HAMK
Hämeen ammatti-
korkeakoulu

Kyberturvallisuuden hallintajärjestelmä

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus

Kevät 2024

Silja Markku

HAMK
Hämeen ammatti-
korkeakoulu

Tietojenkäsittelyn koulutus
Tekijä Silja Markku
Työn nimi Kyberturvallisuuden hallintajärjestelmä
Ohjaaja Ismo Turve

Tiivistelmä
Vuosi 2024

Opinnäytetyön aiheena on kyberturvallisuuden hallintajärjestelmän tutkiminen ja kehittäminen. Tutkimuksen päämääränä oli syventyä kyberturvallisuuden käsitteisiin, standardeihin, sekä luoda käytännöllinen pieni Excel pohjainen prototyyppi hallintajärjestelmästä. Lisäksi arvioitiin kyberturvallisuuden hallintajärjestelmän merkitystä organisaation toiminnassa. Tässä opinnäytetyössä toteutettu hallintajärjestelmä on suunnattu pienille yrityksille, joilla ei välttämättä ole erillistä IT-osastoa. Tutkimuksen toteutuksessa ei ole mukana ulkoista toimeksiantajaa.

Opinnäytetyössä syvennyttiin aluksi kyberturvallisuuden peruskäsitteisiin, käyden läpi yleisimmät hyökkäystyypit, kyberhyökkäyksen elinkaari, sekä yleisimmät uhkatekijät. Lisäksi tarkasteltiin kattavasti riskienhallinnan perusteita, ja hallintajärjestelmän määritelmää. Tutkimuksen tietopohja rakentui laajasti verkkojulkaisuista, artikkeleista, blogikirjoituksista, dokumenteista ja eri alan standardeista. Tutkimusmenetelmänä käytettiin teoriapohjaista analyysia sekä kyberturvallisuuden ammattilaisen haastattelua. Opinnäytetyö toteutettiin tutkimuksellisena kokonaisuutena.

Tutkimuksessa havaittiin hallintajärjestelmän tuomat hyödyt organisaatiolle, sekä hallintajärjestelmän roolin tärkeys osana strategiaa. Tutkimuksen päätelmänä voidaan todeta, että kyberturvallisuuden hallintajärjestelmä on olennainen tekijä liiketoiminnan jatkuvuuden tukemisessa ja auttaa organisaatioita pysymään ajan tasalla oman kyberturvallisuutensa tilanteesta.

Avainsanat Kyberturvallisuus, riskienhallinta, tietoturvakäytännöt, kyberturvallisuuden hallintajärjestelmä

Sivut 62 sivua ja liitteitä 2 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Degree Programme in Business Information Technology
Author Silja Markku
Subject Cybersecurity Management System
Supervisors Ismo Turve

Abstract
Year 2024

This thesis focuses on investigating and refining a cybersecurity management system. The aim of this research was to explore the fundamental concepts and standards within cybersecurity and to craft a pragmatic, scaled-down Excel prototype of the management system. Furthermore, an evaluation was conducted on the importance of the cybersecurity management system within organizational functions. The system developed in this thesis caters specifically to small businesses that lack a dedicated IT department. It's important to note that there was no external commissioning party involved in overseeing the research process.

The thesis embarked on an exploration of fundamental cybersecurity concepts, addressing prevalent attack types, the lifecycle of cyberattacks, and emerging threats. Additionally, this thesis conducted an in-depth analysis of risk management fundamentals and the conceptual framework of a management system. Drawing extensively from a diverse array of sources including online publications, articles, blog posts, documents, and industry standards, the research established a robust knowledge base. Methodologically, the study employed a combination of theory-based analysis and interviews with cybersecurity experts. It is essential to note that the thesis was executed as a research endeavor.

In this thesis, the benefits brought by the management system to the organization were observed, as well as the importance of the management system's role as part of the strategy. As a conclusion of the research, it can be stated that a cybersecurity management system is an essential factor in supporting business continuity and helps organizations stay updated on their cybersecurity status.

Keywords Cyber security, risk management, security practices, threat assessment, cyber security management system

Pages 62 pages and appendices 2 pages

Sanasto

Kyberturvallisuus

Kyberturvallisuus käsittää erilaisia toimenpiteitä, käytäntöjä ja teknologioita, joita käytetään suojaamaan dataa, verkkoja ja ohjelmistoja digitaalisessa ympäristössä.

Haavoittuvuus

Kyberturvallisuuden kontekstissa haavoittuvuus viittaa tietojärjestelmän tai ohjelmistojen heikkouteen, joka voi altistaa organisaation kyberhyökkäykselle.

Kyberhyökkäys

Kyberhyökkäys on yritys hyödyntää tietojärjestelmiä- ja verkkoja, tai niihin liittyvää teknologiaa häirintätarkoituksessa.

Kyberturvallisuuden hallintajärjestelmä

Kyberturvallisuuden hallintajärjestelmä on kokonaisuus, joka käsittää prosesseja, resursseja, käytänteitä, sekä toimenpiteitä, joilla varmistetaan organisaatiolle tehokas kyberturvallisuus.

Riskienhallinta

Riskienhallinta on prosessi, jonka avulla organisaatio tunnistaa, arvioi ja valvoo kyberturvallisuuteen liittyviä riskejä.

Tietoturva- ja uhkakartoitus

Uhkakartoitus on prosessi, jonka avulla voidaan arvioida sekä tunnistaa mahdolliset riskit, jotka vaikuttavat organisaation tietoturvaan.

ISO 27001

ISO 27001 on kansainvälinen standardi, joka määrittelee vaatimuksen kyberturvallisuuden hallintajärjestelmälle. Standardi oheistaa suunnittelussa, toteutuksessa ja ylläpidossa.

NIST Cybersecurity framework

National Institute of Standards and Technology:n kehittämä tietoturvakehys. Kehys tarjoaa välineitä ja suosituksia Kyberturvallisuuden hallintaan.

PiTuKri

Pilvipalveluiden turvallisuuden arviointikriteeristö, josta lyhenne PiTuKri, on työkalu pilvipalveluiden turvallisuuden arviointiin.

GDPR

Yleinen tietosuoja-asetus (General Data Protection Regulation) on Euroopan Unionin asetus, joka astui voimaan 2016, ja jonka soveltaminen alkoi 25 toukokuuta 2018. GDPR on

yhtenäinen tietosuojakehys EU:n jäsenvaltioille, ja se koskee jokaista organisaatioita, joka käsittelee henkilötietoja.

Nollapäivähaavoittuvuus

Nollapäivähaavoittuvuudeksi kutsutaan sellaista haavoittuvuutta järjestelmässä, johon ei ole löytynyt vielä paikkausta.

IoT-laite

Internet of Things, eli esineiden internet. IoT-laitteet ovat nettiin yhdistettyjä laitteita, kuten älykelloja, autoja tai jääkaappeja. Internetin välityksellä laitteet jakavat tietoa toisilleen.

Haktivisti

Haktivistiksi luokitellaan henkilö, tai ryhmä, joka käyttää tietoverkkoja poliittisten, sosiaalisten tai ideologisten tavoitteiden edistämiseen tai ilmaisemiseen.

APT ryhmä

Advanced Persistent Threat- ryhmät ovat järjestäytyneitä kyberuhkatekijöitä, joilla on tietotaitoa ja resursseja suorittaa edistyneitä kyberhyökkäyksiä.

SWOT-analyysi

SWOT koostuu sanoista strengths, weaknesses, opportunities ja threats. Analyysin avulla voidaan tunnistaa edellä mainittuja projekteissa tai työtehtävissä.

Incident response process

Häiriötilanteisiin reagoinnin prosessi sisältää häiriön havaitsemisen, reagoimisen, sekä tilanteesta toipumisen.

Tietoturvakäytännöt

Tietoturvakäytännöt tarkoittavat prosesseja, toimenpiteitä tai muita toimintatapoja, joilla suodataan järjestelmiä, verkkoja, tietoja tai muuta dataa.

Sisällys

1 Johdanto 1

2 Kyberturvallisuus ja sen merkitys 2

2.1 Kyberturvallisuuden perusteet 2

2.1.1 Uhat ja haavoittuvuudet 3

2.1.2 CIA Triad 4

2.1.3 Kyberhyökkäyksen määritelmä 5

2.1.4 Kyberhyökkäyksen vaiheet 6

2.1.5 APT-ryhmät 8

2.2 Hyökkäystyypit 9

2.2.1 Haittaohjelmat 9

2.2.2 Tietojenkalastelu 11

2.2.3 Nollapäivähaavoittuvuus 11

2.2.4 Man-in-the-Middle hyökkäys 11

2.2.5 Palvelunestohyökkäys 12

2.2.6 SQL-injektio 12

2.2.7 Käyttäjän manipulointi 13

2.2.8 IoT-laitteet 13

2.2.9 Kyberterrorismi ja kybersodankäynti 13

2.2.10 Kyberhyökkäyksen seuraukset 14

2.3 Riskienhallinta 16

2.3.1 Riskienhallinnan perusteet 17

2.3.2 Haavoittuvuuksien ja uhkien tunnistaminen sekä arviointi 17

2.3.3 SWOT-analyysi 19

2.3.4 Riskien tunnistaminen ja arviointi 21

2.3.5 Riskien hallintatoimenpiteet 24

2.3.6 Incident response process 26

2.3.7 Tiedonhallinta 27

3 Kyberturvallisuuden hallintajärjestelmä 28

3.1 ISO 27001:2023 28

3.2 ISO 27002:2022 29

3.3 NIST Cybersecurity Framework version 1.1 29

3.4 PiTuKri 30

3.5 Parhaat tietoturvakäytännöt 31

3.5.1 Vahva pääsynhallinta 32

3.5.2 Tietojen salaaminen ja eheys 32
3.5.3 Jatkuvuuden hallinta 33
3.5.4 Henkilökunnan koulutus 34
3.5.5 Järjestelmien ja ympäristöjen suojaaminen 35
3.5.6 Fyysinen turvallisuus 36
4 Kyberturvallisuuden hallintajärjestelmä organisaatiossa 37
4.1 Kyberturvallisuuden hallintajärjestelmän edut 37
4.2 Kyberturvallisuuden hallintajärjestelmän käyttöönotto 37
4.3 Henkilöstön sitouttaminen ja strategian suunnittelu 38
4.4 Prototyyppi hallintajärjestelmästä 39
5 Tulokset ja pohdinta 42
6 Yhteenveto 43
Lähteet 44

Kuvat, komennot, ohjelmakoodit, taulukot ja kaavat

Kuva 1 CIA Triad (Singh 2021) 4

Kuva 2 Cyber Kill Chain (Lockheed Martin, n.d.) 7

Kuva 3 SWOT-analyysi (Thinkcurity, n.d.) 20

Kuva 4 Kuinka arvioida kyberturvallisuuden riskejä (Knowles, 2024) 23

Kuva 5 Esimerkki riskirekisteristä (Hyperproof Team, 2023) 26

Taulukko 1 Uhkien tunnistaminen ja arviointi (Stine & Quinn & Witte & Gardner, 2020 s.14–16) 18

Taulukko 2 Riskin todennäköisyyden laskeminen asteikolla 1–5 (Cobb, 2024) 22

Liitteet

Liite 1. Aineistonhallintasuunnitelma

Liite 2. Haastattelukysymykset

1 Johdanto

Digitaalisen maailman kasvun myötä organisaatiot ja yritykset ovat entistä alttiimpia monenlaisille kyberuhille. Yritysten palveluiden kasvaessa myös kyberturvallisuus ja sen merkitys korostuu. Tietoturvaongelmat, kuten haittaohjelmat, tietovuodot ja murrot, vaativat tehokkaita käytänteitä, joiden avulla voidaan suojata organisaation arkaluontoisia tietoja ja varmistaa liiketoimintaprosessien jatkuvuus. Digitaalisten uhkien skaala on laaja, ja organisaatiot ovat alttiita niin tarkoituksellisille hyökkäyksille, kuin sattumanvaraisille uhille. Kyberturvallisuuden tulisi kytkeytyä tiiviisti organisaation kulttuuriin, ja toimintaan.

Tämän opinnäytetyön tarkoituksena on tutkia kyberturvallisuuden hallintajärjestelmän roolia pienyritysten tietoturvan parantamisessa. Tutkimus keskittyy hallintajärjestelmän suunnitteluun ja tehokkuuden arviointiin pienen organisaation kontekstissa. Keskeisenä lähtökohtana on ymmärtää kyberturvallisuuden peruskäsitteitä ja tarkastella kyberturvallisuuden merkitystä. Opinnäytetyössä käydään läpi myös lyhyesti erilaisia kyberturvallisuuden standardeja, jotka tarjoavat ohjeita kyberturvallisuuden parantamiseen, sekä hyviin käytäntöihin. Tutkimus kartoittaa erilaisia uhkia, ja riskejä, sekä siten miten niiltä voidaan parhaiten suojautua. Tarkoituksena on tarjota kattavasti tietoa kyberturvallisuuden aiheista, sekä antaa näkökulmaa kyberturvallisuuden hallintajärjestelmän suunnitteluun ja toteutukseen, sekä tarjoamaan parannusehdotuksia turvallisuuskäytäntöihin.

Opinnäytetyössä pyritään osoittamaan, että kattavalla ja ennakoivalla kyberturvallisuuden hallintajärjestelmällä organisaatiot voivat suojata arvokkaita tietojaan ja varmistaa liiketoiminnan sujuvuuden digitalisoidussa toimintaympäristössä. Tutkimuksen tuloksia voidaan hyödyntää varsinkin niissä pienyrityksissä, joilla ei välttämättä ole erillistä IT-osastoa. Opinnäytetyön tarkoituksena on tuottaa käytännönläheistä tietoa, sekä suosituksia, jotka ovat helposti ymmärrettävissä ja toteutettavissa. Tutkimuksen tarkoituksena on tuoda kyberturvallisuus helposti lähestyttäväksi, ja painottaa sen tärkeyttä.

Opinnäytetyössä vastataan seuraaviin tutkimuskysymyksiin:

- Miten riskejä voidaan kartoittaa?
- Miten riskeiltä suojaudutaan?
- Mitkä ovat parhaat tietoturvakäytännöt?
- Mikä on kyberturvallisuuden hallintajärjestelmä?

2 Kyberturvallisuus ja sen merkitys

Kyberturvallisuus käsittää käytänteitä, teknologioita ja prosesseja, joilla suojellaan digitaalisessa ympäristössä olevia ohjelmistoja, dataa sekä tietoverkkoja, mutta myös fyysisiä laitteistoja. Kyberturvallisuuteen liittyy ennakoivien toimenpiteiden toteuttaminen tietojen suojaamiseksi hyökkäyksiltä, häiriöiltä ja muilta vaaroilta. Vahva strategia kyberturvallisuudessa takaa yritykselle nopean toipumisen häiriötilanteesta, palautumisen normaalitilanteeseen, sekä toiminnan jatkuvuuden. (Goutam 2021). Kyberturvallisuuden ja tietoturvan pääasiallinen ero piilee siinä, että kyberturvallisuus keskittyy suojaamaan digitaalista ympäristöä, kun taas tietoturva kattaa laajemmin tiedon turvaamisen. Tietoturvaan kuuluu myös fyysisen datan ja laitteiston turvaaminen. Kyberturvallisuus ja tietoturva ovat kuitenkin arkikielessä muovautuneet tarkoittamaan samaa asiaa. (F-Secure, n.d. a)

Internetin kasvaneen käyttäjämäärän myötä myös kyberrikollisuus on kasvanut. Kyberrikollisuus on kansainvälinen ongelma, sillä se ei tunne maiden välisiä rajoja. Jatkuvasti kasvavassa ja muuttuvassa digitaalisessa ympäristössä on varastoituna valtavasti dataa, ja suurin osa siitä on arkaluontoista. Vaikka omaa organisaatiotaan ei pitäisi kyberrikollisten mielestä merkittävänä, tämä ei tarkoita, ettei voisi joutua rikollisten kohteeksi. Tieto on rikollisille arvokasta valuuttaa. (Goutam, 2021)

Kyberrikolliset, toiselta nimitykseltään verkkorikolliset ovat usein yksittäisiä toimijoita, joskin suurempien hyökkäyksien takana saattaa olla järjestäytynyttä rikollisuutta. Kohteet rikollisille saattavat valikoitua sattumanvaraisesti, sillä toimijoilla on yleensä käytössään automatisoituja hyökkäysprosesseja, joita hyödyntämällä he etsivät verkosta jatkuvasti haavoittuvia ohjelmistoja. Hyökkääjillä ei välttämättä myöskään ole mitään merkittäviä motiiveja, useimmat vain kokeilevat erilaisten työkalujen toimintaa, tietämättä täysin itsekään, mitä työkalut tekevät. (F-Secure n.d. a)

Riittämättömät toimet koskien oman organisaation kyberturvaa voivat johtaa merkittäviin taloudellisiin menetyksiin, mainehaittaan, arkaluontoisten tietojen vaarantumiseen tai katoamiseen, tai pahimmassa tapauksessa jopa koko organisaation kaatumiseen. (F-Secure n.d. a)

2.1 Kyberturvallisuuden perusteet

Digitalisaation edetessä kyberturvallisuudesta on tullut kriittinen osa liiketoiminnan suunnittelua ja toteutusta. Jatkuvasti digitalisoituva ympäristö ja sen mukana tulleet

järjestelmät luovat uusia mahdollisuuksia, mutta samalla myös merkittäviä ja huomioonotettavia riskejä. Yhä yleistyvät ja monimutkaistuvat kyberuhat, ja uhkatekijät nostavat tarpeen kehittää organisaation kyberturvallisuutta, jotta hyökkäyksiltä voidaan suojautua riittävästi. Tämän luvun tavoitteena on antaa katsaus kyberturvallosuuden perusteisiin, ja syventää ymmärrystä kyberturvallisuuden käsitteistä.

