KYBERTURVALLISUUS

Case: Felix Solutions Oy

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ylemmän ammattikorkeakoulututkinnon opinnäytetyö

Teknologiaosaamisen johtaminen, Hämeen ammattikorkeakoulu

2021

Sami Vartio

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Koulutus Teknologiaosaamisen johtaminen, YAMK — Tiivistelmä

Kampus Hämeen ammattikorkeakoulu

Tekijä Sami Vartio — Vuosi 2021

Työn nimi Kyberturvallisuus, Case: Felix Solutions Oy

Ohjaajat Pasi Laine

TIIVISTELMÄ

Opinnäytetyön tavoitteena on tutkia ja kartoittaa kyberturvallisuuteen liittyviä keskeisiä käsitteitä ja säädöksiä. Opinnäytetyössä on otettu huomioon tietoturvan ja kyberturvallisuuden erot, termit, säädökset ja standardit sekä yleiset käytännöt. Opinnäytetyön tarkoitus on selvittää, tarjoaako kyberturvallisuus uusia liiketoimintamahdollisuuksia pienelle tai keskisuurelle It-yritykselle. Opinnäytetyössä on myös sivuttu johtamisen ominaisuudet ja vaatimukset, jotka tulisi ottaa huomioon kyberturvallisuudessa. Aineistona tässä työssä on käytetty alan kirjallisuutta, julkaisuja sekä nettilähteitä.

Avainsanat kyberturvallisuus, tietoturva, kyberuhat, riskienhallinta, johtaminen

Sivut 42 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Name of Degree Programme MEng

Campus Häme University of Applied Sciences

Abstract

Author Sami Vartio

Year 2021

Subject Cyber security, Case: Felix Solutions Oy

Supervisors Names

ABSTRACT

The purpose of this thesis is to study and clarify the key concepts and regulations related to cyber security. The thesis takes into account the differences between information security and cyber security, terms, regulations and standards, as well as general practices. The objective of the thesis is to find out whether cyber security offers business opportunities for a small or medium-sized IT company. The thesis also reference the characteristics and requirements of management, which taken into account in cyber security. Literature, publications and online sources in the field have been use as source material in this study.

Keywords cyber security, information security, cyber threats, risk management

Pages 42 pages

Sisällys

Kuvat, taulukot ja kaavat

KYBERSANASTO

Kybertoimintaympäristö on digitaalisen informaation käsittelyyn tarkoitettu, toisiinsa yhteydessä olevista tietokoneista ja muista laitteista sekä tietoverkoista muodostunut ympäristö.

Kyberturvallisuus on kybermaailman turvallisuutta. Se tarkoittaa sitä, että erilaiset kybermaailmaan kohdistuvat uhat ovat hallinnassa, ja kybermaailma toimii oikein ja virheettömästi. Tällöin esimerkiksi kybermaailman toimivuudesta riippuvainen kriittinen infrastruktuurikin toimii oikein ja on luotettavaa.

Kyberuhka tarkoittaa mahdollisuutta sellaiseen kybermaailmaan vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa kybermaailman oikean ja virheettömän toiminnan.

Kyberpuolustus on kyberturvallisuuden maanpuolustuksellinen osa-alue. Siihen kuuluvat kybermaailmassa tapahtuva ja sitä koskeva tiedustelu, maanpuolustuksen kannalta merkityksellisten kyberympäristöjen suojaaminen ja tiettyihin kyberympäristöihin vaikuttaminen. Kyberpuolustuksesta vastaa Suomessa Puolustusvoimat.

Informaatiovaikuttaminen on vaikuttamista saatavilla olevan informaation sisältöön ja kulkuun sekä sitä kautta eri vaiheissa olevan tapahtumasarjan lopputulokseen. Tavoitteena voi olla esimerkiksi kansalaisten mielipiteiden muokkaaminen.

IoT (Internet of Things) eli esineiden internet tarkoittaa internetin laajentumista laitteisiin ja koneisiin, joita voidaan ohjata ja mitata verkon kautta. Esineiden internet on yhä useamman arkea: esimerkiksi pesukone voi olla yhteydessä internetiin.

Kriittinen infrastruktuuri tarkoittaa kaikkia niitä palveluita, järjestelmiä ja rakenteita, jotka ovat yhteiskuntamme toiminnalle elintärkeitä. Esimerkki tästä on sähköverkko.

Palvelunestohyökkäys tarkoittaa verkkohyökkäystä, jossa pyritään estämään tietyn verkkopalvelun tarkoitettu käyttö. Tavallisimmin hyökkäys toteutetaan kohdistamalla palveluun niin paljon verkkoliikennettä, että palvelu ei enää suoriudu tehtävistään.

Phishing eli tietojenkalastelu on toimintaa, jolla pyritään saamaan haltuun luottamuksellisia tietoja (esimerkiksi henkilö- tai tilitietoja) esiintyen tiedon saantiin oikeutettuna tahona. Näiden tietojen avulla voidaan sitten pyrkiä saavuttamaan esimerkiksi taloudellista hyötyä.

Päivitys (ohjelmistopäivitys). Ohjelmistot ovat monimutkaisia, ja niissä onkin käytännössä aina virheitä. Lisäksi ohjelmistoihin saatetaan tarvita uusia ominaisuuksia. Virheitä korjataan

ja ominaisuuksia lisätään päivittämällä ohjelmistoja. Päivitys tarkoittaa ohjelmiston muuttamista siten, että aiempi versio korvataan uudella ohjelmistoversiolla.

Tietojärjestelmä on ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoituksena on informaatiota käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi.

Tietoturva viittaa kaikkiin niihin järjestelyihin, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturvaan kuuluvat muun muassa tiedon, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Yksilötasolla tietoturva tarkoittaa tärkeiden tietojen ja laitteiden suojaamista.

Trolli on viesti tai henkilö, jonka ensisijainen tavoite on ärsyttää ihmisiä, aiheuttaa ristiriitoja tai aiheuttaa turhien viestien kirjoittamista. Yleensä trollaaja esittää jostakin aiheesta äärimmäisen mielipiteen vastustajien kantaa halventaen ja muiden argumentteja huomioon ottamatta.

Varmuuskopiointi tarkoittaa jonkin tärkeän tiedon kopiointia ja varastointia jonnekin muualle kuin sen alkuperäinen sijainti. Jos alkuperäinen tieto häviää tai tuhoutuu, voidaan tieto palauttaa varmuuskopioista.

(Lönnqvist & Moilanen 2017, ss. 7–10)

Kyberturvallisuuskeskus on Liikenne- ja viestintäviraston alainen viranomainen, jonka toiminta alkoi 1. tammikuuta 2014. Sen vastuulle siirtyivät kaikki CERT-toiminnot. Vuoden 2018 loppuun saakka Kyberturvallisuuskeskus toimi Viestintäviraston alaisuudessa.

(Wikipedia, 2019)

1 JOHDANTO

Yrityksen kannattaa panostaa kyberturvallisuuteen normaalia enemmän, sillä tietoturvariskit ovat olemassa niin pienissä, keskisuurissa kuin suurissakin yrityksissä. Tietoturvan tärkeys saattaa unohtua varsinkin pienemmissä yrityksissä, vaikkakin ohjeistukset tietoturvariskien välttämiseen koskevat kaiken kokoisia yrityksiä. Tietomurrot tai -vuodot aiheuttavat toteutuessaan suurta haittaa. Opinnäytetyössä perehdytään kyberturvallisuuteen ja selvitetään mitä tarkoitetaan kyberturvalla. Kyberturvallisuudella tarkoitetaan niitä toimenpiteitä, joilla organisaatio suojaa liiketoiminnassaan tarvittavat järjestelmät, ohjelmistot, laitteet ja tietoliikenneyhteydet kyberuhkilta. Kun tieto- ja kyberturvallisuus toteutetaan oikein, se ei vaikeuta tai estä käyttäjän toimintaa, vaan tehostaa liiketoimintaa.

Opinnäytetyössä pyritään selvittämään pienen It-yrityksen haasteita liittyen kyberturvallisuuteen, etsitään mahdollisia uhkia sekä kehitetään ja testataan kyberturvallisuuden käyttöön liittyviä toimintoja. Pystyykö kyberturvallisuus tarjoamaan uusia liiketoimintamahdollisuuksia pienelle tai keskisuurelle It-yritykselle ja kuinka kyberturvallisuus toteutuu? Case-yritys on vuonna 2017 perustettu Felix Solutions Oy. Yritys on It-yritys, joka toimii Uudellamaalla. Yrityksen tietopalveluihin kuuluu mm. tietotekniikka, verkkopalvelut ja konsultointipalvelut.

Opinnäytetyö on aloitettu jo vuonna 2017, jolloin aiheesta oli erittäin niukasti tietoa saatavilla verrattuna nykyhetkeen. Runkona ja punaisena lankana työssä on käytetty Kyberturvallisuuskeskuksen ohjeistusta, joka ilmestyi tammikuussa 2020. Verkkojulkaisujen lisäksi tiedon ja inspiraation lähteenä aineistosta löytyy myös erilaisia tietoturvakäsikirjoja sekä alan tietolehtiä. Tutkimuksessa on käyty läpi Kyberturvallisuuskeskuksen oppaita, harjoituksia ja niiden perusteella tehty erilaisia testejä.

Tämä opinnäytetyö soveltaa tapaustutkimuksen (case study) laadullisia menetelmiä, joten kyseessä on laadullinen tapaustutkimus. Metsämuurosen (2008, s. 16) mukaan tapaustutkimus määritellään empiiriseksi tutkimukseksi, joka tutkii monipuolisilla ja monilla tavoin hankituilla tiedoilla nykyistä tapahtumaa tietyssä ympäristössä. Tapaustutkimus on määritelty myös yksinkertaisesti toiminnassa olevan tapahtuman tutkimukseksi. Tapaustutkimus koostuu kirjallisuusosuudesta sekä empiirisestä havainto-osuudesta.

1.1 Tutkimuksen tarkoitus

Opinnäytetyön tarkoituksena on selvittää case-yrityksen kyberturvallisuuteen liittyviä haasteita ja etsiä vastauksia mahdollisiin uhkiin. Tämä laadullinen tapaustutkimus pyrkii selvittämään case-yrityksen Felix Solutions Oy:n kyberturvallisuuden käyttöön liittyvien toimintojen kehittämistä ja testaamista sekä tuodaan tutkimuksen myötä esille nousevia kehitystarpeita.

1.2 Tutkimuskysymys

Opinnäytetyön varsinainen tutkimuskysymys on: Tarjoaako kyberturvallisuus uusia liiketoimintamahdollisuuksia pienelle tai keskisuurelle It-yritykselle ja kuinka kyberturvallisuus toteutuu? Kybermaailmassa ohjeet ja suositukset parantaa yrityksen toimintojen luotettavuutta ja ne liittyvät yleensä toiminnan kehittämiseen.

1.3 Tutkimuksen rakenne

Opinnäytetyö alkaa johdannolla ja keskeisten käsitteiden määrittelyllä. Johdannon ja teoreettisen viitekehyksen jälkeen tehdään katsaus kyber-termin historiaan ja edetään kyberturvallisuuden kautta kyberuhkiin. Tieto- ja kyberturvaa ohjaavat tietyt vaatimukset ja näitä vaatimuksia ohjaa lainsäädäntö ja viranomaiset. Mietitään, mitä pitää sisällään kyberturvallisuuden johtaminen, kuinka hallitaan riskejä ja mitä vaatimuksia kyberturvallisuus tuo tullessaan yritykselle. Tämän jälkeen edetään kyberturvallisuuden tarkastelusta ja kuvauksesta tutkimuksen empiiriseen osuuteen, jossa muodostetaan kokonaisnäkemys case-yrityksen käytössä olevista menetelmistä ja työkaluista kyberosaamiseen ja tietoturvaan liittyen. Lopuksi case-yritykseen tehdään kyberturvatestaus ja havainnoidaan sekä raportoidaan mahdolliset turva-aukot sekä pohditaan tulevaisuuden kehitystarpeita.

2 TUTKIMUSMETODIT

2.1 Tutkimusstrategiat

Koppa (2015, -a) joka on Jyväskylän yliopiston avoimen yliopiston sivusto, kertoo että tutkimusstrategialla tarkoitetaan niitä periaatteellisia valintoja, jolla tutkimus on tarkoitus toteuttaa. Tutkimusstrategia on tutkimuksen menetelmällisten ratkaisujen kokonaisuus, joka ohjaa tutkimuksen menetelmien valintaa ja käyttöä sekä teoreettisella että käytännöllisellä tasolla. Tutkimusstrategian käsite on laaja ja sitä määritellään menetelmäkirjallisuudessa eri tavoin.

2.1.1 Laadullinen tutkimus vs. määrällinen tutkimus

Metsämuuronen (2003, s. 162) kertoo, että laadullisella eli kvalitatiivisella tutkimuksella tarkoitetaan kokonaista joukkoa erilaisia tulkinnallisia tutkimuskäytäntöjä. Kvalitatiivista tutkimusta on vaikea määritellä selvästi, koska sillä ei ole teoriaa, joka olisi vain sen omaa. Kvalitatiivisella tutkimuksella ei myöskään ole täysin omia metodeja. Metsämuuronen (2003, s. 167) jatkaa, että keskeiset kvalitatiivisessa metodologiassa käytettävät tutkimusmetodit ovat havainnoiminen, tekstianalyysi, haastattelu ja litterointi.

Koppa (2015, -b) kertoo, että määrällinen eli kvantitatiivinen tutkimus on tieteellisen tutkimuksen menetelmäsuuntaus, joka perustuu kohteen kuvaamiseen ja tulkitsemiseen tilastojen ja numeroiden avulla. Määrällisessä tutkimuksessa ollaan kiinnostuneita erilaisista luokitteluista, syy- ja seuraussuhteista, vertailusta ja numeerisiin tuloksiin perustuvasta ilmiön selittämisestä. Määrälliseen menetelmäsuuntaukseen sisältyy runsaasti erilaisia laskennallisia ja tilastollisia analyysimenetelmiä. Laadullisen ja määrällisen menetelmäsuuntauksen välistä eroa usein korostetaan, vaikka molempia suuntauksia voidaan käyttää myös samassa tutkimuksessa ja molemmilla suuntauksilla voidaan selittää, tosin eri tavoin, myös samoja tutkimuskohteita.

2.1.2 Tapaustutkimus

Koppa (2015, -c) kertoo, että tapaustutkimukseksi kutsutaan tutkimusstrategiaa, jonka tarkoituksena on tutkia syvällisesti vain yhtä tai muutamaa kohdetta tai kokonaisuutta. Tutkimusstrategiana tapaustutkimus määrittyy väljästi ja sitä voidaan toteuttaa eri analyysimenetelmien avulla. Tutkimuksessa voidaan yleisesti puhua tapauksista (case), joilla viitataan yksittäisiin tutkimuskohteisiin, jotka yhdessä muodostavat tutkimuksen keskiössä olevien tutkimuskohteiden suppeaan joukkoon.

