Erno Kattilakoski, Vili Pokela, Niko Tuikka

AUTOMAATIOVERKKOJEN TIETOTURVA

Tutkimus automaatioverkkojen mahdollisista tietoturvariskeistä

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutusohjelma / automaatio
Tammikuu 2020

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Tammikuu 2020	**Tekijä/tekijät** Erno Kattilakoski, Vili Pokela, Niko Tuikka
Koulutusohjelma Tieto- ja viestintätekniikan koulutusohjelma		
Työn nimi AUTOMAATIOVERKKOJEN TIETOTURVA		
Työn ohjaaja Hannu Ala-Pöntiö, Tom Tuunainen		**Sivumäärä** 50 + 3
Työelämäohjaaja Jukka Häkkilä		

Tämän opinnäytetyön tavoitteena on tutkia automaatioverkkojen tietoturvaa standardien näkökulmasta ja verrata näitä standardeja CABB Oy:n tietoturvajärjestelmään. Lisäksi tutkitaan, mitä erilaisia tietoturvauhkia ja tietoturvariskejä on olemassa niin Suomessa kuin maailmalla ja millaisia vaikutuksia niillä on tai voi olla.

Työhön kuuluu myös CABB Oy:n automaatioverkkoihin suoritettava skannaus, jonka avulla voidaan kartoittaa mahdollisia tunnettuja tietoturvariskejä ja verrata niitä F-Securen tietokantaan. Skannaus näyttää vertailun jälkeen suoritettavat toimenpiteet tietoturvariskien korjaamiseksi.

Opinnäytetyön tuloksena saatiin kattava tutkimus CABB Oy:lle sen tietoturvansa tasosta ja mahdollisista haavoittuvuuksista. Tutkimuksen tulokset ovat salaisia.

Asiasanat
Automaatioverkko, Standardi, Tietoturva, Tietoturvahyökkäys, Tietoturvauhka, Tietoturvastandardi, Palomuuri, Pääsynhallinta

ABSTRACT

Centria University of Applied Sciences	**Date** January 2020	**Author** Erno Kattilakoski, Vili Pokela, Niko Tuikka
Degree programme Bachelor of Engineering, Information and Communications Technology		
Name of thesis Security of automation networks		
Instructor Hannu Ala-Pöntiö, Tom Tuunainen		**Pages** 50 + 3
Supervisor Jukka Häkkilä		

The goal of this thesis is to examine the security of CABB Oy automation networks by comparing the security of their automation networks to the security standards made by IEC/ISO. In addition, this thesis includes examination of various security threats and risks that exist both in Finland and around the world and how these threats could affect a company.

This thesis also includes the scanning and mapping of potential security threats to CABB Oy: automation networks. The results of the scans are then compared to the F-Secure database of known threats. Afterwards the scan results show the measures to be taken to fix potential security threats.

As the result of this thesis we acquired a comprehensive analysis for CABB Oy about the level of their security and of potential vulnerabilities. The results of this research are classified information.

Key words
Access control, Automation network, Information security, Information security attack, Information security threat, Standard, Firewall

KÄSITTEIDEN MÄÄRITTELY

Backup	Varmuuskopio jostain tiedostosta
DoS	Palvelunestohyökkäys yhdeltä päätteeltä (Denial of Service)
DDoS	Palvelunestohyökkäys monelta eri päätteeltä (Distributed Denial of Service)
HAVARO	Tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä
IDS	Tunkeilijan havaitsemisjärjestelmä, joka tarkkailee tulevaa ja lähtevää liikennettä (Intrusion Detection System)
IEC	Kansainvälinen sähköalan standardointiorganisaatio (International Electrotechnical Commission)
IoT	Joukko erilaisia teknisiä laitteita, jotka kommunikoivat keskenään Internetin välityksellä (Internet of Things)
ISO	Kansainvälinen standardisoimisjärjestö (International Organization for Standardization)
I/O	Signaalien siirtäminen eri komponenttien välillä. Tulo/Lähtö (Input/output)
IP	Numerosarja, joka toimii laitteiden osoitteena ja joka huolehtii datan siirrosta ja yhteydestä toisiin laitteisiin. (Internet Protocol)
KNX	Standardoitu tietoliikenneprotokolla, jota käytetään rakennusautomaatiossa
LAN	Lähiverkko (Local Area Network)
Lon	Ohjausverkko (Local Operating Network)
Malware	Yleinen nimitys haittaohjelmalle
Mbus	Hajautettu järjestelmä, jossa usea keskusyksikkö on liitetty samaan väylään
ModBus	Sarjaliikenneprotokolla, joka mahdollistaa laitteiden välisen kommunikoinnin
NAT	Internet-tekniikka, jossa tehdään osoitemuunnos IP:lle
Palomuuri	Ohjelma tai laite, joka rajoittaa verkossa tapahtuvaa liikennettä ja estää tunkeutumiset
PIN-koodi	Tunnusluku, jota käytetään salasanana (Personal Identification Number)
Ransomware	Haittaohjelma, joka kiristää käyttäjää
Reititin	Eri verkkoja yhdistävä laite
Spyware	Haittaohjelma, joka vakoilee käyttäjää
VPN	virtuaalinen yksityisverkko (Virtual Private Network)
WLAN	Langaton lähiverkko (Wireless Local Area Network)

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

KUVIOT

KUVAT

1 JOHDANTO

1.1 Työn tavoitteet

Tämän opinnäytetyön tavoitteena on tutkia automaatioverkkojen tietoturvaa standardien näkökulmasta ja verrata näitä standardeja CABB Oy:n tietoturvajärjestelmään. Lisäksi työhön kuuluu myös CABB Oy:n automaatioverkkoihin suoritettava skannaus, jonka avulla voidaan kartoittaa mahdollisia tunnettuja tietoturvariskejä. Skannaus näyttää myös suoritettavat toimenpiteet tietoturvariskin korjaamiseksi. Tulokset vertailusta standardeihin ja verkkojen skannauksesta kuuluvat opinnäytetyön salaiseen osaan, joka luovutetaan CABB Oy:lle.

1.2 Yleistä

Teknologian nopean kehityksen myötä tietoturvasta on tullut suuri huolenaihe nykypäivän yrityksille, ja ihan syystäkin. Tietoturvahyökkäyksiä tapahtuu maailmalla lähes päivittäin, ja uusia tapoja tietoturvahyökkäyksille ja tietojenkalasteluille syntyy samaan tahtiin kuin keinoja, jolla voidaan puolustautua niitä vastaan. Nykypäivänä IT-verkkojen tietoturva on paljon automaatioverkkojen tietoturvaa edellä, ja siksi tämä aihe on tällä hetkellä hyvinkin ajankohtainen. Tietojenkalastelu ja tietoturvahyökkäyksien tekeminen ja suunnittelu ovat nykyään ihan ammattirikollisuuden tasolla. Kalasteltu tieto tai tietoturvahyökkäyksen vahingot saattavat aiheuttaa pahimmillaan yritykselle jopa miljoonien vahingot. Pahimmassa tapauksessa saattaa aiheutua jopa henkilövahinkoja. Tämän vuoksi on todella tärkeää, että automaatioverkkojen tietoturvaan panostetaan ja tutkitaan keinoja parantaa tietoturvaa. (Laaksonen 2006, 15–16.)

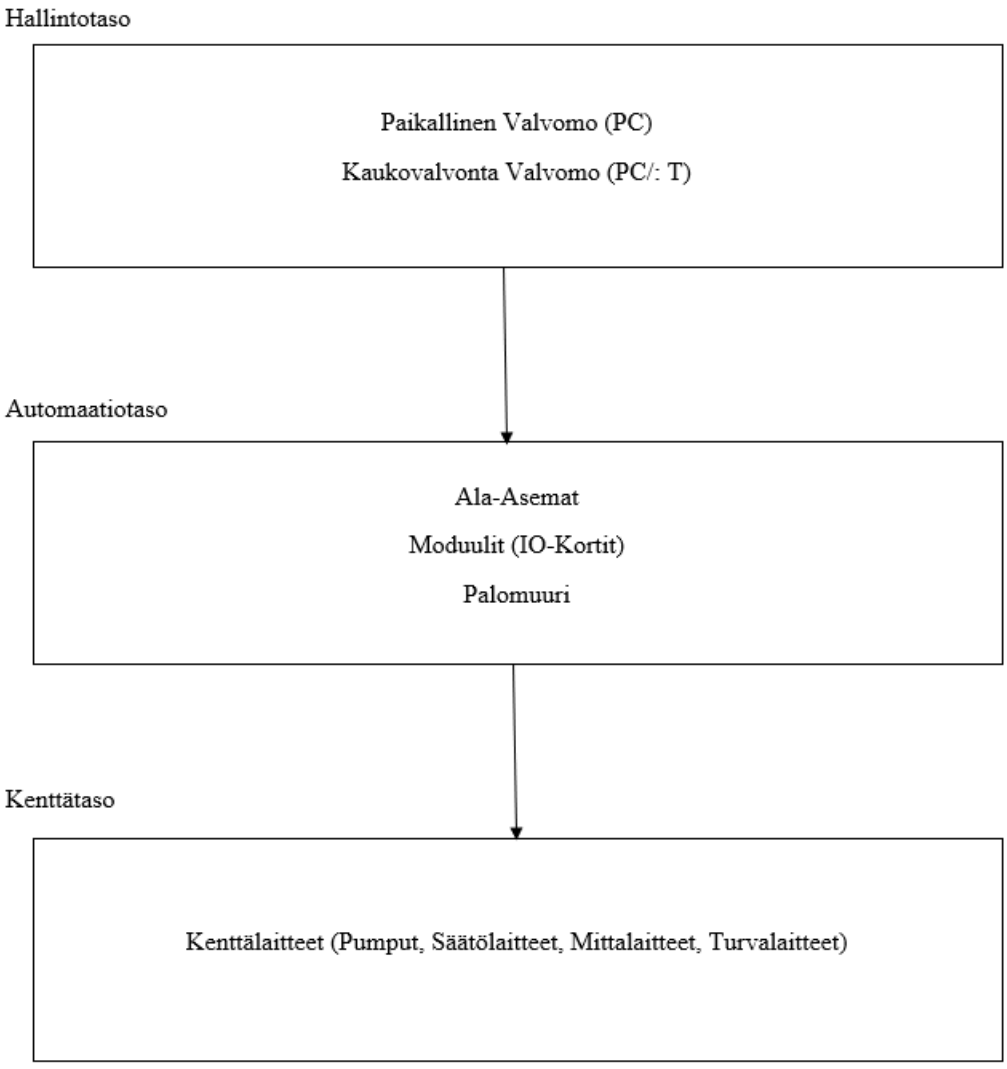
Tässä opinnäytetyössä tutkitaan automaatioverkkojen tietoturvan rakennetta, automaatioverkkojen tietoturvaa standardien näkökulmasta ja tutkitaan erilaisia tietoturvahyökkäyksiä ja tapoja, joilla voidaan hyökätä järjestelmään ja kalastella salaista tietoa. Lisäksi opinnäytetyöhön kuuluu myös tietoturvaskannaus, joka toteutetaan CABB Oy:n automaatioverkkoihin. Tämän skannauksen avulla voidaan etsiä mahdollisia tietoturvauhkia, joita verkoissa esiintyy. Skannaus näyttää myös tapoja, joilla tietoturvariski saadaan eliminoitua. Verrataan myös CABB Oy:n tietoturvajärjestelmää standardien määrittelemään järjestelmään ja tutkitaan, onko sen tietoturvajärjestelmänsä standardien mukainen ja löytyykö siitä mahdollisesti jotain kehittämiskohteita tai kehittämisalueita.

1.3 CABB Oy

CABB Oy on maailmanlaajuinen yritys, joka toimii kemian alalla ja on johtava valmistaja kasvinsuojeluaineteollisuudessa. Yrityksen asiakkaina on maailman johtavia kemianalan yrityksiä. CABB Oy:llä on viisi tuotantopaikkaa neljässä eri maassa, ja ne työllistävät noin 1 000 työntekijää. Nämä tuotantopaikat sijaitsevat Suomessa, Sveitsissä, Yhdysvalloissa ja kaksi Saksassa. Hienokemikaalituotanto alkoi Kokkolassa vuonna 1984 Kemiran nimellä. Vuonna 2011 KemFine myytiin CABB AG:lle. CABB AG:n tuotantonsa on sopimusvalmistusta. Kokkolan tehtaalla valmistetaan kasvinsuojeluaineita ja niiden välituotteita. Lisäksi he valmistavat lääkeaineiden välituotteita, joista heidän asiakkaansa valmistavat varsinaisia lääkkeiden vaikuttavia aineita, ja niistä taas valmistetaan lääkevalmisteita. CABB Oy työllistää Kokkolan tehtaallaan noin 200 henkilöä.
(CABB Oy. 2020.)

2 AUTOMAATIOVERKKOJEN RAKENNE

Automaatioverkon rakenne koostuu yleensä kolmesta erilaisesta tasosta, jotka ovat hallintotaso, automaatiotaso ja kenttätaso. Automaatiotasoja ja kenttätasoja voi olla myös monta. Näillä tasoilla on omat merkityksensä rakenteessa, ja ne kommunikoivat keskenään toimiakseen oikein. (KUVIO 1.)



KUVIO 1. Automaatioverkon rakenne (mukaillen Piikkilä 2011, 67)

Hallintataso pitää sisällään valvomot, paikalliset valvomot ja etävalvomot. Hallintataso on yhteys käyttäjän ja järjestelmän välillä, ja sitä ohjataan yleensä valvomosta käsin tietokoneelta. Yleensä yhteys toimii järjestelmän lähiverkossa (LAN), mutta monesti myös internetin välityksellä käyttäen TCP-IP protokollaa. Etäkäyttö on myös mahdollista, mutta siihen sisältyy erilaisia tietoturvariskejä. Valvomoon tulee perustiedot järjestelmän tiedoista, ja sieltä käsin tehdään järjestelmän käyttötoimenpiteitä, ja jos prosessissa tapahtuu virheitä tai on häiriöitä, siitä tulee hälytys valvomoon. Valvomosta seurataan prosessin kulkua ja raportoidaan tapahtumia.

Automaatiotaso koostuu alakeskuksien laitteista. Sinne kuuluu erilaiset säätimet, ohjainyksiköt ja niihin yhdistettävät I/O-moduulit, ja se voi myös sisältää kiinteän I/O-pistemäärän yksikön. Alakeskus sisältää ohjelmat prosessien ohjauksiin I/O-pisteiden välillä, ja ohjaukseen näiden välillä on yleensä käytetty lähiverkkoa. Yleensä automaatiotasolla on myös palomuuri, jonka läpi kaikki tietoliikenne kulkee.

Kenttätaso sisältää erilaisia antureita ja toimilaitteita, jotka mittaavat prosessissa tapahtuvia asioita, kuten sen tilaa ja olosuhteita. Eri olosuhteita, joita mitataan, ovat yleensä lämpötila, paine-ero, tilavuus ja monet pitoisuudet. Lisäksi mittauksien perusteella säädellään prosessia valvomosta käsin toimilaitteiden avulla. Kommunikaatioon eri laitteiden välillä käytetään yleensä jännite- tai virtaviestintää. Yleisimpiä käytettäviä kenttäväylästandardeja automaatiossa ovat ModBus, Lon, KNX ja Mbus. Siinä käytetään myös monesti langattomia yhteyksiä WLAN ja Bluetooth. (ST-Käsikirja 17. 2012, 93.)

2.1 I/O-pisteet

Tärkeä osa automaatiojärjestelmää ovat input/output-pisteet, eli I/O-pisteet. Ne yleensä sijaitsevat automaatiotason ala-asemien I/O-moduuleilla. Kenttätason laitteet yhdistetään ala-asemien I/O-moduuleiden I/O-liittimille. Automaatiojärjestelmän suuruus ilmaistaan yleensä pistemäärällä, joilla tarkoitetaan fyysisiä pisteteitä (DI/DO/AI/AO) ja niiden kokonaismäärää. Pisteet voivat olla myös tehtyjä, eli ohjelmallisia. Silloin pisteellä ei ole omaa fyysistä liityntää ala-asemalla. Hyviä esimerkkejä tällaisista ovat esimerkiksi kirjautumistiedot, joita lasketaan indikointipisteiden avulla, tai kenttäväylän välityksellä siirrettävät tiedot. (Contec. 2020. Digital I/O Basic Knowledge.)

Digital input eli DI-pisteet, ne ovat fyysisiä sisääntuloja, joilla on ainoastaan kaksi eri tilaa (0 tai 1). Näitä asentoja sanotaan NO (normal open) tai NC (normal close) tiloiksi. Tila määrittyy sen mukaan,

onko kosketin kiinni- vai aukiasennossa. Asentotietoa sanotaan yleensä kärkitiedoksi kaksiasentoisuuden ja kosketintekniikan takia. DI-sisääntuloon ei tule omaa ulkoista jännitettä. Sen takia sieltä voidaan syöttää pienoisjännitettä, muun muassa 24V tasajännitettä, ja tällöin voidaan mitata, onko ”kärki” avoin vai suljettu. DI-pisteitä käytetään indikointitietojen tuomiseksi järjestelmään. Näihin pisteisiin voidaan myös tuoda hälytykset, esimerkiksi hätäpysäytykset ja impulssien sisääntulot ja eri mittarien tiedot. DI-pisteiden tila eri käyttötarkoituksien mukaan voi olla muun muassa päällä/pois, kiinni/auki, hälytys/normaali tai käy/seis. (Contec. 2020. Digital I/O Basic Knowledge.)

Digital output eli DO-pisteillä, on vain kaksi eri tilaa 0/1. Ne ovat niin kuin DI-pisteet paitsi ulostuloja. Digital output käyttää nimityksiä NO/NC, riippuen siitä onko sen ohjaus tavallisesti auki vai kiinni. Näitä pisteitä käytetään muun muassa, kun halutaan ohjata pumppuja, puhaltimia, valaistusta tai muuta käyntilupaan ja päälle. Riippuen järjestelmistä niitä voidaan ohjata pienois- tai verkkojännitteellä. Kun ohjataan verkkojännitteellä, voidaan viedä vain ohjauksen vaativa virta. (Contec. 2020. Digital I/O Basic Knowledge.)

Analog input -pisteet (AI-pisteet) ovat analogisia sisääntuloja, joita hyödynnetään mittauksissa. AI-pisteet käyttävät usein vastusmittauksia tai virta- ja jännitemittauksia sisääntuloissa. Ne käyttävät yleensä sisääntuloviestinä yleensä 0–10 V tai 0–20 mA viestiä. Mittauksien luotettavuus riippuu käytetyn laitteen mittapisteen ja anturin biteistä, ylinen käytettävän bittimäärä on vähintään 16 bittiä. (Contec. 2020. Analog I/O Basic Knowledge.)

Analog output (AO-pisteet) ovat analogisia ulostuloja. Ne kuljettavat säätöviestejä toimilaitteiden välillä. Ne ovat myös moniasentoisia kuten AI-pisteet, ja ne käyttävät myös samoja jännite- ja virtaviestejä kuin ne, mutta bittimäärä tulee olla vähintään 8 bittiä. Esimerkiksi pumput ja venttiilit käyttävät AO-pisteitä viemään viestiä, joilla ne ajetaan auki- tai kiinniasentoon. (Contec. 2020. Analog I/O Basic Knowledge.)

2.2 Palomuuri

Palomuuri on oleellinen osa tietoturvan kannalta. Sen tarkoituksena on rajoittaa verkossa tapahtuvaa liikennettä ja estää mahdolliset verkkoon tunkeutumiset ja hallita verkosta lähtevään liikennettä. Kaikki

lähtevä ja saapua liikenne tapahtuu palomuurin kautta, ja se on ensimmäinen laite, joka käsittelee tapahtuvaa liikennettä. Palomuuria pystyy myös itse säätelemään. Voidaan suodattaa yhteyksiä siten, että saadaan käyttöön vain tarvittavat yhteydet. (Laaksonen 2006, 186–188.)