2.1.1 Uhat ja haavoittuvuudet

Kyberuhka tarkoittaa mahdollista riskiä, jonka tarkoituksena on vahingoittaa tai häiritä tietojärjestelmiä, tai verkkoja. Kyberuhat koostuvat usein järjestelmien tai verkkojen haavoittuvuuksista, joita hyödyntämällä rikolliset voivat päästä käsiksi organisaation tietoihin. Kyberuhat voivat ilmetä erilaisina toimintoina, kuten tietomurtoina- ja vuotoina, haittaohjelmina tai palvelunestohyökkäyksinä. Uhkatekijöiksi mielletään henkilöt tai ryhmät, jotka uhkaavat kyberturvallisuutta toiminnallaan. (Johnson, Badger, Waltermire, Snyder & Skorupka, 2016, s. 10)

Haavoittuvuus tarkoittaa mitä tahansa heikkoutta järjestelmässä, jota hyödyntämällä rikolliset voivat mahdollistaa vahingon toteutumisen, kuten järjestelmään murtautumisen. Järjestelmien haavoittuvuuksia etsitään jatkuvasti laitevalmistajien sekä kehittäjien, mutta myös verkkorikollisten toimesta. Haavoittuvuuksia voi ilmetä esimerkiksi tietojärjestelmissä, sovelluksissa, laitteissa, tietokannoissa tai vanhentuneissa ohjelmistoversioissa. Haavoittuvuuksien etsintä on jatkuvaa kilpajuoksua verkkorikollisten ja kehittäjien kesken. (SecurityScorecard, 2021a)

Yleisimpiä haavoittuvuuksia järjestelmissä ovat vanhentuneet käyttöjärjestelmäversiot, heikot salasanat, huonosti konfiguroidut järjestelmät, kuten esimerkiksi palomuuri, huonosti suojattu data, monivaiheisen tunnistautumisen puuttuminen, riittämätön pääsynhallinta, sekä huonosti suojatut IoT-laitteet. Näitä heikkouksia käyttäen hyökkääjät voivat päästä käsiksi järjestelmään ja tietoihin. Joskus hyökkääjät pääsevät hyödyntämään sellaista haavoittuvuutta, joka ei ole vielä yleisessä tiedossa. Nollapäivähaavoittuvuudeksi kutsutaan siis sellaista haavoittuvuutta, johon ei ole löydetty paikkausta. Verkkorikolliset voivat helposti käyttää nollapäivähaavoittuvuuksia hyväkseen, sillä nämä eivät välttämättä ole kehittäjien tiedossa, ja haavoittuvuuden hyödyntämiseen ei olla osattu varautua. (SecurityScorecard, 2021a)

2.1.2 CIA Triad

CIA Triad on kyberturvallisuuden malli tai käsite, joka on koostuu keskeisistä huomioonotettavista periaatteista yrityksen kyberturvallisuutta suunnitellessa. CIA koostuu sanoista Confidentiality, eli luottamuksellisuus, Integrity eli eheys, ja Availability eli saatavuus. CIA Triad tarjoaa kolme keskeisintä periaatetta kyberturvallisuuden suunnitteluun sekä arviointiin (kuva 1). (Fortinet, n.d. a)

Kuva 1 CIA Triad (Singh 2021)

CIA Triadissa kuvatun luottamuksellisuuden (Confidentiality) tarkoituksena on varmistaa, että yrityksellä on riittävä yksityisyyden taso tietoja käsiteltäessä ja säilytettäessä. Datan tulee olla suojattu niin, etteivät ulkopuoliset pääse siihen käsiksi missään vaiheessa. Data tulee luokitella, ja sitä tulee käsitellä sen arkaluontoisuuden mukaan. Tärkeintä luottamuksellisuuden takaamiseksi ovat datan suojaus, riittävästä pääsynhallinnasta huolehtiminen, tiedon oikea luokittelu, sekä turvalliset tietoverkkoyhteydet dataa säilytettäessä tai siirrettäessä. (Hashemi-Pour, 2023)

Datan eheyden (Integrity) tarkoituksena on varmistaa, että tieto, jota esitetään, on oikeaa, muokkaamatonta sekä luotettavaa koko sen elinkaaren ajan. Dataa ei tulisi muokata silloin kun se on liikkeessä, eli matkalla lähteestä määränpäähän. Data tulisi myös suojata riittävästi REST-vaiheessa, eli levossa. Silloin kun data ei ole käytössä, datan luvattoman käytön ei tulisi olla mahdollista. Tärkeintä eheyden varmistamiseksi on tiedon validointi eli varmennus oikeaksi ja paikkansapitäväksi, riittävästä pääsynhallinnasta huolehtiminen, riittävästä suojauksesta huolehtiminen datan siirrossa, sekä datan säännöllinen varmuuskopiointi. (Fortinet, n.d. a)

Datan helppo saatavuus, sekä käytettävyys tulee varmistaa niille osapuolille, joilla on siihen valtuudet. Datan saatavuuden (Availability), eli kolmannen periaatteen tarkoituksena on taata nopea ja helppo pääsy käsiksi dataan niille, joilla on siihen oikeus. Tarkoituksena on estää häiriöt tai palvelunestohyökkäykset, sekä varmistaa ettei datan saatavuuteen kohdistu kohtuuttoman pitkää aikaa. Datan nopean saatavuuden varmistamiseksi tulisi huolehtia järjestelmien riittävästä tehokkuudesta, jotta dataa voidaan käsitellä mahdollisimman vaivattomasti. Yleensä tämä toteutuu varmuuskopioiden tai jonkin muun vikaturvan muodossa. Järjestelmissä tulisi huolehtia riittävästä viansietokyvystä, kuormituksen tasapainottamisesta, sekä skaalautuvuudesta. Lisäksi tulisi huolehtia riittävästä järjestelmän valvonnasta ja kunnossapidosta sekä kehittää palautumissuunnitelma häiriötilanteen varalle. (Fortinet, n.d. a)

Näiden kolmen periaatteen avulla voidaan varmistaa järjestelmien riittävä tehokkuus ja turvallisuus. CIA Triad auttaa myös organisaation riskienhallinnassa, noudattamaan säännöksiä, sekä takaa liiketoiminnan nopean jatkuvuuden. CIA Triad on työkaluna myös arvioimaan käytänteiden ja järjestelmien tehokkuutta, silloin kun jokin ei toivottu tilanne, kuten tietomurto tapahtuu.

2.1.3 Kyberhyökkäyksen määritelmä

Kyberhyökkäykseksi kutsutaan tapahtumaa jossa verkkorikollinen saa pääsyn tietojärjestelmään tarkoituksenaan aiheuttaa vahinkoa. Verkkorikollisten tavoitteena on usein häiriköidä liiketoimintaa, varastaa tai poistaa dataa, tai jopa tuhota järjestelmiä kokonaan. Kyberhyökkäykset etenevät vaiheittain, alkaen yleensä tiedustelulla ja haavoittuvuuksien etsinnällä, edeten löydetyn haavoittuvuuden hyödyntämiseen, ja sitä hyödyntäen järjestelmään ja tietoihin käsiksi pääsyyn, edeten aina tietomurtoon asti. (Team Nuggets, 2023)

Kyberhyökkäyksen takana voi olla sattumanvarainen yksittäinen toimija, jonka tarkoituksena on häiritä liiketoimintaa, kiristää saamillaan tiedoilla. Kyseessä voi olla myös henkilökohtainen motiivi, kuten esimerkiksi yrityksen entinen työntekijä, jonka työsuhde on päättynyt huonoissa merkeissä. Kyberhyökkäyksen takana voivat olla myös niin kutsutut haktivistit. Haktivistien toiminta liitetään kuitenkin useammin kyberterrorismiin sekä kybersodankäyntiin, kuin yksittäisiin hyökkäyksiin organisaatioita vastaan. Haktivistitien eli aktiivisten hakkereiden tarkoituksena ei usein ole aiheuttaa yritykselle vahinkoa henkilökohtaisista syistä, vaan kiinnittää huomiota toiminnallaan. Usein tällaisen toiminnan takana on poliittisia, tai uskonnollisia syitä. Haktivistit kokevat yrityksen edustavan heidän mielestään vääränlaisia arvoja ja hyökkäävät yritystä, organisaatiota tai jopa valtiollisia

toimijoita vastaan kostaakseen heille. Joskus haktivistien toiminnan motiivina on pelkästään kyberterrorismi, eli yleisen häiriön aiheuttaminen. (IBM, n.d.)

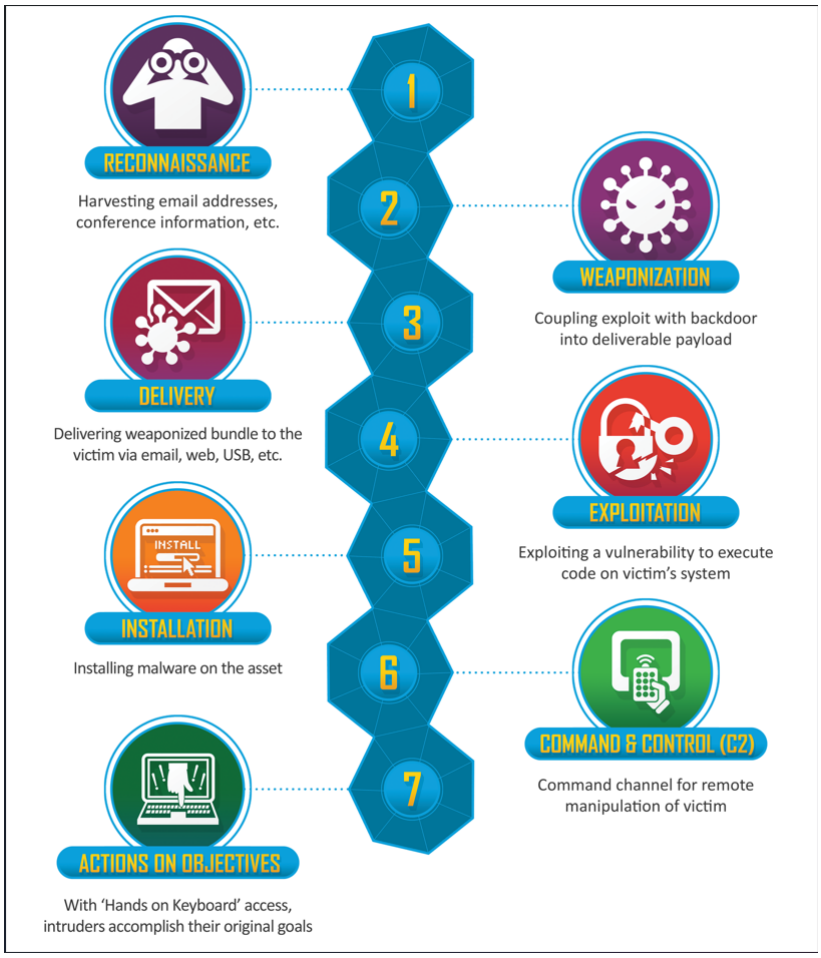
Yksi tunnetuimmista haktivistien ryhmistä on löyhästi järjestäytynyt Anonymous. Anonymous ryhmä sai alkunsa vuonna 2003 4chaniksi kutsutulla verkkosivulla. Ryhmä sai kansainvälistä huomiota toiminnallaan 2000-luvun puolivälissä, mutta vuoteen 2018 mennessä ryhmän toiminta oli vähentynyt huomattavasti. Vuonna 2020 ryhmä on kuitenkin osittain palannut toimintaan. Anonymous-ryhmän tuntomerkkeinä on jäsenien käyttämät Guy Fawkes -maskit, sekä se, ettei ryhmään ole onnistuttu liittämään yksittäisiä ihmisiä. Ryhmän jäsenet toimivat anonyymisti ryhmän nimen takaa. Useimmiten Anonymous vastustaa valtiollisia toimijoita, ja suuria yrityksiä, joiden ryhmä kokee harjoittavan sensuuria, sekä edustavan eriarvoisuutta. Ryhmän hajallisen toiminnan vuoksi ei kuitenkaan ole voitu tarkasti määritellä mitä arvoja itse Anonymous kollektiivisesti edustaa. (Zulhuni, 2023)

Yksi ryhmään liitetyistä monista tunnetuista hyökkäyksistä on nimeltään Operation Anon Down. Heinäkuussa 2015 Anonymous ryhmä julistautui olevansa palvelunestohyökkäysten takana, jotka kohdistuivat RCMP:n nettisivuihin. RCMP on lyhenne sanoista Royal Canadian Mounted Police. Poliisi oli saanut ilmoituksen Site C Dam -projektia koskevaa tapaamista häiriköivästä henkilöstä. Saapuessaan paikalle poliisit törmäsivät kuitenkin toiseen henkilöön, jolla oli kasvoillaan Guy Fawkes maski, ja poliisi päätyi erehdyksen vuoksi ampumaan henkilön. Kyseessä oli kuitenkin eri henkilö, kuin jota poliisille saapunut ilmoitus koski. Anonymousin väitteen mukaan ammuttu henkilö olisi ollut Anonymous ryhmän jäsen. Kostoksi tapahtuneesta Anonymous kohdisti RCMP:n nettisivuille palvelunestohyökkäyksiä, ja uhkasi julkistaa ampumisesta vastuussa olleen poliisin henkilötietoja. RCMP:n nettisivut olivat tapahtumaa seuraavana sunnuntaina hetken aikaa poissa käytöstä. (Ha, 2015)

2.1.4 Kyberhyökkäyksen vaiheet

Kyberhyökkäys koostuu eri vaiheista, jotka tunnetaan cyber kill chain, tai cyber attack life cycle nimityksillä. Nämä vaiheet kuvailevat erilaisia toimenpiteitä, joita hyökkääjän täytyy suorittaa päästäkseen tavoitteeseensa, eli saadakseen pääsyn tietoverkkoon, tai järjestelmään. Kyberhyökkäysten eri vaiheiden tunnistaminen auttaa organisaatiota tunnistamaan uhkia, ja hallitsemaan niihin liittyviä riskejä. (Team Nuggets, 2023) Lockheed Martin kuvasi Cyber Kill Chain kehyksessään mallin (Kuva 2), jossa kuvataan kyberhyökkäyksen seitsemää eri vaihetta.

Kuva 2 Cyber Kill Chain (Lockheed Martin, n.d.)



Ensimmäisessä vaiheessa (Tiedustelu, Reconnaissance) hyökkääjät keräävät tietoa yrityksestä, sekä sen henkilökunnasta. Tietoa voidaan kerätä esimerkiksi yrityksen sosiaalisen median sivuilta, tai yrityksen työntekijöiden profiileista. Tiedusteluvaiheessa pyritään myös mahdollisuuksien mukaan keräämään tietoa yrityksen tietoverkon, tai järjestelmien ja laitteiden mahdollisista haavoittuvuuksista. Tiedusteluvaiheen tarkoituksena on tutustua kohteeseen, ja kerätä mahdollisimman paljon tietoa. (Team Nuggets, 2023)

Kyberhyökkäyksen toinen vaihe (Aseistaminen, Weaponization) on kerätyn tiedon käyttäminen kohdetta vastaan. Hyökkääjät koostavat yhteen tiedot kohteen eri järjestelmistä, ja kehittävät työkalut tunnistettujen haavoittuvuuksien hyödyntämistä varten. Työkalut voivat olla esimerkiksi täysin uutta haittakoodia, tai jonkin olemassa olevan haittaohjelman käyttämistä uudelleen, pienillä muutoksilla. (Cybersecurity Exchange, 2022)

Kolmannessa vaiheessa (Toimitus, Delivery), hyökkääjät käyttävät koostamaansa työkalua kohdetta vastaan. Työkalu voi olla esimerkiksi tietojenkalastelutarkoituksessa tehty väärennetty sähköpostiviesti, joka sisältää haittaohjelman, tai linkki väärennetyille

nettisivuille. Toimitusvaiheen tarkoituksena on saada kohde luovuttamaan käyttäjätunnuksensa, tai lataamaan haittaohjelma laitteelle, jonka avulla hyökkääjä saa pääsyn kohteen verkkoon. (Cybersecurity Exchange, 2022)

Neljäs vaihe (Hyödyntäminen, Exploitation), tarkoittaa sitä, että hyökkääjät aloittavat haavoittuvuuden hyödyntämisen valitsemallaan työkalulla. Päästyään käsiksi kohteensa tietoverkkoon tai järjestelmään hyökkääjät alkavat tutkia ympäristöään saadakseen paremman kuvan verkosta, järjestelmistä tai ohjelmistoista, sekä saatavilla olevista käyttäjätileistä. (Maddyness, 2023)

Viidennessä vaiheessa (Asennusvaihe, Installation) hyökkääjien tavoitteena on saada kohteen verkkoon asennettua pysyvä pääsy itselleen, eli takaovi, jota hyödyntämällä hyökkääjä pääsee verkkoon aina uudelleen sisälle. Hyökkääjä pyrkii usein myös saamaan järjestelmänvalvojan oikeudet, poistamaan käytöstä palomuurin sääntöjä, ja joissain tapauksissa asentamaan etätyöaseman käyttöön itsellensä. Hyökkääjän tavoitteena on pysyä verkossa mahdollisimman kauan huomaamatta. Asennusvaiheessa hyökkääjä saattaa asentaa verkkoon myös pelkästään haittaohjelmia, jotka leviävät samassa verkossa olevista laitteista toisiinsa. (Maddyness, 2023)

Kuudennetta vaihetta kyberhyökkäyksessä kutsutaan komento- ja hallinta vaiheeksi (Command and Control). Saatuaan pääsyn kohteen tietoverkkoon, luotuaan pysyvän pääsyn, sekä saatuaan järjestelmänvalvojan oikeudet, hyökkääjällä on täysi mahdollisuus hallita kohteen tietoverkkoa, ohjelmistoja ja järjestelmiä. Hyökkääjä voi siis kerätä kohteesta arkaluontoisia tietoja, tai esiintyä yrityksen henkilöstönä. (DNV, n.d.)

Kyberhyökkäyksen seitsemäs (Actions, Toiminta), ja viimeinen vaihe on lopullisen tavoitteen saavuttaminen. Riippuen hyökkääjästä, kyberhyökkäyksen tavoite voi vaihdella. Kohteen laitteet voidaan esimerkiksi liittää bottiverkkoon ja sitä kautta käyttää niitä palvelunestohyökkäyksessä, tai kohteen laitteille voidaan asentaa haittaohjelma, joka salaa yrityksen tiedot, mahdollistaen rahallisen kiristyksen salausavainta vastaan. Tavoitteena voi olla myös pelkästään yrityksen liiketoiminnan häiritseminen toimintojen estämisellä, ja yleisen häiriön aiheuttaminen. (DNV, n.d.)

2.1.5 APT-ryhmät

APT-ryhmät, lyhenne sanoista Advanced Persistent Threat, ovat järjestäytyneitä kyberuhkatekijöitä, joilla on tietotaitoa ja resursseja suorittaa edistyneitä kyberhyökkäyksiä. APT-ryhmät toimivat usein seitsemänvaiheisen Cyber Kill Chain viitekehyksen puitteissa.

Yksi tunnetuimpia APT-ryhmiä on Pohjois-Korealainen Lazarus, joka on ollut toiminnassa jo yli 10 vuoden ajan. Lazarus-ryhmästä ei tiedetä paljoa, mutta ryhmän toiminta on väitetysti Pohjois-Korean hallituksen rahoittamaa. Ryhmän toiminta painottuu lähinnä kybervakoiluun sekä sabotaasiin. (NCC Group, n.d.)

Yksi tunnetuimmista Lazarukseen liitetyistä kyberhyökkäyksistä on toukokuussa 2017 levinnyt haittaohjelma nimeltään WannaCry. WannaCry on mato, jonka kohteena oli Microsoft Windows -käyttöjärjestelmä. Mato levisi Microsoft Windows laitteille hyödyntäen EternalBlue nimistä haavoittuvuutta. Microsoft oli julkaissut haavoittuvuudelle korjauksen, mutta WannaCry ehti kuitenkin levitä laitteille, joilla ohjelmistoa ei ollut vielä päivitetty. WannaCry salasi käyttäjien tiedostoja, vaatien ensin 300 dollarin arvoista lunnasmaksua kryptovaluutalla. Myöhemmin maksu nousi 600 dollariin. WannaCry ehti levitä vain muutamien tuntien sisällä 150 eri maassa. Jos lunnaita ei maksanut, WannaCry uhkasi poistaa salatut tiedostot kokonaan. Turvallisuustutkija Marcus Hutchins löysi WannaCryn tappokytkimen, englanniksi kill switch, joka hidasti merkittävästi haittaohjelman leviämistä. (Malwarebytes, n.d. a; Cloudflare, n.d.)

2.2 Hyökkäystyypit

Ymmärtämällä erilaiset hyökkäystavat ja niiden taustalla vaikuttavat motiivit, organisaatiot voivat tehokkaammin vahvistaa kyberpuolustustaan ja lieventää riskejä. Kyberhyökkääjät käyttävät monipuolisesti erilaisia menetelmiä ja taktiikoita puolustusten murtamiseksi ja haavoittuvuuksien hyödyntämiseksi. Tässä luvussa tutustutaan erilaisiin kyberhyökkäystyyppeihin, jotka vaihtelevat hienovaraisista tunkeutumisista häiritseviin iskuihin ja tietojen varastamiseen. Lisäksi luvussa käsitellään kybersodankäynnin ja kyberterrorismin keskeisiä käsitteitä.

