Opinnäytetyö (AMK)

Insinööri (AMK), Tuotantotalous

2024

Leevi Soikkeli

Tuotantolaitosten kyberturvallisuus

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Insinööri (AMK), Tuotantotalous

2024 | 44 sivua

Leevi Soikkeli

Tuotantolaitosten kyberturvallisuus

Opinnäytetyössä perehdyttiin suomalaisten tuotantolaitosten kyberturvallisuuden nykytilanteeseen, kehityskohteisiin sekä uusiin teknologioihin, joita mahdollisesti tullaan käyttämään tuotantolaitoksissa. Työn tarkoituksena on antaa lukijalle kokonaisvaltainen tilannekatsaus tuotantolaitoksien kyberturvallisuuden tilanteesta, kyberuhkien taloudellisista vaikutuksista, sekä uusien teknologioitten tuomista uhkakuvista.

Opinnäytetyössä suoritettiin kattava kirjallisuuskatsaus kyberturvallisuuden ajankohtaisimpiin julkaisuihin, tuotantolaitoksien digitalisoinnin teoriaan teollisuus 4.0, viranomaisohjeistuksiin, teknologiaratkaisuihin sekä vallitseviin tietoturvakäytänteisiin.

Opinnäytetyön tuotoksena syntyi kattava tilannekatsaus suomalaisten tuotantosektorin yritysten kyberturvallisuuden tilasta sekä käsitys mitkä kyberuhat uhkaavat tuotantolaitosten toimintaa eniten.

Asiasanat:

Kyberturvallisuus, Tuotantojärjestelmät, Tekoäly, Yritysstrategiat, Riskienhallinta

Bachelor’s | Abstract

Turku University of Applied Sciences

Bachelor of Engineering, Industrial Management and Engineering

2024 | 44 pages

Leevi Soikkeli

Cybersecurity of Production Facilities

The thesis explored the current situation of cyber security in Finnish production facilities, development targets and new technologies that will possibly be used in production facilities. The purpose of the work is to give the reader a comprehensive overview of the cyber security situation of production facilities, the economic effects of cyber threats, and the threat images brought by new technologies.

The thesis conducted a comprehensive literature review of the most current publications on cyber security, the theory of digitization of production facilities, industry 4.0, official guidelines, technological solutions, and prevailing information security practices.

The result of the thesis was a comprehensive overview of the state of cyber security of Finnish manufacturing companies and an understanding of which cyber threats threaten the operations of production facilities the most.

Keywords:

Cyber Security, Production Systems, Artificial Intelligence, Corporate Strategies, Risk Management

Sisältö

Kuvat

Kuviot

Taulukot

Käytetyt lyhenteet tai sanasto

Airgap: Fyysisesti erotettu tietoliikenneverkko

CFS: (Cyber Security Framework) Kyberturvallisuuden ohjekehys

Deepfake: Syväväärennös

Distributed Denial-of-Service Attack: Palvelunestohyökkäys

EDI: (Electronic Data Interchange) Organisaatioiden välinen tiedonsiirto

ERP: (Enterprise Resource Planning) Toiminnanohjausjärjestelmä

Full-Duplex: Kaksisuuntainen tietoliikenneyhteys

NIST: Yhdysvaltain standardisointi ja teknologiainstituutti

NotPetya: Mato-haittaohjelma

Ransomware: Kiristyshaittaohjelma

Sandbox: Virtuaalinen kehitysalusta

SCADA: (Supervisory Control and Data Acquisition) Ohjelmistotyyppi

Simplex: Yksisuuntainen tietoliikenneyhteys

Stuxnet: Tuotannonohjausjärjestelmiä vastaan suunniteltu haittaohjelma

Tekoäly: Tietokonealgoritmi, joka jäljittelee ihmisten älykkyyttä

Zero-day attack: Nollapäivähaavoittuvuus

1 Johdanto

Globaalissa ja digitaalisessa yhteiskunnassa esiintyy teknologian tuomia uhkia, näitä uhkia kutsutaan kyberuhiksi, joita ovat tietojärjestelmiin kohdistuvat palvelunestohyökkäykset, tietomurrot sekä haittaohjelmat.
Nämä uhat uhkaavat myös globaalia valmistus-toimitusketjua mikä nojaa vahvasti erinäisiin tietojärjestelmiin sekä digitaaliseen tiedonvaihtoon.

Tuotantolaitoksiin kohdistetut kyberhyökkäykset ovat uhka yhteiskuntien toimintavarmuudelle sillä monet tuotantolaitokset kuten lämpö- ja sähkötuotantolaitokset, keskusvarastot, sekä vedenjalastomot, ovat kriittisiä yhteiskunnan toimivuudelle ja ihmisten hyvinvoinnille.

Tämän opinnäytetyön tarkoituksena on laatia selvitys, kuinka erilaisia kyberturvaratkaisuja ja tuotteita voidaan käyttää tuotantolaitosten sekä yhteiskunnan huoltovarmuuden kannalta kriittisten toimintojen suojaamiseen.
Mikä on suomalaisten tuotantolaitosten kyberturvallisuuden tilanne?
Sekä, miten kehittyvät uudet teknologiat ja niiden tuomat uhat tulee ottaa huomioon tulevaisuuden tuotannon kehittämisessä.

Työssä käytetään teoreettista viitekehystä, joka yhdistää toimitusketjujen hallinnan ja kyberturvallisuuden tuotantotalouden ja tietotekniikan näkökulmasta. Käsiteltäviä teorioita ovat teollisuus 4.0, kyberturvallisuuden sekä riskienhallinnan periaatteita.

Tutkimuksen tulokset voivat tarjota apua tuotantolaitosten erinäisten prosessien, kuten valmistuksen ja tiedonvaihdon turvallisuuden kehittämiseen.
Työn tarkoituksena on vastata seuraaviin tutkimuskysymyksiin.
Mitkä ovat keskeiset tekijät, jotka tekevät tuotantolaitoksista houkuttelevan kohteen kyberhyökkäyksille? Mikä on tuotantolaitosten kyberturvallisuuden tilanne Suomessa? Millaisia teknologisia ratkaisuja ja työkaluja on saatavilla tuotantolaitosten kyberturvallisuuden parantamiseksi?
Lopuksi minkälaisia tietoturvauhkia liittyy tekoälyyn?

Opinnäytetyö on ajankohtainen, sillä merkittävällä osalla valmistussektorin yrityksistä on puutteita kyberturvallisuuden osalta. Puutteet ovat moninaisia, jotka ovat yhdistelmä toimialojen toimintakulttuuria sekä toimialojen vaihtelevaa kehitystä digitalisaation osalta. Teollisuudessa on käytössä monia manuaalisesti suoritettavia tietojenkäsittelyyn liittyviä työvaiheita, joita voitaisiin digitalisoida. Lisäksi merkittävien kyberhyökkäysten vähäinen esiintyvyys, sekä yleisimpien kyberhyökkäysten vähäinen taloudellinen vaikutus osaltaan kontribuoi yritysten puutteisiin kyberturvallisuuden osalta.

Yhteiskunnan kannalta, tuotantolaitosten puutteet kyberturvallisuudessa heikentävät huoltovarmuutta ja yritysten kykyä toimia kriisitilanteissa.

2 Kyberturvallisuus

2.1 Mitä kyberturvallisuudella tarkoitetaan?

Kyberturvallisuuden käsitettä kuvataan Puolustusvoimien henkilöstölle suunnatussa kyberturvallisuuden käsikirjassa olevan kokonaisvaltainen tavoitetila, jossa suojellaan ja ylläpidetään digitaalisten tietojärjestelmien ja niiden käyttäjien luottamusta, eheyttä ja saavutettavuutta (Laari ym. 2019, 9).

2.2 Kyberturvallisuuden nykytilanne Suomessa

Huoltovarmuuskeskuksen vuonna 2020 teetättämässä kyberturvakyselyssä tuotanto- ja palvelualan yrityksille selviää, että kaikkien toimialojen kyberturvallisuuden keskiarvo on tasolla 3 missä asiat ovat määritelty ja suunniteltu. Asteikko on välillä 1 ei tehdä, 5 kehitetään jatkuvasti riskilähtöisesti. Tulos 4 kuvastaisi, että asioita tehdään johdonmukaisesti.
Kyselyn tulos kuvastaa puutteita kyberturvallisuuden eri osa-alueilla, ja kyselyssä heikoimmin pärjäsivät tuotantosektorien yritykset.

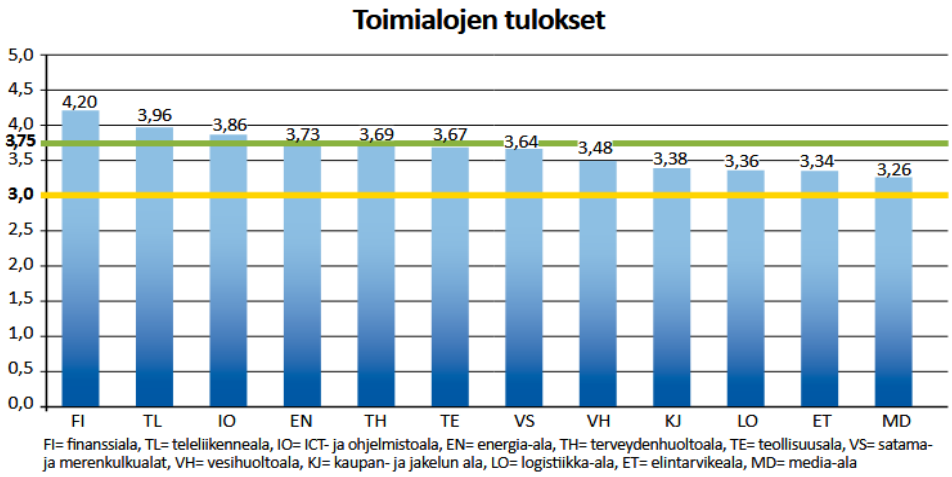
Kyselyn tuloksista nähdään, että parhaiten pärjänneet toimialat ovat finanssiala, teleliikenneala sekä ICT- ja ohjelmistoala, joiden tulos ylitti kaikkien alojen keskiarvon tuloksella 3,75.

Tuotanto- ja logistiikka-alojen yritykset pärjäsivät kyselyssä kohtalaisesti, mutta selkeitä puutteita yritysten kyberturvallisuudessa havaittiin.

Monet tuotantosektorin yritykset suoriutuivat kyselyssä samankaltaisesti ja näiden kehityskohteet olivat samoja. Eniten puutteita havaittiin yritysten kyberturvallisuusstrategian, kyberturvallisuusarkkitehtuurin ja teknisen jäljitettävyyden osalta. Puutteet ovat luonteeltaan perusasioita, joita ei ole korjattu, johtuen toiminta-alan työskentelykulttuurista tai taloudellisista syistä. Yleinen havainto kaikkien alojen osalta oli, ettei kyberturvallisuusasioita käsitellä yrityksen hallituksen ja omistajien kesken. (Huoltovarmuuskeskus 2020, 21–22.)

Lähes yksinään digitaalisiin tietojärjestelmiin nojaavien toimialojen johtaminen kyberturvallisuudessa on odotettua. Kaupan-alan ja logistiikka alan heikko pärjääminen kyselyssä, osoittaa puutteita yhteiskunnan huoltovarmuuden osalta. Logistiikkaa voidaan pitää yhtä merkittävänä kuin kaupan teon mahdollistavaa digitaalista maksujärjestelmää. Erot alojen välillä voidaan selittää eroilla lainsäädännössä, sekä toimijoiden määrällä.
Kaupan ja logistiikan alalla on merkittävästi enemmän toimijoita kuin finanssi, ja ICT-alalla ja lisäksi toimijat ovat usein itsenäisiä toimijoita, jotka aliurakoidaan suurten logistiikkaketjun kautta tekemään toimituksia.