Palomuureja on olemassa erilaisia. Laitepohjaisia palomuureja sekä ohjelmallisia. Laitepohjaiset palomuurit ovat erilisiä palomuureja, jotka ovat omia laitteita, ja ne tulevat laitteiden väliin. Myös monissa reitittimissä on sisäänrakennettu palomuuri. Laitepohjaisia palomuureja kehittää esimerkiksi Palo Alto Networks -yhtiö, jonka palomuureja käytetään esimerkiksi suurissa toimistoissa tai keskisuurissa yrityksissä (Paloguard.com 2020.) Ohjelmallinen palomuuri on tietokoneessa itsessään. Esimerkiksi nykyisissä Windows-tietokoneissa on valmiina olemassa Windows Defender, jossa on palomuuri. (Laaksonen 2006, 186–188.)

Ohjelmistopalomuurit ovat yleensä yksinkertaisia käyttää, ja niissä on valmiina jo palomuurit käytössä, joten niille ei tarvitse tehdä itse mitään ja niissä on virustorjunta samassa. Yleisimpiä tunnettuja palomuureja ovat Avast, F-Secure ja Norton. Laitepalomuurit ovat yleensä valmiina jo reitittimissä, mutta asetukset ovat hyvin suppeat ja ne olisi hyvä konfiguroida kunnolla, jos haluaa turvallisen yhteyden normaalissa yksityisessä käytössä se ei ole niin välttämätöntä, mutta yrityksien yksityisyyden suojaamiseksi se voi olla hyvinkin tärkeää. (Laaksonen 2006, 186–188.)

PA-3020 on Palo Alto Networksin valmistama PA-3000 -sarjan rautapalomuuri. PA-3000 -sarja pitää sisällään kolme erisuuruisen suorituskyvyn palomuuria. PA-3020 on tämän sarjan perusmalli. PA-sarja on suunniteltu nopean internet-yhteyden käyttöön. Ne hallitsevat verkoissa tapahtuvaa liikennettä käyttämällä erillistä prosessointia ja muistia hallitsemaan verkkoa, tietoturvaa ja uhkien torjuntaa ja hallintaa. Se käyttää PAN-OS -käyttöjärjestelmää, joka on tarkoitettu tietoturvallisuuteen. Se järjestelee luonnollisesti liikkuvan liikenteen, sovellukset, uhat ja sisällön. Käyttäjä voi itse ohjelmoida laiteresurssit ja määrittelemään kaikki tietoturvaan liittyvät toimenpiteet. Käyttäjä pystyy itse App-ID -sovelluksella hallitsemaan portteja ja sovelluksia. Sovelluksen kautta voidaan hallita myös lähtevää liikennettä, voidaan sallia tai estää liikennettä ja vaikka tarkastaa, onko tuleva liikenne turvallista. Voidaan estää tunnettuja ja tuntemattomia uhkia, ja haittaohjelmia ja vakoiluohjelmia. (Paloguard. 2020.)

2.3 Tietoliikennelaitteisto

Automaatioverkko pitää sisällään paljon erilaisia teknisiä laitteita, reitittimiä, palvelimia, tietokoneita, kytkimiä ja muita. Yhdessä näistä laitteista koostuu kattava automaatioverkosto.

Reititin on verkkolaite, joka yhdistää laitteet toisiinsa. Se on myös ensimmäinen laite, joka estää verkkoon tunkeutumista. Sen tehtävänä on välittää tarvittavaa tietoa verkon eri laitteiden välillä. Reititin on yleensä vähintään kahden verkon välissä, ja sen pitää tietää, miten verkot ovat toisiinsa yhteydessä, jotta se voi tehdä tietoliikenteelle oikean valinnan. Sen tarkoituksena on valita nopein reitti, jotta yhteys olisi mahdollisimman nopea suuntaan ja toiseen. Tähän vaikuttavat reitinpituus, reitittimen nopeus ja reitille annetut säännöt. (Mitchell. 2020.)

Palvelin on eräänlainen tietokone, jonka tarkoituksena on käsitellä pyyntöjä ja toimittaa tietoja laitteiden välillä. Se välittää käskyt ja tiedot internetin tai VLAN:in kautta koneelta toiselle. Palvelimia on useita erilaisia. Automaatioverkossa monesti on käytössä niin sanottuja datakeskuksia, jotka koostuvat useista palvelimista. Datakeskus voi sisältää tuhansia erilisiä palvelimia, jotka sitten käsittelevät eri tietoja ja pyyntöjä. Kyseiset keskukset keräävät paljon lämpöä, kun monta laitetta on samassa tilassa, joten niiden jäähdytyksen pitää olla kunnossa, että laitteet eivät ylikuumene. (Fisher. 2020.)

2.4 Automaatioverkkojen tietoturvallisuus

Yleinen tietoturvallisuus yleensä pitää sisällään tietoturvapolitiikkaa, riskianalyysejä, tietoturvallisuustavoitteita, erilaisia tietoturvan osa-alueita, uhkia ja suojautumismenetelmiä. Tietoturvapolitiikka pitää sisällään perustan turvallisuuden kehittämiselle. Tietoturvapolitiikka selostaa yleisen käsitteen mikä on suojauksen tarkoitus? Mikä on yrityksessä yleisesti noudatettava suojaustaso? Kenen vastuulla on ylläpito? Yleinen tietoturvapolitiikka auttaa muodostamaan yksityiskohtaisia teknisiä ohjeita. (Tuunainen. 2019, 2–25.)

Riskianalyysit auttavat kohdistamaan toimenpiteet oikein erilaisilla menetelmillä. Ensimmäiseksi kerätään mahdolliset riskit, sen jälkeen tehdään riskien yksityiskohtainen analyysi ja tehdään suunnitelma ja toimenpiteet riskien ehkäisemiseksi. Tietoturvallisuustavoitteiden tavoitteen on varmistaa tietojen luottamuksellisuus, eheys, käytettävyys, käyttäjän tunnistaminen ja käyttäjän valtuuttaminen. (Tuunainen. 2019, 2–25.)

Tietoturvallisuus pitää sisällään eri osa-alueita hallinnollinen osa-alue sisältää tietoturvallisuuspolitiikkaa, riskianalyysiä, tietoturvaluokituksia ja ylläpitokäytänteitä. Tavoitteena tällä on luoda perusta toimivalle tietoturvallisuudelle. Fyysinen osa-alue sisältää kulunvalvontaa ja tilojen suojausta, joka sisältää henkilöstön kolutusta turvalliseen suojaukseen. Tällä varmistetaan asianmukainen laitteiden suojaus. Tekniselle osa-alueelle hommataan luotettavat käyttöjärjestelmät ja sovellukset. Varmistetaan, että tietoliikenne on kunnossa. Näin saadaan varmistettua luotettava tekniikan toiminta. (Tuunainen. 2019, 2–25.)

Salakuuntelu on yksi yleinen uhka, ja sitä vastaan usein suojaudutaan käyttämällä salausta ja kertakäyttösalasanoja. Tietojen tuhoaminen on myös yksi uhka ja tämän vuoksi yleensä säilytetään varmuuskopioita tärkeistä tiedostoista. Monesti koitetaan kalastella tietoja toisena esiintymällä ja tämän takia yleensä käyttäjän joudutaan tunnistamaan jollakin toisella tapaa, esimerkiksi sormenjäljellä tai PIN-koodilla. Tietomurrot ovat myös yleisiä, ja niiltä suojaudutaan palomuureilla ja tiedostojen salakirjoituksella. Yleisimmät suojautumismenetelmät ovat, virustorjunta, turvallisuustiedotteet, tietoturva-ajattelu ja varmuuskopiointi. On hyvä muistaa tarkistaa, että varmuuskopiot toimivat. Yleisin tietoturvallisuusaukko johtuu ohjelmavirheestä, käyttäjän huolimattomuudesta tai suunnittelussa tapahtuneesta virheestä. (Tuunainen. 2019, 2–25.)

2.4.1 Käyttöturvallisuus

Tarkoituksena on löytää turvalliset ja suojatut laitteet turvalliseen käyttöön, ja hankkia suojatut yhteydet laitteiden välille ja palomuurit. Reititin on tärkeä osa lähiverkkoa. Se liittää lähiverkon runkoverkkoon ja välittää IP-paketin seuraavaan reitittimeen, sen IP-osoitteen perusteella. Reitittimen käyttöturvallisuudessa on otettava huomioon muutamia suojausasioita: etäkäyttöä varten oletussalasanat tulisi vaihtaa, porttien IP-osoitteita ei tulisi käyttää kuin pelkästään liikenteen välittämiseen, reitittimen tarpeettomat protokollat tulisi poistaa käytöstä. (Tuunainen 2019, 2–11.)

Palomuuri on iso-osa suojausta. Se on ohjelmallisesti tai laitteellisesti toteutettu järjestelmä. Se rajoittaa tulevaa ja lähtevää liikennettä suodatuslistoihin perustuen. Palomuuri päästää läpi liikennettä pääsylistoihin perustuen. Palomuuri sallii itselleen osoitetun liikenteen luotettavista IP-osoitteista ja sallii omasta verkosta käynnistetyn istunnon liikenteen. Se myös estää liikenteen verkossa, jos se on tulossa kielletystä

osoitteesta, julkisesta verkosta tai tuntemattomasta IP-osoitteesta. Palomuuri ei kuitenkaan suojaa sallittuja palveluja, jos modeemit on yhdistetty toisiinsa ja palomuuri ei ole niiden välissä. Se ei myöskään estä haittaohjelmien siirtymistä, jos se esimerkiksi tulee sallitusta osoitteesta. Melkein jokaisesta palomuurista löytyy jokin ohjelmiston tietoturva-aukko. (Tuunainen 2019, 2–11.)

On olemassa myös muita ohjelmia järjestelmän suojaamiseksi. VPN eli virtual private network, se on virtuaalinen erillisverkko, joka siis muodostaa yksityisen verkon, joka voidaan yhdistää julkiseen verkkoon ilman että omaa todellista IP-osoitetta käytetään tai sijaintia saadaan selville. NAT eli network address translation, eristää oman sisäverkon osoitteet internetin julkisista osoitteista. Se muuttaa sisäverkon oman osoitteen julkiseksi yhdistyessä internettiin. IDS eli intrusion detection system on eräänlainen tunkeilijan havaitsemisjärjestelmä. Se tarkkailee tulevaa ja lähtevää liikennettä, havaitsee tunkeutumisyritykset ja muuttaa suojausasetuksia, ja se toimii tarkkailtavan lähiverkon rinnalla. (Tuunainen 2019, 2–11.)

2.4.2 Päätelaitteiden suojaus

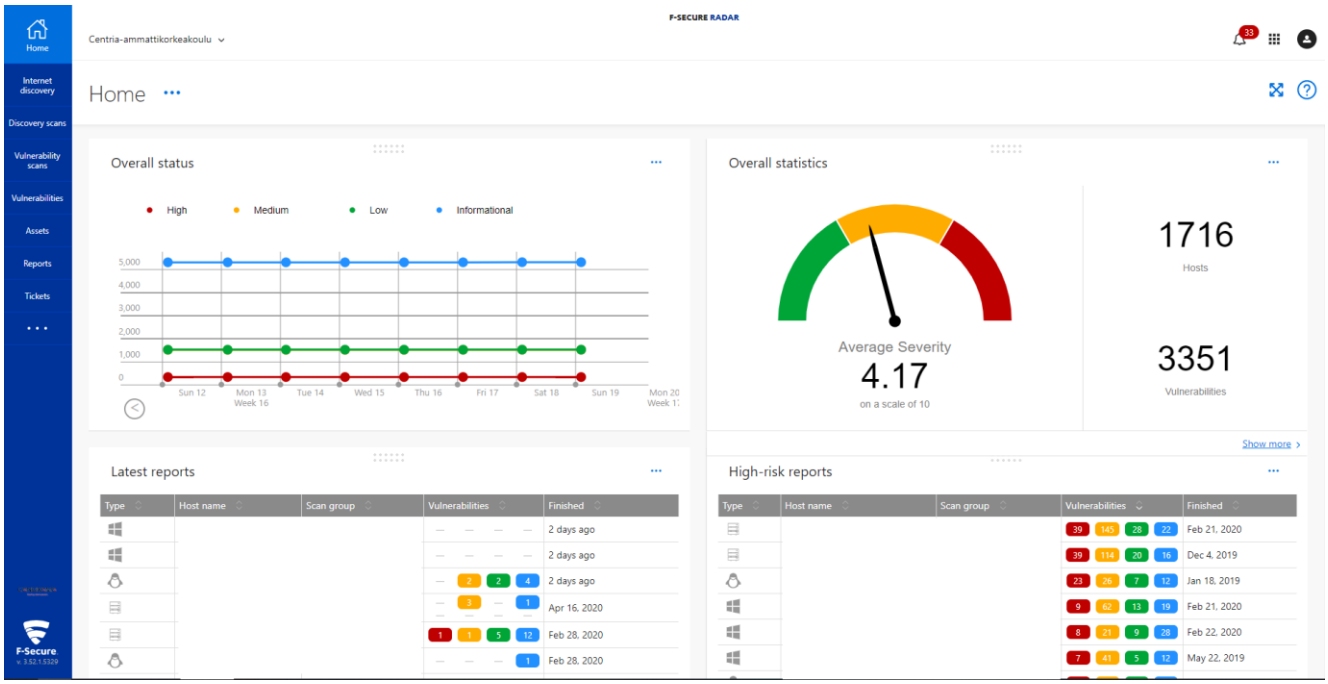
Päälaitteiden tietoturvassa turvaominaisuuksien tehtävä on eristää ohjelmat ja niiden toimiminen keskenään, ja eriyttää ohjelmien käsittelemät tiedot toisistaan. Turvaominaisuudet rajoittavat käyttäjien toimia sen mukaan minkälaiset valtuudet heillä on ja salaavat tallennetut tiedot. Palomuurin ja virustorjunnan tehtäviin kuuluu havaita ja estää haittaohjelmien toiminta ja estää väärinkäyttö ja tietojen oikeudeton käyttö. Työantajalla on mahdollisuus rajoittaa käyttäjien toimia ja rajoittaa käytössä olevien järjestelmien ja laitteiden määrää. Uusien ja päivitettyjen päätelaitteiden ja palvelujen käyttöönottoon liittyvät riskit on mahdollista kartoittaa ja sitä myötä ennaltaehkäistä.
(Tuunainen 2019, 2–8.)

Päälaitteille tallentuu yleensä tärkeitä tietoja. Päälaitteelle tallentuu käyttäjien itse tallentamat tai siirtämät tiedot, väliaikatiedot, varmuuskopiot ja muut prosessiin liittyvät asiat. Siellä on myös sovelluksien ja järjestelmien tallentavat tiedot, käyttäjien kirjautumisen mahdollistavat tiedot, päälaitteiden ja sen selaimen ominaisuuksien tunniste- ja sijaintitiedot, päätelaitteen ja sen sovellusten pää asetustiedot ja sovellusten päätelaitteelle ja sovelluksiin tallennettavat tiedot.
(Tuunainen 2019, 2–8.)

Mahdollisia hyökkäyksiä ja turvallisuusriskejä voi tapahtua käyttäjän virheestä tai sitten hyökkäyksen kohteeksi johtuneesta. Käyttäjäkohtaisia riskejä voi olla, että käyttäjä vahingossa asentaa jonkin ohjelman, joka sitten sisältää haittaohjelman, tai kytkee järjestelmään toisen laitteen, jossa ei suojausta ole. (Tuunainen 2019, 2–8.)

2.4.3 F-Secure Radar

F-Secure Radar on yrityksille ja miksi ei myös yksityisille tarkoitettu skannausohjelma (KUVA 1), jonka tarkoituksena on löytää tietokoneestasi tai verkostasi haavoittuvuuksia. Sillä pystyy tunnistamaan ja hallitsemaan sisäisiä ja ulkoisia tietoturvauhkia. Käyttäjä saa raportit mahdollisista riskeistä ja näin pystytään varmistamaan se, että yrityksen tietoturva on säädösten mukaiset. Se pystyy skannaamaan koko lähiverkon, jolloin se näkee myös katvealueet ja niissä piilevät mahdolliset haavoittuvuudet ja uhat, jotka voivat olla heikkoja hyökkäyksille. (F-Secure.com. 2019.)



KUVA 1. F-Secure Radar kotinäkymä

Radar-ohjelma sisältää monia erilaisia työkaluja. Security Centerin hallinnasta käsin pysytään koko ajan tilanteen tasalla, mitä tietoturvahaavoittuvuuksia ja muita vahinkoja tapahtuu. Se valmistelee valmiit standardi- ja tapauskohtaiset raportit valmiiksi uhista. Internet Asset Discovery luo luettelon potentiaalisista hyökkäyksistä verkkouhka-arvioinnin perusteella. Kartoitustarkistukset havaitsevat hyökkäys-

pinta-alan verkon ja muiden porttien tietoturvahaavoittuvuuksien skannauksella. Haavoittuvuuksien tarkistuksien avulla voidaan havaita haavoittuvuudet, jotka ovat ihan yleisessä tiedossa. Ne pitää yleensä sisällään järjestelmien ja verkkosovelluksien haavoittuvuudet. Haavoittuvuuksien hallinnasta voidaan itse hallita oman järjestelmän haavoittuvuuksia ohjelman antamien tietoturvahälytyksien perusteella. PCI DSS- säädöksenmukaisuus, voi varmistaa, että oma järjestelmän ja verkko on nykyisten ja tulevien tietoturvasäädösten mukainen, ja tätä myötä vähentämään oman järjestelmän haavoittuvuutta sekä tietomurtoriskiä. (F-Secure. 2019.)

F-Secure Radar arvioi verkkojen haavoittuvuuksia täsmällisesti. Yritysten sisäverkkoihin ja laitteisiin luodaan jatkuvasti erilaisia tietovarantoja ja uusia sovelluksia, jotka sitä mukaan avaavat uusia haavoittuvuuksia ja ovia hyökkääjille. Nykyään digitalisoituvassa maailmassa yritysten tulee olla koko varuillaan ja pitää omat turvallisuusasiat ajan tasalla. Tietoturvavastaavilla onkin iso vastuu, koska heidän tulee olla ajan tasalla kaikista mahdollisista uusista haavoittuvuuksista ja hyökkäyksistä, ja heidän tulee pitää omat järjestelmät säädösten mukaisina ja tätä myötä he pystyvät minimoimaan tietoturvauhat.
(F-Secure. 2019.)

Yrityksien hyökkäyspinta-alat ovat kaikilla yrityksillä erikokoisia, mahdolliset hyökkäyspinta-alat koostuvat verkoista, ohjelmistoista, verkkosovelluksista ja yhteyksistä ja kommunikoinnista näiden välillä. F-Secure Radarin tarkoitus on löytää nämä hyökkäyspinta-alat ja yksilöt, jossa järjestelmä on haavoittuvimmillaan. Se antaa sinulle ohjeita, miten pienentää tätä kyseistä pinta-alaa ja neuvoo käyttäjää suojautumaan hyökkäyksiltä myös tulevaisuudessa. Radarin avulla saadaan kartoitettua yrityksellesi turvallisen suojauksen, kun on selvillä tunnetut sekä tuntemattomat haavoittuvuudet, kaikkien ohjelmistojen ja laitteiden kontrollointi, haittaohjelmasivustot, kumppanien ja alihankkijoiden tietoturvakäytännöt ja yritykseen kohdentuva verkkourkinta. (F-Secure. 2019.)

3 TIETOTURVASTANDARDIT

Tietoturvastandardit ovat kansainvälisten järjestöjen ISO:n (International Organization For Standardization) sekä IEC:n (International Electrotechnical Commission) luomia, ohjeistavia asiakirjoja. Ohjeistavalla tarkoitetaan sitä, että kukin organisaatio soveltaa standardia ja määrittelee omat toimintamallinsa kyseisen standardin puitteissa.
Kansainväliset ja kotimaiset lainsäädännöt asettavat siis organisaatioille suoria ja epäsuoria tietoturvallisuuteen liittyviä yleisluontoisia velvoitteita, mutta näiden velvoitteiden noudattaminen käytännön toteutuksena on kuitenkin jätetty organisaatioiden omalle vastuulle. Organisaation kannalta on kuitenkin tärkeää kuunnella ja noudattaa näiden standardien ohjeistusta, sillä se auttaa organisaatiota kehittämään omaa tietoturvaansa. Lainsäädäntöönkin on viime vuosina tullut suuri määrä tietoturvaan liittyviä lakeja ja säädöksiä, joiden avulla pyritään parantamaan tietoturvaa ja määrittämään tietoturvatoimenpiteitä erilaisissa tilanteissa. (Laaksonen 2006, 18.)