Metsämuuronen (2008, s. 17) kertoo, että tapaustutkimus tarjoaa luonnollisen pohjan yleistämiselle ja se sallii yleistykset. Lisäksi tapaustutkimukset ovat usein askel toimintaan, koska niiden lähtökohta on usein toiminnallinen ja tuloksia sovelletaan myös käytännössä. Tapaustutkimus palvelee monenlaista lukijakuntaa, sillä sen raportointi on mahdollista tehdä kansantajuiseksi ja siinä on mahdollista välttää tavanomaiselle tutkimukselle tyypillistä tiedeslangia. Tapaustutkimukseen liittyvä epistemologinen kysymys kuuluukin, mitä voidaan oppia yhdestä tapauksesta?

2.1.3 Reliabiliteetti ja validiteetti

Metsämuurosen (2002, s. 11) mukaan tutkimusmenetelmän luotettavuutta on perinteisesti kuvattu kahdella termillä: reliabiliteetilla ja validiteetilla. Molemmat termit tarkoittavat luotettavuutta, mutta reliabiliteetilla viitataan tutkimuksen toistettavuuteen. Jos mitataan tai testataan samaa ilmiötä monta kertaa samalla mittarilla, kuinka samanlaisia tai toisistaan poikkeavia tuloksia saadaan? Jos mittari on reliaabeli, ovat vastaukset eri mittaus/testauskerroilla melko samanlaiset. Validiteetti puolestaan kertoo, mitataanko sitä mitä on tarkoitus mitata. Mitataanko asiakasyrityksen kyberturvallisuutta vai siihen välillisesti olevaa tekijää?

3 KYBER

Jo muinaiset kreikkalaiset keksivät kyberin. Kreikan sana cybernetice (tai kubernetes) tarkoitti alun perin ohjausta ja hallintaa. Kohteena saattoi olla kansa, jolloin sana viittasi hallintokoneistoon, tai vene, jolloin sana merkitsi laivan ruorimiestä. Kyber merkitsee siis ohjausta, kontrollia ja hallintaa. Toisen maailmansodan jälkeen alkaneella elektroniikan aikakaudella kyber-termi sai uuden merkityksen. Syntyi kybernetiikaksi kutsuttu tiede, joka tutki elollisten olentojen ja teknisten laitteiden välistä viestintää sekä monimutkaisia ohjaus- ja säätöjärjestelmiä, jotka uusi sähkötekniikka teki mahdolliseksi. (Järvinen, 2018, s. 11)

3.1 Kybernetiikka

Ennen kuin William Gibson tieteisromaanissaan Neurovelho (alkuteos Neuromancer) ilmestyi vuonna 1984, suomennos 1991 yhdisti kyber- ja space-sanat yhdeksi kokonaisuudeksi, kyber oli ehkä tunnetuin tutkimusalan, kybernetiikan, määrittäjänä. Kybernetiikan juuret johdetaan Norbert Wienerin vuonna 1948 julkaisemaan teokseen Cybernetics; Or Control and Communivation in the Animal and the Machine, jossa hän tutki ohjaamisen ja valvonnan (control) suhdetta viestintään. Wienerin mukaan tehokas toiminta vaatii ennen kaikkea viestintää – oli kyse sitten orgaanisen tai mekaanisen järjestelmän ohjaamisesta. (Limnéll ym., 2014, ss. 29–30)

3.2 Bittimaailma

Limnéll ym., (2014, ss. 29–30) jatkaa, että kyber tarkoittaa kybernetiikan lisäksi myös bittien maailmaa, me kaikki elämme arkeamme kybermaailmassa. Meitä ympäröi fyysinen, atomien maailma. Fyysiseen maailmaan kuuluvat esimerkiksi kello kädessäsi, auto tai työpöytäsi. Atomien maailma on konkreettista, silmin havaittavaa. Tämän fyysisen maailman rinnalla on ihmisen luoma keinotekoinen, bittien maailma. Tähän maailmaan kuuluvat muun muassa internet, sosiaalinen media, erilaiset tietoverkot- ja järjestelmät sekä ohjelmistot älypuhelimessa. Tällöin puhutaan digitaalisesta maailmasta. Viime vuosikymmeninä arkemme on muuttunut erittäin nopeasti. Lähes kaikkien arkisten asioiden hoitoon käytetään tietojärjestelmiä, tietoverkkoja ja ohjelmistoja, eli kybermaailmaa. Meistä kukaan ei voi jättäytyä kybermaailman ulkopuolelle ja on tärkeää, että jokainen ymmärtää perusasiat siitä.

Kyber on enemmänkin digitaalista maailmaa kuvaava yhdyssanan etuliite, joka saa merkityksen, kun siihen lisätään tarvittava loppuosa, kuten kyber -rikollisuus, kyber -uhka tai kyber -turvallisuus. (Limnéll ym., 2014, ss. 29–30)

4 TIETOTURVA, TURVALLISUUS JA KYBERTURVALLISUUS

Fyysinen atomien maailma ja digitaalinen bittien maailma eivät ole erillisiä ja toisistaan riippumattomia. Lähitulevaisuuden megatrendeistä on fyysisen ja bittien tiivis kietoutuminen yhteen. Bitit ovat ottaneet merkittävällä tavalla vallan atomeista, fyysisen maailman toiminnot ovat tulleet riippuvaisiksi bittien maailman toimivuudesta. Bittien häiriötilanteet vaikuttavat välittömästi fyysiseen maailmaan. Bittien ja fyysisen maailman voimistuva yhteen kietoutuminen on yksi keskeinen syy siihen, miksi kyberturvallisuus on tällä hetkellä niin tärkeäksi koettu asia. Fyysinen maailma ja bittien maailma sulautuvat yhteen. (Limnéll ym., 2014, ss. 31–32)

Järvisen (2018, s. 14) mukaan termejä tietoturvallisuus ja kyberturvallisuus käytetään usein ristiin. Molemmissa on kyse samasta asiasta: datan suojaamisesta ja tietojärjestelmien toiminnan varmistamisesta. Toiminnoiden tavoitteilla on kuitenkin selvä ero.

4.1 Tietoturva

Järvinen (2018, s. 14) kertoo, että tietoturva pyrkii tietojen, tiedostojen ja yksittäisten koneiden suojaamiseen. Kun teet varmuuskopioita tiedostostasi, asennat päivityksiä ohjelmiin ja pähkäilet salasanojen kanssa, olet tekemisissä tietoturvan kanssa. Tietoturvallisesti toimimalla suojaat sekä omia tietojasi että perheen ja työnantajan toimintaa, sillä tietoturvasta huolehtiminen on jokaisen kansalaisvelvollisuus.

Helsingin kaupungin (2021) kehittämismenetelmäohjelman (Kehmet) mukaan tietoturvallisuus on yksi osa organisaation kokonaisturvallisuutta ja riskienhallintaa. Tietoturvatoiminnalla toteutetaan osaltaan organisaation strategiaa sekä arvoja. Tietoturvallisuustoimet tähtäävät kaikkina aikoina tietojen riittävän eheyden, käytettävyyden ja luottamuksellisuuden varmistamiseen. Eheydellä tarkoitetaan tiedon

yhtäpitävyyttä alkuperäisen tiedon kanssa. Käytettävyydellä tarkoitetaan tietoturvallisuuden yhteydessä sitä, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. Luottamuksellisuudella tarkoitetaan, ettei kukaan sivullinen saa tietoa.

Tietoturvallisuustoimet tulee aina suhteuttaa suojattavan kohteen arvoon, tietoturvallisuuteen ei kannata käyttää yhtään enempää rahaa ja työtä kuin tiedon ja toiminnan luonne vaatii. Näin ollen julkisen tiedon suojaamiseen ei tarvita aivan samanlaisia toimenpiteitä kuin esimerkiksi terveystietojen. Tietoturvajärjestelyjen tarkoituksena on varmistaa tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus siten, että tietoihin liittyvät riskit tulevat huomioiduiksi. Tietojen tulee olla käytettävissä niitä työ- tai palvelutehtävissä tarvitseville. Tiedot pitää suojata vääristymiseltä. Käyttörajoitettuihin tietoihin pääsy tulee varmistaa käyttöoikeuksia hallinnoimalla. Tietoturvajärjestelyiden riittävyys suhteessa tunnistettuihin tietoriskeihin tulee tarkastaa osana sisäistä valvontaa ja riskienhallintaa. (Järvinen, 2010, s. 15)
Järvinen (2010, s. 15) jatkaa, että tietoturva ja tietosuoja kuulostavat samalta ja aiheuttavat helposti sekaannuksia. Koska yksityisyydensuoja olisi hankala lausua, on päädytty kahteen samantyyppiseen termiin. Tietoturvan kohteena on tieto itse ja tietosuojan kohteena on ihminen.

Tietosuoja on yksi tietoturvallisuuden näkökulma. Tietoturvaa lähellä on myös kyberturvallisuus, jolla tarkoitetaan yhteiskunnallisesti merkittävien kohteiden ja sähköisten toimintojen turvallisuutta. (Helsingin kaupunki, 2021)

Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmä (VAHTI) on julkaissut useita hyviä tietoturvallisuuteen liittyviä oppaita ja ohjeita. VAHDISTA lisää luvussa 10.2 ja alaluvussa 10.2.1.

4.1.1 Hallinnollinen tietoturvallisuus

Leppänen (2006, s. 285) kirjoittaa, että hallinnollinen tietoturvallisuus koostuu tietoturvallisuuden johtamisen ja hallinnan prosesseista ja se kuuluu turvallisuusjohtamiseen. Teknologiayrityksissä painotetaan tietoturvallisuutta aivan erityisesti ja pidetään jossain

määrin synonyyminä turvallisuusjohtamiselle, jota se ei ole. Hallinnollinen tietoturvallisuus koostuu seuraavista elementeistä: tietoturvallisuuspolitiikka ja ohjeisto, resursointi, johtaminen, vastuiden määrittely, yhteys liiketoimintastrategiaan, toipumissuunnitelma ja kriittisten tapahtumien johtaminen, henkilöstöturvallisuus ja käytännön tietoturvallisuustoimenpiteet. Leppänen (2006, s. 285) jatkaa, että hallinnollinen tietoturvallisuus on osa turvallisuusjohtamista ja kokonaisvaltaista riskienhallintaa. Tietoyhteiskunnassa sillä on erityispainotus, mutta siltikin se on vain osa kokonaisuutta.

4.1.2 Käyttöturvallisuus

Leppäsen (2006, s. 304) mukaan käyttöturvallisuuden tavoitteena on minimoida käytöstä aiheutuvien riskien toteutuminen. Hän jatkaa, että työpaikalla tietokoneiden tulisi olla yksilöllisiä ja työntekijäkohtaisia. Kaikki tietokoneet pitäisi turvamerkitä ja luetteloida. Pöytäkoneiden fyysinen suojaus olisi järjestettävä niin, että ulkopuolisilla ei ole pääsyä koneen sisäosiin. Esimerkkinä mainittakoon tapaus, jossa henkilöstö oli ihmetellyt syytä koneiden hidasteluun. Huoltotyön yhteydessä paljastui, että koneesta puuttui lisämuisti. Tutkimuksissa selvisi, että kaikista muistakin pöytäkoneista oli hävinnyt lisämuistit. Tekijäksi paljastui siivoojan murrosikäinen poika, joka oli avaimilla päässyt tiloihin ja varastanut kaikista koneista lisämuistit yhden viikonlopun aikana. (Leppänen, 2006, s. 304)

4.2 Turvallisuus teknologiassa

Kun kaikkea digitalisoidaan, kannattaa kysyä onko suomalaisessa yhteiskunnassa ja elämässä asioita, joita ei kannata digitalisoida, kertovat Limnéll & Iloniemi (2018, ss. 154–155.) Heidän mukaansa yksi tällainen on vaalit. Vuonna 2017 sähköistä ja internetäänestämistä pohtinut oikeusministeriön työryhmä päätyi toteamaan, ettei se suosittele äänestämisen digitalisointia, koska riskit ovat suuremmat kuin hyödyt. Ihmisten luottamus vaalien rehellisyyteen ja oikeellisuuteen on toimivan demokratian edellytys ja äänestäessämme luotamme edelleenkin fyysiseen kynään ja äänestyslippuun. Vaalien turvallisuudesta ja luotettavuudesta huolehtiminen on noussut merkittäväksi puheenaiheeksi juuri teknologiaan

perustuvien vaikutuskeinojen takia. Vaalien turvaaminen tulee nousemaan jatkossa yhä merkityksellisemmäksi asiaksi.

Limnéllin ja Iloniemen (2018, ss. 154–155) mukaan vaalien luotettavuutta voidaan pyrkiä horjuttamaan monin tavoin äänestystavasta riippumatta. Mikään äänestysjärjestelmä, perinteinen analoginen tai digitaalinen, ei ole aukottoman turvallinen, ja siksi haavoittuvien kohtien tunnistaminen on välttämätöntä. Digitaalisessa toimintaympäristössä on tärkeää erottaa *kybertekniset* ja *kyberpsykologiset* vaikuttamisen keinot. Kybertekniset viittaa keinoihin, joissa esimerkiksi murtaudutaan tietojärjestelmiin ja muutetaan siellä olevia tietoja tai vuodetaan niitä julkisuuteen. Kyberpsykologisissa on kyse vaikuttamisesta ihmisten ajatteluun ja asenteisiin ja siten pyrkimykseen muuttaa ihmisten käyttäytymistä tai saada ihmiset olemaan tekemättä mitään. Kybertekninen ja -psykologinen vaikuttaminen eivät ole toisiaan poissulkevia, vaan päinvastoin kehityssuuntana on näiden vaikutuskeinojen yhä tiiviimpi yhteen kietoutuminen. Limnéll & Iloniemi (2018, ss. 154–155) lisäävät, että yleisen tietouden lisääminen vaaleihin vaikuttamiseen varautumisessa on erittäin tärkeää. Oleellista on tiedostaa, että teknologian aikakaudella vaikuttamisen keinot muuttuvat nopeasti ja uusiin vaikutuskeinoihin on kyettävä reagoimaan nopeasti.

4.3 Kyberturvallisuus

Järvinen (2018, s. 13) kertoo, että kyberturvallisuus-termi tuli Suomeen vuonna 2011. Valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta päätti maaliskuussa käynnistää kansallisen kyberturvallisuusstrategian laatimisen. Tavoitteena oli parantaa verkkohyökkäysten havainnointikykyä sekä kyberuhkien valvontaa ja ennaltaehkäisyä. Kyseessä oli tiettävästi ensimmäinen kerta, kun kyberturvallisuus-sanaa käytettiin Suomessa tässä merkityksessä.