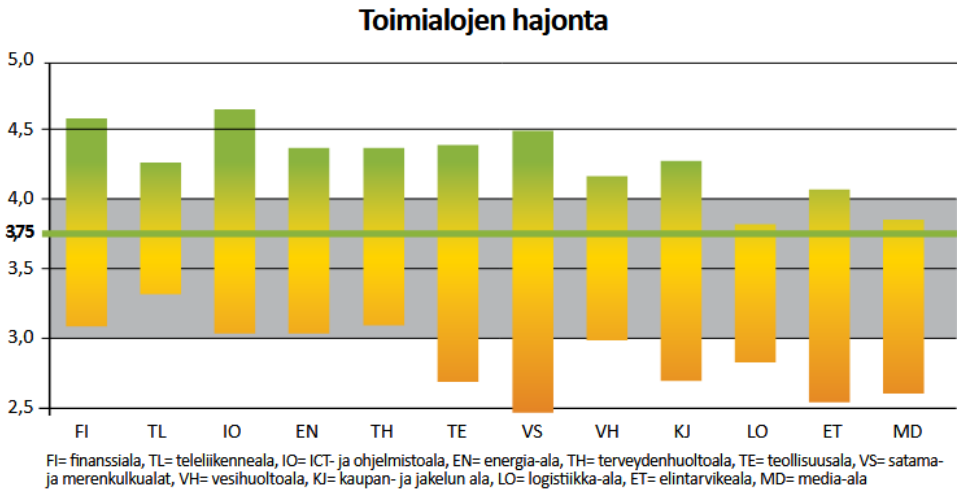
Kuvaajassa 1. kuvataan eri toimialojen tuloksia.



Kuvio 1. Toimialojen tuloksia (Huoltovarmuuskeskus 2020, 8).

Yleisesti monilla aloilla nähtiin merkittävää hajontaa mitattujen tulosten välillä. Syitä tulosten vaihtelevuudelle olivat yritysten kokoerot, käytettävissä olevat resurssit, toimialakohtainen säännöstely ja lainsäädäntö, asiakasvaatimukset, sekä toimialalla vallitseva digitalisaation kehitys. (Huoltovarmuuskeskus 2020, 8.)

Kuviossa 2. kuvataan suomalaisten toimialojen hajontaa Huoltovarmuuskeskuksen teetättämässä kyberturvallisuuskyselyssä. Tuloksissa nähdään kohtalaisesti hajontaa kauttaaltaan eri toimialojen kesken. Tuotantoalojen kesken eniten hajontaa nähdään teollisuuden, kaupan- ja jakelu alan sekä elintarvikealan kesken. Lisäksi merkittävänä mainintana, eniten hajontaa toimialan kesken on satama- ja merenkulkualalla. (Huoltovarmuuskeskus 2020, 8).



Kuvio 2. Toimialojen hajonta (Huoltovarmuuskeskus 2020, 8).

Satama- ja merenkulkualan suuri hajonta on suomalaisen yhteiskunnan huoltovarmuuden kannalta huolestuttavaa, sillä merkittävä osa Suomen ulkomaankaupasta kulkee meriteitse. Suomen Varustamot ry:n mukaan, merikuljetusten osuus Suomen viennistä on 94,4 % ja tuonnin osuus 96,6 % (Kauppalehti 2024).

Tuotantoyritysten laaja hajonta osoittaa, etteivät suomalaiset yritykset erityisesti panosta kyberturvallisuuteen sen enempään kuin mitä on välttämätöntä. Kyberturvallisuuttaa ei koeta sellaisena riskinä mikä pitäisi sisällyttää yrityksen riskinhallintastrategiaan, eikä taloudellisia panostuksia tehdä, vaikka teknologian käyttö yleisesti lisääntyy. Panostukset kyberturvallisuuden lisäämiseen, voidaan nähdä osittain kustannustehottomina, mitä korkeampaa suojausta yritykselle lähdetään rakentamaan.

Kyberturvallisuus ei itsessään lisää työn tuottavuutta tai myyntiä, vaan on kuluerä, jota mukautetaan todennäköisyyksien ja kustannustehokkuuden kautta.

Suomalaisen yhteiskunnan näkökulmasta, yritysten kyberturvallisuuden lisäämistä voitaisiin lisätä tarkastelemalla lainsäädäntöä ja alakohtaisia säädöksiä. Yhteiskunnan huoltovarmuuden parantaminen ei kuitenkaan aina ole linjassa yritysten taloudellisten tavoitteiden kanssa, joten säännöstelyn lisäämisen kynnys voi olla korkea lainsäätäjien ylittää.
Siksi valtion olisi hyvä tukea suomalaisten yritysten kyberturvallisuutta tarjoamalla asiantuntijapalveluita ja viranomaistiedotteita.

2.3 Kyberhyökkäykset

Kyberhyökkäyksellä tarkoitetaan toimintaa, jolla pyritään vahingoittamaan tai ottamaan haltuun oikeudettomasti kohdeympäristön tietoliikenneverkkoja, laitteita tai järjestelmiä (Laari ym. 2019, 37). Kyberhyökkäysten yleisimpiä motiiveja ovat taloudellisen hyödyn saavuttaminen, kybervakoilu sekä sabotaasit.

2.3.1 Kiristyshaittaohjelmat (Ransomware)

Kiristyshaittaohjelmilla tarkoitetaan verkkorikollisten käyttämää kyberhyökkäyksen muotoa, jossa tarkoituksena on päästä käsiksi kohdeyrityksen arkaluontoiseen dataan ja evätä kohdeyrityksen pääsy dataan käyttämällä salausalgoritmeja. Kun kohteen pääsy arkaluonteiseen tietoon on evätty, kohteelle esitetään taloudellinen vaatimus tiedon takaisin saamiseksi.

Vaatimuksen maksaminen ei takaa, että yritys pääse takaisin käsiksi salattuun dataan ja kyseessä voi olla vain keino salata toiminnan todellinen tarkoitus, tiedon tuhoaminen tai hyökkääjät eivät vain palauta varastettuja tietoja (Liikenne- ja viestintävirasto Traficom 2022, 2).

2.3.2 Palvelunestohyökkäykset (Distributed Denial-of-Service Attack)

Palvelunestohyökkäyksessä kohteen tietoliikenneverkossa olevaan resurssiin tai sovellukseen kohdistetaan merkittävä määrä verkkoliikennettä, joka hidastaa tai estää resurssin tai sovelluksen käytön. Palvelunestohyökkäystä voidaan pitää matalankynnyksen hyökkäysmuotona, sillä se on verrattain helppoa suorittaa. Hyökkäyksestä ei varasteta tietoa kohteesta, joten sitä voidaan pitää lähinnä häirintänä ja haitantekona (Liikenne- ja viestintävirasto Traficom 2022b, 2).

2.3.3 Nolla-päivä-haavoittuvuudet (Zero-day attack)

Nolla-päivä haavoittuvuudella viitataan ohjelmistossa tai tietojärjestelmässä olemassa olevaan haavoittuvuuteen, josta järjestelmän ylläpitäjä ei ole tietoinen. Nolla-päivä haavoittuvuuksia voi ilmetä käyttöjärjestelmissä, ohjelmistoissa tai avoimen lähdekoodin osissa.

Haavoittuvuuksien avulla hyökkääjä saa pääsyn kohteen tietojärjestelmään tämän huomaamatta. Nolla-päivä hyökkäyksiä on kahdentyyppistä: kohdistettua ja kohdistumatonta. Kohdistetussa nollapäivä hyökkäyksissä, haitallista koodia uitetaan kohteen tietojärjestelmään naamiomailla se vaikuttamaan harmittomalta. Kohdistamattomissa hyökkäyksissä, hyökkääjä hyödyntää järjestelmissä ja ohjelmistoissa olemassa olevia haavoittuvuuksia saadakseen yhteyden kohteen tietojärjestelmään (Kaspersky 2024).

2.3.4 Väliintulohyökkäys (Man-In-The-Middle-Attack)

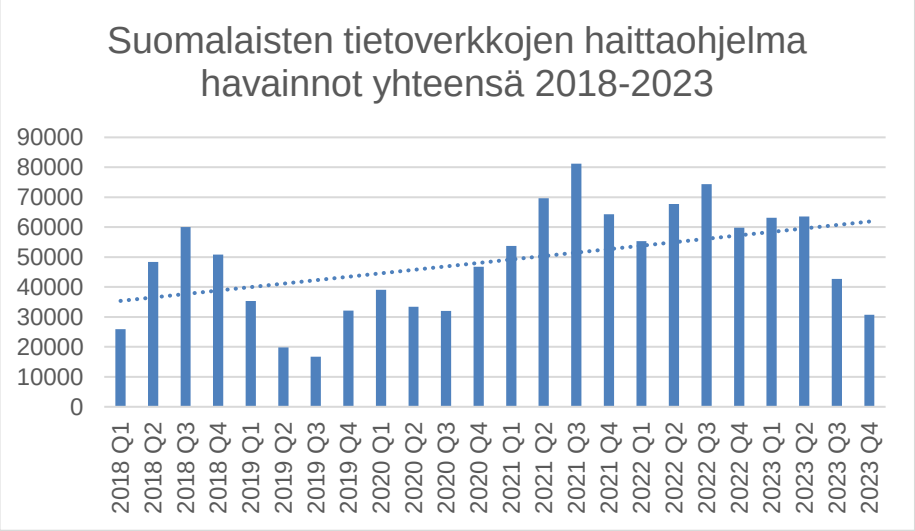
Väliintulohyökkäyksellä tarkoitetaan kyberhyökkäysmuotoa, jossa hyökkääjä kaappaa kahden toimijan välisen tietoliikenteen ja pyrkii kuuntelemaan tai imitoimaan toista osapuolta. Hyökkäyksen tarkoituksena on kerätä arkaluontoisia tietoja, kuten salasanoja, pankkikorttitietoja tai henkilötietoja. Hyökkäysten motiivi on usein taloudellinen hyöty (Mallik 2019, 109–111).

2.3.5 Tietojenkalastelu (Phishing)

Tietojenkalastelussa hyökkääjä pyrkii hankkimaan käyttäjän arkaluontoisia tietoja, kuten pankkikorttitietoja, henkilötunnuksia tai salasanoja taloudellisen hyödyn saavuttamiseksi. Tietojenkalastelua on mahdollista suorittaa monella eri tavalla, kuten luomalla kopioita olemassa olevien yritysten ja palveluiden verkkosivustoista, jotka tallentavat käyttäjän syöttämät tiedot. Kalastelu voi olla myös sähköpostitse tai puhelimitse tapahtuvaa, jolloin hyökkääjä pyrkii hankkimaan arkaluontoista tietoa tekeytymällä, kohteen luottamaksi tahoksi (Bhavsar ym. 2018, 1–2).

2.4 Kyberhyökkäysten esiintyminen Suomessa

Liikenne- ja viestintävirasto Traficom on vuodesta 2006 seurannut haittaohjelmien esiintyvyyttä suomalaisissa tietoliikenneverkoissa. Haittaohjelmien esiintymistiheyden seuranta antaa viranomaisille käsityksen eri verkkorikollisryhmien toiminnan kestosta ja laadusta. Tilannetieto mahdollistaa trendien tunnistamisen ja kohteena olevien toimintasektorien ohjeistamisen.

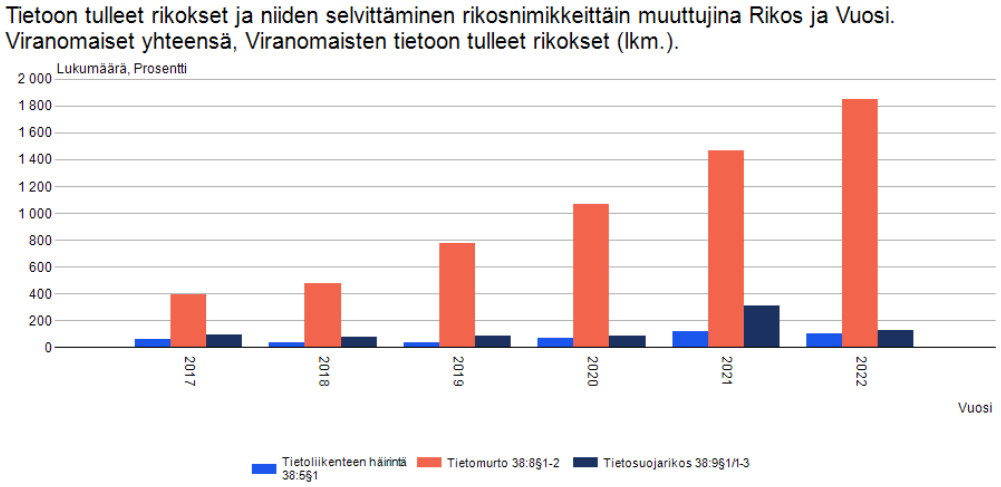


Kuvio 3. Suomalaisten tietoverkkojen haittaohjelma havainnot yhteensä 2018–2023 (Liikenne- ja viestintävirasto Traficom 2024).

