Eemeli Seppänen

KIRISTYSOHJELMAHYÖKKÄYKSET JA KRIITTISEN INFRASTRUKTUURIN JÄRJESTELMIEN RISKIT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Seppänen Eemeli
Kiristysohjelmahyökkäykset ja kriittisen infrastruktuurin järjestelmien riskit
Jyväskylä: Jyväskylän yliopisto, 2024, 33 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Vuorinen, Jukka

Suurten kiristysohjelmahyökkäyksien määrä on kasvanut huomattavasti viimeisen kymmenen vuoden aikana. Hyökkäysten lisääntyessä myös kriittiseen infrastruktuuriin kohdistuvat iskut ovat yleistyneet. Tunnettuja esimerkkejä ovat esimerkiksi WannaCry- ja NotPetya-kiristysohjelmat, jotka ovat aiheuttaneet suurta taloudellista vahinkoa usealle alan toimijalle. Tämä tutkielma tarkasteli kriittisen infrastruktuurin teknologisia haavoittuvuuksia keskittyen erityisesti kiristysohjelmahyökkäyksiin, kriittisen infrastruktuurin järjestelmäkokonaisuuksiin ja niiden välisten yhteyksien luomiin riskeihin. Tutkielma jakoi eri järjestelmäkokonaisuudet informaatioteknologian järjestelmiin, operationaalisen teknologian järjestelmiin ja teollisuuden esineiden internetin järjestelmiin. Tutkimuksessa vastataan tutkimuskysymyksiin ”minkälaisia riskejä tieteellinen kirjallisuus on tunnistanut kriittisen infrastruktuurin järjestelmäkokonaisuuksista suhteessa kiristysohjelmahyökkäyksiin? ja ”mihin järjestelmiin tapahtuneet kiristysohjelmahyökkäykset ovat kohdistuneet?”. Tutkielma analysoi aiheen tieteellistä kirjallisuutta ja merkittäviä tietomurtoja kuvailevalla kirjallisuuskatsauksella. Tutkielmassa vertailtiin eri järjestelmien ja niiden välisten yhteyksien riskejä peilaten niitä toteutuneisiin kiristysohjelmahyökkäyksiin. Tutkielmassa myös pohdittiin tulevia kehityskulkuja teollisuuden esineiden internetin laitteiden yleistyessä. Tutkielman tuloksien mukaan kriittisen infrastruktuurin laajojen järjestelmäkokonaisuuksien riskejä on tunnistettu laajasti tieteellisessä kirjallisuudessa. Tuloksien mukaan myös teollisuuden esineiden internetin riskejä on pyritty tarkastelemaan hypoteettisten hyökkäystilanteiden kautta, mutta niiden varsinaista roolia tulevissa hyökkäyksissä ei olla vielä täysin tunnistettu. Järjestelmien välisiin yhteyksiin ja niiden lisääntymiseen pitäisi kiinnittää enemmän huomiota tulevaisuudessa. Tuloksista paljastuu, että eri järjestelmien välisten yhteyksien lisääntyminen luo todennäköisesti riskejä erityisesti niille järjestelmille, joita ei ole luotu tietoturvallisuus etusijalla.

Asiasanat: kiristysohjelmat, kriittinen infrastruktuuri, operationaalinen teknologia, teollisuuden esineiden internet

ABSTRACT

Seppänen, Eemeli
Ransomware attacks and the risks of critical infrastructure systems
Jyväskylä: University of Jyväskylä, 2020, 33 pp.
Information Systems Science, Bachelor´s Thesis
Supervisor(s): Vuorinen, Jukka

A trend of ransomware attacks on critical infrastructure has started as cybercriminal groups look for targets willing to pay large sums to recover their important data. As the amount of notorious ransomware attacks on critical infrastructure increase, more rigorous analysis of the common vulnerabilities and the risks they create for critical infrastructure is needed. This thesis aimed to create a wide understanding of why and how these attacks should be addressed by answering the following research questions: "how has current scientific literature recognized the risks of ransomware attacks on different systems used by critical infrastructure?" and "which systems are targeted in ransomware attacks on critical infrastructure?". By analysing these issues this thesis aimed to give a concrete example of how ransomware attacks tend to happen to the multiple technological systems modern critical infrastructure utilize in their daily operations, and how the increasing interconnectedness of these systems has affected the situation. This thesis found that modern critical infrastructure employs different kinds of systems with varying levels of security in their implementations. Previous attacks suggest that a system connected to the internet often makes critical infrastructure vulnerable to attack, even in situations where the connected system is not directly used in operational actions. Furthermore, we find that the interconnectedness of these systems creates risks that have been underappreciated when developing new technology aimed at increasing efficiency.

Keywords: ransomware, critical infrastructure, operational technology, industrial internet of things

TAULUKOT

SISÄLLYS

1 JOHDANTO

Riggsin ym. (2023) mukaan merkittävien kyberhyökkäysten määrä on lisääntynyt huomattavasti viimeisen kymmenen vuoden aikana. Merkittävä kyberhyökkäys määritellään tässä kontekstissa hyökkäyksenä, joka kohdistuu valtion virastoihin, puolustusalaan, teknologiayrityksiin sekä kaikkiin muihin kriittisen infrastruktuurin toimijoihin, kun hyökkäyksen tuottama vahinko on yli miljoona Yhdysvaltain dollaria. He ennustavatkin, että merkittävien kyberhyökkäysten määrän kasvu saattaa kiihtyä eksponentiaalisesti lähivuosina (Riggs ym., 2023).

Kyberhyökkäyksien nopea kasvun vuoksi sen riskit tulisi ottaa paremmin huomioon myös tietojärjestelmätieteen alalla. Lisääntyneet hyökkäykset luovat suuria riskejä organisaatioille, joille normaalin toiminnan pysähtyminen muutamaksi päiväksi voi merkitä suuria tappioita.

Yksi merkittävä ja nykypäivänä usein kohdattu kyberhyökkäyksen muoto on kiristysohjelmahyökkäys. Hyökkäyksessä kiristysohjelma lukitsee tai salaa järjestelmän tai sen tärkeitä tiedostoja, jonka jälkeen ohjelma vaatii lunnassumman maksua tietojen tai järjestelmän palauttamiseksi (Symantec, 2015). Kiristysohjelmahyökkäyksen kohteeksi voi joutua periaatteessa mikä tahansa laite tai tietojärjestelmä, mutta Ozin, Arışin, Levin ja Uluagacin (2022) mukaan hyökkäyksen kohteen valikoitumiseen ja hyökkäyksen tavoitteiden onnistumiseen vaikuttaa kohteen halukkuus maksaa lunnaat. Kriittisen infrastruktuurin tärkeä asema modernissa yhteiskunnassa voi siis tehdä siitä houkuttelevan kohteen, sillä lyhyetkin käyttökatkot voi tuottaa suuria ongelmia.

Kriittiseen infrastruktuuriin kohdistuvien kiristysohjelmahyökkäyksien lisääntymistä ei ole käsitelty riittävästi tieteellisessä kirjallisuudessa. Tämän tutkimuksen tavoite oli tukea tulevaa tutkimusta kartoittamalla, miten tieteellisessä kirjallisuudessa on käsitelty eri kriittisen infrastruktuurin toimijoiden käyttämien järjestelmätyyppien haavoittuvuuksia kiristysohjelmahyökkäyksille. Tutkimus pyrki kartoittamaan eri järjestelmätyyppien omia haavoittuvuuksia sekä järjestelmien välisiä yhteyksiä, jotka voivat lisätä riskejä eri tarkoituksiin suunniteltuissa järjestelmissä. Kriittinen infrastruktuuri jaetaan tarkastelussa yleisen käytänteen mukaisesti informaatioteknisiin (IT) järjestelmiin sekä operationaalisen teknologian (OT) järjestelmiin. Näiden järjestelmätyyppien lisäksi

tarkasteluun otetaan teollisuuden esineiden internetin (IIoT) laitteet, joiden käyttö vaihtelee eri järjestelmäkokonaisuuksien välillä, mutta joiden käytön uskotaan lisääntyvän teknologian kehittyessä (Al-Hawawreh ym, 2023). Tutkimuksen tavoite on siis vastata seuraaviin tutkimuskysymyksiin:

- Minkälaisia riskejä tieteellinen kirjallisuus on tunnistanut kriittisen infrastruktuurin järjestelmäkokonaisuuksista suhteessa kiristysohjelmahyökkäyksiin?
- Mihin järjestelmiin tapahtuneet kiristysohjelmahyökkäykset ovat kohdistuneet?

Hyökkäysten määrän lisääntyminen ja aihetta moniulotteisesti tutkivan kirjallisuuden puute luo tarpeen aiheen tieteelliselle tarkastelulle. Tämä tutkimus pyrkii vastaamaan tarpeeseen analysoimalla lähteitä, jotka käsittelevät kiristysohjelmahyökkäyksiä sekä kriittisen infrastruktuurin tietoturvariskejä. Tarkoituksena oli luoda kokonaiskuva aiempien tutkimuksien löydöksistä, jotka liittyvät kriittisen infrastruktuurin järjestelmäkokonaisuuksiin, järjestelmäkokonaisuuksien välisiin yhteyksiin ja kiristysohjelmahyökkäysten mahdollisiin vaikutuksiin.

Tutkimukseen on kerätty tieteellisiä lähteitä hyödyntäen tietokantoja kuten JYKDOK, Scopus, IEEE Xplore ja Google Scholar-hakukonetta. Käytettyjä hakusanoja ovat ”ransomware”, ”critical infrastructure”, ”risks”, ”operational technology”, ”internet of things” ja niiden eri yhdistelmiä. Valitut tieteelliset julkaisut on rajattu niihin, joiden julkaisulehti on saanut Julkaisufoorumin arvosteluasteikolla vähintään arvosanan 1. Tällä rajoituksella on pyritty varmistamaan valittujen artikkelien laatu. Lisäksi artikkelien arvioinnissa on huomioitu niiden julkaisuajankohta, viittausten määrä ja lehden merkitys tieteenalalla. Tieteellisten lähteiden valinnassa on myös huomioitu niiden julkaisuvuosi siinä määrin, kun se vaikuttaa ymmärrykseemme kiristysohjelmista ja kriittisestä infrastruktuurista. Suurin osa lähteistä on kuitenkin varsin uusia, sillä aiheesta käytävä tieteellinen keskustelu on lisääntynyt viime vuosina. Tieteellisten lähteiden lisäksi tutkielmassa on hyödynnetty alan virastojen ja yritysten raportteja ja tietopankkeja. Esimerkiksi Yhdysvaltain kyberpuolustusvirasto CISA:n raportteja on hyödynnetty laajasti luvun 4 esimerkkitapausten käsittelyssä.

Tutkielma analysoi toisessa luvussa kiristysohjelmien yleisiä piirteitä kuten niiden eri tyyppejä ja yleisiä toimintatapoja. Tutkielman kolmannessa luvussa analysoidaan yleisiä riskejä, joita kriittisen infrastruktuurin toimijat kohtaavat eri järjestelmäratkaisujen ja niiden haavoittuvuuksia hyödyntävien hyökkäysten vuoksi. Luvussa luodaan myös kokonaiskuva järjestelmien välisistä yhteyksistä. Tutkielman neljännessä luvussa tarkastellaan miten kiristysohjelmahyökkäykset voivat vaikuttaa näihin järjestelmiin ja kriittiseen infrastruktuuriin esimerkkitilanteiden kautta.