Elinkeinoelämän keskusliitto EK (2016) määrittelee kyberturvallisuuden seuraavasti:

Kyberturvallisuus on turvallisuuden osa-alue, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan kriittisiin toimintoihin. Kybermaailma ja kriittinen infrastruktuuri ovat kietoutuneet toisiinsa tiukasti. Kriittisellä infrastruktuurilla tarkoitetaan yhteiskunnan toiminnalle välttämättömiä palveluita,

järjestelmiä ja rakenteita. Esimerkkeinä ovat maksujärjestelmät, liikenteen ohjausjärjestelmät ja sähköverkko.

Rouskun (2014, ss. 54– 55) mukaan kyberturvallisuus keskittyy vahvasti ICT-järjestelmien turvaamiseen niiden toimintaa uhkaavia riskejä vastaan. Pääpaino on niissä ympäristöissä, jotka ovat yhteyksissä tietoverkkoihin ja etenkin internetverkkoon. Useimmat kyberturvallisuuden pettämiseen liittyvät uutiset koskevatkin internetin kautta tehtyjä kyberhyökkäyksiä. Hyökkäyksillä on heikennetty tietoturvallisuutta, yksityisyyden suojaa sekä toimintojen käytettävyyttä eli tehty palvelunestohyökkäys. Rousku (2014, ss. 54–55) pohtii, voidaanko esimerkiksi klemmaria pitää kyberuhkana? Kyllä voidaan, sillä huhtikuussa 1997 klemmari väärässä paikassa aiheutti junien pysähtymisen Etelä-Suomen pääradoilla. Kymmenet junat pysähtyivät tunniksi tietokonevian takia. Vian syyksi paljastui klemmari, joka oli juuttunut tietokoneen huoltamiseen ja tarkastukseen käytettävän näppäimistön väliin, jonka vuoksi tietojärjestelmään oli jatkuvasti virrannut virhetietoa. Järjestelmä oli lopulta tukkiutunut ja junaliikenne jouduttiin pysäyttämään varotoimenpiteenä. Samana vuonna matkantekoa haittasivat myös ratatyöt, joten Suomen kuluttajaliitto suositti VR:lle korvausten maksamista.

5 KYBERUHKAT

Teknologiateollisuuden (2020) julkaisun mukaan kyberuhkat ovat haitallisia tapahtumia tai kehityskaaria, jotka saattavat vaikuttaa organisaation toimintaan, talouteen, sen hallussa olevaan tietoon ja jopa liiketoiminnan jatkuvuuteen. Kyberuhkalla tarkoitetaan sellaista uhkaa, joka toteutuessaan vaarantaa yhteiskunnan elintärkeän toiminnon tai muun kybertoimintaympäristöstä riippuvaisen toiminnon.

Seuraavassa alaluvussa on esitelty muutama esimerkki hakkerityypeistä ja organisaatioon kohdistuvista kyberuhkista Cyber Finland:in (2021) mukaan.

5.1 Hakkerityypit

Cyber Finland (2021) jakaa hakkerit eri tyyppeihin eri väristen hattujen avulla seuraavasti:

Mustista hatuista lukee usein uutisissa. He murtautuvat pankkien ja isojen yhtiöiden tietoverkkoon varastaakseen rahaa tai luottokorttitietoja. Mustat hatut ovat vastakohta valkoisille hatuille, jotka ovat niin sanottuja eettisiä hakkereita.
Valkoiset hatut ovat hakkerimaailman hyviä tyyppejä ja sankareita, jotka auttavat poistamaan viruksia ja testaamaan yhtiöiden tietoturvaa. Valkoisella hatulla on tyypillisesti IT-alan tutkinto ja he työskentelevät tietokoneiden ja tietoturvan parissa.
Mustan ja valkoisen hatun välistä löytyy harmaat hatut, jotka eivät varsinaisesti tee pahaa mutta ei myöskään hyvää hakkeroinnillaan. Nämä kolme päätyyppiä kattavat suurimman osan hakkereista.
Vihreät hatut ovat aloittelevia hakkereita, siniset hatut ovat myöskin vielä aloittelijoita, mutta he janoavat vaan kostoa esimerkiksi heitä netissä kiusanneelle.
Viimeisimpänä hakkerimaailmasta löytyy punaiset hatut, joilla on suurin vallan halu. Valkoisten hattujen tavoin he pyrkivät myös estämään mustien hattujen toiminnan ja he haluavat tuhota kokonaan mustan hatun. Virusten avulla ja hakkeroimalla he aiheuttavat tuhoa mustan hatun koneelle, joskus he myös sabotoivat mustan hatun elämää. (Cyber Finland, 2021)

Konttinen (2017) kertoo Kauppalehden Vieraskynä -blogissa, että Red Team- eli maalihyökkäyksellä yritys itse palkkaa hakkerit tunkeutumaan omiin järjestelmiinsä. Kyberturvamaailmassa tämä on läpäisytestauksen kehittynyt muoto. Red team on sodankäyntiin liittyvä termi, jota käytetään “vihollisyksikön” nimenä taisteluharjoituksissa. Termi on vakiintunut myös tietoturvan maailmassa.

5.2 Tietojenkalastelu

Kyberturvallisuuskeskus (2020, osa I, ss. 4–5) joka on Liikenne- ja viestintävirasto Traficomin alainen viranomainen, kertoo julkaisussaan, että tietojenkalastelun (eng. Phishing) tavoitteena on saada rikollisten haltuun käyttäjätunnus- ja salasanapareja tai muita käyttäjälle

tai organisaatiolle arvokkaita tietoja, kuten maksukorttitietoja. Esimerkiksi verkkopalvelun käyttäjä voidaan huijata vierailemaan rikollisten tekemällä internetsivustolla, joka muistuttaa ulkoasultaan palvelun aitoa sisäänkirjautumissivustoa. Kun käyttäjä syöttää tiedot huijaussivustolle, ne päätyvät rikollisten käyttöön. Näitä tietoja voidaan hyödyntää monin tavoin riippuen rikollisten motiiveista, haltuun saadun käyttäjätilin haltijan roolista tai tehtävistä organisaatiossa. Useimmiten rikolliset pyrkivät huijaamaan itselleen mahdollisimman monta sähköpostitunnusta. Tämän jälkeen he kirjautuvat tileille ja etsivät laskutukseen liittyviä hakusanoja. Näiden tietojen pohjalta luodaan valelaskuja, jossa hyödynnetään oikean laskun tietoja ja kontekstia. Tiliä voidaan hyödyntää myös uusiin tietojenkalasteluviesteihin, joita lähetetään uhrin kontakteille. Varastetuilla käyttäjätunnuksilla on puolestaan mahdollista vakoilla yrityssalaisuuksia. Onnistuneeseen tietojenkalasteluun voi liittyä myös maine- ja sääntelyriskejä. Kyberturvallisuuskeskus (2020, osa I, ss. 4–5) muistuttaa, että erityisen yleistä tietojenkalastelu on Microsoft Office 365 -ympäristössä. Se on Suomessa suosittu palvelu, eivätkä kaikki organisaatiot osaa käyttää riittävästi suojauskeinoja. Suomessa Microsoft Office 365 -tietojenkalastelun uhriksi on joutunut jo useita satoja organisaatioita ja niistä aiheutuneet vahingot lasketaan useissa miljoonissa euroissa. Hyökkääjät voivat esimerkiksi udella käyttäjätunnuksia ja salasanoja tai tekeytyä organisaation hallituksen jäseneksi sähköpostissa. Sen jälkeen he voivat luoda ja lähettää esimerkiksi huijaussähköposteja, joiden avulla organisaation taloushallintoa harhautetaan maksamaan väärennettyjä laskuja. (Kyberturvallisuuskeskus, 2020, osa I, ss. 4–5)

5.3 Haittaohjelmat

Kyberturvallisuuskeskus (2020, osa I, s. 7) tietää, että haittaohjelmat ovat tietokoneohjelmia, jotka aiheuttavat ei-toivottuja tapahtumia tietojärjestelmässä tai sen osissa. Yleensä haittaohjelmat leviävät sähköpostien liitetiedostojen, haittaohjelmilla saastutettujen verkkosivustojen sekä haavoittuvien palvelinten kautta. Haittaohjelma voi olla lähes harmiton, mutta entistä useammin niistä on myös vakavaa haittaa. Kyberturvallisuuskeskus (2020, osa I, s. 7) jatkaa, että maailmalla on yleistynyt ilmiö, jota kutsutaan nimellä Big Game Hunting. Termillä viitataan siihen, että rikollinen valitsee kohteikseen erityisen houkuttelevia ja rahakkaita organisaatioita. Hyökkäyksessä rikollinen tunkeutuu organisaation järjestelmiin ja

levittäytyy sen verkkoon. Lopuksi hyökkääjä käynnistää salatun kiristyshaittaohjelman, joka hidastaa ja haittaa organisaation toimintaa tai lamauttaa sen lähes kokonaan. Tämän jälkeen kiristetään lunnaita salauksen purkamiseksi. Nimensä mukaisesti hyökkääjät pyrkivät löytämään kohteita, joilla on hyvä maksukyky. Myös suuri käyttäjä- tai asiakasmäärä tekevät kohteesta houkuttelevan. (Kyberturvallisuuskeskus, 2020, osa I, s. 7)

5.4 Palvelunestohyökkäykset

Palvelunestohyökkäysten (eng. Denial of Service, DoS) merkitys on kasvanut sitä mukaa, kun yhteiskunta ja liiketoiminta ovat tulleet riippuvaisemmiksi internetistä. Palvelunestohyökkäykset tulee tuntea sekä ilmiönä että tekniikaltaan, jotta niiltä voi suojautua tehokkaasti (Kyberturvallisuuskeskus, 2020, osa I, s. 8). Tässä opinnäytetyössä asioita käsitellään hyökkäykseen varautuvan yrityksen ja sen liiketoiminnan näkökulmasta, mutta sama näkökulma pätee missä tahansa varautuvassa organisaatiossa ja sen ydintehtävässä.

Kyberturvallisuuskeskuksen (2020, osa I, s. 8) mukaan palvelunestohyökkäykset ovat internetissä jo arkipäivää ja niitä tehdään Suomessakin tuhansittain joka vuosi. Palveluestohyökkäyksessä verkkoa kuormitetaan ylimääräisellä tietoliikenteellä ja tavoitteena on lamaannuttaa jokin palvelu tai tietojärjestelmä. Usein hyökkäyksen kohteena on organisaation julkinen internetsivusto tai esimerkiksi asiakkaiden hyödyntämä palvelu. Hyökkäykset kestävät yleensä niin kauan, kun niillä on vaikutusta kohteen toimintaan. Useimmiten se loppuu, kun palvelunestohyökkäys saadaan torjuttua ja palvelun toiminta palautettua entiselleen. Monesti hyökkääjä kuitenkin vain vaihtaa kohdetta, ja keskittyy seuraavaksi johonkin muuhun saman kohdeorganisaation palveluun. Suurin osa kohdatuista kyberuhkista ei kohdistu yhteen ja tietoisesti valittuun organisaatioon. Kyberturvallisuuskeskus (2020, osa I, s. 8) kertoo, että kyberrikollisuus on luonteeltaan erittäin moraalitonta. Tavoitteena on löytää organisaatioiden järjestelmistä ja prosesseista heikkouksia, joita voi hyödyntää rikolliseen tarkoitukseen. Toiminta on yleensä kansainvälistä ja pitkälle automatisoitua ja muiden rikollisten tavoin kyberrikollisia kiinnostaa mahdollisuus nopeaan rahan saantiin. Kaiken lisäksi merkittävä osa kyberhyökkäyksistä toteutetaan hyvin yksinkertaisilla välineillä, muun muassa erilaiset huijaussähköposteilla, joiden avulla pyritään keräämään organisaation käyttäjien käyttäjätunnuksia ja salasanoja. Siksi kyberturvallisuutta

voi parantaa yksinkertaisilla keinoilla, kuten kouluttamalla henkilöstöä tunnistamaan huijausyritykset. Organisaation tulisi huolehtia, että yrityksen henkilöstöllä on tarpeeksi kyberturvallisuus osaamista. (Kyberturvallisuuskeskus, 2020, osa I, s. 8)

5.5 Käyttäjän manipulointi

The Finnish Terminology Centre (2018) on laatinut suosituksen tietotekniikan termistä Social Engineerin. Sen mukaan termi voi tarkoittaa sekä sosiaalista manipulointia, inhimillistä hakkerointia tai käyttäjän manipulointia. Manipuloinnin tarkoitus on saada käyttäjä paljastamaan pääsy yrityksen salattuihin tietoihin. Se voi olla huijaus (tai sen yritys) saada uhri luottamaan hyökkääjään tarpeeksi. Luottamusta voidaan kerätä esiintymällä jonain luotettavana tahona, kuten esimerkiksi valtiollisena palveluna, pankkina tai ko. yrityksen teknisenä tukena. Manipuloinnin tavoitteena voi olla tietojenkalastelun lisäksi haittaohjelman asentaminen uhrin koneelle. Manipulointi voi kohdistua yhteen tai useampaan henkilöön. (The Finnish Terminology Centre, 2018)

Elinkeinoelämän Keskusliiton asiantuntija Mika Susi (2015) selvittää artikkelissaan, mitä käyttäjän manipuloinnilla tarkoitetaan, mitä sillä tavoitellaan ja keneen se voi kohdistua. Paras tapa suojautumiseen olisi ihmispalomuuri. Manipuloinnin tavoitteena saattaa olla välitön taloudellinen hyöty tai yritykselle kriittisen tiedon varastaminen. Joskus sen taustalla voi olla myös poliittinen motiivi. Yrityksen tietoja havittelevan hyökkääjän on usein helpompi huijata ihmistä kuin murtaa tietojärjestelmien tekniset suojaukset.

5.6 Informaatiovaikuttaminen

Lönnqvist & Moilanen (2017, s. 12) kertovat, että tietoon – eli informaatioon – pyritään vaikuttamaan koko ajan. Esimerkkejä arjessa tällaisesta vaikuttamisesta ovat mm. mainonta tai valistuskampanjat, joilla meitä yritetään saada syömään terveellisemmin tai liikkumaan enemmän. Tietoon vaikuttaminen on merkittävä osa myös valtioiden välisiä suhteita ja erilaisia kriisejä. Tällaisissa tapauksissa puhutaan informaatiovaikuttamisesta tai informaatiosodankäynnistä. Niillä tarkoitetaan vaikuttamista kansalaisiin, päätöksentekijöihin ja toimintakykyyn ohjailemalla saatavilla olevaa informaatiota ja sen kulkua.