Kuviosta 3. näkee, että vuodesta 2018 vuoteen 2023 mitattujen havaintojen esiintyvyys pitkällä aikavälillä on kasvussa, mutta kuvaajasta nähdään, että haittaohjelmien esiintyvyydessä on syklisyyttä.

Tämä johtuu eri verkkorikollisten suorittamista haittaohjelmakampanjoista, sekä erinäisistä yhteiskunnallisista tapahtumista, kuten nähtiin 2020 koronaviruspandemian aikana, kun monet työntekijät siirtyivät etätyöskentelemään. (Liikenne- ja viestintävirasto Traficom 2024.)

Kun tarkastellaan Suomen poliisin tietoon tulleiden kyberrikoksien määriä (Kuvio 4.), nähdään myös kasvua tietomurtojen, tietoliikenteen häirinnän ja tietosuojarikosten osalta. Tietoon tulleista rikosnimikkeistä, tietomurtojen osuus on moninkertainen verrattuna tietoliikenteen häirintään ja tietosuojarikoksiin. (Suomen virallinen tilasto 2024.)



Kuvio 4. Tietoon tulleet rikokset ja niiden selvittäminen rikosnimikkeittäin muuttujina Rikos ja Vuosi. Viranomaiset yhteensä, Viranomaisten tietoon tulleet rikokset (lkm.). 2017–2022 (Suomen virallinen tilasto 2024).

Poliisin tietoon tulleiden rikosten määrä on suhteessa varsin pieni verrattuna Traficomin haittaohjelmien seurantatilastoihin. Traficom havaitsi vuoden 2020 aikana 151 381 yksittäistä haittaohjelmaa Suomen tietoliikenneverkoissa. (Liikenne- ja viestintävirasto Traficom 2024.) Poliisin tietoon tuli noin 2000 rikosilmoitusta erinäisistä kyberrikoksista. (Suomen virallinen tilasto 2024.) Tämä on noin 1,3 % kaikista Traficomin havainnoista.

Ero tehtyjen havaintojen ja tietoon tulleiden rikosten määrissä, osoittaa ettei merkittävä osa haittaohjelmista joko saastuta kohteita, merkittävä osa kohteista ei havaitse saastumista tai kohde ei ilmoita haittaohjelmasta poliisille. Yleisimmät kyberhyökkäykset ovat luonteeltaan sellaisia, kuten yksinkertaiset haittaohjelmat ja kalasteluyritykset etteivät ne aiheuta merkittävää taloudellista vahinkoa ja ovat teknisesti sellaisia mitä päivitetyt tietojärjestelmät ja valveutuneet työntekijät pystyvät havaitsemaan ja torjumaan.
Poliisin tietoon tulevat vain merkittävimmät ja suurinta vahinkoa aiheuttavat kyberhyökkäykset, sillä yritysten tulee itse arvioida, milloin kyberhyökkäyksestä ilmoittamisesta viranomaisille on hyötyä. Erityisesti pörssiyhtiöihin kohdistuneissa kyberhyökkäyksissä, julkisuuteen ilmoittamisella voi olla vaikutuksia yritysten osakekurssiin sekä imagollisia haittoja ja vaikutuksia.

2.4.1 Toimijat

Suomen valtioneuvoston selvityksessä, yhteiskuntien digitalisoitumisen ja kyberympäristöjen kasvun myötä, Suomeen kohdistuu niin vakavaa kyberrikollisuutta kuin Suomen kansallista turvallisuutta uhkaavia vihamielisiä valtiollisia toimijoita (Valtioneuvosto 2023, 11).

2.4.2 Valtiolliset toimijat

Valtiollisessa kybertoiminnassa on yleensä kyseessä kybervakoilusta, jossa valtiollinen toimija pyrkii hankkimaan salaista tietoa vieraan maan maanpuolustuksesta, kriittisestä infrastruktuurista tai poliittisesta päätöksenteosta. Lisäksi valtiolliset toimijat kohdistavat kybervakoilua huipputeknologiaa kehittäviin yrityksiin ja tutkimuslaitoksiin, sekä yliopistojen tutkimustuloksiin.

Kybervakoilua on vaikea havaita sillä käytetyt menetelmät ovat erittäin kehittyneitä ja hyökkäysten havaitseminen on erittäin vaikeata.

Valtiollisessa kybervakoilussa hyökkääjä pyrkii saamaan täyden hallinnan kohteen tietojärjestelmistä.

Valtiollista kybertoimintaa voidaan myös käyttää alemman kynnyksen sotilaallisena vaikutuskeinona, ennen perinteisempää sotilaallista vaikuttamista. (Valtioneuvosto 2023, 12–13)

2.4.3 Ei-Valtiolliset toimijat

Ei-valtiollisilla toimijoilla tarkoitetaan kyberrikollisia, joiden tavoitteena on taloudellinen hyöty kiristämällä kyberhyökkäyksen kohdetta tältä varastetulla arkaluontoisella tiedolla tai myymällä tämä tieto.
Kyberrikollisryhmät tarjoavat erinäisiä palveluita, joita myös valtiolliset toimijat käyttävät, hämätäkseen hyökkäyksen todellisen toteuttajan identiteetin (Valtioneuvosto 2023, 13).

2.4.4 Kyberhyökkäysten maantiede

Mapping the global geography of cybercrime with the World Cybercrime Index tutkimuksessa arvioitiin eri maista suoritetun kyberrikollisuuden merkitystä, arvioiden teknisen osaamisen, hyökkäysten vaikutuksen sekä tehtyjen kyberhyökkäystyyppien kokonaisvaikutusta. Tutkijat laativat maailman kyberrikollisuus indeksin (The World Cybercrime Index - WCI) mittaaman tätä kokonaisvaikutusta.

Tutkimuksesta selviää, että korkeimman kokonaistuloksen sai Venäjä WCI tuloksella 58,39. Tulos on selkeästi korkein, toisella sijalla olevan Ukrainan tulos oli 36,44 ja kolmannella sijalla olevan Kiinan 27,86.
Mainittujen maiden lisäksi muita toistuvia maita olivat Yhdysvallat, Romania ja Nigeria. Kaikki maat toistuvat useasti mitattujen parametrien kuten, hyökkäysten teknisyyden, hyökkäysten määrien, tietomurtojen, petosten sekä rahanpesun kärkimaina (Bruce ym. 2024, 1–8).

Rank	Country	I	P	TS	WCI Score	Tech	Attacks	Data	Scams	Cash
1	Russia	8.96	8.81	8.73	**58.39**	82.17	81.34	65.18	21.70	41.56
2	Ukraine	8.37	8.29	8.24	**36.44**	52.97	50.76	36.01	11.20	31.27
3	China	8.22	7.70	7.81	**27.86**	40.22	24.24	34.89	15.83	24.13
4	United States	7.99	7.21	7.21	**25.01**	27.64	17.68	30.36	22.72	26.63
5	Nigeria	8.25	6.49	5.80	**21.28**	7.93	8.41	23.04	52.17	14.86
6	Romania	7.12	7.04	7.15	**14.83**	17.83	9.17	22.50	13.15	11.49
7	North Korea	7.91	7.23	7.38	**10.61**	8.66	25.33	13.01	2.17	3.88
8	United Kingdom	7.86	7.21	6.75	**9.01**	5.04	4.75	5.80	7.86	21.63
9	Brazil	6.90	6.35	6.32	**8.93**	13.70	8.77	10.29	7.28	4.64
10	India	7.90	6.60	6.65	**6.13**	4.46	3.62	6.81	12.75	3.01
11	Iran	6.88	6.45	6.64	**4.78**	8.62	10.00	3.59	0.94	0.72
12	Belarus	6.84	7.20	7.32	**3.87**	11.92	5.58	1.85	--	--
13	Ghana	8.57	6.83	6.09	**3.58**	1.23	0.76	2.97	10.36	2.57
14	South Africa	6.95	5.35	5.50	**2.58**	1.20	0.65	0.58	7.17	3.30
15	Moldova	7.38	7.19	7.56	**2.57**	6.70	0.98	2.43	0.83	1.88

I = Impact; P = Professionalism; TS = Technical skill, Technical = *Technical products/services*, Attacks = *Attacks and extortion*, Data = *Data/identity theft*, Cash = *Cashing out and money laundering*. I, P, and TS are scored out of 10. 'WCI Score', and all columns following, are scored out of 100. Each country's top score across all cybercrime types is shaded in grey.

Taulukko 1. Tietoverkkorikollisuuden maailmanlaajuisen maantieteen kartoittaminen World Cybercrime Index -indeksin mukaan (Bruce ym. 2024, 8).

Taulukossa 1. listatut autoritääriset valtiot kuten Iran, Venäjä, Valko-Venäjä, Kiina sekä Pohjois-Korea listautuvat WCI-indeksi mittausten mukaan 15 korkeitten sijoittuvien valtioiden joukkoon. Kyseiset valtiot korostuvat tietomurtojen ja kehittyneiden kyberhyökkäysten osalta, jotka ovat merkittävä riski tuotantolaitoksille. Näiden maiden kyberrikolliset ovat myös merkittävä uhka suomalaisille yrityksille, sillä taloudellisten motiivien lisäksi, ryhmittymien toimintaa ohjaavat mahdollisesti myös poliittiset motiivit.
Autoritääriset valtiot käyttävät kyberrikollisryhmiä osana vaikuttamis- ja tiedustelutoimintaa, jota kohdistetaan länsimaalaisiin valtioihin ja suuryrityksiin.

Petoksien ja erinäisten verkkohuijausten alkuperä juontaa juurensa merkittävissä määrin vähemmän kehittyneihin maihin kuten, Intia, Nigeria, Ghana ja Etelä-Afrikka. Verkkohuijaukset eivät ensisijaisesti kosketa yrityksiä, mutta yrityksiin kohdistetaan myös tietojenkyselykampanjoita kyseisistä maista.

Verkkorikollisuus on globaali-ilmiö ja hyökkääjä voi sijaita missä päin maailmaa tahansa ja uhri valikoitua sattumanvaralta. Kohteet valikoituvat kuitenkin usein koon ja menestymisen todennäköisyyden mukaan ja kohdistuvat ensisijaisesti suurimpien markkinoiden kimppuun Yhdysvalloissa, Aasiassa ja Lähi-Idässä.

3 Tuotantolaitokset

3.1 Tuotantolaitosten toiminta

Kielitoimiston sanakirjan määritelmän mukaan tehdas on tuotantolaitos, jossa valmistetaan koneellisesti tuotteita (Kielitoimiston sanakirja 2024).

Tulevaisuuden tuotantolaitoksella ei tarkoiteta pelkästään fyysistä rakennusta, jossa tuotteita valmistetaan, vaan kyseessä on monesta valmistajasta ja alihankkijasta koostuvasta kokonaisuudesta. Tuotantolaitoksissa tulee olemaan tulevaisuudessa yhä enemmän digitaalisia ratkaisuja parantamaan nykyisiä valmistustekniikoita. Lisääntyvä digitalisaatio kasvattaa tarvetta tiedonvaihdolle valmistajien ja koneiden kesken (Anumbe ym. 2022, 1–3).

Tiedonvaihtoon ja automaation hallintaan tarvitaan erinäisiä ohjausjärjestelmiä, jotka kommunikoivat usean eri tietokannan ja toimijan kanssa. Toiminnanohjauksen kompleksisuus lisää tehokkuuden lisäksi myös kyberturvallisuuteen liittyviä riskejä, joita tulee hallita toimintasuunnitelmin, teknisin ratkaisuin ja kouluttamalla henkilökuntaa uusimmilla käytänteillä.