2.2.1 Haittaohjelmat

Haittaohjelmaksi kutsutaan mitä tahansa ohjelmistoa, joka on suunniteltu aiheuttamaan vahinkoa järjestelmälle tai koneelle käyttäjän tietämättä. Haittaohjelmia ilmenee erilaisina mutta pääosassa ne voidaan jakaa viruksiin, troijalaisiin, matoihin, mainosohjelmiin, vakoiluohjelmiin, kiristysohjelmiin, sekä botteihin. (Arctic Wolf, 2023)

Virukset ovat haitallisia ohjelmistoja, jotka leviävät laitteeseen ja tiedostoihin. Aktivoiduttuaan laitteella virus kopioi itsensä ja levittäytyy ympäriinsä, usein vahingoittaen laitteen dataa, haitaten toimintoja, sekä mahdollistaa luvattoman pääsyn laitteelle. (Shea & Harford, 2023)

Troijalainen, joka on lyhenne troijalaisesta hevosesta, on haitallinen ohjelma, joka on saatu näyttämään aidolta ohjelmistolta. Näin käyttäjä houkutellaan lataamaan haitallinen ohjelma laitteellensa. Troijalainen sisältää haitallista koodia, jonka suoritettuaan se voi toimia laitteella huomaamatta. Troijalainen voi avata laitteelle takaoven, varastaa tietoja, tai mahdollistaa muiden haittaohjelmien pääsyn laitteelle. Troijalainen ei leviä itsestään laitteelle, vaan se vaatii aina toimenpiteitä käyttäjältä. (Arctic Wolf, 2023; Shea & Harford, 2023)

Madot ovat virusten lailla haitallisia ohjelmistoja, jotka leviävät laitteessa kopioiden ja levittäen itseään. Toisinkuin virus, mato ei vaadi tiedostoa, jonka mukana se leviää, vaan madot hyödyntävät erilaisia haavoittuvuuksia päästäkseen sisään laitteelle. Madot eivät vaadi myöskään käyttäjältä toimenpiteitä levitäkseen. Madot voivat saastuttaa kokonaisia tietoverkkoja, ja levitä siten laitteesta toiseen nopealla tahdilla. (Malwarebytes, n.d. b)

Mainosohjelma on haittaohjelma, joka esittää laitteen käyttäjälle tunkeilevia, ei pyydettyjä mainoksia. Mainosohjelmat saattavat usein asentua aidon ohjelmiston tai sovelluksen mukana. Kaikki mainosohjelmat eivät välttämättä ole itsessään haitallisia laitteelle, mutta ne saattavat johdatella käyttäjänsä lataamaan haitallisia ohjelmistoja laitteelleen mainosten kautta. (Arctic Wolf, 2023)

Vakoiluohjelma asentuu käyttäjän laitteelle huomaamatta. Vakoiluohjelmat ovat suunniteltu toimimaan laitteessa taustalla, ja keräämään tietoa laitteen käyttäjästä. Vakoiluohjelma voi kerätä tietoa muun muassa näppäimistön painalluksista, selainhistoriasta, tai seurata laitteen fyysistä sijaintia. Näin vakoiluohjelma voi kerätä käyttäjän tunnuksia ja salasanoja, sekä välittää selainhistoriaa kolmansille osapuolille esimerkiksi markkinoinnin tarkoitusta varten. Vakoiluohjelmista on kehitetty erilaisia versioita, joiden kohteena on erityisesti mobiililaitteet. (Shea & Harford, 2023)

Kiristyshaittaohjelmat ovat yksi haittaohjelmien yleisimmistä muodoista. Kiristyshaittaohjelma salaa laitteen tiedostoja, tai voi jopa lukita laitteen, jonka jälkeen kiristyshaittaohjelman levittämisen takana oleva hyökkääjä vaatii lunnaita vastineeksi salauspurkuavaimen toimittamisesta. Lunnaat vaaditaan usein maksamaan kryptovaluutalla, kuten bitcoineilla. Kiristyshaittaohjelma leviää laitteelle usein sähköpostin liitetiedostona, haitalliselta verkkosivulta- tai mainoksesta. (Malwarebytes, n.d. c)

Bottiverkko eli botnet on tietokoneohjelmista, eli boteista koostuva verkko. Botti on itseään kopioiva haittaohjelma, joka leviää usealle eri laitteelle, ja muodostaa näin saastuneista laitteista ketjun, eli bottiverkon. Botit ovat kytkeytyneet toisiinsa tietoverkon välityksellä. Bottiverkon avulla saastuneet laitteet voidaan valjastaa osallistumaan esimerkiksi

palvelunestohyökkäykseen, tai roskapostitukseen. Laite liitetään bottiverkkoon usein käyttäjän tietämättä. (Arctic Wolf, 2023)

2.2.2 Tietojenkalastelu

Tietojenkalastelu, toiselta nimeltään verkkourkinta, tai phishing, on yritys saada haltuunsa käyttäjän tunnuksia, salasanoja tai muita henkilökohtaisia tietoja. Usein tietojenkalasteluyritykset kohdistuvat sähköpostiin tai puhelimeen, jolloin käyttäjä saa viestin, jossa pyydetään lataamaan jokin tiedosto, tai siirtymään jollekin nettisivulle. Ladattu tiedosto voi sisältää haittaohjelman, joka vakoilee käyttäjän toimia laitteella. Usein sähköpostien sisältämät linkit nettisivuille ovat jäljitelmiä esimerkiksi pankkien kirjautumissivuista. Linkin takana oleva sisältö voi vaatia käyttäjää vahvistamaan tilinsä tai tunnistautumaan, jolloin hyökkääjä saa käyttäjän tunnukset haltuunsa. Näennäisesti aitojen näköiset sivut on tarkoitushakuisesti luotu harhauttamaan käyttäjiä. Todellisuudessa kuitenkin kaikki kirjautumisen yhteydessä annetut tiedot tallentuvat hyökkääjän hallitsemalle palvelimelle. (F-Secure, n.d. b)

2.2.3 Nollapäivähaavoittuvuus

Nollapäivähaavoittuvuus on haavoittuvuus järjestelmässä, jota kehittäjät tai jälleenmyyjä eivät ole havainneet, tai sille ei ole vielä korjausta. Nollapäivähaavoittuvuus, englanniksi zero-day vulnerability, viittaa haavoittuvuuteen järjestelmässä. Nollapäivähyökkäys taas viittaa siihen, että hyökkääjät ehtivät käyttää haavoittuvuutta hyväkseen heti sen löydyttyä, niin että sen korjaamiseksi ei ole ehditty tehdä toimenpiteitä. Nollapäivähaavoittuvuutta hyödyntäen tehtyä hyökkäystä kutsutaan nollapäivähyökkäykseksi, englanniksi zero-day attack, ja hyökkäys toteutetaan usein haittakoodin avulla. Hyökkääjät etsivät uusia haavoittuvuuksia jatkuvasti, joskus löytäen niitä ennen kehittäjiä. Nollapäivähaavoittuvuudet paikataan usein heti seuraavassa ohjelmistopäivityksessä tai sovelluksen versiossa, mutta riippuen nollapäivähaavoittuvuudesta, ratkaisun kehittämiseen voi kulua aikaa. (Kaspersky, n.d. a; Posey & Shea, 2023)

2.2.4 Man-in-the-Middle hyökkäys

Man-in-the-Middle hyökkäys eli väliintulo- tai mies välissä-hyökkäys, toteutetaan niin että hyökkääjä asettaa itsensä kahden toistensa kanssa kommunikoivan osapuolen väliin. Osapuolet uskovat kommunikoivansa toistensa kanssa, mutta todellisuudessa keskustelua ohjaa hyökkääjä, joka seuraaja hallitsee kommunikaatiota sekä tiedon kulkua, esimerkiksi kahden osapuolen viestittelyä. Toistensa kanssa kommunikoivat osapuolet voivat olla

muutakin kuin vain ihmisiä, esimerkiksi käyttäjä ja palvelin. Hyökkääjä voi hyödyntää verkon haavoittuvuuksia, tai huonoja turvallisuusprotokollia ja ohjata internet-liikenteen väärennetylle nettisivulle. Väärennetyn nettisivun kautta hyökkääjä voi saada haltuunsa käyttäjän tunnuksia ja salasanoja. (Fortinet, n.d. b; Yasar & Cobb, 2022)

2.2.5 Palvelunestohyökkäys

Palvelunestohyökkäys on yritys häiritä palvelimen, nettisivun tai tietoverkkoyhteyden normaalia toimintaa ylirasittamalla sen kapasiteettia käsitellä saapuvaa internet-liikennettä. Palvelunestohyökkäyksen tarkoituksena on tukkia kohteen, kuten nettisivun kaista, lähettämällä jatkuvia pyyntöjä palvelimelle eri IP-osoitteista. Täten nettisivut eivät ole saatavilla aidoille käyttäjille. Palvelunestohyökkäys hidastaa kohteen toimintaa, voiden jopa kaataa kyseisen palvelimen kokonaan. (Radware n.d.)

Palvelunestohyökkäyksiä on kahdenlaisia, palvelunestohyökkäys, englanniksi tunnettu denial-of-service attack DoS, jossa hyökkäys tehdään käyttäen yksittäistä Internet yhteyttä. Hajautettu palvelunestohyökkäys, englanniksi distributed denial-of-service attack DDoS, koostuu usein kaapatuista koneista, jotka muodostavat yhdessä bottiverkon. Hajautetussa palvelunestohyökkäyksessä internet-liikenne tulee useasta eri IP-osoitteesta. (Imperva, n.d.)

2.2.6 SQL-injektio

SQL-injektio on kyberhyökkäyksen tyyppi, joka kohdistuu tietokantapohjaiseen sovellukseen, tai nettisivuihin. Termi SQL tarkoittaa Structured Query Language, eli kyselykieltä, jolla relaatiotietokantaan voi suorittaa erilaisia komentoja, kuten tietojen lisäystä, päivitystä, poistoa tai vain tietojen katselua. (Loshin & Sirkin, n.d.)

SQL-injektiossa hyökkääjä syöttää esimerkiksi nettisivulla olevaan hakukenttään, tai lomakkeeseen SQL-komentoja, ja voi tätä kautta saada pääsyn tietokannan kaikkiin tietoihin. Näin hyökkääjä voi päästä katselemaan esimerkiksi nettisivulle rekisteröityneiden käyttäjien tunnuksia, jotka ovat taltioitu tietokantaan. SQL-injektion onnistuminen johtuu usein käyttäjäsyötteen riittämättömästä hallinnoinnista, eli siitä että käyttäjän lomakkeeseen syöttämää tietoa ei suodateta kunnolla erilaisista merkkijonoista, tai kirjaimista. Lomakkeeseen voidaan siis syöttää erilaisia komentoja tai haittakoodia, joka menee suodattamattomana järjestelmään, ja sitä kautta tietokantaan, mahdollistaen luvattoman pääsyn tietoihin. Nettisivun, tai sovelluksen ohjelmakoodin ei tulisi koskaan käsitellä käyttäjän syöttämää tietoa suoraan. (Acunetix, n.d.; Zhu, 2023)

2.2.7 Käyttäjän manipulointi

Käyttäjän manipulointi, englanniksi social engineering, tarkoittaa erilaisia tapoja, joilla hyökkäyksen uhreja pyritään huijaamalla luovuttamaan henkilökohtaisia tietojaan, omia käyttäjätunnuksiaan tai saavuttamaan muuta rahallista hyötyä uhrista. Käyttäjän manipulointi perustuu enemmän ihmisten hyväuskoisuuden ja inhimillisten erehdysten hyödyntämiseen, kuin varsinaisiin teknisiin keinoihin. Hyökkäys tapahtuu usein yhteydenpidolla käyttäjän kanssa suoraan, esimerkiksi sähköpostitse. Käyttäjän manipulointia kohdistuu niin yrityksiin, kuin yksittäisiin henkilöihin. Yleensä tavoitteena on saada pääsy yrityksen tietoihin, tietoverkkoon, tai saada käyttäjä lataamaan laitteellensa jokin haittaohjelma. Hyökkääjä tekeytyy usein tahoksi johon kohde luottaa, kuten esimerkiksi työnantajaksi, tai yrityksen IT-henkilöksi. (Thomas, 2022; Cisco, n.d.)

2.2.8 IoT-laitteet

Huonosti suojatut IoT-laitteet voivat aiheuttaa yritykselle huomattavan tietoturvariskin. IoT-laitteella on usein käytössään rajallisemmat resurssit, josta johtuen datan suojaaminen ja turvaaminen ei ole yhtä edistynyttä, kuin esimerkiksi tietokoneella. Hyökkääjä voi siis hyödyntää yrityksen tietoverkkoon yhdistettyä huonosti suojattua IoT-laitetta verkkoon käsiksi pääsemisessä. Tämä mahdollistaa hyökkääjälle liikkumisen verkossa huomaamatta. Päästyään käsiksi yrityksen verkkoon, hyökkääjä voi pyrkiä saamaan oikeudet yrityksen arkaluontoisiin tietoihin, tai levittää haittaohjelmia muihin laitteisiin. IoT-laite voidaan myös liittää bottiverkkoon, jota hyödynnetään palvelunestohyökkäyksessä. (Ansari, 2023; Balbix, n.d.)

2.2.9 Kyberterrorismi ja kybersodankäynti

Kyberterrorismiksi kutsutaan sitä, kun tietokoneen teknologiaa, yleisesti internetiä, käytetään terroritekojen välineenä. Kyberterrorisimin hyökkäykset kohdistuvat usein tietojärjestelmiin, ohjelmistoihin ja dataan, tarkoituksena aiheuttaa häiriötä, pelkoa tai muuta harmia kohteelle. Kyberterrorismin motiivina on usein tukea jotakin poliittista aatetta tai arvoja, tai vaihtoehtoisesti motiivina voivat olla myös muut uskonnolliset tai yhteiskunnalliset syyt. Haktivistit ja APT-ryhmät ovat usein liitetty kyberterrorismin tekoihin. Kyberterrorismin välineenä käytetään usein yleisiä kyberhyökkäyksen tyyppejä, kuten viruksia, matoja, haittaohjelmia tai palvelunestohyökkäyksiä. Kyberterrorismin kohteena on usein yhteiskunnan toiminnan kannalta tärkeät perusrakenteet. Kyberterrorismille ei ole tarkkaa yleistä määritelmää, usein teon takana oleva motiivi paljastaa sen, luokitellaanko kyberhyökkäys terrorismiksi. (Sheldon & Terrell Hanna, 2024)

Kybersodankäynnissä kyberhyökkäyksiä käytetään sodankäynnin välineenä viholliseksi miellettyä valtiota vastaan. Kybersodankäynnin tarkoituksena on usein sama kuin tavallisella sodankäynnillä, heikentää vihollista. Kybersodankäynnin välineinä voivat olla esimerkiksi kybervakoilu, tärkeiden tietoverkkojen sabotaasi- ja häirintä, sekä manipulaatio- ja propagandan levittäminen. Kybersodankäynnin, sekä kyberrikosten, -ja terrorismin raja on häilyvä, ja kuten kyberterrorismille, ei kybersodankäynnille ole virallista tarkkaa määritelmää. Kybersodankäynniksi kuitenkin lasketaan se, että toimien tarkoituksena on edistää valtion etua sodankäynnissä. Kybersodankäynnissä kohteeksi valikoituvat usein samat kuin kyberterrorismissa, yhteiskunnan tärkeät rakenteet. (Buxton, 2023; S. Gillis & Terrell Hanna & Ferguson, 2023)

Yksi tunnetuimmista kybersodankäyntiin liitetyistä hyökkäyksistä on mato nimeltään Stuxnet. Mato löydettiin ensimmäisen kerran vuonna 2010, kun maailmalla levisi tieto, että mato oli saastuttanut Iranin ydinvoimalaitoksen järjestelmän. Iranin ydinvoimalaitoksen laitteet eivät olleet turvallisuussyistä yhdistettynä internettiin tai muihin verkkoihin, joten uskotaan, että mato toimitettiin ydinvoimalaitoksen järjestelmään fyysisen USB-muistitikun välityksellä. Stuxnet hyödynsi aikaisemmin löytämättömiä nollapäivähaavoittuvuuksia Windows -käyttöjärjestelmässä päästäkseen käsiksi ydinvoimalaitoksen tietoverkkoon. Stuxnet tuhosi järjestelmän infrastruktuuria Iranin uraanin rikastuslaitoksella, tarkoituksenaan häiritä kehitteillä olevaa ydinaseohjelmaa. Stuxnet lähetti tuhoavaa koodia järjestelmään aiheuttaakseen vahinkoa tuotantoprosessille, lähettäen samanaikaisesti virheellisesti oikeita lukemia prosessista rikastuslaitoksen valvomoon. Stuxnet mahdollisti toimiessaan myös teollisuusvakoilun, sillä se pystyi lähettämään saastuttamastaan järjestelmästä tietoja takaisin sitä ylläpitävälle palvelimelle. Stuxnet löydettiin tuotantoprosessin tarkastusten yhteydessä vuonna 2010, mutta Stuxnetin kehityksen uskotaan alkaneen jo vuonna 2005. Toistaiseksi Stuxnetin kehittäjää ei olla pystytty tunnistamaan. Stuxnet oli ensimmäinen digitaalinen ase, joka pystyi aiheuttamaan fyysistä vahinkoa kohteellensa. Tapahtunut ei ollut ensimmäinen kybersodankäynnin hyökkäys, mutta sitä pidetään yhtenä aikansa edistyneimpänä. (Kaspersky, n.d. b)

2.2.10 Kyberhyökkäyksen seuraukset

Onnistuneen kyberhyökkäyksen vaikutukset ovat merkittäviä, ja niitä ei tulisi aliarvioida. Yksi yleisimmistä seurauksista on suorat rahalliset menetykset. Rahaa voi kadota suoraan varkauden seurauksena tai esimerkiksi kiristyksen myötä. Näitä taloudellisia menetyksiä lisäävät usein myös vastatoimenpiteisiin ja palautumiseen liittyvät kustannukset. IT-henkilöstön lisätyö ja mahdolliset ulkoiset asiantuntijaresurssit aiheuttavat kuluja. Kyberhyökkäyksen selvittäminen ja analysointi sekä ulkopuolisten konsulttien käyttö voivat

nostaa kustannuksia entisestään. Palautumis- ja korjaustoimenpiteet vievät myös arvokasta aikaa, joka olisi muuten voitu käyttää liiketoiminnan kannalta tuottavammin. Lisäksi tietovuotoon johtanut kyberhyökkäys voi heijastua yrityksen arvon laskuna markkinoilla. (Huang & Wang & Wei & Madnick, 2023; Banach, 2019)

Kyberhyökkäys voi johtaa laajaan tietovuotoon, paljastaen yrityksen arkaluontoisia tietoja, rahaliikennettä tai asiakkaiden henkilötietoja. Tämä voi aiheuttaa merkittävää vahinkoa yrityksen maineelle, luottamukselle ja immateriaaliomaisuudelle. Luottamuksen menetys heijastuu välittömästi yrityksen maineeseen ja voi johtaa merkittävien asiakassuhteiden ja kumppanuuksien menetykseen. Immateriaaliomaisuuden paljastuminen puolestaan voi aiheuttaa arvokkaiden liikesalaisuuksien paljastumisen, mikä haittaa yrityksen kilpailukykyä pitkällä aikavälillä. Tietovuodon seuraukset voivat siis ulottua laajalle ja vaikuttaa merkittävästi yrityksen toimintaan ja menestykseen. (Fancher, Gelinne, Mossburg, 2016; Banach, 2019)

Kyberhyökkäyksen ja tietovuodon laajuudesta riippuen, yritystä voidaan pitää oikeudellisesti vastuussa tapahtuneesta. Erityisesti jos asiakkaiden arkaluontoisia tietoja paljastuu hyökkäyksen seurauksena, voidaan päätellä, että yrityksen tietoja tai järjestelmiä ei ole suojattu asianmukaisesti. Tämä voi johtaa mahdollisiin korvausvaatimuksiin tietyissä tapauksissa. Yritysten on siis tärkeää ymmärtää vastuunsa ja velvollisuutensa tietoturvan suhteen, jotta voidaan minimoida riski oikeudellisista seuraamuksista ja säilyttää asiakkaiden luottamus. (Banach, 2019)

Psykoterapiakeskus Vastaamon tietomurto on yksi Suomen suurimmista, ja tunnetuimmista kyberhyökkäyksistä, joka vaikutti tuhansiin suomalaisiin. Vastaamon tietomurto oli niin mittava, että se sai myös kansainvälistä huomiota. Vastaamon potilastietokantaan kohdistui laiton tietomurto arviolta marraskuussa 2018. Vastaamon palvelimen tietokantaportti oli jäänyt avoimeksi verkkoon päivitysten myötä, ja oli kokonaisuudessaan huomaamatta auki arviolta puolentoista vuoden ajan. Palvelimen pääkäyttäjäksi pääsi väitetysti oletustunnuksilla, ja sen lisäksi Vastaamon palomuuri oli väärin konfiguroitu, jonka vuoksi se päästi kaiken tietoliikenteen lävitse. Vastaamon potilastietokantaan kohdistui murtoja vuosina 2018–2019, kunnes vuonna 2019 tietokanta tyhjennettiin, ja tilalle jätettiin kiristysviesti. Potilastietokanta sisälsi väitetysti ainakin potilaskertomuksia, sekä henkilötietoja. (Kantomaa, 2021; Mäntysalo, 2023; Tietosuojakeskus, n.d.)

Viimeisen tietokantamurron jälkeen nimetön kiristäjä otti yhteyttä ensin Vastaamon johtoon ja henkilökuntaan, sekä myöhemmin asiakkaisiin. Kiristäjä kirjoitti Tor-verkossa sijaitsevalle keskustelualustalle englanniksi hakkeroineensa Vastaamon tietokannan. Kiristäjä vaati

yritykseltä 40 bitcoinin lunnaita, varastettujen tietojen julkaisemisen uhalla. Vastaamo jätti reagoimatta kiristäjän viesteihin, jonka seurauksena tämä aloitti julkaisemaan asiakkaiden tietoja 100 kappaletta päivässä, niin kauan että lunnaat maksettaisiin. Myöhemmin kiristäjä muutti toimintaansa ja lähestyi myös yksittäisiä Vastaamon asiakkaita. Asiakkailta vaadittiin ensin 200 euron lunnaita, mutta myöhemmin maksu nousi 500 euroon, vastineeksi siitä, ettei heidän tietojaan julkaistaisi. Kiristäjä teki kuitenkin kriittisen virheen ja latasi verkkoon 10 gigatavun kokoisen tiedoston. Tämä tiedosto oli kuitenkin saatavilla vain muutamien tuntien ajan, eikä sen tarkka sisältö ole siksi tiedossa. Tämä virhe johti lopulta kiristäjän henkilöllisyyden selvittämiseen, sekä rikosoikeudelliseen vastuuseen saattamiseen. (Hämäläinen & Rummukainen, 2020; Hämäläinen, 2021; Yle, 2020)

Vastaamon silloinen toimitusjohtaja erotettiin virastaan, ja hänet korvasi aikaisemmin hallituksen puheenjohtajana toiminut henkilö. Vastaamon yhtiön silloinen pääomistaja käynnisti oikeudellisia toimenpiteitä koskien aikaisemmin kirjoitettua kauppasopimusta, ja yritys asetettiin selvitystilaan. Myöhemmin myös Vastaamon uudeksi toimitusjohtajaksi nimetty aikaisempi hallituksen puheenjohtaja, sekä koko hallitus erosivat virastaan. Helmikuussa 2021 Vastaamo haettiin konkurssiin, ja osa sen toiminnasta myytiin eteenpäin. Vastaamon tietomurtojen aikainen toimitusjohtaja tuomittiin sittemmin oikeudessa tietosuojarikoksesta. (Hevonoja, 2020; Maaseudun tulevaisuus, 2021; Taleva, 2021; Svahn & Karppi, 2021; Mäntysalo & Salumäki, 2023)

Vastaamo on yksi esimerkki siitä, miten tuhoisat seuraukset riittämättömällä tietoturvasta huolehtimisella, ja onnistuneella kyberhyökkäyksellä voi olla.