He jatkavat, että teknologia on muuttanut suomalaista viestintäympäristöä huomattavasti. Perinteisellä medialla ei ole enää pitkään aikaan ollut viestinnällistä monopolia, vaan kuka tahansa voi saavuttaa hyvinkin suuria yleisöjä internetin ja sosiaalisen median kautta. Siksi informaatiovaikuttaminenkin on nykyisin helpompaa – ja usein huomaamattomampaa – kuin aiemmin. On tärkeää, ettemme usko kaikkea, mitä esimerkiksi sosiaalisessa mediassa näemme. Siellä välitettävä tieto voi olla tahallisesti vääristeltyä tai täysin virheellistä. On olemassa jopa kokonaisia verkkosivustoja, joiden tarkoituksena on levittää virheellistä ja jonkin tietyn toimijan etuja palvelevaa tietoa. Tällöin voidaan puhua valemediasta – oikeat mediat tarkistavat välittämänsä tiedot ja pyrkivät aina mahdollisimman virheettömään viestintään, vaikka niilläkin toki on usein omia tavoitteita ja tarkoitusperiä.
Lönnqvistin & Moilasen (2017, s. 13) mukaan informaatiovaikuttamiselta (eng. Informational influence) suojautuminen perustuu osaamiseen ja tietoon. Informaation lähdettä kannattaa aina pyrkiä arvioimaan sitä koskevan tiedon perusteella ja samasta aiheesta kannattaa pyrkiä hankkimaan tietoa useista eri lähteistä. Tällöin voi kehittää ns. media- tai monilukutaitoaan, joka on yksi modernin yhteiskunnan uusista kansalaistaidoista. (Lönnqvist & Moilanen, 2017, ss. 12–13)

5.7 Esineiden Internet

Logistiikan maailman (2021) mukaan esineiden Internetin (eng. Internet of Things, IoT) tekniikoiden avulla voidaan kytkeä laitteita Internet-verkkoon. Laitteista voidaan lukea tietoa, tai laitteita voidaan ohjata Internetin yli. Kytkettävä esine voi olla vaikka yksittäinen lämpömittari tai suurempi kokonaisuus kuten ajoneuvo. Vaikka Esineiden Internet on melko uusi käsite, automaatiotekniikassa on käytetty pääpiirteissään samankaltaisia ratkaisuja jo vuosikymmeniä. Erona aikaisempaan automaatiotekniikkaan otettiin ensin käyttöön termi M2M, machine-to-machine yhtenä e-liiketoiminnan muotona, vrt. B2C business-to-consumer. Yhtenä erinomaisena, laajasti käytössä olevana M2M-ratkaisuna voidaan pitää kiinteistöjen sähkömittareiden etälukua. (Logistiikan maailma, 2021)

IoT-laitteet toimivat sekä fyysisessä maailmassa että verkossa. Alla olevassa kuvassa (1) havainnollistetaan, kuinka laitteet kytkeytyvät verkkoon ja elämään.

Kuva 1. Internet of Things. Lähde: Huffington Post

Kuva 1: Esineiden maailma (Logistiikan maailma, alun perin Huffington Post, 2021).

Yle:n uutisissa (Kellman, 2019) kyberasiantuntija Jussi Eronen kertoo, ettei esineiden internetin tietoturvasta ole juuri ole säätelyä ja ongelmaan on herätty EU:ssa vasta viime vuosien aikana. Hän jatkaa, että älyjääkaappi on hyvä esimerkki tällaisesta laitteesta. Liikenne- ja viestintävirasto Traficomissa tutkitaan, voitaisiinko kuluttajia auttaa antamalla enemmän tietoa laitteiden tietoturvasta. Hyviksi havaituille laitteille voitaisiin antaa tietoturvamerkki, joka viestii kuluttajalle, että perusasiat on hoidettu kunnialla ja laitteelle on valmistajan tuki. Jussi Erosen mukaan älylaitteita voidaan hakkeroida esimerkiksi haittaohjelmien käyttöön. Näin voi käydä, jos ohjelmistojen kehityksessä ei ole otettu huomioon tietoturvaa.

5.8 Vakavimmat kyberuhkat Suomelle

Ollila (2021, ss. 40–41) kirjoittaa tietotekniikan ammattilaismedia Tivi:ssa, että eri kohteisiin suuntautuu erityyppisiä kyberuhkia. Valtionhallintoon kohdentuvat vakavammat kyberuhat ovat kiristysyritysten ohella tiedon laittomaan hankintaan liittyviä aikeita, jolloin yleensä puhutaan verkkovakoilusta. Ulkoministeriö koki tällaisen julkisuudessakin olleen tapahtuman vuonna 2013. Todennäköisesti myös eduskunnan postijärjestelmään murtautuminen vuoden 2020 syyskuussa oli samaa lajia. Kybermurtojen havaitseminen tapahtuu valitettavan usein reaktiivisesti, kun jokin turvatyökalu tunnistaa haitallisen tai poikkeavan toiminnan.

Limnéll & Iloniemi (2018, s. 174) ovat sitä mieltä, että teknologian kehittyminen tuo uusia kyvykkäitä toimijoita turvallisuuden ja sodankäynnin areenoille. Kyberhyökkäykset saattavat antaa väärän vaikutelman siitä, ettei kysymys olisi vakavasta tapahtumasta, koska ihmishenkiä ei välttämättä menetetä. Kuitenkin hyökkäykset yhteiskunnan kriittistä infrastruktuuria vastaan saattaa aiheuttaa aineellisten tappioiden lisäksi myös ihmishenkien menetyksiä. Vakavimpina suomalaisen yhteiskunnan kyberuhkina lähitulevaisuudessa voi pitää laajalle kriittiseen infrastruktuuriin (sisältäen finanssialan, terveydenhuollon, energiantuotantoon ja -jakelun) kohdistuvaa kyberhyökkäystä tai laajamittaista datamanipulaatiota. Massiivinen valtionhallinnon organisaation ja yhteiskunnan toimivuuden kannalta keskeisen yrityksen tietovuoto on myös vakava uhka. Limnéll & Iloniemi (2018, s. 174) tietävät, että Suomi on pitkälle kehittyneenä tietoyhteiskuntana erittäin riippuvainen tietoverkkojen ja -järjestelmien toiminnasta, minkä vuoksi kybertoimintaympäristön kautta tulevat uhkat ovat kokonaisturvallisuuden kannalta hyvin merkittävä tekijä.

6 RISKIENHALLINTA

Rouskun (2014, s. 61) mukaan riskienhallinnan tulisi olla ensimmäinen ja kaikkein tärkein termi. Kaikki tietoturvallisuuden ja jatkuvuuden hallinnan kehittämisessä tehtävä työ on riskienhallintaa. Ilman riskienhallintaa osa investoinneista kohdistuu vääriin kohteisiin, jotka pohjautuvat mutu- (musta tuntuu, tekijän huom.) tai rahi- (ravistettu hihasta, tekijän huom.) menetelmillä arvioituihin kehittämiskohteisiin. Osa kehittämisestä saattaa kohdistua oikeisiin kohteisiin, mutta osa ei.

Jordan ja Silcock (2006, ss. 36–37) kertovat, että riskienhallinnasta vastaavan näkökulma IT:n hallintoon alkaa siitä, että hän ymmärtää riskien liittyvän kaikkiin yrityksen toimintoihin. Korkeimmalla tasolla tämä ilmenee siinä, kuinka yritykseltä odotettujen tavoitteiden, esimerkiksi tuottavuuden, täyttäminen vaikuttaa suoraan niihin riskirajoihin, joilla sen pitää toimia. Riskienhallinnasta vastaava johtaja ymmärtää myös, mikä suhde on riskillä ja tuotolla. Mitä enemmän riskejä yritys sietää ja hoitaa hyvin, sitä paremman tuoton osakkaat saavat.

Kyberturvallisuuskeskuksen (2020, osa III, s. 14) mukaan organisaatiot tekevät usein riskiarviointeja ainoastaan vaatimustenmukaisuuden noudattamiseksi. Näitä voivat olla esimerkiksi ulkoisista tekijöistä, kuten sääntelyvaatimuksista johtuvat velvoitteet, asiakkaiden vaatimukset tai lakisääteiset vaatimukset. Tässä on kuitenkin vaarana, että riskinhallinnasta tulee vain ”rasti ruutuun” toimintaa. Tällaisessa tilanteessa organisaatiot voivat luulla hallitsevansa riskejä, vaikka ne ovat ainoastaan toimineet määritellyn prosessin mukaisesti. Vaatimusten noudattaminen ja turvallisuus eivät ole sama asia. Ne voivat olla päällekkäisiä, mutta yleisiä turvallisuusvaatimuksia voidaan noudattaa käytännössä heikoilla turvallisuuskäytännöillä. Kyberturvallisuuskeskus muistuttaa, että hyvä riskienhallinta ulottuu pelkkää vaatimusten noudattamista pidemmälle. (Kyberturvallisuuskeskus, 2020, osa III, s. 14)

6.1 Kyberturvallisuus riskienhallintaprosesseihin

Kyberturvallisuuskeskus (2020, osa III, s. 15) ohjeistaa, että kyberriskien olisi oltava osa organisaation arjen riskienhallintaa, sillä kyberriskien käsitteleminen erillään tai niiden luokitteleminen yksinkertaisesti vain ’tietoteknisiksi riskeiksi’ vaikeuttaa niiden vaikutusten tunnistamista. Samalla saattaa jäädä myös epäselväksi, mitä vaikutuksia organisaation muilla riskeillä voi olla sen kyberturvallisuuteen. Kyberturvallisuustoimenpiteiden tulee tukea ja mahdollistaa liiketoimintaa hallitsemalla digitaaliteknologian käytöstä johtuvia riskejä. Ne eivät kuitenkaan saa estää tai hidastaa olennaisia liiketoimintaa edistäviä toimenpiteitä tai aiheuttaa kustannuksia kohtuuttomasti. (Kyberturvallisuuskeskus, 2020, osa III, s. 15)

6.2 Riskiarviointi

Riskiarvioinnista Kyberturvallisuuskeskus (2020, osa III, s. 15) kertoo, että toiminnan häiriöttömyys on tyypillisesti hyvän kyberturvallisuuden lopputulos. Sitä voi olla hankala mitata, sillä häiriöt voivat johtua myös organisaation kyberturvallisuustoimenpiteistä riippumattomista asioista. Riskiarvioinneissa esitetään tavallisesti jonkinlainen arvio riskin todennäköisyydestä ja vaikutuksista (esimerkiksi pieni - keskisuuri - suuri). Tällaisen arviomenetelmän käyttäminen toimenpiteiden onnistumisen mittarina voi olla houkuttelevaa, mutta täytyy kuitenkin huomioida, että tällaiset arviot saattavat mitata

vajavaisesti organisaation toteuttamia toimenpiteitä. Kyberturvallisuuskeskuksen (2020, osa III, s. 15) mukaan se johtuu siitä, että kyberriskeihin vaikuttavat ulkoiset tekijät (kuten ohjelmistohaavoittuvuudet) muuttuvat nopeasti ja ovat usein organisaation vaikutusmahdollisuuksien ulottumattomissa. (Kyberturvallisuuskeskus, 2020, osa III, s. 15)

6.3 Kyberriskiarvioinnin luotettavuus

Kyberturvallisuuskeskuksen (2020, osa III, s. 15) mukaan kyberriskien hallintaan sovelletaan samoja riskienhallinnan periaatteita kuin muihinkin riskeihin. Kyberturvallisuuden ratkaisut ja teknologiat kehittyvät niin nopeasti, että vaarana on jäädä jälkeen ja käyttää kyberriskien arviointiin vanhentuneita menetelmiä. Sen takia kyberriskejä olisi hyvä arvioida useammin kuin muita riskejä. Kyberturvallisuus on vielä uusi termi ja sen käyttö vakiintumatonta, jonka vuoksi organisaatiolla ei välttämättä ole samanlaista ymmärrystä kyberriskeistä kuin esimerkiksi taloudellisista tai työntekijöiden turvallisuuteen liittyvistä riskeistä. Käytettävissä ei välttämättä ole myöskään tietopohjaa, jonka perusteella riskien arviointi voitaisiin tehdä. Kyberturvallisuuskeskus (2020, osa III, s. 15) huomauttaa, että tämä on syytä huomioida, kun pohditaan kyberriskien arvioinnin luotettavuutta, etenkin jos sen tuloksia verrataan suoraan perinteisiin riskiarviointeihin. (Kyberturvallisuuskeskus, 2020, osa III, s. 15)

7 VARAUTUMINEN JA JATKUVUUS

Rousku (2014, ss. 60–61) arvelee mitä tapahtuu, jos tietojärjestelmään tai palveluun tulee ongelma, eli häiriö? Se saattaa vaikuttaa palvelun toimintaan merkittävästi tai haitata sitä hidastaen. Tavallisella käyttäjällä häiriö saattaa jäädä jopa kokonaan näkymättä. Häiriö pitäisi kuitenkin saada korjattua. Tietojärjestelmällä tulee olla suunnitelma, jonka avulla varaudutaan häiriöihin ja taataan toiminnan jatkuvuus.

Kyberturvallisuuskeskus (2020, osa IV, s. 18) kertoo, että kun organisaatioon tai sen yhteistyökumppaneihin kohdistuvat uhkat ymmärretään, voidaan määrittää myös organisaation kyberturvallisuustoimenpiteet ja -investoinnit. Organisaatiossa olisi tehtävä

tietoinen päätös siitä, miltä uhkilta se pyrkii suojautumaan. Muutoin vaarana on, että yritetään suojautua kaikelta, joka taas johtaa helposti tehottomiin toimenpiteisiin. Kyberturvallisuuskeskus (2020, osa IV, s. 18) muistuttaa, että vain kyberuhkien ymmärtäminen auttaa tekemään tietoisia toimintaa ohjaavia päätöksiä. Keskeistä on tietoisuus hyökkääjien vaikuttimista: Miksi he olisivat kiinnostuneita juuri tästä organisaatiosta? Hyökkääjän motiivi voi toki olla vain se, että organisaatiolla on internetiin kytkettyjä ja helposti haavoitettavia tietokoneita, joita voidaan hyödyntää rikolliseen toimintaan. Kumppanit ja vertaisorganisaatiot ovat usein hyviä lähteitä tiedon saamiseen uhkista ja hyvistä suojauskäytännöistä. Yhteistyösuhteiden ja tiedonvaihdon kehittäminen parantaa merkittävästi kykyä suojautua kyberuhkilta, eikä sitä tule nähdä kilpailuriskinä sillä jaettu tieto koituu lopulta kaikkien hyödyksi, Kyberturvallisuuskeskus (2020, osa IV, s. 18) jatkaa.