3.2 Neljäs teollinen vallankumous

Neljännellä teollisella vallankumouksella viitataan nykyhetkeen, jossa teollisuus siirtyy kasvavissa määrin sisällyttämään autonomisia teknologioita nykyisiin automaatiojärjestelmiin. Nousevia teknologiota ovat tekoäly, autonomiset järjestelmät sekä Iot-laitteet. (Internet of Things) Uudet teknologiset ratkaisut kurovat umpeen fyysisen maailman ja digitaalisen maailman välistä kuilua, joka näyttäytyy älykkäiden ratkaisujen integroimisena nykyisiin teknologioihin ja täysin uusiin ratkaisuihin, joiden tavoitteena on lisätä tehokkuutta. Digitalisaation myötä yritykset ja yhteiskunnat joutuvat mukautumaan muuttuvaan ympäristöön, mikä tulee muokkaamaan ihmisten tapaa työskennellä ja kommunikoida (Ross & Maynard 2021, 1).

3.3 ERP-Järjestelmät (Enterprise Resource Planning)

ERP-Järjestelmällä tarkoitetaan digitaalista työkalua mikä sitoo yrityksen eri osastot kuten, myynnin, tuotannon ja markkinoinnin yhteen. ERP-järjestelmässä osastot pystyvät vaihtamaan ja prosessoimaan tietoa reaaliajassa ja täten tekemään päätöksiä nopealla aikataululla, mitkä liittyvät yrityksen päivittäisiin operaatioihin (Kenge 2020, 34–38).

ERP-järjestelmät sisältävät suuria määriä yritysten arkaluontoista tietoa, kuten yksityiskohtaisia taloudellisia tietoja, yritysten suunnittelutiedostoja, CAD malleja, sekä muita liikesalaisuuksia. ERP-järjestelmien suojaaminen on yrityksen toiminnan kannalta merkittävää, sillä mahdollisen tietomurron seurauksena, yrityksen liiketoiminta voi häiriintyä merkittävästi, johtuen ERP-järjestelmän arkkitehtuurista. ERP-järjestelmä keskittää useita toimintoja yhden ohjelmiston alaisuuteen koska se tekee yrityksen liiketoiminnan suunnittelusta ja toteuttamisesta suoraviivaisempaa, kun tiedonvaihto on sujuvaa. Toimintojen keskittämisellä lisätään mahdollisen tietomurron seuraamuksia, sillä puolustus perustuu yhteen heikkoon kohtaan, eikä arkkitehtuurissa hajauteta toimintoja erilleen, mikä minimoisi tietomurron seuraamuksia.

3.4 EDI-Järjestelmät (Electronic Data Interchange)

EDI-Järjestelmä on digitaalinen työkalu, millä yritykset pystyvät automaattisesti vaihtamaan suuria määriä tietoja nopeasti ja tehokkaasti. EDI-järjestelmiä käytetään esimerkiksi valmistajan ja asiakkaan välillä, mikäli heillä on toistuvia ja suuria tilausmääriä. Valmistajat voivat jakaa reaaliaikaista tilannetietoa tuotannosta asiakkaille, näin asiakkaat pystyvät suunnittelemaan paremmin omaa toimintaansa (Smith ym. 2020).

EDI-järjestelmät ovat yksi potentiaalinen kyberhyökkäyksen kohde, sillä yritysten välinen tiedonvaihto sisältää liikesalaisuuksia, lisäksi EDI-järjestelmä on portti yrityksen IT-järjestelmään, jota kautta olisi mahdollista saastuttaa kyberhyökkäyksen kohteena oleva yritys haittaohjelmalla.

EDI-järjestelmien käyttöön liittyy riskejä, sillä usein tietoja vaihdetaan yritysten kesken suoraan tuotantoympäristöstä ja siksi mahdollisen haittaohjelman leviäminen tai tietomurron estäminen on hyvin tärkeää, koska ympäristöjen sisältämä tieto on luottamuksellista. Tiedon julkaiseminen vapaaseen jakeluun voisi vaikeuttaa yrityksen liiketoimintaa ja aiheuttaa mainehaittaa.

3.5 SCADA-Ohjausjärjestelmä

SCADA-ohjausjärjestelmä on yleisesti teollisuudessa käytössä oleva automaation ohjausjärjestelmä. SCADA:lla ohjataan monenlaisia teollisia ympäristöjä kuten voimalaitoksia, varastoja, sairaaloita sekä tuotantolaitoksia.

SCADA (Supervisory Control And Data Acquisition) on ohjausjärjestelmä, joka mahdollistaa hajautetun automatisoinnin ohjaamisen ja valvonnan. Hajautetulla valvonnalla kohteita voidaan hallita ja tarkkailla keskitetysti, vähentäen henkilöstön tarvetta kohteessa. Tällaisia käyttökohteita voivat olla erilaiset energiavoimalat, kuten tuuli- ja aurinkovoimalat.
Järjestelmällä valvotaan ja ohjataan esimerkiksi tuotantolinjaston eri osa-alueiden automatiikkaa tai voimalaitosten sähköntuotantoa (Yadav & Paul 2021).

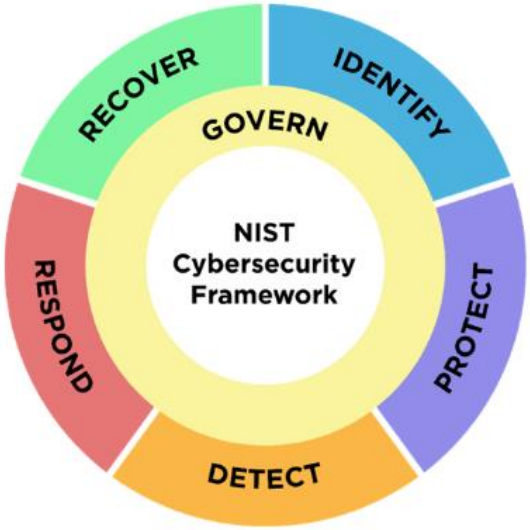
Kyberhyökkäyksen kohdistumisella automaatiojärjestelmään, voi olla merkittäviä vaikutuksia yrityksen liiketoimintakykyyn, kyberhyökkäyksen seurauksena. Mahdollisen kyberhyökkäyksen seurauksena, hyökkääjä voi päästä käsiksi automaation toiminnanohjausjärjestelmään ja aiheuttaa laitteiden fyysisen vahingoittumisen tai estää tuotannon.
Erityisen tärkeää toiminnanohjausjärjestelmien suojaaminen on energiantuotantolaitoksissa, sillä toiminnanohjausjärjestelmän sabotoinnin seurauksena on mahdollista aiheuttaa vaaraa ympäristölle ja estää ihmisten energiansaanti.

Toiminnanohjausjärjestelmiin kohdistuneita kyberhyökkäyksiä suorittavat niin valtiolliset kuin ei-valtiolliset toimijat, erilaisilla motiiveilla.

4 Kyberturvallisuuden edistäminen ja ratkaisut

4.1 Kyberturvallisuuden kokonaisuus organisaatioissa

Yhdysvaltain standardisointi ja teknologiainstituutti NIST (National Institute of Standards and Technology) tarjoaa valtionhallinnon toimijoille ja yrityksille ohjeita kyberuhkiin varautumiseen ja sekä riskienhallintaan ja niiden kartoittamiseen. Kyberuhkiin varautumisen keskiössä on niiden oikea oppinen tunnistaminen, hyökkäyksiltä suojautuminen ja palautuminen.



Kuva 1. Cyber Security Framework (CSF) (Yhdysvaltain standardisointi ja teknologiainstituutti 2024, 5).

NIST ylläpitää kyberturvallisuuden ohjekehystä CSF (Cyber Security Framework) jonka tarkoituksena on toimia oppaana kyberuhkien estämiseen ja kyberhyökkäyksistä palautumiseen. Kuva 1. kuvastaa miten kyberturvallisuuden ohjekehys sisältää 5 ydintoimintoa, joiden avulla yritykset pystyvät laatimaan toimintasuunnitelmia ja ohjeita kyberhyökkäyksien varalta.

Hallitse, tunnista, suojele, havaitse, vastaa ja palaudu.

Hallitse (Govern)

Organisaatio on laatinut itselleen riskienhallintastrategian ja jakanut roolit, vastuut ja toimintakäytänteet erinäisten kybertilanteiden varalta. Organisaatio käyttää hallitse työkalua sitomaan kyberturvallisuusstrategian osaksi organisaation kokonaisturvallisuusstrategiaa.

Tunnista (Identify)

Organisaatio on tunnistanut siihen kohdistuvat riskit ja se tiedostaa sen käytössä olevat laite- ja ohjelmistokokonaisuudet sekä toimittajat.

Suojele (Protect)

Organisaatio on tunnistanut siihen kohdistuvat riskit ja niiden vaikutukset organisaation toiminnoille. Organisaatio pyrkii laskemaan riskiä käyttämällä metodeja niiden todennäköisyyden ja vaikutusten laskemiseksi. Keinoja voivat olla vahvennus ja pääsynhallinta, henkilöstön kouluttaminen sekä fyysisten ja virtuaalisten alustojen hyödyntäminen.

Havaitse (Detect)

Organisaation tulee seurata sen ympäristön toimintaa säännöllisesti ja seurata poikkeavia tapahtumia, jotka voivat viitata mahdolliseen tietomurtoon tai kyberhyökkäykseen.

Vastaa (Respond)

Kun mahdollinen kyberhyökkäys tapahtuu, tulee välittömät toimet aloittaa hyökkäyksen estämiseksi ja minimoimiseksi.
Välittömiä toimia seuraa tapauksen analysointi, jatkoseuraamusten pienentäminen sekä tarvittaville osapuolille raportointi ja viestintä.

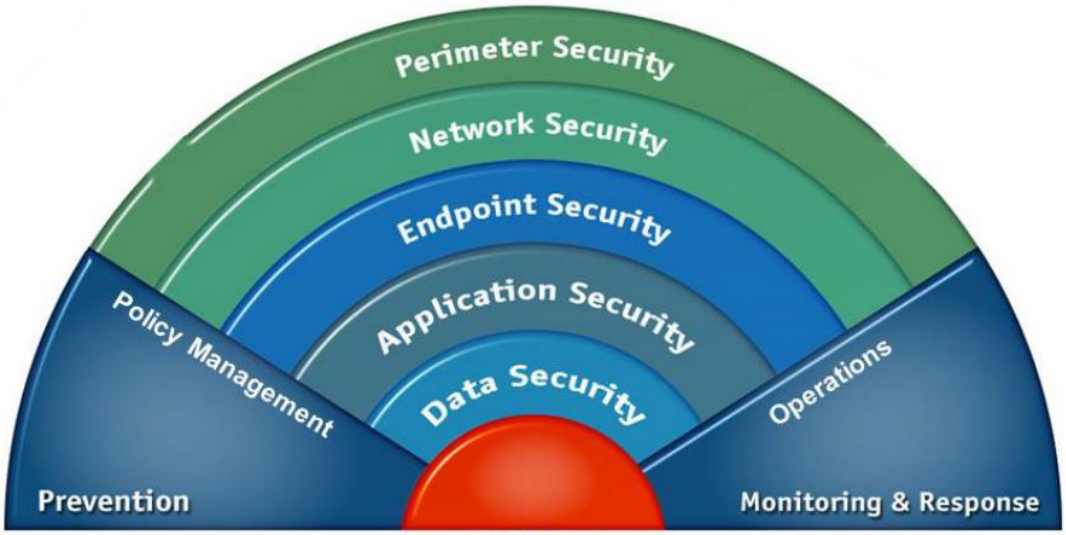
Palaudu (Recover)

Organisaatio palautuu normaaliin operointiin ja kyberhyökkäyksen vaikutukset ovat estetty. Organisaatio viestii tarvittavista jatkotoimenpiteistä mahdollisten kumppanien kanssa (Yhdysvaltain standardisointi ja teknologiainstituutti 2024, 2–5).