2 KIRISTYSOHJELMAT

2.1 Kiristysohjelman määritelmä

Symantecin (2015) mukaan kiristysohjelma on haittaohjelma, joka estää laitteen halutun käytön esimerkiksi lukitsemalla laitteen tai salaamalla käyttäjälle tärkeitä tiedostoja. Kiristysohjelmaan kuuluu usein kiristysvaihe, jossa ohjelma kiristää käyttäjää salauksen tai laitteen lukituksen poistamiseksi (Symantec, 2015). Keshavarzin ja Ghaffaryn (2020) määritelmä on hyvin samankaltainen, mutta he erikseen painottavat, kuinka kiristysohjelman toiminta voi perustua sekä datapohjaiseen, että ei-datapohjaiseen kiristämiseen. Datapohjainen kiristäminen viittaa esimerkiksi tietokoneiden tärkeiden tiedostojen käytön estämiseen. Ei-datapohjainen kiristäminen voi puolestaan olla esimerkiksi tietokoneen käyttöjärjestelmän käytön esto, jolloin esto ei kohdistu tiettyyn käyttäjälle tärkeään dataan, vaan itse laitteen yleiseen käyttöön (Keshavarzi & Ghaffary, 2020). Kiristysohjelman määritelmä voi siis hieman vaihdella eri näkökulmista tarkasteltuna, mutta niille yhteistä on tietokoneen halutun käytön estäminen ja sillä kiristäminen. Määritelmä ei näiden määritelmien valossa ole juurikaan muuttunut viime vuosina, vaikka kiristysohjelmahyökkäyksissä on nähty uusia trendejä.

Kiristysohjelmahyökkäyksen kohteena voi olla mikä tahansa tietokone, mutta kriittisten infrastruktuurin merkitys yhteiskunnan toiminnalle tekee niistä houkuttelevia kohteita taloudellisesti motivoituneille hyökkääjille (Riggs ym., 2023). Tämä oletettavasti johtuu suuren organisaation maksukyvystä ja normaalin toiminnan jatkuvuuden kriittisyydestä. Kiristysohjelmahyökkäys voi kohdistua muullekin laitteelle kuin tietokoneelle, mutta erityisesti Windows-pohjaiset tietokoneet ovat kiristysohjelmahyökkäyksien yleisin kohde (Oz ym., 2022).

2.2 Kiristysohjelmatyypit ja toimintamallit

Kiristysohjelmat voidaan jakaa erilaisiin tyyppeihin riippuen niiden toimintaperiaatteista. Jako salaavien ja lukitsevien kiristysohjelmien välillä on yksi yleinen ja yksinkertainen tapa luokitella kiristysohjelmia (Oz ym., 2022). Kiristysohjelmilla on kuitenkin monia muunlaisia toimintaperiaatteita, joita tarkastelemalla voimme saada selvemmän kuvan erilaisista kiristysohjelmatyypeistä. Muita tyyppejä on esimerkiksi pyyhkijäohjelma ja vuoto-ohjelma, joiden toimintatavat ja usein myös motiivit eroavat lukitsevista ja salaavista ohjelmista (Keshavarzi & Ghaffary, 2020). Näiden lisäksi on tärkeää ymmärtää kiristysohjelma palveluna toimintamalli, sillä sitä on pidetty merkittävänä syynä kiristysohjelmahyökkäysten viimeaikaiseen yleistymiseen (Keshavarzi & Ghaffary, 2020). Kiristysohjelma palveluna ei tule käsittää muista kiristysohjelmatyypeistä erillisenä tyyppinä, vaan mahdollisena toimintamallina eri kiristysohjelmahyökkäyksien suorittamiseen.

2.2.1 Salaavat kiristysohjelmat

Symantecin (2015) mukaan salaavat kiristysohjelmat käyttävät kryptografisia salausmenetelmiä tietojärjestelmiin ja niiden tiedostoihin, jolloin tietojen käyttö estyy, ellei salausta pureta salausavaimella. Kryptografisten menetelmien kehittyneisyyden vuoksi salauksen murtaminen ilman avainta voi olla käytännössä mahdotonta (Symantec, 2015). Salauksen tehokkuus kiristämisen välineenä tekee salaavasta kiristysohjelmasta vaarallisen kiristysohjelmatyypin. Salaava kiristysohjelma myös antaa hyökkäyksen kohteelle käsityksen, että salatut tiedostot voidaan vielä palauttaa maksamalla vaadittu lunnassumma. Tämä käsitys palvelee niitä hyökkääjiä, joiden tavoitteena on taloudellinen hyöty. Kiristysohjelman saastuttamaa laitetta voi usein käyttää osittain normaalisti, mutta ohjelman salaamia tiedostoja ei voi enää käyttää (Symantec, 2015).

2.2.2 Lukitsevat kiristysohjelmat

Lukitsevat kiristysohjelmat lukitsevat järjestelmän käytön hyödyntämällä järjestelmän omia turvallisuusmekanismeja, kuten näytönlukitusta, käyttäjätilin salasanaa ja tietokoneen käynnistykseen käytetyn master boot record-osion salausta (Riggs ym., 2023). Al-rimyn, Maarofin ja Shaidin (2018) mukaan Lukitseva kiristysohjelma siis kykenee estämään pääsyn järjestelmään ilman, että kiristysohjelma itse salaa varsinaisia tiedostoja tai käyttöjärjestelmää. Salausmekanismin puutteen vuoksi hyökkäyksen kohteella ei ole samankaltaista painetta lunnassumman maksamiseen, sillä järjestelmä ja sen tiedostot voidaan palauttaa ilman salauksen murtamista (Al-rimy ym., 2018). Lukitseva kiristysohjelma siis yleensä estää pääsyn tietokoneen käyttöjärjestelmään tai käyttäjän tilille, mutta ohjelma ei salaa tietokoneen muistissa olevia tiedostoja, jolloin niiden palauttaminen toiselle laitteelle tai uuteen käyttöjärjestelmään on usein mahdollista. Oz ym. (2022)

huomauttavatkin, että salauksen puute on lukitsevien kiristysohjelmien suurin heikkous, joka pienentää niiden uhkaa verrattuna salaaviin kiristysohjelmiin.

2.2.3 Muita kiristysohjelmatyyppejä

Kiristysohjelmien kentältä löytyy myös muunlaisia ohjelmia, jotka toimivat kiristysohjelmien tapaisesti, mutta joiden käsittäminen kiristysohjelmana ei ole kiistatonta. Esimerkiksi pyyhkijäohjelma, englanniksi wiper, voi näyttäytyä kiristysohjelmana, mutta usein ohjelman perimmäinen tarkoitus on poistaa hyökkäyksen kohteena olevan järjestelmän tiedostot (Keshavarzi & Ghaffary, 2020). Tästä syystä Keshavarzi ja Ghaffary (2020) huomauttavat, että pyyhkijäohjelma voidaan käsittää myös omana haittaohjelmaperheenään. Ohjelman käyttö on kuitenkin yleistä erilaisissa kyberhyökkäyksiin liittyvissä kiristystilanteissa, joten he käsittävät sen yhdeksi kiristysohjelmatyypiksi. Pyyhkijäohjelmahyökkäyksen motivaatio voi kuitenkin olla erilainen kuin useimmilla kiristysohjelmahyökkäyksillä, sillä se soveltuu paremmin tuhoaviin hyökkäyksiin kuin kiristykseen (Keshavarzi & Ghaffary, 2020).

Toinen yleisistä kiristysohjelman toimintatavoista eroava ohjelmatyyppi on niin sanottu vuoto-ohjelma, englanniksi leakware, joka kiristää hyökkäyksen kohdetta tietojen vuotamisella avoimeen internettiin, mikäli lunnassummaa ei makseta (Razaulla ym., 2023). Keshavarzi ja Ghaffary (2020) pitävät tätä kiristysohjelmatyyppiä varsin vaarallisena, sillä varmuuskopioiden pitäminen ei riitä kriittisten tiedostojen suojaamiseen. Vuoto-ohjelmahyökkäyksen lunnaiden maksu ei myöskään takaa hyökkäyksen kohteelle varsinaista turvaa tiedostojen vuotamisen varalta, sillä hyökkääjällä on pääsy tiedostoihin myös lunnasmaksun jälkeen. Vuoto-ohjelmaan voi sisältyä myös lukitsevan tai salaavan kiristysohjelman piirteitä (Keshavarzi & Ghaffary, 2020).

2.2.4 Kiristysohjelma palveluna

Kiristysohjelma palveluna, englanniksi ransomware-as-a-service tai RaaS, on palveluna myytävä kiristysohjelmahyökkäyksiin käytetty toimintamalli, jossa kiristysohjelmahyökkäys tilataan niitä tarjoavalta palveluntuottajalta. RaaS-palveluita alkoi ilmestymään noin vuonna 2015, kun verkkorikollisuusjärjestöt alkoivat tehdä hyökkäyksen aloittamisesta yksinkertaista ja haluttuun kohteeseen helposti räätälöitävää (Oz ym., 2022). RaaS-palveluiden yleistyminen on uskottu olevan merkittävä osatekijä kiristysohjelmahyökkäysten lisääntymiseen, sillä hyökkäyksen tilaaja ei tarvitse itse aloitetun hyökkäyksen vaatimia tietoteknisiä taitoja (Keshavarzi & Ghaffary, 2020).

Bakerin (2023) mukaan RaaS-operaattori, eli kiristysohjelmapalvelun ylläpitäjä tarjoaa käyttäjälle tarvittavat ohjauspaneelit ja maksukanavat kiristysohjelmahyökkäyksen toteutukseen. Niiden avulla asiakas voi itse määritellä hyökkäyksen uhrin ja kiristyssumman. Asiakas usein hallitsee itse salauksen poistoon tarvittavia salausavaimia, jotka asiakas voi itse antaa hyökkäyksen uhrille, mikäli asiakas niin päättää. RaaS-palvelulle on monta hinnoittelujärjestelmää,

esimerkiksi kuukausimaksut, voittojen jakaminen RaaS-palveluntarjoajan kanssa ja lisensointimaksut (Baker, 2023).

2.3 Yleiset toimintavaiheet

Kiristysohjelmahyökkäyksen vaiheita voidaan tarkastella samankaltaisessa kontekstissa kuin muitakin haittaohjelmahyökkäyksiä. Haittaohjelmahyökkäyksien vaiheiden analysointiin tietoturva-alalla käytetään usein Lockheed Martinin (ei pvm.) kehittämää viitekehystä, kyberhyökkäysketjua, englanniksi cyber kill chain. Kiristysohjelmahyökkäyksen kulun analysointi tieteellisessä kirjallisuudessa usein pitkälti vastaa Lockheed Martinin esittämää mallia, vaikka mallia ei eksplisiittisesti mainittaisikaan. Malliin kuuluu yleensä seitsemän hyökkäyksen kulkua kuvaavaa vaihetta. Mallin vaiheet ovat kohteen tiedustelu, haittaohjelman aseistaminen, kohdelaitteelle toimitus, haavoittuvuuden hyötykäyttö, ohjelman asentaminen, kommunikaatio hyökkääjän oman palvelimen kanssa ja haluttujen toimintojen suorittaminen (Lockheed Martin, ei pvm.).

