TURUN YLIOPISTO
Kauppakorkeakoulu

Ransomware-hyökkäysten ennaltaehkäisy

Tietojärjestelmätieteen kandidaatintutkielma

Laatija:
Martta Iso-Kuortti

Ohjaaja:
Samuli Laato

11.12.2024
Turku

Kanditutkielma

Oppiaine: Tietojärjestelmätiede
Tekijä(t): Martta Iso-Kuortti
Otsikko: Ransomware-hyökkäysten ennaltaehkäisy
Ohjaaja(t): Samuli Laato
Sivumäärä: 41 sivua
Päivämäärä: 11.12.2024

Ransomware-hyökkäykset ovat yksi merkittävistä yritysten tietoturvahaasteista, ja niiden torjuminen edellyttää monitasoista lähestymistapaa, jossa yhdistyvät tekniset ja ei-tekniset ennaltaehkäisymenetelmät. Tämä kandidaatintutkielma keskittyy ransomware-hyökkäysten ennaltaehkäisyyn ja tarjoaa kattavan analyysin akateemisessa kirjallisuudessa käsitellyistä menetelmistä. Työssä tarkastellaan teknisiä ratkaisuja, kuten pääsynhallintaa, kerrostettua suojausta ja Zero Trust -arkkitehtuuria, sekä ei-teknisiä menetelmiä, kuten käyttäjäkoulutusta, tietoturvapolitiikkoja ja turvallisuuskulttuurin kehittämistä.

Tutkimuksen päätavoite on selvittää, mitä ennaltaehkäiseviä tietoturvatoimia yritysten tulisi ottaa käyttöön suojautuakseen ransomware-hyökkäyksiltä. Lisäksi tutkielmassa arvioidaan menetelmien soveltuvuutta ja tehokkuutta yritysympäristössä. Tutkimustulokset osoittavat, että tehokas suojaus edellyttää teknisten ratkaisujen ja inhimillisten toimintamallien yhdistämistä. Tutkimus perustuu akateemiseen kirjallisuuteen ja tarjoaa käytännön suosituksia organisaatioille ransomware-hyökkäysten ennaltaehkäisyyn.

Avainsanat: ransomware, ennaltaehkäisy, tietoturva, kyberturvallisuus

Sisällys

Kuviot

Taulukot

1 Johdanto

Ransomware-hyökkäysten määrä ja niiden vaikutukset ovat kasvaneet yhä viime vuosina, ja ne muodostavat vakavan uhan niin yrityksille kuin yhteiskunnan kriittisille infrastruktuureille (Zimba & Chishimba, 2019b). Ransomware-hyökkäykset toimivat pääsääntöisesti estämällä pääsyn tärkeisiin tietoihin salauksen avulla ja vaatimalla lunnaita tietojen palauttamiseksi. Tämä kyberuhka on kasvanut yksittäisten käyttäjien kohdistamisesta laajamittaisiin organisaatioihin, joissa taloudelliset menetykset voivat nousta miljooniin dollareihin. (Djenna ym., 2024.) Hyökkäysten kehittyneisyys, kuten kryptovaluuttojen hyödyntäminen maksutapana ja kyberrikollisten käyttämät erilaiset hyökkäysvektorit, vaikeuttavat ransomware-hyökkäysten jäljittämistä ja torjuntaa (Nadir & Bakhshi, 2018).

Ransomware-hyökkäykset ovat kehittyneet viimeisen kahden vuosikymmenen aikana yksinkertaisista opportunistista hyökkäyksistä kehittyneiksi ja tarkasti suunnitelluiksi hyökkäyksiksi, jotka kohdistuvat yhä enemmän suuryityksiin ja julkisiin organisaatioihin. (Zimba & Chishimba, 2019b.) Näiden hyökkäysten kehittyminen on edistänyt tarvetta tarkastella sekä teknisiä että ei-teknisiä toimenpiteitä niiden ennaltaehkäisemiseksi. Yritykset ovat joutuneet kohtaamaan yhä monimutkaisempia hyökkäyksiä, joissa käytetään vahvoja salausalgoritmeja, kuten AES (advanced encryption standard) ja RSA (rivest–shamir–adleman), mikä tekee tiedostojen palauttamisesta mahdotonta ilman hyökkääjän antamaan avainta (Nadir & Bakhshi, 2018).

WannaCry -hyökkäys, joka käynnistettiin toukokuussa 2017, on yksi tunnetuimmista ransomware-hyökkäyksistä. Se levisi nopeasti maailmanlaajuiseksi, aiheuttaen tuhoa yli 150 maassa ja vaikuttaen satoihin yrityksiin ja organisaatioihin, mukaan lukien terveydenhuoltoalan toimijat, kuten Iso-Britannian National Health Service (NHS). WannaCry käytti hyväkseen Microsoftin Windows-käyttöjärjestelmässä olevaa SMB-protokollan haavoittuvuutta, joka tunnetaan nimellä EternalBlue. Hyökkäyksen seurauksena lukuisten organisaatioiden toiminta keskeytyi, joka johti miljoonien dollarien taloudellisiin tappioihin. (Chen & Bridges, 2017.) WannaCry osoitti, miten nopeasti ransomware voi levitä ja kuinka vakavat sen vaikutukset voivat olla, erityisesti silloin kun kyseessä on julkiset palvelut ja kriittiset infrastruktuurit.