7.1 Uhkien arviointi

Kyberturvallisuuskeskus (2020, osa IV, s. 18) neuvoo priorisoimaan mahdolliset uhkat, sillä merkittävien uhkien ja mahdollisten hyökkääjien kartoittaminen helpottaa päätöksentekoa siitä, miltä uhkilta organisaation tulisi suojautua aktiivisesti. Asiantuntijat ymmärtävät uhkien teknisen luonteen ja hallitus puolestaan tiedostaa, miksi organisaatio saattaa olla houkutteleva kohde hyökkääjille. Lisäksi on tärkeää keskustella jo etukäteen kaikista sellaisista päätöksistä, joilla voi olla merkittävää vaikutusta organisaation uhkaprofiiliin. Tällä tavoin toimien teknisillä asiantuntijoilla on riittävästi aikaa toteuttaa tarvittavat suojautumistoimenpiteet. (Kyberturvallisuuskeskus, 2020, osa IV, s. 18)

7.1.1 Liike- ja ammattisalaisuudet

Laaksosen ym. (2006, ss. 75–76) mukaan yritysten liike- ja ammattisalaisuuksien pysyminen salaisuuksina edellyttää aktiivisia toimenpiteitä, koska kyse on tiedoista, jotka eivät ole yleisessä tiedossa ja niillä on taloudellista arvoa. Liiketoiminnan kannalta on tärkeää, että kilpailuetua sisältävät yrityssalaisuudet pysyvät myös salassa. Yrityssalaisuudet voivat koskea esimerkiksi tuotekehitystietoja, prototyyppejä tai muuta tutkimustietoa. Liike- ja

ammattisalaisuus-, sekä yrityssalaisuustermiä ei ole missään laissa yksiselitteisesti määritelty, mutta lähtökohtana voidaan pitää sitä, että niillä tarkoitetaan samaa asiaa.
He jatkavat, että rikoslain 30:11 pykälän määritelmä yrityssalaisuuden käsitteestä tarkoitetaan liike- tai ammattisalaisuutta tai muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinoharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedon hänelle. Lähtökohtana on, että yrityssalaisuudella tulee olla taloudellista arvoa yritykselle, jotta se voisi olla yrityssalaisuus. Yrityssalaisuutta kuvaa myös hyvin se, että sen omistajalla tulee olla intressi ja pyrkimys säilyttää se salaisuutena ja ei-julkisena tietona. Yrityksen sisälläkään kaikki työntekijät eivät pääse käsiksi yrityssalaisuuksiin, koska yrityksen tulee osoittaa salassapitointressiä yrityssalaisuuksiensa osalta. (Laaksonen ym., 2006, ss. 75–76)

7.2 Kohdistamattomat hyökkäykset

Kyberturvallisuuskeskus (2020, osa VI, s. 19) kertoo, kuinka kohdistamattomassa hyökkäyksessä hyökkääjä haluaa saavuttaa samalla kertaa tuhansia potentiaalisia uhreja yhden valikoidun kohteen sijaan. Hyökkääjät käyttävät usein automaattisia ja yleisesti saatavilla olevia välineitä, jotka esimerkiksi skannaavat julkisia verkkosivustoja tai muita palveluja haavoittuvien järjestelmien tai palvelujen löytämiseksi. Kun sellainen löytyy, sama työkalu hyödyntää automaattisesti sen haavoittuvuutta esimerkiksi tietomurron toteuttamiseksi. Tällaisen massahyökkäyksen vaikutukset voivat olla yhtä vakavia kuin kohdistetun hyökkäyksen. Kyberturvallisuuskeskuksen (2020, osa VI, s. 19) mukaan kyberturvallisuuden hyvä perustaso suojaa järjestelmät valtaosasta kohdistamattomia hyökkäyksiä.

7.3 Varautuminen

Seuraavassa alaluvussa on lueteltu Ollilan (2021, ss. 40–41) ohjeistuksia Tivi-lehdessä, kuinka organisaatiossa tulisi varautua kyberuhkia varten.

7.3.1 Varautuminen organisaatiossa

Ollilan (2021, ss. 40–41) ohjeita varautumiseen:

- Huomioi kiristyshaittauhka riskiarvioissa
- Tee suunnitelma kriisin varalta. Huomioi suunnitelmassa myös viestintä sisäisesti ja tarvittaessa ulkoisesti.
- Harjoittele varmuuskopioiden palauttamista.
- Testaa havainnointikyky siitä näkökulmasta, havaitaanko esimerkiksi rikollisten yleisesti käyttämät haittaohjelmat tai leviämisen sisäverkossa.
- Huolehdi perustietoturvasta. Tähän sisältyvät esimerkiksi verkon segmentointi ja päivitykset. Tietoverkon segmentoinnilla tarkoitetaan tietoverkon jakamista pienempiin osiin. Segmentoinnilla pyritään parantamaan verkon tietoturvaa ja suorituskykyä.

Ollila (2021, ss. 40– 41) jatkaa, että tärkeintä on varmistaa, että varmuuskopiot voidaan palauttaa myös tilanteessa, jossa organisaation keskitetty käyttövaltuushallinta on saavuttamattomissa. Lisäksi varmuuskopiot tulee voida tarkastaa sen varalta, että hyökkääjän hankkima jalansija organisaatioon on varmuuskopioitu.

7.3.2 Varautuminen kotona

Entä kuinka varautua kotona? Lönnqvist & Moilanen (2017, s. 5) ohjeistavat pohtimaan omaa selviytymisstrategiaa, koska siihen on tarjolla paljon tietoa. Kybermaailmassa esiintyvät vakavat häiriöt vaikuttaisivat elämäämme hyvin samalla tavoin kuin esimerkiksi laaja sähkökatko. Siksi kannattakin tutustua Puolustusministeriön julkaisemaan oppaaseen ”Pahasti poikki”. Lisäksi kannattaa pitää huoli, että kotona on varastossa kotivara – ruokaa ja muita päivittäin välttämättä tarvittavia tavaroita noin viikon ajaksi.

7.4 Jatkuvuus

Rousku (2014, ss. 60–61) kertoo, että jatkuvuudenhallintasuunnitelmalla organisaation tulisi varmistaa, että vahingot häiriötilanteiden sattuessa pysyisivät mahdollisimman pieninä.

Käytännössä suunnitelmat perustuvat organisaation bisneksen jatkuvuuden takaamiseen. Tällöin toiminnot, joiden häiriöillä ei ole suurta merkitystä organisaation toimintaan, jäävät pienemmälle huomiolle. Toimintojen keskinäiset toiminnot tulisi osata arvioida ja kuvata oikealla tavalla. Muutoin ei välttämättä tiedetä, mikä toiminto vaikuttaa mihinkin toimintoon. (Rousku, 2014, ss. 60–61)

8 KYBERTURVALLISUUSOSAAMINEN

Kyberturvallisuuskeskuksen (2020, osa VII, s. 27) mukaan kyberturvallisuusosaajien kysyntä kasvaa jatkuvasti. Tämä aiheuttaa haasteita organisaatioiden tarvitseman osaamisen saatavuudelle ja organisaatiossa on tärkeää miettiä, millaista asiantuntemusta tarvitaan nyt ja tulevaisuudessa sekä miten osaaminen hankitaan. Global Information Security Workforcen tekemän tutkimuksen mukaan pelkästään Euroopassa tulee olemaan vuoteen 2022 mennessä 350 000 kyberturvallisuusammattilaisen saatavuusvaje. Kyberturvallisuuskeskus (2020, osa VII, s. 27) muistuttaa, että organisaatiossa tulee selvittää, millaista kyberturvallisuuteen liittyvää asiantuntemusta se tarvitsee, sillä kyberturvallisuuteen liittyy monia erilaisia taitoja, jotka vaihtelevat esimerkiksi tietoverkkojen turvallisuudesta aina riskien- ja poikkeamienhallintaan asti. Ensin kannattaa pohtia, mitä taitoja organisaatio tarvitsee tärkeimpien tavoitteiden saavuttamiseksi ja riskien hallitsemiseksi. Sen jälkeen voidaan arvioida, mitä näistä taidoista ei voida hankkia ulkoistettuna. Tulee määritellä, miten nopeasti organisaatio tarvitsee näitä taitoja. Jos on tarkoitus kehittää nykyisen henkilöstön osaamista, kannattaa huomioida, että riittävän asiantuntemuksen saavuttaminen vie aikaa. Yksittäiset kurssit eivät vielä tee kenestäkään kyberturvallisuuden asiantuntijaa, sen lisäksi on oltava myös mahdollisuus kehittää käytännön osaamistaan. Lisäksi Kyberturvallisuuskeskus (2020, osa VII, s. 27) ohjeistaa, että jos asiantuntemusta tarvitaan nopeasti, konsultin tai asiantuntijan palkkaaminen on parempi vaihtoehto.

8.1 Johtaminen

Laaksosen ym. (2006, ss. 115–116) mukaan nykyaikaisella johtajalla tulee olla tietotaitoa ja valmiudet taloushallinnon, henkilöstöhallinnon ja tietotekniikan alueilta. Tähän listaan

voidaan lisätä myös tietoturvallisuus. Toimivan tietoturvallisuuden perustana on täsmällinen johtaminen sekä tietoturvallisuuden liittäminen tiiviisti organisaation varsinaiseen liiketoimintaan. Johtamisen taito on kyky motivoida ja opettaa. Tietoturvallisuus on mahdollista saada osaksi työntekijöiden jokapäiväistä toimintaa, kun se yksinkertaisesti sisällytetään henkilöiden rutiineihin. (Laaksonen ym., 2006, ss. 115–116)

8.1.1 Strateginen johtaminen

Kamensky (2010, s. 319) kertoo, että strategisella johtamisella on kolme suurta haastetta: Luoda menestysstrategia, toteuttaa se ja uudistaa strategia ajoissa riittävän voimakkaasti. Strategian toteuttamista pidetään vaikeimpana alueena ja sen tuomaa haastetta ei pidä koskaan väheksyä.

Kamensky (2010, s. 319) jatkaa, että strategisten suunnitelmien täydellinen toteutuminen olisi luonnonlakien vastaista. Täydellisen toteutumisen esteet tulevat sekä organisaation ympäristöstä että organisaation sisältä. Nykyinen ja tuleva ympäristö nostavat kaikkien osaamisalueiden eli tietojen, taitojen, näkemyksen, halun ja rohkeuden vaikeuskerrointa. Näkemyksen vaateet kasvavat voimakkaasti. On tärkeää hahmottaa tulevaisuuden näkemys, mutta yhä tärkeämpää on näkemys nykyisestä todellisuudesta. Muutososaaminen ja vuorovaikutusosaaminen nousevat yhä ratkaisevammiksi. (Kamensky, 2010, s. 319)

8.1.2 Kyberjohtaminen

Valtioneuvoston tutkimuksessa ”Kyberturvallisuuden strateginen johtaminen Suomessa” Lehto ym. (2018, s. 81) kertovat, että kyberturvallisuuden strateginen johtaminen on digitaalisen toimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistamista, asettamista, toiminnan ja varautumisen yhteensovittamista sekä laajamittaisten häiriöiden hallinnan johtamista. Kyberturvallisuudessa menestyäkseen yhteiskunnan on kyettävä sovittamaan eri toimijat ja yhteensovittamaan voimavarat sekä toimintatavat mahdollisimman tehokkaasti asetettujen yhteiskunnan strategisten tavoitteiden saavuttamiseksi.

Limnéllin & Iloniemen (2018, ss. 177–178) mukaan kyberuhkia vastaan toimiminen edellyttää uudenlaisia tapoja toimia yritysten ja julkisten toimijoiden välillä sekä myös kansainvälisessä yhteistyössä. Kyberuhkista on aktiivisesti jaettava tietoa ja tapahtuneista hyökkäyksistä sekä arvioitava tulevia haavoittuvuuksia tai vaikuttamisen keinoja. Keskeisintä on yhteisen tilannetietoisuuden kehittäminen ja kansainvälisen yhteistyön tiivistäminen. Kyberuhkiin vastaaminen edellyttää vahvaa ja keskitettyä havainnointi-tilannekuva-johtamisen kyvykkyyttä sekä yhteistyötä muiden kanssa. Kyberturvallisuuden – ja turvallisuuden – strategisessa johtamisessa tarvitaan tilanneymmärrystä, selkeitä johtamisvastuita ja -rooleja, saumatonta tiedonkulkua ja -vaihtoa. Limnéll & Iloniemi (2018, ss. 177–178) jatkavat, ettei kybervaikuttaminen perustu kineettiseen voimaan vaan älykkyyteen ja innovatiivisuuteen. ”Kybertaistelut” voittaa se, joka käyttää huipputeknologiaa älykkäämmin ja tehokkaammin.

9 FORENSIIKKA

Uhkakuvat -teoksessa Limnéll & Iloniemi (2018, s. 160) kertovat, että teknologiaan ja digitalisaatioon yhdistyvien uhkien tulevaisuuden arviointi on haasteellista kahdesta syystä. Ensimmäiseksi kyse on teknologian kehityksen kiihtyvästä muutosnopeudesta, jolloin myös ennakointi on haasteellisempaa. Esimerkiksi kyberrikollisten käyttämät toimintatavat saattavat puolen vuoden päästä jo olla toisenlaisia. Toiseksi kyse on digitaalisen ja fyysisen maailman sulautumisesta turvallisuuden näkökulmasta yhdeksi maailmaksi. Se luo osaltaan epävarmuutta ja lisähaastetta Suomen turvallisuuteen vaikuttavien uhkatekijöiden ennustettavuuteen. (Limnéll & Iloniemi, 2018, s. 160)

Tampereen yliopiston (n.d.) Cyber Security -kurssin verkkoaineistomateriaalin mukaan tietorikosten tutkimista kutsutaan nimellä forensiikka, sillä sana 'forensic' tarkoittaa oikeusopillista ja termiä 'computer forensics' käytetään erilaisista jäljitystoimista, joilla selvitetään, mitä rikoksesta epäilty on tehnyt omalla tai jonkun muun tietokoneella. Tutkittava rikos voi tietysti liittyä aivan muihin asioihin kuin tietotekniikkaan.