Vaiheiden määrä vaihtelee eri tutkimusten välillä, mutta niiden esittämät toimet ovat erittäin samankaltaisia. Al-rimy ym. (2018) esittävät viiden askeleen mallin, jossa haitallinen koodi ensin saadaan kohdelaitteeseen, jonka jälkeen ohjelma kerää tietoa kohdelaitteesta, muodostaa yhteyden hyökkääjän omaan palvelimeen, tunnistaa tärkeät tiedostot kohdelaitteen muistista, salaa ne ja viimeisenä kiristää hyökkäyksen kohdetta. Esitetyssä mallissa kuitenkin huomioidaan vain salaavan kiristysohjelman vaiheet.

Keshavarzi ja Ghaffaryn (2020) esittämä malli on hyvin samankaltainen, mutta se sisältää myös kuudennen vaiheen, jossa lunnasrahan saatuaan hyökkääjä joko purkaa salauksen, poistaa lukituksen tai ei tee mitään. Mallissa huomioidaan myös lukitsevat kiristysohjelmat vaihtoehtoisella toimintapolulla, jossa tietojen salaamisen sijaan järjestelmä lukitaan (Keshavarzi & Ghaffary, 2020).

Ozin ym. (2022) malli taas on jo esitettyjä malleja tiiviimpi, sillä se sisältää vain murtautumis-, kommunikaatio-, tuhoamis-, ja kiristämisvaiheet. Mallissa kutsuttu tuhoaminen viittaa kaikkiin vihamielisiin keinoihin, kuten tietojen salaamiseen tai järjestelmän lukitsemiseen (Oz ym., 2022). Mallissa ei käsitellä erillistä tietojen keräämistä kohdelaitteesta, tärkeiden tiedostojen tunnistamista tai Keshavarzin ja Ghaffaryn (2020) esittämää kuudetta vaihetta, jossa kuvataan lunnasrahojen maksamisen jälkeistä tilannetta.

Dargahin ym. (2019) malli on käsitellyistä malleista ainoa, joka eksplisiittisesti viittaa Lockheed Martinin kyberhyökkäysketjuun. Malli kuitenkin jättää pois kyberhyökkäysketjun tiedusteluvaiheen, sillä heidän mukaansa sitä ei voida pitää varsinaisena kiristysohjelmahyökkäykselle ominaisena vaiheena (Dargahi ym., 2019).

Käsiteltyjen lähteiden perusteella saamme kiristysohjelmahyökkäyksestä monivaiheisen kuvan, jossa järjestelmään ensin murtaudutaan usein tietoteknistä haavoittuvuutta hyödyntäen, jonka jälkeen ohjelma kerää tietoja

järjestelmästä, muodostaa yhteyden hyökkääjän omalle palvelimelle, salaa tärkeät tiedostot tai lukitsee koko järjestelmän, kiristää hyökkäyksen kohdetta ja lopulta päättää hyökkäyksen saatuaan lunnassumman. Vaiheiden tarkastelusta myös huomaamme, etteivät kiristysohjelmien perustavanlaatuiset toimintaperiaatteet ole juurikaan muuttuneet eri tutkimusten ajankohtien välillä.

Kiristysohjelmahyökkäyksessä on monta vaihetta, mutta tietyt vaiheet ovat erityisen kriittisiä tutkielman aiheelle. Myöhemmän analyysin kannalta tärkeitä vaiheita ovat erityisesti järjestelmään murtautuminen, tiedostojen manipulointi ja hyökkäyksestä palautuminen. Nämä vaiheet ovat tutkielman kannalta kriittisiä siksi, että niiden avulla voimme pyrkiä ymmärtämään miten kiristysohjelmat vaikuttavat kriittisen infrastruktuurin järjestelmiin. Analysoimalla murtautumisvaihetta saamme ymmärryksen siitä, miten kiristysohjelma voi murtautua suojattuun järjestelmään. Manipulointivaihe on myös kriittinen analyysin kannalta, sillä manipulointivaihe luo todennäköisesti suurimman esteen kriittisen infrastruktuurin järjestelmien toiminnalle. Hyökkäyksestä palautuminen on myös kriittinen vaihe, sillä se vaikuttaa normaalin toiminnan palauttamiseen.

2.3.1 Järjestelmään murtautuminen ja asentuminen

Kiristysohjelma voi murtautuu laitteeseen, kuten tietokoneeseen, käyttäen järjestelmän haavoittuvuutta, joka sallii vieraan koodin ajamisen laitteella (Oz ym., 2022). Tällaisessa tilanteessa laitteen käyttäjä ei aktiivisesti itse aja haitallista tiedostoa, vaan sen pääsy koneeseen perustuu haavoittuvuuksiin esimerkiksi laitteen käyttöjärjestelmässä, joka mahdollistaa laitteen hallinnan. Automaattisesti leviävät kiristysohjelmat kuten WannaCry leviävät organisaation järjestelmissä laitteesta laitteeseen hyödyntäen näitä haavoittuvuuksia (Symantec, 2017). Dargahin ym. (2019) mukaan leviäminen perustuu usein joko laitteen etäkäyttöominaisuuden tai Windowsin tiedostojen jakoon käytettyä Server Message Block (SMB)-protokollan haavoittuvuuksiin.

Kiristysohjelma voi kuitenkin päätyä kohdelaitteeseen myös käyttäjän asentamana. Mahdollisia tapoja kiristysohjelman pääsyyn koneelle on esimerkiksi malvertising, eli haitalliset mainokset, roskaposti ja tietojenkalastelu (Dargahi ym, 2019; Keshavarzi & Ghaffary, 2020). Malvertising-hyökkäyksessä kiristysohjelma tekeytyy yleisesti käytetyksi tietokoneohjelmaksi ja sen lataussivustolle ostetaan mainoksia esimerkiksi hakukoneen hakutulossivulta (Cozens, 2023). Tässä leviämistavassa käyttäjä siis luulee ladanneensa etsimänsä ohjelman ja asentaa sen laitteelleen. Roskapostitse leviävä kiristysohjelma voi myös sisältää haitallisen linkin, joka ohjaa uskottavan näköiselle sivustolle, mutta ohjelma voi myös olla osa sähköpostin liitetiedostoa (Keshavarzi & Ghaffary, 2020). Dargahin ym. (2019) mukaan kiristyshaittaohjelma saattaa olla tekeytynyt esimerkiksi normaalin näköiseksi Microsoft Word-tiedostoksi, jonka ajettaessa kiristyshaittaohjelma asentuu laitteeseen. Microsoft Office-tuoteperheen makro-ominaisuudet ja PDF-tiedostojen JavaScript-koodi tekee niistä mahdollisia haittaohjelmien asentumiskanavia (Keshavarzi & Ghaffary, 2020).

Kiristysohjelman asentamisvaihe käyttää erilaisia teknisiä metodeja laitteen turvamekanismien kuten virustorjuntaohjelmien välttämiseksi, ettei käyttäjä

ehdi reagoida hyökkäykseen ennen lunnasvaatimuksen esittämistä (Keshavarzi & Ghaffary, 2020).

Kiristysohjelma siis usein murtautuu käyttäjän laitteeseen tekeytymällä yleisesti käytetyksi, luotettavaksi ohjelmaksi tai muuksi tiedostomuodoksi. Päästyään organisaation verkkoon tietyt kiristysohjelmatyypit voivat myös siirtyä toisiin samassa verkossa oleviin laitteisiin aiemmin esitetyillä keinoilla ja niiden haavoittuvuuksilla. Yksi käyttäjävirhe voi siis riskeerata koko organisaation verkon turvallisuuden, mikäli laitteiden virustorjuntaohjelmisto ei havaitse hyökkäystä ja organisaation verkosta löytyy haavoittuvuuksia. Myöhemmissä luvuissa käsitellään tarkemmin sitä, miten esimerkiksi kriittisen infrastruktuurin toimijat ovat pyrkineet erottelemaan järjestelmiään, jotta hyökkäyksen leviämispotentiaali pienenisi.

Kiristysohjelman laitteeseen murtautumisvaihe on hyvin samankaltainen kuin muillakin yleisillä haittaohjelmilla. Kiristysohjelmien toiminnan erot muihin yleisiin haittaohjelmiin nousevat esiin vasta myöhemmissä vaiheissa.

2.3.2 Tiedostojen manipulointi

Tässä erityisesti kiristysohjelmille ominaisessa vaiheessa kiristysohjelma manipuloi järjestelmää ja sen tiedostoja joko lukitsemalla järjestelmän hyödyntäen järjestelmän omia ominaisuuksia, salaamalla tiedostot kryptografisin menetelmin tai aloittamalla tärkeiden tiedostojen poiston (Keshavarzi & Ghaffary, 2020).

Tiedostojen manipulointivaihe on siis usein ensimmäinen vaihe, jossa kiristysohjelmatyyppi ja hyökkäyksen mahdolliset motiivit voivat tulevat esiin. Manipulointivaiheessa tehdyt toimet voivat siis johtaa pysyvään tai väliaikaiseen tilanteeseen, jossa hyökkäyksen kohde menettää pääsyn kriittisiin tiedostoihin tai kokonaiseen järjestelmään.

2.3.3 Hyökkäyksestä palautuminen

Tiedostojen manipuloinnin jälkeen kiristysohjelma aloittaa varsinaisen kiristysvaiheen, jossa ohjelma vaatii hyökkäyksen kohteelta lunnassummaa. Lunnassumma vaihtelee hyökkääjän ja hyökkäyksen kohteen mukaan. Al-Hawawreh, Hartog ja Sitnikova (2019) nostavat esimerkiksi kiristysohjelma WannaCry:n, joka vaati vain muutaman sadan dollarin lunnassummaa. Ozin ym. (2022) mukaan lunnasvaatimuksen summa vaihteleekin usein sen perusteella, kuinka suuri organisaatio on ja kuinka kriittisenä hyökkääjä pitää sen toimintaa. Korkeat lunnassummat johtavat myös uusien tietoteknisesti taidokkaiden hyökkääjien palkkaamiseen, jolloin myös erittäin kohdistetut ja monimutkaiset hyökkäykset on mahdollisia (Oz ym., 2022). Kohdistetuissa hyökkäyksissä lunnasvaatimukset voivat nousta miljooniin dollareihin (Al-Hawawreh ym., 2019). Taloudellisesti motivoidut kiristysohjelmat yleensä pitävät lupauksensa tiedostojen palauttamisesta, sillä tunnettu huijaustapaus voi johtaa tilanteeseen, jossa kaikki kohteet lopettavat lunnaiden maksamisen (Dargahi ym, 2019). Viranomaiset eivät kuitenkaan suosittele lunnaiden maksamista, sillä se ei takaa tiedostojen palauttamista

ja voi johtaa uusiin hyökkäyksiin tai lunnasvaatimuksiin (CISA, 2021a). Lunnassumma vaaditaan usein virtuaalivaluuttana kuten Bitcoinina vahvan sääntelyn puutteen ja valuuttalompakkojen pseudonymisyyden takia (Oz ym., 2022; Conti, Gangwal & Ruj, 2018).

Salaavan kiristysohjelman salaus on usein mahdotonta purkaa ilman hyökkääjän hallussa olevaa salausavainta (Symantec, 2015). Siksi usein ainoa tapa palauttaa tärkeät tiedostot ilman lunnaiden maksamista on tiedostojen palauttaminen varmuuskopioista. Lukitsevasta kiristysohjelmasta voi yleensä palautua esimerkiksi käyttöjärjestelmän uudelleenasennuksella (Oz ym., 2022).