2.3 Riskienhallinta

Riskienhallinta muodostaa yhden kyberturvallisuuden kulmakiven. Riskienhallinta on ennaltaehkäisevää toimintaa, sekä aktiivista vastaamista jatkuvasti muuttuviin uhkiin. Tässä luvussa tarkastellaan riskienhallinnan periaatteita, niiden soveltamista ja merkitystä osana kyberturvallisuuden hallintajärjestelmää.

Riskienhallinta on yksi kyberturvallisuuden keskeisimmistä osista, joka tarjoaa lähestymistavan, jolla suojellaan yrityksen digitaalista omaisuutta. Riskienhallinta on epätoivotun toiminnan, kuten kyberhyökkäyksen este, ja se vaikuttaa suoraan organisaation liiketoiminnan kestävyyteen ja menestykseen. Sitoutuminen riskienhallintaan mahdollistaa tehokkaan reagoinnin ja sopeutumisen kyberuhkiin. (Knowles, 2024)

2.3.1 Riskienhallinnan perusteet

Riskiksi määritellään tapahtuma, tai mahdollisuus, joka johtuu digitaalisen omaisuuden haavoittuvuuden hyödyntämisestä. Tapahtumasta, eli kyberhyökkäyksestä voi seurata tietomurto, häiriö palvelussa, tai se voi johtaa merkittäviin rahallisiin menetyksiin, tai aiheuttaa yritykselle mainehaittaa. (Tunggal 2023a)

Riskienhallinta on jatkuva prosessi, joka koostuu uhkien ja haavoittuvuuksien tunnistamisesta, havaitsemisesta, arvioimisesta, sekä niihin vastaamisesta. Riskienhallinta on yrityksen jokaisen työntekijän vastuulla. Riskienhallinta alkaa yrityksen digitaalisen omaisuuden tunnistamisella. Digitaaliseksi omaisuudeksi luokitellaan kaikki digitaaliset resurssit, joita yritys tarvitsee jokapäiväisessä toiminnassaan. Digitaalista omaisuutta ovat kaikki data tai tieto, jota yrityksellä on hallussaan. (Knowles, 2023)

Digitaaliseksi omaisuudeksi lukeutuu kaikki mahdollisista asiakastiedoista työntekijöiden tietoihin, yrityksen liikevaihto- ja rahaliikenne, sekä immateriaaliomaisuus kuten patentit, tavaramerkit tai muut tekijänoikeudet. Digitaaliseksi omaisuudeksi lukeutuvat myös kaikki järjestelmät, alustat, sovellukset, palvelimet sekä ohjelmistot, joita yrityksellä on käytössään. Digitaalista omaisuutta ovat siis esimerkiksi tiedostot, sähköpostit, sosiaalisen median tilit, nettisivun domainit, tietokannat, lisensoidut ohjelmistot, pilvipalvelut tai lähdekoodi. Digitaaliseksi omaisuudeksi luokitellaan myös kaikki fyysinen omaisuus, jolla näitä säilytetään. Digitaalista omaisuutta ovat siis esimerkiksi myös tietokone ja puhelin, mutta myös fyysiset palvelimet sekä reitittimet, joita yrityksellä on käytössään. (Hill, 2023)

Riskien hallitsemiseksi on olennaista kehittää systemaattinen lähestymistapa, joka kattaa riskien todennäköisyyden arvioinnin, luokittelun, sekä sopivien turvallisuustoimenpiteiden määrittelyn. Jokaisen riskin vakavuuden arviointi tulee suorittaa tapauskohtaisesti. Tämä sisältää arvion siitä, onko riski estettävissä, siedettävissä, tai hyväksyttävissä. On tunnistettava, onko riski mahdollista täysin eliminoida vai onko se siedettävä osana normaalia liiketoimintaa. Jokainen riski on erilainen, ja toimenpiteet riskin hallitsemiseksi saattavat vaihdella riippuen sen merkityksestä ja vaikutuksesta organisaatioon. Riskien hallinnassa tärkeää on riskien jatkuva arviointi, ja turvallisuustoimenpiteiden mukautus vastaamaan muuttuvaa uhkakuvaa. (Tunggal, 2023b)

2.3.2 Haavoittuvuuksien ja uhkien tunnistaminen sekä arviointi

Haavoittuvuuksien ja uhkien tunnistaminen sekä arviointi ovat keskeisiä toimenpiteitä kyberturvallisuutta, ja riskienhallintaa suunniteltaessa. Uhka viittaa laajasti kaikkiin

mahdollisiin haitallisiin tapahtumiin, jotka johtuvat haavoittuvuuksista. Uhat voivat olla joko tarkoituksellisia, tai tahattomia riippuen uhkatyypistä, ja sen alkuperästä. Haavoittuvuus puolestaan kattaa kaikki heikkoudet järjestelmässä tai tietoverkossa. Haavoittuvuutta hyödyntämällä voidaan saada luvaton pääsy tietoihin tai järjestelmään. (Puzder, 2023)

Uhkien ja haavoittuvuuksien tunnistamisessa olennaisinta on harkita, mitkä yrityksen osa-alueet ovat erityisen haavoittuvaisia. On tarpeellista määritellä digitaaliseen omaisuuteen kohdistuvat uhat, miten niitä voidaan mahdollisesti hyödyntää, ja suunnitella riittävät turvallisuustoimenpiteet haavoittuvuuksien ehkäisemiseksi. Riskienhallinnan kannalta on tärkeää arvioida haavoittuvuuksien ja uhkien kriittisyyttä, vaikutusta, sekä todennäköisyyttä tapahtua. Näin voidaan määrittää uhan kriittisyys ja taso, sekä se millä aikataululla korjaavat toimenpiteet tulee suorittaa. Tämä auttaa hahmottamaan, mitkä riskit ovat hyväksyttäviä ja hallittavissa, sekä mitkä tulee eliminoida, jotta voidaan turvata liiketoiminnan jatkuvuus. Taulukko 1 Uhkien tunnistaminen ja arviointi esittelee kuinka oman organisaation digitaalista omaisuutta voidaan kartoittaa. Lisäksi kuvataan millaisia ovat mahdolliset uhkatekijät sekä miten uhan kriittisyyttä voidaan arvioida. Riskin tason arvioimalla voidaan määrittää tarvittavat toimenpiteet. On myös oleellista ymmärtää, että uhat ja haavoittuvuudet muuttuvat jatkuvasti uhkakuvan myötä. (PSR, 2022; RiskOptics, 2023)

Taulukko 1 Uhkien tunnistaminen ja arviointi (Stine & Quinn & Witte & Gardner, 2020 s.14–16)

Kohde	**Uhka/ haavoittuvuus**	**Uhkatekijä**	**Vaikutus (1–5)**	**Todennäköisyys (1–5)**	**Kriittisyys**	**Ratkaisu**	**Riskin taso**
Tietokone	Laiterikko	Huolimattomuus	4	5	20	Varmuuskopiointi, huolellisuus	Hyväksyttävä
Ohjelmisto	Haitta-ohjelma	Haktivisti	4	4	16	Virustorjunta-ohjelma, palomuuri	Estettävä/ Siedettävä
Arkaluontoinen data	Luvaton käyttö/ tietomurto	Haktivisti tai muu ilkivaltainen taho	5	5	25	Riittävä pääsynhallinta ja valvonta	Eliminoitava

Uhkina ja haavoittuvuuksina ilmenevät erilaiset kyberhyökkäystyypit, kuten palvelunestohyökkäykset, haittaohjelmat ja tietojenkalastelu. Lisäksi on otettava huomioon myös ulkoiset uhkatekijät, kuten erilaiset luonnonkatastrofit, jotka voivat vaikuttaa yrityksen fyysiseen omaisuuteen, sekä ilkivalta tai murtovarkaudet. Fyysisiä ja ulkoisia uhkia ovat esimerkiksi tulipalot, vesivahingot tai laitteistoviat. Sisäisiin uhkiin ja haavoittuvuuksiin kuuluvat puolestaan yrityksen omat työntekijät, olivatpa he sitten huolimattomia tai pahantahtoisia. Erityisen merkittävä uhkatekijä on inhimilliset virheet. Uhkakuvaa täydentävät järjestelmälliset uhat, jotka liittyvät suunniteltuihin kyberhyökkäyksiin. Nämä hyökkäykset ovat usein kokeneiden toimijoiden toteuttamia, joilla on selkeä ja määritelty tavoite. Toisaalta epäjärjestelmälliset hyökkäykset voivat olla toimijoiden, joilla ei ole selkeää tavoitetta tai toimintamallia. (SecurityScorecard, 2021b)

Digitaalisen omaisuuden tunnistamisen ja uhkien sekä haavoittuvuuksien arvioinnin lisäksi haavoittuvuuksien hallinnassa on välttämätöntä pysyä ajan tasalla kyberturvallisuuden trendeistä ja jatkuvasti muuttuvasta uhkakuvasta. Tämä vaatii aktiivista seurantaa ja reagointia uusiin uhkiin. Analysoimalla aiempia tietomurtoja voidaan tunnistaa mahdollisia yhtäläisyyksiä oman yrityksen haavoittuvuuksiin, joka voi auttaa parantamaan puolustusmekanismeja. (SecurityScorecard, 2021b)

Yrityksen kumppaneiden luotettavuuden ja turvallisuuden arvioiminen, erityisesti ohjelmistojen hankinnassa, on osa tehokasta haavoittuvuuksien hallintaa. Jatkuva penetraatiotestaus on myös yksi tärkeä toimenpide, jonka avulla voidaan tunnistaa uusia haavoittuvuuksia ajoissa ja varmistaa, että puolustusmekanismit ovat riittävät. Pääsynhallinta ja käyttäjien oikeuksien valvonta ovat keskeisiä keinoja estää luvaton pääsy tietoihin. Lisäksi datan on oltava suojattuna sekä lepo- että siirtovaiheessa, jotta haavoittuvuuksia ei voida hyödyntää tietoon murtautumiseksi. Jatkuvaa valvontaa on suoritettava sekä tietoverkossa, että järjestelmissä jotta voidaan varmistaa nopea reagointi ja mahdollisten uhkien havaitseminen ennen niiden aiheuttamaa vahinkoa. Nämä toimenpiteet yhdessä muodostavat kokonaisvaltaisen lähestymistavan haavoittuvuuksien hallintaan ja kyberturvallisuuden ylläpitoon. (SecurityScorecard, 2021b)

2.3.3 SWOT-analyysi

Digitaalisen omaisuuden, sekä niihin kohdistuvien erilaisten uhkien ja haavoittuvuuksien tunnistamisen ja arvioinnin lisäksi voidaan suorittaa SWOT-analyysi (Kuva 3) haavoittuvuuksien hallinnan strategisen näkökulman vahvistamiseksi. SWOT koostuu

sanoista strengths, weaknesses, opportunities, sekä threats. SWOT-analyysi auttaa yritystä tunnistamaan omat vahvuutensa, sekä mahdollisuutensa, mutta samalla tiedostamaan heikot kohdat sekä mahdolliset uhat. (Stine & Quinn & Witte & Gardner, 2020 s.24)

Kuva 3 SWOT-analyysi (Thinkcurity, n.d.)

Vahvuuksien osalta yrityksen vahvat tietoturvakäytännöt, pätevä henkilöstö ja nykyaikainen teknologia muodostavat vahvan perustan digitaalisen omaisuuden suojaamiselle. Pääsynhallinta ja käyttöoikeuksien valvonta voivat olla erityisiä vahvuuksia, jotka auttavat estämään luvatonta pääsyä tietoihin. (Thinkcurity, n.d.)

Heikkouksien osalta yrityksen haavoittuvuudet voivat liittyä vanhentuneisiin tietoturvakäytäntöihin, riittämättömään koulutukseen tai teknologisiin rajoituksiin. Tunnistamalla nämä heikkoudet yritys voi keskittyä niiden vahvistamiseen ja parantamiseen. (Thinkcurity, n.d.)

Mahdollisuudet voivat sisältää uusien tietoturvastrategioiden, teknologisten innovaatioiden ja kumppanuuksien hyödyntämisen. SWOT-analyysi auttaa tunnistamaan ne alueet, joilla yritys voi hyödyntää mahdollisuuksia parantaakseen kyberturvallisuuttaan. (Thinkcurity, n.d.)

Uhat kattavat laajan kirjon potentiaalisia riskejä, kuten uusia ja kehittyneempiä kyberhyökkäystapoja tai ulkoisten toimijoiden uhkia. Näiden uhkien ymmärtäminen on kriittistä varautumisen kannalta. (Thinkcurity, n.d.)

Säännöllisesti tehty SWOT-analyysi auttaa organisaatiota pysymään ajan tasalla kyberturvallisuuden tilasta ja mahdollisista muutoksista ympäristössä. Tämä mahdollistaa ennakoivan toiminnan ja auttaa organisaatiota valmistautumaan ja reagoimaan tehokkaasti muuttuviin uhkiin ja mahdollisuuksiin. (Windsor Group Sourcing Advisory, 2023)

2.3.4 Riskien tunnistaminen ja arviointi

Riskienhallinta tulisi aloittaa tunnistamalla ja dokumentoimalla kaikki organisaation digitaaliset omaisuudet, mukaan lukien laitteistot, ohjelmistot, tietoverkot, varastot ja pilvipalvelut. Digitaalisesta omaisuudesta tulee luoda tarkka inventaario, joka sisältää jokaisen omaisuuserän sijainnin, käyttötarkoituksen ja merkityksen organisaatiolle. Seuraavaksi tulee analysoida mitkä ovat ne uhat ja haavoittuvuudet, jotka kohdistuvat digitaaliseen omaisuuteen. Jokaisen uhan ja haavoittuvuuden vakavuutta, sekä vaikutusta tulisi arvioida. Aikaisemmassa luvussa esiintyvä Taulukko 1 antaa suuntaa uhkien ja haavoittuvuuksien kriittisyyden arviointiin. Digitaalinen omaisuus tulee myös luokitella sen mukaan, miten tärkeä niiden merkitys on organisaatiolle. Erityistä huomiota tulisi kiinnittää sellaisiin omaisuuseriin, joiden vahingoittuminen voi aiheuttaa organisaatiolle merkittävää haittaa. (Tunggal, 2024; Cobb, 2024)

Lisäksi on hyvä arvioida uhan tai haavoittuvuuden mahdollisuutta ja todennäköisyyttä. Taulukko 2 esittelee yksinkertaisen menetelmän riskin todennäköisyyden ja vakavuuden arvion laskemiseksi, kun arviointiasteikko on yhdestä viiteen. Kun vakavuus ja todennäköisyys riskille on pisteytetty, pisteet kerrotaan yhteen, jolloin tulokseksi saadaan riskin kriittisyys. Alla oleva taulukko antaa suuntaa sille, kuinka vakavana riskiä voidaan pitää. (Cobb, 2024)

Taulukko 2 Riskin todennäköisyyden laskeminen asteikolla 1–5 (Cobb, 2024)

Todennäköisyys					
Vakavuus	Harvinainen (1)	Epätodennäköinen (2)	Mahdollinen (3)	Todennäköinen (4)	Varma (5)
Merkityksetön (1)	1	2	3	4	5
Pieni (2)	2	4	6	8	10
Kohtalainen (3)	3	6	9	12	15
Suuri (4)	4	8	12	16	20
Kriittinen (5)	5	10	15	20	25

Vihreä: Hyväksyttävä riski

Keltainen: Siedettävä / Estettävä riski

Punainen: Eliminoitava riski

Riskien hallitsemiseksi on tärkeää kehittää kattava riskien lieventämissuunnitelma. Tämä suunnitelma sisältää toimenpiteitä ja käytäntöjä, joilla pyritään vähentämään tunnistettuja riskejä ja niiden mahdollisia vaikutuksia. Lisäksi on olennaista dokumentoida ja raportoida riskit ja niiden seuraukset asianmukaisesti, jotta organisaation johto ja sidosryhmät voivat ymmärtää niiden merkityksen ja vaikutukset. On myös tärkeää arvioida riskin seurauksia organisaatiolle kokonaisvaltaisesti, jotta voidaan ymmärtää niiden vaikutukset liiketoimintaan, ja sen jatkuvuuteen. Jatkuvalla arvioinnilla ja valvonnalla organisaatio voi tunnistaa uusia riskejä, arvioida niiden vaikutuksia ja reagoida niihin nopeasti. Tämä edistää organisaation kykyä sopeutua muuttuviin uhkiin ja säilyttää korkea tietoturvataso pitkällä aikavälillä.

(Tunggal, 2024) Kuva 4 Knowles esittää riskien arvioinnin kuusi eri askelta, joiden avulla riskien arviointia voidaan suorittaa tehokkaasti.

Kuva 4 Kuinka arvioida kyberturvallisuuden riskejä (Knowles, 2024)

Ensimmäisessä vaiheessa tulee luetteloida kaikki omaisuuserät, mukaan lukien yrityksen digitaalinen omaisuus. Tämä vaihe on keskeinen, sillä se mahdollistaa kattavan kuvan yrityksen omaisuudesta ja sen arvosta. Seuraavassa vaiheessa jokainen omaisuuserä tulee priorisoida sen kriittisyyden ja tärkeyden mukaan. Tämä auttaa resurssien kohdentamisessa ja riskienhallinnan priorisoinnissa. Kolmannessa vaiheessa tunnistetaan kaikki mahdolliset uhat ja uhkatekijät, jotka kohdistuvat omaisuuseriin. Tämä vaihe auttaa ymmärtämään potentiaalisia riskejä ja valmistautumaan niihin asianmukaisesti. Neljännessä vaiheessa

keskitytään tunnistamaan kaikki haavoittuvuudet, joita omissa digitaalisissa ympäristöissä voi olla. Tämä auttaa varmistamaan, että mahdolliset heikkoudet ja puutteet korjataan ennen kuin ne aiheuttavat vakavia ongelmia. Viidennessä vaiheessa pohditaan uhkatilanteen todennäköisyyttä, jotta voidaan arvioida, kuinka suuri riski eri uhkatekijöiden toteutumisella on. Viimeisessä, kuudennessa vaiheessa kootaan arvio uhkatilanteen toteutumisen seurauksista ja kustannuksista. Tämä auttaa organisaatiota hahmottamaan uhkatilanteen mahdolliset vaikutukset liiketoimintaan ja varautumaan niihin asianmukaisesti. (Knowles, 2024)

2.3.5 Riskien hallintatoimenpiteet

Riskien, haavoittuvuuksien, sekä uhkien tunnistaminen ja arviointi ovat vain riskienhallinnan alkua. Organisaation täytyy määritellä mitkä ovat ne toimenpiteet, joita tehdään, kun riski havaitaan. Riskin hallitsemiseksi tulee olla määritettyjä tiettyjä askeleita riskin lieventämiseksi. Pelkkä riskien tunnistaminen ja arviointi eivät riitä. On myös välttämätöntä suunnitella ja toteuttaa konkreettisia toimenpiteitä riskien hallitsemiseksi, kun ne ilmenevät. Organisaation on tiedettävä etukäteen, mitä toimia se ottaa käyttöön riskien vähentämiseksi tai torjumiseksi, jotta se voi vastata tehokkaasti mahdollisiin uhkiin ja haavoittuvuuksiin.

