelmistolla. Haavoittuvuusskanneri kykenee tunnistamaan tietoverkoista erilaiset järjestelmät ja verkossa olevat laitteet mm. tietokoneet, palvelimet ja tietokannat. Haavoittuvuusskannerin löytämät ja tunnistamat järjestelmät testataan tunnettujen haavoittuvuuksien varalta hyödyntäen eri asetuksia mm. käyttöjärjestelmät, avoimet portit, sovellukset ja järjestelmien konfiguraatiot. Haavoittuvuusskanneri hyödyntää tunnistuksessa olemassa olevia tietokantoja tunnetuista haavoittuvuuksista. (Rapid 7, n.d.-a)

On tärkeää ottaa huomioon, että haavoittuvuusskannaus voi tuottaa vääriä tuloksia. Haavoittuvuusskannausohjelmisto ei välttämättä osaa tunnistaa esim. tilannetta, jossa organisaation tietyssä käyttöympäristössä palvelut ovat tarkoituksella konfiguroitu tietyllä tavalla, ja skanneri tulkkaakin ne virheellisesti haavoittuvuuksiksi. (SFS-EN ISO 27005:2018, s. 48)

7.2.2 Tunkeutumistestaus (penetration testing)

Tunkeutumisentestauksella yritetään saada pääsy organisaation järjestelmiin jäljitellen samoja menetelmiä ja työkaluja kuin haitallinen toimija eli hakkeri. Tunkeutumisentestauksella haetaan lisäarvoa organisaation määrittämään haavoittuvuuksien arviointeihin, joten se ei saisi olla tärkein tapa haavoittuvuuksien tunnistamiseen. (National Cyber Security Centre, 8.8.2017.-b)

7.2.3 Tietoturvatestaus ja -arviointi

Tietoturvatestaus ja tietoturva-arviointi ovat tunnistamiseen hyödynnettäviä menetelmiä. Kyseisiä menetelmiä voidaan hyödyntää haavoittuvuuksien tunnistamiseen riskien hallinnan prosessin kautta. Tietoturvatestiä varten suunnitellaan ja kehitetään testimetodi, joka voi olla esim. automatisoitu skripti. Tällaisen testauksen on tarkoitus testata tietoturvallisuuden hallintakeinoja, kuten ne olisivat otettuna käyttöön oikeaan tuotantoympäristöön. Testin lopputulemana arvioidaan vastasiko käytössä olleet hallintakeinot haluttuja tietoturvallisuuden vaatimusten tasoja. (SFS-EN ISO 27005:2018, s. 48)

7.2.4 Kirjastojen ja lähdekoodin haavoittuvuuksien seuranta

Ulkopuolisten eli kolmansien osapuolien luomien kirjastojen ja lähdekoodien osalta haavoittuvuuksien seurantaa tulee tehdä. Seurannassa voidaan hyödyntää ISO 27002 -standardin alaluvun 8.28 Turvallisen ohjelmoinnin hallintakeinoa. (SFS-EN ISO 27002:2022, s. 102)

Threat Intelligencen mukaan turvallinen koodin (secure code) arviointi tarkoittaa, että sovelluksen lähdekoodia tulee seurata haavoittuvuuksien varalta. Yksi syy tähän on, koska

haavoittuvuus on voinut joutua koodiin tahattomasti jo sovelluksen kehitysvaiheessa. Koodia voidaan tutkia manuaalisesti tarpeeksi pätevän henkilön toimesta. Manuaalinen koodin tutkiminen saattaa viedä aikaa ja rahallinen kustannus voi olla suuri, joten koodin arviointiin on kehitetty ohjelmistoja, jolla koodin arviointia voidaan automatisoida. Manuaalisessa ja automatisoidussa koodin tutkimisessa on omat puutteensa, jonka vuoksi suositellaan hyödynnettävän molempia menetelmiä. (Threat Intelligence, 2023)

7.2.5 Bug Bounty –ohjelma

Bug Bounty -ohjelma tarkoittaa sitä, että organisaation järjestelmiä ja palveluita testataan haavoittuvuuksien varalta palkkiota vastaan, yleensä rahallista. Ohjelmien testaukseen on valjastettu avoin laaja globaali yhteisö, jossa testaajat ovat yleensä ns. hyväntahtoisia valkohattuhakkereita. Bug Bounty -ohjelmassa osaava tekijä voi ansaita isojakin summia. (Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus, 2019)

Bug Bounty -ohjelman aloituksessa on hyvä varautua siihen, että se ottaa aikaa. Turhia ilmoituksia eli virheitä voidaan rajata pois määrittämälle niille raja-arvot. Bug Bounty -ohjelman ylläpito ja ilmoitusten seuranta vaatii myös osaamista organisaation sisältä haavoittuvuuksien tunnistamisessa ja arvioinnissa. Jos omaa osaamista ei ole, tällöin voidaan harkita osaajien palkkaamista organisaation ulkopuolelta. (Kyberturvallisuuskeskus, 2019.-a)

7.2.6 Tietolähteet haavoittuvuuksista

Internetistä löytyy paljon hyviä ja ammattimaisia tietolähteitä, joista löytyy ajan tasaista tietoa haavoittuvuuksista ja uhista. Yksi hyvä tietolähde haavoittuvuuksien tunnistamiseen, arviointiin ja käsittelyyn liittyen on suomalainen kansallinen tietoturvatoimija viestintä- ja liikennevirasto Traficomin Kyberturvallisuuskeskus. Tietolähteitä voivat olla organisaation henkilöstä ja jopa asiakkaat. Organisaation olisikin hyvä tunnistaa ja luetteloida omaan käyttöönsä sopivat tietolähteet.

Kyberturvallisuuskeskus kokoaa ajan tasalla olevaa tietoa havaituista haavoittuvuuksista maailmalla, tieto löytyy mm. haavoittuvuudet nimisellä sivustolla. Esimerkkinä haavoittuvuudet osiossa näkyi vuoden 2023 ajalta haavoittuvuuksista ilmoituksia, joista

kriittisiä oli 7 kappaletta. Viimeisin ilmoitus koskettaa Applen tuotteissa havaittuja kriittisiä haavoittuvuuksia. (Kyberturvallisuuskeskus, n.d.-c)

Viikkokatsaus on Kyberturvallisuuskeskuksen luoma raportti, johon he keräävät tietoja kybermaailman tapahtumista nopealla aikataululla. Esimerkissäni Kyberturvallisuuskeskuksen viikkokatsaus - 13/2023 raportissa nostetaan esiin ensimmäisenä merkittävimmät tapahtumat, Hack and Leak -ilmiö ja 3CXDesktopApp -videoneuvotteluohjelmistoon kohdistuneen toimitusketjuhyökkäyksen (Supply Chain Attack). Molempiin löytyy sivustolta linkit tarkempiin ja yksityiskohtaisimpiin tietoihin. (Kyberturvallisuuskeskus, n.d.-d)

Kyberturvallisuuskeskus myös luo ja ylläpitää Kybersää-nimistä raporttia, johon he keräävät kyberin olennaiset tapahtumat yhteen maailmalta. Kybersäässä yhdistyy tietoja viikoittaisista kuin kuukausittaisten muiden Kyberturvallisuuskeskuksen raporttien yhteenvedoista. Kybersää raportin tarkoituksena on olla lyhyt ja ytimekäs, mutta silti ymmärrettävä. (Kyberturvallisuuskeskus, n.d.-e)

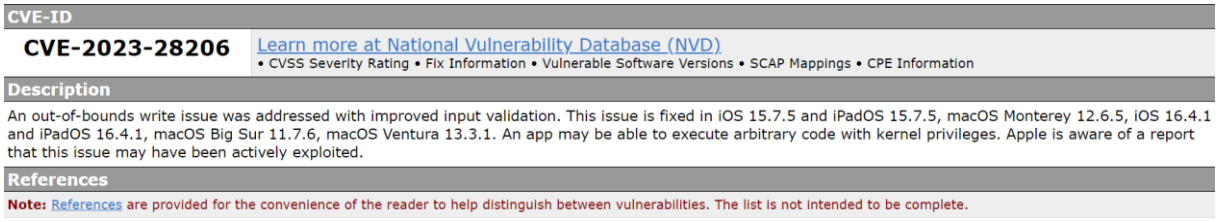
Kyberturvallisuuskeskus toimittaa tietoa eri sähköpostijakeluina, joista yksi on CERT-FI-ALERT-varoitukset, jossa jaetaan päivittäin julkaistava haavoittuvuuskooste. Kyseisen koosteen voi tavan kansalainenkin tilata. Saadakseen kyseisiä varoitusilmoituksia, siihen löytyy Kyberturvallisuuskeskuksen sivulta selkeä ohje. Käytännössä sinun tulee lähettää posti tiettyyn osoitteeseen tietyssä formaatissa (aihe, sisältö) ja saat paluupostiin ilmoituksen jakelulistalle pääsystä. (Kyberturvallisuuskeskus, n.d.-f)

Yleisesti löydetyistä haavoittuvuuksista muodostetaan toimittajariippumaton CVE-tunniste. CVE-lyhenne tulee sanoista Common Vulnerability and Exposures, josta suora suomennos on yleinen haavoittuvuus ja altistuminen. CVE:tä voidaan hyödyntää haavoittuvuuksien tunnistamisen helpottamiseksi eri foorumeilla ja tiedon jakamisessa muiden kanssa. CVE-tietuetta yleisesti hyödynnetään helpottamaan tarkistusta tilanteessa, jossa selvitetään sisältääkö julkaistu uudempi ohjelmistopäivitys korjauksen saman CVE-tunnisteen mukaiseen haavoittuvuuteen. Kuvan 2 esimerkissä CVE-tunniste on muotoa CVE-2023-28206, josta CVE on alkuosa, 2023 vuosiluku ja 28206 juokseva tunniste. Jos haavoittuvuudesta on luotu CVE-tunniste yleensä, tieto löytyy myös NIST (National Institute

of Standards and Technology) NVD (National Vulnerability Database) tietokannasta. (Nixu, 2014)

Kuva 2 sisältää CVE-2023-28206 haavoittuvuuden tiedot Mitren CVE-sivuilta katsottuna. Esimerkkinä oleva CVE-2023-28206 koskee Applen tuotteissa olevaa kriittistä haavoittuvuutta, joka mahdollistaa mielivaltaisen koodin suorittamiseen kernelin oikeuksilla (Kyberturvallisuuskeskus, 2023.-b

Kuva 2. CVE Mitre CVE-2023-28206 tiedot (CVE Mitre, n.d.)