3 KRIITTISEN INFRASTRUKTUURIN JÄRJESTELMIEN JA NIIDEN VÄLISTEN YHTEYKSIEN RISKIT

3.1 Kriittisen infrastruktuurin määritelmä ja osa-alueet

Yhdysvaltain kyberpuolustusviraston CISA:n (ei pvm.) mukaan jopa 16 yhteiskunnan osa-aluetta voidaan käsittää osaksi kriittistä infrastruktuuria. Lista sisältää esimerkiksi terveydenhuollon, valtion virastot, energiasektorin, puolustussektorin ja monen muun valtion turvallisuudelle ja taloudelle merkittävän osa-alueen. Makrakisin, Koliaksen, Kambourakisin, Riegerin ja Benjaminin (2021) määritelmä kriittiselle infrastruktuurille on samansuuntainen. Heidän mukaansa kriittiseksi infrastruktuuriksi voidaan käsittää entiteetit ja järjestelmät, jotka ovat niin välttämättömiä yhteiskunnan toiminnan kannalta, että niiden toimimattomuus vaarantaisi julkisen terveyden, kansallisen turvallisuuden ja taloudellisen hyvinvoinnin (Makrakis ym, 2021). CISA:n luokituksen mukaiset yhteiskunnan osa-alueet täyttävät myös Makrakisin ym. (2021) määritelmän.

3.2 Kriittisen infrastruktuurin järjestelmät ja riskit

Kriittistä infrastruktuuria ohjataan usein teollisilla ohjausjärjestelmillä, jotka muodostuvat informaatioteknologian ja operationaalisen teknologian järjestelmistä (Perrett & Wilson, 2023). Informaatioteknologinen (IT) järjestelmä voidaan käsittää niinä järjestelminä, joilla tuetaan kriittisen infrastruktuurin organisaation liiketoimintaa (Makrakis ym., 2021). Tietojärjestelmätieteelle yleiset toiminnanohjausjärjestelmät lukeutuvat siis myös IT-järjestelmiin. Operationaalisen teknologian (OT) järjestelmä taas vastaa organisaation käyttämien, usein teollisten koneiden ohjaamisesta (Makrakis ym., 2021). Perrettin ja Wilsonin (2023)

mukaan OT-järjestelmiksi voidaan käsittää kaikki ne järjestelmät, jotka eivät ole osa yritystoimintaan käytettyä IT-järjestelmää. OT-järjestelmän laitteisiin voi kuulua esimerkiksi ohjelmoitavan logiikan (PLC) laitteet ja teolliset valvontaohjelmistot (SCADA) (Perrett & Wilson, 2023). OT-järjestelmät siis vastaavat usein varsin kriittisten teollisten laitteiden ohjaamisesta, joiden toimintakyky on tärkeää kriittiselle infrastruktuurille kuten tehtaille ja sähkölaitoksille. OT-järjestelmät siis eroavat IT-järjestelmistä niiden käyttötarkoituksen perusteella.

Hyökkäys kriittistä infrastruktuuria vastaan voi mahdollisesti tapahtua myös hyökkäyksellä esineiden internetin laitteisiin, joita eri organisaatiot ovat ottaneet käyttöön IT- ja OT-järjestelmien ohjaamiseen. Al-Hawareh ym. (2019) osoittivat tutkimuksessaan, että yleistyneiden teollisuuden esineiden internetin, IIoT:n, laitteiden haavoittuvuudet voivat toimia hyökkäysrajapintana, jolla kriittisen infrastruktuurin toimintoja voidaan lamauttaa. Makrakis ym. (2021) huomauttavat, että organisaatioiden tulisi huomioida lisääntyneet tietoturvariskit, mikäli IIoT-laitteita halutaan lisätä osaksi organisaation järjestelmäkokonaisuutta.

Yhdistämällä nämä kolme teknologista järjestelmää saamme käsityksen niistä järjestelmistä, joita useat kriittisen infrastruktuurin toimijat käyttävät. Eri järjestelmien käyttöaste ja toimijan riippuvuus sen toiminnasta vaihtelee toimijoiden välillä. Esimerkiksi IIoT-laitteiden käyttöönoton houkute voi kuitenkin olla merkittävä, sillä ne voivat huomattavasti helpottaa eri järjestelmien hallintaa (Dhirani, Armstrong & Newe, 2021). Taulukko 1 kuvaa näitä järjestelmiä ja niiden merkitystä kokonaisuuden toiminnalle. Järjestelmiä ja niiden välisiä rajoja tarkastellessa on kuitenkin tärkeä muistaa Nicolin (2021) havainto, että IT- ja OT-järjestelmät voivat olla yhteydessä toisiinsa myös ilman teollisuuden esineiden internettiä.

Taulukko 1 Kriittisen infrastruktuurin eri järjestelmät (Makrakis ym., 2021)

Järjestelmä	**Käyttötarkoitus**	**Esimerkki**
Informaatioteknologien järjestelmä	Käytetään yrityksen liiketoiminnan hallinnoimiseen.	Windows-päätelaite
Operationaalisen teknologian järjestelmä	Ohjaa operationaaliseen toimintaan käytettyjä laitteita.	Teolliset koneet
Teollisuuden esineiden internet	Mahdollistaa laitteiden hallinnan, tarkkailun ja datan keräämisen.	Tarkkailusensorit

3.2.1 Informaatioteknologian riskit

Informaatioteknologiaa käytetään kriittisessä infrastruktuurissa niihin tehtäviin, jotka eivät suoraan liity operationaaliseen toimintaan. Näihin toimiin voi kuuluu esimerkiksi liiketoiminta. Informaatioteknologiset laitteet on usein liitetty avoimeen internettiin, sillä toiminta muiden organisaatioiden kanssa vaatii myös kommunikaatiota oman infrastruktuurin ulkopuolelle (Nicol, 2021). Mahdollisia IT-järjestelmien osia ovat sähköpostipalvelimet ja liiketoiminnan ohjelmistot kuten toiminnanohjausjärjestelmät (Staves, Gouglidis, Maesschalck & Hutchison,

2024). IT-järjestelmät ovat siis pitkälti yhteydessä internettiin. Informaatioteknologian avoimet yhteydet vaikuttavat olevan kaikista riskialttein osa kriittisen infrastruktuurin järjestelmäkokonaisuutta. Informaatioteknologian riskeihin voidaan siis ajatella kuuluvan pitkälti samat riskit, kuin muihinkin internettiin kytkettyihin laitteisiin. Tieteellisen kirjallisuuden tunnistamia informaatioteknologian riskejä kriittisen infrastruktuurin järjestelmäkokonaisuuksissa voidaan siis pitää samansuuntaisina informaatioteknologian yleisten riskien kanssa. Haittaohjelmat voivat päästä IT-järjestelmän laitteisiin yleisin tartuntamenetelmin, kuten sähköpostin liitetiedostona (Dargahi ym., 2019). Ozin ym. (2022) mukaan myös Windows-laitteiden laaja käyttö saattaa lisätä riskiä kiristysohjelmahyökkäykseen, sillä useat kiristysohjelmat kohdistuvat Windows-laitteisiin. Tämä on myös riski kriittisen infrastruktuurin IT-kokonaisuudelle, sillä ne ovat myös usein Windows-pohjaisia, kuten aiemmat hyökkäystilanteet ovat osoittaneet (esim. Makrakis ym, 2021).

Historialliset esimerkit kriittisen infrastruktuurin hyökkäyksistä viittaavat siihen, että hyökkäys pelkkään IT-järjestelmään voi olla tarpeeksi lamauttamaan myös OT-järjestelmän käytön, sillä liiketoiminta on tärkeää myös kriittisessä infrastruktuurissa. Makrakis ym. (2021) nostavatkin merkittäviksi esimerkeiksi vuonna 2012 tapahtuneet saudi-arabialaisiin öljyntuottajiin ja vuoden 2021 yhdysvaltalaiseen Colonial Pipelineen kohdistuneet kyberiskut, joissa IT-järjestelmien lamautuminen johti lopulta myös OT-järjestelmien alasajoon. Näistä esimerkeistä voimme päätellä, että vaikka teollisten laitteiden ohjaamiseen käytetyt OT-järjestelmä olisivatkin hyvin suojattu ja turvassa hyökkäykseltä, voi organisaation toiminta osoittautua kannattomaksi, mikäli normaalia toimintaa ei voida jatkaa ilman informaatioteknologisia järjestelmiä.

Informaatioteknologian suuri riski on siis ovat yhteys avoimeen internettiin, joka voi kiristysohjelmahyökkäyksessä johtaa liiketoiminnan estymiseen. Avointa yhteyttä muihin internetin laitteisiin voidaan siis pitää yhtenä merkittävänä riskitekijänä informaatioteknologian järjestelmissä, jonka tieteellinen kirjallisuus on tunnistanut myös kriittisen infrastruktuurin osalta. Tämä on huomioitu taulukossa 2, jossa on kuvattu eri järjestelmäkokonaisuuksista tunnistettuja riskejä. Taulukossa on myös huomioitu Ozin ym. (2022) havainto Windows-laitteiden tuomista turvallisuusriskeistä IT-järjestelmille. Aiemmat havainnot viittaavat siihen, että IT-järjestelmien riskialttius voi vaikuttaa koko organisaation toimintaan (Makrakis ym., 2021).

3.2.2 Operationaalisen teknologian riskit

Parkerin, Wun ja Christofidesin (2023) mukaan useat nykyisten tehtaiden käyttämät OT-järjestelmät on valmistettu ajassa, jolloin kyberhyökkäyksen riskiä ei otettu huomioon järjestelmää suunniteltaessa. Heidän mukaansa sama OT-järjestelmä voi olla ollut käytössä aina tehtaan valmistumisesta lähtien, jolloin järjestelmän ikä ja vanhat käytänteet kuten tietoliikenteen salauksen puute tekevät siitä riskialttiin modernille hyökkäykselle. Vanhentuneen järjestelmän päivitykseen voi olla korkea kynnys, sillä uusien päivitysten toteuttaminen saattaa johtaa järjestelmän normaalin toiminnan epävakautumiseen. Järjestelmän vakautta

onkin pidetty yhtenä tärkeimmistä OT-järjestelmän ominaisuuksista (Parker ym., 2023). Boreniuksen, Gopalakrishnan, Tjernbergin ja Kantolan (2022) analyysistä ilmenee, että tietyille OT-laitekokonaisuuksille ei välttämättä asenneta tietoturvapäivityksiä, sillä ne on pidetty kokonaan erillisenä IT-järjestelmistä ja niiden tietoverkoista. Näissä, kuten kaikissa muissakin teknologisissa järjestelmissä, on kuitenkin aina hyökkäysriski, sillä haittaohjelmat kuten kiristysohjelmat voivat kulkea laitteisiin myös fyysisesti esimerkiksi työntekijän muistitikulta (Borenius, Gopalakrishnan, Tjernberg & Kantola, 2022). OT-järjestelmien hallinnasta ja päivityksestä vaikuttaa siis olevan erilaisia näkemyksiä riippuen laitteen roolista ja yhteyksistä muihin järjestelmiin. Järjestelmien päivittämistä pidetään siis riskialttiina ja joskus mahdottomana, sillä laitteet ovat usein iäkkäitä ja niiden toimintavarmuus on oltava korkea. Toisaalta päivittämätön järjestelmä voi olla riskialttiimpi hyökkäykselle, mikäli haittaohjelma pääsee murtautumaan siihen.