Hyökkäyksen tyypistä riippumatta jälkiselvittelyyn liittyy yleensä forensiikkaa. Ollila (2021, ss. 40–41) kirjoittaa, että Ulkoministeriön tietohallintojohtaja Ari Uusikartano on sitä mieltä, että tällöin tutkitaan hyökkäystyökaluja ja sitä, mistä vastapuoli on kiinnostunut. Haetaan motiivia

ja tahoa, joka on toiminnan takana. Ongelmien välttäminen riippuu siitä, onko hyökkäysvektori ja metodiikka aiemmin tunnettu. Näin ei välttämättä aina ole, vaikka turvallisuudessa voi ennakoida, torjuja on pakotettu olemaan reaktiivinen. Hyökkäyksen jälkeen yksittäisen tapauksen vastatoimet voivat kestää kuukausia, jopa vuosia. Turvatoimet pitää uudistaa, mikä tarkoittaa salasanojen vaihtoa, kaksivaiheista tunnistamista, pääsynhallinnan kehittämistä jne. Joskus koko tekninen ympäristö on rakennettava uudelleen. Ari Uusikartano näkee hyötyjä myös turva-arkkitehtuuristandardien noudattamisessa. Kriittisille toiminnoille on suositeltavaa hankkia myös sertifiointi, kuten ISO27001-tietoturvasertifikaatti. (Ollila, 2021, ss. 40–41)

Poliisi.fi (2020) kertoo, että kyberrikokset käsittävät kaiken tietoverkoissa tapahtuvan tai tietoverkkoja hyödyntävän rikollisuuden. Tietoverkkorikosten yhteydessä käytetään usein jakoa tietoverkkosidonnaisiin (cyber dependent) ja tietoverkkoavusteisiin (cyber enabled) rikoksiin:

Tietoverkkosidonnaiset rikokset kohdistuvat tietoverkkoihin ja tietojärjestelmiin. Rikoksen tekeminen on mahdollista ainoastaan tietokoneita ja tietoverkkoja käyttäen. Tällaisia tekoja ovat esimerkiksi tietojärjestelmän häirintä eli palvelunestohyökkäykset, tietomurrot tai datavahingonteko. (Poliisi.fi, 2020)

Tietoverkkoavusteisissa rikoksissa hyödynnetään tietoverkkoja tai tietojärjestelmiä osana rikoksen tekemistä. Kyse on sinänsä perinteisestä rikollisuudesta kuten petoksista, huumausainerikollisuudesta, rahanpesusta, mutta joiden toteuttamiseen tietoverkot tuovat uusia tekotapoja. Tietoverkot mahdollistavat rikoksen tekemisen tietoverkkojen avulla, mutta teko ei kohdistu tietoverkkoon tai tietojärjestelmään. (Poliisi.fi, 2020)

9.1 Laki liikenne ja viestintärikoksista

Laki Liikenne- ja viestintävirastosta luvun 1 mukaan liikenne- ja viestintävirasto on liikenne- ja viestintäministeriön hallinnonalalla toimiva keskushallinnon virasto, joka hoitaa liikenteen ja sähköisen viestinnän viranomaistehtäviä. Luvun 2 Liikenne ja viestintäviraston organisaatio ja johtaminen 5 §:n mukaan Kyberturvallisuuskeskus toimii organisatorisesti ja toiminnallisesti erillisenä suoraan pääjohtajan alaisuudessa ja vastaa valtakunnallisista tietoturvallisuustehtävistä. 3 §:n mukaan Kyberturvallisuuskeskuksen tehtävänä on tukea,

ohjata ja valvoa tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä. Keskus ylläpitää kansallisen kyberturvallisuuden tilannekuvaa. Kyberturvallisuuskeskuksen toiminta edistää ja varmistaa tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuutta. (Laki Liikenne- ja viestintävirastosta 935/2018 § 1, § 3, § 5)

9.2 Rikoslaki

Tieto- ja viestintärikokset liitettiin osaksi rikoslain 38 lukua (lakimuutos 21.4.1995/578). Laki Tieto- ja viestintärikoksista (21.4.1995/578) käsittää seuraavat pykälät:

1	§	Salassapitorikos (21.4.1995/578)
2	§	Salassapitorikkomus (21.4.1995/578)
3	§	Viestintäsalaisuuden loukkaus (10.4.2015/368)
4	§	Törkeä viestintäsalaisuuden loukkaus (21.4.1995/578)
5	§	Tietoliikenteen häirintä (21.4.1995/578)
6	§	Törkeä tietoliikenteen häirintä (21.4.1995/578)
7	§	Lievä tietoliikenteen häirintä (21.4.1995/578)
7 a	§	Tietojärjestelmän häirintä (10.4.2015/368)
7 b	§	Törkeä tietojärjestelmän häirintä (10.4.4015/368)
8	§	Tietomurto (10.4.2015/368)
8 a	§	Törkeä tietomurto (10.4.2015/368)
8 b	§	Suojauksen purkujärjestelmärikos (7.11.2014/919)
9	§	Tietosuojarikos (5.12.2018/1051)
9 a	§	Identiteettivarkaus (10.4.2015/368)
10	§	Syyteoikeus (13.5.2011/441)
11	§	Menettämisseuraamus (10.4.2015/368)
12	§	Oikeushenkilön rangaistusvastuu (11.5.2007/540)
13	§	Määritelmät (10.4.2015/368)

(Laki Tieto- ja viestintärikoksista 21.4.1995/578)

Suomen Tietotoimisto STT (2020) kertoo, että Helsingin seudun kauppakamarin Yritysten rikosturvallisuus 2020 -selvityksestä selviää, kuinka yritysvakoilu ja tietoriskit ovat yleistyneet

yrityksissä. Rikosturvallisuusselvitykseen vastasi lähes 300 yritystä pääkaupunkiseudulta. Kaikista vastaajayrityksistä 17 prosenttia, suurista yrityksistä 31 prosenttia ja teollisuudesta 21 prosenttia arvioi, että niihin on kohdistunut yritysvakoilua ja tiedon urkkimista. Vuonna 2017 vain kahdeksan prosenttia vastaajista kertoi yrityksiinsä kohdistuneesta yritysvakoilusta tai tiedon urkkimisesta. Laiton kiinnostus yritysten tietoon on kolmessa vuodessa kaksinkertaistunut. Selvityksen mukaan tiedon digitaalisuus tuo mukanaan kyberuhkia etenevässä määrin. (STT, 2020)

10 VAATIMUS- JA SUOJAUSTASOT

Järvinen & Rousku (2017, ss. 31–32) kertovat, että Suomessa viranomaisten tietoturvallisuutta ja kaikkien henkilöiden tietosuojaa säädellään lainsäädännöllä. Etenkin henkilötietojen osalta EU:n tietosuoja-asetus toi uutta sääntelyä, josta tuli velvoittavaa toukokuussa 2018. Jos näitä rikotaan, seurauksena saattaa olla tutkintapyyntö ja oikeusprosessi.

He jatkavat, että valtionhallinto, muu julkishallinto ja myös yksityiset organisaatiot saattavat edellyttää osana palvelua tiettyjen tietoturvallisuuden vaatimusten täyttämistä. Ne ovat silloin osa sopimusta ja jos sopimusten mukaan ei toimita ja tapahtuu, saattaa organisaatio joutua maksamaan korvauksia tai sanktioita. Organisaatio, joka ei huolehdi tietoturvallisuudesta tai henkilötietojen käsittelystä, joutuu yleensä median eteen. Se puolestaan saattaa johtaa maineen ja luottamuksen heikentymiseen ja sitä kautta vaikuttaa merkittävästi yrityksen talouteen. Jos turvallisuus ja tiedon saatavuus pettää, organisaatio saattaa menettää käyttökatkon aikana rahaa maineen menetyksen lisäksi.

Järvinen & Rousku (2017, ss. 31–32) muistuttaa, että toteutettaessa tieto- ja kyberturvallisuus oikein, sen ei pitäisi vaikeuttaa, saati estää käyttäjän toimintaa. Sen tulisi sen sijaan tehostaa liiketoimintaa, nykyisen ja uuden teknologian käyttämistä. (Järvinen & Rousku, 2017, ss. 31–32)

Tieto- ja kyberturvaa ohjaavat tietyt vaatimukset, jotka riippuvat organisaation toimialasta, lainsäädännöstä, käsiteltävistä tiedoista ja asiakasvaatimuksista. Seuraavissa luvuissa tutustutaan Kansallinen turvallisuusauditointikriteeristö Katakriin, joka on viranomaisten auditointityökalu ja VAHTI:in, joka on Valtiovarainministeriön asettama Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä.

10.1 Katakri 2020

Kansallisen turvallisuusviranomainen NSA julkaisi Katakri 2020:n, eli viranomaisten tietoturvallisuuden auditointityökaluksi tarkoitetun kansallisen auditointikriteeristön 18. joulukuuta 2020 verkkoversiona, kertoo Ulkoministeriö (2020).

Katakri on viranomaisten tietoturvallisuuden auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa. Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset. Katakrin vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. (Ulkoministeriö, 2020)

10.1.1 Katakrin versiot

Ulkoministeriön (2020, s. 2) julkaisussa kerrotaan, että ensimmäinen Katakri valmistui vuonna 2009 osana hallituksen sisäisen turvallisuuden ohjelmaa. Katakri valmisteltiin puolustusministeriön johdolla viranomaisten ja elinkeinoelämän yhteistyössä. Tämän jälkeen vastuu Katakrin jatkohallinnoinnista ja päivityksestä siirrettiin sisäministeriölle, jonka koordinoimana Katakrin ensimmäinen päivitysversio valmistui vuonna 2011.

Elokuussa 2012 sisäministeriö asetti neuvoa antavan työryhmän, jonka esityksestä keskeiset ministeriöt päättivät tammikuussa 2014, että päävastuu Katakrin ylläpidosta ja hallinnoinnista siirtyy ulkoministeriössä toimivalle Kansalliselle turvallisuusviranomaiselle (NSA). Katakrin kolmas, vuonna 2015 julkaistu versio uudisti Katakrin rakenteen ja keskittyi turvallisuusluokitellun tiedon tietoturvallisuuteen.

Katakrin neljännen version päivitystyö ja hallinnointi on ollut NSA:n yhteistyöryhmän alatyöryhmäksi perustetun ohjausryhmän vastuulla. Ohjausryhmässä ovat olleet edustettuina toimivaltaisten viranomaistahojen lisäksi elinkeinoelämän edustajat. Katakri on osoittautunut toimivaksi työkaluksi, jolla on merkittävää arvoa myös Suomen maineelle tietoturvallisuuteen liittyvissä kysymyksissä sekä suomalaiselle yritysmaailmalle laajemminkin. Katakrin neljännen version päivitystyön taustalla keskeisimpänä tekijänä on ollut vastaaminen 2020 alusta uusiutuneen kansallisen lainsäädännön muutoksiin. Neljännessä versiossa on huomioitu myös

digitaalisen tietojenkäsittelyn kehitysaskeleita, sekä täydennetty työkalun tarkoituksenmukaiseen käyttöön liittyviä ohjeistuksia. (Ulkoministeriö, 2020, s. 2)

10.1.2 Katakrin osa-alueet

Ulkoministeriön (2020, s. 5) julkaisussa Katakri on jaettu kolmeen osa-alueeseen:

- Turvallisuusjohtamista koskevassa osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä sekä riittävät henkilöstöturvallisuuden menettelyt turvallisuusluokiteltujen tietojen suojaamiseen.
- Fyysistä turvallisuutta koskevassa osa-alueessa kuvataan turvallisuusluokiteltujen tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset.
- Teknistä tietoturvallisuutta koskevassa osa-alueessa kuvataan puolestaan tekniselle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset.

Vaatimukset mahdollistavat erilaisia toteutustapoja. (Ulkoministeriö, 2020 s. 5)

10.2 VAHTI

VAHTI on julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja keskeisten palveluiden tuottamisesta vastaavien organisaatioiden laajapohjainen yhteistyö-, valmistelu- ja koordinaatioelin, jonka toiminnasta vastaa Digi- ja väestötietovirasto. (DVV 2020)

VAHTI edistää julkisen hallinnon digitaalista turvallisuutta ja koordinoi palvelutuotannosta vastaavien organisaatioiden yhteistyötä. VAHTI raportoi toiminnastaan säännöllisesti valtiovarainministeriön asettamille ryhmille sekä muille keskeisille sidosryhmille, kuten Turvallisuuskomitealle. VAHTI käsittelee tiedonhallintalautakunnan antamia suosituksia. (DVV, 2020)

10.2.1 VAHTIn päätavoitteet

DVV (2020) kertoo, että VAHTIn päätavoitteita ovat julkisen hallinnon toiminnan ja ICT-palveluiden turvaaminen sekä uuden teknologian turvallisen käyttöönoton mahdollistaminen. Lisäksi tavoitteena on taata kansalaisten ja sidosryhmien luottamus julkiseen hallintoon sekä yhteistyön kehittäminen kansallisesti ja kansainvälisesti myös elinkeinoelämän kanssa.

10.3 Suojaustasot

Jotta tietoja voidaan käsitellä oikein, ne pitää luokitella organisaatiossa voimassa olevan luokituksen mukaisesti, ohjeistavat Järvinen & Rousku (2017, s. 46.) He jatkavat, että useimmissa valtionhallinnon organisaatioissa tämä on toteutunut vuonna 2010 voimaan tulleen tietoturvallisuusasetuksen (681/2010) mukaisesti. Asetuksen mukaan salassa pidettävä tieto luokitellaan neljään suojaustasoon (ST IV = matalin suojaustaso, ST I = korkein suojaustason, salaisin tieto).

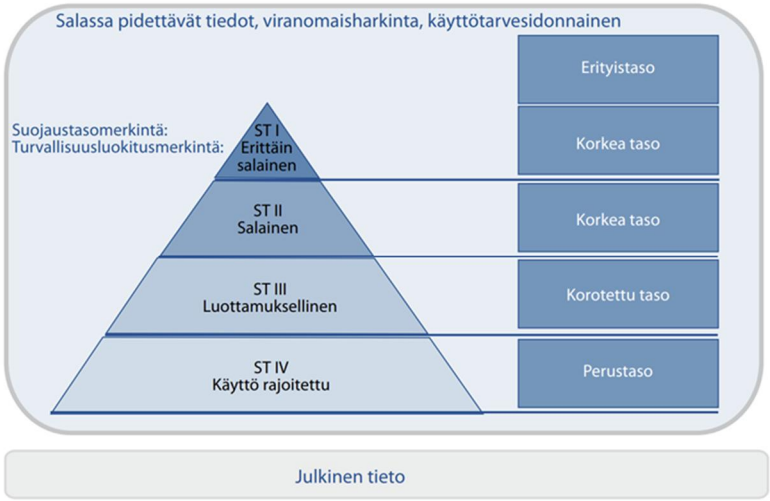
Valtiovarainministeriön (2012, s. 25) teknisen ICT-ympäristön tietoturvataso-ohjeen mukaan tietoaineistot tulee luokitella niiden tietosisällön mukaan. Tietoturvallisuusasetus ja VAHTI määrittelevät yksityiskohtaisella tasolla tietoaineistojen käsittelylle asetetut velvoitteet. Salassa pidettävän, harkinnanvaraisesti julkisen sekä käyttörajoitteisen tietoaineiston käsittelyä ohjataan suojaustasojen avulla tietoturvallisuusasetuksen pykälässä 9 osoitetulla tavalla.