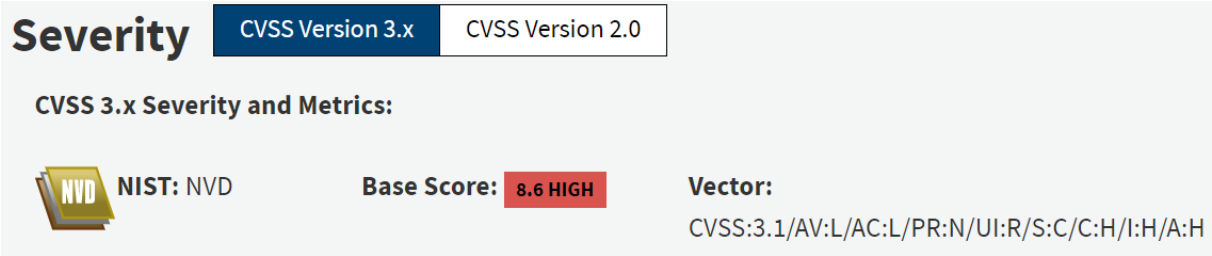
CVE-ohjelma (CVE Program) on luotu tarpeeseen, jotta voidaan tunnistamaa, määritellä ja luetteloida yleisesti julkistetut kybermaailmaan liittyvät haavoittuvuudet. Jokaisesta haavoittuvuudesta löytyy oma yksilöity tietue CVE-luettelosta. CVE-ohjelmaan liittyneet kumppanit (CVE Partners) julkaisevat tietoa löydetyistä ja tunnistetuista haavoittuvuuksista ympäri maailman. Samalla kumppanit määrittävät tunnistetuille haavoittuvuuksille CVE-tunnisteen. (CVE, n.d.)

CVSS (Common Vulnerability Scoring System) on valmistajasta riippumaton malli määritellä ja ilmoittaa haavoittuvuuden vakavuus numeroarvosanoin. Arvo ilmoitetaan väliltä 0.0–10.0 ja mitä suurempi arvo sen kriittisempi korjattava haavoittuvuus on kyseessä. CVE-tietueessa on yleensä linkitys NVD:n tietokantaa, jossa on mainittuna myös CVSS-arvo. CVSS-arvoa voidaan seurata, kun halutaan arvioida haavoittuvuuden vaikuttavuutta ja sen vaikutusta riskinä. CVSS-järjestelmää ylläpitää ja kehittää FIRST, joka koostuu eri tietoturvatahoista. Suomesta FIRST:iin kuuluva taho on kansallinen liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. (Nixu, 2014)

Kuva 3 sisältää esimerkin tunnisteen CVE-2023-28206 haavoittuvuuden CVSS-arvosta, jossa base score (kanta-arvo) on 8.6. Base-arvo muodostuu eri vectorin luokituksista, jossa mm. AV:L tarkoittaa, että AV on hyökkäysvektori ja L tarkoittaa, että haavoittuvuutta voidaan

hyödyntää vain sisäverkosta. Jos vectorissa olisikin AV:L tilalla AV:N, joka tarkoittaisi haavoittuvuutta voitaneen hyödyntää verkon yli, jolloin haavoittuvuuden vakavuus olisi merkittävämpi ja base score nousisi huimasti. NIST:in Common Vulnerability Scoring System Calculatorilla voikin itse kokeilla mistä haavoittuvuuden base score muodostuu. (NIST NVD, n.d.-b)

Kuva 3. CVE-2023-28206 Detail (NIST NVD, 2023.-a)

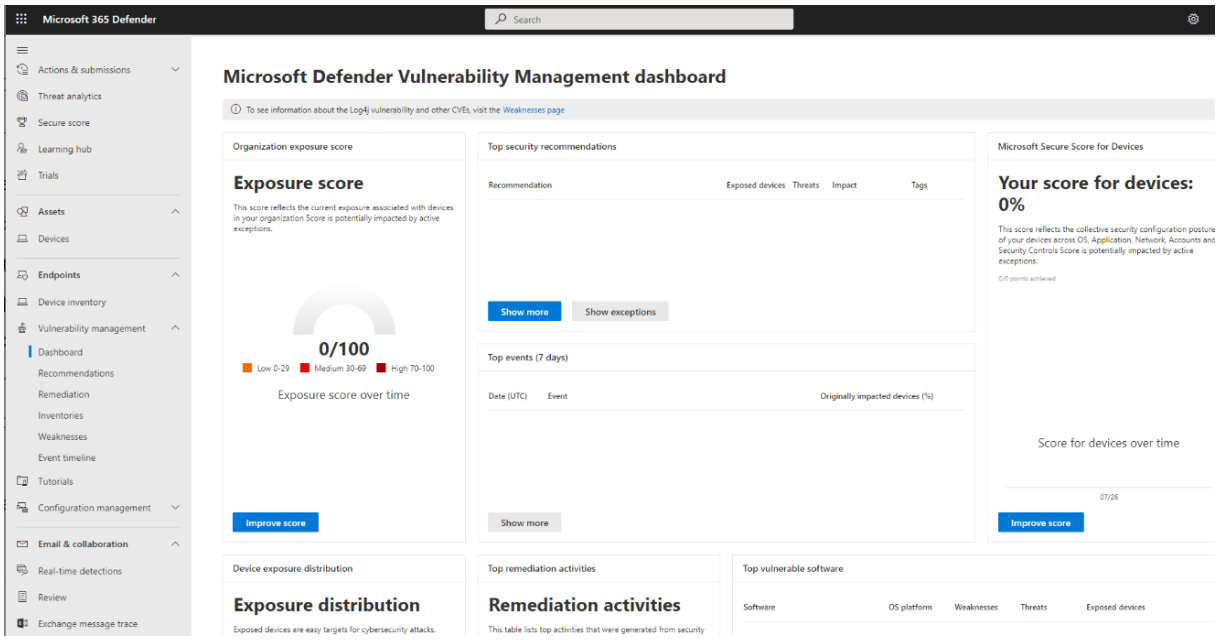


7.2.7 Muut haavoittuvuuksien tunnistustyökalut

Haavoittuvuuksien tunnistamiseen on olemassa useita automatisoituja järjestelmiä. Yksi suosittu ja laajasti maailmalla käytetty ohjelmisto on Microsoftin 365 Defender Vulnerability Management. Kyseinen tuote on pilvipohjainen ja ns. agentiton tuote.

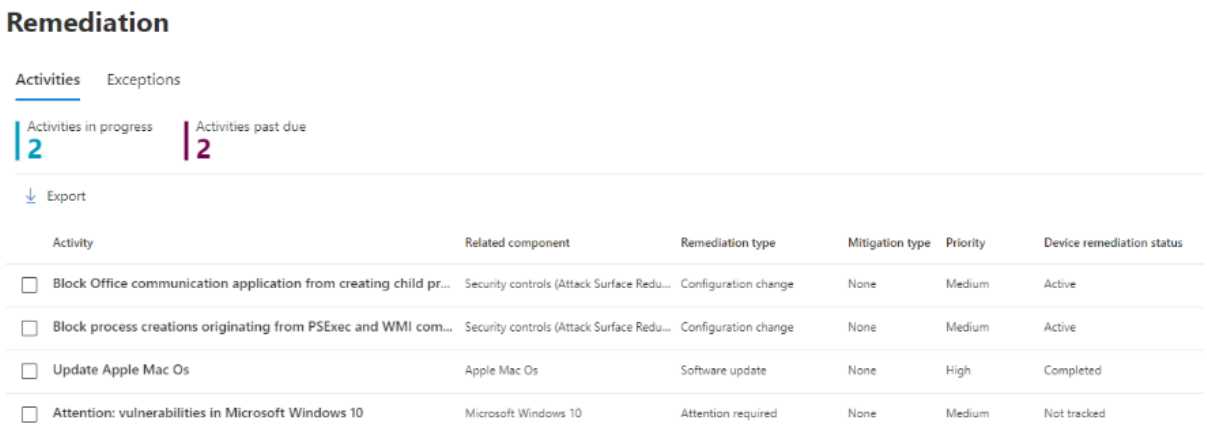
Microsoft Defender for Endpoint portaalin Vulnerability Management konsolinäkymästä nähdään organisaation tietoteknisen ympäristön haavoittuvuudet CVE ja CVSS-luokiteltuna. Kuva 4 on näkymä Microsoft 365 Defender Vulnerability Management dashboardista (haavoittuvuuden hallinta konsolinäkymä). (Vangel ym., 2022)

Kuva 4. Microsoft 365 Defender Vulnerability Management dashboard (Vangel ym., 2022)



Microsoft 365 Defender Vulnerability Management dashboard näkymä näyttää tiedot koostetusti haavoittuvuuksista mm. exposure score. Exposure score (altistumisen pisteytys) arvo kertoo numeroarvolla tiedon organisaation tilasta haavoittuvuuksien mahdolliseen haitalliseen hyväksi käyttämiseen. Mitä pienempi exposure score, sen parempi tilanne on organisaation tietoteknisessä ympäristössä. Kuva 5 sisältää remedation activities (korjaukset toiminta) valikossa suositellut korjaustoimet löydettyjen haavoittuvuuksien suhteen (Vangel ym., 2022)

Kuva 5. Microsoft 365 Defender Vulnerability Management Remediation näkymä (Vangel ym., 2022)



7.3 Teknisten haavoittuvuuksien arviointi

Kun haavoittuvuudet on tunnistettu käyttäen eri menetelmiä mm. haavoittuvuusskannaus, tulisi raportit käydä läpi ja arvioida toteutettavat jatkotoimenpiteet sekä haavoittuvuudet verraten riskeihin. Tunnistettujen haavoittuvuuksien osalta voidaan hyödyntää teknisenä hallintakeinona järjestelmän paikkausta (patching), lieventämistä (mitigation) tai haavoittuvuuden poistamista organisaation tietoteknisestä ympäristöstä (remediation). (SFS-EN ISO 27002:2022, s. 103)

Yksinkertaisimmillaan riskit voidaan arvioida hyödyntäen CVSS-arvoa ja yhdistämällä tietoa järjestelmän kriittisyydestä sekä haavoittuvuuden vaikuttavuudesta organisaatiossa.