Suomessa ei vielä tällä hetkellä ole olemassa sellaista lakia, joka olisi säädetty organisaatioiden tai yksityisten käyttäjien tietoturvaoikeuksista tai velvoitteista. Organisaatiot haluavatkin ennemmin ohjeistusta tai suuntaa-antavia kannanottoja viranomaisilta siitä, että miten saadaan tuotettua mahdollisimman turvallinen ja tehokas tietoturvajärjestelmä. Yksi suurin ongelma organisaatioille tietoturvallisuuden alalla on se, että tekniikka ja laitteistot kehittyvät niin kovaa vauhtia, että se kiihdyttää kilpailua markkinoilla. Samalla nopea kehitys mahdollistaa uusia tapoja käsitellä tietoa ja informaatioita. Nopean kehityksen kanssa samaan aikaan säädetään myös uusia yksityisyyden suojaa koskevia lakeja, jotka taas rajaavat useita teknisiä keinoja tehokkaan tietoturvajärjestelmän toteutuksessa. (Laaksonen 2006, 21.)

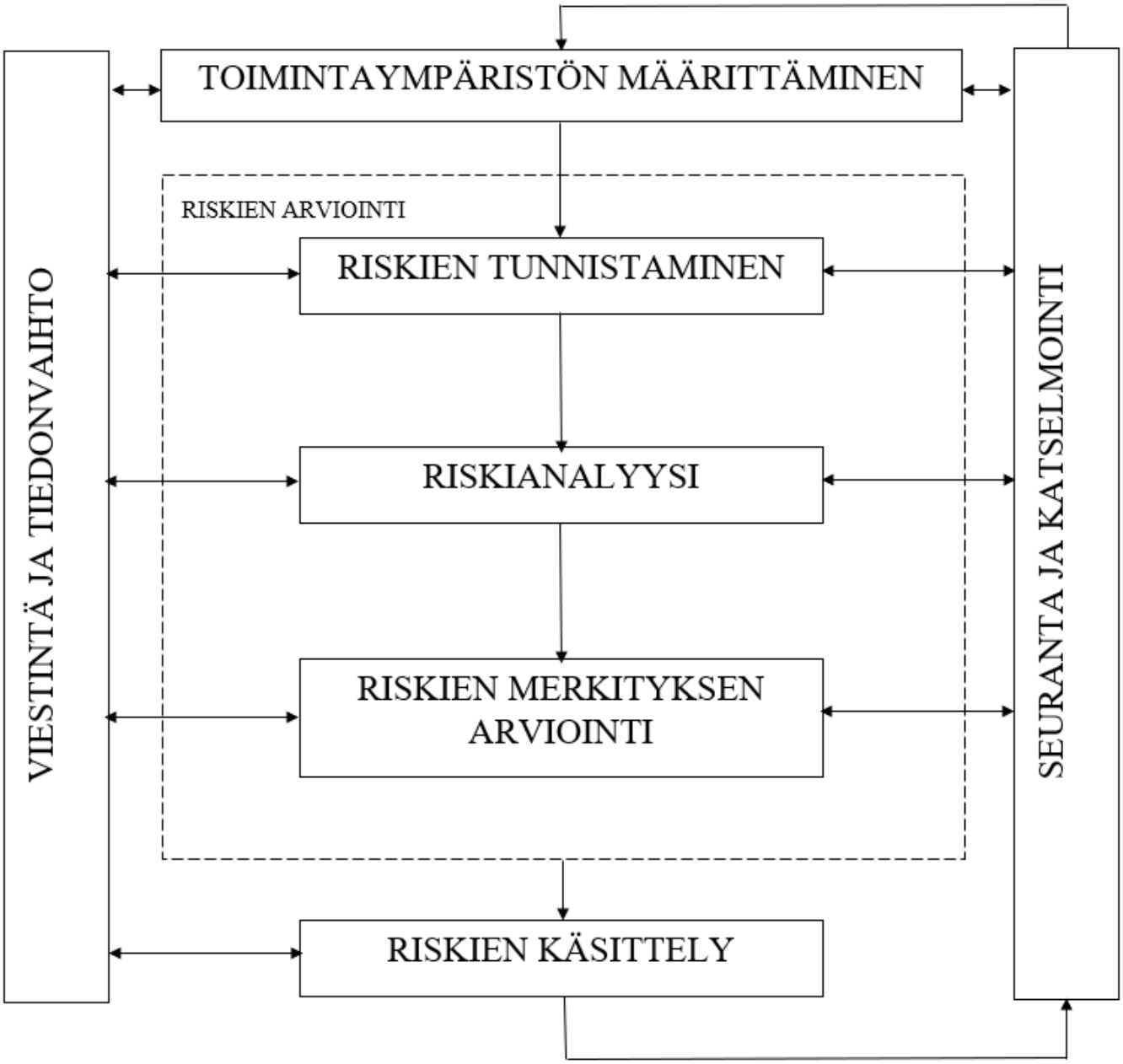
3.1 Tietoturvallisuuden hallintajärjestelmät

Tietoturvastandardi ISO/IEC 27001:2017 “Tietoturvallisuuden hallintajärjestelmät” on kansainvälinen asiakirja, joka ohjeistaa organisaatioita, kuinka luodaan tarvittavat tietoturvallisuuden hallintajärjestelmät, kuinka ne käytännössä toteutetaan ja kuinka näitä kyseisiä hallintajärjestelmiä ylläpidetään ja parannetaan, jotta tietoturvallisuus pysyisi standardien mukaisena. Kun organisaatio tekee päätöksen käyttöönottaa nämä standardien ohjeistamat tietoturvallisuuden hallintajärjestelmät, on se organisaatiolle strateginen päätös. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Tietoturvastandardia ISO/IEC 27001:2017 voidaan käyttää määrittämään ja arvioimaan ovatko organisaation tietoturvavaatimukset riittävän korkeat. Tietoturvastandardissa esiintyvät asiat on järjestetty niiden suositeltuun toteuttamisjärjestykseen. Tietoturvastandardissa ISO/IEC 27001:2017 kerrotaan myös tärkeimmät tietoturvallisuuden hallintajärjestelmiin liittyvät sanastot, yleiskuvaukset, määritelmät ja aihealueeseen liittyvät termit. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Näiden tietoturvallisuuden hallintajärjestelmien toteuttamiseen ja luomiseen vaikuttavat organisaation koko, organisaation tarpeet ja tavoitteet, organisaation vaatimukset tietoturvallisuuden suhteen ja organisaation käytössä olevat prosessit. Kaikki nämä edellä mainitut asioihin vaikuttavat tekijät tulevat todennäköisesti muuttumaan tulevaisuudessa. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Tietoturvallisuuden hallintajärjestelmät suojaavat riskinhallintaprosessin (KUVIO 2) avulla organisaatiossa esiintyvän tiedon luottamuksellisuutta, tarvittavan tiedon saatavuutta ja tiedon eheyttä. Ne myös vahvistavat organisaation sisällä luottamusta siihen, että riskejä hallitaan turvallisesti ja asianmukaisesti. Tietoturvallisuuden hallintajärjestelmien liittäminen johtamis- ja hallintarakenteisiin on erittäin tärkeää. On myös kriittisen tärkeää, että tietoturvallisuus otetaan huomioon aina, kun suunnitellaan organisaation sisäisiä prosesseja, tiedonhallintakeinoja ja tietojärjestelmiä.
Kun organisaatioon suunnitellaan tietoturvallisuuden hallintajärjestelmiä, pitää varmistua siitä, että ne toteutetaan organisaation tarpeiden ja vaatimusten mukaisesti.
(SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)



KUVIO 2: Riskienhallintaprosessi (mukaillen SFS-ISO/IEC 27005:2018, 8)

3.1.1 Organisaation toimintaympäristö ja soveltamisalan määrittäminen

Ensimmäisenä kun organisaatiossa lähdetään kartoittamaan sen tietoturvallisuuden hallintajärjestelmiä, on ymmärrettävä organisaation toimintaympäristö. Organisaation tulee ymmärtää ja määrittää sen ulkoiset ja sisäiset tekijät ja asiat, jotka vaikuttavat organisaation kykyyn saavuttaa halutut tulokset tietoturvallisuuden hallintajärjestelmältä. Näihin asioihin kuuluvat organisaation itse määrittämät sidosryhmät, jotka vastaavat tietoturvallisuuden hallintajärjestelmistä. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Määritetyt sidosryhmät asettavat ja määräävät organisaation tietoturvallisuutta koskevat pykälät ja vaatimukset. Nämä sidosryhmien asettamat pykälät ja vaatimukset pohjautuvat lakisääteisiin vaatimuksiin, sekä sopimusvelvoitteisiin tietoturvallisuuden kannalta. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Seuraavaksi organisaatiossa on päätettävä mahdollisista tietoturvallisuuden hallintajärjestelmien soveltamisesta ja rajaamisesta, jotta voidaan määritellä järjestelmän soveltamisala. Organisaation päättäessä tietoturvallisuuden hallintajärjestelmien soveltamisalasta, täytyy sen ottaa huomioon edellä mainitut ulkoiset ja sisäiset tekijät ja sidosryhmien asettamat vaatimukset. Lisäksi täytyy ottaa huomioon oman organisaation kuin myös muiden organisaatioiden riippuvuudet ja toimintojen rajapinnat. Tämän kyseisen soveltamisalan täytyy olla saatavilla dokumentoituna tietona.
(SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

3.1.2 Ylimmän johdon luottamus ja vastuu hallintajärjestelmään

On tärkeää, että organisaation ylimmällä johdolla on täysi luottamus tietoturvallisuuden hallintajärjestelmään. Ylimmän johdon tulee osoittaa sitoutumista ja johtajuutta organisaationsa tietoturvallisuuden hallintajärjestelmään. Heidän tulee varmistaa, että aiemmin laaditut tietoturvatavoitteet ja tietoturvapolitiikka ovat yhdenmukaisia organisaation strategisten tavoitteiden kanssa. Heidän pitää myös varmistua siitä, että laaditun tietoturvallisuuden hallintajärjestelmän osoittamat vaatimukset koskevat myös organisaation prosesseja ja että ne vaatimukset yhdistetään näihin kyseisiin prosesseihin. Lisäksi ylimmän johdon tulee varmistaa, että tietoturvallisuuden hallintajärjestelmän vaatimat resurssit ovat juuri oikeat heidän organisaatiolleen ja että nämä resurssit ovat saatavilla. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Ylimmän johdon tulee myös informoida muita organisaation jäseniä siitä, kuinka tärkeää on noudattaa tietoturvallisuuden hallintajärjestelmän ja tietoturvallisuuden hallinnan kannalta laadittuja tietoturvavaatimuksia, jotta tietoturvallisuus ei vaarantuisi. Ylin johto on myös vastuussa siitä, että laadittu tietoturvallisuuden hallintajärjestelmä saavuttaa ennalta määritetyt tavoitteet. Heidän vastuullaan on myös ohjata ja tukea työntekijöitään tietoturvallisuuden hallintajärjestelmän kehittämisessä, ja tällä tavoin he edistävät hallintajärjestelmän jatkuvaa kehitystä. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Ylin johto huolehtii organisaation tietoturvapolitiikan laatimisesta. Tietoturvapolitiikan tulee soveltua organisaation strategisiin tavoitteisiin. Tietoturvapolitiikan tulee sisältää aiemmin laaditut tietoturvatavoitteet, ja tämän tietoturvapolitiikan tulee määrittää perusta organisaation tietoturvatavoitteille. Tietoturvapolitiikan tulee sitoutua laadittujen tietoturvallisuuden vaatimusten täyttämiseen. Tietoturvapolitiikan tulee myös sitoutua organisaation tietoturvallisuuden hallintajärjestelmän jatkuvaan parantamiseen. Tietoturvapolitiikan tulee olla dokumentoitua tietoa, ja sen tulee olla tiedossa koko organisaatiossa. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Ylimmän johdon tulee varmistaa, että organisaatiossa määritellään ja jaetaan vastuut ja valtuudet tietoturvallisuudesta vastaavien henkilöiden kesken. Ylin johto myös vastaa siitä, että organisaation tietoturvallisuuden hallintajärjestelmät ovat kansainvälisessä ISO/IEC 27001:2017 standardissa esitettyjen vaatimusten mukaiset. Ylin johto myös määrittää henkilön organisaatiosta, joka vastaa heille tietoturvallisuuden suorituskyvystä raportoinnista.
(SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Organisaation tietoturvallisuuden hallintajärjestelmän soveltuvuuden, vaikuttavuuden ja asianmukaisuuden kannalta on tärkeää, että ylin johto katselmoi suunnitelluin aikavälein, että kaikki sujuu suunnitelmien ja vaatimusten mukaisesti. Ylimmän johdon katselmuksessa tulee ottaa huomioon aiempien ylimmän johdon tarkastusten takia käynnistettyjen hallintajärjestelmän parannuksia koskevien toimenpiteiden tilanne. Katselmuksessa tulee ottaa huomioon myös organisaation sisäisten- ja ulkoisten tekijöiden muutoksien aiheuttamat tekijät tietoturvallisuuden hallintajärjestelmälle. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Näiden muutosten aiheuttamia mahdollisia toimenpiteitä tulee myös kartoittaa ja toteuttaa mahdollisimman pian. Ylimmän johdon tulee myös laatia organisaation tietoturvan tasoa koskeva raportti. Tähän

raporttiin tulee sisältyä poikkeamat ja niitä korjaavat toimenpiteet, mittauksen ja seurannan tulokset, sisäisten auditointien tulokset ja tietoturvatavoitteiden täyttyminen. Johdon katselmuksessa tulee myös ottaa huomioon organisaation sidosryhmien palaute, tietoturvariskien arviointiprosessin tuottama palaute ja riskinkäsittelysuunnitelman nykyinen tilanne.
(SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

3.1.3 Tietoturvariskien arvioiminen

Organisaation suunnitellessa tietoturvallisuuden hallintajärjestelmää tulee ottaa huomioon organisaation sisäiset- ja ulkoiset tekijät, jotka vaikuttavat organisaation kykyyn saavuttaa haluttu tulos tietoturvallisuuden hallintajärjestelmältä. Lisäksi on myös otettava huomioon sidosryhmien aiemmin asettamat vaatimukset. Tämän jälkeen on tärkeää hahmottaa mahdolliset tietoturvariskit ja miten toimitaan niiden sattuessa. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Organisaation tulee varmistaa, että suunniteltu tietoturvallisuuden hallintajärjestelmä saavuttaa halutut tulokset, ja se estää ja vähentää mahdollisia tietoturvauhkia. Organisaation tulee myös olla selvillä siitä, miten toimitaan tiettyjen tietoturvariskien sattuessa. Lisäksi organisaation tulee suunnitella, että miten tietoturvallisuuden hallintajärjestelmä sisällytetään organisaation prosesseihin. Organisaation tulee myös arvioida tietoturvauhkien sattuessa tehtävien toimenpiteiden vaikuttavuus ja mahdolliset taloudelliset tappiot. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Kun arvioidaan mahdollisia tietoturvauhkia, tulee organisaation luoda tietoturvakriteerejä. Näihin tietoturvakriteereihin määritellään tietoturvariskien hyväksymiskriteerit ja sellaiset kriteerit, jotka koskevat tietoturvariskien arvioinnin suorittamista. Organisaation tulee myös varmistua, että tietoturvauhkien arvioinnit tuottavat toisiinsa verrattavissa olevia, päteviä ja yhdenmukaisia tuloksia. On tärkeää, että tämän arviointiprosessin avulla tunnistetaan organisaation tietoturvallisuuden hallintajärjestelmän alaisuuteen kuuluvat tiedon eheyden, luottamuksellisuuden ja tiedonsaatavuuden menettämiseen liittyvät tietoturvariskit. Tietoturvariskien arviointiprosessista tulee olla dokumentoitua tietoa organisaation käytettäväksi. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Tietoturvariskejä arvioidessa tulee myös arvioida riskien toteutumisten aiheuttamia seuraamuksia ja sitä, kuinka todennäköistä on, että kyseinen tietoturvariski voisi tapahtua. Lisäksi tietoturvariskeille tulee

määrittää riskin taso. Tulee myös arvioida, onko mahdollista välttää kyseinen tietoturvariski jollain tapaa vai onko kyseinen riski aina olemassa.
(SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Organisaation tietoturvan tasoa ja tietoturvallisuuden hallintajärjestelmän vaikuttavuutta arvioimalla saadaan kartoitettua mahdollisia tietoturvahaittoja ja tietoturvariskejä. Organisaation tulee määrittää, mitä prosesseja sen täytyy mitata ja seurata. Näihin seurattaviin prosesseihin lukeutuvat tietoturvaprosessit ja hallintakeinot. On myös määritettävä, mitä seuranta-, analysointi-, arviointi- ja mittausmenetelmiä käytetään, jotta varmistetaan kelvollinen arviointitulos. Näillä edellä mainituilla menetelmillä tulisi saavuttaa yhdenvertaiset tai toisiinsa verrattavat tulokset, jotta menetelmistä saatuja tuloksia voidaan pitää kelvollisina. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

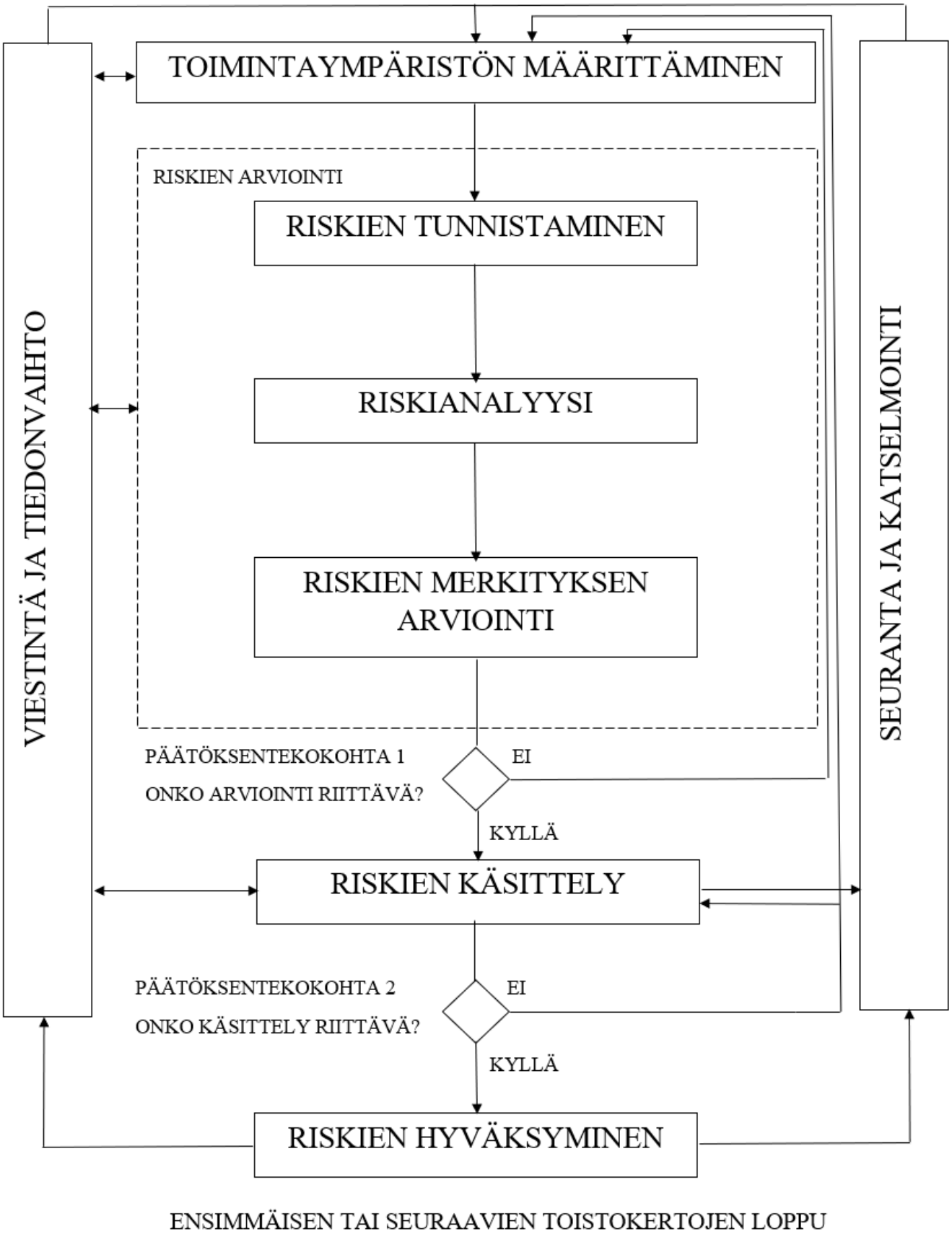
Organisaation on myös suunniteltava, milloin näitä seurantoja ja mittausmenetelmiä voitaisiin toteuttaa. On myös tärkeää määrittää ne henkilöt, jotka nämä mittaukset ja seurannat toteuttavat. Näistä mittausmenetelmistä ja seurannoista saadut tulokset tulee arvioida ja analysoida. Organisaatiossa on siis päätettävä myös ne henkilöt, jotka nämä arvioinnit ja analysoinnit suorittavat. Mittausmenetelmistä ja seurannoista saadut tulokset tulee dokumentoida asianmukaisesti, ja niistä tulee säilyttää dokumentoitua tietoa todisteena.
(SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