Toinen merkittävä esimerkki ransomware-hyökkäyksestä on NotPetya, joka käynnistettiin kesäkuussa 2017. NotPetya levisi verkossa hyödyntämällä EternalBlue- ja EternalRomance -haavoittuvuuksia Windowsin SMB-protokollassa. Hyökkäys alkoi tartunnan saaneella tietokoneella, joka suoritti verkon ARP-skannauksen etsiäkseen uusia kohteita. NotPetya käytti tartunnan

saaneiden koneiden kirjautumistietoja levitäkseen muihin järjestelmiin. Toisin kuin WannaCry, se ei levinnyt epidemiatyyppisesti, vaan ainoastaan ensimmäisen tartunnan saanut laite suoritti kaikki myöhemmät tartunnat ennen muiden laitteiden aktivoitumista. NotPetya myös salasi kiintolevyn NTFS-tietojärjestelmän, mikä esti tietojen palautuksen. Tämä teki tiedostojen palauttamisesta mahdotonta, mikä aiheutti vakavia häiriöitä monille organisaatioille globaalisti. (Nguyen ym., 2024.)

Akateemisessa kirjallisuudessa on esitetty useita lähestymistapoja ransomware-hyökkäysten ennaltaehkäisyyn. Näihin kuuluu muun muassa teknisten menetelmien, kuten pääsynhallinnan ja kerrostetun suojauksen hyödyntäminen hyökkäysten ennaltaehkäisemiseksi. (Alshaikh ym., 2020.) Toisaalta myös ei-tekniset menetelmät, kuten työntekijöiden koulutus ja tietoturvapolitiikan tehostaminen, ovat osoittautuneet keskeisiksi ransomware-hyökkäysten ehkäisemisessä (Ibrahim & Ade, 2023). Vaikka perinteiset tietoturvamenetelmät eivät enää riitä torjumaan näitä yhä monimutkaisempia uhkia, esimerkiksi Zero Trust -arkkitehtuuria ja muita ennakoivia menetelmiä on alettu soveltaa yrityksissä (Ahn ym., 2024).

Tämän tutkimuksen päätavoitteena on analysoida, mitä ennaltaehkäiseviä tietoturvatoimia yritysten tulisi ottaa käyttöönsä ennaltaehkäistäkseen ransomware-hyökkäyksiä. Sakib ym., (2023) tuovat esiin, että sekä ihmisten tekemät virheet että teknologiset puutteet voivat johtaa ransomware-hyökkäysten onnistumiseen. Tällöin tehokas tietoturva vaatii monikerroksellisia ratkaisuja, joissa yhdistetään sekä teknisiä että organisatorisia toimenpiteitä. Tässä kanditutkielmassa pyritään tuomaan yhteen aiempi tutkimus, joka käsittelee ransomware-hyökkäysten torjumiseen tarkoitettuja teknisiä ja ei-teknisiä toimenpiteitä, sekä arvioimaan, mitkä näistä toimenpiteistä ovat keskeisimpiä nykyaikaisessa yritys- ja organisaatioympäristössä.

Tämän työn päätutkimuskysymys on: **Mitä tietoturvatoimia yritysten tulisi ottaa käyttöönsä ennaltaehkäistäkseen ransomware-hyökkäyksiä?**

Tutkimus tarkastelee myös kahta tarkentavaa tutkimuskysymystä:

1. Mitä teknisiä ja ei-teknisiä ransomware-hyökkäysten torjumiseen tarkoitettuja ennaltaehkäisymenetelmiä on käsitelty akateemisessa kirjallisuudessa?
2. Mitkä ransomwaren ennaltaehkäisymenetelmät ovat tehokkaimpia yritysnäkökulmasta?

Näiden kysymysten kautta tutkimus pyrkii ymmärtämään, miten organisaatiot voivat parhaiten suojautua ransomware-hyökkäyksiltä ja mitä toimia voidaan ottaa käyttöön hyökkäysten torjumiseksi.

Luvussa 2 tarkastellaan ransomware-hyökkäysten eri muotoja, niiden etenemisen vaiheita sekä vaikutuksia yritystasolla. Tämä luo pohjan tutkimuskysymysten tarkastelulle ja antaa kontekstin erilaisten ennaltaehkäisymenetelmien tarpeellisuuden ymmärtämiselle. Luvussa 3 keskitytään akateemisessa kirjallisuudessa käsiteltyihin ransomware-hyökkäysten ennaltaehkäisymenetelmiin, jotka jaotellaan teknisiin ja ei-teknisiin lähestymistapoihin. Luvussa arvioidaan näiden menetelmien tehokkuutta ja soveltuvuutta yritysympäristössä, tarjoten vastauksia päätutkimuskysymykseen ja tarkentaviin alatutkimuskysymyksiin käytännön näkökulmasta. Lopuksi luvussa 4 esitetään työn johtopäätökset ja annetaan käytännön ohjeistusta yrityksille sekä näkökulmia tulevaisuuden tutkimukselle.