7.3.1 Priorisointi

Haavoittuvuuksien priorisointiin on yleisesti käytetty CVSS-arvoa. CVSS-arvoa on lähinnä käytetty, kun ei oikein muutakaan tapaa ole keksitty. Tenablen mukaan CVSS-arvon hyödyntäminen priorisointiin ei ole kovin tehokas tapa ja se on vanhentunut. CVSS-arvo ilmaisee lähinnä, kuinka helposti haavoittuvuutta voidaan hyväksikäyttää (exploit) ja mikä on onnistuneen hyväksikäytön vaikutus. CVSS-arvossa ei oteta huomioon, että onko kyseistä haavoittuvuutta koskaan aiemmin hyväksikäytetty kyberhyökkäyksissä. (Aboud, J, 2020)

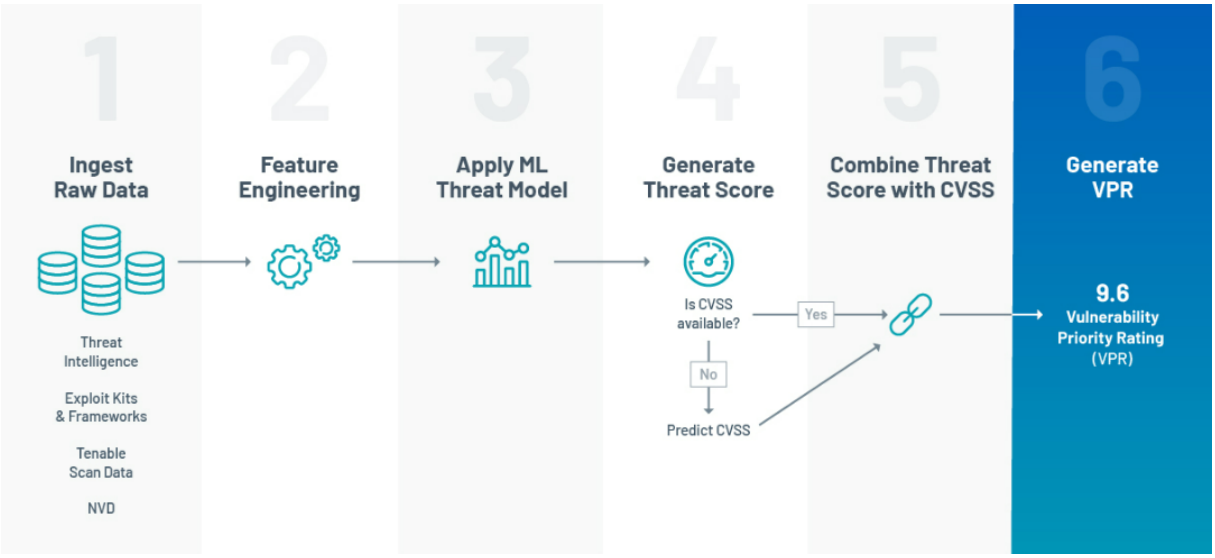
CVSS-arvo määritetään noin kahden viikon sisällä haavoittuvuuden löytämisestä eikä arvoa myöhemmin arvioida uudestaan. Esimerkkinä haavoittuvuus, jonka CVSS-arvo on 6.0 ja it-tiimi käsitteleekin vain yli 7.0 arvon olevia haavoittuvuuksia. Myöhemmin tulevaisuudessa kyseisen haavoittuvuuden CVSS base score arvo on edelleen 6.0 vaikka haavoittuvuutta hyväksikäytetäänkin jo maailmalla ja silloin kyseinen haavoittuvuus muuttuisikin kriittisemmäksi korjattavaksi. Toisin sanoen pelkkää CVSS-arvoa hyödyntämällä priorisoinnissa voi jäädä tärkeitä haavoittuvuuksia käsittelemättä. CVSS-arvon sijaan tulisi hyödyntää riskipohjaista haavoittuvuuksien hallintaa. Riskipohjaisesta haavoittuvuuksien priorisointia käytettäessä organisaation tulee ymmärtää riskit haavoittuvuuksien hyväksikäytön tapahtuessa. (Aboud, J, 2020)

Haavoittuvuuksien priorisointia helpottaakseen Tenable on luonut oman vakavuusluokitteluarvon nimeltä VPR (Vulnerability Prioritization Ranking). VPR on kehitetty auttamaan organisaatioita tekemään tehokasta ja vaikuttavaa haavoittuvuuksien korjaamista. VPR auttaa organisaatiota haavoittuvuuksien korjauksien priorisoinnissa. Järjestelmän taustalla on teknologia nimeltä Predictive Prioritization (ennakoiva priorisointi), jonka tuotosta VPR on. Luokittelu tehdään asteikolla kriittinen, korkea, keskitaso ja matala. (Tai, W., 2020)

VPR on kehitetty mm. vähentämään henkilöstön kuormaa kohdistamalla resurssit sellaisten haavoittuvuuksien paikkaamiseen, joita maailmalla on jo käytetty hyväksi. Toisin sanoen ajatuksena on, että ei yritetä poistaa kaikkia CVSS-arvon mukaan kriittisen luokituksen saaneita haavoittuvuuksia, joita saattaa olla lukumäärältään liikaa eikä niitä koskaan keritä korjaamaan. Pelkän CVSS-arvon sijasta suositaan älykästä priorisointia, jossa hyödynnetään uhkatietoa maailmalta. (Tai, W., 2020)

VPR käyttää koneoppimista ennusteiden luomiseen ja hyödyntää yhtenä tietonaan CVSS-arvoa (Common Vulnerability Scoring System) sekä yhdistelee siihen uhkatietoa eri lähteistä esim. IoC. IoC (Indicator of Compromise) arvo on ns. digitaalinen jälki oletetusta jo tapahtuneesta tietomurrosta. Kuva 6 sisältää miten VPR-arvon muodostamisprosessissa tietoa käsitellään, josta lopuksi muodostuu lopullinen VPR-arvo. (Tai, W., 2020)

Kuva 6. VPR (Vulnerability Prioritization Ranking) Pipeline (Tai, W., 2020)



7.4 Teknisten haavoittuvuuksien käsittely

Ohjelmistojen päivittämisiä varten tulisi luoda hallintaprosessi. Hallintaprosessilla varmistetaan korjaustiedostojen ja sovelluspäivitysten asentaminen ohjelmistoihin. Tärkeissä muutoksissa muutokset tehdään aluksi kopioon ja alkuperäinen ohjelmisto säilytetään entisellään. Muutokset tulisi aina testata ja dokumentoida, jotta voidaan myöhemmin käyttää mahdollisesti uudestaan. Riippumaton taho testaa, arvioi ja hyväksyy muutokset. Tärkeää tässäkin, että kaikki dokumentoidaan huolellisesti. (SFS-EN ISO 27002:2022, s. 103)

Teknisten haavoittuvuuksien käsittelyssä noudatettavat asiat:

- Tunnistettuihin haavoittuvuuksiin, joihin vastattava soveltuvin keinoin ja luotavan aikataulun mukaisesti oikein ajoitetuin toimin
- Teknisen haavoittuvuuden käsittely kiireyden mukaisesti, jossa voidaan hyödyntää muutoksenhallintaa tai tietoturvahäiriötä varten luotua menettelyä
- Käytettävissä korjaustiedostoissa tulee olla ottaa huomioon, että niin sisäinen kuin ulkoinen lähde on luotettu
- Korjaustiedostot tulee aina testata, jotta ne eivät aiheuta ongelmia tuotannolle. Toisin sanoen korjaustiedoston riskiä tulee verrata haavoittuvuuden riskiin.
- Riskille haavoittuvimmat järjestelmät tulee huomioida ja ottaa työn alle ensimmäisenä.
- Tulee kehittää korjaus, joka on yleensä päivitys tai tiedosto, jossa haavoittuvuus on korjattu.
- Korjauksen tai käsittely on todennettava varmistuakseen toimivuudesta.
- Tulee luoda keinot, jolla voidaan todentaa korjauksen aitous.
- Korjauksen puuttuessa tai jos sen asentamisesta joudutaan pidättäytymään esim. tuotannon häiriön vuoksi, tuolloin voidaan hyödyntää muita hallintakeinoja
    - Hyödynnetään haavoittuvuuden ohittavia ratkaisuja, joita voi tiedustella ohjelmiston toimittajalta tai tietoa ammattimaisista asiaan vihkiytyneistä lähteistä.
    - Haavoittuvuuksiin liitoksissa olevat palvelut tai ominaisuudet voidaan ottaa pois päältä.