Teknisiä ratkaisuja riskienhallinnassa ovat esimerkiksi ohjelmistopäivityksistä huolehtiminen. Uudet päivitykset tulisi asentaa heti, kun ne ovat saatavilla. Hyökkääjät etsivät ohjelmistojen haavoittuvuuksia aktiivisesti, ja löytävät ne usein hyvin nopeasti. Säännöllisillä päivityksillä voidaan huolehtia siitä, että omat järjestelmät pysyvät turvallisena. Ohjelmistopäivitykset voidaan myös automatisoida laitteella, jolloin niiden asennuksesta ei tarvitse huolehtia itse. (Security Scorecard, 2021c)

Teknisiin toimenpiteisiin kuuluu palomuurien ja virustorjunnan asentaminen laitteille. Palomuuri on keskeinen osa verkon turvallisuutta, sillä se valvoo ja hallitsee verkkoliikennettä sekä estää luvattomat pääsy-yritykset tietoverkkoon. On kuitenkin ensiarvoisen tärkeää varmistaa, että palomuuri on asennettu oikein ja konfiguroitu asianmukaisesti. Väärin asennettu palomuuri voi päästää kaiken liikenteen läpi, jolloin sen tehokkuus heikkenee merkittävästi eikä se tarjoa riittävää suojaa verkkoon. (Security Scorecard, 2021c)

Riskienhallinnan osana tulee myös harkita käyttäjien pääsyoikeuksia. Rajoittamalla pääsynhallintaa voidaan merkittävästi rajoittaa hyökkääjän liikkumista verkossa. Tämä tarkoittaa käyttäjien oikeuksien rajaamista vain niihin tehtäviin, joissa niitä tarvitaan, ja oikeuksien poistamista heti, kun niitä ei enää tarvita. Tällainen toimintamalli vaikeuttaa

merkittävästi hyökkääjän mahdollisuuksia levittäytyä verkossa tai kasvattaa oikeuksiaan, mikäli hän saa haltuunsa käyttäjän tunnukset. (J.P. Morgan, 2022)

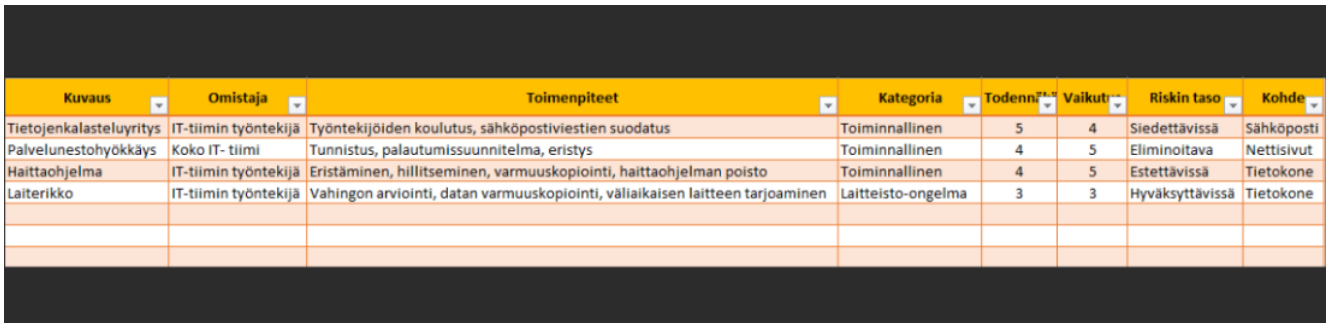
Säännöllisillä varmuuskopioilla varmistetaan kriittisen datan ja järjestelmien nopea palautuminen häiriötilanteessa. Varmuuskopiointiprosessi voidaan automatisoida, mikä vähentää inhimillisten virheiden mahdollisuutta, kuten varmuuskopion unohtamista tai virheellistä suorittamista. On tärkeää varmistaa, että varmuuskopiot säilytetään vähintään kahdessa eri paikassa, jotta varmuuskopiot ovat suojassa mahdollisilta vaaratilanteilta tai vahingoilta. (Chachak, n.d.)

Haavoittuvuuksien ja uhkien valvonta ja analysointi on yksi riskienhallinnan tärkeimmistä osista. Jatkuvalla valvonnalla voidaan löytää haavoittuvuuksia ennen pahantahtoisia tahoja, sekä pysyä kartalla oman verkon ja järjestelmien tilanteesta. (Chachak, n.d.)

Palautumissuunnitelma on keskeinen osa kyberhyökkäyksestä tai muusta häiriötilanteesta toipumisessa. On ensiarvoisen tärkeää, että jokainen organisaation työntekijä tuntee omat vastuunsa ja tehtävänsä kyseisessä tilanteessa. Palautumissuunnitelman avulla varmistetaan, että häiriötilanteessa tarvittavat resurssit otetaan käyttöön ja että ollaan valmiita toimimaan tilanteen edellyttämällä tavalla. (J.P. Morgan, 2022)

Lisäksi teknologisten ratkaisujen ohella, riskien hallinnassa voidaan käyttää riskirekisteriä. Riskirekisteri on dokumentti, johon kerätään tiedot kaikista organisaation kohtaamista riskeistä sekä toteutetuista toimenpiteistä niiden hallitsemiseksi. Riskirekisteri auttaa organisaatiota ymmärtämään ja luokittelemaan kohtaamansa riskit sekä tunnistamaan parhaat käytännöt niiden lieventämiseksi. Historiatiedon säilyttäminen riskeistä on tärkeää, koska se auttaa organisaatiota ymmärtämään, mitkä osa-alueet vaativat lisäresursseja tai huomiota. Lisäksi riskirekisterin (Kuva 5) avulla voidaan tunnistaa toistuvia riskejä ja kehittää ennaltaehkäiseviä toimenpiteitä niiden varalle. (Hyperproof Team, 2023)

Kuva 5 Esimerkki riskirekisteristä (Hyperproof Team, 2023)



Kuvaus	Omistaja	Toimenpiteet	Kategoria	Todenn	Vaikut	Riskin taso	Kohde
Tietojenkalasteluyritys	IT-tiimin työntekijä	Työntekijöiden koulutus, sähköpostiviestien suodatus	Toiminnallinen	5	4	Siedettävissä	Sähköposti
Palvelunestohyökkäys	Koko IT- tiimi	Tunnistus, palautumissuunnitelma, eristys	Toiminnallinen	4	5	Eliminoitava	Nettisivut
Haittaohjelma	IT-tiimin työntekijä	Eristäminen, hillitseminen, varmuuskopiointi, haittaohjelman poisto	Toiminnallinen	4	5	Estettävissä	Tietokone
Laiterikko	IT-tiimin työntekijä	Vahingon arviointi, datan varmuuskopiointi, väliaikaisen laitteen tarjoaminen	Laitteisto-ongelma	3	3	Hyväksyttävissä	Tietokone

2.3.6 Incident response process

Incident Response Process, eli palautumissuunnitelma, viittaa ohjeisiin, joita organisaatio noudattaa joutuessaan kyberhyökkäyksen kohteeksi. Palautumissuunnitelman tavoitteena on tunnistaa, reagoida, lieventää ja palautua häiriötilanteesta. Suunnitelman tarkoituksena on varautua turvallisuuspoikkeamiin, sekä tukea nopeaa palautumista liiketoiminnan jatkuvuuden takaamiseksi. (Irei, 2024)

Palautumissuunnitelman kehittäminen alkaa valmistautumisella. Tämä sisältää mahdollisten turvallisuusuhkien tunnistamisen, riskien arvioinnin sekä vastuualueiden määrittelyn organisaation sisällä. Seuraava vaihe on tilanteen arviointi. Kun tietomurto tapahtuu, tilanne on ensin kartoitettava ja analysoitava. On tärkeää selvittää, milloin ja missä tietomurto on tapahtunut, miten se havaittiin ja miten laajalle sen vaikutukset ulottuvat. (Ellis, n.d.; Tunggal, 2023c)

Kun tilanne on kartoitettu, tulee keskittyä vahingon hallitsemiseen. Vahinko tulee rajata, ettei se pääse vaikuttamaan organisaatiossa enempää, mutta sitä ei vielä tulisi eliminoida kokonaan. Tämä voi tarkoittaa esimerkiksi saastuneiden verkkojen rajaamista pois käytöstä, tai vaarantuneiden tilien sulkemista. Tapahtunutta vahinkoa tulisi kuitenkin päästä analysoimaan myöhemmin, jotta se voidaan jäljittää alkujuurilleen. Kun tilanne on saatu haltuun, ja vahinko on analysoitu, voidaan siirtyä eliminoimaan vahinko kokonaan. Tämä voi tarkoittaa esimerkiksi haittaohjelman poistoa, ja ohjelmistojen päivitystä. (Ellis, n.d.; Tunggal, 2023c;)

Lopuksi, kun kaikki uhat on saatu poistettua, järjestelmät ja data voidaan palauttaa normaaliin toimintatilaan. Tämä sisältää varmuuskopioiden palauttamisen, tarvittaessa järjestelmien uudelleenasennuksen sekä muiden turvallisuustoimenpiteiden käyttöönottamisen. Kun tilanne on saatu täysin normalisoitua, seuraava askel on tapahtuneen analysointi. Selvitetään mikä aiheutti ongelman ja miten vastaavilta tilanteilta

voitaisiin jatkossa välttyä. Näin päivitetään myös palautumissuunnitelmaa tulevia tilanteita varten. (Ellis, n.d.; Tunggal, 2023c;)

2.3.7 Tiedonhallinta

Arkaluontoiseksi dataksi voidaan määritellä monenlaisia tietoja, kuten taloudelliset tiedot, henkilötiedot ja liiketoiminnan kannalta olennaiset tiedot. Esimerkkejä taloudellisista tiedoista ovat pankkitiedot ja maksukorttitiedot, kun taas liiketoiminnan kannalta tärkeitä tietoja voivat olla esimerkiksi erilaiset liikesalaisuudet ja immateriaaliomaisuus. Henkilötietoihin kuuluu esimerkiksi osoitteet, syntymäajat ja jopa IP-osoitteet. On kuitenkin tärkeää huomata, että Euroopan komission mukaan henkilötiedot voidaan määritellä kaikkiin tunnistettavissa oleviin tietoihin henkilöstä, mikä laajentaa käsitettä entisestään. Tämä tarkoittaa sitä, että henkilötietoihin voi kuulua paljon muutakin kuin pelkät perinteiset henkilötunnukset tai nimitiedot. (Rudderstack, n.d.; Euroopan komissio tietosuojaryhmä, 2007, s.12)

Tiedon tulisi olla luokiteltu sen arkaluontoisuuden mukaan, jotta sitä osataan käsitellä luokittelun vaatimalla tavalla. Pääsynhallinnan merkitys korostuu erityisesti arkaluontoisen datan käsittelyssä, sillä on tärkeää varmistaa, että dataan on pääsy vain niillä, joille se on tarkoitettu. On olennaista suojata arkaluontoista dataa riittävästi sekä levossa, että käsittelyvaiheessa, ja erityisesti silloin kun tietoa tarvitsee siirtää. Tietoa siirrettäessä on huolehdittava turvallisesta yhteydestä ja varmistettava tiedon salaaminen tarvittaessa. Varmuuskopioinnin merkitys korostuu arkaluontoista tietoa säilytettäessä, sillä se varmistaa, että tietoa voidaan palauttaa tarvittaessa ja estää sen mahdollinen menetys. Lisäksi henkilökunnan kouluttaminen eri luokkien tietojen käsittelystä on tärkeää, jotta varmistetaan oikea ja turvallinen tietojenkäsittelykäytäntöjen noudattaminen. (Rudderstack, n.d.; Hutsix n.d.)

Arkaluontoista tietoa käsitellessä tulee olla tietoinen myös laista ja määräyksistä. GDPR eli General Data Protection Regulation on Euroopan parlamentin, unionin neuvoston ja komission yleinen tietosuoja-asetus, joka hyväksyttiin huhtikuussa 2016, ja sitä alettiin soveltamaan toukokuussa 2018. Euroopan komission mukaan GDPR:ää sovelletaan silloin kun yritys käsittelee henkilötietoja ja sijaitsee EU:ssa, ja silloin kun yritys sijaitsee EU:n ulkopuolella, mutta käsittelee tavaroiden tai palveluiden tarjoamiseen liittyvien henkilöiden tietoja. GDPR koskee kaikkia EU:n jäsenvaltioita. Kyseessä on suoraan sovellettava, sekä velvoittava asetus, eikä tämä vaadi jäsenvaltioilta uutta lainsäädäntöä. GDPR:n tavoitteena on edistää yksityisyyden suojaa, ja varmistaa henkilötietojen oikeudenmukainen käsittely. (Euroopan Unioni, 2022; Opitietosuojaa.fi, n.d.)

3 Kyberturvallisuuden hallintajärjestelmä

Kyberturvallisuuden hallintajärjestelmä, tunnettu myös nimellä Cyber Security Management System (CSMS), on kokonaisvaltainen viitekehys, joka kattaa ohjeistuksen, toimintaperiaatteet ja varotoimenpiteet, joiden avulla yritykset voivat tunnistaa ja arvioida kyberturvallisuuden riskejä sekä suojautua näitä riskejä vastaan tehokkaasti. Kyberturvallisuuden hallintajärjestelmä suojaa organisaation tietoja, toteuttaa riskienhallintaprosessin ja antaa sidosryhmille varmuuden siitä, että organisaatiossa otetaan asianmukaisesti huomioon kaikki riskit. On otettava huomioon, että kyberturvallisuuden hallintajärjestelmän vaatimukset ja tarpeet muuttuvat jatkuvasti ajan kuluessa. (Cyber Cops, 2023)

Tässä opinnäytetyössä järjestelmä on suunniteltu antamaan ohjeita ja parhaita käytäntöjä riskienhallinnasta, tietojen ja järjestelmien suojelusta, siitä kuinka tietojen luottamuksellisuus, eheys ja saatavuus säilytetään, sekä varmistamaan liiketoiminnan jatkuvuus. Lisäksi tässä luvussa tutustutaan lisäksi muutamaan kyberturvallisuuden standardiin, sekä parhaisiin tietoturvakäytäntöihin. Järjestelmän tietopohjana toimii ISO 27001- ja ISO 27002 -standardit.

3.1 ISO 27001:2023

ISO 27001:2023 -standardi on yhteistyössä ISO:n ja IEC:n kehittämä joukko vaatimuksia tietoturvallisuuden hallintajärjestelmälle. ISO ja IEC määrittelevät itsensä seuraavasti: ”ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) muodostavat maailmanlaajuiseen standardisointiin erikoistuneen järjestelmän. ISOn tai IEC:n kansalliset jäsenjärjestöt osallistuvat kansainvälisten standardien laadintaan näiden järjestöjen perustamissa komiteoissa, jotka käsittelevät eri tekniikan aloja.” (SFS-EN ISO/IEC 27001:2023, s. 5)

ISO 27001:2023 on kansainvälinen standardi, joka tarjoaa kattavat vaatimukset ja ohjeistukset tehokkaan kyberturvallisuuden hallintajärjestelmän kehittämiseen. Standardi sisältää yksityiskohtaiset suuntaviivat järjestelmän suunnittelulle, ylläpidolle ja jatkuvan parantamisen tukemiselle. Standardi tarjoaa viitekehyksen, jonka avulla organisaatiot voivat hallita ja suojata digitaalista omaisuuttaan sekä arkaluontoista dataa. Standardin keskeiset osa-alueet kattavat riskien arvioinnin ja käsittelyn, tietoturvapolitiikan kehittämisen, pääsynhallinnan, johdon sitoutumisen kyberturvallisuuteen sekä jatkuvuuden parantamisen. (SFS-EN ISO/IEC 27001:2023)

3.2 ISO 27002:2022

ISO ja IEC määrittelevät ISO27002:2022 -standardin seuraavasti: ”Asiakirja on tarkoitettu viiteasiakirjaksi tietoturvariskien käsittelyn hallintakeinojen määrittämisen ja toteuttamiseen standardin ISO/IEC 27001 mukaisessa tietoturvallisuuden hallintajärjestelmässä.” (SFS-EN ISO/IEC 27002:2022) ISO 27002 on kansainvälinen standardi kuten ISO 27001, ja se tarjoaa ohjeita ja parhaita käytänteitä tietoturvan valvomiseen.

ISO 27002 -standardi tarjoaa ohjeita ja käytänteitä tietoturvan hallintajärjestelmän perustamiseen, toteutukseen sekä ylläpitoon. ISO 27002 tarjoaa myös ohjeita tietoturvallisuuden hallintajärjestelmän parantamiseen. Standardi syventyy parhaisiin tietoturvakäytäntöihin kattavammin kuin ISO 27001, ja onkin siksi hyvä standardi ISO 27001:n rinnalla kyberturvallisuuden hallintajärjestelmää rakennettaessa. Standardin keskittyy laajasti organisaation tietoturvaan, tietojen turvallisuuteen sekä henkilöstön tietoturvaan- ja turvallisuuteen. Standardi kattaa myös fyysisen turvallisuuden kuten kulunvalvonnan, laitteiden suojauksen, työskentelyn turva-alueilla sekä sen, kuinka suojaudutaan fyysisiä ympäristön aiheuttamia uhkia vastaan. (SFS-EN ISO/IEC 27002:2022)

ISO 27001 ja ISO 27002 ovat sovellettavissa eri kokoisille ja eri aloilla toimiville organisaatioille, sillä standardien keskeinen periaate on organisaation tietojen suojaaminen. ISO/IEC standardisarjasta löytyy täydentäviä ohjeita ja vaatimuksia tietoturvallisuuden kokonaishallintaprosessin eri näkökulmista. Lisäksi ISO/IEC standardeja on laadittu erityisesti tiettyjen toimialojen tarpeisiin, kuten esimerkiksi pilvipalveluille, tietosuojalle sekä terveydelle. (SFS-EN ISO/IEC 27002:2022)

3.3 NIST Cybersecurity Framework version 1.1

NIST, eli National Institute of Standards and Technology, on Yhdysvaltain kauppaministeriön (United States Department of Commerce) jäsen, ja yksi maan vanhimmista tieteen laboratorioista. NIST pyrkii edistämään innovaatioita ja teollisuuden kilpailukykyä, mikä sisältää myös standardien kehittämisen. (NIST, 2022)

NIST:n kehittämä Cybersecurity Framework käsittää ohjeita, suuntaviivoja, ja parhaita käytäntöjä kyberturvallisuuden hallintaan ja kehittämiseen organisaatioissa. NIST:n viitekehys tarjoaa joustavia toimintatapoja, joita voidaan soveltaa eri toimialoilla. Viitekehyksen avulla organisaatio voi tunnistaa omat kyberturvallisuuden tarpeensa sekä kehittää menetelmiä kyberuhkien ja hyökkäysten tunnistamiseen, havaitsemiseen,

suojaamiseen ja niistä palautumiseen. (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018)

Viitekehys keskittyy kolmeen eri osa-alueeseen, jotka ovat viitekehyksen ydin, toteutus, sekä kehityksen profiilit. Viitekehyksen ydin keskittyy kyberturvallisuuden eri toimiin, mahdollisiin tuloksiin, sekä tieteellisiin viitteisiin. Toteutus keskittyy tarjoamaan organisaatioille työkaluja omiin kyberturvallisuuden lähestymistapoihin, sekä niiden ymmärtämiseen, joka auttaa saavuttamaan kyberturvallisuuden tavoitteet. Kehityksen profiilit auttavat organisaatiota priorisoimaan kyberturvallisuustoimet liiketoimintansa vaatimusten, riskiensietokyvyn ja resurssien mukaan. NIST:n kehittämä viitekehys tarjoaa ohjeita riskienhallintaan, kyberturvallisuuden hallintatoimiin, sekä jatkuvuuden parantamiseen. (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018)

NIST Cybersecurity Framework Versio 1.1 on paranneltu julkaisu versiosta 1.0, joka on julkaistu helmikuussa 2014. Viitekehyksestä on tulossa versio 2.0, joka on ilmoitettu julkaistavaksi helmikuun lopulla vuonna 2024. (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018; NIST Cybersecurity Framework n.d.)