2 Ransomwaren eri muodot, hyökkäyksen etenemisen eri vaiheet ja vaikutukset yritystasolla

Ransomware-hyökkäykset ovat viime vuosikymmeninä kehittyneet merkittävästi sekä teknisten että operatiivisten ominaisuuksien osalta, mikä on tehnyt niistä merkittävän uhan yrityksille ja organisaatioille (Zimba & Chishimba, 2019b). Näiden hyökkäysten tehokas torjunta ja hallinta edellyttävät kokonaisvaltaista ymmärrystä ransomwaren eri muodoista, toimintamekanismeista ja vaikutuksista. Tämä luku tarjoaa yleiskatsauksen ransomwaren keskeisiin ilmenemismuotoihin ja hyökkäyksen etenemisen eri vaiheisiin. Lisäksi tarkastellaan hyökkäysten vaikutuksia yritysnäkökulmasta, korostaen sekä taloudellisia että toiminnallisia seurauksia. Näin saadaan kattava kuva ransomware-hyökkäysten toimintalogiikasta ja niiden aiheuttamasta monimuotoisesta uhkakentästä.

2.1 Ransomwaren eri muodot

Ransomware-hyökkäysten tehokas ehkäisy edellyttää ymmärrystä niiden erilaisista muodoista ja toimintatavoista. Eri ransomware-tyypit hyödyntävät vaihtelevia mekanismeja tiedostojen salaamiseen tai järjestelmien käyttöoikeuksien estämiseen, mikä tarkoittaa, että ennaltaehkäisy- ja torjuntastrategiat on kohdennettava hyökkäysten erityispiirteisiin. Eri ransomware-muodot vaativat toisistaan poikkeavia lähestymistapoja, sillä niiden käyttämät salaus- ja jakelutekniikat vaihtelevat keskenään. Ymmärtämällä näiden uhkien toiminnallisia eroja voidaan ennaltaehkäisyn painopistealueet määrittää paremmin ja suojautua laajemmalta hyökkäyskirjolta.

Ransomware-hyökkäykset voidaan jakaa useisiin eri muotoihin, jotka hyödyntävät erilaisia menetelmiä uhrin tiedostojen salaamiseen tai järjestelmän käyttöoikeuksien estämiseen. Yleisimmät ransomware-tyypit ovat crypto-ransomware, locker-ransomware, doxware, scareware ja ransomware as a Service (RaaS). (Prasad & Kumar, 2024.) Zimba ja Chishimba (2019b) käsittelevät tutkimuksessaan myös crypto- ja locker-ransomwaren yhdistelmää hybrid-ransomwarea ja Mcintosh ym., (2024) esittävät tutkimuksessaan modernit ransomware-hyökkäykset, jotka hyödyntävät salauksen lisäksi tietojen varastamista. Ransomwaren tyypin valinta riippuu hyökkääjän tavoitteista, kuten tietojen salauksesta, pääsyn estämisestä tai pelkästä kiristämisestä (Anghel & Racautanu, 2019).

Crypto-ransomware, joka tunnetaan myös nimellä encrypting ransomware, salaa tiedostot tehokkailla salausalgoritmeilla, kuten AES ja RSA, estäen uhria käyttämästä tietojaan ilman purkuavainta. Crypto-ransomware keskittyy tiedostojen pysyvään hallintaan, mikä tekee siitä

erityisen vahingollisen, koska salauksen purkaminen ilman avainta on käytännössä mahdotonta. Hyökkäys alkaa usein sähköpostin tai haitallisten linkkien välityksellä, ja kun haittaohjelma on asennettu, se aloittaa tiedostojen salaamisen nopeasti. Hyökkääjät vaativat lunnaat usein kryptovaluutassa anonymiteettinsa säilyttämisesti, ja tietojen palauttamatta jättäminen voi johtaa pysyvään menetykseen. (Mohurle & Patil, 2017.) Tämä tekee crypto-ransomwaresta merkittävän uhan yrityksille, joiden toiminta on riippuvaista tiedostojen käytettävyydestä. Tyypillisiä esimerkkejä crypto-ransomwaresta ovat CryptoWall ja Locky, jotka hyödyntävät vahvoja salaustekniikoita. CryptoWall käyttää RSA-2048-salausta ja leviää usein sähköpostiliitteiden tai haitallisten verkkosivujen kautta. Locky taas lähetetään tyypillisesti haitallisten sähköpostiliitteiden avulla, joissa on makroja sisältäviä asiakirjoja hyödyntäen AES-salausta. (Anghel & Racautanu, 2019.)