- Pääsynrajoittamisen eri teknologioiden lisääminen, kuten palomuurien, sopeuttamista tai laajentamista verkon reunoille.
- Käytetään tarkoituksenmukaisia verkkoliikenteen suodattimia.
- Valvonnan lisäämistä havaitsemaan aidot haitallisten toimijoiden hyökkäykset.
- Haavoittuvuuksista tulee informoida.

Lisäksi tulisi huomioida ohjelmistojen automaattisten päivitysten mahdollisuus ja sen käyttöönotto, jos toimittajalta sellainen mahdollisuus löytyy. Tässä tulee huomioida myös ohjelmiston toimittajan julkaisemat tiedot päivityksistä liittyen tietoturvallisuuteen. (SFS ISO27002:2020, ss. 103–104)

7.4.1 Korjaaminen (remediate) ja paikkaaminen (patching)

Korjaaminen on toiminto, jolla haavoittuvuus saadaan poistettua organisaation tietoteknisestä ympäristöstä. Kun organisaation ympäristöstä löytyy haavoittuvuus, korjaamalla tai paikkaamalla se saadaan poistettua ennen kuin siitä tulee uhka. (Tori Sitcawich, 2020.-c)

Paikkaus eli patching on toimenpide, jossa omaisuuserän (asset) haavoittuvuus tai ohjelmistovirhe korjataan esim. asentamalla tuoreempi ohjelmistoversio, jossa kyseiset ongelmat ovat korjattu tai niitä ei ole. Paikkaaminen kuuluu yleensä paikkaamisen hallintaan (patch management), joka on taas tärkeä osa haavoittuvuuksien hallinnan kokonaisuudessa. (Rapid 7, n.d.-b)

7.4.2 Lieventäminen (mitigate)

Lieventämistä voidaan hyödyntää, kun löydettyyn haavoittuvuuteen ei voida reagoida ajoissa johtuen järjestelmän tuotannon keskeytymisestä tai haavoittuvuuteen ei ole vielä paikkausta saatavilla. Näissä tilanteissa organisaatio voi tehdä ehkäiseviä toimia, jolla haavoittuvuuden hyväksikäytön (exploit) mahdollisuutta voidaan rajoittaa. (Tori Sitcawich, 2020.-c)

Lieventämistoimenpide voi olla keskitetyn palvelunestohyökkäyksen tapahtuessa, että ohjataan epäilyttävä verkkoliikenne eri paikkaan suodatusta varten. Yleensä lieventämistoimenpide on vain väliaikainen ratkaisu, koska haavoittuvuus taustalla säilyy. (Tori Sitcawich, 2020.-c)

ISO 27002 -standardin alaluvussa 8.8 Teknisten haavoittuvuuksien hallintakeino suosittelee lieventämisen hallintakeinoina seuraavia: 8.20 Verkkoturvallisuus, 8.21 Verkkopalvelujen turvaaminen ja 8.22 Verkkojen eriyttäminen. Verkkoturvallisuutta voidaan hyödyntää yhtenä lieventävänä toimena, jossa rajoitetaan järjestelmien verkkoyhteyksiä sekä tietoliikennettä suodataan palomuureja hyödyntäen. Verkkopalvelujen turvaamisella voidaan rajoittaa palveluihin pääsyä hyödyntämällä mm. verkkopalvelujen seurantaa tai sallimalla pääsy palveluihin tietyistä verkoista esim. VPN-yhteyden läpi. Verkkojen eriyttämisellä verkkoympäristö pilkotaan eri segmentteihin eli aliverkkoihin ja liikennettä aliverkoista toiseen hallitaan ja tarpeeton liikenne estetään. Kyseisellä menettelyllä voidaan tehokkaasti estää haitallisten toimien mahdollisuutta levitä laajasti organisaatiossa. Lisäksi yleensä on järkevää, että osa verkoista eristetään internetistä. (ISO27002:2020, ss. 121–124)

8 Tavoitteet ja menetelmät

Tämän opinnäytetyön käytännön osio koostuu työpaikalla toteutetuista useista työpajatyyppisistä kokouksista. Työpajoissa hyödynnetään toimintatutkimuksen spiraalimallin vaiheita eli aluksi suunnitellaan työpajojen materiaalit, esitykset, vaiheistus ja määritetään haluttu lopputulos. Seuraavaksi on toiminta itse työpajoissa. Työpajoissa havainnoidaan työn etenemistä ja aineiston toimivuutta sekä suullista palautetta mukanaolijoilta. Työpajojen aikana ja jälkeen reflektoidaan omaa toimintaa, ajatuksia ja mitä syvällisiä ajatuksia heräsi. Kaiken näiden vaiheiden jälkeen kehitetään toimintaa ja parannetaan suunnitelmaa seuraavaan työpajaan. Mainittuja vaiheita toistetaan, kunnes saavutetaan paranneltu toivottu lopputulos.

Toimintatutkimus voidaankin mieltää eräänlaisena reflektiivisenä spiraalimallisena rakenteena. Toimintatutkimuksen spiraalimallissa hyödynnetään suunnittelua, toimintaa, havainnointia ja reflektointia, jonka jälkeen toimintaa pyritään muuttamaan parempaan suuntaan ja näitä vaiheita toistetaan, kunnes saavutetaan haluttu lopputulos. Toimintatutkimuksen keskiössä onkin ajatus, että reflektiivisen pohdinnan kautta saavutetaan parempi lopputulos eli toiminta kehittyy. (Puusa ym., 2020)

Työpajoissa esitetty teoria-aineisto pohjautuu opinnäytetyön viitekehyksen aiheisiin. Osa työpajojen teorian lähteistä hyödynnettiin vain esitysten koostamiseen. Opinnäytetyön tarkoituksena on tutkia teoriaa haavoittuvuuksien hallinnasta ja vastaavista malleista. Keskiössä ovat ISO 27000 sarjan standardit, erityisesti ISO 27001 ja ISO 27002.

8.1 Tavoitteet

Työn tavoitteena on tutkia mitä kaikkea organisaatiolta edellytetään, kun se kertoo toteuttavan teknisten haavoittuvuuksien hallintaa ISO 27001:sen mukaisesti. ISO 27002 -standardi ohjeistaa yksityiskohtaisemmin teknisten haavoittuvuuksien hallintakeinon edellytykset ja suositukset.

Standardien ohjeistusten ja muun aihetta tukevan teorian perusteella sekä organisaatiossa järjestettävillä työpajoilla on tarkoitus kehittää organisaatiolle sopiva ISO 27001 vaatimuksia

vastaava teknisten haavoittuvuuksien hallintaprosessi (hallintakeino). Teknisten haavoittuvuuksien hallintakeinosta tehdään lopuksi varsinainen teknisten haavoittuvuuksien hallinnan prosessikaavio. Lisäksi työn tavoitteena on tuoda esiin teknisten haavoittuvuuksien hallintaan liittyviä huomioita ns. parhaista käytännöistä. Parhaita käytäntöjä hyödyntäen organisaation on mahdollista toteuttaa kustannustehokasta teknisten haavoittuvuuksien hallintaa.

8.2 Menetelmät

Tässä opinnäytetyössä hyödynnetään eri oppimisen ja kehittämisen menetelmiä. Hyödynnettäviä menetelmiä ovat dokumenttianalyysi, ryhmäkeskustelu ja visuaalinen menetelmä. Kyseisten menetelmien hyödyntämisen tarkoitus on päästä suunniteltuihin tavoitteisiin.

Dokumenttianalyysia käytetään tutkiessa erilaisia dokumentteja ja standardiasiakirjoja. Lisäksi dokumenttianalyysin menetelmää hyödynnetään työpajoista saatavien raporttien, päiväkirjojen sekä muistioiden analysoinnissa. Kyseisiä dokumentteja ja asiakirjoja käytetään tulevan työpajan eli ryhmäkeskustelun suunnitteluun ja toteutukseen.

Työpajoissa hyödynnetään vuorovaikutteista ryhmäkeskustelua, jotta päästään toivottuun lopputulokseen. Yhdessä keskustellen ja teoriatietoon pohjaten suunnitellaan organisaatiolle sopiva ja toimiva teknisten haavoittuvuuksien hallintaprosessi, johon nimetään prosessin roolit ja vastuut käytännössä.

Visuaalista menetelmää käytetään työpajojen aikana hahmottamaan teknisten haavoittuvuuksien hallintaprosessia. Visuaalisen menetelmän työkaluina käytetään Microsoftin Power Pointtia ja Visiota.

9 Tutkimustyö

Tutkimustyö toteutettiin Etelä-Pohjanmaan hyvinvointialueen organisaatiossa. Etelä-Pohjanmaan hyvinvointialueen tietohallintopalvelu osaltaan vastaa alueen laajan ja monipuolisen tietoteknisen ympäristön it-tuesta, suunnittelusta, kehittämisestä ja ylläpidosta. Tietohallintopalveluiden tietoturvaryhmän jäsenet valittiin mukaan suunnittelemaan ja toteuttamaan teknisten haavoittuvuuksien hallintaprosessia, koska työn aihe edellyttää tuntemusta organisaation tietoteknisestä ympäristöstä sekä tietoturva-asioista.

9.1 Tutkimusympäristö

Etelä-Pohjanmaan hyvinvointialue (HYVAEP) tuottaa palveluita laajalla asiakasjoukolle, joka koostuu 192 150 asukkaasta ja kattaa 18:sta Etelä-Pohjanmaan kuntaa. HYVAEP on aloittanut organisaationa vasta hiljattain vuoden alusta (1.1.2023), jolloin aiempi Etelä-Pohjanmaan sairaanhoitopiiri lakkasi olemasta. HYVAEP vastaa sosiaali- ja terveydenhuollon sekä pelastustoimen palveluiden tuottamisesta ja organisoinnista Työvoima koostuu noin 10 000 henkilöstä. (Etelä-Pohjanmaan hyvinvointialue, n.d.)