3.1.4 Tietoturvariskien käsitteleminen ja tietoturvatavoitteet

Tietoturvariskien arvioimisen lisäksi organisaation tulee toteuttaa tietoturvariskien käsittelyprosessi. Tässä prosessissa valitaan mahdolliset tietoturvariskien käsittelyvaihtoehdot, huomioon ottaen tietoturvariskien arviointiprosessin tuottamat tulokset. Lisäksi tässä käsittelyprosessissa määritellään sellaiset hallintakeinot, jotka auttavat kartoitettujen tietoturvariskien hallinnoimiseen (KUVIO 3). Organisaatiot voivat halutessaan itse suunnitella nämä kyseiset hallintakeinot, tai sitten he voivat ottaa mallia muista lähteistä. Muilla lähteillä tarkoitetaan esimerkiksi kansainvälisien standardien luomia esimerkkejä. Standardeja apuna käyttämällä organisaatiot voivat varmistua siitä, ettei mitään tärkeitä hallintakeinoja ja hallintatavoitteita jää ottamatta huomioon. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Organisaation on myös tärkeää laatia tietoturvariskien käsittelysuunnitelma. Tällöin riskien omistajalta haetaan hyväksyntä laaditulle käsittelysuunnitelmalle ja niille tietoturvariskeille, jotka jäävät vielä jäljelle. Tietoturvariskien käsittelyprosessista ja käsittelysuunnitelmasta tulee laatia ja säilyttää dokumentoitua tietoa. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Tämän tietoturvariskien käsittelyprosessin jälkeen on organisaation asetettava itselleen tietoturvatavoitteet. Nämä tavoitteet tulee asettaa niille kuuluville tasoille ja toiminnoille. Tietoturvatavoitteiden on oltava yhdensuuntaisia aiemmin laaditun tietoturvapolitiikan kanssa. Tietoturvatavoitteiden tulee olla mitattavissa, jos se vain on mahdollista. Tietoturvatavoitteissa tulee ottaa myös huomioon tietoturvavaatimukset ja tietoturvariskien arviointiprosessin ja tietoturvariskien käsittelyprosessin tulokset. Tietoturvatavoitteista tulee viestittää muulle organisaatiossa työskenteleville. Tietoturvatavoitteita tulee myös tarvittaessa päivittää. Näistä tietoturvatavoitteista tulee myös olla dokumentoitua tietoa organisaatiossa. Kun laaditaan ja suunnitellaan organisaation tietoturvatavoitteita, tulee ottaa huomioon, minkälaisia resursseja siihen tarvitaan, ketkä siitä vastaavat, työn valmistuminen ja kuinka saatuja tuloksia tulee arvioida. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)



KUVIO 3: Tietoturvariskien hallintaprosessi (mukaillen SFS-ISO/IEC 27005:2018, 8)

3.1.5 Tietoturvallisuuden hallintajärjestelmien tukitoiminnot

Organisaatiossa tulee määrittää ja varata tietoturvallisuuden hallintajärjestelmän luomiseen, ylläpitämiseen ja toteuttamiseen tarvittavat resurssit. Organisaation tulee määrittää tietoturvallisuuden hallintajärjestelmän ohjauksessa työskentelevien henkilöiden pätevyys ja lisäksi niiden henkilöiden pätevyys, jotka ovat vastuussa organisaation prosesseista, jotta tietoturvallisuus säilyy. Näiden henkilöiden pätevyys voidaan varmistaa koulutusten, harjoittelun, sekä työkokemuksen perusteella. Tarvittaessa tulee huolehtia organisaatiossa työskentelevien henkilöiden kouluttamisesta, sekä arvioida tehtyjen toimenpiteiden vaikutusta tietoturvallisuuteen. Organisaatio voi myös tarvittaessa palkata tai vuokrata tärkeisiin tehtäviin pätevää henkilökuntaa. Tietoturvallisuuskoulutuksista ja pätevyyksistä tulee säilyttää dokumentoitua tietoa, joka toimii tarvittaessa näyttönä työntekijän pätevyydestä. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Organisaation johtotehtävissä työskentelevien henkilöiden on oltava perillä organisaation tietoturvapolitiikasta. Lisäksi heidän tulee olla tietoisia siitä, kuinka he voivat omalla toiminnallaan edistää organisaation tietoturvallisuuden hallintajärjestelmän toimintaa ja millaista hyötyä organisaatio saavuttaa tietoturvallisuuden parantamisella. Lisäksi heidän tulee olla perillä siitä, mitä tapahtuu, jos organisaation tietoturva pettää ja millaisia seuraamuksia siitä voi tulla. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Organisaation tulee myös määrittää, millaista sisäistä ja ulkoista viestintää tarvitaan kertomaan muulle organisaatiolle tietoturvallisuuden hallintajärjestelmästä ja sen noudattamisesta. On päätettävä, mitä, mistä, milloin ja keiden kanssa asiasta viestitään. Organisaation tulee myös määrittää, millaiset viestintäprosessit ovat mahdollisia organisaation sisällä.
(SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

3.1.6 Dokumentoitu tieto hallintajärjestelmästä

Organisaation tietoturvallisuuden hallintajärjestelmän tulee sisältää kansainvälisessä standardissa ISO/IEC 27001:2017 määritelty dokumentoitu tieto. Organisaatio määrittää lisäksi itse, että mitkä dokumentoidut tiedot tulee säilyttää, koska ne ovat organisaation tietoturvallisuuden hallintajärjestelmän laadun kannalta välttämättömiä. Dokumentoidun tiedon laajuus vaihtelee organisaatioiden välillä, sillä

siihen vaikuttavat organisaation koko ja prosessien, tuotteiden ja toimintojen tyyppi. Laajuuteen voi vaikuttaa myös organisaation prosessien välinen vuorovaikutus. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Kun organisaatiossa luodaan dokumentoitua tietoa, on otettava huomioon asianmukainen kuvaus ja merkintä dokumentissa. Dokumentissa tulee näkyä päivämäärät, otsikot, viitenumerot ja kuka dokumentin on laatinut. Näiden lisäksi on otettava huomioon myös dokumentin tallennusmuoto ja tallennusvälineet. Lopuksi tulee tarkistaa ja hyväksyä dokumentin soveltuvuus ja riittävyys. Tietoturvallisuuden hallintajärjestelmän dokumentoitua tietoa tulee hallita siten, että se on aina tarvittaessa saatavilla ja että se on oikeanlaisessa tallennusmuodossa. Pitää myös varmistua siitä, että se on asianmukaisesti suojattu. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Organisaation tulee varmistua, että dokumentoitu tieto pysyy muuttumattomana, ja sen asiaton käyttö tulee olla estetty. Lisäksi pitää varmistua siitä, että tietoja ei luovuteta luvatta eteenpäin. Organisaation tulee myös huolehtia dokumentoidun tiedon turvallisesta hävittämisestä, mikäli tieto on vanhentunutta tai sitä ei enää tarvita. Organisaation tulee myös määrittää, kenellä on valtuudet tarkastella tai muuttaa dokumentoitua tietoa organisaation sisällä. Dokumentoidun tiedon jakelu tulee myös rajoittaa organisaation sisäisestikin. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

3.1.7 Sisäinen auditointi

Organisaation tulee tehdä sisäisiä auditointeja sovituin aikavälein. Näistä sisäisistä auditoinneista voidaan määritellä, onko suunniteltu tietoturvallisuuden hallintajärjestelmä organisaation aiemmin laatimien vaatimusten mukainen. Lisäksi sisäisissä auditoinneissa voidaan verrata organisaation tietoturvallisuuden hallintajärjestelmää kansainvälisiin standardeihin. Sisäisissä auditoinneissa voidaan lisäksi myös määritellä, miten tietoturvallisuuden hallintajärjestelmien ylläpitäminen on onnistunut. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Organisaation tulee laatia, suunnitella ja toteuttaa auditointiohjelmia, joissa määritetään sisäisten auditointien menetelmät, auditointien suunnitteluvaatimukset, kuinka laaja auditointi on, auditointien vastuut ja auditoinneista raportointi. Näissä edellä mainituissa menetelmissä tulee ottaa huomioon näiden prosessien tärkeys. Lisäksi tulee ottaa huomioon edellisten auditointien tulokset. Organisaation tulee myös

määrittää jokaisen auditoinnin soveltamisala ja arviointikriteerit. Organisaation tulee myös valita auditoijat ja on myös varmistettava, että auditoinnit hoidetaan puolueettomasti. On myös varmistettava, että auditointien raportointi hoidetaan asiasta ymmärtävälle, organisaation johdossa työskentelevälle henkilölle. Auditointiohjelmasta ja auditointien tuloksista tulee säilyttää todisteena dokumentoitua tietoa. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

3.1.8 Hallintajärjestelmän parantaminen

Kun organisaation tietoturvallisuuden hallintajärjestelmää arvioidessa havaitaan poikkeama, tulee organisaation reagoida poikkeamaan mahdollisimman nopeasti joko ryhtymällä korjaaviin toimenpiteisiin sen hallitsemiseksi ja korjaamiseksi tai käsiteltävä poikkeaman syystä aiheutuvat seuraukset. Organisaation tulee arvioida tarvittavat toimenpiteet poikkeaman syyn poistamiseksi, jotta tämä poikkeama ei toistuisi tai esiintyisi missään muussa prosessissa. Tällaisia toteutettavia toimenpiteitä ovat poikkeaman katselmointi, poikkeaman syyn tai syiden selvittäminen tai vastaavien poikkeamien syiden etsiminen. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

Näiden toimenpiteiden jälkeen tulee organisaation toteuttaa ne toimenpiteet, jolla poikkeama saadaan kuitattua. Organisaation tulee myös arvioida jälkeenpäin, kuinka hyvin poikkeaman korjaavat toimenpiteet ovat korjanneet ongelman. Tarvittaessa organisaation tulee myös tehdä muutoksia tietoturvallisuuden hallintajärjestelmään. Poikkeamista ja niistä aiheutuvista korjaavista toimenpiteistä ja niiden tuloksista tulee säilyttää dokumentoitua tietoa. (SFS27001. Tietoturvallisuuden hallintajärjestelmät. 2017.)

3.2 Tietoturvallisuuden hallintakeinojen menettelyohjeet

Tietoturvastandardi ISO/IEC 27002:2017 “Tietoturvallisuuden hallintakeinojen menettelyohjeet” on kansainvälinen asiakirja, joka ohjeistaa organisaatioita tietoturvallisuuden hallintakeinojen menettelyssä. Moniakaan organisaatioiden tietojärjestelmiä ei ole suunniteltu standardien mukaisesti. Tietoturvastandardissa ISO/IEC 27002:2017 organisaatioille tarkoitettuja tietoturvastandardeja ja ohjeistetaan tietoturvallisuuden hallintakäytännöissä. Näihin hallintakäytäntöihin sisältyy hallintakeinojen valinta ja toteuttaminen, kun otetaan huomioon myös organisaation tietoturvallisuudelle haitalliset riskiympäristöt. Tietoturvastandardi ISO/IEC 27002:2017 on suunniteltu sellaisille organisaatioille, jotka aikovat

toteuttaa standardien määrittelemän tietoturvallisuuden hallintajärjestelmän ja jotka aikovat laatia organisaatiolleen omat tietoturvallisuuden hallintaohjeet.
(SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

3.2.1 Tietoturvallisuuden organisoiminen ja tietoturvapolitiikat

Organisaation tulee määrittää ja jakaa kaikki tietoturvaroolit ja tietoturvavastuut organisaation sisällä. Organisaation tulee selkeästi yksilöidä tietoturvallisuusprosessien suorittamista ja yksittäisen omaisuuden suojausta koskevat velvollisuudet. Ne henkilöt, joille on annettu vastuu tietoturvallisuudesta, voivat halutessaan siirtää tiettyjä tietoturvan suojaamistehtäviä muille. Kuitenkin vastuu tietoturvallisuudesta pysyy näillä alkuperäisillä henkilöillä. Heidän tulee siis vahtia, että annetut tietoturvan suojaamistehtävät suoritetaan oikein ja asianmukaisella tavalla. Jos yksittäinen henkilö vastaa jostain tietystä tietoturva-alueesta, tulee siitä ilmoittaa. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Organisaation tulee määritellä ja tunnistaa tietoturvaprosessit ja suojata sen omaisuus. Sen tulee nimetä ne henkilöt, jotka vastaavat kustakin omaisuudesta tai tietoturvaprosessista. Näiden nimettyjen henkilöiden tulee olla päteviä heille annetuilla vastuualueilla ja heille tulee järjestää mahdollisuus seurata kyseisen aihealueen kehittymistä, jotta he kykenevät parhaansa mukaan täyttämään heille myönnetyn tietoturvavastuun. Nämä vastuut ja niiden yksityiskohdat tulee dokumentoida. Lisäksi tietoturvallisuuden valtuustasoista tulisi laatia ja säilyttää dokumentoitua tietoa. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Tietoturvapolitiikka muodostaa perustan organisaation tietoturvallisuuden kehittämiselle. Yleinen organisaation laatima tietoturvapolitiikka muodostaa yksityiskohtaisia teknisiä ohjeita, jotka auttavat organisaatiota tietoturvan hallinnassa. Ylimmän johdon tulee hyväksyä organisaation laadittu tietoturvapolitiikka, jossa määritetään organisaation tavoitteet tietoturvallisuuden kannalta ja se, kuinka niitä lähdetään toteuttamaan. Ylin johto nimittää myös tietoturvapoliitikot, jotka hoitavat organisaation tietoturvapolitiikkaa. Näiden poliitikkojen valinnasta tulee tiedottaa organisaation sisäisesti ja tarvittaessa asiaankuuluville ulkopuolisille tahoille. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Tietoturvapolitiikan tulee sisältää sellaiset lausumat, joissa organisaation tietoturvatavoitteet, tietoturvaperiaatteet ja lausumat itse tietoturvasta määritellään. Nämä lausumat ohjaavat organisaatiossa kaikkea

tietoturvallisuutta koskevaa toimintaa. Tietoturvapolitiikassa lisäksi jaetaan ja määritellään tietoturvavastuut organisaation sisällä. Lisäksi tietoturvapolitiikassa kerrotaan, mitkä prosessit käsittelevät poikkeamia ja poikkeustapauksia. Tietoturvapolitiikassa tulee käsitellä myös, mikä on suojauksen tarkoitus, minkälaista suojaustasoa yrityksessä tullaan noudattamaan ja kenen vastuulla tietoturvapolitiikan ylläpitäminen on. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

3.2.2 Organisaation omaisuuden suojaus ja hallinta

Organisaation sisäinen tieto ja tiedonkäsittelypalveluiden suojattava omaisuus tulee yksilöidä ja organisaation suojattavasta omaisuudesta tulee laatia luettelo, jota ylläpidetään ajan tasalla. Suojattu omaisuus, joka on tiedon elinkaaren kannalta tärkeää, tulee yksilöidä ja dokumentoida. Tämän tiedon elinkaaren tulisi sisältää varastointi, luominen, käsitteleminen, siirtäminen ja tuhoaminen ja poistaminen. Näitä dokumentteja tulee säilyttää ja ylläpitää joko erityisissä tai jo valmiiksi luoduissa luetteloissa. Omaisuusluetteloiden tulee olla tarkkaan laadittuja, ajantasaisia ja toisiinsa verrattavissa olevia luetteloita. Tämän luetteloinnin avulla organisaatio varmistaa, että sen suojaus on vakuuttava. Näitä luetteloita voidaan myös tarvita todisteena työturvallisuuteen, talouteen tai vakuutuksiin liittyvissä asioissa. Standardissa ISO/IEC 27005 on enemmän omaisuuden suojaamista koskevaa tietoa ja esimerkkejä, joita organisaatio voi käyttää apunaan suojattavan omaisuutensa yksilöimisessä. Tällaisen omaisuusluettelon laatiminen on hyvin tärkeää tietoturvariskien hallinnalle. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Omaisuusluetteloiden sisältämälle suojattavalle omaisuudelle tulee aina määrittää jokin omistaja. Näihin omistajiin kelpaa myös yksittäinen henkilö tai jokin muu taho, kunhan heillä on hyväksytty vastuu suojattavan omaisuuden hallinnasta. Tällaista vastuuta varten suoritetaan yleensä prosessi, joka varmistaa, että suojattavan omaisuuden omistajuus voidaan osoittaa tarvittaessa. Suojattavan omaisuuden omistaja on siis vastuussa tästä omaisuudesta ja sen asianmukaisesta hallinnasta koko sen elinkaaren ajan. Suojattavan omaisuuden omistajuus tulee todistaa silloin, kun suojattava omaisuus luodaan tai kun se sisällytetään organisaatioon. Tämän suojattavan omaisuuden omistajan tulee varmistaa, että omaisuus on luetteloitu asianmukaisesti. Hän on myös vastuussa, että omaisuus on suojattu ja luokiteltu. Omistajan tulee myös pääsynhallintapolitiikat huomioon ottaen katselmoida ja määrittää säännöllisesti omaisuuden luokitukset ja pääsyrajoitteet. Lopuksi hänen tulee vielä varmistaa, että omaisuus tuhotaan tai poistetaan asianmukaisella tavalla. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Työsuhteen päättyessä tulee työntekijän palauttaa kaikki hänen vastuullaan ja hallussaan oleva organisaation suojattava omaisuus. Tähän omaisuuteen kuuluvat sekä fyysinen, että sähköinen omaisuus. Jos työntekijällä tai organisaation ulkopuolisella henkilöllä on omistuksessaan organisaatiolta ostettua omaisuutta tai hän on käyttänyt työssään omia laitteita, tulee varmistua siitä, että näistä laitteistoista siirretään tärkeät tiedot takaisin organisaatiolle, jonka jälkeen nämä tulee poistaa asianmukaisesti laitteistosta. Jos taas tämä tieto on tärkeää heidän toimintansa jatkumisen kannalta, tulee tämä kyseinen tieto dokumentoida ja siirtää organisaatiolle. Organisaation tulee varmistaa työsuhteen irtisanomisaikana, ettei irtisanottu työntekijä kopioi mitään organisaatiolle tärkeää tietoa luvattomasti. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