Toinen ransomwaren ilmenemismuoto on locker-ransomware, joka tunnetaan myös nimellä non-encrypting ransomware. Toisin kuin crypto-ransomware, locker-ransomware ei salaa tiedostoja, vaan estää laitteen käytön kokonaan. Uhri näkee lukitusviestin ja maksamalla lunnaat voi saada laitteen takaisin käyttöönsä. (Prasad & Kumar, 2024.) Locker-ransomware estää uhria käyttämästä tietokonetta tai järjestelmää. Esimerkiksi Winlocker ja Reveton lukitsevat käyttöjärjestelmän ja vaativat maksua sen avaamiseksi. Winlocker estää pääsyn koko työpöytäympäristöön ja näyttää täysikokoisen ilmoituksen tietokoneen näytöllä, jossa pyydetään maksua lukituksen avaamiseksi. Reveton taas esittää olevansa laillinen lainvalvontaviranomaisen ilmoitus, joka vaatii sakon maksamista. (Anghel & Racautanu, 2019.)

Zimba ja Chishimba (2019b) käsittelevät tutkimuksessaan hybrid-ransomwarea, toisella nimellä hybrid encryption, joka edustaa kolmannen sukupolven ransomware-malleja. Hybrid-ransomware yhdistää crypto- ja locker-ransomwaren. Hybrid-ransomware on yksi nykyaikaisista ransomwaren muodoista, ja sen yhdistetyt ominaisuudet tekevät siitä erityisen vahingollisen. Näissä hyökkäyksissä yhdistyvät sekä tiedostojen salaus että laitteen käytön estäminen. WannaCry ja SamSam ovat tunnettuja esimerkkejä hybrid-ransomwaresta, jossa hyökkäykset levisivät laajoihin verkostoihin käyttäen worm-tyyppisiä mekanismeja sekä salausalgoritmeja, kuten AES-256 ja RSA. Worm-tyyppisillä mekanismeilla viitataan haittaohjelmiin, jotka pystyvät monistamaan itseään ja leviämään automaattisesti verkon kautta hyödyntämällä järjestelmän haavoittuvuuksia. AES-256 puolestaan on symmetrinen salausalgoritmi, jossa samaa avainta käytetään sekä tiedostojen salaamiseen että niiden avaamiseen. (Zimba & Chishimba, 2019b.)

Doxware tunnetaan myös nimellä leakware. Haittaohjelma ei lukitse tietokoneen käyttöoikeuksia tai salaa tiedostoja, vaan kiristää uhria uhkaamalla julkaista varastettuja tietoja (Anghel & Racautanu, 2019). Hyökkääjät uhkaavat julkistaa uhrin arkaluonteiset tiedot, ellei lunnaiden maksua suoriteta, mikä lisää hyökkäyksen painostusvaikutuksia (Prasad & Kumar, 2024). Doxware on yleisempää organisaatioihin kohdistuvissa hyökkäyksissä, jossa hyökkääjät uhkaavat vuotaa yrityksen luottamuksellisia tietoja, kuten asiakastietoja tai sopimuksia (Anghel & Racautanu, 2019).

Scareware taas manipuloi käyttäjää harhaanjohtavilla viesteillä, kuten väitteillä virustartunnoista. Uhria painostetaan maksamaan korjauspalveluista, jotka ovat todellisuudessa tarpeettomia tai haitallisia. (Prasad & Kumar, 2024.) Scareware ei varsinaisesti salaa tiedostoja tai lukitse järjestelmiä, vaan se luottaa käyttäjän pelon hyödyntämiseen saadakseen uhrin suorittamaan haluttuja toimintoja, kuten maksamaan palvelusta, jota ei oikeasti ole olemassa. Hyökkääjät käyttävät pelottelevia popup-mainoksia, jotka esittävät virheilmoituksia tai väitteitä, jossa käyttäjän laite on vaarantunut. Näiden viestien tarkoitus on huijata käyttäjä asentamaan haittaohjelma tai maksamaan lunnaita jonkin ohjelmiston aktivoimiseksi tai ongelman ratkaisemiseksi. Scareware hyödyntää sosiaalisen manipuloinnin taktiikoita, eikä usein aiheuta pysyvää vahinkoa järjestelmälle, vaan huijaa uhria taloudellisesti tai asentamalla muita haittaohjelmia. (Kovács, 2024.)