Etelä-Pohjanmaan hyvinvointialueen (HYVAEP) tietohallintopalvelu tuottaa ja vastaa Seinäjoen keskussairaalan ja alueen toimipisteiden potilastietojärjestelmistä. Työntekijöitä on tietohallintopalvelussa reilusti yli 70 henkilöä. Tietohallintopalveluiden vastuulla on yli 450 palvelinta ja yli 400 muuta järjestelmää. Tietohallintapalveluiden asiakaskunta koostuu laajasta verkostosta, joka käsittää kaikki HYVAEP:n alueen terveyden- ja sosiaalihuollon toimijat. (Tietohallinto, n.d.)

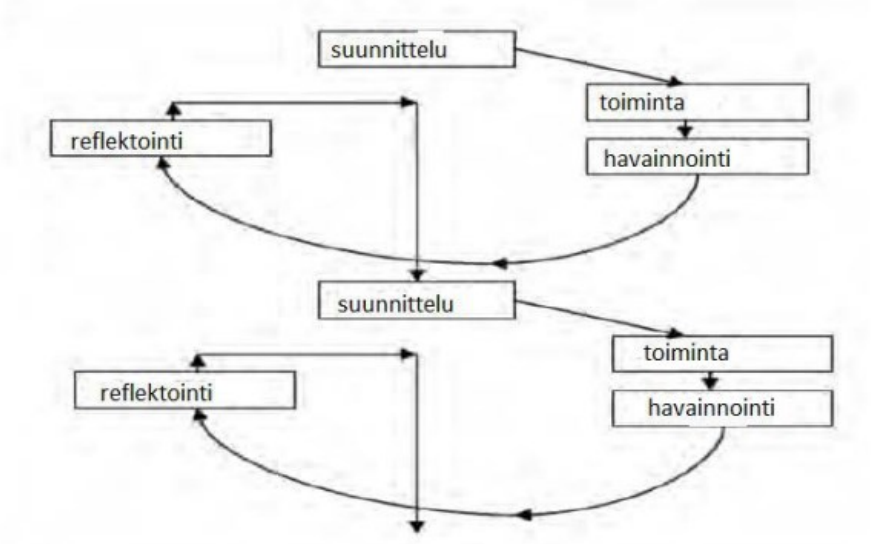
9.2 Toiminnallinen tutkimus

Toimintatutkimus sanastakin voi jo päätellä, että se yhdistää teorian ja käytännön. Toisin sanoen toimintatutkimuksessa pyritään hyödyntämään tutkimusta ja käytäntöä tasapainoisessa suhteessa. Vaikkakin tekeminen suunnittelun sijaan saa herkästi toimintatutkimuksessa suuremman huomion, tulee toimintatutkimuksessa hyödyntää tieteen menettelyjä. (Puusa ym., 2020, s. 256)

> Puusa ja Juuti (2020, s. 256) kuvaavat toimintatutkimuksen käytännön näkökulmaa seuraavasti: Käytännön näkökulmasta toimintatutkimukseen kytkeytyy aina uuden oppimista ja oivaltamista sekä siihen johtavan ymmärtävän prosessin tarkkailua, jonka seurauksena pitäisi käytännön elämässä tapahtua muutoksia ja myös toimintatutkimuksen kohteena olevaan ongelmaan kytkeytyvän teoreettisen ymmärryksen tulisi lisääntyä.

Spiraalimallia voidaankin hyödyntää mainiosti kehittämisprojekteissa, kuten toimintatutkimuksessa. Kuvio 5 sisältää toimintatutkimuksen spiraalimallin. Spiraalimalli kuvastaa prosessin toistuvia kehämäisiä vaiheita. Eteneminen aloitetaan ylhäältä alaspäin. Kehittämistyön kohteena olevat vaiheet eli tehtävät muodostavat itse kehän. Ensimmäisen kehän suorittamisen jälkeen pysähdytään pohtimaan mitä saatiin aikaan ja mitä tulisi seuraavassa kehässä sekä vaiheissa tehdä eri lailla, jotta saadaan aina vain parempi tulos. Kehän suorittamisen jälkeen ennen seuraava kehää, organisoidutaan uudelleen, huomioiden toteutuksien muutokset ja toistuva arviointi. Kehiä voidaan jatkaa niin monta kertaa, kunnes saavutetaan toivottu ja hyväksyttävä lopputulos. Toimintatutkimuksen spiraalimallissa painottuu todellinen toiminta, jossa keskeisenä ovat havainnointi ja toteuttaminen. Havainnointiin ja toteutukseen kytkeytyy olennaisesti niihin liittyvien vuorovaikutustapojen myötä havainnointi ja reflektoiminen, joita vuorotellaan prosessin tulevissa vaiheissa. (Toikko & Rantanen, 2009, s. 66)

Kuvio 5. Toimintatutkimuksen spiraalimalli (Toikko & Rantanen, 2009, s. 67)



9.3 Dokumenttianalyysi

Dokumenttianalyysin on tarkoitus antaa tietoa standardien ohjeistuksista ja vaatimuksista. Erinäiset luotettavat ja ammattimaiset lähteet täydentävät ja selventävät standardien asioita sekä tuovat esiin erilaisia parhaita käytäntöjä. Lisäksi dokumenttianalyysiä hyödynnetään työpajojen muistioiden, päiväkirjan, kirjojen ja artikkelien läpikäynnissä.

9.4 Ryhmäkeskustelut

Ryhmäkeskustelut toteutetaan työpajojen sarjana. Työpajojen tarkoituksena on tuoda mukana oleville henkilöille teoriatietoa teknisten haavoittuvuuksien hallinnasta ISO 27001- ja ISO 27002 -standardien näkökulmasta sekä muista aihetta tukevista lähteistä. Teorian ja työpajatyöskentelyn perusteella suunnitellaan ja toteutetaan ISO 27001 -standardin mukainen teknisten haavoittuvuuksien hallintaprosessi. Teknisten haavoittuvuuksien hallinnan työpajojen ryhmäkeskusteluihin ja suunnitteluun valitaan mukaan Etelä-Pohjanmaan hyvinvointialueen tietohallintopalvelun tietoturvaryhmästä henkilöt. Teknisten haavoittuvuuksien hallinnan näkökulmasta tietoturvaryhmän jäsenillä on tarvittava tuntemus organisaation (HYVAEP) tietoteknisestä ympäristöstä ja sen nykytilasta, mikä auttaa saavuttamaan parhaan lopputuloksen. Tietoturvaryhmän jäseniä on noin 10 ja ryhmää vetää tietoturvapäällikkö ja mukana on teknologiapäällikkö sekä mukana on eri tason suunnittelijoita.

Ryhmäkeskustelut jaetaan useampaan kertaan ja määritetään aiheet työpajakohtaisesti. Työpajat jaetaan ISO 27002 -standardin teknisten haavoittuvuuksien hallintakeinon mukaisesti eli työpajat tulee olemaan haavoittuvuuksien tunnistamisen vaihe, arviointivaihe ja käsittelyvaihe. Suunnitelmana on toteuttaa yhteensä viisi kahden tunnin mittaista työpajaa. Ensimmäinen työpaja sisältää aloituskokouksen ja johdattelun aiheeseen Power Point -esityksen muodossa. Työpaja järjestetään Teamsissa. Esitykseen kerätään yleistä teoriaa tietoturvasta ja ISO 27002 -standardista, joka tukee teknisten haavoittuvuuksien hallintakeinon suunnittelua ja kehitystä. Toisen työpajan aihe on teknisten haavoittuvuuksien tunnistaminen, joka sisältää teorian ISO 27002 teknisten haavoittuvuuksien hallintakeinon haavoittuvuuksien tunnistamisesta. Työpaja järjestetään paikan päällä ja Teamsissa. Kolmas työpaja sisältää vielä teknisten haavoittuvuuksien

tunnistamisen, koska aihe on laaja ja lisäksi uutena aiheena on arviointi. Työpaja järjestetään paikan päällä ja Teamsissa. Neljäs työpaja sisältää teknisten haavoittuvuuksien käsittelyn. Työpaja järjestetään paikan päällä ja Teamsissa. Viides työpaja on ns. päätöskokous, jossa käydään läpi mitä saatiin aikaan ja esitellään lopputuotos eli teknisten haavoittuvuuksien hallinnan prosessikaavio. Kokouksessa tiedustellaan lisäksi palautetta työskentelystä ja lopputuotoksesta. Työpaja järjestetään Teamsissa.

9.5 Visuaalinen menetelmä

Visuaalista menetelmää hyödynnetään työpajoissa. Visuaalisen menetelmän tarkoitus on hahmotella prosessia ja vaiheita hyödyntäen erilaisia kuvioita, piirroksia sekä tekstimuotoa. Visuaalinen menetelmä tuo pohdinnat ja ajatukset konkreettisiksi, jolloin myös prosessin suunnittelu selkeytyy. Visuaalisen menetelmän työkaluina käytetään Microsoftin Power Point ja Visio -ohjelmia.

10 Johtopäätökset, pohdinta ja tulokset

Opinnäytetyön tarkoituksena oli selvittää, kuinka organisaatioon saadaan toteutettua ISO 27001 tietoturvallisuuden hallintajärjestelmät -standardin mukainen teknisten haavoittuvuuksien hallintaprosessi. Tarkemmin tutkittiin mitä organisaatiolta edellytetään, kun organisaatio sanoo toimivan ISO 27001 -standardin mukaisesti ja noudattavansa teknisten haavoittuvuuksien hallintaprosessia. Asiaa selvitettiin ISO 27001 -standardiasiakirjan vaatimuksista ja ohjeistuksista sekä muista alan luotettavista lähteistä. Tutkittu aihetta tarkemmin ISO 27002 -standardista mikä teknisten haavoittuvuuksien hallintakeino on ja mitä käyttöönotto vaatii organisaatiolta. Vertailtiin eri tahojen luomia haavoittuvuuden hallinnan malleja ja työssä esitellään niistä yksi, Crowdstriken haavoittuvuuden hallinnan malli. Opinnäytetyössä pyritään avaamaan mitä eri aiheeseen liittyvät termit tarkoittavat ja avataan mitä asia tarkoittaa käytännössä.