3.4 PiTuKri

PiTuKri eli pilviturvallisuuden arviointikriteeristö toimii pilvipalveluihin tallennetun salassa pidettävän tiedon turvallisuuden arvioinnin työkaluna. PiTuKri on kehitetty huomioiden Suomen kansalliset tarpeet. Kriteeristö käsittelee kansallisesti salatuiksi luokiteltujen, sekä turvallisuusluokiteltujen tietojen suojausperiaatteita. Kriteeristössä esitetyt turvallisuusvaatimukset on suunniteltu pitämään yleisimpien salassa pidettävien tietojen riskit hallittavalla tasolla. Korkeamman turvallisuusluokan tietoihin kriteeristö ottaa kantaa vain yleisen soveltuvuuden arvioinnin yhteydessä, sekä antaa suuntaviivoja tähän. Kriteeristöä voidaan käyttää myös viranomaisten tietojen suojaamisessa, sekä yritysten tarpeisiin. Tulee kuitenkin huomioida, että kriteeristö on tarkoitettu käytettäväksi vain pilvipalveluiden turvallisuutta arvioidessa. (Traficom kyberturvallisuuskeskus, 2019)

PiTuKri on jaettu 11 eri osa-alueeseen, jotka ovat 1. Esiehdot, 2. Turvallisuusjohtaminen, 3. Henkilöstöturvallisuus, 4. Fyysinen turvallisuus, 5. Tietoliikenneturvallisuus, 6. Identiteetin ja pääsyn hallinta, 7. Tietojärjestelmäturvallisuus, 8. Salaus, 9. Käyttöturvallisuus, 10. Siirrettävyys ja yhteensopivuus, ja 11. Muutostenhallinta ja järjestelmäkehitys. PiTuKri:ssa määritellään, että osa-alueista tärkein on ensimmäinen, esiehdot, sillä tämä määrittelee jatkoarvioinnin mahdollisuudet, sekä tukevat salassa pidettävän tiedon suojaamista riskienhallinnassa. Esiehtojen täyttyminen ei tarkoita tiedon olevan riittävästi suojattu, lisäksi

tulee huomioida lopuissa osa-alueissa kuvatut toimenpiteet. Osa-alueet muodostuvat vaatimuskorteista, joissa kuvataan vaatimuksen teema, konkreettinen vaatimus, vaatimuksen soveltamiskohteet, suojaustavoite sekä muita lisätietoja toteuttamisen tueksi. Vaatimukset on suunniteltu joustaviksi ja mahdollistamaan erilaisia toteutustapoja. Osassa vaatimuksista keskitytään salassa pidettävän tiedon suojaamiseen, ja osassa turvallisuusluokitellun salassa pidettävän tiedon suojaamiseen. Jokaisen vaatimuksen yhteydessä on selitetty mihin tietotyyppiin se kohdistuu. (Traficom kyberturvallisuuskeskus, 2019)

Kriteeristö tarjoaa myös esimerkkejä vaatimuskohtien kohdentamisesta, kriteeristön soveltamisesta vaatimuksenmukaisuusarviointiin, sekä viranomaisarvioinnista, ja hyväksynnästä. PiTuKri-arviointikriteeristö on saatavilla Traficomin kyberturvallisuuskeskuksen sivuilta PDF-muodossa, sekä sen lisäksi saatavilla on Excel-muotoinen arviointityökalu. Traficomin kyberturvallisuuskeskuksen mukaan arviointikriteeristö on vapaasti käytettävissä, kun nimetään alkuperäinen lähde. Kriteeristö tarjotaan sellaisenaan, kuin se on sivulla tarjottuna. (Traficom kyberturvallisuuskeskus, 2019)

3.5 Parhaat tietoturvakäytännöt

Organisaatiossa tulee määritellä tietoturvapolitiikka, joka sitoo koko henkilöstöä. On ensiarvoisen tärkeää, että ylin johto sitoutuu tietoturvapolitiikkaan, sillä se luo vankan perustan koko organisaation tietoturvallisuudelle ja varmistaa, että tietoturvaa pidetään tärkeänä tavoitteena liiketoiminnassa. Selkeästi määritelty tietoturvapolitiikka varmistaa liiketoiminnan jatkuvuuden, sekä sen että organisaation toiminta on soinnussa sovellettavien lakien ja asetusten kanssa. Tietoturvapolitiikan tulisi sisältää selkeästi tietoturvallisuuden määritelmät, tavoitteet ja periaatteet, jotka ohjaavat turvallista toimintaa, sekä sitouttavat jatkuvaan tietoturvan parantamiseen. Lisäksi on tärkeää määritellä vastuut ja tehtävät oikeille henkilöille tietoturvatyön toteuttamiseksi ja varmistaa, että organisaatiolla on selkeät prosessit tietoturvapoikkeamien käsittelyä varten. (SFS-EN ISO/IEC 27002:2022)

Tietoturvapolitiikkaa tulee tukea henkilöstötasolla kohdennetuilla toimintaperiaatteilla. Näiden toimintaperiaatteiden tulisi täydentää tietoturvallisuuden hallintakeinojen toteuttamista. Kohdennetut toimintaperiaatteet ovat sellaisia, jotka vastaat tiettyjen ryhmien tarpeisiin, tai kattavat tietyt tietoturvan alueet. Kohdennettujen periaatteiden tulee olla yhdenmukaisia muun tietoturvapolitiikan kanssa. Kohdennettujen toimintaperiaatteiden kehitysvastuu, sekä laadun arviointi on annettava vain pätevälle ja asiantuntevalle henkilöstölle, joka voidaan valtuuttaa hyväksymään ne. Esimerkkejä kohdennetuista tietoturvan toimintaperiaatteista ovat esimerkiksi pääsynhallinta, omaisuudenhallinta, verkkoturvallisuus, varmuuskopiointi, teknisten haavoittuvuuksien hallinta ja fyysinen turvallisuus. (SFS-EN ISO/IEC 27002:2022)

Tietoturvapolitiikka ja sen kohdennetut toimintaperiaatteet tulee katselmoida säännöllisesti. Katselmoinnissa tulee ottaa huomioon jatkuvasti muuttuva uhkakuva, sekä parantamismahdollisuuksien arviointi. Sen lisäksi tulee arvioida onko hallintaa muutettava, jos muutoksia kohdistuu organisaatiossa liiketoimintaan, tekniseen ympäristöön, lakeihin tai asetuksiin, tietoturvariskeihin tai silloin kun tietoturvatapahtumista on saatu uutta tietoa. (SFS-EN ISO/IEC 27002:2022)

Tietoturvapolitiikasta tulee viestiä henkilöstölle, sekä sidosryhmille soveltuvasti ja ymmärrettävästi. On huomioitava henkilöstön rooli organisaatiossa suhteessa tiedon määrän tarpeeseen ja ymmärrettävyyteen. Henkilöstö tulee osaltaan velvoittaa vahvistamaan, että tietoturvapolitiikka on ymmärretty, sekä sitoutumaan siihen. Jos tietoturvapolitiikkaa on tarpeen jakaa ulkopuolisille, on huomioitava luottamuksellisten tietojen riittävä salaus. (SFS-EN ISO/IEC 27002:2022)

3.5.1 Vahva pääsynhallinta

Pääsynhallinta tarkoittaa prosessia, jossa säädetään käyttäjien pääsyä resursseihin, ohjelmistoihin tai tietoihin. Pääsyoikeus voidaan antaa joko käyttäjälle, tai esimerkiksi koneelle tai palvelimelle. Pääsynhallinta on yksi tietoturvakäytäntöjen kulmakivistä. Pääsynhallinnan tarkoituksena on varmistaa, että tietoihin pääsevät käsiksi vain oikeutetut henkilöt. Pääsynhallinnan sääntöjä luokiteltaessa lähtökohtana tulisi olla *vähimmän oikeuden periaate* (principle of least privilege), eli kaikki on kiellettyä, ellei sitä ole erikseen sallittu. Käyttö, - tai katseluoikeus taataan vain tarvittaessa niille, jotka sitä työnkuvansa puolesta tarvitsevat. Oikeudet tulee tarkistaa ja arvioida säännöllisesti. Vahva pääsynhallinta tukee luotettavuutta ja eheyttä tietoja säilytettäessä. Vahva pääsynhallinta tulisi olla mukana jokaisen tietoteknisen ympäristön ylläpidossa ja kehittämisessä. (SFS-EN ISO/IEC 27002:2022)

3.5.2 Tietojen salaaminen ja eheys

Tietoja salattaessa tiedot tulee ensin luokitella sen arkaluontoisuuden, tärkeyden tai muiden kriteereiden mukaan, jotta voidaan määritellä riittävät suojaustoimenpiteet. Tietojen salaus varmistaa tiedon luottamuksellisuuden, aitouden ja eheyden säilyvyyden. Tietojen säilytyksessä, sekä salaamisessa tulee myös ottaa huomioon kansalliset määräykset ja vaatimukset, kuten GDPR. Tietojen suojaamisessa tulee määritellä kohdennetut toimenpiteet, jotta voidaan varmistaa salauksen tehokkuus. Asianmukaisesti toteutettu salaus auttaa ehkäisemään tiedon asiatonta tai virheellistä käyttöä, ja suojelemaan organisaation mainetta. Ulkopuolisia salauspalveluiden toimittajia käytettäessä tulee

huomioida, että osapuolien sopimus kattaa vahinkovastuun, luotettavuuden, sekä vasteaikoihin liittyvät kysymykset. (SFS-EN ISO/IEC 27002:2022)

Tietojen salauksessa tulee määritellä standardit ja salausalgoritmit, joita käytetään, salakirjoituksen vahvuus, erilaiset salausratkaisut, sekä muut käyttöä koskevat käytännöt. Lisäksi tulee määritellä miten salausta käytetään suojaamaan tietoja, jotka sijaitsevat käyttäjien siirrettävillä laitteilla (data on levossa, rest), sekä niitä tietoja, joita siirretään verkon välityksellä käyttäjien laitteelta toiselle (data on siirrossa, in transit). (SFS-EN ISO/IEC 27002:2022)

Tietojen salauksessa on huomioitava myös eri avaintenhallinnan menettelyt, eli salausavainten luonti, suojaus, tiedon palauttaminen, sekä toimenpiteet, jos salausavaimet katoavat. Salausavaimet, sekä laitteet, jolla niitä säilytetään, tulee suojata asianmukaisesti. (SFS-EN ISO/IEC 27002:2022)

Salausalgoritmit auttavat mahdollistamaan tiedon eheyden, sekä estää tiedon muuttumisen tai väärentymisen sen elinkaaren aikana. Lisäksi salaus auttaa todentamaan organisaation tietoturvaa. Salaustekniikkaa voidaan käyttää luomaan todisteita siitä, onko jokin tapahtuma tai toiminto todella tapahtunut. Salauksella voidaan varmentaa käyttäjien identiteetti pääsyoikeutta pyydettäessä. (SFS-EN ISO/IEC 27002:2022)

3.5.3 Jatkuvuuden hallinta

Liiketoiminnan jatkuvuuden kannalta on oleellista määritellä tärkeimmät toiminnot häiriötilanteen sattuessa. Näille toiminnoille tulee määritellä palautumisaikatavoite. Palautumisaikatavoite tarkoittaa siis pisintä hyväksyttävää ajanjaksoa, jonka aikana liiketoiminta, sen prosessit, tai järjestelmät voivat olla poissa käytöstä häiriön aikana tai sen jälkeen. Palautumisaikatavoite on siis aikaikkuna sille ajalle, jolla organisaatiossa pyritään palauttamaan toiminta normaalille tasolle. Palautumisaikatavoite perustuu järjestelmien kriittisyyteen, sekä toiminnan mahdollisen pysähtymisen vaikutukseen. (SFS-EN ISO/IEC 27002:2022)

Organisaatiossa tulisi määritellä strategia, jossa otetaan huomioon häiriötilanteisiin varautuminen, häiriötilanteen hallinta, sekä häiriötilanteesta toipuminen. Häiriötilanne voi tarkoittaa esimerkiksi kyberhyökkäystä, mutta sillä voidaan viitata myös muihin liiketoiminnan kannalta haitallisiin tapahtumiin, kuten esimerkiksi tulipaloon liiketiloissa. Strategiaan perustuen tulee määritellä palautumissuunnitelma (incident response plan), jossa on

määritelty ennalta tarvitut palvelimet, joilla voidaan palauttaa tiedon normaali saatavuustaso häiriötilanteen jälkeen. (SFS-EN ISO/IEC 27002:2022)

Palautumissuunnitelmassa tulee olla määriteltynä eri vastuualueet ja roolit henkilöstölle ja strategia häiriötilanteeseen reagoinnista. Strategiassa eritellään toimintasuunnitelma tieto- ja viestintäteknisille häiriötilanteille, sekä suorituskyky- ja kapasiteettimäärittelyt. Tiedon, sekä palveluiden hallinta on tärkeä osa liiketoiminnan jatkuvuutta. Tehokkaan palautumissuunnitelman avulla voidaan hallita ja toipua tietoturvahäiriöistä, minimoiden niiden vaikutuksia liiketoimintaan. (SFS-EN ISO/IEC 27002:2022)

3.5.4 Henkilökunnan koulutus

Henkilökunnan riittävä tietoturvakoulutus on olennainen osa tietoturvapolitiikkaa. Henkilöstön tulee riittävällä tasolla ymmärtää tieto- ja kyberturvallisuuteen liittyvät käsitteet, sekä uhat ja riskit, joita organisaatio voi kohdata, sekä näihin liittyvät hallitsemistoimenpiteet. Henkilöstön koulutus tulee toteuttaa tietoturvapolitiikan kanssa samassa linjassa, huomioiden kohdennetut toimintaperiaatteet. Koulutuksessa tulee huomioida henkilöstön työnkuva, ja kohdentaa tiedon laajuus ja ymmärrettävyys sen mukaisesti. Lisäksi tulee arvioida henkilöstön tietoturvan ymmärryksen tasoa ennen koulutusta, jotta voidaan varmistaa, että koulutuksen tavoitteet saavutetaan. Riittävää koulutusta tulee järjestää säännöllisin väliajoin, ja koulutusmateriaalin olisi hyvä pohjustua aikaisemmista häiriötilanteista opittuihin asioihin. (SFS-EN ISO/IEC 27002:2022)

Henkilökunnan koulutuksen tulisi kattaa ainakin yksilön vastuu omista tekemisistä, yleiset vastuut liittyen organisaation ja sidosryhmien tietojen suojaamiseen, yleiset tietoturvamenettelyt, sekä tietoturvasta vastaavien yhteystiedot. Lisäksi henkilöstöä tulee neuvoa siinä, mistä saa lisää tietoa ja tukea aiheeseen liittyen. Koulutuksessa tulee painottaa johdon, ja koko henkilöstön sitoutumista yhteiseen tietoturvapolitiikkaan. Organisaation tulee lisäksi varmistaa, että tietoturvasta vastaavilla henkilöillä on riittävät resurssit ja laitteet tietoturvan toteuttamiseksi, sekä mahdollisuus hankkia näitä lisää tarvittaessa. Tietoturvasta vastaaville henkilöille tulee tarjota mahdollisuutta kouluttautua asianmukaisesti, sekä heidän on pidettävä tietämyksensä ajan tasalla. Henkilöstön on tiedostettava tietoturvan merkitys, sekä se miten heidän toimintansa voi vaikuttaa organisaatioon. (SFS-EN ISO/IEC 27002:2022)

3.5.5 Järjestelmien ja ympäristöjen suojaaminen

Tietoturvapolitiikan, sekä henkilöstön riittävän koulutuksen lisäksi tietoturvan parantamiseksi tulee toteuttaa teknisiä ratkaisuja. Haittaohjelmilta suojautuminen on yksi teknisen tietoturvan olennaisimmista askelista. Haittaohjelmilta suojautuminen tulee rakentaa haittaohjelmien havaitsemis- ja korjaustoimenpiteiden varaan. Haittaohjelmien havaitsemis- ja korjaustoimenpiteiden lisäksi on tärkeää ottaa käyttöön hallintakeinoja, joilla estetään luvattomien ohjelmien käyttö laitteilla, kuten ylläpitämällä listaa sallituista ohjelmistoista. Tämän lisäksi on estettävä pääsy haitallisille verkkosivuille organisaation laitteilla sekä säännöllisesti tarkistettava kriittisten ohjelmistojen sisältö. On myös laadittava suojaustoimenpiteitä riskeille, jotka liittyvät ulkopuolisten tarjoamaan sisältöön. On suositeltavaa asentaa haittaohjelmien havaitsemiseen tarkoitettuja ohjelmistoja organisaation hallinnoimille laitteille. Lisäksi verkon ja sähköisten tallennusvälineiden kautta saapuneet tiedot tulee tarkistaa haittaohjelmien varalta, sekä sähköpostien ja muiden viestien liitetiedostojen luotettavuus tulee tarkistaa ennen niiden käyttöä. (SFS-EN ISO/IEC 27002:2022)

Haittaohjelmilta suojautumisen lisäksi on huomioitava teknisten haavoittuvuuksien hallinta. Omaisuuserät tulee olla luokiteltuna, ja luettelossa tulee olla huomioituna vähintään omaisuuden toimittaja, nimi, versionumero, käyttötilanne, sekä käyttäjä. Haavoittuvuuksien hallinnassa tulee olla määriteltynä vastuuhenkilöt ja heidän roolinsa, sekä haavoittuvuuksien seuranta, riskien arviointi, sekä tarvittava tiedon päivittäminen. Lisäksi voidaan toteuttaa suunniteltuja tunkeutumistestejä organisaation ympäristöihin osana haavoittuvuuksien hallintaa. Tunkeutumistestien tulee olla aina ennalta sovittuja, sekä niitä saa suorittaa vain pätevä ja osaava henkilöstö. Tunkeutumistestit tulee dokumentoida, ja niiden tulee olla tarvittaessa toistettavissa. Lisäksi organisaation tulee varmistaa sisäisten ja ulkoisten uhkaraporttien saatavuus ja vastaanotto. (SFS-EN ISO/IEC 27002:2022)

Teknisiä haavoittuvuuksia tulee käsitellä asianmukaisesti. Päivitysten riittävän saatavuuden varmistamiseksi on toteutettava valvottu hallintaprosessi, joka takaa säännölliset ohjelmistopäivitykset. On tärkeää noudattaa määriteltyä aikataulua haavoittuvuuksiin reagoimisessa, käyttää vain luotettavia korjaustiedostoja, ja kiinnittää erityistä huomiota riskialttiisiin ympäristöihin. Lisäksi korjausten aitous tulee varmistaa asianmukaisilla toimenpiteillä. Teknisten haavoittuvuuksien hallinnasta tulee pitää tapahtumalokia, sekä hallinnan prosessi tulee tarkastaa ja arvioida säännöllisesti. (SFS-EN ISO/IEC 27002:2022)

3.5.6 Fyysinen turvallisuus

Digitaalisen turvallisuuden lisäksi myös fyysisestä turvallisuudesta tulee huolehtia. Organisaation on varmistettava, että luvaton pääsy toimistotiloihin estetään tehokkaasti. Fyysiset tiedot ja omaisuus on suojattava luvattomalta käytöltä, esimerkiksi turvaamalla korkean turvallisuustason tilat siten, ettei satunnaisilla henkilöillä ole niihin pääsyä. Lisäksi on tärkeää varmistaa, että sisäiset yhteystiedot, kartat ja muut tietojenkäsittelyn palvelinten sijaintitiedot eivät ole näkyvissä oikeudettomille henkilöille. Toimitiloja tulee myös valvoa riittävästi erilaisilla toimenpiteillä, joita voivat olla esimerkiksi kameravalvontajärjestelmät, vartijat tai muu henkilöstön kulunvalvonta. Valvontajärjestelmän suunnittelua tulee pitää luottamuksellisena, sillä sen paljastuminen voi altistaa turvallisuuspoikkeamille. (SFS-EN ISO/IEC 27002:2022)

4 Kyberturvallisuuden hallintajärjestelmä organisaatiossa

Kyberturvallisuuden hallintajärjestelmä organisaatiossa on olennainen osa nykyaikaista tietoturvaa. Hallintajärjestelmä on suunniteltu suojaamaan organisaation tietoja ja järjestelmiä erilaisilta tietoturvauhilta. Tässä luvussa pohditaan, miksi kyberturvallisuuden hallintajärjestelmä on tärkeä osa organisaation toimintaa, mitä hyötyjä ja haasteita siihen liittyy, sekä millaisia ovat yleisimmät kyberturvallisuuden haasteet, joita pienet yritykset kohtaavat. Pohdintaa varten on haastateltu kyberturvallisuuden ammattilaista, jolla on osaamista ISO 27001 standardin parissa.

4.1 Kyberturvallisuuden hallintajärjestelmän edut

Yksi keskeisimmistä syistä kyberturvallisuuden hallintajärjestelmän käyttöönottamiseen on organisaation tietoturvan parantaminen ja riskienhallinnan tehostaminen. Kyberturvallisuuden hallintajärjestelmä tarjoaa rakenteet, prosessin ja toimenpiteet riskien tunnistamiseen, arviointiin ja hallintaan, joka edistää liiketoiminnan jatkuvuutta. Haastatellun kyberturvallisuuden ammattilaisen mukaan hallintajärjestelmä tarjoaa edellä mainittujen lisäksi mahdollisuuden jatkuvalle toiminnan kehitykselle, sillä kyberturvallisuus on ala, joka vaatii jatkuvaa kehitystä, eikä täydellisyyteen päästä välttämättä koskaan. Hallintajärjestelmän avulla voidaan kuitenkin pyrkiä jatkuvaan toiminnan parantamiseen.

Kyberturvallisuuden hallintajärjestelmän avulla voidaan arvioida omaa kyberturvallisuuden kypsyystasoa, sekä toimintaa kyberturvallisuuden eri osa-alueilla. Kyberturvallisuuden ammattilaisen mukaan hallintajärjestelmän käyttö mahdollistaa sen, että organisaatio voi tunnistaa kehityskohteet ja mahdolliset huomaamatta jääneet osa-alueet, jotka vaativat parannusta. Näiden kehityskohteiden tunnistaminen mahdollistaa tiettyjen kyberturvallisuusriskien pienentämisen tai jopa eliminoinnin. Lisäksi, jos resurssit tai osaaminen eivät riitä, riskienhallintaa voidaan tarvittaessa ulkoistaa.