4.2 Kyberturvallisuuden kerrokset

Kyberturvallisuus koostuu useasta eri kerroksesta, joiden sisällä vaikuttavat erilaiset kyberturvaratkaisut kuten ohjelmistot, laitteet sekä käytänteet. (McCallam 2012).

Kuvassa 2. on esimerkki korkean tason eri kerroksista ja missä järjestyksessä ne muodostavat kokonaissuojan. Turvallisen ympäristön edellytykset ovat, että kaikissa kerroksissa täytyy olla käytössä jokin ratkaisu, että sitä voidaan pitää turvallisena.

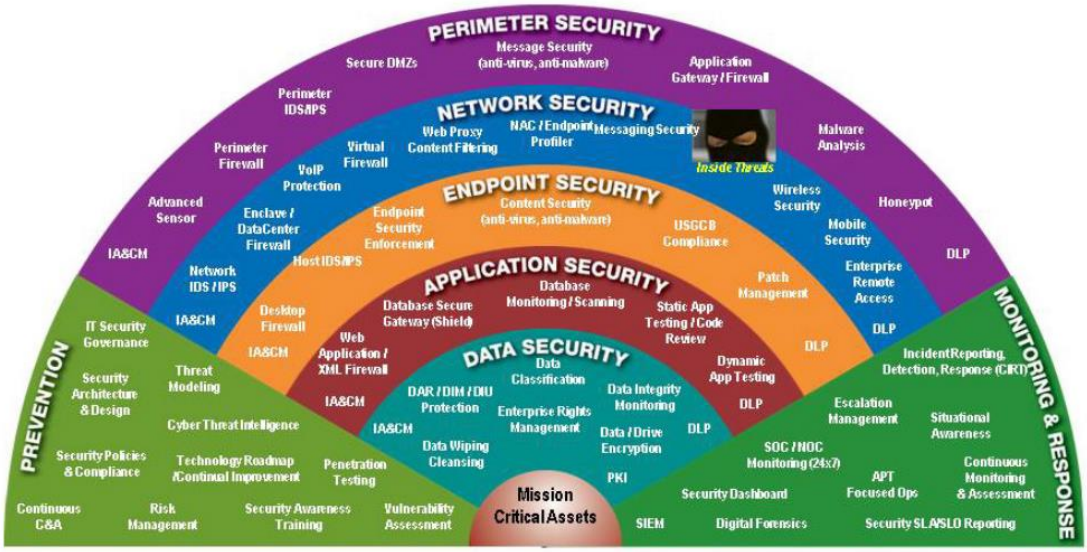


Kuva 2. Korkean tason kuvaus kyberturvan kerroksista (McCallam 2012).

Kyberpuolustuksen 5 pääkerrosta alkaen uloimmasta kerroksesta. Kehäturvallisuus (Perimeter Security) kattaa haittaohjelmien sekä haitallisen liikenteen skannaamisen. Verkkoturvallisuus (Network Security) keskittyy verkkoliikenteen turvaamiseen. Päätelaitteen turvallisuus (Endpoint Security) keskittyy päätelaitteen turvallisuuden takaamiseen, kuten päivitysten asentamiseen sekä haittaohjelmien skannaamiseen.
Ohjelmistoturvallisuus (Application Security) keskittyy ohjelmistojen haavoittuvuuksien skannaamiseen, kuten nollapäivä haavoittuvuuksien ja haittaohjelmien varalta. Tietoturvallisuus (Data Security) hallitsee datan eheyttä ja turvallisuutta, erinäisillä käytänteillä ja protokollilla miten dataa jaetaan ja käytetään.

Kerrossuojautumisen periaatteena on, että IT-ympäristön kyberturvallisuuden riskit ovat hajautettuina usealle kerrokselle. Näin mikäli yksi uloimmista kerroksista pettää, sisempien kerrosten suojaukset estävät kyberhyökkäyksen.

Kuvassa 3. kuvataan kyberpuolustuksen 5 pääkerroksen sisältämät ratkaisut yksityiskohtaisemmin. Kun yritykset kartoittavat kyberturvallisuuden tarpeita, yritykset valikoivat ratkaisuyhdistelmiä eri kerroksiin.



Kuva 3. Yksityiskohtainen kuvaus kyberturvan kerroksista (McCallam 2012).

Kuvassa 3. kuvatut ratkaisut ovat esimerkkitapauksesta ja jokainen tuotantoympäristö ei tarvitse yhtä kattavaa suojausta. Ratkaisujen valinta tulee tehdä todennäköisyysarvioin mukaan sellaisia hyökkäysmuotoja vastaan, mitkä ovat yleisimpiä ja todennäköisimpiä hyökkäysmuotoja kyseiseen järjestelmään.

Täydellistä suojaa on mahdotonta saada ja jokaisen ratkaisun lisääminen lisää kyberpuolustuksen kustannuksia ja pahimmassa tapauksessa voi heikentää IT-järjestelmän turvallisuutta, koska järjestelmän ylläpidon kompleksisuudesta seuraavat haitat ylittävät sen tuomat hyödyt.

4.3 Kyberturvaratkaisut

Kyberturvaratkaisuja ovat niin henkilöstön säännöllinen kouluttaminen, kuin fyysiset laitteet ja ohjelmistot. Kyberturvallisuus koostuu monesta kerroksesta ja niiden muodostamasta kokonaisuudesta. Tietoliikenteen monitorointi, pääsynhallinta, säännölliset päivitykset sekä laadukas koulutus edesauttavat turvaamaan toimintaympäristön turvallisuutta (Pochmara & Świetlicka 2023, 1–5).

Kyberturvallisuuden ohjekehys CFS (kuva.1) auttaa yrityksiä kartoittamaan yritykseen kohdistuvia todennäköisimpiä kyberuhkia. Kyberuhilta suojautuminen on monikerroksista ja yleisesti voidaan ajatella kerrosten lisäämisen, lisäävän myös kyberturvallisuutta. Jokainen lisäkerros lisää aina kustannuksia ja siksi on tärkeää, että yrityksen valitsemat kyberturvaratkaisut ovat oikeasuhteisia, yrityksen todennäköisimpiin kyberuhkiin.

4.3.1 Viruksentorjuntaohjelmat

Viruksentorjuntaohjelma ovat kohdeympäristöön asennettu ohjelmisto mikä skannaa ympäristöön tallennettuja tiedostoja ja asennettuja ohjelmistoja. Viruksentorjuntaohjelmiston tarkoituksena on tunnistaa ja estää haitallisen ohjelmiston tai viruksen leviäminen kohdeympäristöön.

Viruksentorjuntaohjelmat vertaavat asennettuja tiedostoja tunnistettujen haittaohjelmien tietokantaan ja pyrkivät tunnistamaan jo tunnistettujen haittaohjelmien olemassaoloa.

Viruksentorjuntaohjelmat voivat myös analysoida miten ohjelmat toimivat ja ajaa ohjelmia suljetussa ympäristössä, (Sandbox) varmistaakseen että ohjelmat eivät sisällä haitallisia ominaisuuksia (Pérez-Sánchez & Palacios 2022, 1–2).

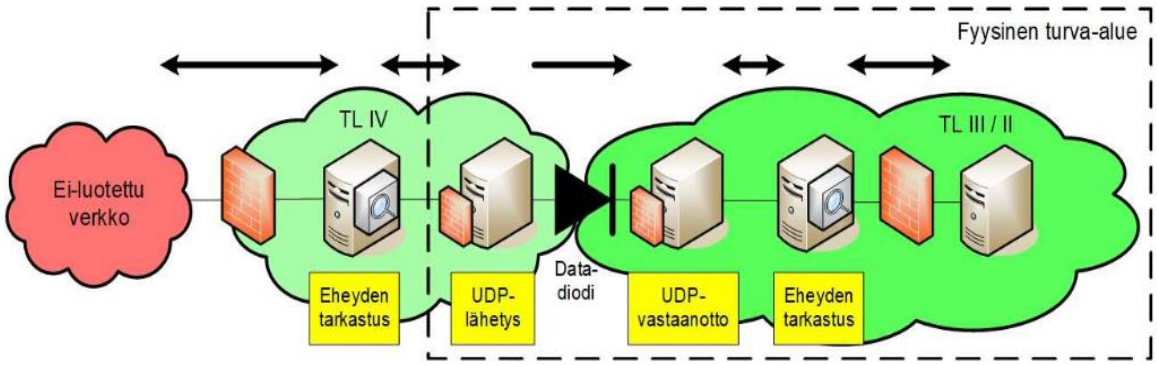
4.3.2 Palomuurit

Palomuuri on työkalu mikä vahtii ja suodattaa kahden tietoliikenneverkon välistä tietoliikennettä. Palomuuri suodattaa liikenteestä ennalta määritettyjä datapaketteja sekä pyrkii estämään ja hidastamaan haittaohjelmien leviämisen kohteen tietoliikenneverkossa (Kaspersky 2024b).

4.3.3 Datadiodit

Datadiodi on elektroninen laite, joka fyysisesti estää tiedon kahdensuuntaisen kulun kahden verkkoympäristön välillä. (Full-Duplex) Datadiodi muuntaa kahdensuuntaisen tiedonkulun yhdensuuntaiseksi (Simplex) muuntamalla signaalin kulkumuotoa datakaapelista, valokuitukaapeliin ja takaisin datakaapeliin (The Hague Security Delta 2019).

Tiedonsiirron yhdensuuntaisuus eristää kaksi toimintaympäristöä toisistaan ”ilma-aukolla” (Airgap) ja mahdollistaa tiedonsiirron luotetun ja turvattoman verkon välillä ilman, että luotetun verkon tietoihin tai sen hallintaan päästään käsiksi (Liikenne- ja viestintävirasto Traficom, 2021).



Kuva 4. Viitteellinen esimerkkitoteutus datadiodiratkaisusta (Liikenne- ja viestintävirasto Traficom, 2021).

Kuvassa 4. kuvataan tiedonsiirtoa ei-luotetusta verkosta turvalliseen verkkoon, datadiodia käyttäen. Datadiodia käytetään eristämään tietoverkot toisistaan ja estämään tiedon kaappaaminen ei-luotetusta verkosta käsin.

5 Kyberhyökkäysten vaikutukset liiketoiminnalle

5.1 Taloudelliset vaikutukset

Teoksessa 'What is the impact of successful cyberattacks on target firms?' teettämässä tutkimuksessa perehdyttiin menestyneihin pörssiyhtiöihin kohdistuneisiin kyberhyökkäysten aiheuttamiin taloudellisiin vaikutuksiin.

Tutkimuksessa todettiin, että yhtiöillä oli kyberhyökkäyksen jälkeen heikentynyt kassavirta, mikä heikentää yhtiöiden maksukykyä. Yrityksillä on erityisesti kasvanut riski konkurssiin kyberhyökkäyksen aikaisena vuotena sekä kohonnut riski sitä seuraavina vuosina. Kyberhyökkäysten seurauksena yritysten S&P luottoluokitus heikkenee vähintään kolmeksi vuodeksi. Lisäksi kyberhyökkäys vaikuttaa pörssiyhtiöiden arvon suhteeseen, käytettäviin varoihin, mikä heikentää yritysten puskuria pärjätä heikossa taloustilanteessa (Kamiya ym. 2018, 26–27).

Yleisimpien kyberhyökkäysten seurauksena ei ole odotettavissa merkittäviä taloudellisia seuraamuksia, sillä yleisimmät kyberhyökkäykset eivät ole merkittäviä seuraamuksiltaan ja ovat yleisesti helposti rajattavissa ja pysäytettävissä. Merkittävät taloudelliset seuraamukset aiheutuvat merkittävien tietomurtojen ja palvelunestohyökkäysten aikana, kun suuria määriä yrityksen arkaluontoista materiaalia on vuotanut julki tai yrityksen operointi on keskeytynyt.

5.2 Yrityksen mainehaitta

Tutkimusartikkelissa “Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018” tutkittiin kyberhyökkäysten vaikutusta yritysten maineeseen vuosien 2002 ja 2018 välisenä aikana. Tutkimuksen löydökset koskien, kärsivätkö yritykset mainehaitasta kyberhyökkäyksen jälkeen olivat, että yritysten maine kasvaa yleisimmissä kyberhyökkäyksissä.