3.2.3 Tietojen suojaustason luokittelu

Organisaation sisäinen tieto tulee lakisääteisten vaatimusten perusteella luokitella. Tietojen suojaustasoon vaikuttavat tiedon kriittisyys, tiedon arvo ja luvattoman muokkaamisen tai tiedon paljastumisen aiheuttamat vahingot. Tietojen suojaustason luokitus varmistaa sen, että kun tiedon suojaustaso on korkea, siihen eivät pääse käsiksi muuta kuin valtuutetut organisaation työntekijät. Tietojen luokittelussa tulee ottaa huomioon lakisääteiset vaatimukset ja organisaation liiketoiminnan tarpeet jakaa kyseistä tietoa. Tietojen lisäksi myös suojattu omaisuus voidaan luokitella sen sisältämän tiedon perusteella. Suojatun omaisuuden tietojen luokittelusta vastaa omistaja, jonka vastuulla tämä suojattu omaisuus on. Tietojen suojaustason arvioinnin tulee sisältää arvioinnin tietojen eheydestä, luottamuksellisuudesta ja saatavuudesta. Siihen tulee myös lisätä muut mahdolliset vaatimukset. Suojaustason arviointiperiaatteiden tulee olla yhdenmukaisia organisaation pääsynhallintapolitiikan kanssa. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Jokaiselle tietojen suojaustasolle tulee antaa nimi, joka kuvaa tietojen kriittisyyttä. Tietoja luokiteltaessa tulisi periaatteiden olla aina yhdenmukaiset, jotta organisaation suojattava omaisuus ja tärkeä tieto luokiteltaisiin aina samalla tavalla. Luokittelu tulisi sisältyä myös organisaation prosesseihin. Omaisuuden luokittelusta saadun dokumentin tulee sisältää arvio suojattavan omaisuuden arvosta. Tämä omaisuuden arvo perustuu omaisuuden kriittisyydestä ja arkaluontoisuudesta organisaatiolle. Tätä luokittelua tulisi päivittää omaisuuden elinkaaren aikana, jos sen arvo, kriittisyys tai arkaluontoisuus organisaatiolle muuttuu. Nämä omaisuuden luokittelut antavat tärkeän kuvan tietoja käsitteleville henkilöille siitä, kuinka tätä omaisuutta tai tietoa tulee suojata. Nämä tiedot voivat joskus lakata olemasta kriittistä tai

arkaluontoista, jos tieto tulee jotain muuta kautta julkiseksi. Tämä tulee ottaa huomioon tietojen suojausluokituksessa, jotta vältettäisiin turhia lisäkustannuksia organisaatiolle tarpeettomien hallintakeinojen toteuttamisesta. Kuitenkin taas liian alhainen suojausluokitus saattaa vaarantaa organisaation markkinaetua tai liiketoiminnasta asetettujen tavoitteiden saavuttamista. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

3.2.4 Tietovälineiden käsitteleminen

Organisaation tulee laatia asianmukainen ohjeistus koskien siirrettävien tietovälineiden hallintaa. Jos organisaation siirrettävä tietoväline siirretään uudelleenkäytettäväksi, tulee sen sisällön palauttaminen tehdä mahdottomaksi. Tietovälineiden siirtoa uudelleenkäyttöä varten tulee aina hankkia lupa, ja siirroista on pidettävä kirjaa. Tietovälineitä tulee säilyttää turvallisessa ja valmistajan määräysten mukaisessa paikassa, josta ne eivät joudu vääriin käsiin. Jos tietovälineelle tallennettu tieto on tärkeää sen luottamuksellisuuden tai eheyden takia, tulee tietoväline suojata mahdollisimman hyvin salaustekniikoiden avulla. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Vanhoista tietovälineistä tulee tarvittavat tiedot siirtää ajoissa uusiin tietovälineisiin, jotta vältetään tiedon katoamista tietovälineen rappeutuessa. Kaikki arvokas tieto tulee varmuuskopioida muutamaan eri tietovälineeseen, jotta vältetään tärkeän tiedon katoamisen tai tuhoutumisen riskit. Siirrettävät tietolähteet tulisi rekisteröidä, tällä vältetään mahdollista tietohävikkiä. Siirrettävät tietovälineasemat tulisi olla sallittuja vain silloin, jos siihen on jokin liiketoiminnallinen tarve. Jos organisaatiossa tulee tarve tallentaa tietoa jollekin siirrettävälle tietovälineelle, tiedonsiirtoa tähän laitteeseen tulisi seurata. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Organisaatiolle tarpeettomat tietovälineet tulee aina hävittää turvallisesti ja organisaation menettelyjen mukaisesti. Turvallista hävittämistä varten tulee organisaation laatia tietovälineiden hävittämistä koskevat menettelyohjeet, jossa kerrotaan, kuinka tietoväline hävitetään niin, ettei luottamuksellista tietoa pääse vääriin käsiin. Menettelyohjeiden määräysten tulee olla oikeassa suhteessa tiedon arkaluonteisuuden kanssa. Luottamuksellista tietoa sisältävät tietovälineet tulee hävittää polttamalla tai silppuamalla, jotta tieto ei mitenkään pääse vääriin käsiin. Kun vanhentuneita tietovälineitä kerätään yhteen, kun ne aiotaan hävittää, tulee ottaa huomioon riskit tiedon kasautumisen kannalta. Jos tietoväline on vaurioitunut, tulee siitä mahdollisesti suorittaa riskien arviointi. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

3.3 Pääsynhallinta

Organisaation tulee laatia pääsynhallintapolitiikka, joka perustuu tietoturvavaatimuksiin ja liiketoiminnallisiin vaatimuksiin. Suojattavan omaisuuden omistajan tulee huolehtia pääsynhallintasäännöistä, pääsyrajoitteista ja pääsyoikeuksista. Näiden edellä mainittujen pääsynhallintakeinojen laajuus riippuu omaisuuden tietoturvaluokituksesta. Pääsynhallintakeinoja on sekä fyysisiä että loogisia. Pääsynhallintapolitiikkaa laatiessa tulee ottaa huomioon liiketoiminnan sovellusten turvallisuusvaatimukset. Lisäksi tulee ottaa huomioon organisaation tiedonjakopolitiikka, järjestelmien ja verkkojen tietoturvapolitiikka ja kaikki lainsäädännöt ja sopimuksiin liittyvät velvoitteet, jotka liittyvät pääsynrajoittamiseen. Pääsynhallintasääntöjä laatiessa tulee lähtökohtana olla, että “kaikki on kiellettyä, jos sitä ei olla erikseen sallittu”. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Monet organisaatiot käyttävät pääsynhallinnassaan rooliperustaista lähestymismallia. Tämä lähestymistapa auttaa organisaatiota yhdistämään liiketoimintaroolit pääsyoikeuksiin. Pääsynhallintapolitiikassa on yleensä kaksi ohjaavaa periaatetta. Ensimmäinen on, että pääsyoikeudet myönnetään ainoastaan silloin, kun työntekijä tarvitsee tietoa tehtävänsä suorittamisessa. Toinen on, että pääsyoikeudet tietojenkäsittelypalveluihin myönnetään vain silloin, jos työntekijä tarvitsee tätä tietojenkäsittelypalvelua työtehtävässään tai työroolissaan. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

3.3.1 Sähköinen pääsynhallinta

Käyttäjälle tulee sallia pääsy ainoastaan sellaisiin verkkopalveluihin ja verkkoihin, joihin hänellä on pääsyoikeudet. Verkkopalveluiden ja verkkojen käyttöä varten tulisi laatia käyttöpolitiikka, joka tulee kattaa ne verkkopalvelut ja verkot, joihin käyttäjillä on sallittu pääsy. Lisäksi käyttöpolitiikan tulee määrittää valtuutusmenettelyt, jotka määrittävät, kenellä on pääsyoikeudet mihinkin verkkopalveluun ja verkkoon. Siinä tulee määritellä myös ohjausmenettely ja ohjauskeinot, joita käytetään verkkoyhteyksien ja verkkopalveluiden suojauksessa. Käyttöpolitiikan tulee sisältää myös verkkopalveluiden käyttäjien henkilöllisyyden todentamisvaatimukset ja kuinka verkkopalveluiden käyttöä tulee seurata. Luvaton ja suojaamaton verkkojen tai verkkopalveluiden käyttö voi vahingoittaa koko organisaation tietoturvallisuutta. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Yksi sähköisen pääsyn hallintakeino on käyttäjien rekisteröinti- ja poistamisprosessi. Tähän hallintaprosessiin tulee sisältyä jokaisen työntekijän yksilöllinen käyttäjätunnus. Yksilöllisen käyttäjätunnuksen

avulla työntekijä voi yhdistää itselleen omat toiminnot ja vastuut, jotka kuuluvat hänen työnkuvaansa. Jos yksilöllisen käyttäjätunnuksen haltija ei työskentele enää yrityksessä, tulee hänen käyttäjätunnuksensa jäädyttää tai poistaa välittömästi. Organisaatiossa tulee myös varmistaa, ettei kenenkään käyttäjätunnusta voida siirtää toisen henkilön käyttöön. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Toinen pääsyoikeuksien hallintakeino on pääsyoikeuksien jakaminen. Tällä prosessilla voidaan määrittää, mitkä oikeudet käyttäjälle annetaan mihinkin organisaation tietoihin tai palveluihin. Tämän hallintakeinon avulla voidaan seurata, ketkä organisaation työntekijät pääsevät käsiksi mihinkin tietoihin. Pääsyoikeudet tietoihin tulee hakea aina joko tietojärjestelmän omistajalta tai sitten organisaation johdolta. Organisaation tulee varmistaa, että kyseisten pääsyoikeuksien tasot ovat yhdenmukaiset organisaation pääsynhallintapolitiikan kanssa. Tulee myös varmistua, ettei esimerkiksi palvelun tuottaja voi myöntää erikseen pääsyä tietoihin, vaan että pääsyoikeudet saa ainoastaan sen jälkeen, kun asianmukaiset pääsyoikeusmenettelyt on suoritettu. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

3.3.2 Turvallinen kirjautuminen ja salasanat

Eräs sähköisen pääsynhallinnan ja tietoturvallisuuden tärkeä ehto on turvallinen kirjautumismenettely. Kirjautumismenettelyllä varmistetaan turvallinen kirjautuminen järjestelmiin ja sovelluksiin, jota luultavasti pääsynhallintapolitiikka velvoittaa. On siis valittava asianmukainen turvallisen kirjautumisen todennusmenettely. Tällä varmistetaan kirjautuvan käyttäjän henkilöllisyys. Jos tieto on erittäin salaista ja tarvitaan todella vahvaa ja turvallista henkilöllisyyden todennusta, salasanat ovat tässä tapauksessa liian heikko todennusmenetelmä. Tässä tapauksessa voidaan todennusmenetelmänä käyttää esimerkiksi tunnistevälineitä, sirukortteja, salausmenetelmiä tai biometrisiä keinoja. Järjestelmään tai sovelluksiin kirjautumismenetelmä tulisi olla suunniteltu niin turvalliseksi, että luvattoman pääsyn riski sinne olisi mahdollisimman pieni. Tämän kirjautumismenetelmän tulisi paljastaa mahdollisimman vähän tietoa siitä järjestelmästä tai sovelluksesta, johon kirjaudutaan. Tällä tavoin ei avustettaisi luvatonta käyttäjää tarpeettomasti. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Hyvän ja turvallisen kirjautumismenettelyn tulisi olla sellainen, ettei se näyttäisi mitään sovellusten tai järjestelmien tunnisteita ennen kirjautumista. Sen tulisi näyttää yleinen varoitus siitä, etteivät tietokoneelle voi kirjautua kuin pelkästään sellaiset käyttäjät, joilla on valtuutettu pääsy. Kirjautumisen aikana

ei saa näkyä ohjeviestiä, joka voisi auttaa luvatonta kirjautujaa. Ennen kuin kaikki kirjautumistiedot on syötetty, järjestelmä ei saa osoittaa niitä kelvollisiksi. Kirjautumisen virhetilanteessa järjestelmä ei saa osoittaa, mitkä tiedot ovat väärin ja mitkä oikein. Järjestelmän tulee myös estää mahdolliset vastahyökkäykset kirjautumistilanteessa. Järjestelmän tulisi kirjata muistiin onnistuneet ja epäonnistuneet kirjautumisyritykset. Jos järjestelmä havaitsee jonkinlaisen tietoturvamurto-yrityksen, tulisi sen käynnistää välittömästi turvallisuustapahtuma tämän murron estämiseksi. Kirjautuessa järjestelmään ei se saisi näyttää kirjoitettua salasanaa näytöllä. Kun järjestelmään on suoritettu onnistunut kirjautuminen, tulisi sen ilmoittaa edellisen kirjautumisen päivämäärä ja kellonaika ja mahdollisten epäonnistuneiden kirjautumisten ajankohdat. Järjestelmän tulee aikakatkaista istunto, jos se havaitsee, että käyttäjä on ollut epäaktiivinen pitkään järjestelmässä. Tällä tavoin vähennetään riskiä, jolloin luvaton pääsy olisi mahdollinen. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Salasanojen hallintajärjestelmän tulee edellyttää käyttäjältä vahvojen ja turvallisten salasanojen käyttämistä. Tämän hallintajärjestelmän tulee pakottaa käyttämään yksilöllistä käyttäjätunnusta ja salasanaa. Järjestelmä tulee sallia käyttäjien valita ja vaihtaa omat salasanansa itse, mutta sen on valvottava samalla, että salasana on tarpeeksi vahva. Salasanaa luotaessa tai vaihtaessa tulee järjestelmän pyytää kirjoittamaan salasana uudelleen, minkä avulla havaitaan mahdolliset kirjoitusvirheet. Järjestelmän tulee pakottaa käyttäjä vaihtamaan tilapäinen salasana uuteen heti ensimmäisellä kirjautumiskerralla. Lisäksi järjestelmä tulee pakottaa käyttäjä vaihtamaan salasanansa uuteen säännöllisin aikavälein. Järjestelmän tulee myös pitää kirjaa käyttäjän aiemmista salasanoista ja estää käyttämästä vanhoja salasanoja tai vanhoja salasanoja muistuttavia salasanoja uudelleen. Järjestelmä ei saa näyttää salasanaa näytöllä kirjautumisvaiheessa. Salasanat tulee säilyttää järjestelmässä turvallisessa muodossa, jotta niitä ei voida varastaa. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

3.3.3 Fyysinen pääsynhallinta

Yksi fyysisen pääsynhallinnan tärkeitä ehtoja on turva-alue. Turva-alueella estetään luvaton pääsy organisaation alueelle, tietojenkäsittelypalveluihin, prosesseihin ja tietoaineistoihin ja estetään niiden toiminnan häiriintyminen tai vahingoittuminen. Turva-alueet tulee määritellä ja niitä tulee noudattaa paikoissa, joissa on organisaation tietojenkäsittelypalveluita ja arkaluontoista tai kriittistä tietoa organisaation prosesseista tai toiminnasta. Fyysisillä turva-alueilla tulee ottaa huomioon, että turva-alue on selkeästi määritetty ja rajattu. Turva-alueen lujuuden ja sijoituksen tulisi riippua sen alueen sisältämän suojattavan

omaisuuden turvallisuusvaatimusten ja laadittujen riskinarviointitulosten perusteella. Jos alueella on tietojenkäsittelypalveluita sisältäviä rakennuksia, tulee niidenkin sijaita turva-alueen sisäpuolella. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Turva-alueen tulee olla fyysisesti ehjä, eikä se saa sisältää aukkoja, joista olisi mahdollista päästä alueelle. Rakennusten ulkokattojen, seinien ja lattioiden tulee olla lujarakenteisia ja rakennusten ulko-ovien ja ikkunoiden tulee olla aina lukossa. Ulko-ovilla tulee olla jokin turvallisen sisäänpääsyn mahdollistava ratkaisu, kuten esimerkiksi kulunvalvonta, jolla varmistetaan luvallinen pääsy rakennukseen. Rakennuksen vastaanotossa tulisi aina olla päivystäjä. Rakennukseen luvattoman pääsyn estämiseksi voidaan myös rakentaa fyysisiä esteitä mahdollisuuksien mukaan. Jokaisessa turva-alueen palo-ovessa tulee olla hälytin, ja näitä hälyttimiä tulee testata aina tietyin aikavälein. Palo-ovien tulee kuitenkin toimia paloturvallisuussäännösten mukaisesti. Organisaation ulko-oviin, ikkunoihin, tietokonehuoneisiin, viestintähuoneisiin tai muihin tärkeisiin huoneisiin tulisi asentaa murtohälyttimet, ja näitä hälyttimiä tulee testata tietyin aikavälein. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Turva-alueella työskennellessä tulee noudattaa organisaation laatimia turvamenettelyjä. Kun näitä turvamenettelyjä suunnitellaan, tulee ottaa huomioon, että turva-alueella työskentelevät ovat tietoisia turva-alueen olemassaolosta tai sen toiminnasta kaikilta niiltä osin, kun on tarpeen. Tahallisen vahingollisen toiminnan välttämiseksi olisi työskentelyä turva-alueella aina valvottava. Jos turva-alue on miehittämätön, tulisi alueen olla lukittuna ja se tulisi tarkastaa säännöllisesti. Kameroiden tai muiden tallennuslaitteiden käytön alueella tulisi olla kielletty ilman erillistä lupaa. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Turva-alueille pääsy tulee suojata kulunvalvonnalla. Kulunvalvonta varmistaa, että alueelle pääsevät vain luvan saaneet henkilöt. Kulunvalvonnassa tulee ottaa huomioon seuraavia asioita: Vierailijoiden saapuessa alueelle tulee kirjata heidän saapumisensa ja poistumisensa ajankohta ja päivämäärä. Kaikkia vierailijoita alueella tulee valvoa, jos heidän saapumistaan alueella ei ole ennalta jo hyväksytty. Vierailijat tulee perehdyttää alueen turvallisuusvaatimuksiin ja siihen, kuinka toimitaan hätätilanteen sattuessa. Vierailijan henkilöllisyys tulee todistaa, ennen kuin hänelle voidaan antaa kulkulupa alueelle. Pääsy sellaisille alueille, joilla varastoidaan ja käsitellään luottamuksellista tietoa, tulee rajoittaa esimerkiksi kaksivaiheisen todennusmenetelmän avulla. Kaksivaiheisessa todennusmenetelmässä tunnistautumiseen tarvitaan kulkuluvan lisäksi myös tunnusluku. (SFS27002, Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017.)

Tietoturvallisuuden kannalta voi joskus olla välttämätöntä valvoa alueita kameravalvonnan avulla. Kameravalvonta ei kuitenkaan aina ole mahdollista, koska laki määrittää, milloin kameravalvonta on sallittua ja milloin ei. Jos nämä lakipykälät eivät täyty, voi organisaatio syyllistyä salakatseluun ja myös salakuunteluun, jos kamera tallentaa myös äänen. Kameravalvontaa käytetään yleensä sellaisissa paikoissa, jossa kulunvalvonta on todella tärkeää, ja sen avulla voidaan myös selvittämään myöhemmin mahdolliset luvattomat sisäänpääsyt ja muut väärinkäytöstilanteet. Kameravalvonnan voi myös liittää osaksi kulunvalvontaa, millä saadaan nostettua alueen turvallisuutta. Lähtökohta luvalliselle kameravalvonnalle on se, että sillä pyritään estämään omaisuuteen kohdistuvia rikoksia. Kameravalvonnan tallenteita saa käyttää vain niihin tarkoituksiin, joita varten kameravalvontaa suoritetaan. Sen jälkeen, kun kameravalvonnan tallenteita ei enää tarvita tai kun nauhoituksesta on kulunut yli vuosi, tulee ne tuhota asianmukaisella tavalla. (Laaksonen 2006, 52-53.)

4 TIETOTURVAHYÖKKÄYKSET

Nykymaailma on verkottunut teknologian myötä hurjaa vauhtia, ja sen myötä tietoturvaongelmat ovat yleistyneet. Tietoturvahyökkäyksiä tehdään monien organisaatioiden ja yksityisten ihmisten verkkolaitteisiin, ja yleisin motivaatio näissä on taloudellinen hyöty hyökkääjälle. Check Point -tietoturvayhtiön tietoturvatutkimuksen mukaan kolme neljästä hyökkäyksestä alkaa sähköpostin mukana saapuneesta tiedostosta. Toisessa Check Pointin tekemässä tutkimuksessa selvisi, että noin 39 prosenttia hyökkäyksistä päätelaitteille tunkeutui verkon palomuurin läpi. Näiden tutkimusten myötä tehtiin johtopäätös, että tietoturvan säilymiseksi tulee sen perustua mahdollisimman hyvään tietoturva-arkkitehtuuriin, jonka osina ovat kehittyneempi uhkientorjunta, mobiililaitteiden tietoturva ja organisaation kriittisten paikkojen eristäminen toisistaan. (Uusi teknologia 2016).

Tietoturvan arkkitehtuuri ja infrastruktuuri vaikuttavat juuri siihen, onko organisaatio mahdollinen hyökkäyskohde. Hakkerit usein käyttävät erilaisia automaattisia työkaluja, jotka skannaavat ja tunnustelevat verkkoa ja joiden avulla he sitten valitsevat mahdollisen hyökkäyskohteensa. (Thomas 2005, 9.) Tämän vuoksi tietoturvan kehittäminen ja parantaminen pienentävät tietoturvahyökkäysten riskiä, vaikkei uhkaa kokonaan poistakkaan.