ISO 27000 -standardisarjan lisäksi teoreettiseen viitekehyksen aiheet avaavat tietoturvallisuutta ja sen merkitystä yleisesti sekä tuodaan esiin mitä uhkia ja haitallisia toimia voi organisaatioon kohdistua, joissa voidaan hyödyntää teknisiä haavoittuvuuksia. Jotta opinnäytetyön terveydenhuoltoon liittyvää näkökulmaa ymmärrettäisiin, otettiin teoreettiseen viitekehykseen mukaan osiot, joissa tuodaan esiin mitä haavoittuvuuksia terveydenhuollon tietojärjestelmissä ja toimintaympäristössä voi olla. Lisäksi esitellään terveydenhuollon tietojärjestelmiä, jotta ymmärretään terveydenhuollon tietoteknistä ympäristöä ja miten sen tietoturvallisuutta säädellään.

Asiaa lähdettiin tutkimaan hakemalla teoriatietoa liittyen haavoittuvuuksien hallintaan. Tietoa aiheesta usein etsittiin internetistä hakusanoilla vulnerability management (haavoittuvuuksien hallinta), jolla löytyikin paljon eri lähteitä aiheeseen liittyen. ISO-standardiasiakirjat saatiin hankittua ilmaiseksi Hamk Finna-palvelun kautta, josta päästiin SFS-tietokantaan standardeja lataamaan. Eniten käytetyt standardit olivat ISO 27000, ISO 27001, ISO 27002 ja ISO 27005. Standardien tekstiä joutui usein avaamaan eri lähteistä, että mitä kyseinen asia tarkoittaa käytännössä. Samalla pyrittiin löytämään ns. parhaita käytäntöjä liittyen haavoittuvuuksien käsittelyyn tai toisin sanoen mitä haavoittuvuuksia kannattaa korjata/ paikata ensi sijassa. Tärkeä asia mikä nousi esiin, oli tunnistettujen haavoittuvuuksien käsittelyn priorisointi. Priorisointia hyödyntämällä pyritään arvioimaan ja

käsittelemään organisaatiolle suurimman uhan muodostavat haavoittuvuudet ennen kuin haitallinen toimija pääsee haavoittuvuutta hyväksikäyttämään. Priorisointi säästää lisäksi henkilöstön resursseja, kun ei yritetä korjata kaikkia haavoittuvuuksia, vaan kohdistetaan resurssit oikein haavoittuvuuksia ja niiden riskejä organisaation tietotekniseen ympäristöön verraten. Priorisoinnissa yleensä hyödynnetään lisäksi uhkatietoa maailmalta esim. onko haavoittuvuutta jo hyödynnetty joissain haitallisissa kybertoimissa.

Kun pohdimme HYVAEP:n tietoturvaryhmän jäsenten kanssa prosessin toteutusta niin melko alussa nousi esiin ajatus, että ei kannata keksiä pyörää kokonaan uudestaan, joka tarkoittaa, että prosessin suunnittelussa hyödynnettiin toimivia jo olemassa olevia prosesseja. Tarkoituksena oli kehittää prosessi, joka on käyttöönotettavissa ilman kovin suuria ponnisteluja ja prosessia voidaan kehittää sekä parantaa jatkuvasti.

Ryhmäkeskustelut olivat opinnäytetyössä varsinaisesti joukko työpajoja. Työpajat tuottivat selkeän tuloksen, koska puheenvuoroja ei varsinaisesta rajattu vaan kehotettiin muitakin keskustelemaan ja tuomaan esiin mielipiteitä aiheista. Kuusi kahden tunnin kokousvarausta oli melko tiukka ajallisesti, koska kaikki kutsutut eivät ehtineet aina olla mukana. Työpajoissa mukana olleet kokivat hyvänä tavan, jossa kokouksen alussa pidin päivän teemasta lyhyehkön teoriaesityksen. Työpajojen esityksiin pyrin ottamaan mukaan myös ns. hyviä ja huonoja puolia sekä menetelmiä. Ryhmäkeskustelut eli työpajat tuottivat liitteen 2 mukaisen teknisten haavoittuvuuksien hallintaprosessin, joka on organisaation käytänteisiin sopiva. Lisäksi hahmoteltiin ja tunnistettiin teknisten haavoittuvuuksien hallinnassa hyödynnettävät oleelliset omaisuuseräluettelot, joista on apua tunnistettaessa haavoittuvuuksia organisaation tietoteknistä ympäristöä. Työpajoissa myös onnistuttiin tunnistamaan ja listaamaan tietolähteet, joista voidaan saada ilmoituksia haavoittuvuuksista sekä tietolähteistä voidaan etsiä ennalta tietoa itsenäisesti.

Dokumenttianalyysin menetelmällä käytiin läpi tietoturvaan ja haavoittuvuuksien hallintaan liittyviä muistioita, artikkeleja, www-sivuja, kirjoja ja standardiasiakirjoja. Analysoiduista materiaaleista tuotettiin materiaalit työpajoihin, joiden pohjalta rakennettiin organisaatioon teknisten haavoittuvuuksien hallintaprosessi.

Visualisointi oli työpajoissa tärkeässä osassa teknisten haavoittuvuuksien hallintaprosessin hahmottelussa. Aluksi aloitimme kirjaamaan Excel-tiedostoon tietolähteitä, joista löytyy organisaatiolle tärkeää tietoa teknisistä haavoittuvuuksista. Samalla kirjattiin, että kuka on vastuussa tietolähteistä ja niiden päivittämisestä. Seuraavaksi työpajoissa syntyneen keskustelun mukaisesti piirsimme Microsoft Power Point -ohjelmalla raakaversiota prosessista, josta siirryimme melko pian Microsoft Visio -ohjelman käyttöön, koska Visio-ohjelmassa oli paremmat toiminnot visualisointiin. Visualisointi osoittautui toivotuksi ja tärkeäksi työkaluksi hahmottamaan prosessin suunnittelua ja luontia, koska siitä näki haavoittuvuuden hallinnan eri vaiheet yhdellä silmäyksellä ja teorian tukemana auttoi luomaan prosessin.

Toiminnallisen tutkimuksen spiraalimalli oli toimiva työpajojen toteutuksessa, koska työpajoissa edettiin usein keskustelemalla aiheesta, jolloin korostui havainnointi ja reflektointi. Havainnoinnin ja reflektoinnin perusteella pystyi valmistautumaan ja parantamaan seuraavan työpajan esityksiä ja materiaaleja.

Tuloksena työni tuotti tilaajalle tietoa ISO 27001 -standardin mukaisesta teknisten haavoittuvuuksien hallinnasta ja tietoturvallisuudesta yleisesti sekä teknisten haavoittuvuuksien hallintaprosessin (liite 2). Lisäksi tunnistimme ja luetteloimme organisaatiolle tärkeät tietolähteet haavoittuvuuksista sekä omaisuuseräluettelot, joista löytyy ajan tasainen tieto mm. laitteista, ohjelmistoista, järjestelmävastuista ja ohjelmistoversioista.

Teknisten haavoittuvuuksien hallintaprosessi on sellainen, että se on helposti jatkokehitettävissä, joka tarkoittaa sitä, että organisaatio voi tarvittaessa lisätä prosessiin uusia vaiheita tai toimintoja. Teknisten haavoittuvuuksien hallintaprosessin käyttöönotto tuottaa organisaatiolle parempaa tietoturvantasoa, koska tietojärjestelmien ja laitteiden haavoittuvuudet tunnistetaan systemaattisesti ja ennakoivasti. Haavoittuvuudet arvioidaan riskiperusteisesti, jossa otetaan huomioon organisaation tietotekninen ympäristö, jota verrataan haavoittuvuuden vaikuttavuuteen. Haavoittuvuudet otetaan käsittelyyn priorisoidusti.

Totesimme myös, että kaikki ISO 27002 -standardin teknisten haavoittuvuuksien hallintakeinon vaatimukset ja ohjeistukset eivät olleet organisaatiolle tarpeellisia ja niistä ei koettu saavan merkittävää hyötyä mm. Bug Bounty -ohjelma. Seuraavissa alaluvuissa, jotka ovat nimeltään 10.1. Teknisten haavoittuvuuksien tunnistamisvaihe, 10.2. Teknisten haavoittuvuuksien analysointivaihe, 10.3. Teknisten haavoittuvuuksien arviointivaihe ja 10.4. Teknisten haavoittuvuuksien käsittelyvaihe avataan Teknisten haavoittuvuuksien hallintaprosessi dokumentin (liite 2) vaiheet.

10.1 Teknisten haavoittuvuuksien tunnistamisvaihe

Teknisten haavoittuvuuksien hallintaprosessi (liite 2) alkaa haavoittuvuuksien tunnistamisvaiheella, jossa pyritään tunnistamaan haavoittuvuudet eri tietolähteistä. Työpajojen yhtenä tuotoksena luetteloimme tunnistetut organisaatiolle merkitykselliset tietolähteet organisaation käyttöön, joista yksi on Kyberturvallisuuskeskus. Eri tietolähteistä organisaatiolle voi tulla ilmoitus ulkoisen toimijan kautta tai haavoittuvuus tunnistetaan tietolähteistä omatoimisesti sisäisen toimijan puolesta. Lisäksi haavoittuvuuksien tunnistamiseen organisaation tietoteknisestä ympäristöstä hyödynnetään toistuvia ja suunniteltuja haavoittuvuusskannauksia, joista vastaa tunnistettu sisäinen toimija.