Tämä johtuu siitä, että yleisimmät kyberhyökkäykset eivät vaikuta merkittävästi yritysten toimintaan, vaan ovat pikemmin hidaste.

Merkittävät kyberhyökkäykset ja tietomurrot sen sijaan vaikuttavat yritysten maineeseen. Mainehaitat ovat kuitenkin yleisesti yritysten kannalta vähemmän merkittäviä, kuin merkittävästä kyberhyökkäyksestä aiheutuvat taloudelliset vahingot, jotka johtuvat liiketoimintaoperaatioiden merkittävistä häiriöistä (Makridis 2021, 1, 7).

Mainehaitta on yritysten kannalta vähäisempi asia kuin taloudelliset vahingot, koska yleisimmät kyberhyökkäykset eivät johda yrityksen liiketoiminnan kannalta merkittäviin seuraamuksiin.

Yritysten mainehaittaa kyberhyökkäyksen seurauksena on vaikea mitata, sillä siihen vaikuttavat monet eri tekijät ja ihmiset näkevät asiat monesta eri näkökulmasta. Vaikka merkittävä osa kyberhyökkäyksistä ei vaikuta negatiivisesti yritysten maineeseen, voivat ilmiselvät laiminlyönnit ja rikokset vaikuttavat siihen. Itse pelkän kyberhyökkäyksen uhriksi joutuminen ei vaikuta yrityksen maineeseen, mutta miten yritys hoitaa kyberhyökkäyksen torjunnan voi.

5.3 Juridiset seuraamukset

Yleisimmät juridiset seuraamukset, mitä yritykset nykyään kohtaavat, liittyvät tietosuojakäytänteisiin ja tiedon tallentamiseen. Yritykset tallentavat asiakkaista ja yksityishenkilöistä merkittävää määrää tietoa ja yritykset ovat aiemmin käyttäneet näitä tietoja tarkoituksettomalla tavalla. Lisäksi henkilötietojen ja asiakaskäyttäytymistietojen jälleenmyyminen on merkittävää liiketoimintaa. Hallitakseen yritysten toimintaa ja parantaakseen yksityishenkilöiden tietosuojaa, Euroopan Unioni kehitti vuonna 2018 yleisen tietosuoja-asetuksen GDPR (General Data Protection Regulation) (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679).

GDPR:n tarkoituksena oli yhtenäistä EU-alueen käytänteitä ja lainsäädäntöä henkilötietojen keräämiseen ja taltiointiin. GDPR:n keskiössä on läpinäkyvyys, yritysten on ilmoitettava mitä tietoja he keräävät ja miten he hyödyntävät niitä. Yksityishenkilöillä on oikeus esittää tietosuojapyyntö rekisterin ylläpitäjälle ja saada tietää, mitä tietoja hänestä on kerätty, sekä vaatia tietojen poistamista. Rekisterin ylläpitäjillä on velvollisuus vastata tähän tietopyyntöön uhkasakon uhalla.

Yritykseen kohdistuneen mahdollisen tietomurron tapauksessa, jossa henkilötietojen vuotamisesta on syytä epäillä merkittävää haittaa, yrityksillä on velvoite ilmoittaa toimimaan tietosuojavaltuutetulle tietomurrosta. Ilmoitusvelvoitteen tarkoituksena on parantaa yksityishenkilöiden oikeusturvaa ja lisätä läpinäkyvyyttä, sillä monet yritykset eivät tiedota ulospäin yleisölle mahdollisesta tietomurrosta, johtuen tietomurrosta koituvista mahdollisista taloudellisista ja imagollisista seuraamuksista.

Tietosuojarikokset ovat käytännössä ainoita juridisia seuraamuksia, mitä yrityksille voi koitua, mikäli yritykset eivät ole riittävällä tavalla noudattaneet tietosuoja-asetusta ylläpitäessään henkilötietorekisteriä.

Esimerkki tietosuojarikoksesta, missä yritys ei täyttänyt velvoitteitaan koskien yleistä tietosuoja-asetusta, kun yritykseen kohdistui merkittävä tietomurto. Lokakuussa 2020, suomalaisen psykoterapiakeskus Vastaamon keräämiä ja tallentamia henkilötietoja ja potilaskertomuksia julkaistiin internetissä. Tietoja julkaissut taho kiristi Vastaamon potilaita sekä toimihenkilöitä maksamaan tälle virtuaalivaluuttaa, ettei hyökkääjä julkaisisi uhrien tietoja (Syyttäjänlaitos 2024).

Vastaamon tietomurrosta paljastui merkittäviä laiminlyöntejä yrityksen johdon toimesta, jotka johtivat ehdolliseen vankeusrangaistukseen Vastaamon silloiselle toimitusjohtajalle. Vastaamon johto oli ohittanut sille tiedossa olevia puutteita tietosuojassa, jotka lopulta johtivat tietomurtoon ja henkilötietojen julkaisuun (Yle 2023).

6 Tuotantolaitoksiin kohdistuneita kyberhyökkäyksiä

6.1 Tapaus: Stuxnet – Kyberhyökkäys Iranin ydinpolttoaineen jalostukseen

Stuxnet on kehittynyt mato-haittaohjelma, joka suunniteltiin hyökkäämään teollisuudessa käytettyjä tuotannonohjausjärjestelmiä (SCADA) vastaan. Haittaohjelman arkkitehtuuri koostui useasta eri ohjelmointikielestä ja sisälsi osia, jotka olivat salattu salausalgoritmeilla, jottei niiden todellinen sisältö selviäisi.

Stuxnet oli suunniteltu saastuttamaan teollisuudessa käytettyjä ympäristöjä ja antamaan hallintaoikeudet ja kyvyn suorittaa komentoja kohteessa, ilman että kohde havaitsee haitallista toimintaa. Mato-haittaohjelmalla on kyky saastuttaa ja levitä useisiin ympäristöihin ja haittaohjelmaa voidaan kohdistaa myös käyttäjiin, jotka työskentelevät toimipaikoissa, joiden ympäristö on suljettu kokonaan pois internetistä. Työntekijöiden käyttämiä USB-laitteita voitiin saastuttaa ja kun nämä veivät laitteita suljettuun ympäristöön, haittaohjelma onnistui leviämään kenenkään huomaamatta. Ohjelmalla oli kyky päivittää itsensä sekä kommunikoida muiden saastuneiden ympäristöjen kanssa.

Stuxnet oli luotu saastuttamaan Iranin ydinohjelmassa käytetty ydinpolttoaineenjalostamo. Stuxnet onnistui tuhoamaan jalostamossa käytetyt sentrifugit, joita käytetään ydinpolttoaineen jalostamisessa. Sentrifugit ovat erittäin herkkiä äkilliselle nopeudenvaihtelulle ja ohjelma onnistui tuhoamaan herkän laitteiston, muuttamalla laitteiden nopeutta siten, ettei laitteiden ohjausjärjestelmissä ilmennyt käyttäjälle mitään poikkeavaa (Baezner & Robin 2017, 6–7, 9–10).

Stuxnet on yksi maailman tunnetuimmista esimerkeistä monikerroksisesta kyberhyökkäyksestä. Hyökkäykseen liittyy useita eri vaiheita ja kaikkia ei varmuudella tunneta, sillä osa haitallisesta koodista oli salattua.
Hyökkäys kuvastaa miten ihminen on minkä tahansa tietojärjestelmän heikoin lenkki, sillä Stuxnet levisi tuotantoympäristöön saastuneelta USB-tallennusvälineeltä.

Tarkkaa tietoa siitä oliko USB-tallennusväline sellainen, jonka laitoksen työntekijä oli poiminut maasta, ei tiedetä. Tapaus silti kuvastaa miten korkean turvatason järjestelmissä, suunnitteluhierarkia missä käyttäjä pääsee omalla toiminnallaan mahdollisesti vaarantamaan tuotantoympäristön toiminnan, ei ole soveltuvaa. Arkkitehtuuri ei ota huomioon ihmisen toiminnasta aiheutuvia virheitä tai vahinkoja.

6.2 Tapaus: NotPetya – Kansainvälinen logistiikkayhtiö Maersk joutuu kiristyshaittaohjelman uhriksi

Vuonna 2017, tuolloin maailman suurin rahtiyhtiö volyymiltaan, Maersk, joutuu kiristyshaittaohjelman uhriksi, kun ukrainalaiset pankit kokivat merkittävän kyberhyökkäyksen. Ukrainalaiset pankit ja Maersk käyttivät samaa ohjelmistoa veronpalautuksien hallitsemiseen ukrainalaisten työntekijöiden palkka-asioihin liittyen. Maersk joutui sivulliseksi uhriksi, kun saastuneet ukrainalaiset pankit, edelleen levittivät haittaohjelma NotPetyaa. Haittaohjelman seurauksena, koko Maerskin verkko saastui vain 7 minuutissa. Haittaohjelma vaikutti merkittävästi yrityksen jokaiseen toiminta-alueeseen ja Maersk joutui kääntymään katastrofisuunnitelmiin ja manuaalisiin asiakastilausmenettelemiin.

Hyökkäyksen seurauksena Maerskille koitui arvioilta 300–350 miljoonan dollarin vahingot, sekä maailmanlaajuisesti hyökkäyksestä koitui noin 10 miljardin dollarin välilliset kustannukset. Maerskin osakekurssi laski vuoden aikana hyökkäyksestä -27 % (Pownall 2019, 3–10).

Stuxnet ja Notpetya ovat hyvin tunnettuja esimerkkejä kyberhyökkäyksistä, jotka ovat onnistuneet merkittävästi häiritsemään tai keskeyttämään hyökkäyksen kohteen toiminnan. Molemmissa tapauksissa, hyökkäykset kohdistettiin korkeasti suojattuun tuotantoympäristöön ja yhteiskunnan kannalta kriittisiin toimintoihin. Tapaukset osoittavat, etteivät edes merkittävät panostukset pysty takaamaan täydellistä kyberturvaa.

7 Tekoälyn vaikutukset kyberturvallisuuteen

7.1 Tekoälyn vaikutukset kyberhyökkäyksiin

Tekoälyllä tarkoitetaan älykästä automaatiota, jossa tietokonealgoritmi pystyy osittaiseen tai täysimittaiseen autonomiaan ja päätöksentekoon.
Tekoälyn avulla on mahdollista generoida tekstiä, kuvia, ohjelmointikoodia sekä ääntä ja sen avulla on mahdollista tunnistaa trendejä kerätystä datasta.
Tekoälyä voidaan käyttää työskentelyn tehostamiseen, teknologian mahdollistamien uusien työkalujen avulla. Kuten kaikessa teknologiassa, tekoälyä voidaan hyödyntää myös haitalliseen toimintaan, kuten kehittyneiden kyberhyökkäysten suunnitteluun ja toteuttamiseen.

Tekoälyllä voidaan automatisoida tehtäviä, joita aiemmin hyökkääjät joutuivat suorittamaan manuaalisesti, näitä voivat olla haavoittuvuuksien etsintä, valvontaohjelmistojen välttely sekä hyökkäyksiä voidaan tehdä nopeammin.
Tekoälyn avulla mahdollistetaan kokonaan uudenlaiset hyökkäysmuodot.

Tekoälyn avulla voidaan luoda myös realistisempia virtuaalisia kopioita ihmisistä ja tehdä yhä kehittyneempiä kuva ja videomanipulaatioita.
Videon ja kuvan lisäksi, tekoälyllä pystytään luoda kopioita ihmisten äänistä ja luoda äänitteitä, joita ei oikeasti tapahtunut, käyttämällä toisen henkilön ääntä haluamalla teksti tai äänisyötteellä. Näitä äänisynteesejä voidaan yhdistää videomanipulaatioihin imitoimaan haluttua ihmistä ns. Deepfake video (Liikenne- ja viestintävirasto Traficom, 2022c, 8–9).