4.1 Hyökkäystyypit ja tavat

Tietoturvaa uhkaavia hyökkäystapoja on monta erilaista, vaikka suurin osa hyökkäyksistä kumminkin tapahtuu sähköpostin kautta joko kalastelulla, urkinnalla tai haittaohjelmilla. (Uusi teknologia 2016.) On myös olemassa tapoja, joihin ei liity tekninen tietokoneosaaminen ollenkaan, vaan huijataan uhri antamaan yksityisiä tietoja, kuten salasanoja sekä käyttäjänimiä. (Norton 2020.) Lisäksi on hyökkäysmenetelmiä, joissa ei koiteta ryöstää tietoja vaan estää tai hidastaa palvelun toiminta kokonaan. Joissakin tapauksissa hyökkäys poistaa osan tiedostoista ja pahimmissa tapauksissa jopa kaikki tärkeät tiedostot kokonaan (Suomen internet opas 2005).

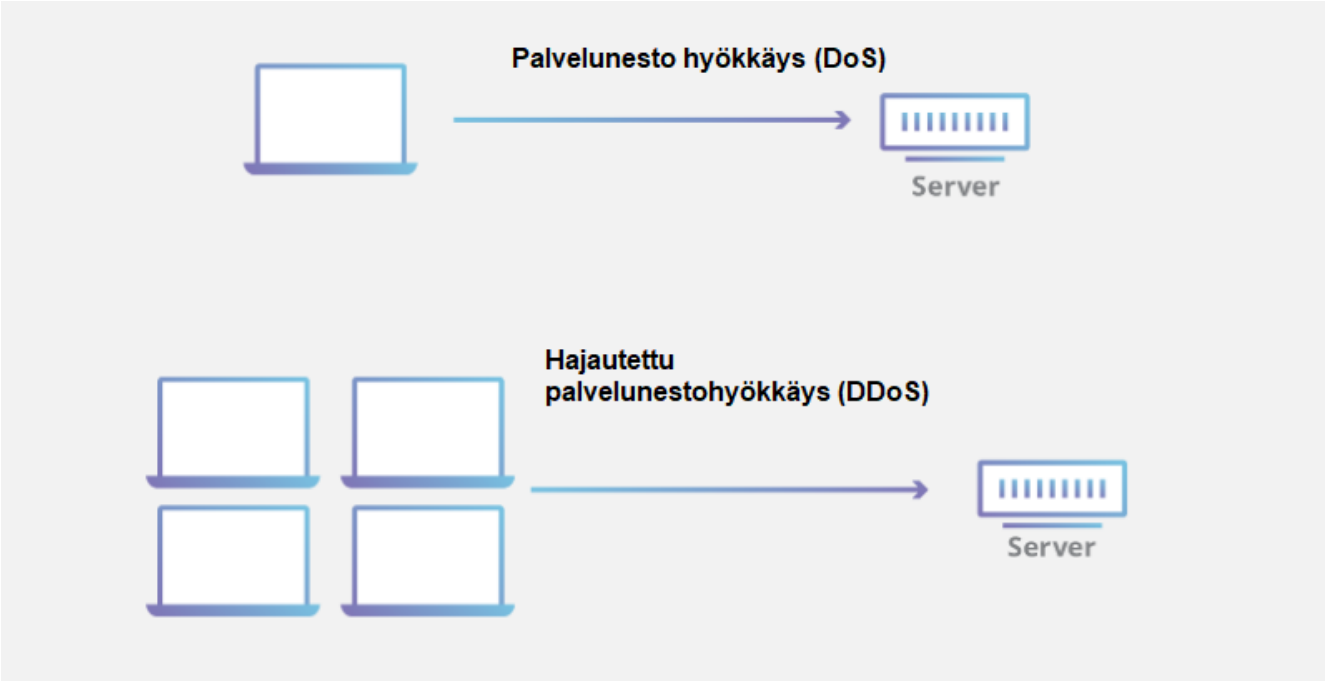
Organisaation henkilöstöä kouluttamalla ja perehdyttämällä tietoturva-asioihin paremmin voidaan pienentää kalastelun ja huijausten onnistumisen riskiä. Myös uusien palomuurien ja tietoturvasovellusten

asennus nostaa tietoturvaa organisaatiossa. (Norton 2020.) Tietoturvastandardien mukaiset menetelmät ovat ohjeistava apu siihen, miten uhkia vastaan kannattaa menetellä organisaatioissa.

4.1.1 Palvelunestohyökkäys

Palvelunestohyökkäys, eli niin sanottu DoS (Denial of Service) hyökkäys on verkkohyökkäystapa, jossa organisaation tai vastaavan verkkosivuille tehdään samanaikaisesti paljon liikennettä niin, että palvelu ei toimi, koska se tukkeutuu ja joissakin tapauksissa kaatuu kokonaan. Jos hyökkäys tehdään monelta eri päätteeltä, käytetään nimitystä DDoS (Distributed Denial of Service). Hajautetussa hyökkäyksessä käytetään hyväksi useita kaapattuja tietokoneita tai verkkolaitteita, joista käytetään taas nimitystä botti-verkosto. Lähes mikä tahansa verkkoa käyttävä laite voi kuulua omistajan tietämättä tällaiseen verkostoon, ja hyökkäys on paljon vaikeampi torjua, koska hyökkäyksiä tulee tällöin monista eri IP-osoitteista samaan aikaan. Kuvassa 2 esitellään yksinkertaistettuna molemmat hyökkäystavat. (Kataja 2015).

Palvelunestohyökkäyksiä vastaan voidaan suojautua esimerkiksi Anti-DoS palveluilla ja teknologialla. Tällaiset palvelut tunnistavat ja erottavat palvelunestohyökkäykset normaalista verkkoliikenteestä ja täten nopeuttavat sen estämistä. Hyökkäystä vastaan suojaudutaan myös ottamalla yhteyttä internetin palveluntarjoajaan ja pyytämällä verkkoliikenteen uudelleenreitittämistä. Myös palomuurien ja reitittimien päivittäminen ja konfigurointi niin, että väärä verkkoliikenne ohjautuu pois, vaikeuttaa palvelunestohyökkäyksen mahdollisuutta. Samoin kannattaa pitää käyttöjärjestelmät ja tietoturvaohjelmat ajan tasalla. (Norton 2020).



KUVA 2. Denial of Service ja Distributed Denial of Service hyökkäys (Mukaillen Cloudflare 2020)

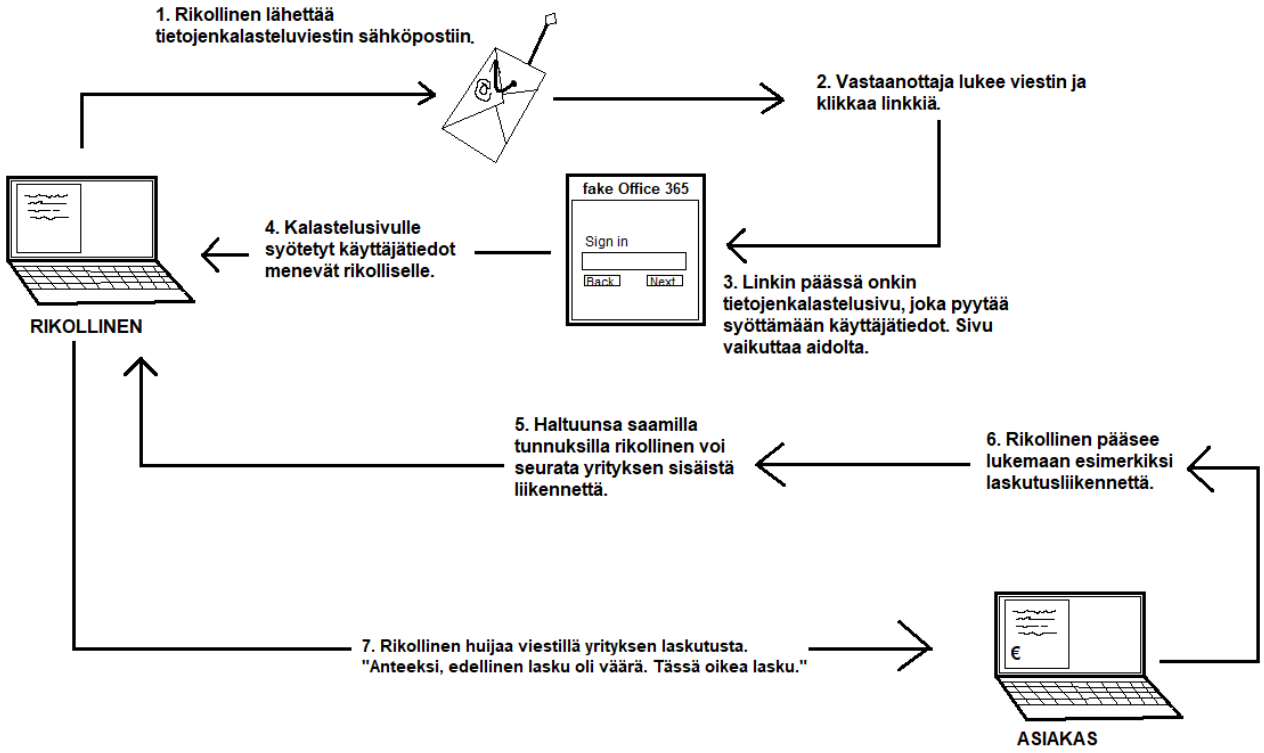
4.1.2 Tietojenkalasteluhyökkäys ja urkinta

Tietojen kalastelu on yksi yleisimmistä tietoturvaloukkaustavoista. Tietojen kalastelussa uhria koitetaan huijata antamaan käyttäjänimi sekä salasana erilaisilla kalastelusivustoilla (Phishing Kit). Tällainen kalastelusivusto on hakkerin luoma www-sivupaketti, joka näyttää aidolta esimerkiksi sähköpostin kirjautumissivulta, mutta todellisuudessa lähettää kirjautumistiedot hakkerille, kun ne sivulla annetaan.

Tietojenkalastelu tapahtuu sähköpostin välityksellä, eli uhrille saapuu sähköposti luotettavalta taholta, kuten oman organisaation sisältä tai toisesta, tutusta organisaatiosta. Vastaanotettu viesti on todella aidon tuntuinen ja sisältönä on yleensä jokin tiedostolinkki tai turvapostilinkki, jonka avattua uhri ohjautuu kalastelusivustolle. Hyökkääjän tavoite on siis saada uhri kirjoittamaan tietonsa tälle sivustolle. Kalastelusivustoja on tehty melkein jokaiselle pilvialustalle, mutta organisaatioihin tehdyt hyökkäykset kohdistuvat usein Office 365- tai Google-palveluihin. Kuvio 4 esittää Office-365 huijauksen vaiheet. (Tietosuojavaltuutetun toimisto. 2020.)

Onnistuneella kalasteluhyökkäyksellä rikollisella on tiedossa kohteen sähköpostin ja siihen liitettyjen pilvipalveluiden ja muiden vastaavien sisältö. Tästä syystä tietojen kalastelua organisaatioissa kannattaa

estää kehittämällä pilvipalveluihin kirjautumista ja valvontaa sekä myös hyödyntämällä niiden lokitus-ominaisuuksia. Myös täytyy suunnitella sekä miettiä, mitä arkaluontoista tietoa sisältäviä dokumentteja ja tiedostoja kannattaa säilyttää ja välittää sähköpostin välityksellä. (Tietosuojavaltuutetun toimisto. 2020.)



KUVIO 4. Office 365 kalastushuijauksen vaiheet. (Mukaillen Kybersää Joulukuu 2019)

4.1.3 Haittaohjelmat

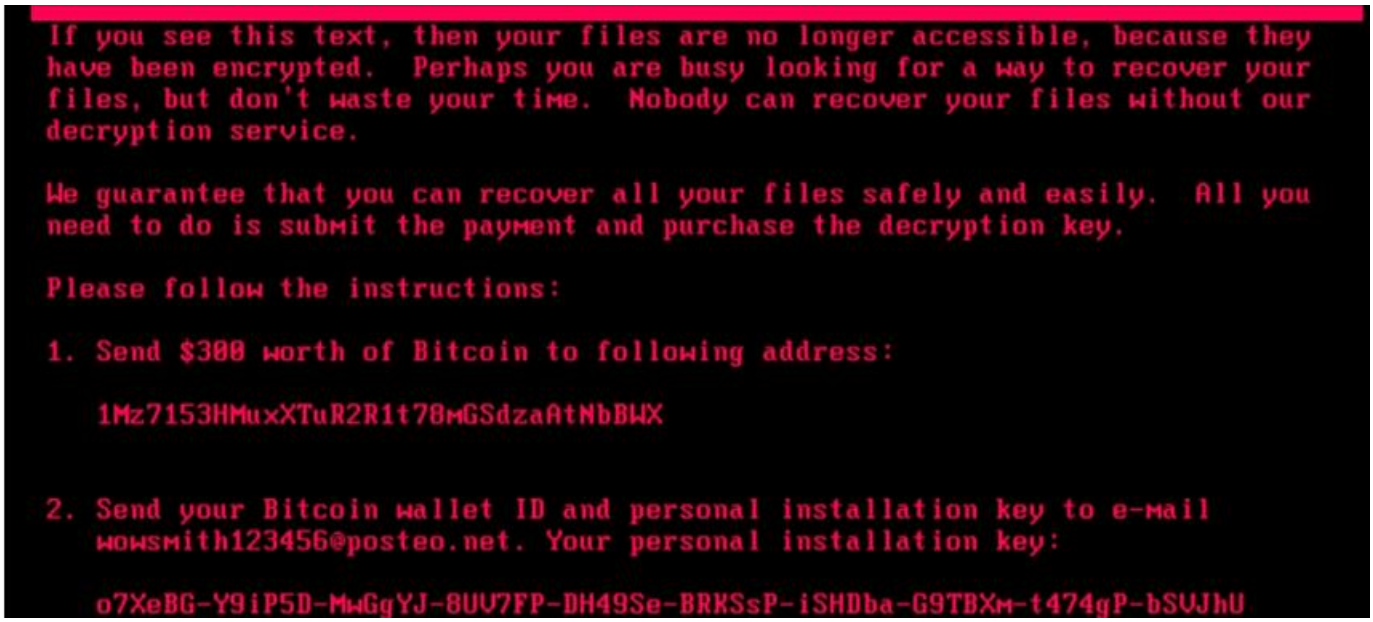
Haittaohjelmat (Malware) ovat yleiskäsite erilaisille tietokoneelle tai muille älylaitteille suunnatuille haittaohjelmille, jotka jollain tavalla aiheuttavat haittaa tai harmia sen käyttäjälle. Tällaisilla ohjelmilla on päämääränä joko vain haitata käyttäjää, vakoilla ja kalastella siltä yksityistietoja tai jopa kiristää käyttäjältä rahaa. (If 2020).

Vakoiluohjelmat (Spyware) ovat haittaohjelmia, jotka keräävät arkaluontoista tietoa uhriltaan. Tämä tieto voi olla esimerkiksi Internet-sivustoja, joita on selattu, sähköpostiosoitteita, salasanoja ja luotto-korttitietoja. Vakoiluohjelmat asentuvat laitteeseen yleensä aina ilman käyttäjän lupaa ja usein vielä jon-kin hyödyllisen ilmaisohjelman lisänä. (Vakoilu ohjelmat. 2019).

Kiristysohjelmat (Ransomware) ovat haittaohjelmia, jotka lukitsevat ja samalla estävät tietokoneen tai laitteen käytön. Ohjelma tämän jälkeen vaatii jonkin tietyn rahasumman, että se ”vapauttaisi” tietokoneen ja mahdollistaisi käytön jälleen. (If 2020.) Vuonna 2017 levisi maailmalla WannaCry niminen kiristysohjelma. WannaCry käyttää hyväkseen SMB-haavoittuvuutta, joka on Windowsin järjestelmissä. Tämän jälkeen se skannaa, onko laitteesta yhteyksiä muihin tietokoneisiin esimerkiksi lähiverkon läpi. Portti, jota se skannaa, on TCP-portti 445. WannaCry salaa ja lukitsee kohteensa ja pyytää lunnaiksi 300 tai jopa 600 dollarin rahamäärää, kuten kuvasta 4 huomaa. (Virtanen. 2017.)

Tietokonevirukset ovat pieniä haitallisia ohjelmia, jotka leviävät tietokoneesta toiseen sähköpostin liitetiedoston, Internet-selaimen tai erilaisten massamuistilaitteiden välityksellä. Viruksia on useita alatyyppejä, mutta yleisimpiä PC-laitteille ovat esimerkiksi makrovirukset tai käynnistyslohkovirukset. Käynnistyslohkovirus on virustyyppi, joka kopioi itsensä tietokoneen käynnistyslohkoon, makrovirus on taas jonkin tietokonesovelluksen, esimerkiksi Wordin avulla tehty makrokielellä. Virukset toimivat yleisesti samalla tavalla: ne kopioivat ja levittävät itseään ja jotkin virukset vielä voivat ”aktivoitua” leviämisen jälkeen. Virukset hidastavat tietokonetta, ja pahimmissa tapauksissa vahinko mitä virus voi saada aikaan on tietojen poistaminen tietokoneesta ja sen kiintolevyistä. (Suomen Internetopas. 2005.)

Parhaiten erilaisilta haittaohjelmilta voi suojautua olemalla varovainen ja pitämällä tietoturvaohjelmat ajan tasalla. Haittaohjelmia voi tarttua tietokoneisiin ja verkkolaitteisiin sähköpostin mukana tulleesta liitetiedostosta tai väärän linkin klikkaamisella epämääräisellä sivustolla. Tämän vuoksi huolellisuus on yksi isoin tekijä haittaohjelmilta suojautumisessa. (Viestintävirasto. 2016.)



KUVA 3. Kuvakaappaus kiristysohjelma Petya:sta (Niemi 2017)

KUVA 4. Kuvakaappaus kiristysohjelma WannaCry:stä (Latto 2020)

4.1.4 Host scanning/Port scanning

Host scanning tai Port scanning on tapa, jossa kohteen verkkoa ja siihen liitettyjä tietokoneita ja laitteita skannataan avoimien tietoliikenneporttien, ohjelmien ja käyttöjärjestelmien haavoittuvuuksia etsien. Tässä tavassa käytetään siihen laadittua ohjelmaa, joka laatii raportin skannauksen kohteesta ja mahdollisista tietoturva-aukoista. Tässä siis ei tehdä vielä varsinaista tunkeutumista, mutta kohde skannataan, jotta löytyisi mahdollisuus siihen ja se lasketaan tietomurron yritykseksi. Porttiskannausta voidaan käyttää myös luvallisessa mielessä, kuten järjestelmien turvallisuusjärjestelyiden selvitykseen. (Kurittu 2017). Tällaisia luvallisia sovelluksia on esimerkiksi F-Securen Radar palvelu.

Porttiskannailua voi ennaltaehkäistä ja siltä voi suojautua pitämällä tietoturvalaitteet ja ohjelmistot ajan tasalla ja aktiivisesti valvomalla, ja ylläpitää niitä. Lokien ja muiden vastaavien työkalujen hyödyntäminen edistää riskien havainnointia ja täten ennaltaehkäisee myös mahdollisia laittomia skannauksia. Tietoturva ei ole pelkkä ohjelmistotuote vaan se on myös tapa toimia uhkia vastaan. (Kurittu. 2017.)

4.1.5 Social Engineering

Social Engineering on tapa, jossa uhria huijataan antamaan arkaluontoista tietoa esimerkiksi esiintymällä IT-tukena tai vastaavana uhrille. Toinen tapa on, että jätetään USB-tikku täynnä haittaohjelmia sellaiseen paikkaan, josta potentiaalinen uhri sen löytäisi. Tällaiseen USB-tikkuun voidaan myös kirjoittaa jotain sellaista, joka houkuttelee sen löytäjää tutkimaan, mitä siinä on, esimerkiksi ”Salaista” tai ”Tärkeää”. Tässä huijaustavassa siis käytetään hyväksi uhrin hyväuskoisuutta ja ymmärtämättömyyttä. Taidokkaat huijaukset voivat saada kohdeuhrin tietämättään antamaan arkaluontoisia tietoja, mikä lopulta johtaa vakavaankin tietomurtoon hyödyntämällä saatuja tietoja. (Norton. 2020).