3.2.3 Teollisuuden esineiden internetin riskit

Teollisuuden esineiden internet on luotu tehostamaan järjestelmien välistä toimintaa ja helppoa ohjaamista (Dhirani, Armstrong & Newe, 2021). Esineiden internet tuo kriittisen infrastruktuurin käyttämiin järjestelmiin uuden kokonaisuuden, jonka mahdolliset tietoturvaongelmat jälleen lisäävät hyökkäysriskiä. IIoT-laitteiden lukumäärä on usein erittäin suuri, jolloin pelkona on useiden heikkojen murtautumiskohteiden leviäminen ympäri kriittisen infrastruktuurin toiminnan järjestelmäkokonaisuutta (Dhirani, Armstrong & Newe, 2021). Boreniuksen ym. (2022) mukaan teollisuuden esineiden internetin haasteisiin kuuluu myös mahdollinen heikko fyysinen turvallisuus. Esimerkiksi sähköverkon toimintaa tarkasteleva laite voi olla asennettu paikkaan, jonka turvallisuustaso ei vastaa esimerkiksi tehtaan tai toimiston turvallisuutta. Laitteita on siis suuri määrä ja osa niistä on paikoissa, joiden fyysistä turvallisuutta ei voida täysin taata. Yhdeksi laitteen turvaamisen keinoksi lukeutuu fyysinen koventaminen, jolla voidaan välttää fyysisiä hyökkäyksiä (Borenius ym., 2022). Stergiopouloksen, Gritzalisin ja Limnaiosin (2020) mukaan teollisuuden esineiden internetin riskeihin kuuluu myös niiden harvoin rajatut kommunikointimahdollisuudet muiden laitteiden ja pilvipalveluiden kanssa lisää niiden tietoturvariskejä.

Taulukko 2 kuvaa eri järjestelmien riskitekijöitä ja mahdollisia hyökkäystilanteita suhteessa kiristysohjelmahyökkäyksiin. Taulukossa on huomioitu usean tieteellisen lähteen esittämät riskit, joita eri järjestelmätyypit kohtaavat teknisen toteutuksensa ja käyttötarkoituksensa vuoksi. Taulukosta ilmenee, että eri järjestelmätyyppien riskit ovat erilaiset. Taulukon analyysiä jatketaan alaluvussa 3.3., jossa tarkasteluun otetaan mukaan eri järjestelmien väliset yhteydet. Mahdollisissa hyökkäysskenaarioissa on käytetty esimerkkeinä sekä toteutuneita hyökkäyksiä että tieteellisessä kirjallisuudessa kuvattuja potentiaalisia hyökkäystilanteita.

Taulukko 2 Eri järjestelmien riskitekijät ja mahdolliset hyökkäystilanteet (Oz ym., 2022; Staves ym., 2024; Borenius ym., 2022; Stergiopoulos ym., 2020)

Järjestelmätyyppi	**Riskitekijät**	**Mahdollinen hyökkäystilanne**
Informaatioteknologia	Yhteydet avoimeen internettiin. Käytettyjen laitteiden Windows-pohjaisuus.	Varausjärjestelmän lukittuminen. Asiakastietokannan menettäminen. Liiketoiminnan toimintakyvyttömyys.
Operationaalinen teknologia	Yleisten tietoturvaominaisuuksien kuten salauksen puute. Järjestelmän jatkuvan käytettävyyden priorisointi tietoturvan sijasta.	SCADA-tarkkailuohjelmiston lukittuminen. Tehtaan toimintakyvyttömyys.
Teollisuuden esineiden internet	Laitteiden välinen, usein hallitsematon kommunikaatio. Laitteiden suuri lukumäärä. Asennetun laitteen fyysinen turvallisuus.	Yksittäisen mittarilaitteen lukittuminen. Tehdaslaitteiden toiminnan tarkkailun estyminen.

3.3 Järjestelmien väliset yhteydet

Nicolin (2021) mukaan operationaalisen teknologian järjestelmät on usein pyritty loogisesti erottamaan informaatioteknologisista järjestelmistä, sillä informaatioteknologian kohtaamat riskit ovat korkeammat. Artikkeli huomauttaa niistä riskeistä, joita informaatioteknologia kohtaa, kun se on yhdistetty internettiin ja on toistuvasti yhteydessä organisaation ulkopuolisiin toimijoihin, kuten asiakkaisiin ja yhteistyökumppaneihin. Tämä erotus ei kuitenkaan ole täydellinen, sillä operationaalisen teknologian laitteisto tarvitsee myös päivityksiä ja konfiguraatiotiedostoja, jotka usein tuodaan järjestelmään informaatioteknologiaa hyödyntäen (Nicol, 2021). Tapahtuneet esimerkit todistavatkin, että suojatut yhteydet informaatioteknologian ja operationaalisen teknologian välillä avaavat mahdollisuuden hyökkäyksiin, jotka eivät vaadi fyysistä pääsyä laitteille (Makrakis ym, 2021). Makrakis ym. (2021) esittivät tutkimuksessaan, että IT-järjestelmään kohdistunut hyökkäys on usein edennyt aina OT-järjestelmiin asti, vaikka kyseessä ei olisikaan ollut tarkasti kohdistettu hyökkäys.

Operationaalisen teknologian kriittisyys on siis pyritty huomioimaan järjestelmien välisen rakenneteen suunnittelussa, mutta usein niiden väliltä yhä löytyy kommunikaatiokanavia, joita pitkin haittaohjelmat voivat kulkea aina operationaaliseen järjestelmään asti. IT- ja OT-järjestelmien välissä on usein niin sanottu demilitarisoitu alue, DMZ, jonka tarkoitus on toimia järjestelmien välisenä välittäjänä ilman, että järjestelmät voivat suoraan kommunikoida keskenään (Makrakis ym., 2021). DMZ-ratkaisu pyrkii siis pitämään suojatumman OT-järjestelmän erossa usein turvattomasta IT-järjestelmästä. Voidaan siis sanoa, että tietoturvallisuuden ja esimerkiksi kiristysohjelmahyökkäyksien välttämisen kannalta

ihannetilanne olisi OT-järjestelmien täydellinen erottaminen muista järjestelmistä, jotka ovat yhteydessä avoimeen internettiin. Liiketoiminnan vaatimukset ja tavoitteet voivat kuitenkin haastaa tämän näkemyksen. DMZ toimii siis eräänlaisena kompromissiratkaisuna, jolla pyritään välttämään haitallinen liikenne, mutta mahdollistamaan järjestelmien välinen kommunikaatio. Nicolin (2021) mukaan IT- ja OT-järjestelmien välillä voi olla yhteyksiä esimerkiksi operationaalisen datan keräämiseen, järjestelmien väliseen sähköpostiyhteyteen tai etäohjaukseen tarkoitetun Virtual Private Network, eli VPN-yhteyden muodostamiseksi. Artikkelin mukaan myös aiemmin mainittujen konfiguraatiotiedostojen ja päivitysten siirtämiseen voidaan käyttää erillistä palvelinta OT-järjestelmässä, joka mahdollistaa kommunikoinnin muiden järjestelmien kanssa.

Jotkut organisaatiot voivat myös sallia OT-järjestelmien tehdä pyyntöjä internet-palvelimille siellä säilytettyjen laitteiden valmistajien teknisten käyttöohjeiden saavuttamiseksi (Nicol, 2021). Nicol (2021) siis esittää laajan kirjon tapoja, joilla OT-järjestelmien erottelusta poiketaan erilaisten liiketoimintaan ja järjestelmän hallintaan liittyvien tavoitteiden saavuttamiseksi. Joitakin näistä kommunikointitavoista on jo käytetty kiristysohjelmahyökkäysten toteutukseen. Tunnettu esimerkki on Colonial Pipelineen kohdistunut hyökkäys, jossa hyökkääjä onnistui kohdentamaan hyökkäyksen OT-järjestelmään käyttäen IT-järjestelmän haavoittuvia VPN-yhteyksiä (Borenius ym., 2022).

Nämä OT:n ja IT:n yhdistämisen riskit on hyvin tunnistettu tieteellisessä kirjallisuudessa. Sarkar, Teo ja Chang (2022) kertovat, kuinka liiketoiminnan innostama lisääntynyt halu monitoroida ja ohjata OT-laitteiden toimintaa on johtanut tilanteeseen, jossa IT-järjestelmät osallistuvat OT-laitteiden hallintaan. OT-laitteet eivät siis pitkälti enää toimi omassa tarkasti ja tarkoituksella erotetussa ympäristössään, vaan ne vuorovaikuttavat myös IT-järjestelmien kanssa (Sarkar ym., 2022). Ashleyn, Gourisetin, Brownin ja Bonebraken analyysin (2022) mukaan internetin laitteiden hakukoneet pystyvät löytämään useita OT-järjestelmiä, jotka ovat kytkettynä avoimeen internettiin. Yhteyden avoimuus yhdistettynä OT-järjestelmien heikkoon tietoturvan tasoon voi johtaa tilanteisiin, jossa hyökkääjä voi löytää haavoittuvaisen laitteen verkko haulla ja aloittaa hyökkäyksen suunnittelun.

Vaikuttaa siis siltä, että yritystoiminnan vaatimukset johtavat usein tilanteeseen, jossa OT-järjestelmän turvallisuudesta tehdään erilaisia kompromisseja järjestelmän tarkan ohjaamisen ja tarkkailun vuoksi. Tehdyt kompromissit voivat vaikuttaa negatiivisesti OT-järjestelmien tietoturvaan. Yhteys organisaation ulkoisiin laitteisiin voi ilmeisesti myös luoda suuria riskejä järjestelmälle, jota ei olla suunniteltu IT-laitteen tavoin tietoturvalliseksi. Analyysin perusteella vaikuttaa siltä, että OT-järjestelmien tietoturvan parantamiseksi täytyisi joko vähentää niiden pääsyä avoimeen internettiin IT-järjestelmien kautta tai suunnitella järjestelmiä, jotka ovat tarpeeksi turvallisia kestämään niihin kohdistuneita hyökkäyksiä. OT-järjestelmien kriittisyys kriittisen infrastruktuurin toiminnan kannalta luo kuitenkin tarpeen priorisoida laitteen turvallisuutta, jolloin ulkoisten yhteyksien estäminen kokonaan vaikuttaa turvallisimmalta tilanteelta. On

kuitenkin epäselvää, onko tämä kaikissa ratkaisuissa mahdollista siten, että myös liiketoiminnan tarpeet ja realiteetit huomioidaan riittävästi.

Esineiden internetin laitteet usein kommunikoivat vanhojen OT-järjestelmien kanssa, joka tuo laitteistolle tietoturvariskejä (Stergiopoulos ym., 2020). Esineiden internetin laitteiden ottaminen osaksi OT-järjestelmien hallintaa vaikuttaa sisältävän samankaltaisia tietoturvaan liittyviä riskejä kuin IT-järjestelmien sisällyttäminen.

Stergiopouloksen ym. (2020) mukaan esineiden internetin laitteita käytetään esimerkiksi öljy- ja kaasualalla mittauslaitteistossa, jotka voivat olla jatkuvassa yhteydessä muiden OT-laitteiden ja -ohjelmistojen kanssa. Esineiden internetin mahdollisuus kommunikoida toisten laitteiden kanssa noudattamatta tietoturvasyistä luotuja laitteiden välisiä hierarkioita on mahdollinen tietoturvariski. Tämä voi johtaa tilanteeseen, jossa IIoT-laite kommunikoi suoraan toisen laitteen kanssa vastoin hierarkian periaatteita (Stergiopoulos ym., 2020). Erilaisten haittaohjelmien leviämisperiaatteiden vuoksi yhteyksiä eri laitteiden välillä tulisi kuitenkin minimoida.