Suojaustasot ovat:

- Suojaustaso I (ST I), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle.
- Suojaustaso II (ST II), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle.
- Suojaustaso III (ST III), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle.
- Suojaustaso IV (ST IV), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetuille yksityiselle tai yleiselle edulle tai, jos kysymys on tietoturvallisuusasetuksen 9 pykälän 2 momenteissa tarkoitetuista

asiakirjoista, jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä. (Valtiovarainministeriö, 2012, s. 25)

Valtiovarainministeriön (2012, s. 27) ohjeistuksen mukaan suojaustaso- tai turvallisuusluokitusmerkinnän omaavan tietoaineiston käsittely edellyttää suojattavalta kohteelta aina vähintään siltä vaaditun tietoturvatason täyttämistä. Tässä yhteydessä tulee huomata, että myös edellytettyä korkeampi tietoturvataso voidaan toteuttaa, jos sille on muita perusteita (esimerkiksi muut vaatimukset tai Yhteiskunnan turvallisuusstrategia). Tietoturvatasojen vaatimuksissa ei ole kuvattu erityistasoa, joka edellyttää korkean tason sekä suojattavan kohteen erityispiirteistä koostuvia lisäkontrolleja.
Kuvassa (2) on esitelty tietoaineiston käsittelyn hierarkia suojaustasoilla.



Kuva 2. Suojaustasot (Valtiovarainministeriö, 2012, s. 27).

Osaan salassa pidettävistä asiakirjoista voidaan tehdä turvallisuusluokittelua koskeva merkintä tietoturvallisuusasetuksen 11 pykälässä säädetyin edellytyksin.
Turvallisuusluokitusmerkintää on sallittua käyttää vain niissä tietoaineistoissa, joissa olevien tietojen oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtin turvallisuudelle, maanpuolustukselle tai muille yleisille eduille siten kuin tietoturvallisuusasetuksessa säädetään. (Valtiovarainministeriö, 2012, s. 25)

10.4 Standardit

Pöyhönen (2018, s. 1) kertoo Jyväskylän yliopiston informaatioteknologian tiedekunnan verkkojulkaisussa, että standardi tai normi on organisaation esittämä määritelmä siitä, miten jokin asia tulisi tehdä. Standardeja ja normeja käyttävät niin eri toimialojen laitevalmistajat ja palveluntarjoajat kuin julkisen sektorin toimijat ja tutkimuslaitokset, omista lähtökohdistaan ja globaalissa toimintaympäristössä toimiessaan. Siksi standardeja on vuosikymmenien saatossa kertynyt useisiin eri tarkoituksiin huomattava määrä.

Pöyhönen (2018, s. 1) raportoi, että merkittävimmät kansainväliset standardisoimisjärjestöt ovat yleinen kansainvälinen standardisointiorganisaatio ISO (International Organization for Standardization) ja sähkötekniikkaan ja elektroniikkaan erikoistunut IEC (International Electrotechnical Commission). Tietotekniikan alalla ISO ja IEC ovat muodostaneet yhteisen komitean alan standardien kehittämiseksi. Kansalliset standardointijärjestöt laativat kansallisia standardeja ja osallistuvat kansainvälisten standardien laadintaan. Suomen kansallinen toimija tällä alueella on Suomen standardisoimisliitto ry (SFS). (Pöyhönen, 2018, s. 1)

SFS toteaa standardien tarkoituksesta seuraavaa: Standardisointi on yhteisten toimintatapojen laatimista. Sen tarkoitus on helpottaa viranomaisten, elinkeinoelämän ja kuluttajien elämää. Standardisoinnilla lisätään tuotteiden yhteensopivuutta ja turvallisuutta, suojellaan kuluttajaa ja ympäristöä sekä helpotetaan kotimaista ja kansainväistä kauppaa. (Suomen Standardisoimisliitto SFS ry.)

10.4.1 ICS

Pöyhösen (2018, s. 4) mukaan ICS on lyhenne sanoista Industrial Control System, käännettynä teollisuuden automaatiojärjestelmä. ICS-alueen standardit ovat pääosin vapaasti saatavilla olevia yhdysvaltalaisia kansallisia standardeja tai suosituksia ja ovat siten käyttökelpoisia kehitettäessä muun muassa teollisuusautomaatiojärjestelmien kyberturvallisuuden hallintaa niiden elinkaaren eri vaiheissa. Seuraava taulukko (1) on osa julkaisua ja siitä ilmenee edellä mainitut standardit.

Information security publications by industry and country.			
Industry	Country	Publication	Paid or public
Cross-industry	International	ISO/IEC27000 Series	Paid
	United States	DoDDirective8500.1: Information Assurance	Public
		DoD Instruction8500.2: Information Assurance Implementation	Public
		DoD Instruction8510.01:DIACAP	Public
		FIPS 199	Public
		FIPS 200	Public
		NIST 800 Series	Public

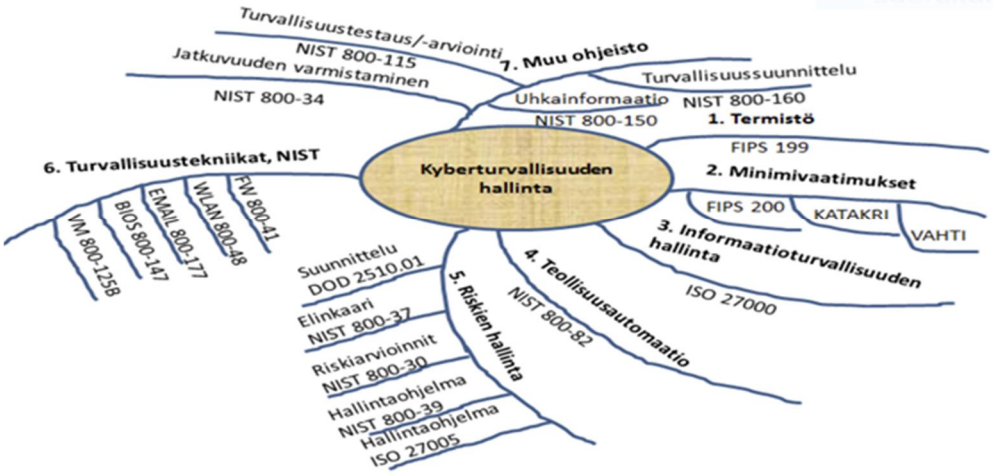
TAULUKKO 1. ICS-alueen standardeja (Knowles ym., 2015, 60)

Taulukko 1. ICS-alueen standardeja. (Pöyhönen, alun perin Knowles ym. 2018, s. 4)

Taulukossa esiintyvän ISO/IEC 27000-perheen tärkeimmiksi kotimaisten organisaatioiden kyberturvallisuuden hallinnan apuvälineiksi voidaan nähdä kuuluvan alastandardit, joissa kuvataan tietoturvallisuuden hallintajärjestelmän vaatimukset (27001:2005) ja riskienhallinnan toteutus (27005:2011). Lisäksi tärkeä alastandardi ICS:n osalta on ISO/IEC27019:2013, joka sisältää suhteellisen uudet ohjeet ja suositukset energia-alan sovellusten kyberturvallisuudesta. Edellä mainitussa julkaisussa on todettu ISO/IEC 27000-standardisarjan tietoturvallisuuden hallintaa koskevan menettelyohjeen ISO/IEC27002 olevan laajimmin käytetty standardi ICS-järjestelmien operoinnissa, vaikka tarjolla on myös ICS-specifisiä standardeja. (Pöyhönen, s. 4)

10.4.2 Ohjeet ja suositukset

Kuvassa (3) on esitetty taulukkoon (1) luetteloiduista standardista eräitä keskeisimpiä kyberturvallisuuden hallintaan liittyviä suosituksia, ohjeita ja standardeja, joiden avulla organisaatio voi kehittää ICS-toimintaympäristöönsä liittyviä hallinnollisia ja teknillisiä kykyjään toimintansa parantamiseksi kyberympäristöissä toimintaa varten. Lisäksi kuva sisältää merkittävimmät kansalliset Katakri- ja VAHTI-ohjeet.



Kuva 3. Kyberturvallisuuteen liittyvät standardit. (Pöyhönen, 2018, s. 2)

Ohjeet ja suositukset liittyvät yleensä toiminnan kehittämiseen. Kybermaailmassa ne avustavat käyttäjäänsä parantaen organisaation toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. Toiminnot saattavat olla esimerkiksi kyberturvallisuuden johtamisen ja hallinnoinnin tai teknillistä tietojärjestelmien, tietoverkkojen ja ICT-palvelujen kehittämistä, ylläpitoa tai käyttöä. (Pöyhönen, s. 2)

11 OMA TUTKIMUS JA TESTAUS

11.1 Case: Felix Solutions Oy

Tämä laadullinen tapaustutkimus pyrkii selvittämään case-yrityksen Felix Solutions Oy:n toiminnan kehittämistä. Tutkimuksessa keskitytään ensisijaisesti kyberturvallisuuden käyttöön liittyvien toimintojen kehittämiseen ja testaamiseen. Felix Solutions Oy on perustettu vuonna 2017, ja sen tietopalveluihin kuuluu mm. tietotekniikka, verkkopalvelut ja erilaiset konsultointipalvelut. Henkilöstöä yrityksessä on 2 ja yhtiömuoto on osakeyhtiö.

Tutkimuksen empiirisessä osuudessa tehdään konkreettisia havaintoja case-yrityksen kyberturvallisuudesta. Koska yritys on vain pieni pk-yritys, yrityksen johtajalla on kokonaisvastuu sen toiminnasta, kehittämisestä ja kehittämiskohteiden täytäntöönpanosta.

Tutkimuksen aikomus on selvittää ja testata yrityksen asiakkaiden kyberturvallisuuden kannalta tärkeät aukot ja tarvittaessa paikata ne niin, että asiakasyritys on kyberturvallisuuden suhteen täysin aukoton ja turvallinen. Tässä tutkimuksessa on käyty läpi Kyberturvallisuuskeskuksen oppaita, harjoituksia ja tehty erilaisia testejä.

11.2 Hack the Box

Storås (2020, s. 62) kertoo, että tietomurtoja voi opiskella laillisesti Hack the Box -alustalla. Hack the Box pelillistää tietomurrot ja hyökkäykset ja palvelua pääsee käyttämään vasta, kun osaa murtautua alustalle sisään. Alustalla on tarjolla useita erilaisia mahdollisuuksia testata ja kehittää omia hakkerointitaitoja. Aivan aloittelijoille Hack the box ei sovi, sillä koodaustaitoja tarvitaan sekä virtualisoitu linux-ympäristö. Hack the box:in voi ladata osoitteessa: https://www.hackthebox.eu/

11.2.1 Damn Vulnerable Web Application

Damn Vulnerable Web App, DVWA sisältää nimensä mukaisesti paljon haavoittuvuuksia. DVWA on haavoittuva verkkosovellus eri kyberturvakonseptien tutkimiseen ja suojaustyökalujen testaamiseen. Tämän sovelluksen pystyy lataamaan omalle

työasemalle.Sovelluksen päätavoitteena on auttaa tietoturva-ammattilaisia testaamaan taitojaan ja työkalujaan oikeudellisessa ympäristössä, auttamaan web-kehittäjiä ymmärtämään paremmin verkkosovellusten suojausprosesseja ja oppimaan verkkosovellusten turvallisuutta omassa ympäristössä. Lisätietoa löytyy osoitteesta https://dvwa.co.uk/ (pirun haavoittuva verkkosovellus, n.d.)

11.2.2 Muita sovelluksia

Johtavista pilvipalveluista, kuten esimerkiksi Amazon Web Services (AWS) ja Microsoft Azure saa myös ostaa valmiin alustan.

11.3 Skannaus

Saarelainen (2016, s. 19) kertoo, kuinka Tee se itse -tietoturvatarkistuksessa yrityksen it-ammattilainen ottaa hetkeksi päähänsä verkkorikollisen mustan hatun. Työkalut ovat pitkälti maksuttomia, eikä niiden käyttö vaadi gurun taitoja.
Hän jatkaa, kuinka verkon skannaus paljastaa, mitä laitteita verkkoon on kytkettynä. Skannausta motivoi usein halu saada varma kuva omista verkoista, niiden rakenteesta, sisältämistä järjestelmistä ja palvelimista. Verkkoskannauksen tyypilliset löydökset ovat päivittämättä jäänyt palvelin, työntekijän itse virittämä langaton tukiasema tai verkkoon päin avoin palvelu, jonka kuuluisi normaalisti olla kiinni.
Saarelainen (2016, ss. 19–20) on koonnut Tee se itse -skannaajan muistilistan:

1. Työkalut. Hanki ja opettele kunnolla kourallinen ohjelmia.
2. Valtuudet. Hanki valtuutus oman yrityksen johdolta. Pyydä lupa palvelimien ylläpidosta vastaavalta taholta, myös pilvipalvelulta. Jaa yhteystiedot avainhenkilöille.
3. Viesti. Kerro yrityksen sisäisesti, mitä tuleman pitää ja milloin. Muista myös palveluntarjoajat.
4. Luetteloi. Tee luettelo tiedossa olevista palvelimista ja jokaisen tarkoituksesta. Kirjaa myös tiedot palomuureista sekä verkkolaitteista.
5. Varmista. Skannauksen pitää kohdistua vain omiin verkkoihin ja palveluihin. Varmista oikeat asetukset.

6. Aja. Skannaa ensin verkkosi ulkoapäin. Tarkista sitten verkon segmenttejä sisäpuolelta työasemaverkosta.
7. Toimi. Käy läpi tulokset, pyri sulkemaan riskialttiit palvelut ja palvelimet, tee tarvittavat päivitykset.
8. Viestitä tuloksista. Keskustele löydöksistä.
9. Uusi tarkastukset säännöllisesti.

Saarelaisen (2016, s. 20) mukaan skannerit kuuluvat arkeen tietoturvan ammattilaisilla eli eettisillä tai valkohattuisilla hakkereilla. Hyökkääjät eli mustahatut käyttävät urkintaretkillään täysin samoja välineitä.

11.3.1 Rapid7

On olemassa maksullisia työkaluja, joita voi ladata myös ilmaiseksi. Rapid7:n ohjelmistot ovat arvostettuja ja samasta paikasta löytyy haavoittuvuus, hyökkäys- ja skriptikoodeja kuten Vulnerability & Exploit Database.

11.3.2 CISecurity ja OWASP

Skannauksissa ja testauksissa havaittuja haavoittuvuuksia ja tietoturvapoikkeamia voidaan ”tukkia” päivittämällä ohjelmistot uusimpiin versioihin ja koventamalla järjestelmä, jotta vastaavia tietoturva-aukkoja ei löydy. Skannauksissa ja kovennuksissa hyödynnettyjä palveluja ovat mm. CISecurity ja OWASP.