10.2 Teknisten haavoittuvuuksien analysointivaihe

Seuraavaksi haavoittuvuus tulee tunnistaa tai toisin sanoen analysoida. Analysointivaiheessa selvitetään, että onko organisaatiossa käytössä laitteita, järjestelmiä tai ohjelmistoja, joita tietolähteistä tunnistettu haavoittuvuus koskettaa. Jos analysointi tuottaa tuloksen, että haavoittuvuus koskettaa organisaatiota niin seuraavaksi edetään haavoittuvuuden arviointivaiheeseen. Jos tunnistettu haavoittuvuus ei kosketa organisaatiota, kuitataan tapahtuma valmiiksi. Analysointivaiheessa voidaan hyödyntää organisaation sisäisten ja ulkoisten toimijoiden osaamista ja tietoutta.

10.3 Teknisten haavoittuvuuksien arviointivaihe

Arviointivaiheessa selvitetään haavoittuvuuden kriittisyys eli arvioidaan riskit, jotka kohdistuvat organisaatioon. Haavoittuvuuden riskien arvioinnissa hyödynnetään CVSS-arvoa

ja organisaation omaa sisäistä järjestelmien kriittisyysluokittelua. Arvioinnissa on tärkeää huomioida myös haavoittuvuuden vaikuttavuus eli kuinka laajan uhan haavoittuvuus muodostaa organisaatioon, jos haavoittuvuutta onnistutaan hyväksikäyttämään. Arviointivaiheessa pyritään hyödyntämään priorisointia. Arviointivaiheessa pyritään päättämään haavoittuvuuden korjaukset/ paikkaukset tai jos korjausta ei ole saatavilla niin pohditaan joku muu hallintakeino, jolla haavoittuvuuden hyväksikäytön uhkaa voidaan pienentää. Jos haavoittuvuuteen ei ole saatavilla korjausta tai muuta hallintakeinoa ei voida toteuttaa, voidaan riski joutua hyväksymään. Arviointivaiheessa voidaan hyödyntää organisaation sisäisiä ja ulkoisia toimijoita.

10.4 Teknisten haavoittuvuuksien käsittelyvaihe

Arvioinnin kriittisyyden ja vaikuttavuuden tuloksena haavoittuvuuden käsittelyssä, joko hyödynnetään normaalia tukitoimintaprosessia, tietoturvapoikkeaman (tietoturvahäiriö) menettelyä tai muutoksenhallintaa. Haavoittuvuuden käsittelyssä on mukana useita sisäisiä ja ulkoisia tahoja. Sisäiset ja ulkoiset tahot on tunnistettu sekä tiedossa organisaatiolla eikä niitä tässä työssä avata sen enempää. Korjausten tai muiden hallintakeinojen vaikuttavuus tulisi aina todentaa. Lisäksi on tärkeää, että haavoittuvuuksien käsittelyssä on aikaraja, jonka sisällä varsinainen korjaus tai muu hallintakeino on toteutettu. Luodussa prosessissa hyödynnetään organisaation omia sisäisiä SLA:n (service level agreement) menettelyn aikoja.

Suunniteltu prosessi ja teknisten haavoittuvuuksien hallinnan merkittävyys on tärkeää perehdyttää henkilöstölle hyvin, joka taas tukee koko organisaation teknisten haavoittuvuuksien hallintaa ja parantaa sitä kautta teknistä tietoturvaa. Toki yhtä tärkeää on, että prosessin parissa toimivat henkilöt saavat koulutusta aiheeseen ja koulutus on toistuvaa.

Kokonaisuudessaan voisi todeta opinnäytetyön täyttäneen vaaditut tavoitteet eli vastattiin kaikkiin tutkimuskysymyksiin ja saatiin luotua tuotoksena teknisten haavoittuvuuksien hallinnan prosessikaavio, joka oli kehittämistyön tavoitteena. Luotua teknisten haavoittuvuuksien hallintaprosessia on helppo lähteä toteuttamaan ja laajentamaan tarvittaessa. Suosituksena organisaatiolle oli, että prosessilla olisi erilliset nimetyt vastuulliset, jotka panostaisivat prosessin kokonaisuuden seurantaan ja kehittämiseen.

Opinnäytetyön tilaajan palaute työstä oli, että opinnäytetyön rakenne oli selkeä ja siinä avataan eri käsitteet sekä niiden erot selkeästi. Työpajamallia, jossa asiantuntijat kerättiin yhteisen pöydän ääreen, pidettiin tehokkaana tapana suunnitella ja pohtia teknisten haavoittuvuuksien hallinnan prosessia. Hyvänä pidettiin työpajoissa suunnittelun tueksi annettua teoriatietoa. Tilaaja piti opinnäytetyön aihetta ajankohtaisena ja tärkeänä organisaation tietoturvallisuuden kehittämisessä. Opinnäytetyötä ja sen tuotoksena valmistunutta haavoittuvuuksien hallintaprosessia pidettiin helpottavana tekijänä ajatellen prosessin käyttöönottoa ja tietoturvallisuuden kehittämistä organisaatiossa. Tilaajan ja opinnäytetyön kirjoittajan välisen kommunikoinnin todettiin olleen onnistunutta. Lisäksi tilaajalle oli ilmennyt opinnäytetyön kirjoittajan tietoturvallisuuden asiantuntemus, joka oli selkeästi nähtävissä hyvin valmistellusta työstä. Kokonaisuudessaan opinnäytetyö vastasi tilaajan odotuksia.

11 Yhteenveto

Tässä opinnäytetyössä opin lukemaan tietoturvallisuuteen liittyviä standardeja tarkemmin ja ymmärsin niiden edellyttämät vaatimukset sekä ohjeistukset paremmin. Työssäni opin myös, että isohkon organisaation vakiintuneet käytänteet eivät ole niin helposti muutettavissa ja se vaatii aikaa sekä lisää resurssia toteuttamaan uusia toimintatapoja.

Tutkimuskysymyksiin vastaaminen onnistui kaiken kaikkiaan hyvin. Tutkimuksen tarkoitus oli vastata kolmeen kysymykseen. Ensimmäinen tutkimuskysymys oli: Kuinka teknisten haavoittuvuuksien hallinta toteutetaan ISO 27001 -standardin mukaisesti? Tutkimuskysymykseen vastaamiseen ISO 27001 -standardista selvisi, että liitteen A hallintakeinot, joista teknisten haavoittuvuuksien hallinta on yksi, hallintakeinojen olevan ns. suosituksia ja organisaatio voi ottaa ne käyttöön sellaisenaan, muokata niitä tai muodostaa omat organisaatiolle sopivat hallintakeinot. Liitteen A hallintakeinot ovat kehitetty auttamaan ja tehostamaan tietoturvariskien käsittelyä. Vaikka organisaatio päätyisikin toteuttamaan omat hallintakeinot niin tulee ne miettiä aina tietoturvariskeihin pohjaten.

Toinen tutkimuskysymys oli: Millä työtavoilla saamme toteutettua ISO 27001 mukaisen teknisten haavoittuvuuksien hallintaprosessin? Tutkimuskysymykseen vastaamiseen hyödynnettiin työtapoina dokumenttianalyysia, ryhmäkeskustelua ja visualisointia, jotka auttoivat pääsemään tavoitteeseen.

Kolmas tutkimuskysymys oli: Miten saamme toteutettua organisaatiolle toimivan ISO 27001 mukaisen teknisten haavoittuvuuksien hallintaprosessin? Tutkimuskysymykseen vastaamiseen hyödynnettiin hankitun teoriatiedon lisäksi työpajoissa mukana olleiden henkilöiden tietoutta tietohallinnon prosesseista, tietoturvallisuudesta ja teknisestä osaamista sekä hyödynnettiin tietohallinnon osittain jo olemassa olevia prosesseja ja toimintamalleja.

Tulevaisuudessa prosessia voisi kehittää paremmaksi ja mahdollisesti ottaa mukaan uusia menetelmiä, joita ISO 27002 -standardissa suositeltiin teknisten haavoittuvuuksien hallintakeinon osalta esim. Bug Bounty. Osa menetelmistä jätettiin pois, koska niistä ei koettu saavan merkittävää hyötyä verraten nykytilanteeseen.

Lähteet

Aboud, J. (27.4.2020). *Why You Need to Stop Using CVSS for Vulnerability Prioritization*. Tenable. https://www.tenable.com/blog/why-you-need-to-stop-using-cvss-for-vulnerability-prioritization

Baker, K. (28.2.2023). *THE 12 MOST COMMON TYPES OF MALWARE*. Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

Barros, A. (25.10.2019). *The New Vulnerability Management Guidance Framework.* Gartner. https://blogs.gartner.com/augusto-barros/2019/10/25/new-vulnerability-management-guidance-framework/

Chai W. (1.2.2023) *What is the CIA Triad?.* Haettu 26.2.2023 osoitteesta https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Crowdstrike. (12.10.2022.-a). *VULNERABILITY MANAGEMENT?.* Haettu osoitteesta 1.3.2023 https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/

Crowdstrike. (12.10.2022.-b). *VULNERABILITY MANAGEMENT LIFECYCLE.* https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/vulnerability-management-lifecycle/

Crowdstrike. (20.12.2021.-c). *WHAT IS RISK BASED VULNERABILITY MANAGEMENT?*. https://www.crowdstrike.com/cybersecurity-101/risk-based-vulnerability-management/

Crowdstrike. (28.2.2023.-d). *Threat actor.* https://www.crowdstrike.com/cybersecurity-101/threat-actor/

CVE. (n.d.). *About the CVE Program.* https://www.cve.org/About/Overview

CVE Mitre. (n.d.). *CVE-2023-28206*. Haettu osoitteesta 15.4.2023 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28206