Social Engineering huijauksia voi ennaltaehkäistä ja niitä vastaan voi suojautua kouluttamalla organisaation henkilöstöä olemaan varovaisia ja pitämällä tietoturvan tasoa korkealla. Organisaation henkilöstön täytyy olla tietoinen siitä, millaista tietoa voi jakaa ja kenelle. Tuntemattomalta työpaikan henkilöltä saatu epämääräinen viesti tai puhelu ei välttämättä ole täysin luotettava, sellaisena esiintyminen on yllättävän helppoa. Vastaavasti myös tuntemattomia USB-tikkuja tai vastaavia löytyneitä laitteita ei kannata käyttää. Vain luotettavat ja tunnetut laitteet ovat käyttökelpoisia, jottei tietomurtoa pääsisi tapahtumaan. (Norton. 2020.)

4.2 Tietoturvahyökkäykset maailmalla

Kyberuhka on globaali ja huomionarvoinen käsite. Tietoturvahyökkäyksien kohteena voi olla mikä tahansa organisaatio tai henkilö, missä päin maailmaa tahansa. Hyökkääjän motiivina voi olla taloudellinen hyöty, esimerkiksi kiristysohjelmien avulla tai organisaation verkon haavoittuvuuksien hyväksikäytön kautta. Esimerkkinä WannaCry:n ilmestyminen vuonna 2017 kun kaikki organisaatiot tai yritykset eivät olleet päivittäneet kiristysohjelman käyttämää haavoittuvuutta. (Virtanen 2017.) Kohteena hyökkääjillä ovatkin yleensä sellaiset organisaatiot, joilla on huono tietoturva ja tietoturvaosaaminen. Hyvää osaamista edellyttää taas koulutus ja kokemus alalla, joita ei ihan joka paikasta maailmaa taas löydy.

Viisi suurinta kyberuhkaa tällä hetkellä ovat haavoittuvuuksien hyväksikäyttö, tietojen kalastelu, kiristyshyökkäykset, epäselvä vastuunjako ja organisaatioiden osaamattomuus hallita kyberriskejä. Myös erilaiset poliittiset tilanteet maailmalla kasvattavat kyberiskun mahdollisuuksia. Esimerkiksi Iranin ja Yhdysvaltojen välien kiristyminen Lähi-idässä voi johtaa kyberiskuun Iranin puolelta vastakeinona Yhdysvaltojen toimiin sen alueella. (Kybersää Joulukuu. 2019.)

Japanissa yksi maailman suurimpia elektroniikkaosia ja laitteita valmistava organisaatio Mitsubishi Electric koki merkittävän tietomurron kesäkuussa 2019. Paikallisten uutistoimistojen, Asahi Shimbun ja Nikkein, mukaan hyökkäys sai alkunsa Kiinassa olevilta kumppaneilta, joista se levisi Japanissa oleviin yksiköihin ja tunkeutui yhtiön tietoverkkoon päästen jopa 14 eri osaston tietoihin, kuten myynnin- ja päähallinnon tietoihin. Uutistoimistojen mukaan hyökkääjänä oli Kiinaan sidoksissa oleva kybervakoiluryhmä nimeltään Tick. (Cimpanu. 2020.) Amerikkalainen tietotekniikan yhtiö Microsoft otti haltuunsa noin 50 pohjoiskorealaisten hakkereiden käyttämiä verkkotunnusta, jotka oli tehty jäljittelemään Microsoftin omia palveluita. Näiden tunnuksien avulla koitettiin kalastella kohdistetusti tiettyjä Microsoftin asiakkaita ja saada haltuun tärkeitä käyttäjätietoja. (Kybersää joulukuu. 2019.)

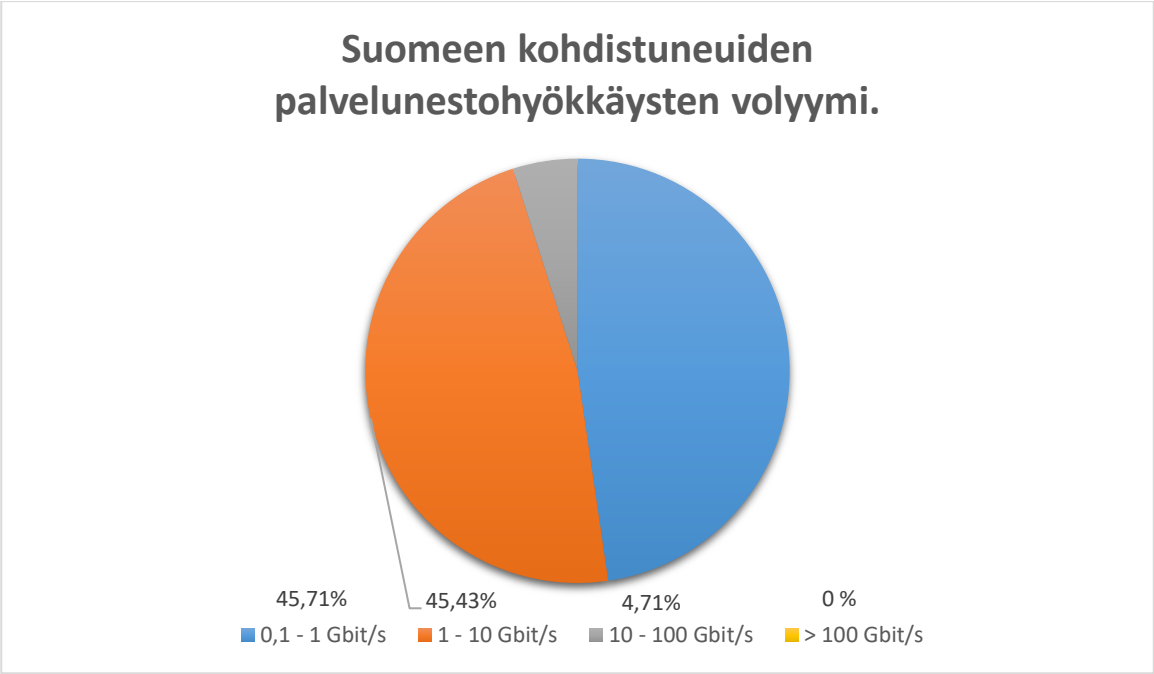
4.3 Tietoturvahyökkäykset Suomessa

Suomessa tämänhetkiset yleisimmät tietoturvauhat ovat lähinnä tietojen kalastelu- ja erilaiset huijausyritykset. Office 365 palveluun perustuva kalasteluhuijaus on yleinen riesa suomalaisissa organisaatioissa ja johtaa edelleen tietomurtoihin lähes joka päivä (Kybersää joulukuu. 2019.) Myös haittaohjelmien lisääntymistä on havaittu Suomessa ja maailmalla, muun muassa QSnatch haittaohjelma on saas-

tuttanut verkkotallennuslaitteita ainakin vuoden verran. QSnatch haittaohjelma on suomalaisten havaitsema haittaohjelma, jonka kyberturvallisuuskeskuksen asiantuntijat olivat löytäneet lokakuussa 2019. Tämä kehittynyt haittaohjelma varastaa tunnuksia ja salasanoja, mikä mahdollistaa pääsyn laitteelle tallennettuun arkaan dataan. Suomessa näitä QSnatch havaintoja oli päivittäistasolla noin 200. (Kybersää lokakuu. 2019.)

Palvelunestohyökkäyksiä Suomessa havaitaan liki päivittäin, volyymiltään yli 10 Gbit/s kokoisena. Suurin osa näistä on noin 1–15 minuutin kestoisia. Muuten palvelunestohyökkäysten tilanne Suomessa on pysynyt kohtuullisen rauhallisena, minkä voi havaita kuviosta 5 ja 6, missä kuukauden tilanne esitetään graafisesti. Traficomin arvion mukaan suurin osa palvelunestohyökkäyksissä käytetyistä bottiverkoista toimii kodin verkkolaitteilla ja IoT laitteilla, mistä syystä kuluttajien olisi hyvä alkaa kiinnittämään huomiota internetiin kytkettyjen laitteiden tietoturvaan jo, kun laitetta valitaan käyttöön. (Kybersää marraskuu. 2019.)

KUVIO 5. Palvelunestohyökkäysten kesto Suomessa. (Mukaillen Kybersää marraskuu 2019)



KUVIO 6. Palvelunestohyökkäysten volyymi Suomessa. (Mukaillen Kybersää marraskuu 2019)

Suomen kyberturvallisuuskeskuksella on ollut käytössä HAVARO vuodesta 2011 asti. HAVARO on tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä, eli tutkiva sensoriverkosto, joka havaitsee ja löytää vakavia tietoturvauhkia. HAVARO:n avulla eri organisaatioiden verkkoliikenteestä voidaan tunnistaa vahingolliseksi tunnistettua tai tavallisesta poikkeavaa liikennettä ja täten suojautua tietoturvauhkilta ja rajoittaa vahinkoja. (Traficom 2016.)

4.4 Tietoturvahyökkäyksen vaikutus organisaatioon

Tietoturvahyökkäykset ovat merkittävä uhka organisaatiolle, sen taloudelle ja toiminnalle. Tietoturvaan täytyisi organisaatiossa aina panostaa, mikäli riskiä tietoturvaloukkaukselle halutaan pienentää. Tietoturvan eteen täytyy tehdä koko ajan töitä, se täytyy ottaa vakavasti joka päivä ja ihmisiä täytyy kouluttaa säännöllisesti sen tiimoilta. Suomeen ja Suomessa oleviin organisaatioihin kohdistuu melko vähän tietoturvahyökkäyksiä, mutta maailmanlaajuisen trendin mukaisesti on täälläkin nähty viime vuosina vakavia tietojenkalasteluhyökkäyksiä. (Viitaila 2019.)

Onnistunut tietoturvahyökkäys voi lamauttaa organisaation toimintaa ja pysäyttää esimerkiksi tuotantoa tai palvelua johtaen suuriin taloudellisiin tappioihin. Organisaatioon kohdistuneessa onnistuneessa tie-

tokalastelussa voi paljastua arkaa tietoa, jota voidaan käyttää esimerkiksi teollisuusvakoiluun tai vastaavaan rahalliseen hyötyyn. Esimerkkinä lamauttavasta hyökkäyksestä on, kun Kokemäen kaupunki joutui palvelunestohyökkäyksen uhriksi ja sen sähköiset palvelut poistettiin tilapäisesti kokonaan käytöstä pois. Hyökkäyksen takia kaupungin maksu- ja sähköpostiliikenne olivat poistuneet käytöstä kokonaan, mikä taas johti ongelmiin sosiaalihuollon kautta maksettavissa toimeentulotuissa. (MTV uutiset 2019.)

Organisaation tietoturvan ylläpitämiseksi ja riskien hallittu kontrollointi vaatii ns. tietoturvahygienian osaamisen, eli tietoturvan perusasiat. Tällaista on muun muassa käyttäjätunnuksien turvallinen suojaus, sähköpostien ja verkkoselainten suojaus ja turvallinen käyttötapa ja ohjelmistojen päivitysten asentaminen heti kun mahdollista. Lisäksi organisaation henkilön koulutus ja tietoturvaosaamisen ylläpito on tärkeää. Kyberhyökkäyksissä rikolliset osaavat käyttää hyväksi sellaisia tilanteita, joissa ihminen tekee päätökset ja arviot. (Viitaila 2019.)

5 TYÖN TOTEUTUS JA TULOKSET

Opinnäytetyön käytännön osuuteen kuuluvien standardien vertailujen CABB Oy:n tietoturvakäytäntöihin ja verkkojen skannauksesta saadut tulokset ovat salaista tietoa, josta emme voineet opinnäytetyön julkiseen osuuteen kirjoittaa. Pohdimme seuraavaksi kuitenkin yleisesti työn etenemistä, miten työ onnistui ja millaisia haasteita kohtasimme tehdessämme tätä työtä.

5.1 Työn eteneminen

Työ alkoi siitä, kun sovimme tapaamisen CABB Oy:n edustajan Jukka Häkkilän kanssa. Keskustelimme yhteisesti siitä, mitkä olisivat opinnäytetyön keskeiset lähtökohdat, jota lähdetään tutkimaan. Työn tavoitteena oli tutustua yleisesti tietoturvastandardeihin ja sen jälkeen verrata niitä CABB Oy:n tietoturvakäytäntöihin ja tutkia, miten heidän käytäntönsä eroavat standardien ohjastamista käytännöistä. Opinnäytetyöhön haluttiin lisäksi myös tuoda tietoturvaskannaus, joka tehtäisiin CABB Oy:n automaatioverkkoihin. Tämän skannaus suoritettiin yhdessä Centrian-Ammattikorkeakoulun Pietarsaaren yksikön kanssa ja apunamme skannauksessa oli Tom Tuunainen, joka työskentelee TKI-kehittäjänä Centrian-Ammattikorkeakoulun Pietarsaaren yksikössä. Lisäksi toimeksiantaja ehdotti, että jakaisimme työt kolmeen eri vastuualueeseen. Sovimme, että Vili Pokela vastaa skannauksesta ja automaatioverkkojen rakenteen tutkimisesta, Niko Tuikka vastaa tietoturvastandardien tutkimisesta ja niiden vertaamisesta CABB Oy:n tietoturvakäytäntöihin ja Erno Kattilakoski vastaa tietoturvahyökkäystapojen tutkimisesta.

Sovimme suoritettavan skannauksen ajankohdaksi maaliskuun, mutta skannaus kuitenkin hieman viivästyi, sillä Koronavirus aiheutti vierailukiellon koko Kokkolan tehdasalueelle. Pidimme aiemmin sovittuna ajankohtana Skype-palaverin, jossa sovimme, että skannaus suoritettaisiin etänä. Toimitimme skannauskoneen CABB Oy:lle ja he kytkivät sen heidän verkkoonsa itse. Skype-palaverissa haastattelimme myös CABB Oy:n työntekijöitä Taneli Känsäkangasta ja Sami Långia CABB Oy:n tietoturvakäytännöistä ja vertasimme heidän käytäntöjään standardeihin.

5.2 Työn tulokset standardeista

Tietoturvastandardien vertailusta CABB Oy:n tietoturvakäytäntöihin saimme seuraavanlaisia tuloksia: Tietoturvariskien arviointia painotetaan standardeissa erittäin tärkeänä. Tällä tavoin arvioidaan koko ajan tietoturvallisuuden hallintajärjestelmän toimivuutta ja kartoitetaan riskien todennäköisyyttä ja niistä mahdollisesti aiheutuvia tuhoja ja tappiota. Standardit painottavat lisäksi dokumentoidun tiedon laatimisen ja säilyttämisen tärkeyttä. Jokaisesta tietoturvallisuuden hallintajärjestelmän eri osa-alueesta tulisi standardien ohjeistamana säilyttää ja ylläpitää dokumentoitua tietoa.

Tietovälineiden käsitteleminen ja tuhoaminen turvallisesti ja asianmukaisesti on myös standardien ohjeistuksen mukaan todella tärkeää, ettei tärkeää salaista tietoa pääse vuotamaan julkiseksi tai ettei tärkeää tietoa tuhoudu. Tietoturvallisuudesta standardit painottavat myös sekä fyysisen että sähköisen pääsynhallinnan tärkeyttä. Fyysisellä pääsynhallinnalla tarkoitetaan kulunvalvontaa, turva-alueen rajausta ja ylläpitoa ja tärkeiden ovien lukitsemista. Sähköinen pääsynhallinta tarkoittaa taas salasanakäytäntöjä, tietojen salausta ja sitä, että sallitaan pääsy vain sellaisiin verkkoihin ja verkkopalveluihin, jota työntekijä tarvitsee oman työtehtävänsä suorittamiseen.

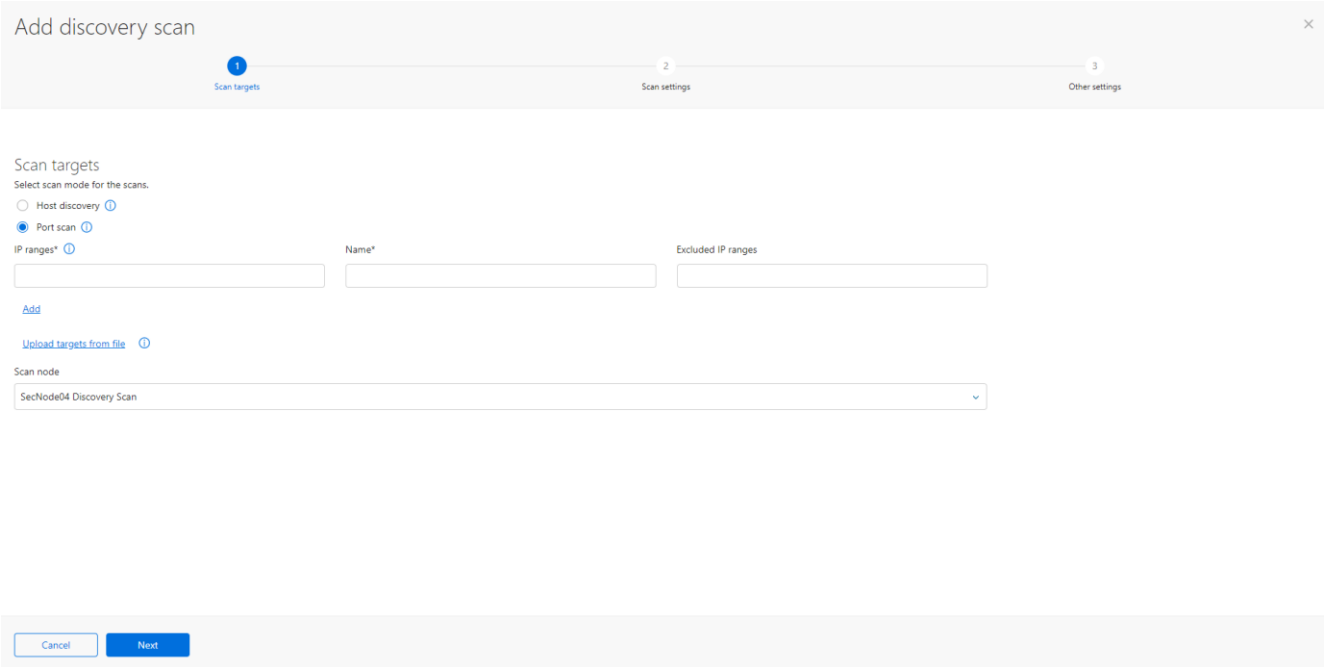
Hallintajärjestelmien ylläpitoa ja parantamista varten standardit ohjeistavat, että organisaatio nimittää vastuuhenkilöt tai vastuuryhmän, joka huolehtii tietoturvapoikkeamista ja siitä, että organisaation tietoturvan hallintajärjestelmää parannetaan jatkuvasti mahdollisuuksien mukaan.