Ransomware as a Service (RaaS) -palvelumalli mahdollistaa jopa kokemattomien rikollisten käyttävän ransomware-työkaluja hyökkäysten suorittamiseen helppokäyttöisten hallintapaneeleiden avulla. (Prasad & Kumar, 2024.) RaaS toimii palvelumallina, joka mahdollistaa teknisesti kokemattomien käyttäjien suorittaa ransomware-hyökkäyksiä hyödyntämällä valmiita alustoja. Alustat tarjoavat valmiit työkalut, kuten mukautettavat ransomware-paketit ja infrastruktuurin, esimerkiksi maksujärjestelmät ja command-and-control-palvelimet. RaaS-käyttäjät voivat ostaa valmiita ransomware-paketteja, ja lunnaiden maksaminen tapahtuu usein kryptovaluutoilla. RaaS-alustojen kehittäjät hyötyvät jakamalla voittoa käyttäjien kanssa, yleensä ottamalla noin 30 % lunnaista. RaaS ei ainoastaan tarjoa haittaohjelmaa, vaan myös teknistä tukea ja ohjeita hyökkäyksen toteuttamiseen. Hyökkääjä voi itse räätälöidä haittaohjelman valitsemalla kohteeseen sopivat ominaisuudet, jonka jälkeen alusta hoitaa infrastruktuurin. Haittaohjelma levitetään tietojenkalasteluviesteillä, haitallisilla liitteillä, verkkosivujen kautta tai hyödyntämällä järjestelmän haavoittuvuuksia. Haittaohjelman aktivoiduttua kohdekoneessa, se salaa tiedostoja tai estää pääsyn järjestelmään. (Alwashali ym., 2021.)

Mcintoshin ym. (2024) tutkimuksessa käsitellään moderneja ransomware-hyökkäyksiä, jotka ovat siirtyneet kaksoiskiristystaktiikkaan, jossa hyökkääjät eivät pelkästään salaa tiedostoja, vaan myös

varastavat niitä. Varastetut tiedot toimivat lisäpainostuskeinona hyökkääjien uhkaamalla julkaista, myydä tai käyttää arkaluonteisia tietoja, ellei lunnaiden maksamista suoriteta. Datan eksfiltraatio on tehnyt moderneista hyökkäyksistä entistä kohdennetumpia ja vaarallisempia. Eksfiltraation onnistuminen tarkoittaa, että hyökkääjä voi uhata yrityksen mainetta ja liiketoimintaa, vaikka tiedostot olisi palautettu varmuuskopioista. Tutkimuksessa korostetaan, että jotkut ransomware-variantit sisältävät myös vakoiluominaisuuksia. Hyökkäykset voivat kerätä tietoa pitkällä aikavälillä, esimerkiksi tiedusteluvaiheen aikana, ennen toimitus- ja leviämisvaiheita (kuvio 1). Tämä tiedustelutoiminta mahdollistaa hyökkäysten kehittyneemmän suunnittelun ja tehokkuuden. Hyökkääjät voivat esimerkiksi tunnistaa kohdeyrityksen kriittisimmät järjestelmän ja tiedot, mikä tekee hyökkäyksestä täsmällisemmän. (Mcintosh ym., 2024.)

2.2 Ransomwaren etenemisen eri vaiheet

Ransomware-hyökkäykset noudattavat usein monivaiheista prosessia, joka voi sisältää tiedustelun, hyökkäyksen toimittamisen, tiedostojen salaamisen sekä kiristyksen. Hyökkääjät pyrkivät maksimoimaan vahingon hyödyntämällä sekä teknisiä haavoittuvuuksia että inhimillisiä heikkouksia, kuten sosiaalista manipulointia. (Prasad & Kumar, 2024). Näiden vaiheiden tarkempi ymmärrys on keskeistä tehokkaiden torjunta- ja ennaltaehkäisystrategioiden kehittämisessä. Vaikka ransomware-hyökkäysten vaiheet voivat vaihdella ja niissä voidaan painottaa eri elementtejä, tutkimuksissa on tunnistettu niille yhteisiä päävaiheita, jotka esiintyvät erilaisissa hyökkäyksissä. Nämä vaiheet eivät aina noudata täysin samaa kaavaa, mutta hyökkäykset jakavat usein samoja keskeisiä elementtejä, jotka on esitetty alla olevassa kuviossa.

Kuva 1 Ransomware-hyökkäysten vaiheet pohjautuen lähteeseen (Prasad & Kumar, 2024)

Ransomware-hyökkäyksen ensimmäisessä vaiheessa (kuvio 1) hyökkääjät keräävät mahdollisimman paljon tietoa kohdejärjestelmästä. Tiedusteluun voi sisältyä verkkoarkkitehtuurin, järjestelmien haavoittuvuuksien ja käyttäjätunnusten kartoitusta. Lisäksi hyökkääjät voivat

hyödyntää sosiaalista manipulointia, kuten tietojenkalastelua (eng. phishing), saadakseen pääsyn kriittisiin tunnistetietoihin. Tietojen hankkimiseen voidaan käyttää avoimen lähdetiedustelun menetelmiä, kohdistettuja tietopyyntöjä tai haavoittuvuusskannauksia. Näin hyökkääjät pystyvät suunnittelemaan mahdollisimman tehokkaan hyökkäysstrategian. Kerätyn tiedon pohjalta hyökkääjät laativat suunnitelman hyökkäyksen toteuttamiseksi. Suunnitteluvaiheessa analysoidaan tunnistetut haavoittuvuudet ja valitaan hyökkäyksen kohdistamiseen käytettävät menetelmät. Hyökkääjät voivat esimerkiksi valmistella haitallisia ohjelmistoja, jotka hyödyntävät havaittuja haavoittuvuuksia, tai räätälöidä tietojenkalastelukampanjoita erityisesti kohdeorganisaatioita varten. Tavoitteena on maksimoida hyökkäyksen vaikutus ja varmistaa, että kriittiset järjestelmät saadaan lamautettua. (Prasad & Kumar, 2024.)