Taulukkoon 3 on koottu näitä eri järjestelmätyyppien mahdollisia rooleja hyökkäyksen leviämistilanteissa. Taulukolla siis havainnollistetaan esimerkiksi sitä, miten tietty järjestelmä saattaa olla pääosin hyökkäyksen kohde, kun taas toinen toimii usein haittaohjelman tartuntakohtana.

Taulukko 3 Järjestelmätyyppien mahdolliset roolit hyökkäyksen leviämistilanteessa (Nicol, 2021; Makrakis ym., 2021; Stergiopoulos ym., 2020, Borenius ym., 2022)

Järjestelmätyyppi	**Mahdollinen rooli hyökkäyksen leviämistilanteessa**
IT-järjestelmä	IT-järjestelmän saastuminen internetin kautta. Haittaohjelman leviäminen organisaation jaettuun verkkoon ja muihin järjestelmiin.
OT-järjestelmä	Toisen järjestelmän kautta levinneen hyökkäyksen kohde. Fyysisen laitteen kautta levinneen hyökkäyksen kohde. Verkkoyhteydellisen OT-järjestelmän saastuminen internetin kautta.
IIoT-järjestelmä	IIoT-järjestelmän saastuminen internetin kautta. IIoT-laitteen saastuminen fyysisessä hyökkäyksessä. Haittaohjelman levittäminen organisaation jaettuun verkkoon ja muihin järjestelmiin.

4 HYÖKKÄYKSET JÄRJESTELMIÄ VASTAAN

Kiristysohjelmahyökkäyksen mahdolliset vaikutukset kriittiseen infrastruktuuriin eri järjestelmiin ovat laajat. Hyökkäys voi kohdistua mihin vain kolmesta aiemmin esitetystä järjestelmästä, eli informaatioteknologisiin järjestelmiin, operationaalisen teknologian järjestelmiin tai teollisuuden esineiden internettiin. Kiristysohjelmilla on myös mahdollisuus liikkua näiden järjestelmien välillä. Tarkastelemalla toteutuneita ja potentiaalisia kiristysohjelmahyökkäyksiä voimme pyrkiä rakentamaan selkeämpää kuvaa siitä, mihin järjestelmiin hyökkäykset yleensä kohdistuvat, ja millaisia vaikutuksia eri järjestelmiin kohdistuneilla hyökkäyksillä voi olla. OT- ja IT-järjestelmien kohdalla tarkoituksena on peilata toteutuneita kiristysohjelmahyökkäyksiä 3. luvussa luotuun kriittisen infrastruktuurin järjestelmien kokonaiskuvaan. Teollisuuden esineiden internetin hyökkäyksien kohdalla analysoidaan mahdollisia hyökkäystapoja, sillä julkisista lähteistä ei toistaiseksi ole tietoa varsinaisista toteutuneista kiristysohjelmahyökkäyksistä teollisuuden esineiden internetin laitteita vastaan. Analyysissä käytetyt kiristysohjelmahyökkäykset on kerätty tieteellisestä kirjallisuudesta ja Yhdysvaltain kyberpuolustusvirasto CISA:n raporteista. Analyysiin valitut hyökkäykset ovat sellaisia, joista löytyy luotettavaa asiantuntija- tai tieteellistä tietoa.

4.1 Eri järjestelmien kiristysohjelmahyökkäykset

4.1.1 IT-järjestelmien kiristysohjelmahyökkäykset

WannaCry on tunnettu IT-järjestelmiin kohdistunut salaava kiristysohjelma (National Audit Office, 2017). WannaCry kiristysohjelmaa käytettiin Makrakis ym. (2021) mukaan esimerkiksi Iso-britannian julkista terveydenhuolto-organisaatio NHS:ää vastaan. WannaCry keskittyy Windows-pohjaisiin käyttöjärjestelmiin, erityisesti Windows 7 käyttöjärjestelmään ja vanhoihin Windows Server-palvelinohjelmistoihin (Makrakis ym, 2021). Hyökkäyksen kohteiksi joutuneet

järjestelmät voivat siis olla esimerkiksi päätelaiteita, sähköpostipalvelimia ja muita IT-tason järjestelmiä. Saastutettuaan yhden organisaation laitteen, WannaCry kykenee leviämään muihin yhdistettyihin laitteisiin (Symantec, 2017). WannaCry voi siis potentiaalisesti levitä kaikkiin haavoittuvaisiin laitteisiin, jotka ovat samassa verkossa. Tämä leviämistapa korostaa tarvetta pyrkiä erittelemään toiminnalle tärkeitä laitteita toisistaan. Itsestään leviäminen tekee WannaCry:n riskistä laajan, sillä hyökkäys ei välttämättä ole kohdistettu, vaan automaattisesti haavoittuvuuden kautta levinnyt. Razaulla ym. (2023) esittävät, että WannaCry-hyökkäysten motiivi ei välttämättä ollut taloudellinen, vaan kyseessä saattoi olla tahto levittää paniikkia hyökkäyksen kohteissa. Siitä huolimatta WannaCry:n aiheuttama taloudellinen vahinko on noussut heidän mukaansa yhteensä noin 4 miljardiin dollariin (Razaulla ym., 2023).

Ghafurin ym. (2019) mukaan hyökkäys NHS:ään ei johtanut yhdenkään potilaan kuolemaan, mutta he pitävät sitä huonona mittarina mahdollisesti aiheutuneesta vahingosta ja vaarasta potilaiden terveyteen. Hyökkäys NHS:ään johti noin 5,9 miljoonan punnan liiketoiminnan menetykseen, mutta summa olisi voinut nousta jopa 35 miljoonaan puntaan, mikäli hyökkäys olisi levinnyt laajemmin organisaation IT-järjestelmiin (Ghafur ym, 2019).

NotPetya on toinen hyvin tunnettu, Windows-koneisiin kohdistettu salaava kiristysohjelma. Solonin ja Hernin (2017) mukaan NotPetya:n kohteita olivat esimerkiksi ukrainalaiset ministeriöt, pankit, lentokentät ja muut merkittävät organisaatiot. Myös yrityksiä ukrainan ulkopuolella, esimerkiksi tanskalainen logistiikkayritys Maersk, joutui hyökkäyksen kohteeksi (Solon & Hern, 2017). Fayin (2018) mukaan NotPetya perustuu samaan haavoittuvuuteen ja leviämistapaan kuin WannaCry. NotPetya on siis mahdollinen riski kaikille Windows-laitteille, jotka ovat samassa verkossa. Artikkelissa painotetaan, kuinka NotPetya eroaa useasta kiristysohjelmasta siinä, että se salaa koko järjestelmän eikä vain sen osia. Salauksen lisäksi ohjelma toimii kuten lukitusohjelma, eli se tuhoaa tietokoneen käynnistämiseen käytetyn master boot recordin (Fayi, 2018). Cimpanun (2018) mukaan Maersk joutui korvaamaan noin 45 000 päätelaitetta ja 4 000 palvelinta palauttaakseen järjestelmän normaalin toiminnan. Yrityksen oman arvion mukaan hyökkäyksen aiheuttama taloudellinen vahinko saattoi olla jopa 300 miljoonaa Yhdysvaltain dollaria (Cimpanu, 2018). Capanon (2021) mukaan hyökkäys vaikutti Maerskin kykyyn lastata konttilaivoja ja aiheutti merkittävän ongelman yrityksen kykyyn toimittaa tuotteita.

WannaCry ja NotPetya kiristysohjelmien kohteet ovat hyviä esimerkkejä siitä, minkälaista taloudellista vahinkoa kiristysohjelmahyökkäys voi tuottaa kriittisen infrastruktuurin toimijalle. NHS:än esimerkki myös osoittaa, että hyökkäys voi aiheuttaa riskejä myös terveydenhuollon toiminnalle, joka voi pahimmassa tilanteessa johtaa potilaan kuolemaan. Nostetut esimerkit osoittavat, että organisaation järjestelmään murtautunut kiristysohjelma voi levitä järjestelmässä nopeasti ja johtaa tuhansien laitteiden toimintakyvyttömyyteen. Esimerkit myös nostavat esille varmuuskopioinnin tärkeyden. Capanon (2021) mukaan Maerskin palvelimien varmuuskopiot tuhoutuivat hyökkäyksessä, mutta Maersk saivat palautettua tärkeät tiedot, sillä yksi yrityksen toimistoista sattui

olemaan hyökkäyksen aikana irti yrityksen verkosta. Esimerkistä ilmenee, että varmuuskopiointi ei itsessään riitä, vaan varmuuskopiot tulisi myös säilyttää irrallaan yrityksen muista järjestelmistä.

WannaCry:n ja NotPetya:n leviämistapa korostaa myös järjestelmien välisten yhteyksien riskitekijöitä, sillä nämä esimerkkikiristysohjelmat kykenevät leviämään automattisesti Windows-pohjaisten laitteiden välillä (Symantec, 2017; Fayi, 2018). Tämä mahdollistaa siis puutteellisesti eroteltujen järjestelmäkokonaisuuksien välillä siirtymisen, mikäli molemmissa järjestelmissä käytetään Windows-pohjaisia laitteita. Kuten seuraavasta esimerkistä ilmenee, myös operationaalisessa teknologiassa käytetään Windows-pohjaisia laitteita, esimerkiksi SCADA-valvontaohjelmistoissa (CISA, 2020; CISA, 2021b).

4.1.2 OT-järjestelmien kiristysohjelmahyökkäykset

Yhdysvaltain kyberpuolustusvirasto CISA:n raportin (2020) mukaan nimeämätön kiristysohjelma murtautui yhdysvaltalaisen maakaasun kompressointilaitoksen IT- ja OT-järjestelmien Windows-pohjaisiin laitteisiin, estäen laitoksen turvallisen toiminnan kahden vuorokauden ajaksi. Hyökkäyksen uskotaan alkaneen laitoksen IT-järjestelmistä, josta se pääsi leviämään OT-järjestelmiin epäonnistuneen järjestelmien erottamisen vuoksi. Hyökkäys johti tilanteeseen, jossa OT-järjestelmään yhdistettyjen teollisten koneiden tarkkailuun tarkoitettujen laitteiden käyttö estyi. Hyökkäyksen kohde päätti pysäyttää toimintansa kokonaan kahden päivän ajaksi, jonka jälkeen toiminta saatiin palautettua normaaliksi. Raportin mukaan normaali toiminta saatiin palautettua uusien laitteiden ja varmuuskopioiden avulla (CISA, 2020). Raportista ei kuitenkaan ilmene, mitä kautta kiristysohjelmahyökkäys pääsi varsinaisesti leviämään IT-järjestelmistä OT-järjestelmiin. Esimerkki kuitenkin korostaa järjestelmien erottelemisen kriittisyyttä. Aiempien havaintojen mukaan erotteleminen voidaan toteuttaa esimerkiksi demilitarisoidulla alueella, joka ohjaa kahden järjestelmän välistä kommunikaatiota. Erottelu voidaan myös tehdä poistamalla kaikki järjestelmien väliset yhteydet, mutta se saattaa toimia vastoin liiketoiminnan tavoitteita.