4.2 Kyberturvallisuuden hallintajärjestelmän käyttöönotto

Hallintajärjestelmän käyttöönotto on prosessi, joka vaatii suunnittelua, oman kyberturvallisuuden tilan arviointia, resurssien kohdentamista, ja organisaation sekä erityisesti johdon sitoutumista.

Kyberturvallisuuden ammattilaisen suosituksesta ensimmäinen askel on tunnistaa oman organisaation turvallisuuden tilanne. Tämä tapahtuu suorittamalla kattava arviointi

kyberturvallisuuden tilasta, jonka avulla tunnistetaan ne osa-alueet, jotka vaativat kehittämistä tai ovat jääneet kokonaan toteuttamatta. Tärkeä lisätoimenpide on laatia koko organisaatiota sitouttava tietoturvapolitiikka, joka määrittelee tietyt toimintatavat ja ohjeistukset. Tällä varmistetaan, että kaikki organisaation jäsenet ovat tietoisia turvallisuusvaatimuksista ja toimivat yhdenmukaisesti.

Kyberturvallisuuden hallintajärjestelmän käyttöönottoon liittyy myös haasteita. Yksi merkittävimmistä on hallintajärjestelmän sulauttaminen organisaation toimintaan. Lisäksi kyberturvallisuuden uhkat ja teknologiat kehittyvät jatkuvasti, mikä vaatii järjestelmän jatkuvaa päivittämistä ja kehittämistä. Myös kyberturvallisuuden ammattilaisen näkemyksen mukaan yksi haastavimmista asioista on turvallisen toiminnan jalkauttaminen päivittäiseen toimintaan. Kyberturvallisuuden tulisi olla sisäänrakennettuna kaikessa organisaation toiminnassa, sen sijaan että se nähdään erillisenä lisänä liiketoiminnan strategian päällä. Lisäksi on tärkeää, että kyberturvallisuudesta huolehtiminen on jokaisen työntekijän vastuulla, sen sijaan että vain tietotekniikan yksikkö huolehtisi siitä.

4.3 Henkilöstön sitouttaminen ja strategian suunnittelu

Kyberturvallisuuden hallintajärjestelmän rinnalla on olennaisen tärkeää varmistaa työntekijöiden sitouttaminen turvallisuuskäytäntöjen noudattamiseen. Kyberturvallisuuden ammattilaisen suositus tähän on panostaa henkilöstön koulutukseen ja yleisen tietoisuuden lisäämiseen. On myös tärkeää toistuvasti käydä läpi näitä aiheita, jotta voidaan varmistua, että henkilöstö ymmärtää ne kunnolla. Lisäksi on hyödyllistä korostaa turvallisia toimintatapoja, jotta ne juurtuvat osaksi organisaation kulttuuria, ja varmistaa ettei nämä toimintatavat haittaa tai hidasta työntekoa. Voidaan myös harkita, onko tarpeellista määritellä seuraamuksia niille työntekijöille, jotka eivät noudata sovittuja turvallisuuskäytäntöjä.

Kun valitaan kyberturvallisuuden strategiaa, on tärkeää ottaa huomioon organisaation liiketoiminnan tavoitteet ja kohdentaa strategia sekä toimenpiteet näiden mukaisesti. Kyberturvallisuuden ammattilainen korostaa, että merkittävässä asemassa ovat myös erilaiset lainsäädännöt, joita on noudatettava kyberturvallisuutta toteutettaessa. Lisäksi on keskeistä huomioida riittävä resursointi riskien hallintaa toteutettaessa sekä valittaessa sopivia teknisiä työkaluja.

Yleisimpiä kyberturvallisuuden haasteita pienille organisaatioille ammattilaisen mukaan ovat riittämättömät resurssit sekä se ettei henkilöstön koulutukseen välttämättä pystytä panostamaan riittävästi. Tietoturvakulttuurin vakiinnuttaminen organisaatiossa voi olla haastavaa, jos tarvittavia resursseja ei ole käytettävissä. Erityisesti yhteiskunnallisesti

merkittävillä toimialoilla toimivien organisaatioiden on oltava erityisen valppaina, sillä heillä saattaa olla hallussaan haluttuja tietoja, mikä voi tehdä heistä houkuttelevan kohteen kyberhyökkääjille.

Kyberturvallisuuden ammattilaisen näkemyksen mukaan hallintajärjestelmä tarjoaa kuitenkin tehokkaan keinon torjua riskejä ja määrittää selkeät vastuut ja toimintaperiaatteet. Lisäksi hallintajärjestelmän, erityisesti riskienhallinnan, jatkuvalla ylläpidolla voidaan asianmukaisesti varautua häiriötilanteisiin ja vastata hyökkäyksiin tehokkaasti.

Yhteenvetona voidaan todeta, että kyberturvallisuuden hallintajärjestelmä on tärkeä osa organisaation turvallisessa toiminnassa, sekä riskienhallinnassa. Hallintajärjestelmän avulla organisaatio voi tehokkaasti suojautua erilaisilta kyberuhilta ja varmistaa liiketoiminnan jatkuvuuden. Systemaattinen lähestymistapa, jatkuva kehitys ja henkilöstön osallistaminen ovat avainasemassa onnistuneen kyberturvallisuuden hallintajärjestelmän toteuttamisessa ja ylläpitämisessä.

4.4 Prototyyppi hallintajärjestelmästä

Opinnäytetyössä kehitettiin Excel-työkirjaprototyyppi, jonka tarkoituksena on helpottaa kyberturvallisuuden hallintajärjestelmän kehittämistä ja ylläpitoa. Työkirja koostuu erilaisista välilehdistä, joilla on jokaisella oma merkityksensä osana hallintajärjestelmää. Tätä prototyyppiä on lähdetty kehittämään riskienhallinnan näkökulmasta, ja sen painopiste on riskeihin liittyvissä prosesseissa, ei niinkään teknisten toiminnallisuuksien toteuttamisessa. Työkirja tarjoaa kattavia ohjeita, sekä valmiita pohjia erilaisiin riskienhallinnan prosesseihin, esimerkiksi riskirekisterin ylläpitoon yhdessä paikassa. Työkirjan avulla voidaan myös arvioida organisaation kyberturvallisuuden kypsyyden tasoa.

Kyberturvallisuuden kypsyystaso -välilehti tarjoaa ensimmäisenä vaiheena mahdollisuuden arvioida organisaation kyberturvallisuuden kypsyystasoa. Välilehti koostuu erilaisista taulukoista, joissa käydään läpi organisaation toteuttamia kyberturvallisuustoimenpiteitä. Kunkin kysymyksen kohdalla käyttäjä voi valita alasvetovalikosta vastauksen: ei toteutettu, osittain toteutettu tai kokonaan toteutettu. Kun kaikkikin kysymyksiin on vastattu, saadaan kokonaiskuva oman kyberturvallisuuden tilanteesta. Tämä auttaa tunnistamaan huomiotta jääneet osa-alueet, sekä missä ollaan jo onnistuttu. Oman kypsyystason arviointi on jatkuva prosessi, ja tarkoituksena on, että omaa tilaa käydään arvioimassa täällä säännöllisesti.

Digitaalisen omaisuuden -välilehdellä käsitellään digitaalisen omaisuuden käsitettä ja sen hallintaa. Esimerkkejä digitaalisista omaisuuseristä esitetään yhdessä rekisterin kanssa, joka auttaa niiden tehokkaassa hallinnassa. Lisäksi välilehdellä on linkki toiselle välilehdelle, jossa tarjotaan valmis rekisteripohja digitaalisen omaisuuden ylläpitoa varten.

Riskien kartoittamisen -välilehdellä käsitellään ensin haavoittuvuuksien ja uhkien tunnistamisen käsitettä ja käydään läpi niiden määritelmät. Lisäksi esitetään SWOT-analyysi haavoittuvuuksien hallinnan strategisen näkökulman vahvistamiseksi. Välilehdellä esitellään lisäksi menetelmiä uhkien tunnistamiseksi ja kuinka niiden vaikutusta ja todennäköisyyttä voidaan arvioida asteikolla 1–5.

Tällä välilehdellä käsitellään myös riskien kvalitatiivista arviointia, jossa arviointiasteikko vakavuudelle ja todennäköisyydelle on 1–5. Arviointiasteikolla 1 merkitsee pienintä ja 5 suurinta arvoa. Jokainen riski saa pisteytyksen todennäköisyydeltään ja vakavuudeltaan yhdestä viiteen, ja nämä pisteet summataan yhteen. Tämä summa osoittaa riskin kriittisyyden tason. Riskit, joiden pisteytys on 2–6, katsotaan hyväksyttäviksi, kun taas riskit, joiden pisteytys on 8–12, luokitellaan siedettäviksi. Erityisen korkean riskin tapauksessa, joiden pisteytys on 15–25, pyritään poistamaan riski kokonaan. On kuitenkin tärkeää huomata, että tämä taulukko on vain suuntaa antava. Todellinen riskien arviointi vaatii tapauskohtaista harkintaa, jossa otetaan huomioon omaisuuserän merkitys ja erityiset uhkakuvat.

Kvalitatiivisen arvioinnin lisänä on esitelty riskienhallinnan kuusi eri päävaihetta, sekä hieman sitä, millaisia teknisiä toimenpiteitä riskien hallitsemiseksi voidaan toteuttaa. Välilehdellä on myös linkki riskirekisterin esittelyyn.

Riskirekisteri -välilehdellä esitellään riskirekisteriä ja sen tarkoitusta. Lisäksi näytetään kuva toteutetusta riskirekisteristä. Riskien todennäköisyyttä, vaikutusta ja kriittisyyttä, sekä riskien tasoa on arvioitu riskirekisterissä käyttäen kvalitatiivisen arvioinnin periaatteita, jotka on esitelty riskien kartoittamisen välilehdellä. Lisäksi välilehdellä on linkki valmiiseen riskirekisteripohjaan.

Tietoturvakäytännöt -välilehdellä esitellään tietoturvapolitiikkaa ja sen tarkoitusta, sekä jaetaan parhaita yleisiä tietoturvakäytäntöjä.

Incident response -välilehdellä esitellään jatkuvuuden hallintaa palautumissuunnitelman muodossa. Ensin käydään läpi palautumissuunnitelman vaiheet, jonka jälkeen käsitellään sen merkitystä liiketoiminnan jatkuvuuden varmistamisessa Välilehti sisältää myös valmiin palautumissuunnitelman pohjan, jota organisaatiot voivat soveltaa omiin ympäristöihinsä.

Omaisuuden hallinnan mallipohjan -välilehdellä on valmiiksi laadittu taulukkomuotoinen mallipohja digitaalisen omaisuuden hallintaan. Organisaatiossa voidaan suoraan hyödyntää tätä sisäistä mallipohjaa omaisuuden hallintaan ja sen seuraamiseen. Mallipohjassa on tarkat kentät omaisuuserien luokittelua varten, mukaan lukien kohde, sijainti, omistaja, versionumero tai käyttöjärjestelmä ja kriittisyys organisaatiolle. Lisäksi mukana on myös käytöstä poistuneiden omaisuuserien seuranta.

Riskirekisterin mallipohjan -välilehdellä on valmiiksi laadittu taulukkopohjainen mallipohja riskirekisterin ylläpitoon. Riskeistä kuvataan tunnistenumero, nimi, kuvaus, omistaja, tehdyt toimenpiteet riskin lieventämiseksi tai poistamiseksi, kategoria todennäköisyys, vaikutus, kriittisyys, riskin taso, riskin tila ja mahdollisuus kommenttimahdollisuus.

Taulukko laskee automaattisesti todennäköisyyden ja vaikutuksen pisteytyksen ja näyttää tuloksen kriittisyyden kohdassa. Riskin taso määräytyy automaattisesti kriittisyyden arvon perusteella. Arvoasteikko on aikaisemmin riskien kartoittamisessa käytetty pisteytysväli, jossa arvot 2–6 katsotaan hyväksyttäviksi, arvot 8–12 luokitellaan siedettäviksi, ja erityisen korkean riskin tapauksessa, joiden arvo on 15–25, pyritään poistamaan riski kokonaan.

Tämän opinnäytetyön tuloksena syntyneellä Excel-pohjaisella prototyypillä olisi täysin valmiiksi työkaluksi kehitettynä edellytykset tarjota käytännöllinen ja kustannustehokas ratkaisu organisaation tarpeisiin kyberuhkien hallinnassa. Jo olemassa olevien välilehtien lisäksi tähän voitaisiin lisätä esimerkiksi tehtävänhallintaa, jossa voidaan seurata meneillään olevia, tulevia ja jo suoritettuja tehtäviä kyberturvallisuuden saralla. Tämä auttaa ylläpitämään kokonaiskuvaa ja pysymään ajan tasalla tehtävien tilasta ja etenemisestä. Näin organisaatio pystyy tehokkaasti reagoimaan ja varautumaan mahdollisiin kyberuhkiin sekä parantamaan kyberturvallisuuttaan systemaattisesti ja suunnitelmallisesti.

5 Tulokset ja pohdinta

Opinnäytetyön tuloksena syntyi perusteellinen tarkastelu kyberturvallisuuden käsitteistä, riskienhallinnan menetelmistä ja lyhyt katsaus kyberturvallisuuden hallintajärjestelmän mahdolliseen sisältöön. Tutkimusprosessi perustui kattavaan kirjallisuuskatsaukseen, alan parhaiden käytäntöjen tutkimiseen, sekä teemahaastatteluun. Lisäksi opinnäytetyön tuloksena luotiin alustava malli kyberturvallisuuden hallintajärjestelmästä, joka toteutettiin Excel-pohjaisena prototyyppinä. Hallintajärjestelmä sisältää lyhyen arvioinnin organisaation nykyisestä kyberturvallisuustilanteesta sekä kattavia ohjeita ja esimerkkejä tietoturvallisuuden kehittämiseen, hallinnointiin ja parantamiseen.

Työkalu on suunniteltu avuksi esimerkiksi ulkoisten konsulttien kanssa yhteistyössä, tarjoten käytännön ohjeita ja suosituksia tietoturvaratkaisujen kehittämiseen ja toteuttamiseen. Hallintajärjestelmä on suunnattu pienten organisaatioiden kyberturvallisuuden parantamiseen. Hallintajärjestelmän tarkoituksena on tuoda kyberturvallisuutta helpommin lähestyttäväksi, ja ymmärrettäväksi sellaisille organisaatioille, joilla ei välttämättä ole resursseja tai pätevyyksiä ymmärtää ja toteuttaa kyberturvaa riittävällä tasolla.

Tutkimuksen toisena tuloksena voidaan pitää järjestelmän vaikutusten arviointia organisaation toimintaan. Tämä arviointi osoitti, että kyberturvallisuuden hallintajärjestelmä parantaa merkittävästi organisaation tietoturvaa ja vähentää riskiä tietomurroille ja tietovuodoille. Lisäksi järjestelmän hallinta auttaa organisaatiota saavuttamaan tietoturvallisuuden standardeja ja säädöksiä. Jatkuvan koulutuksen tarjoaminen henkilöstölle, järjestelmän säännöllinen tarkastaminen ja päivittäminen vastaamaan muuttuvia uhkia ja tarpeita, sekä vahva sitoutuminen johdolta ovat tärkeitä askelia kyberturvallisuuden parantamiseen. Voidaan siis todeta, että kyberturvallisuuden hallintajärjestelmä tarjoaa organisaatiolle tehokkaan ja kokonaisvaltaisen lähestymistavan kyberturvaan, auttaen suojaamaan arvokkaita tietoja, varmistamaan niiden eheyden, sekä takaamaan liiketoiminnan jatkuvuuden.

Tämän tutkimuksen tuloksena syntynyt pienimuotoinen hallintajärjestelmä voi toimia pohjana laajemmalle kaupalliselle tuotteelle. Kyberturvallisuus voi usein olla vaikeasti hahmotettavaa, ja tiedon määrä voi ylittää omat tarpeet, mikä vaikeuttaa olennaisen löytämistä. Tarkoituksena on tiivistää keskeiset tiedot olennaisimmista osa-alueista ja esittää ne ymmärrettävässä muodossa, jotka kaikki voivat helposti omaksua. Hallintajärjestelmä auttaa tunnistamaan omat tarpeet ja syventymään niiden osa-alueiden relevantteihin toimenpiteisiin. Tulevaisuudessa tästä hallintajärjestelmästä on mahdollista kehittää täysimittainen kaupallinen tuote, joka vastaa käyttäjien kokonaisvaltaisiin tarpeisiin.

6 Yhteenveto

Opinnäytetyössä syvennyttiin laajasti kyberturvallisuuden peruskäsitteisiin ja riskien hallintaprosessiin. Tutkimuksen aikana perehdyin syvällisesti erilaisiin uhkiin ja haavoittuvuuksiin sekä niiden kartoittamiseen ja riskien hallinnan etenemiseen. Lisäksi tutkimuksessa tarkasteltiin erilaisten uhkatekijöiden, kuten haktivistien ja APT-ryhmien, määritelmiä. Opinnäytetyössä käsiteltiin myös käytännön esimerkkejä jo toteutuneista kyberhyökkäyksistä, mikä antoi ymmärrystä hyökkäysten eri vaiheista. Tutkimuksen aikana tutustuttiin laajasti myös siihen, mitä kaikkea on otettava huomioon riskienhallintaprosessissa.

Opinnäytetyön tutkimuksen aikana opin myös konkreettisesti mitä kyberturvallisuuden hallintajärjestelmä tarkoittaa, ja mitä se pitää sisällään. Tutkimuksen aikana opin miten hallintajärjestelmää voi kehittää, ja pohdin aktiivisesti, mikä on olennaista tietoa, joka tulisi sisällyttää hallintajärjestelmään. Lisäksi kuultiin kyberturvallisuuden ammattilaisen näkökulma pienten organisaatioiden riskeistä, sekä siitä millaisia hyötyjä hallintajärjestelmä tarjoaa. Lisäksi tutustuin alan eri standardeihin, merkittävimpinä ISO 27001, jolle hallintajärjestelmä perustuu, sekä ISO 27002, joka tarjosi syventävää tietoa hallintajärjestelmän toteutuksen tueksi.

Opinnäytetyössä onnistuttiin vastaamaan kysymyksiin:

- Miten riskejä voidaan kartoittaa?
- Miten riskeiltä suojaudutaan?
- Mitkä ovat parhaat tietoturvakäytännöt?
- Mikä on kyberturvallisuuden hallintajärjestelmä?

Kysymyksiin löytyi tietoa erilaisista verkkojulkaisuista, blogikirjoituksista, dokumenteista, sekä alan standardeista. Näiden lisäksi hallintajärjestelmän hyötyjen tutkinnassa menetelmänä oli teemahaastattelu, ja haastattelun pohjalta toteutettu pohdinta. Seuraavana tavoitteena voisi olla kyberturvallisuuden hallintajärjestelmän kehittäminen kokonaiseksi tuotteeksi, jota käyttäjät voivat hyödyntää.