Hyökkäyksen toimitusvaiheessa (kuvio 1) ransomware siirretään kohdejärjestelmään. Yleisimpiä menetelmiä ovat tietojenkalasteluviestit, haitalliset linkit, ohjelmistojen haavoittuvuuksien hyödyntäminen ja etätyöpöytäyhteyksien väärinkäyttö. Vuonna 2022 yleisin ransomware-hyökkäysten toimitustapa oli tietojenkalasteluviestit, joita käytettiin noin 38 % tapauksista. Tämän lisäksi haittaohjelmia levitettiin hyödyntämällä ohjelmistojen haavoittuvuuksia (26 %), etätyöpöytäprotokollan haavoittuvuuksia (20 %) sekä muita menetelmiä (16 %). Hyökkääjät voivat käyttää myös muita edistyneitä keinoja, kuten exploit-paketteja ja haitallista mainontaa, joilla hyödynnetään verkkoselaimen tai ohjelmistojen haavoittuvuuksia. (Prasad & Kumar, 2024.) Esimerkiksi WannaCry-ransomware hyödynsi EternalBlue-protokollan haavoittuvuuksia päästäkseen nopeasti leviämään yritysverkoissa (Zimba & Chishimba, 2019b).

Kun ransomware on asennettu kohdejärjestelmään, se aloittaa leviämisvaiheen (kuvio 1), jonka tavoitteena on laajentaa vaikutusalaa verkossa. Leviämisessä voidaan käyttää usein lateraalisia liikkeitä, joissa hyödynnetään verkon sisäisiä haavoittuvuuksia ja saavutetaan uusia kohteita, kuten varmuuskopiojärjestelmiä. Tämä vaihe voi sisältää myös käyttäjätunnusten väärinkäyttöä ja järjestelmävalvojan oikeuksien hankkimista. Leviämisen tarkoituksena on laajentaa hyökkäyksen vaikutuksia ja estää järjestelmien palauttaminen. (Prasad & Kumar, 2024.) WannaCry-hyökkäyksen kaltaisilla ransomwareilla, jotka sisältävät kyseisiä worm-ominaisuuksia, on kyky skannata sekä paikallisia että julkisia IP-osoitteita naapuriverkoissa. Tämä mahdollistaa ransomware-hyökkäyksen laajenemisen ei vain sisäverkkoihin vaan myös ulkoisiin järjestelmiin. Hyökkäyksessä voidaan käyttää esimerkiksi preudorandom number generator (PRNG) -mekanismeja, jotka luovat näennäissatunnaisia IP-osoitteita skannausprosessiin. Näin esimerkiksi WannaCry hyödyntää PRGN:ää generoimaan IP-osoitealueita, jotka skannataan sekä paikallisissa että julkisissa verkoissa. Kaikki ransomwaret eivät kuitenkaan toimi samalla tavalla, sillä leviämisominaisuudet, kuten

worm-tyyppiset ominaisuudet ja PRNG:n käyttö, ovat tyypillisiä kehittyneille kolmannen sukupolven ransomwareille. Aikaisemmat ransomwaret eivät sisältäneet tällaisia mekanismeja, vaan ne olivat yksinkertaisempia ilman kykyä laajentaa vaikutusaluettaan automaattisesti. (Zimba & Chishimba, 2019b.)

Salausvaiheessa (kuvio 1) ransomware hyödyntää kehittyneitä salaustekniikoita uhrin tiedostojen lukitsemiseksi ja niihin pääsyn estämiseksi. Ransomware luo salausavaimet, jotka välitetään usein hyökkääjän komentopalvelimelle turvallisen avaintenvaihtomekanismin avulla. Joissakin tapauksissa ransomware voi suorittaa salauksen täysin paikallisesti ilman ulkoista yhteyttä, kuten SamSam-ransomware, mikä tekee sen havaitsemisesta ja estämisestä haastavampaa. (Prasad & Kumar, 2024.) Modernit ransomware-mallit käyttävät edistyneitä hybridisalaustekniikoita, jotka yhdistävät symmetristä ja epäsymmetristä salausta. Hybridimalleissa ransomware generoi symmetrisen avaimen, kuten AES, joka salaa yksittäiset tiedostot. Tämä avain salataan hyökkääjän hallussa olevalla RSA-avaimella, mikä tekee AES-avaimen palauttamisen uhrille lähes mahdottomaksi ilman hyökkääjän yksityistä RSA-avainta. (Zimba & Chishimba, 2019b.)