5.3 Työn tulokset skannauksesta

Skannaustyö aloitettiin 14.4.2020, kun Taneli Känsäkangas oli saanut kytkettyä Linus-pohjaisen skannaustietokoneen CABB Oy:n verkkoon. Kun tietokone oli saatu kytkettyä verkkoon, se automaattisesti päivitti itsensä ja oli sitten heti käyttövalmiina. Tarkoituksena oli skannata kahdesta eri verkosta portit ja haavoittuvuudet tällä tapaa löydämme mahdolliset tietoturvariskit ja heikkoudet, joista mahdollinen hyökkääjä voisi koittaa tunkeutua verkkoon. Kun skannaustietokone oli kytketty piuhalla CABB Oy:n verkkoon, pystyimme käynnistämään etäyhteydellä skannauksen verkosta F-Secure Radar -sovelluksen

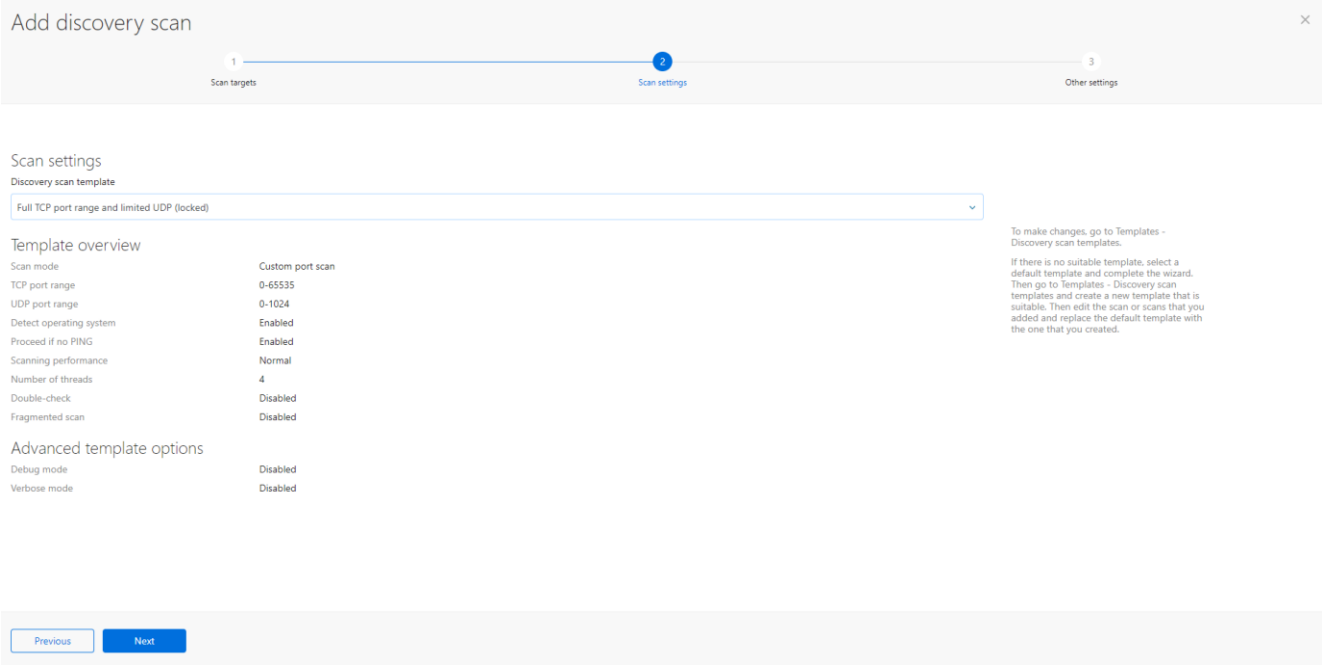
kautta. Tarkoituksena oli ensin skannata heidän toinen ei niin tärkeä verkko, jotta näemme, onnistuuko skannaus toivotulla tavalla.

Kun aloitetaan uusi skannaus, Radariin luodaan uusi discovery scan (KUVA 5), johon syötetään yrityk-seltä saadut IP-osoitealueet. Valitaan Port scan -valinta ja syötetään IP-osoite IP-ranges kohtaan. Tämän jälkeen nimetään projekti ja valitaan haluttu Scan node, joka sisältää tietokannat tunnetuista tietoturva-riskeistä. Skannaus vertaa saatuja tuloksia tähän tietokantaan ja hakee tietokannasta tarvittavat korjaavat toimenpiteet tietoturvariskin korjaamiseksi.



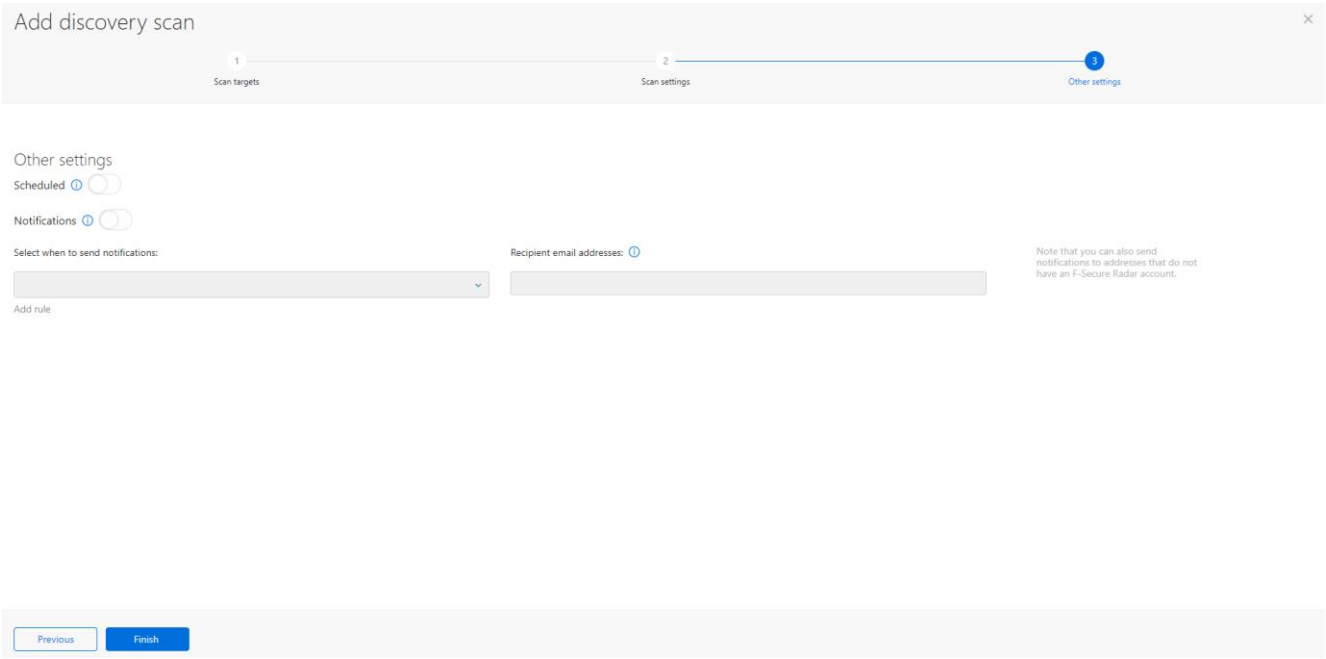
KUVA 5. Skannauksen IP-osoitealueiden määrittäminen.

Seuraavaksi määritetään skannauksen asetukset (KUVA 6). Käytimme skannauksessa valmiiksi luotuja asetuksia ”Full TCP port range and limited UDP (locked)”. Tämä esiasetus määrittää TCP ja UDP-porttien skannausalueet.



KUVA 6. Skannauksen asetuksien määrittäminen.

Viimeisessä kohdassa voidaan määrittää skannauksen aloituksen ajankohta ja lisätä ilmoituksia skannauksen vaiheista (KUVA 7). Määritetyt ilmoitukset lähetetään sähköpostiin. Tämän jälkeen voidaan aloittaa skannaus.



KUVA 7. Skannauksen lisäasetusten määrittäminen.

F-Secure Radarissa on kaksi erilaista skannausosiota. Ensimmäinen osio on Discovery Scan, jonka tehtävänä on skannata portit ja ilmoittaa tulokset sitten erillisenä Excel-tiedostona. Toinen osio on nimeltään Vulnerability Scans, joka sitten skannaa verkon haavoittuvuuksia. Se tekee näistä sitten yhteenvedon Word-tiedostoon, josta on nähtävissä haavoittuvuudet ja näihin mahdolliset korjaukset.

Ensimmäinen verkko, jota aloitimme skannaamaan, oli vain yleinen verkko. Tästä verkosta on pääsy ulkomaailmaan ja näin varmistimme, että jos skannauksessa tapahtuu jotain, se ei vaikuta tuotantoon millään tavalla. Ensin aloitettu skannaus kesti noin yhden päivän ja 15 tuntia skannauksen pituus riippuu hyvin paljon siitä, paljonko skannattavia alueita on. Täältä löytyi muutama tietoturvariski, johon Radar sitten heti tarjosi mahdollisia korjauksia.

Kun ensimmäinen skannaus oli lähtenyt hyvin käyntiin ilman mitään virheitä, käynnistimme toisen skannauksen, joka sisälsi sitten servereitä ja Clientteja. Tässä verkossa oli enemmän skannattavaa, joten

skannaus kesti noin kaksi päivää. Täältäkin löytyi muutamia haavoittuvuuksia ja pari informatiivista asiaa, joihin Radar ilmoittaa mahdolliset korjaustavat.

Kun skannaukset oli saatu hoidettua kunnolla loppuun ilman ongelmia, jotka vaikuttaisivat prosessin kulkuun, Taneli Känsäkangas pyysi, voisimmeko skannata vielä yhden heidän verkkonsa. Tämän viimeisimmän verkon skannauksessa ei mennyt kuin 20 tuntia ja verkosta ei löytynyt haavoittuvuuksia tai avoimia portteja.

5.4 Tulokset tietoturvahyökkäyksistä

Suurimmat tietoturvauhat tai tietoturvahyökkäysuhat tehtaalla ovat tällä hetkellä tietojenkalastelu ja Social Engineering -tyyliset sähköpostihuijaukset. Social Engineering on siis käytännön huijausyritys, esimerkiksi IT-tukena esiintyminen, eikä se yleensä sinänsä liity millään tavalla tekniikkaan. Näissä tietoturvahyökkäystavoissa uhka painottuu enemmän organisaation henkilöstön tietoturvakoulutukseen, kokemukseen ja yleiseen tietoon siitä, mitä asioita saa jakaa tai välittää eteenpäin.

Pienenä mutta mahdollisena uhkana ovat myös palvelunestohyökkäykset, mutta täälläpäin ei niin suurina volyymeinä kuin muualla maailmassa. Palvelunestohyökkäyksiä vastaan on kuitenkin varustauduttu, joten sellaisen onnistuminen on harvinaista.

Koska suurempaa osaa onnistuneista tietoturvahyökkäyksistä ei päästetä julkiseen tietoon, on niitä vaikea tutkia tai tietoa niistä etsiä. Onnistuneiden hyökkäysten salailu johtuu yleensä organisaation tietoturvan ylläpitämissyistä, koska jos niistä alkaa yleisesti keskustelemaan tai julkistamaan, voi se johtaa toisiin, vakavampiin hyökkäyksiin.

Kaiken kaikkiaan perehdytykset ja koulutukset tietoturva-asioihin pienentävät riskejä kalasteluiden sekä huijausyritysten onnistumisiin. Oikeat tietoturvan ”pelisäännöt” pitävät tietoturvariskit pieninä. Mikään järjestelmä tai vastaava ei ole täydellisen varma, vaan aina on pieni uhka tietoturvahyökkäykselle.

6 POHDINTA JA JOHTOPÄÄTÖKSET

Opinnäytetyön suunnittelu ja eteneminen alkoi mielestämme hyvin ja saimme jaettua aihealueet suhteellisen tasaisesti, vaikka Niko Tuikan alue standardeista olikin periaatteessa laajin. Vili Pokelan osuus skannauksen aloittamisesta ja suorittamisesta myöhästyi hieman koronan aiheuttamien toimenpiteiden takia, mutta loppujen lopuksi sekin saatiin setvittyä järkevästi niin, että se suoritettiin etänä. Opinnäytetyön laajuus oli kolmelle ihmiselle mielestämme sopiva.

Jos tällaisen työn olisi suorittanut yksin, olisi laajuus todennäköisesti ylikuormittanut tekijää eikä opinnäytetyöstä olisi tullut yhtä laadukasta, eikä sitä tehdessä olisi välttämättä oppinut yhtä paljon kuin kolmen ryhmässä tehdessä. Näin saimme kaikki perehtyä paremmin omaan alueeseemme työssä ja pystyimme antamaan omia näkökulmia siitä, miten työn kanssa kannattaa edetä.

Tavoitteina työn alussa meillä oli saada tehtyä vertailu CABB Oy:n tietoturvasta verraten sitä tietoturvastandardeihin. Vertailu sujui mielestämme ajatusten mukaisesti, ja saimme tehtyä sopivan tietopaketin, joka kuuluu opinnäytetyön salaiseen osioon. Työn tavoitteisiin kuului myös suorittaa skannaus CABB Oy:n automaatioverkkoon, jolla kartoitetaan mahdollisia tietoturvariskejä ja mahdollisesti myös korjausehdotuksia näille mahdollisille riskeille. Skannauksen aloittamisessa oli viivettä Korona-tilanteen takia, mutta se suoritettiin lopulta CABB Oy:n henkilökunnan avulla. Skannauskone toimitettiin heille, ja he toimivat paikan päällä, kun me otimme tulokset ylös etänä. Kun skannaus saatiin aloitettua, sujui se ongelmitta ja saimme analysoitua tulokset, joten sekin puoli työstä onnistui tavoitteidemme mukaisesti, ehkä vähän viiveellä vain. Skannaus ja sen tulokset ja analysointi kuuluvat myös tämän opinnäytetyön salaiseen osioon.

Haasteina työssä oli standardikirjojen ymmärtäminen niitä luettaessa, koska teksti oli hieman vaikea ymmärtää täysin, johtuen niiden tekstityylistä, joka oli virallista asiakirjatyylistä tekstiä. Lisäksi koronaviruksen aiheuttamat toimenpiteet hidastivat työn etenemistä, palaverien suunnittelua sekä pitoa ja myös työhön kuuluvan skannauksen aloittamista ja suorittamista.

Kaiken kaikkiaan työ onnistui mielestämme hyvin ja ongelmista huolimatta työ eteni sopivassa tahdissa.

LÄHTEET

CABB Oy. CABB esitys tammikuu 2020. 2020. PDF-dokumentti. Viitattu 9.5.2020.

Cimpanu, C. Mitsubishi Electric discloses security breach, China is main suspect. Verkkoartikkeli. Saatavissa: https://www.zdnet.com/article/mitsubishi-electric-discloses-security-breach-china-is-main-suspect/. Viitattu 20.2.2020.

Cloudflare. 2020. What is a Denial-of-Service (DoS) Attack? Saatavissa: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/. Viitattu 16.3.2020.

Contec. Analog I/O Basic Knowledge. Verkkoartikkeli. Saatavissa: https://www.contec.com/support/basic-knowledge/daq-control/analog-io/ Viitattu 13.4.2020

Contec. Digital I/O Basic Knowledge. Verkkoartikkeli. Saatavissa: https://www.contec.com/support/basic-knowledge/daq-control/digital-io/ Viitattu 13.4.2020

Fisher, T. 2020. What is a Router and how does it work? Saatavissa: https://www.lifewire.com/what-is-a-router-2618162 Viitattu 20.4.2020

F-Secure. 2019. F-Secure Radar. Saatavissa: https://www.f-secure.com/fi/business/products/vulnerability-management/radar Viitattu 13.4.2020.

F-Secure. 2019. Vakoiluohjelmat. Saatavissa: https://help.f-secure.com/product.html?home/safe-mac/latest/fi/spyware-safe-mac-latest-fi. Viitattu 13.2.2020.

If. 2020. Kyberterminologiaa. Saatavissa: https://www.if.fi/yritysasiakkaat/vakuutukset/vastuuvakuutukset/tietoturvavakuutus/kyberterminologiaa. Viitattu 24.1.2020.

Kataja, J. 2015. Mikä on palvelunestohyökkäys? Verkkoartikkeli. Saatavissa: https://www.zoner.fi/mika-on-palvelunestohyokkays/. Viitattu 13.2.2020.

Kurittu, A. 2017. Tietomurtojen ennaltaehkäisy, havaitseminen ja tutkinta. Viestintävirasto. Saatavissa: https://teknologiateollisuus.fi/sites/default/files/kurittu_viestintavirasto.pdf. Viitattu 5.3.2020.

Kybersää lokakuu 2019. 2019. Traficomin kuukausiraportti tietoturvasta. PDF-dokumentti. Viitattu 20.2.2020.

Kybersää joulukuu 2019. 2019. Traficomin kuukausiraportti tietoturvasta. PDF-dokumentti. Viitattu 14.2.2020.

Kybersää marraskuu 2019. 2019. Traficomin kuukausiraportti tietoturvasta. PDF-dokumentti. Viitattu 20.2.2020.

Laaksonen, M. 2006. Yrityksen tietoturvakäsikirja. Helsinki Edita Publishing Oy.

Latto, N. 2020. What is WannaCry, exactly? Avast. Saatavissa: https://www.avast.com/c-wannacry. Julkaistu 27.2.2020. Viitattu 22.3.2020.

Mitchell, B. 2020. What is a Server? Saatavissa: https://www.lifewire.com/servers-in-computer-networking-817380 Viitattu 20.4.2020

MTV uutiset. 2019. Kokemäen kaupunki on joutunut tietoturvahyökkäyksen kohteeksi – sähköiset palvelut toistaiseksi pois käytöstä. Saatavissa: https://www.mtvuutiset.fi/artikkeli/kokemaen-kaupunki-on-joutunut-tietoturvahyokkayksen-kohteeksi-sahkoiset-palvelut-toistaiseksi-pois-kaytosta/7496842. Viitattu 12.3.2020.

Niemi, V. 2017. TM-infopaketti: kaikki mitä sinun tulee tietää Petya-kiristysohjelmasta – keskeistä kysymystä ja vastausta. Verkkoartikkeli. Saatavissa: https://tekniikanmaailma.fi/tm-infopaketti-kaikki-mita-sinun-tulee-tietaa-petya-kiristysohjelmasta-7-keskeista-kysymysta-ja-vastausta/. Viitattu 13.3.2020.

Norton. 2020. What is social engineering? Tips to help avoid becoming a victim. Verkkoartikkeli. Saatavissa: https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html. Viitattu 20.2.2020.

PaloGuard. 2020. Palo Alto Networks Enterprise Firewall PA-3020. Verkkoartikkeli. Saatavissa: http://www.paloguard.com/Firewall-PA-3020.asp Viitattu 13.4.2020

Piikkilä, V. 2011. Rakennusautomaatiojärjestelmät. Luentomateriaali. Tampereen ammattikorkeakoulu. Tampere.

ST-Käsikirja 17. Rakennusautomaatiojärjestelmät. 2012. Sähköinfo Oy.

Suomen Internetopas. 2005. Tietokonevirukset. Saatavissa: http://www.internetopas.com/yleistietoa/virukset/. Viitattu 13.3.2020.

SFS27001. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. 2017. Suomen Standardisoimisliitto SFS

SFS27002. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. 2017. Suomen Standardisoimisliitto SFS

SFS27005. Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta. 2018. Suomen Standardisoimisliitto SFS

Thomas, T. 2005. Verkkojen tietoturvaperusteet. Helsinki: Edita Prima Oy.

Tietosuojavaltuutetun toimisto. 2020. Tietojen kalasteluun perustuvat tietoturvaloukkaukset. Saata vissa: https://tietosuoja.fi/tietojenkalastelu. Viitattu 13.2.2020.

Tuunainen, T. 2019. Tietoturvallisuus. Luentomateriaali Centria-ammattikorkeakoulu Oy. Pietarsaari.

Traficom. 2016. Havaro havainnoi ja varoittaa tietoturvaloukkauksista. Verkkoartikkeli. Saatavissa: https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/05/ttn201605241520.html. Viitattu 12.3.2020.

Uusi teknologia. 2016. Tietoturvahyökkäys alkaa omista laitteista. Verkkoartikkeli. Saatavissa: https://www.uusiteknologia.fi/2016/09/26/tietoturvahyokkays-alkaa-omista-laitteista/. Viitattu 24.1.2020.

Viestintävirasto. 2016. Selviytymisopas kiristyshaittaohjelmia vastaan. Viestintäviraston julkaisu 005/2016. Saatavilla https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf. Viitattu 10.3.2020.

Viitaila, M. 2019. Microsoftin tietoturvaraportti: Tietoturvayhteisön suojaustoimet ovat pakottaneet kyberrikollisia muuttamaan toimintaansa. Saatavissa: https://news.microsoft.com/fi-fi/2019/03/01/microsoftin-tietoturvaraportti-tietoturvayhteison-suojaustoimet-ovat-pakottaneet-kyberrikollisia-muuttamaan-toimintaansa/. Viitattu 12.3.2020.

Virtanen, J. 2017. Näin toimii WannaCry-haittaohjelma – ”Uudet hyökkäykset ovat väistämättömiä”. Saatavissa: https://www.tivi.fi/uutiset/nain-toimii-wannacry-haittaohjelma-uudet-hyokkaykset-ovat-vaistamattomia/9000bc54-1498-3ea1-9096-b219ba0a3de9. Julkaistu 15.5.2017. Viitattu 22.3.2020.