Vuonna 2021 CISA (2021b) julkaisi tiedotteen, jossa kerrottiin yleisellä tasolla eri Yhdysvaltain vesihuollon organisaatioihin kohdistuneista kiristysohjelmahyökkäyksistä. Raportti kertoo kolmesta vuonna 2021 tapahtuneesta kiristysohjelmahyökkäystä, jossa kohteena oli OT-järjestelmä. Esimerkkien tapauksissa hyökkäykset oli kohdistuneet operationaalisen teknologian SCADA-valvontaohjelmistoihin (CISA, 2021b). Raportista ei ilmene, mille käyttöjärjestelmälle haavoittuvat ohjelmistot perustuivat. Al-Hawawrehin, Alazabin, Ferragin ja Hossainin (2024) mukaan OT-järjestelmät, jotka käyttävät Windows-pohjaisia SCADA-ohjelmistoja ovat erityisen haavoittuvia kiristysohjelmahyökkäyksille. Tämä saattaa johtua siitä, että useat kiristysohjelmat on suunniteltu Windows-hyökkäyksiin. Esimerkiksi haittaohjelmien tunnistamiseen erikoistunut Virustotal (2021) on raportoinut, että vuonna 2021 analysoiduista kiristysohjelmista noin 95% löytyi Windowsin käyttämistä tiedostotyypeistä. Windows-pohjaisuus voidaan siis käsittää myös tietynlaisena riskitekijänä OT-järjestelmissä. Raportista ei

myöskään ilmene, miten haittaohjelma pääsi OT-järjestelmään. Mahdollisia tapoja voi olla esimerkiksi järjestelmien riittämätön erottelu.

4.1.3 IIoT-järjestelmien kiristysohjelmahyökkäykset

Julkisuuteen tulleita teollisuuden esineiden internetin järjestelmien kiristysohjelmahyökkäyksiä ei toistaiseksi ole (Al-Hawawreh ym., 2024). IT- ja OT-järjestelmien yhteiskäytön historiallinen esimerkki kuitenkin luo perusteet näkemykselle, jossa lisääntyneet eri järjestelmien väliset yhteydet tuo uusia uhkia kokonaisuudelle.

Al-Hawawreh ym. (2024) pitävät IIoT-laitteisiin kohdistuvien kiristysohjelmien kehittämistä väistämättömänä kehityskulkuna, mikäli nykyinen IIoT-laitteiden kasvavan käyttöönoton trendi jatkuu. He pitävät mahdollisina riskeinä uusien laitteiden mahdollisia vielä tuntemattomia haavoittuvuuksia ja IIoT-laitteiden ohjaamiseen käytettyjen järjestelmien tietomurtoja, joissa kiristysohjelma voi tunkeutua myös yksittäisille IIoT-laitteille (Al-Hawawreh ym., 2024) Esimerkiksi Al-Hawawreh ym. (2019) loivat testiskenaarion, jossa kiristysohjelmaa käytettiin operatiivisen teknologiaan yhdistettyä IIoT-laitetta vastaan. Skenaariosta paljastui, että IIoT-laitteet ovat houkutteleva kohde kiristysohjelmahyökkääjälle, sillä ne voivat vaikuttaa suoraan teollisten koneiden tarkkailuun ja ohjaamiseen. Skenaariota varten luotu kiristysohjelma onnistui salaamaan laitteen paikallisia tiedostoja kuten varmuuskopioita, logitiedostoja (Al-Hawawreh ym, 2019). Tutkimuksen tulokset yhdistettynä laitteiden käytön kasvavaan trendiin tekee kehityskulusta huolestuttavan. Vaikuttaa siltä, että suuri IIoT-laitteisiin kohdistunut kiristysohjelmahyökkäys ei ole pelkästään teoreettinen mahdollisuus, vaan todennäköinen tulevaisuuden kehityskulku. Mahdolliset konkreettiset riskit kriittiselle infrastruktuurille voivat realisoitua joko IIoT-laitteiden toiminnan lakkaamisena tai haittaohjelmien murtautumisena muihin järjestelmiin IIoT-laitteiden kautta.

4.2 Järjestelmäkokonaisuuden kiristysohjelmahyökkäykset

Eri kriittisen infrastruktuurin järjestelmien hyökkäyksien analyysistä selvisi, että hyökkäykset järjestelmiin voivat vaikuttaa kriittisen infrastruktuurin järjestelmäkokonaisuuden toimintaan monella eri tavalla. Kiristysohjelmahyökkäyksiä kohdentuu IT- ja OT-järjestelmiin. Hyökkäykset avoimempiin IT-järjestelmiin voivat lisäksi johtaa haittaohjelman pääsyyn OT-järjestelmiin, kuten ilmeni CISA:n (2021b) raportin nimettömästä esimerkkitapauksesta. Kuten aikaisemmassa analyysissä todettiin, tieteellisessä kirjallisuudessa on tunnistettu erilaisia tilanteita, joissa kiristysohjelmat voivat levitä IT-järjestelmistä operationaaliseen teknologiaan. Esimerkeistä ei ilmene mitä yhteyskanavaa pitkin kiristysohjelma on levinnyt, mutta tieteellisestä kirjallisuudesta poimittuja potentiaalisia leviämiskanavia olivat esimerkiksi sähköposti- ja etäkäyttöyhteys (Nicol, 2021).

Esimerkeistä myös ilmeni, että IT-järjestelmiin kohdistuva hyökkäys voi olla riittävä aiheuttamaan merkittävää vahinkoa kriittisen infrastruktuurin toimijalle, kuten kävi ilmi NHS:n tapauksessa (Ghafur ym., 2019). Järjestelmäkokonaisuutta suunniteltaessa ei siis voida keskittyä ainoastaan OT-järjestelmien suojaamiseen, vaikka ne usein nähdään kaikista kriittisempänä osana järjestelmäkokonaisuutta. IT-järjestelmien suojaamisessa tulee ottaa huomioon, miten hyökkäyksen leviäminen voidaan estää IT-laitteiden välillä. WannaCry:sta ilmeni, että esimerkiksi etäkäyttöominaisuuksien haavoittuvuudet voi johtaa haittaohjelman leviämiseen (Dargahi ym., 2019). Esimerkeistä siis ilmenee, että aikaisempi analyysi tieteellisen kirjallisuuden tunnistamista järjestelmien välisistä yhteyksistä ja niiden riskeistä pitävät paikkansa myös käytännössä. Riskien todellisuus korostaa tarvetta järjestelmien ja niiden välisten yhteyksien uudelleenharkinnalle tai tietoturvatoimien kiristämiselle. Tunnistettuja tieteellisen kirjallisuuden ehdotuksia olivat esimerkiksi järjestelmien välisten yhteyksien vähentäminen ja erilaisten ratkaisujen kuten DMZ:n käyttö järjestelmien välisten yhteyksien hallitsemiseen (Nicol, 2021; Makrakis ym., 2021)

Maerskin ongelmat NotPetya:n kanssa tuovat ilmi varmuuskopioinnin merkityksen toiminnan palauttamiselle hyökkäyksen jälkeen (Capano, 2021).

Tieteellisessä kirjallisuudessa tiedetään vielä varsin vähän teollisuuden internetin laitteiden vaikutuksista kiristysohjelmahyökkäyksien ja kriittisen infrastruktuurin tulevaisuuteen. Al-Hawawrehin ym. (2019) tutkimuksen perusteella vaikuttaa kuitenkin siltä, että myös IIoT-laitteet ovat haavoittuvia kiristysohjelmahyökkäyksille. Tieteellisestä kirjallisuudesta ei kuitenkaan vielä ilmene, onko IIoT-laitteet mahdollisia hyökkäysväyliä IT- tai OT-järjestelmiä vastaan. On kuitenkin myös mahdollista, että pelkkä hyökkäys IIoT-laitteita vastaan riittää lamauttamaan tulevaisuuden kriittisen infrastruktuurin toimijan, kuten nykypäivänä on käynyt IT-järjestelmien kanssa (Makrakis ym, 2021). IIoT-järjestelmien riskien tunnistamiseen tarvitaan siis uutta tieteellistä tietoa, jotta hyökkäyksiin voidaan varautua ennen niiden yleistymistä.

5 YHTEENVETO

Tämän kandidaatintutkielman tavoite oli tutkia kiristysohjelmahyökkäyksiä suhteessa kriittiseen infrastruktuuriin, erityisesti keskittyen kriittisen infrastruktuurin erinäisiin järjestelmiin ja niiden välisiin suhteisiin. Tutkielman tavoite oli paremmin ymmärtää näitä järjestelmiä sekä sitä, miten kiristysohjelmat voivat vaikuttaa niiden toimintaan. Analyysin myötä vastattiin seuraaviin johdannossa määriteltyihin tutkimuskysymyksiin:

- Minkälaisia riskejä tieteellinen kirjallisuus on tunnistanut kriittisen infrastruktuurin järjestelmäkokonaisuuksista suhteessa kiristysohjelmahyökkäyksiin?
- Mihin järjestelmiin tapahtuneet hyökkäykset ovat kohdistuneet?

Kysymyksiin vastattiin ensin perehtymällä kiristysohjelmiin ja niiden yleisiin toimintatapoihin. Sen jälkeen luotiin kokonaiskuva eri kriittisen infrastruktuurin järjestelmistä, niiden välisistä yhteyksistä ja yhteyksien luomista riskeistä. Tutkielman toisessa luvussa havaittiin, että kiristysohjelmia on monenlaisia erilaisin ominaisuuksin. Niiden samankaltaisuus löytyy yhteisestä tarkoituksesta estää jonkun järjestelmän, laitteen tai tiedostojen käytön (esim. Symantec, 2015). Sen lisäksi ohjelma yleensä myös kiristää käytön palauttamisella. Kolmannessa luvussa kriittisen infrastruktuurin kokonaiskuva jaettiin aiempien tieteellisten tutkimuksen yleisen tavan mukaisesti informaatioteknologian järjestelmiin ja operationaalisen teknologian järjestelmiin. Näiden lisäksi tutkielmassa huomioitiin myös teollisuuden esineiden internetin järjestelmät, joiden rooli on korostunut tutkimuksen edetessä. Luvussa myös analysoitiin niitä riskejä, joita tämä järjestelmärakenne ja niiden väliset suhteet aiheuttavat kokonaisuuden toiminnalle ja tietoturvalle. Neljännessä luvussa jatkettiin näiden taustatietojen analysointia suhteessa kiristysohjelmahyökkäyksiin. Analyysissä käytiin läpi monta aiempaa kiristysohjelmahyökkäystä suhteessa IT- ja OT-järjestelmiin. Teollisuuden esineiden internetin osalta keskityttiin mahdollisiin kiristysohjelmahyökkäystilanteisiin, sillä julkisuuteen ei ole toistaiseksi tullut teollisuuden esineiden internetin laitteisiin kohdistuneita kiristysohjelmahyökkäyksiä. Mahdollisia

kiristysohjelmatilanteita johdettiin tieteellisestä kirjallisuudesta, jossa mahdollisia hyökkäystilanteita on analysoitu empiirisin kokein ja laitteiden teknisiä ominaisuuksia analysoimalla.