Lunnasvaatimusvaiheessa (kuvio 1) uhri saa viestin, jossa ilmoitetaan tiedostojen salauksesta ja esitetään ohjeet lunnaiden maksamiseen. Lunnaat vaaditaan usein maksettavaksi esimerkiksi kryptovaluutassa, kuten bitcoinissa, anonymiteetin säilyttämiseksi. Viestissä voi olla esimerkiksi uhkauksia, kuten tietojen pysyvästä tuhoamisesta tai julkaisemisesta, ellei maksua suoriteta määräajassa. (Prasad & Kumar, 2024.) Esimerkiksi WannaCry antoi uhreille 72 tuntia aikaa maksaa lunnasvaatimukset ennen tietojen lopullista menetystä (Zimba & Chishimba, 2019a). Hyökkääjät voivat tarjota myös yhteydenottokanavia, kuten sähköpostiosoitteen tai Tor-verkon sivuston, joiden kautta uhri voi ottaa yhteyttä hyökkääjiin ja saada lisäohjeita tai jopa neuvotella maksun suuruudesta (Prasad & Kumar, 2024).

Hyökkäyksen loppuvaiheissa (kuvio 1) hyökkääjät voivat myös kiristää uhria uhkaamalla pysyvällä tiedostojen tuhoamisella tai niiden julkistamisella. Hyökkääjät saattavat uhata tuhota salatut tiedostot pysyvästi, mikäli lunnaat jätetään maksamatta. Uudemmat ransomware-variantit, kuten Maze ja REvil, yhdistävät tiedostojen salauksen ja varastamisen. Hyökkääjät uhkaavat julkaista varastetut tiedostot julkisesti tai myydä niitä, ellei lunnaita makseta. Joissakin tapauksissa hyökkääjät voivat vaatia lisälunnaat uhaten julkaista varastettuja tietoja useissa erissä, mikäli heidän vaatimuksiinsa ei suostuta. Tämä kaksinkertainen kiristysstrategia lisää hyökkäyksen vaikutusta ja painostaa uhria maksamaan lunnaat mahdollisimman nopeasti. (Prasad & Kumar, 2024.)

Yrityksille hyökkäyksen loppuvaihe tarkoittaa usein merkittäviä kustannuksia, kuten tuotantokatkoja, tietojen palauttamisyrityksiä sekä tietoturvajärjestelmien parantamiseen liittyviä toimenpiteitä. Lisäksi on mahdollista, ettei tiedostoja saada palautettua, vaikka lunnaat maksettaisiin, mikä korostaa tehokkaiden varmuuskopio- ja ennaltaehkäisystrategioiden tärkeyttä. (Zimba & Chishimba, 2019b.) Hyökkäyksen loppuvaihe ei pääty pelkästään lunnaiden maksamiseen, vaan sen seuraukset voivat ulottua syvemmälle yrityksen toimintaan, aiheuttaen huomattavia taloudellisia ja operatiivisia tappioita. Seuraavassa alaluvussa (2.3) tarkastellaan vaihtoehtoja, joita yrityksillä on vastata hyökkäyksiin, kuten lunnaiden maksaminen tai maksamatta jättäminen sekä näiden ratkaisujen vaikutuksia.

2.3 Ransomware-hyökkäysten vaikutukset yritystasolla

Ransomware-hyökkäysten vaikutuksesta yritykset voivat joutua maksamaan lunnaita, menettämään kriittisiä tietojaan pysyvästi tai kokea pitkien käyttökatkosten seurauksena suuria toimintakuluja (Al-Rimy ym., 2018). Connollyn ym., (2020) tutkimus käsittelee ransomware-hyökkäysten vaikutuksia organisaatioihin ja selvittää, mitkä tekijät vaikuttavat hyökkäysten vakavuuteen. Tutkimuksen mukaan yrityksen sektorilla ja tietoturvan tasolla on merkittävä vaikutus hyökkäysten seurauksiin. Erityisesti yksityisen sektorin yritykset, joilla on heikompi tietoturvapositio, kärsivät suhteellisesti vakavampia taloudellisia ja toiminnallisia menetyksiä kuin julkisen sektorin toimijat. Tutkimuksessa todettiin, että kohdennetut hyökkäykset, joissa hyökkääjät käyttävät räätälöityjä haittaohjelmia ja tunkeutuvat järjestelmiin, aiheuttavat usein suuria lunnasvaatimuksia sekä pitkiä käyttökatkoksia, mitkä voivat pahimmillaan lamaannuttaa yrityksen toiminnan pitkiksi ajoiksi. (Connolly ym., 2020.)