Lähteet

Acunetix (n.d.). *What is SQL Injection (SQLi) and How to Prevent It*. Acutenix nettisivut. Haettu 26.1.2024 osoitteesta https://www.acunetix.com/websitesecurity/sql-injection/

Ansari K. (2023). *IoT Cyber Security: Trends, Challenges and Solutions*. Knowledge Hut nettisivut. Haettu 28.1.2024 osoitteesta https://www.knowledgehut.com/blog/security/Iot-cyber-security#how-can%C2%A0iot%C2%A0cybersecurity%C2%A0be-improved?%C2%A0

Arctic Wolf (2023). *10 Most Common Types of Malware Attacks*. Arctic Wolf nettisivut. Haettu 201.1.2024 osoitteesta https://arcticwolf.com/resources/blog/8-types-of-malware/

Balbix (n.d.). *IoT Security Challenges and Problems*. Balbix nettisivut. Haettu 28.1.2024 osoitteesta https://www.balbix.com/insights/addressing-iot-security-challenges/

Banach Z. (2019). *5 Ways a Cyberattack Can Hurt Your Organization.* Invicti nettisivut. Haettu 7.2.2024 osoitteesta https://www.invicti.com/blog/web-security/5-ways-a-cyberattack-can-hurt/

Buxton O. (2023). *Cyber Warfare: Types, Examples, and How to Stay Safe*. Avast nettisivut. Haettu 29.1.2024 osoitteesta https://www.avast.com/c-cyber-warfare

Chachak E. (n.d.). *7 Ways To Reduce Technology Risks*. Cyberdb nettisivut. Haettu 9.2.2024 osoitteesta https://www.cyberdb.co/7-ways-to-reduce-technology-risks/

Cisco (n.d.). *What is Social Engineering?* Cisco nettisivut. Haettu 28.1.2024 osoitteesta https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html

Cloudflare (n.d.). *What was the WannaCry ransomware attack?* Cloudflare nettisivut. Haettu 28.1.2024 osoitteesta https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

Cobb M. (2024). *How to perform a cybersecurity risk assessment in 5 steps*. Techtarget. Haettu 6.2.2024 tietoa ja mallinnus taulukolle 2. osoitteesta https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step

Cyber Cops (2023). *What Is Cybersecurity Management, and Why Is it Important?* LinkedIn. Haettu 13.2.2024 osoitteesta https://www.linkedin.com/pulse/what-cybersecurity-management-why-important-cyber-cops/

Cybersecurity Exchange (2022). *The Cyber Kill Chain: The Seven Steps of a Cyberattack*. Eccouncil.org. Haettu 28.1.2024 osoitteesta https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

DNV (n.d.). *Recognizing the seven stages of a cyber-attack*. DNV nettisivut. Haettu 28.1.2024 osoitteesta https://www.dnv.com/cybersecurity/cyber-insights/recognizing-the-seven-stages-of-a-cyber-attack.html

Ellis D. (n.d.). *6 Phases in the Incident Response Plan*. Security Metrics nettisivut. Haettu 11.2.2024 osoitteesta https://www.securitymetrics.com/blog/6-phases-incident-response-plan

Euroopan Unioni tietosuojaryhmä (2007). *Lausunto 4/2007 henkilötietojen käsitteestä*. Dokumentaatio haettu 11.2.2024 osoitteesta https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_fi.pdf

F-Secure (n.d. a) *Mitä on kyberturvallisuus?* F-Secure nettisivut. Haettu 15.1.2024 osoitteesta https://www.f-secure.com/fi/articles/what-is-cyber-security

F-Secure (n.d. b). *What is phishing*. F-Secure nettisivut. Haettu 24.1.2024 osoitteesta https://www.f-secure.com/gb-en/articles/what-is-phishing

Fancher D., Gelinne J., Mossburg E. (2016). *Seven hidden costs of a cyberattack*. Deloitte nettisivut. Haettu 28.1.2024 osoitteesta https://www2.deloitte.com/us/en/pages/finance/articles/cfo-insights-seven-hidden-costs-cyberattack.html

Fortinet (n.d. a). *CIA Triad*. Fortinet nettisivut. Haettu 22.1.2024 osoitteesta https://www.fortinet.com/resources/cyberglossary/cia-triad

Fortinet (n.d. b). *Man-in-the-Middle Attack: Types and Examples*. Fortinet nettisivut. Haettu 26.1.2024 osoitteesta https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack

Gillis A., Terrell Hanna K., Ferguson K. (2023). *cyberwarfare.* TechTarget. Haettu 29.1.2024 osoitteesta https://www.techtarget.com/searchsecurity/definition/cyberwarfare

Goutam R.K. (2021). *Cybersecurity Fundamentals: Understand the Role of Cybersecurity, Its Importance and Modern Techniques Used by Cybersecurity Professionals.* Google kirjat. Haettu 15.1.2024 osoitteesta https://books.google.fi/books?hl=fi&lr=&id=scUwEAAAQBAJ&oi=fnd&pg=PT21&dq=Cybersecurity+importance&ots=wYXzh3ID1q&sig=2wHgmebl6TD3d_vnvklygW8yTzI&redir_esc=y#v=onepage&q=Cybersecurity%20importance&f=false

Ha T. T. (2015). *Anonymous claims attack on RCMP website*. The Globe and Mail nettisivut. Haettu 18.1.2024 osoitteesta https://www.theglobeandmail.com/news/national/anonymous-claims-attack-on-rcmp-website/article25584147/

Hämäläinen V.P. (2021). *Uudet tiedot: Vastaamon potilaiden tiedot olivat ehkä jopa vuosia suojaamatta netissä – tietoturva-asiantuntija: "Älyvapaata".* Yle. Haettu 7.2.2024 osoitteesta https://yle.fi/a/3-11750220

Hämäläinen V.P., Rummukainen A. (2020). *Yksi heistä on kiristäjä.* Yle. Haettu 7.2.2024 osoitteesta https://yle.fi/a/3-11616210

Hashemi-Pour C., Chai W. (2023). *CIA triad (confidentiality, integrity and availability).* TechTarget. Haettu 22.1.2024 osoitteesta https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Hevonoja, J. (2020). *Tietoturvaskandaalissa rypevän Vastaamon toimitusjohtajalle potkut – yhtiön hallituksen mukaan pimitti tietomurtoa 1,5 vuotta*. Yle. Haettu 7.2.2024 osoitteesta https://yle.fi/a/3-11614453

Hill C. (2023). *What are Digital Assets?* Media Valet nettisivut. Haettu 3.2.2024 osoitteesta https://www.mediavalet.com/blog/what-are-digital-assets

Huang K., Wang X., Wei W., Madnick S. (2023). *The Devastating Business Impacts of a Cyber Breach*. Harvard Business Review nettisivut. Haettu 15.1.2024 osoitteesta https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

Hyperproof Team (2023*). How to Build and Maintain a Risk Register (Plus Examples & a Risk Register Template).* Hyperproof team nettisivut. Haettu 9.2.2024 tietoa, sekä mallinnus kuvaan 5. osoitteesta https://hyperproof.io/resource/risk-register-key-benefits/

IBM (n.d.). *What is a cyberattack?* IBM nettisivut. Haettu 18.1.2024 osoitteesta https://www.ibm.com/topics/cyber-attack

Imperva (n.d.). *Distributed Denial of Service (DDoS)*. Imperva nettisivut. Haettu 26.1.2024 osoitteesta https://www.imperva.com/learn/ddos/denial-of-service/

Irei A. (2024). *What is incident response? A complete guide.* TechTarget. Haettu 11.2.2024 osoitteesta https://www.techtarget.com/searchsecurity/definition/incident-response

Johnson C., Badger L., Waltermire D., Snyder J., Skorupka C. (2016). *NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing*. Dokumentaatio haettu 16.1.2024 osoitteesta https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Kantomaa R. (2021*). Oikeuden paperit paljastavat: Näin Vastaamon tietomurto tapahtui – salainen kauppasumma paljastui*. MTV-uutiset. Haettu 7.2.2024 osoitteesta https://www.mtvuutiset.fi/artikkeli/oikeuden-paperit-paljastavat-nain-vastaamon-tietomurto-tapahtui-salainen-kauppasumma-paljastui/8055050

Kaspersky (n.d. a)*. What is a Zero-day Attack? - Definition and Explanation.* Kaspersky nettisivut. Haettu 26.1.2024 osoitteesta https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

Kaspersky (n.d. b). *Stuxnet explained: What it is, who created it and how it works*. Kaspersky nettisivut. Haettu 29.1.2024 osoitteesta https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet

Knowles M. (2024). *Cybersecurity Risk Management: Frameworks, Plans, & Best Practices.* Hyperproof nettisivut. Haettu 3.2.2024 tietoa ja kuva 4. osoitteesta https://hyperproof.io/resource/cybersecurity-risk-management-process/

Lockheed M. (n.d.). *The Cyber Kill Chain*. Haettu 22.1.2024 kuva 2. osoitteesta https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Loshin P., Sirkin J. (n.d.). *Structured Query Language (SQL).* TechTarget. Haettu 26.1.2024 osoitteesta https://www.techtarget.com/searchdatamanagement/definition/SQL

Maaseudun tulevaisuus (2021*). Psykoterapiakeskus Vastaamo ajetaan alas – terapeuttien vastaanotot jatkuvat selvitystilan ajan.* Maaseudun tulevaisuus nettisivut. Haettu 7.2.2024 osoitteesta https://www.maaseuduntulevaisuus.fi/uutiset/50252c85-f0ac-5276-9c31-dab2e8f6d2ee

Maddyness (2023). *7 Stages of the cyber attack lifecycle.* Maddyness nettisivut. Haettu 28.1.2024 osoitteesta https://www.maddyness.com/uk/2023/05/13/7-stages-of-the-cyber-attack-lifecycle/

Malwarebytes (n.d. a). *WannaCry*. Malwarebytes nettisivut. Haettu 28.1.2024 osoitteesta https://www.malwarebytes.com/wannacry

Malwarebytes (n.d. b). *Computer Worm*. Malwarebytes nettisivut. Haettu 22.1.2024 osoitteesta https://www.malwarebytes.com/computer-worm

Malwarebytes (n.d. c). *Ransomware* Malwarebytes nettisivut. Haettu 22.1.2024 osoitteesta https://www.malwarebytes.com/ransomware

Mäntysalo J. (2021). *Vastaamossa käytettiin yksinkertaisia salasanoja, kunnes tapahtui tuhoisa tietomurto – tuomio tietosuojarikoshaarasta annetaan tänään.* Yle. Haettu 7.2.2024 osoitteesta https://yle.fi/a/74-20027486

Mäntysalo J., Salumäki T. (2023*). Ehdolliseen vankeuteen tuomittu Ville Tapio pyytää anteeksi Vastaamon tietomurron uhreilta: ”Olen todella pahoillani*” Yle. Haettu 7.2.2024 osoitteesta https://yle.fi/a/74-20027598

Morgan J.P. (2022). *12 tips for mitigating cyberattacks*. J.P. Morgan nettisivut. Haettu 9.2.2024 osoitteesta https://www.jpmorgan.com/insights/cybersecurity/ransomware/12-tips-for-mitigating-cyber-risk

NCC Group (n.d.). *The Lazarus group: North Korean scourge for +10 years*. NCC Group nettisivut. Haettu 28.1.2024 osoitteesta https://www.nccgroup.com/us/the-lazarus-group-north-korean-scourge-for-plus10-years/

NIST (n.d.) *NIST Cybersecurity Framework*. NIST nettisivut. Haettu 14.2.2024 osoitteesta https://www.nist.gov/cyberframework

NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).* Dokumentaatio haettu 14.2.2024 osoitteesta https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

NIST (2022). *About NIST*. NIST nettisivut. Haettu 14.2.2024 osoitteesta https://www.nist.gov/about-nist

Opitietosuojaa.fi (n.d.). *EU:n tietosuoja-asetus*. Opitietosuojaa.fi nettisivut. Haettu 11.2.2024 osoitteesta https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus

Posey B., Shea S. (2023) *zero-day (computer)*. TechTarget. Haettu 26.1.2024 osoitteesta https://www.techtarget.com/searchsecurity/definition/zero-day-vulnerability

PSR (2022). *Identify your vulnerabilities and threats.* PSR nettisivut. Haettu 4.2.2024 osoitteesta https://protectivesecurity.govt.nz/information-security/lifecycle-2/assess-the-risks/identify-your-vulnerabilities-and-threats/

Puzder D. (2023). *Vulnerabilities, Threats, and Risks Explained*. Washington University St. Louis nettisivut. Haettu 4.2.2024 osoitteesta https://informationsecurity.wustl.edu/vulnerabilities-threats-and-risks-explained/

Radware (n.d.). *What is A DDoS Attack?* Radware nettisivut. Haettu 26.1.2024 osoitteesta https://www.radware.com/cyberpedia/ddospedia/ddos-meaning-what-is-ddos-attack/

RiskOptics (2023). *Threat, Vulnerability, and Risk: What's the Difference?* RiskOptics nettisivut. Haettu 4.2.2024 osoitteesta https://reciprocity.com/blog/threat-vulnerability-and-risk-whats-the-difference/

Rudderstack (n.d.). *How To Handle Your Company's Sensitive Data.* Rudderstack nettisivut. Haettu 11.2.2024 osoitteesta https://www.rudderstack.com/learn/data-security/how-to-handle-your-company-s-sensitive-data/

Security Scorecard (2021a). *What is a Cybersecurity Vulnerability? Definition and Types.* Security Scorecard nettisivut. Haettu 16.1.2024 osoitteesta https://securityscorecard.com/blog/what-is-a-cybersecurity-vulnerability/

Security Scorecard (2021b). *How to Identify and Prepare for Network Security Threats and Vulnerabilities.* Security Scorecard nettisivut. Haettu 4.2.2024 osoitteesta https://securityscorecard.com/blog/identify-network-security-threats-and-vulnerabilities/e

SecurityScorecard (2021c). *8 Top Strategies for Cybersecurity Risk Mitigation*. Security Scorecard nettisivut. Haettu 9.2.2024 osoitteesta https://securityscorecard.com/blog/6-strategies-for-cybersecurity-risk-mitigation/

Shea S., Harford I. (2023). *12 common types of malware attacks and how to prevent them.* TechTarget. Haettu 20.1.2024 osoitteesta https://www.techtarget.com/searchsecurity/tip/10-common-types-of-malware-attacks-and-how-to-prevent-them

Sheldon R., Terrell Hanna K. (2024). *cyberterrorism.* TechTarget. Haettu 29.1.2024 osoitteesta https://www.techtarget.com/searchsecurity/definition/cyberterrorism

Singh R. (2021). *CIA Triad- The Mother of Data Security*. Insentra nettisivut. Haettu 22.1.2024 kuva 1. osoitteesta https://www.insentragroup.com/au/insights/geek-speak/secure-workplace/cia-triad-the-mother-of-data-security/

Stine K., Quinn S., Witte G., Gardner R.K. (2020). *Integrating Cybersecurity and Enterprise Risk Management (ERM).* Haettu 4.2.2024 tietoa ja mallinnus taulukkoon 1. osoitteesta https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf

Suomen Standardisoimisliitto SFS ry. (2022). *SFS-EN ISO/IEC 27002:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. Suomen Standardisoimisliitto SFS ry*. Dokumentaatio haettu 14.2.2024 SFS Online nettisivuilta.

Suomen Standardisoimisliitto SFS ry. (2023*). SFS-EN ISO/IEC 27001:2023. (2023). Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardisoimisliitto SFS ry*. Haettu 14.2.2024 SFS Online nettisivuilta.

Svahn N., Karppi T. (2021). *Tietomurron kohteeksi joutunut psykoterapiakeskus Vastaamo on haettu konkurssiin – selvitysmies jatkajasta: "Kiinnostuneita tahoja oli monta".* Yle. Haettu 7.2.2024 osoitteesta https://yle.fi/a/3-11784072

Taleva K. (2021). *Vastaamon hallitus erosi tehtävästään.* Iltalehti. Haettu 7.2.2024 osoitteesta https://www.iltalehti.fi/kotimaa/a/c8665d75-53ca-47c2-9822-622f22a84c05

Team Nuggets (2023). *The 6 Stages of the Cyber Attack Lifecycle*. CBT Nuggets nettisivut. Haettu 16.1.2024 osoitteesta https://www.cbtnuggets.com/blog/certifications/security/the-6-stages-of-the-cyber-attack-lifecycle

Thinkcurity (n.d.). *How to Perform a SWOT Analysis on Your Security Firm.* Thinkcurity nettisivut. Haettu 6.2.2024 tietoa ja kuva 3. osoitteesta https://www.thinkcurity.com/articles/how-to-perform-a-swot-analysis-on-your-security-firm

Thomas M. (2022). *What Is Social Engineering? A Look Into the Sophisticated World of Psychological Cyber Crime*. Builtin nettisivut. Haettu 28.1.2024 osoitteesta https://builtin.com/cybersecurity/what-is-social-engineering

Tietosuojakeskus (n.d.). *Case Vastaamo*. Tietosuojakeskuksen nettisivut. Haettu 7.2.2024 osoitteesta https://tietosuojakeskus.fi/case-vastaamo/

Traficom kyberturvallisuuskeskus (2019). *Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri).* Traficomin kyberturvallisuuskeskuksen nettisivut. Dokumentaatio haettu osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Tunggal A. B. (2023a). *What is Cybersecurity Risk? A Thorough Definition*. Upguard nettisivut. Haettu 3.2.2024 osoitteesta https://www.upguard.com/blog/cybersecurity-risk

Tunggal A. B. (2023b). *What is Cybersecurity Risk Management? Preventing Cyber Attacks.* Upguard nettisivut. Haettu 3.2.2024 osoitteesta https://www.upguard.com/blog/cybersecurity-risk-management

Tunggal A. B. (2023c). *What is an Incident Response Plan?* Upguard nettisivut. Haettu 11.2.2024 osoitteesta https://www.upguard.com/blog/incident-response-plan

Tunggal A.B. (2024). *Cybersecurity Risk Assessment.* Upguard nettisivut. Haettu 6.2.2024 osoitteesta https://www.upguard.com/blog/how-to-perform-a-cybersecurity-risk-assessment

Windsor Group Sourcing Advisory (2023). *The Benefits of an IT SWOT Analysis*. LinkedIn. Haettu 6.2.2024 osoitteesta https://www.linkedin.com/pulse/benefits-swot-analysis-windsor-group-computer-services/

Yasar K., Cobb M. (2022). *man-in-the-middle attack (MitM.* TechTarget. Haettu 26.1.2024 osoitteesta https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM

Yle (2020). *Yle seurasi Vastaamon tietomurtoa: Näin kiristäjä ilmestyi Tor-verkon foorumille, poliisi pyytää harkintaa asiaan liittyvien yksityiskohtien julkaisemisessa*. Yle nettisivut. Haettu 7.2.2024 osoitteesta https://yle.fi/a/3-11612399

Zhu M. (2023) User input sanitization and validation: securing your app. Tiny nettisivut. Haettu 26.1.2024 osoitteesta https://www.tiny.cloud/blog/input-sanitization/#h_186580937330816903612324 32

Zulhuni M. (2023). *Who is really behind the Anonymous hacker group?* Techwire Asia nettisivut. Haettu 18.1.2024 osoitteesta https://techwireasia.com/07/2023/anonymous-hacker-group-who-are-they-and-where-are-they-now/

Liite 1: Aineistonhallintasuunnitelma

Tutkimuksellinen työ:

Opinnäytetyöllä ei ole toimeksiantajaa, joten opinnäytetyön omistaja on sen kirjoittaja.

Aineisto säilytetään oman koneen C-asemalla, sekä varmuuskopio omalla henkilökohtaisella pilviasemalla, sekä koulun tarjoamalla yksityiseen käyttöön tarkoitetulla pilviasemalla. Kellään muulla ei ole pääsyä kerättyyn aineistoon, kuin kirjoittajalla. Tutkimustyössä käytetyt lähteet löytyvät lähdeluettelosta. Aineistoa säilytetään opinnäytetyön kirjoittamisen jälkeen vaadittu vähintään yksi vuosi. Lähteet ovat Zoterossa tallessa, sekä varmuuskopiona Zotero-tilillä.

Kuvia saa käyttää tutkimustyössä, tekijänoikeudella suojattujen teosten käyttötapoja pidetään kohtuullisena käyttönä, tai ne voivat kuulua tekijänoikeuslaissa tarkoitettuihin rajoituksiin tai poikkeuksiin, kuten kohtuullinen levitys. Kohtuulliseksi käytöksi luetellaan voittoa tavoittelematon opetuksellinen käyttö.

Haastattelu pidetään sekä nauhoitetaan Teamsin avulla. Haastattelu litteroidaan Word tiedostoon, joka säilytetään koneen C-asemalla. Materiaalista tehdään varmuuskopio samaan paikkaan kuin opinnäytetyöstä, henkilötietoja ei kuitenkaan tallenneta pilviasemalle. Haastattelujen tulokset prosessoidaan opinnäytetyön kappaleessa 4. Haastattelu anonymisoidaan. Haastattelutiedostoja säilytetään vaadittu 1 vuosi.

Muilla kuin opinnäytetyön tekijällä ei ole pääsyä aineistoon.

Opinnäytetyöaineiston jatkokäyttö työn valmistumisen jälkeen

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

Liite 2: Haastattelukysymykset

Haastattelu toteutettiin 5.3.2024. Haastateltavana oli kyberturvallisuuden ammattilainen, jolla on osaamista ISO 27001 standardin parissa.

Mitkä ovat yleisimmät kyberturvallisuuden haasteet pienissä organisaatioissa?

Mitkä ovat yleisimmät tietoturvahyökkäystyypit, joita pienet yritykset kohtaavat, ja miten kyberturvallisuuden hallintajärjestelmä voi auttaa niitä torjumaan näitä hyökkäyksiä?

Mitä etuja kyberturvallisuuden hallintajärjestelmän käyttö voi tarjota pienille organisaatioille?

Mitä riskejä voidaan kohdata, jos ei käytetä kyberturvallisuuden hallintajärjestelmää?

Millaisia käytännön toimenpiteitä hallintajärjestelmän käyttöönottaminen vaatii?

Mitä toimenpiteitä pienet yritykset voivat toteuttaa varmistaakseen työntekijöidensä tietoturvakäytäntöjen noudattamisen?

Mitä tekijöitä tulisi ottaa huomioon valitessaan kyberturvallisuuden strategiaa?