Dataguard. (25.5.2022). *Information Security Management System: What it does and who needs it.* Haettu 26.2.2023 osoitteesta https://www.dataguard.co.uk/blog/information-security-management-system-what-it-does-and-who-needs-it

Enisa. (3.11.2022). *Threat Landscape 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Etelä-Pohjanmaan hyvinvointialue. (n.d.). *Hyvinvointialue*. Haettu osoitteesta 19.6.2023 https://www.hyvaep.fi/hyvinvointialue/

Fortra. (9.11.2021). *Data Privacy vs. Data Security: What's the Difference?.* https://www.fortra.com/blog/data-privacy-vs-data-security-whats-difference

Imperva. (n.d.). *Cyber Security Threats.* https://www.imperva.com/learn/application-security/cyber-security-threats/

Intellfence. (7.6.2021). *What is the difference between Information Security and Data privacy?*. https://www.intellfence.com/what-is-the-difference-between-information-security-and-privacy/

Irwin L. (19.10.2020). *What is the ISO 27000 series of standards?.* IT Governance. https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards

Kaspersky. (n.d.-a). *Vulnerability Exploits & Malware Implementation Techniques.* Haettu osoitteesta 9.7.2023 https://www.kaspersky.com/resource-center/threats/malware-implementation-techniques

Kaspersky. (11.5.2023.-b). *CVE-2023-28252 zero-day vulnerability in CLFS.* https://www.kaspersky.com/blog/nokoyawa-zero-day-exploit/47788/

Kyberturvallisuuskeskus. (20.8.2019.-a). *Bug Bounty -ohjelmien avulla tietoturvaongelmat voi kääntää PR-voitoiksi.* Traficom Liikenne- ja viestintävirasto. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/bug-bounty-ohjelmien-avulla-tietoturvaongelmat-voi-kaantaa-pr-voitoiksi

Kyberturvallisuuskeskus. (11.4.2023.-b). *Kriittisiä haavoittuvuuksia Applen tuotteissa - päivitä heti*. Traficom Liikenne- ja viestintävirasto. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_5/2023

Kyberturvallisuuskeskus. (n.d.-c). *Haavoittuvuudet*. Traficom Liikenne- ja viestintävirasto. Haettu osoitteesta 13.4.2023 https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet?limit=20&offset=0&query=&sort=updated

Kyberturvallisuuskeskus. (n.d.-d). *Kyberturvallisuuskeskuksen viikkokatsaus - 13/2023*. Traficom Liikenne- ja viestintävirasto. Haettu osoitteesta 13.4.2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-132023

Kyberturvallisuuskeskus. (n.d.-e). *Kybersää*. Traficom Liikenne- ja viestintävirasto. Haettu osoitteesta 13.4.2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa

Kyberturvallisuuskeskus. (n.d.-f). *Tilaa uutiskirjeitä*. Traficom Liikenne- ja viestintävirasto. Haettu osoitteesta 13.4.2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita

Kyberturvallisuuskeskus. (n.d.-g). *Terveydenhuoltoalan kyberuhkia*. Traficom Liikenne- ja viestintävirasto. Haettu osoitteesta 19.7.2023 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Terveydenhuoltoalan_kyberuhkia.pdf

Laurio, J-M. (14.10.2014). *HAAVOITTUVUUDEN VAKAVUUDEN LUOKITTELU LÄHTEE CVSS-ARVOSTA*. Nixu. https://www.nixu.com/fi/blog/haavoittuvuuden-vakavuuden-luokittelu-lahtee-cvss-arvosta

Limnéll, J., Klaus, M. & Salminen, M. (2014). *Kyberturvallisuus*. Docendo.

Puusa, A. & Juutti, P. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Gaudeamus.

National Cyber Security Centre. (14.10.2015.-a). *Understanding vulnerabilities.* Haettu osoitteesta 24.3.2023 https://www.ncsc.gov.uk/information/understanding-vulnerabilities

National Cyber Security Centre, (8.8.2017.-b). *Penetration Testing*. Haettu osoitteesta 27.3.2023 https://www.ncsc.gov.uk/guidance/penetration-testing

NIST NVD. (10.4.2023.-a). *CVE-2023-28206 Detail*. https://nvd.nist.gov/vuln/detail/CVE-2023-28206

NIST NVD. (n.d.-b). *Common Vulnerability Scoring System Calculator*. Haettu osoitteesta 19.7.2023 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Nixu. (7.10.2014). *CVE – HAAVOITTUVUUSMAAILMAN KOLME TÄRKEÄÄ KIRJAINTA*. https://www.nixu.com/fi/blog/cve-haavoittuvuusmaailman-kolme-tarkeaa-kirjainta

O'Sullivan, S., Davis, C., Simpson, D., Lobo, A. & Savell, S. (8.3.2023). *What is Microsoft Defender Vulnerability Management*. Microsoft. https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide#risk-based-intelligent-prioritization

Rapid 7. (n.d.-a). *Vulnerability Management Process*. Haettu osoitteesta 26.3.2023 https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/

Rapid 7. (n.d.-b). *Patch Management Definition & Best Practices*. Haettu osoitteesta 2.4.2023 https://www.rapid7.com/fundamentals/patch-management/

Rousku K. (2014). *Kyberturvaopas*. *Tietoturvaa kotona ja työpaikalla.* Talentum.

SFS-EN ISO 27000:2022. (2022). *Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto.* SFS Online.

SFS-EN ISO 27001:2022. (2022). *Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.* SFS Online.

SFS-EN ISO 27002:2022. (2022). *Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot.* SFS Online.

SFS-EN ISO 27005:2018. (2018). *Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta.* SFS Online.

Souppaya, M. & Scarfone, K. (1.4.2022). *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology.* NIST SP 800-40r4. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

Tai, W. (16.4.2020). *What Is VPR and How Is It Different from CVSS?.* Tenable. https://www.tenable.com/blog/what-is-vpr-and-how-is-it-different-from-cvss

Threat Intelligence. (10.3.2023). *Secure Code Reviews: What is it, Benefits and Checklist.* https://www.threatintelligence.com/blog/secure-code-reviews

Tietohallinto. (n.d.). *Tietohallinto.* Haettu osoitteesta 17.7.2023 https://www.epshp.fi/sairaanhoitopiiri/tuki-_ja_hallintopalvelut/tietohallinto

Tietosuojavaltuutetun toimisto. (n.d.-a). *Mikä on henkilötieto?.* Haettu osoitteesta 17.7.2023 https://tietosuoja.fi/mika-on-henkilotieto

Tietosuojavaltuutetun toimisto. (n.d.-b). *Tietosuojavaltuutetun toimisto valvoo tietosuojaoikeuksiasi.* Haettu osoitteesta 17.7.2023 https://tietosuoja.fi/tietosuojavaltuutetun-toimisto

Tietosuojavaltuutetun toimisto. (n.d.-c). *Usein kysyttyä EU:n tietosuoja-asetuksesta.* Haettu osoitteesta 17.7.2023 https://tietosuoja.fi/gdpr

Toikko, T. & Rantanen, T. (2009). *Tutkimuksellinen kehittämistoiminta. 3. korjattu painos.* [Tampereen Yliopistopaino Oy – Juvenes Print]. https://urn.fi/URN:ISBN:978-951-44-7732-4

Tori Sitcawich. (14.9.2020.-c). *Vulnerability Remediation vs. Mitigation: What's the Difference?*. Rapid 7. Haettu osoitteesta 2.4.2023 https://www.rapid7.com/blog/post/2020/09/14/vulnerability-remediation-vs-mitigation-whats-the-difference/

Vangel, D., Jupudi, A. & Athavale, M. (28.9.2022). *Use your vulnerability management dashboard in Microsoft Defender for Business.* Microsoft. https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-view-tvm-dashboard?view=o365-worldwide

Valvira. (n.d.-a). *Asiakastietolain mukaiset sosiaali- ja terveydenhuollon tietojärjestelmät.* Haettu 25.6.2023 osoitteesta https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat

Valvira. (n.d.-b). *Tietojärjestelmien luokittelu.* Haettu osoitteesta 19.7.2023 https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat/tietojarjestelmien-luokittelu

Vuorinen, S. (23.5.2019). *Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille.* Sosiaali- ja terveysministeriö. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161683/J14_Kyberturvallisuus_WEB.pdf?sequence=1&isAllowed=y

Liite 1: Aineistonhallintasuunnitelma

Opinnäytetyön aineisto koostuu esityksistä työpajoihin, työpajojen muistiot, luonnostelut prosessista ja lopuksi valmis prosessiluonnostelma. Tiedot talletetaan eri tiedostoihin, joita säilytetään HAMK:in henkilökohtaisessa OneDrive-verkkopalvelussa. Tietojen varmuuskopiointi tehdään säännöllisesti ulkoiselle tallennusvälineelle, jota säilytetään lukitussa tilassa.

Työssä huolehditaan mahdollisista luottamuksellisten ja arkaluonteisten tietojen suojasta. Aineistot, joissa käsitellään organisaation mahdollisesti arkaluontoista tietoa, säilytetään organisaation verkkoasemalla, johon on pääsy vain tietoon oikeutetuille henkilöille.

Opinnäytetyössä jätetään julkaisematta organisaatiosta yksilöiviä tunnistettavia tietoja henkilöistä, laitteistoista tai järjestelmistä, kuten palvelimien nimet tai IP-osoitteet.

Työssä julkaistut kuvat ovat joko omia tai otettu julkisista lähteistä ja niihin viitataan työssä oikeaoppisesti.

Opinnäytetyön tekijä säilyttää aineiston tietoturvallisesti vuoden ajan opinnäytetyön hyväksymispäivästä, jotta opinnäytetyön tulokset voidaan tarvittaessa varmistaa ja hävittää tämän jälkeen aineiston tietoturvallisesti.

Liite 2: Teknisten haavoittuvuuksien hallintaprosessi