Tutkielmassa havaittiin, että kriittisen infrastruktuurin laajat järjestelmäkokonaisuudet aiheuttavat merkittäviä turvallisuusriskejä. Turvallisuusriskit syntyvät tilanteissa, joissa yksittäisen tai useamman järjestelmän käyttö estyy. Tutkielmassa myös havaittiin, että kiristysohjelmat voivat kulkea eri järjestelmien välillä, mikäli järjestelmistä löytyy haavoittuvuuksia, eikä järjestelmiä olla tehokkaasti eroteltu toisistaan (Makrakis ym, 2021). Järjestelmien väliset yhteydet lisäävät merkittävästi eri järjestelmäkokonaisuuksien riskejä, sillä ne voivat mahdollistaa hyökkääjälle pääsyn järjestelmän osaan, jonka suunnitteluperiaate ei ole keskittynyt turvallisuuteen (Parker ym., 2023).

Tutkielman keskeisimpiä johtopäätöksiä on se, että teknologisen kehityksen tuoma kehityskulku on johtanut siihen, että yhä useampi kriittisen infrastruktuurin järjestelmä on yhteydessä keskenään. Järjestelmien rajojen hämärtyminen vaikuttaa johtavan tilanteeseen, jossa erityisesti tietoturvattoman operationaalisen teknologian järjestelmiin on päästy murtautumaan informaatioteknologian järjestelmien kautta. Liiketoiminnallisten hyötyjen tavoittelu järjestelmien välisiä yhteyksiä suunniteltaessa on mahdollistanut tämän kehityskulun (Sarkar ym., 2022). Tieteellisessä kirjallisuudessa uskotaan pitkälti tulevaan kehitykseen, jossa teollisuuden esineiden internetin kehityskulut johtavat samankaltaiseen tilanteeseen operationaalisen teknologian kanssa, jolloin myös hyökkäysmahdollisuudet lisääntyvät (esim. Al-Hawawreh ym., 2024). Tulevaisuuden kriittisen infrastruktuurin ja tieteellisen tutkimuksen tulisi siis keskittyä löytämään uusia tapoja vähentää riskejä tilanteissa, joissa järjestelmien välinen interaktio on välttämätöntä. Tämä voitaisiin toteuttaa esimerkiksi uusilla teknologisilla ratkaisuilla tai tietoturvaperiaatteilla, joilla yhteyksien tuomia riskejä minimoidaan.

Toinen merkittävä johtopäätös on se, ettei kriittisen infrastruktuurin lamautuminen ei välttämättä vaadi hyökkäystä tiettyyn toiminnan kannalta kriittiseen järjestelmään tai laitteeseen, sillä kriittisen infrastruktuurin yritysten käyttämillä laitteilla on usein tärkeä merkitys kokonaisuuden toimintaan ja kannattavuuteen. Aikaisemmat esimerkit hyökkäyksistä osoittavat, että myös informaatioteknologian toimimattomuus voi johtaa normaalin toiminnan alasajoon (esim. Makrakis ym., 2021). Tämä johtopäätös korostaa sitä, ettei järjestelmien väliset yhteydet ole ainoa järjestelmien tuoma riski. Haittaohjelma kuten kiristysohjelma voi siis aiheuttaa merkittävää vahinkoa päästyään vain yhteen kriittisen infrastruktuurin käyttämistä järjestelmistä.

Tutkielman aiheesta aukenee monenlaisia jatkotutkimusaiheita, joiden avulla kriittisen infrastruktuurin järjestelmiä voitaisiin kehittää turvallisemmiksi. Yksi selkeä aihe on teollisuuden esineiden internetin rooli tulevaisuuden kiristysohjelmahyökkäyksissä. Erityisesti empiiriset koeasetelmat havainnollistaisivat miten mahdollinen hyökkäys IIoT-laitetta vastaan vaikuttaisi järjestelmäkokonaisuuden toimintakykyyn. Tärkeää olisi myös kartoittaa IIoT-järjestelmien välisiä yhteyksiä IT- ja OT-järjestelmiin ja miten se vaikuttaa kokonaisuuden riskeihin. Toinen mahdollinen jatkotutkimusaihe koskee uusia ratkaisuja, joilla

voidaan minimoida järjestelmien välisten yhteyksien riskejä. Vaikuttaa siltä, että nykyaikaisten organisaatioiden liiketoiminnalliset tarpeet vaativat järjestelmien välistä kommunikaatiota. Mikäli järjestelmien välisiä yhteyksiä ei voida rajata pois, tulisi niitä pyrkiä kehittämään tietoturvallisemmiksi. Kolmas aiheen tarkastelussa noussut kysymys on eri käyttöjärjestelmien riskit. Tässä tutkielmassa käsiteltyjen tietojen perusteella vaikuttaa siltä, että nykytilanteessa Windows-käyttöjärjestelmän kiristysohjelmariskit ovat varsin korkeat verrattuna muihin käyttöjärjestelmiin, kuten Linuxiin (esim. Oz ym., 2022). Aihe tarvitsee lisätarkastelua, sillä rajallisilla tiedoilla on vaikea tehdä asiasta vahvoja johtopäätöksiä. Tutkimuksessa tulisi myös huomioida onko muiden käyttöjärjestelmien kiristysohjelmahyökkäyksien määrät huomattavasti kasvaneet.

LÄHTEET

Al-Hawawreh, M., Alazab, M., Ferrag, M. A., & Hossain, M. S. (2024). Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms. *Journal of Network and Computer Applications*, *223*, 103809. https://doi.org/10.1016/j.jnca.2023.103809

Al-Hawawreh, M., Hartog, F. D., & Sitnikova, E. (2019). Targeted ransomware: a new cyber threat to edge system of Brownfield industrial internet of Things. *IEEE Internet of Things Journal*, *6*(4), 7137–7151. https://doi.org/10.1109/jiot.2019.2914390

Al-rimy, B. a. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, *74*, 144–166. https://doi.org/10.1016/j.cose.2018.01.001

Ashley, T., Gourisetti, S. N. G., Brown, N., & Bonebrake, C. A. (2022). Aggregate attack surface management for network discovery of operational technology. *Computers & Security*, *123*, 102939. https://doi.org/10.1016/j.cose.2022.102939

Baker, K. (2023, 30. tammikuuta). What is Ransomware as a Service (RaaS)? CrowdStrike. Haettu 28.3.2024 osoitteesta https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

Borenius, S., Gopalakrishnan, P., Tjernberg, L. B., & Kantola, R. (2022). Expert-Guided Security Risk assessment of evolving power grids. Energies, 15(9), 3237. https://doi.org/10.3390/en15093237

Capano, D. E. (2021, 30. syyskuuta). Throwback attack: How NotPetya ransomware took down Maersk. Industrial Cybersecurity Pulse. Haettu 5.4.2024 osoitteesta https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/

Cimpanu, C. (2018, 25. tammikuuta). Maersk reinstalled 45,000 PCs and 4,000 servers to recover from NotPetya attack. BleepingComputer. Haettu 5.4.2024 osoitteesta https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/

CISA. (ei pvm.). Critical infrastructure sectors. Cybersecurity and Infrastructure Security Agency. Haettu 1.4.2024 osoitteesta https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

CISA. (2020, 18. helmikuuta). Ransomware impacting Pipeline Operations. Cybersecurity and Infrastructure Security Agency. Haettu 5.4.2024 osoitteesta https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-049a

CISA. (2021a, heinäkuu). Rising Ransomware Threat To Operational Technology Assets. Cybersecurity and Infrastructure Security Agency. Haettu 28.4.2024 osoitteesta https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf

CISA. (2021b, 25. lokakuuta). Ongoing cyber threats to U.S. water and wastewater Systems. Cybersecurity and Infrastructure Security Agency. Haettu 28.4.2024 osoitteesta https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a

Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. Computers & Security, 79, 162–189. https://doi.org/10.1016/j.cose.2018.08.008

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*,

15(4), 277–305. https://doi.org/10.1007/s11416-019-00338-7

Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors*, 21(11), 3901. https://doi.org/10.3390/s21113901

Fayi, S. Y. (2018). What Petya/NotPetya ransomware is and what its remidiations are. In *Advances in intelligent systems and computing* (pp. 93–100). https://doi.org/10.1007/978-3-319-77028-4_15

Ghafur, S., Kristensen, S. R., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *Npj Digital Medicine*, *2*(1). https://doi.org/10.1038/s41746-019-0161-6

Keshavarzi, M., & Ghaffary, H. R. (2020). I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion. *Computer Science Review*, *36*, 100233. https://doi.org/10.1016/j.cosrev.2020.100233

Lockheed Martin. (ei pvm.). Cyber Kill chain. Haettu 28.4.2024 osoitteesta https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Industrial and critical infrastructure Security: Technical analysis of Real-Life Security Incidents. *IEEE Access*, *9*, 165295–165325. https://doi.org/10.1109/access.2021.3133348

National Audit Office. (2017, 24. lokakuuta). Investigation: WannaCry cyber attack and the NHS - NAO report. haettu 28.4.2024 osoitteesta https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

Nicol, D. M. (2021). The ransomware threat to Energy-Delivery systems. *IEEE Security & Privacy*, *19*(3), 24–32. https://doi.org/10.1109/msec.2021.3063678

Oz, H., Arış, A., Levi, A., & Uluagac, A. S. (2022). A survey on Ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys*, *54*(11s), 1–37. https://doi.org/10.1145/3514229

Parker, S., Wu, Z., & Christofides, P. D. (2023). Cybersecurity in process control, operations, and supply chain. Computers & Chemical Engineering, 171, 108169. https://doi.org/10.1016/j.compchemeng.2023.108169

Perrett, K., & Wilson, I. (2023). A cyber resilience analysis case study of an industrial operational technology environment. *Environment Systems & Decisions*, *43*(2), 178–190. https://doi.org/10.1007/s10669-023-09895-1

Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B. C. M., & Assi, C. (2023). The Age of Ransomware: A survey on the evolution, taxonomy, and research directions. *IEEE Access*, *11*, 40698–40723. https://doi.org/10.1109/access.2023.3268535

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for Cyber-Secure critical infrastructure. *Sensors*, *23*(8), 4060. https://doi.org/10.3390/s23084060

Sarkar, S., Teo, M. Y., & Chang, E. (2022). A cybersecurity assessment framework for virtual operational technology in power system automation. *Simulation Modelling Practice and Theory*, *117*, 102453. https://doi.org/10.1016/j.simpat.2021.102453

Solon, O., & Hern, A. (2017, 14. heinäkuuta). "Petya" ransomware attack: what is it and how can it be stopped? The Guardian. Haettu 5.4.2024 osoitteesta https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how

Staves, A., Gouglidis, A., Maesschalck, S., & Hutchison, D. (2024). Risk-based safety scoping of adversary-centric security testing on Operational Technology. *Safety Science*, *174*, 106481. https://doi.org/10.1016/j.ssci.2024.106481

Stergiopoulos, G., Gritzalis, D., & Limnaios, E. (2020). Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns. *IEEE Access*, *8*, 128440–128475. https://doi.org/10.1109/access.2020.3007960

Symantec. (2015). The evolution of ransomware. Haettu 19.4.2024 osoitteesta https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf

Symantec. (2017, 23. lokakuuta). What you need to know about the WannaCry Ransomware. Symantec Enterprise Blogs. Haettu 19.4.2024 osoitteesta https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware-attack

Virustotal. (2021). Ransomware in a global context. Haettu 6.4.2024 osoitteesta from https://assets.virustotal.com/reports/ransomware-in-a-global-context-2021