7.2 Hyökkäykset ja suojautuminen

Tekoälyä voidaan käyttää kyberhyökkäysten suunnittelemiseen, niiden toteuttamiseen tai edistyneiden haittaohjelmien kehittämiseen. Koneoppia (Machine Learning) voidaan hyödyntää analysoimaan hyökkäyksen kohteen IT-järjestelmien hierarkiaa, jonka avulla voidaan käyttää tiedossa olevia toimivia hyökkäyksiä järjestelmiä vastaan, ilman että hyökkääjä joutuu tekemään pitkään kestävää tiedustelua ja taustatyötä (Vassilev ym. 2023, 6). Kohteen tiedustelu antaa hyökkääjälle paremman kokonaiskuvan mihin kohdentaa hyökkäystä ja mitä kohde on mahdollisesti tallentanut järjestelmäänsä. Tekoäly tehostaa päätöksentekokykyä ja kykenee autonomiseen toimintaan, jolloin haittaohjelma pystyy vain ilmoittamaan hyökkääjälle löytäneensä jotain arvokasta.

Tekoälyä voidaan hyödyntää lisäämään tietoturvaa kyberhyökkäyksiä vastaan, analysoimalla tietoliikennettä epäilyttävän liikenteen osalta sekä analysoimaan aiemmin tehtyjen hyökkäyksien yhtäläisyyksiä, kyberinfrastruktuurin parantamiseksi (Das & Sandhane 2021, 6).

Samaa menetelmään kuin hyökkäyksessä voidaan käyttää IT-järjestelmien puolustamiseen. Tekoäly on tehokas oppimaan kuvioita ja malleja tapahtumien joukosta ja ymmärtää syy seuraus suhteita koneluettavasta datasta paremmin kuin ihmiset, mahdollistaen suuremman data määrän tehokkaamman prosessoimisen.

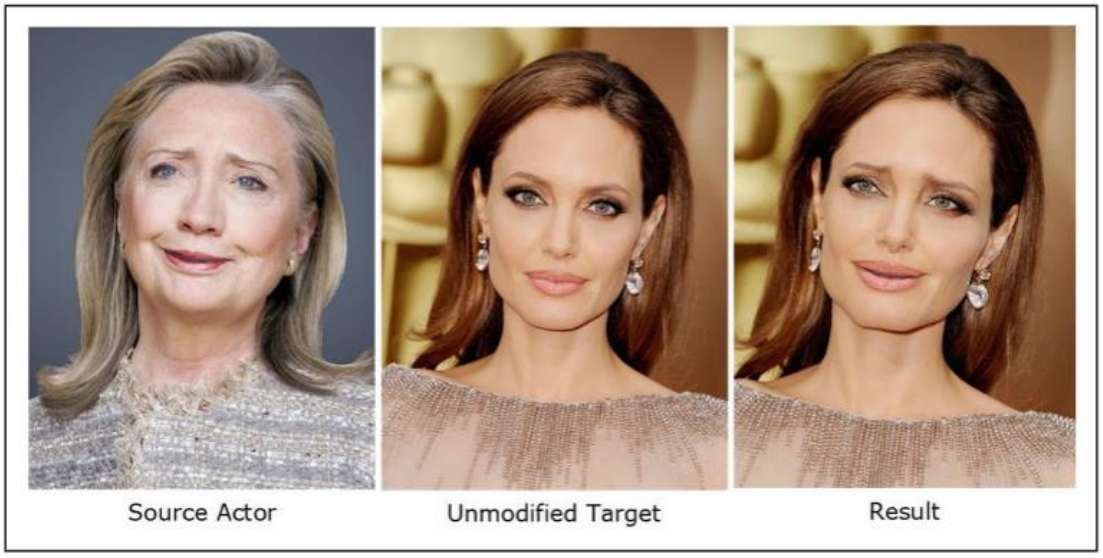
Opinnäytetyön kirjoitushetkellä, vuoden 2024 kesällä, tekoälyn avulla luodut kyberhyökkäykset ovat hyvin muuttuvassa tilassa, ja ilmiö tekoälyn ympärillä on hyvin aktiivinen ja uusia tuotteita ja avoimen lähdekoodin ratkaisuja julkaistaan jatkuvasti. Yleinen trendi tekoälyn ympärillä on lisääntyvä autonomia ja monimutkaisten tehtävien suorittaminen. Tilanne tekoälyyn liittyvien kyberuhkien osalta on todennäköisesti muutaman vuoden sisällä erilainen kuin tällä hetkellä.

Yritysten on kuitenkin tärkeää tunnistaa tekoälyyn liittyvä potentiaali ja sen tuomia uhkakuvia hyvissä ajoin, vaikka teknologian tila ei ole tällä hetkellä vielä vakiintunut.

7.3 Syväväärennökset (Deepfake)

Syväväärennöksillä (Deepfake) tarkoitetaan videomanipulaatiota, jossa imitoidaan halutun ihmisen kasvonpiirteitä, eleitä ja ääntä. Tarkoituksena on luoda realistinen kopio kohdehenkilöstä ja luoda virtuaalinen kopio kyseisestä henkilöstä kontekstissa, jota ei ikinä tapahtunut. Virtuaalisen kopion ohjaamiseen käytetään lähdevideota, jossa kuka tahansa henkilö pystyy toistamaan halutut eleet ja liikkeet, mitkä virtuaalinen kopio toistaa.
Näitä virtuaalisia kopioita voidaan käyttää tallentamaan videoita tai käyttämään reaaliajassa, kuten videopuhelussa, esiintymällä valheellisella identiteetillä (Yhdysvaltain kotimaan turvallisuusvirasto 2024, 5).

Deepfake virtuaalisilla kopioilla kenestä tahansa ihmisestä voidaan luoda virtuaalinen ”nukke” jolla voidaan elehtiä ja kommunikoida videon välityksellä tai reaaliajassa. Nukkea ohjataan vertailuvideolla, jolla esitetään halutut eleet ja kasvonilmeet. Deepfake videoon voidaan myös sisällyttää kenen tahansa henkilön ääni, jota halutaan imitoida (Masood ym. 2022, 18).



Kuva 5. Visuaalinen esitys ”nukkemestari” menetelmästä, lähdevalokuva (vas.), kohdevalokuva (kesk.), kasvon eleiden risteytys (oik.) (Masood ym. 2022, 18).

Kuvassa 5. esitetään, miten lähdevalokuvan henkilön kasvonilmeitä, manipuloidaan kohdevalokuvan kasvoilla.

Syväväärennökset luovat todellisen uhan ihmisille tunnistaa videon aitoutta teknologian kehittyessä ja tultaessa useamman käyttäjän saataville.
Hong Kongissa sijaitseva monikansallinen yritys joutui deepfake-huijauksen uhriksi, kun yrityksen työntekijät luulivat keskustelevansa videopuhelun välityksellä yrityksen talousjohtajan kanssa, kun todellisuudessa he keskustelivat kyberrikollisen kanssa, joka oli tekeytynyt talousjohtajaksi. Lisäksi kaikki muut henkilöt, videopuhelussa olivat myös deepfake väärennöksiä, yhtä henkilöä lukuun ottamatta, uhria, joka ajautui rikollisten ansaan. Kyberrikolliset onnistuivat huijaamaan yritykseltä 200 miljoonaa Hong Kongin dollaria, joka vastaa noin 25 miljoonaa Yhdysvaltain dollaria (CNN 2024).

Syväväärennökset tarjoavat kehittyneen teknologisen manipulaatioratkaisun matalalla kynnyksellä. Madaltunut kynnys päästä käsiksi kyseiseen teknologiaan yhdistettynä merkittävillä teknologisilla kehitysaskelilla, tekevät Deepfake videoista petollisen uhkakuvan tulevaisuuden kyberuhille. Olemme nähneet jo ensimmäisen ison mittakaavan Deepfake huijauksen, kun Hong Kongissa sijaitsevalta yritykseltä onnistuttiin huijaamaan 25 miljoonan Yhdysvaltain dollarin edestä varallisuutta.

On vain ajan kysymys, kun Deepfake videoita aletaan käyttämään yhä kehittyneempiin tietojenkalastelu ja huijausvideoihin. Teknologian kyvykkyys yhdistettynä motivoituneella hyökkääjällä on vaarallinen yhdistelmä.
On todennäköistä, että ensisijaisesti Deepfake teknologiaa tullaan näkemään perinteisten huijausviestien laadun paranemisessa kuin merkittävissä määrin yrityksiin kohdistetuissa yksilöllisissä huijauksissa kuten Hong Kongilaiseen yritykseen tehtiin.

On kuitenkin mahdollista, että deepfake videoita aletaan kasvavissa määrin käyttämään yrityksiin kohdistuvissa kalastelukampanjoissa.

8 Johtopäätökset ja kehitysideat

8.1 Johtopäätökset

Opinnäytetyö osoittaa miten kyberturvallisuuden tilanne eri valmistussektoreilla vaihtelee johtuen käytettävissä olevien resurssien määrästä, toimialojen säännöstelystä, osaamisessa sekä yritysten toimintakulttuurista.
Yleisesti suomalaisissa tuotantolaitoksissa tilanne on kohtuu hyvällä tasolla, mutta puutteita kyberturvallisuuden perusteiden kanssa on yleisesti monessa yrityksessä. Merkittävimpinä puutteina ovat kyberturvallisuusstrategian puuttuminen sekä tietojärjestelmiin liittyvän dokumentoinnin taltiointi.

Puutteet kuvastavat yritysten suhtautumista kyberturvallisuuteen kulueränä, sillä kyberturvallisuuden toimenpiteet ja työkalut eivät itsessään lisää yritysten myyntiä tai paranna tulosta. Kyberturvallisuuden tarkoituksena on antaa yrityksille toimintaedellytykset toimia ja estää merkittävien liiketoimintahäiriöiden tapahtuminen.

Yritystoimintaan liittyy aina riski ja monesti riski on taloudellinen.
Kyberturvallisuuden puutteiden realisoituminen merkittäväksi taloudelliseksi seuraamukseksi on yritysten näkökulmasta epätodennäköisempää kuin kyberturvallisuus asiantuntijoiden. Yritykset ovat valmiita hyväksymään tämän riskin ja jotkut yritykset elävät riskien kanssa, osaamisen puuttumisen takia.

Tuotantolaitokset voivat olla houkuttelevia kohteita kyberhyökkäyksille niiden merkityksen kannalta valtion keskeisimmille toiminnoille, kuten energiantuotannon ja isojen keskusvarastojen osalta.
Kyberrikollisten tavoittelema taloudellinen hyöty on myös yksi merkittävä motiivi, mikä saavutetaan kiristämällä kohdeyritystä varastetuilla liikesalaisuuksilla.

Tuotantolaitosten eri tiedonvaihtojärjestelmien ja toiminnanohjausjärjestelmien turvaamiseksi on useita ratkaisuja, käytänteitä ja ohjelmistoja.
Ratkaisujen käyttämistä tulisi arvioida yrityksen IT-järjestelmän ja todennäköisten uhkien perusteella, siten että ne muodostavat monikerroksisen

kokonaisuuden, joka vastaa todennäköisimpiin kyberuhkiin.
Yritysten on tunnistettava toimintaympäristönsä ja siihen kohdistuvat todennäköisimmät kyberuhat. Tekijöitä, jotka vaikuttavat kyberuhkiin ovat yrityksen liiketoiminta-alue sekä liiketoimiala.

Suurilla kyberhyökkäyksillä voi olla merkittäviä taloudellisia vaikutuksia yrityksen toimintakykyyn. Yleisimmät kyberhyökkäykset eivät yleensä aiheuta hyökkäyksen kohteena olevalle yritykselle merkittäviä taloudellisia vahinkoja tai merkittävää mainehaittaa. Merkittävät laiminlyönnit tietosuojassa voivat johtaa rikosoikeudellisiin toimenpiteisiin, mikäli yrityksen johto on laiminlyönyt sille osoitettuja velvoitteita yleisen tietosuoja asetuksen mukaisesti (GDPR). Yritysten keräämän tiedon määrän kasvun takia ja muuttuva lainsäädännön takia yritykset voivat tietämättään syyllistyä tietosuojarikokseen, mikäli he eivät noudata yleisessä tietosuoja asetuksessa määritettyjä velvoitteita.