11.3.3 Palvelunestohyökkäys DDoS

Palvelunestohyökkäyksen eli DDoS:n pystyy kuka tahansa tekemään omalta kotitietokoneeltaan, tai ostamaan palveluna pimeästä verkosta, esimerkiksi Darknetin kautta bottiverkkoa hyödyntämällä. Myös yritykset myyvät palveluinaan palvelunestohyökkäyksiä. Palvelunestohyökkäyksiin on mahdollista rakentaa myös automaattiset suojausmekanismit, mm. Silverline tarjoaa suojausta.

DDoS voidaan tehdä esimerkiksi näin valmiilla skriptiohjelmalla:

DDoS Scripts: https://bit.ly/3l3CLCY

Low Orbit Ion Cannon: https://bit.ly/30oReSj

try to DDoS my website: http://ddos.networkchuck.com

Build Your Own Botnet: https://bit.ly/30tJm22

DdoS on helppoa, mutta pitää muistaa, että se on laitonta ilman lupaa.

12 JOHTOPÄÄTÖS JA KEHITYSEHDOTUKSET

Case-yritys Felix Solutions Oy:llä on hyvä mahdollisuus tarjota yrityksille kyberturvallisuuspalveluita ja siihen liittyvää konsultointia toteutusten muodossa. Tämä tarkoittaa käytännön palvelimien ja eri järjestelmien konfigurointia, erilaisia luvallisia hakkerointi- ja haavoittuvuustestauksia, auditointeja kuten esimerkiksi Red-Teaming, haavoittuvuusskannauksia ja palvelunestohyökkäyksiä eri menetelmillä ja välineillä, sekä asiakkaiden järjestelmiin soveltuvien estojärjestelmien kartoituksia ja käytännön asetuksia räätälöitynä.

Maailmalla vallitsevan koronatilanteen vuoksi yritysten henkilöstön siirtyessä etätöihin ja yritysten ja organisaatioiden tietojärjestelmien siirtyessä julkiseen nettiin, myös kyberriskit kasvavat. Kyberturvallisuus vaatiikin jatkuvaa IT-uutisten seuraamista, tiedon päivittämistä ja sosiaalisen median tarkkailua, kuten esimerkiksi Reddit, Twitter, Youtube vain muutama mainitakseni. Lisäksi erilaiset harrastajien ja ammattilaisten sivustot ovat hyödyllisiä informaation lähteitä. Kannattaa pysyä ajan hermolla mieluummin kuin odottaa passiivisesti jotain tapahtuvaksi.

12.1 Case-yrityksen kyberosaamisen nykytila

Case-yrityksen liiketoimintaan liittyen keskeisiä osaamisalueita ovat tietoturvan laatujärjestelmät, toiminnallisuus, laatu, testaus ja järjestelmäkehitys sekä eri teknologioiden hallittavuus ja tuotekehitys. Operointi ja ylläpito ja sitä kautta luottamuksellisuus, saatavuus ja turvallisuus ovat kyberturvallisuuden osaamista case-yrityksessä.

Kyberturvallisuutta voi parantaa kouluttamalla henkilöstöä tunnistamaan huijausyritykset. Yrityksen, tässä tapauksessa johtajan tuleekin huolehtia, että yrityksen henkilöstöllä on tarpeeksi kyberturvallisuus osaamista. Kybervalvonnan ulkoistaminen kannattaa, sillä usein asiakkaan oma valvonta on kallista ja vaatii korkeaa erityisosaamista. Kybervalvonta valvoo asiakasyrityksen kyberympäristöä ja turvallisuutta ja havainnoi tietoliikenneverkon tapahtumia sekä reagoi mahdollisiin kyberuhkiin. Sen tärkein ominaisuus on yritystä vastaan kohdistuneen kyberhyökkäysten havaitseminen. Kybervalvonta toteutuu useimmiten 24/7

periaatteella, joten asiakkaan tulisi olla valmiudessa jatkuvasti mahdollisten kyberhyökkäysten varalta.

12.2 Kehitysehdotukset

Kehitysehdotuksena Felix Solutions Oy voisi panostaa esimerkiksi SIEM-järjestelmien asennuksiin. SIEM tulee sanoista Security Information and Event Management, ja se tarkkailee yrityksen / organisaation tietojärjestelmiä ja tietoverkkoja sekä hälyttää havaitessaan poikkeavaa toimintaa. Myös GitHub-toiminnot, kuten bugien seurannat ja CVE-haavoittuvuustiedot olisi hyvä liittää osaksi yritystoimintaa. CVE-lyhenne tulee sanoista Common Vulnerabilities and Exposures joka tarkoittaa vapaasti käännettynä yleisiä haavoittuvuuksia ja paljastuneita tietoturvapuutteita.

Case-yritys Felix Solutions Oy pystyy auttamaan hyökkäysten torjunnassa ja toiminnoiden palautumisessa, joita hyökkäys on mahdollisesti jo pystynyt tuhoamaan tai anastamaan. Lisäksi pyrkimyksenä on kehittää asiakasyrityksen It-ympäristö turvallisemmaksi, jotta vastaavaa ei tapahtuisi jatkossa. Kun asiakas tuntee ympäristönsä ja tietää, mihin suojaus ja havainnointi halutaan kohdentaa, Felix Solutions Oy osaa rakentaa havainnointikykynsä riittävän kattavaksi ja kykenee erottamaan kyberhyökkäyksen normaalista toiminnasta ja reagoimaan hälytyksiin. Tulevaisuuden tarpeena voisi nähdä markkinoinnin lisäämisen ja case-yrityksen verkkosivujen päivittämisen, jota kautta yritys saa lisää asiakkaita. Kumppanuuksien solmiminen sekä kyber- ja tietoturvallisuus sertifikaattien suorittaminen on myös erittäin hyödyllistä tulevaisuutta ajatellen.

Jyväskylän yliopisto, Informaatioteknologian tiedekunta (2021) kiteyttää kyberturvallisuuden seuraavasti:
"Kybermaailman ymmärtäminen ja siihen liittyvien uhkien hallinta vaatii uudenlaista, monitieteistä osaamista."

Lähteet

Cyber Finland. (2021). *Hakkerointi.* Noudettu osoitteesta https://cyberfinland.fi/hakkerointi/

Damn Vulnerable Web App. (n.d.). *Pirun haavoittuva verkkosovellus.* Noudettu osoitteesta https://dvwa.co.uk/

DVV. (2020). *VAHTI.* Digi- ja väestötietovirasto. Noudettu osoitteesta https://dvv.fi/vahti

Elinkeinoelämän keskusliitto EK. (16.11.1016) *Viikon kysymys: Mitä on kyberturvallisuus?* Noudettu osoitteesta https://ek.fi/ajankohtaista/uutiset/viikon-kysymys-mita-on-kyberturvallisuus/

Hack The Box. (2021). *Massiivinen hakkerointipeli.* Noudettu osoitteesta https://www.hackthebox.eu/

Helsingin kaupunki. (2021). *Helsingin kaupungin Kehmet-ohjelma.* Noudettu osoitteesta https://kehmet.hel.fi/poikkileikkaavat-toiminnot/tietoturva-ja-tietosuoja/

Jordan, E. & Silcock, L. (2006). *Strateginen IT-riskien hallinta.* Edita Publishing Oy.

Jyväskylän yliopisto. (12.3.2021). *Informaatioteknologian tiedekunta.* IT-tiedekunta. Noudettu osoitteesta https://www.jyu.fi/it/fi/tiedekunta

Järvinen, P. (2010). *Yksityisyys, turvaa digitaalinen kotirauhasi*. Docendo Oy Jyväskylä.

Järvinen, P. (2018). *Kyberuhkia ja somesotaa*. Docendo Oy Jyväskylä.

Järvinen, P. & Rousku, K. (2017). *Työpaikan tietoturvaopas.* Talentum Media.

Kamensky, M. (2010). *Strateginen johtaminen, menestyksen timantti.* Talentum Media Oy.

Kellman, K. (12.7.2019). *Kyberasiantuntija: Esineiden internetin tietoturvasta ei ole juuri ole säätelyä – ongelmaan on herätty EU:ssa vasta viime vuosien aikana.* Noudettu osoitteesta https://yle.fi/uutiset/3-10874555

Konttinen, S. (24.3.2017). *Red team -hyökkäyksellä testaat yrityksesi tietoturvan.* Vieraskynä. https://blog.kauppalehti.fi/vieraskyna/f-secure-red-team-hyokkayksella-testaat-yrityksesi-tietoturvan

Koppa. (15.1.2014. -a). *Tutkimusstrategiat.* Jyväskylän yliopisto. Noudettu osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat

Koppa. (23.4.2015. -b). *Tapaustutkimus.* Jyväskylän yliopisto. Noudettu osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/tapaustutkimus

Koppa. (23.4.2015. -c). *Määrällinen tutkimus.* Jyväskylän yliopisto. Noudettu osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/maarallinen-tutkimus

Kyberturvallisuuskeskus. (2020). *Yrityksen hallituksen vastuu.* Noudettu osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Laaksonen, M., Nevasalo, T., Tomula, K. (2006). *Yrityksen tietoturvakäsikirja: Ohjeistus, toteutus ja lainsäädäntö.* Edita Publishing Oy. Helsinki.

Laki Liikenne- ja viestintävirastosta 935/2018. Noudettu osoitteesta https://finlex.fi/fi/laki/alkup/2018/20180935

Laki Tieto- ja viestintävirastosta 21.4.1995/578. Noudettu osoitteesta https://finlex.fi/fi/laki/ajantasa/1889/18890039001#L38

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J. & Salminen, M. (2018). *Kyberturvallisuuden strateginen johtaminen Suomessa.* Noudettu osoitteesta https://tietokayttoon.fi/documents/10616/6354562/282018Kyberturvallisuuden+strateginen+johtaminen..pdf/efea3c33-3c74-4cf6-b237-d49b4f10ab83?version=1.0

Leppänen, J. (2006). *Yritysturvallisuuskäytännössä, turvallisuusjohtamisen portfolio*. Talentum Media Oy.

Limnéll, J., Majewski, K. & Salminen, M. (2014). *Kyberturvallisuus*. Docendo. Jyväskylä.

Limnéll, J. & Iloniemi, J. (2018). Uhkakuvat. Docendo. Jyväskylä.

Logistiikan maailma. 2021. *Esineiden internet.* Noudettu osoitteesta https://www.logistiikanmaailma.fi/logistiikka/digitalisaatio/esineiden-internet/

Lönnqvist, I. & Moilanen, P. (2017). Kybersanasto. Teoksessa Jyväskylän yliopisto (toim.), *Kyberin taskutieto: keskeisin kybermaailmasta jokaiselle* (ss. 7–10). Jyväskylän yliopisto & Maanpuolustuskoulutusyhdistys. Noudettu osoitteesta https://jyx.jyu.fi/bitstream/handle/123456789/53510/978-951-39-7009-3.pdf

Metsämuuronen, J. (2002). *Tilastollisen kuvauksen perusteet. 2. painos.* International Methelp Ky.

Metsämuuronen, J. (2003). *Tutkimuksen tekemisen perusteet ihmistieteissä. 2.painos.* International Methelp Ky.

Metsämuuronen, J. (2008). *Laadullisen tutkimuksen perusteet. 3. painos*. International Methelp Ky.

Ollila, K. (2021). CIO: Kyberturva nousi johdon asialistalle. *Tivi, 2021(2),* 40–41.

Poliisi.fi. (2020). *Kyberrikokset.* Noudettu osoitteesta https://poliisi.fi/kyberrikokset

Puolustusministeriö. (2015). *KATAKRI – Kansallinen turvallisuusauditointikriteeristö*. Noudettu osoitteesta http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Pöyhönen, J. (55/2018). *Standardit, ohjeet ja suositukset osana teollisuusorganisaatioiden kyberturvallisuuden hallintaa : CIRP-raportti 2017.* 2. painos. Jyväskylän yliopisto. Informaatioteknologian tiedekunnan julkaisuja. Noudettu osoitteesta http://urn.fi/URN:NBN:fi:jyu-202005123149

Rousku, K. (2014). *Kyberturvaopas: tietoturvaa kotona ja työpaikalla.* Talentum Media. Viro.

Saarelainen, A. (2016). *Tietoturva.* Tivi, 2016(8), 19-20.

Storås, N. (2020). *Kuukauden sovellus.* Tivi, 2020(12), 62.

STT. (14.12.2020). *Yritysvakoilu ja tietoriskit yleistyneet yrityksissä.* Suomen Tietotoimisto. Noudettu osoitteesta https://www.sttinfo.fi/tiedote/yritysvakoilu-ja-tietoriskit yleistyneet-yrityksissa?publisherId=26487429&releaseId=69896372

Susi, M. (21.9.2015). *Onko yrityksesi joutunut inhimillisen hakkeroinnin kohteeksi?* Elinkeinoelämän keskusliitto. Noudettu osoitteesta https://ek.fi/ajankohtaista/uutiset/onko-yrityksesi-joutunut-inhimillisen-hakkeroinnin-kohteeksi/

Tampereen yliopisto. (n.d.). *Cyber Security.* Noudettu osoitteesta https://sec.cs.tut.fi/maso/materiaali.php?id=525

Teknologiateollisuus. (2020). *Digitaalinen turvallisuus yhä tärkeämpää.* Noudettu osoitteesta https://teknologiateollisuus.fi/fi/tyomarkkinat/yritysturvallisuus/digitaalinenturvallisuusyha-tarkeampaa

The Finnish Terminology Centre. (2018). *Tietotekniikan termitalkoot.* Noudettu osoitteesta http://www.tsk.fi/tsk/termitalkoot/en/node/267?page=get_id&id=ID0214&vocabulary_code=TSKTT

Ulkoministeriö. (18.12.2020). Katakri 2020. Tietoturvallisuuden auditointityökalu viranomaisille. Noudettu osoitteesta https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Valtionvarainministeriö. (2021). *Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivusto.* Noudettu osoitteesta https://www.vahtiohje.fi/web/guest/home

Wikipedia. (2019). *Kyberturvallisuuskeskus.* Noudettu osoitteesta https://fi.wikipedia.org/wiki/Kyberturvallisuuskeskus

KUVA

Logistiikan maailma. (2021). Esineiden maailma [kuva]. Noudettu osoitteesta https://www.logistiikanmaailma.fi/logistiikka/digitalisaatio/esineiden-internet/

Pöyhönen, J. (2018). Kyberturvallisuuteen liittyvät standardit [kuva]. Noudettu osoitteesta http://urn.fi/URN:NBN:fi:jyu-202005123149

Pöyhönen, J. (2018). ICS-alueen standardit. [taulukko]. Noudettu osoitteesta http://urn.fi/URN:NBN:fi:jyu-202005123149

Valtiovarainministeriö. (2021). Suojaustasot [kuva]. Noudettu osoitteesta https://www.vahtiohje.fi/web/guest/home