Tekoälyyn liittyvät mahdollisuudet ja tietoturvauhat ovat jatkuvasti kehittyvä aihe ja lopullisia vaikutuksia on vielä vaikeaa tietää. Yritysten tulee pysyä ajan tasalla nopeasti kehittyvän teknologian parissa, sillä kehittyneet hyökkäysmuodot kuten autonomiset haittaohjelmat sekä Deepfake syvävääreennökset voivat johtaa merkittäviin taloudellisiin vahinkoihin, elleivät yritykset tunnista muuttunutta uhkakuvaa. Tekoälyn saavutettavuus madaltaa kynnystä käyttää tekoälyä osana haittaohjelmakampanjoita ja sen tekniset ominaisuudet mahdollistavat jopa amatöörille tuloksia mitä aiemmin ei olisi voinut saavuttaa.

Tuotantoyritysten on kehitettävä osaamistaan vastaamaan nykyistä teknologista kehitystä sekä muuttaa suhtautumistaan kyberturvallisuuteen pelkkänä taloudellisena kuluna. Tekoälyn kehityksen nykynopeudella tuotantoyritykset meinaavat jäädä digitalisaatiossa ja kyberturvallisuudessa jälkeen muita toimialoja.

Tietoisuuden lisääminen tuotantoyritysten kesken on keskiössä nykyisen tilanteen kääntämiseksi.

8.2 Kehitysideat

Tuotantoyritysten kyberturvallisuudessa on merkittävää vaihtelua ja esiin nousseet puutteet ovat kyberturvallisuusstrategian sekä teknisen dokumentoinnin puuttuminen. Puutteet ovat luonteeltaan sellaisia, etteivät ne vaadi merkittäviä taloudellisia panostuksia, jos lainkaan.

Suomalaiset tuotantoyritykset tarvitsevat lisää kyberturvallisuuden osaamista ja yritysten omistajat tietoa kyberturvallisuuden integroimiseksi osaksi yrityksen kokonaisturvallisuusstrategiaa. Yritysten on kartoitettava puutteet kyberturvallisuudessa mikä sisältää käytössä oleva teknologian kartoittamisen, puutteet tietoturvakäytänteissä, henkilöstön koulutustason ja osaaminen sekä teknisen dokumentaation kartoittamisen. Koska monelta yritykseltä puuttuu tarvittava osaaminen toteuttaa kyberturvallisuuden edistämistä ja ylläpitoa, joutuvat he työskentelemään asiantuntija yrityksen kanssa korjatakseen puutteet. Suomen valtion intresseissä on edistää yleistä huoltovarmuutta ja valtio voisi edistää ja tukea kyberturvallisuuden edistämistä kehittämällä valtionvirastojen ja eri yritysten tiedonvaihtoa sekä tukea erinäisten kyberturvaratkaisuitten hankintaa.

Tekoälyn nopea kehitysvauhti pakottaa yritykset heräämään uuden teknologian tuomiin uhkakuviin sekä hankkimaan osaamista, joka edistää nykyisten puutteiden korjaamista. Uudet teknologiat kuten tekoäly muovaavat teknologista kenttää yhä nopeampaa tahtia kuin mitä aikaisemmin on nähty. Yritykset, joilla on ollut puutteita jo aikaisemmin, tulevat huomaamaan, etteivät heidän nykyiset järjestelmänsä pysty suojaamaan heitä uudenlaisilta uhilta.

Jatkotutkimus ideana opinnäytetyön pohjalta olisi tutkia pitkällä aikavälillä miten suomalaisten tuotantoyritysten kyberturvallisuuden tilanne kehittyy.
Asiasta ei ole vielä julkisesti saatavilla olevaa tutkimustietoa.
Jatkotutkimus voisi auttaa tuotantoyrityksiä paremmin ymmärtämään miten yritysten osaaminen kehittyy vastaamaan teknologista kehitystä sekä millaisia puutteita yritysten toiminnassa esiintyy.

Lähteet

Anumbe, N.; Saidy, C. & Harik, R. 2022. A Primer on the Factories of the Future. Sensors, 22(15), 5834. Viitattu 16.5.2024. https://www.mdpi.com/1424-8220/22/15/5834

Baezner, M. & Robin, P. 2017. CSS CYBER DEFENSE PROJECT Hotspot Analysis: Stuxnet. Center for Security Studies (CSS), ETH Zürich. Viitattu 2.6.2024. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf

Bhavsar, V., Kadlak, A. ja Sharma, S. 2018. Study on Phishing Attacks, International Journal of Computer Applications. Viitattu 16.5.2024. https://www.researchgate.net/publication/361086563_Deepfakes_generation_and_detection_state-of-the-art_open_challenges_countermeasures_and_way_forward

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N. ja Varese, F. 2024. Mapping the global geography of cybercrime with the World Cybercrime Index. Viitattu 16.5.2024. https://doi.org/10.1371/journal.pone.0297312

Das, R. ja Sandhane, R. 2021. Artificial Intelligence in Cyber Security, J. Phys. Viitattu 16.5.2024. https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (ETA:n kannalta merkityksellinen teksti) Viitattu 1.6.2024. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Huoltovarmuuskeskus. 2020. Kyberturvallisuuden nykytila eri toimialoilla keskeiset havainnot. Viitattu 2.6.2024. https://www.huoltovarmuuskeskus.fi/files/b3671ecb5d0b5b431174fec9350e0251b75227ba/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf

Kamiya, S., Kang, J-K., Kim, J., Milidonis, A. ja Stulz, R. M. 2018. 'What is the Impact of Successful Cyberattacks on Target Firms?', NBER Working Paper No. 24409. Viitattu 16.5.2024. https://www.nber.org/system/files/working_papers/w24409/w24409.pdf

Kaspersky. 2024. Mikä nollapäivähyökkäys on? Määritelmä ja selitys. Viitattu 16.5.2024. https://www.kaspersky.fi/resource-center/definitions/zero-day-exploit

Kaspersky. 2024b. What is a firewall? Definition and explanation. Viitattu 16.5.2024. https://www.kaspersky.com/resource-center/definitions/firewall

Kauppalehti 2024. Suomen varustamot varautuvat nyt poikkeustilanteeseen Itämerellä – Ulkomaankaupasta kulkee meritse peräti 96 prosenttia. Viitattu 16.5.2024. https://www.kauppalehti.fi/uutiset/suomen-varustamot-varautuvat-nyt-poikkeustilanteeseen-itamerella-ulkomaankaupasta-kulkee-meritse-perati-96-prosenttia/8668ee32-4aec-447b-acff-296ebad1d94a

Kenge, R. 2020. A Research Study on the ERP System Implementation and Current Trends in ERP. Shanlax International Journal of Management. Viitattu 2.6.2024. https://www.researchgate.net/publication/344453940_A_Research_Study_on_the_ERP_System_Implementation_and_Current_Trends_in_ERP

Kielitoimiston sanakirja. 2024. Tehdas. Viitattu 16.5.2024. https://www.kielitoimistonsanakirja.fi/tehdas

Laari, J.; Flyktman, M.; Härmä, V.; Timonen, P. & Tuovinen, S. 2019. #kyberpuolustus: Kyberkäsikirja Puolustusvoimien henkilöstölle. Viitattu 16.5.2024. https://urn.fi/URN:ISBN:978-951-25-3120-2.

Liikenne- ja viestintävirasto Traficom. 2024.Traficomin haittaohjelmahavainnot. Viitattu 16.5.2024. https://tieto.traficom.fi/fi/tilastot/traficomin-haittaohjelmahavainnot?toggle=Muita%20tietol%C3%A4hteit%C3%A4%20ja%20lis%C3%A4tietoja

Liikenne- ja viestintävirasto Traficom. 2021. Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista. Viitattu 16.5.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Yhdyskaytavaratkaisuohje.pdf.

Liikenne- ja viestintävirasto Traficom. 2022. Toimintaohje – Kiristyshaittaohjelma. Viitattu 16.5.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/KiristyshaittaohjelmaToimintaohje.pdf.

Liikenne- ja viestintävirasto Traficom. 2022b. Toimintaohje – Palvelunestohyökkäys. Viitattu 16.5.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf.

Liikenne- ja viestintävirasto Traficom. 2022c. Tekoälyn mahdollistamat kyberhyökkäykset. Viitattu 16.5.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TRAFICOM_Teko%C3%A4lyn_mahdollistamat_kyberhy%C3%B6kk%C3%A4ykset%202022-12-12_web.pdf

Makridis, C. A. 2021. Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018, Journal of Cybersecurity. Viitattu 16.5.2024. https://doi.org/10.1093/cybsec/tyab021

Mallik, A. 2019. 'MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS', Cyberspace: Jurnal Pendidikan Teknologi Informasi. Viitattu 16.5.2024. https://www.researchgate.net/publication/335385872_MAN-IN-THE-MIDDLE-ATTACK_UNDERSTANDING_IN_SIMPLE_WORDS

Masood, M., Nawaz, M., Malik, K., Javed, A., Irtaza, A. ja Malik, H. 2022. Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward, Applied Intelligence. Viitattu 16.5.2024. https://www.researchgate.net/publication/361086563_Deepfakes_generation_and_detection_state-of-the-art_open_challenges_countermeasures_and_way_forward

McCallam, D.H., 2024. An Analysis of Cyber Reference Architectures. Viitattu 16.5.2024. https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-IST-170/EN-IST-170-09.pdf

Yhdysvaltain standardisointi ja teknologiainstituutti. 2024. The NIST Cybersecurity Framework (CSF) 2.0. Viitattu 16.5.2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Pochmara, J. & Świetlicka, A. 2023. Cybersecurity of Industrial Systems—A 2023 Report. Electronics. Viitattu 16.5.2024. https://www.mdpi.com/2079-9292/13/7/1191

Pownall, C. 2019. The Context and Impact of Maerk's NotPetya cyber attack. Viitattu 16.5.2024. https://www.researchgate.net/publication/346080185_The_Context_and_Impact_of_Maerk's_NotPetya_cyber_attack

Ross, P. & Maynard, K. 2021. Towards a 4th industrial revolution. Intelligent Buildings International. Viitattu 2.6.2024. https://www.tandfonline.com/doi/full/10.1080/17508975.2021.1873625

Smith, J. R.; Yost, J. & Lopez, H. 2020. Electronic data interchange and enterprise resource planning technology in supply chain contracts. Computers & Industrial Engineering. Viitattu 16.5.2024. https://www.sciencedirect.com/science/article/pii/S0360835220300644.

Suomen virallinen tilasto (SVT): Rikos- ja pakkokeinotilasto 2024. Helsinki: Tilastokeskus. Viitattu 16.5.2024. https://stat.fi/tilasto/rpk

The Hague Security Delta 2019. Understanding the Strategic and Technical Significance of Technology for Security: The Case of Data Diodes for Cybersecurity.

Viitattu 16.5.2024. https://securitydelta.nl/media/com_hsd/report/246/document/HSD-Rapport-Data-Diodes.pdf

Valtioneuvosto 2023. Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa. Viitattu 16.5.2024. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164793/VN_2023_31.pdf?sequence=1&isAllowed=y.

Vassilev, A. (NIST), Oprea, A. (Northeastern University), Fordyce, A. (Robust Intelligence) & Anderson, H. (Robust Intelligence). 2024. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. Viitattu 2.6.2024. https://csrc.nist.gov/pubs/ai/100/2/e2023/final

Syyttäjänlaitos. 2024. Vastaamo-tietomurron käsittely Syyttäjälaitoksessa. Viitattu 16.5.2024. https://syyttajalaitos.fi/vastaamo

Yadav, G. & Paul, K. 2021. Architecture and security of SCADA systems: A review. International Journal of Critical Infrastructure Protection. Viitattu 16.5.2024. https://www.sciencedirect.com/science/article/pii/S1874548221000251.

Yle 2023. Psykoterapiakeskus Vastaamon entinen toimitusjohtaja Ville Tapio tuomittiin tietosuojarikoksesta kolmen kuukauden ehdolliseen vankeusrangaistukseen. Viitattu 16.5.2024. https://yle.fi/a/74-20027598