Zimba ym., (2019a) korostavat, että WannaCry-hyökkäys aiheutti maailmanlaajuisesti laajoja taloudellisia tappioita, kun sen kohteiksi joutui yli 300 000 uhria muutamassa päivässä. Joissakin tapauksissa yritykset joutuivat käyttämään miljoonia dollareita järjestelmien palauttamiseen. Tämä tapahtui joko maksamalla lunnaat, kuten Hollywood Presbyterian Medical Center maksoi 17 000 dollaria tai Hancock Health 55 000 dollaria. Vaihtoehtoisesti yritykset hyödynsivät varmuuskopioita, mikä kuitenkin aiheutti merkittäviä kustannuksia palautusprosessin ja tuotannonmenetysten vuoksi. Atlantan kaupunki esimerkiksi käytti yli 2,6 miljoonaa dollaria palautustoimenpiteisiin, vaikka lunnasvaatimukset olivat vain 50 000 dollaria. WannaCry-tyyppiset itsestään leviävät hyökkäykset voivat lamaannuttaa koko yritysverkoston ja vahingoittaa myös etävarmuuskopioita, mikä moninkertaistaa vaikutukset ja kustannukset. (Zimba & Chishimba, 2019a.)

Paquet-Cloustonin ym., (2019) tutkimus tuo esille ransomware-hyökkäysten merkittäviä taloudellisia vaikutuksia yrityksille ja organisaatioille. Esimerkiksi Locky- ja CryptXXX -ransomware-suvut ovat keränneet yhteensä miljoonia dollareita lunnaita, Locky yksinään jopa 7,8 miljoonaa dollaria vuosina 2016–2017 ja CryptXXX noin 1,9 miljoonaa dollaria. SamSam-hyökkäykset ovat erityisesti ransomware-iskuja, joissa hyökkääjät tunkeutuvat järjestelmään ja salaavat kriittisiä tietoja vaatiakseen huomattavia lunnaita niiden palauttamiseksi. Näissä hyökkäyksissä rikolliset usein käyttävät räätälöityjä haittaohjelmia ja kohdentavat hyökkäyksensä tarkoin valittuihin yrityksiin ja julkisiin organisaatioihin, mikä mahdollistaa lunnasvaatimusten asettamisen jopa kymmeniin tuhansiin dollareihin. (Paquet-Clouston ym., 2019.)

Vuosi 2023 toi esiin yhä vakavampia ransomware-hyökkäysten vaikutuksia yrityksiin ja yhteiskunnallisiin palveluihin. Esimerkiksi Royal Mailin hyökkäys tammikuussa 2023 pysäytti kansainväliset postikuljetukset yli kuudeksi viikoksi ja aiheutti merkittäviä taloudellisia menetyksiä sekä asiakasluottamuksen heikkenemistä. Lisäksi LockBit-ransomware-ryhmä vaati yritykseltä alun perin 80 miljoonan dollarin lunnaita, ja lopulta tämä summa neuvoteltiin puoleen. Royal Mail kieltäytyi kuitenkin maksamasta alkuperäistä lunnasvaatimusta, ja LockBit julkaisi myöhemmin neuvotteluasiakirjat osoittaakseen vaatimusten alentamisen. Royal Mail ole kuitenkaan kommentoinut, maksettiinko lunnaita osittain vai ei, jättäen lopullisen tilanteen epäselväksi. Muita merkittäviä tapauksia olivat Minneapolisin koulupiirin hyökkäys, joka johti yli 100 000 henkilön yksityistietojen vuotamiseen, sekä Capital hyökkäys, jossa kriittiset hallinnon sopimuksiin liittyvät tiedot päätyivät pimeään verkkoon. Dallasin kaupungin tapauksessa hyökkäys katkaisi palveluja, ja kaupungin hallinnon korjauskustannukset nousivat jopa 8,5 miljoonaan dollariin. (Teichmann & Boticiu, 2024.)

Humayun ym., (2021) huomauttavat, että ransomware-hyökkäykset ovat kasvaneet erityisen nopeasti myös IoT-ympäristössä (eng. internet of things) viime vuosina, sillä ne hyödyntävät IoT-laitteiden laajentunutta käyttöä ja järjestelmien yhteyksiä. Ransomware-hyökkäykset IoT-järjestelmissä voivat aiheuttaa yrityksille ja organisaatioille merkittäviä taloudellisia tappioita ja käyttökatkoja, koska hyökkäykset pystyvät lamauttamaan kriittisiä toimintoja koko verkostossa. IoT:n kasvun myötä hyökkäysten vaikutukset eivät rajoitu pelkästään yksittäisiin laitteisiin, vaan niillä on potentiaalia häiritä kokonaisia toimitusketjuja tai infrastruktuureja. Tämä voi johtaa operatiivisiin ongelmiin, jotka vaikuttavat yritysten toiminnan jatkuvuuteen ja aiheuttavat kustannuksia miljoonien dollareiden edestä. (Humayun ym., 2021.)

Ransomware-hyökkäykset ovat yhä monimuotoisempia ja kohdistuvat erityisesti haavoittuviin sektoreihin, kuten terveydenhuoltoon, rahoitukseen ja julkisin palveluihin, joissa tietojen menetys ja mainehaitat voivat olla erityisen suuria. Ransomware-as-a-Service (RaaS) -malli on madaltanut hyökkäysten toteuttamiskynnystä, mikä lisää yrityksille kohdistuvaa painetta varautua ja parantaa resilienssiään kyberturvallisuusstandardien avulla. Ransomware-hyökkäysten suorat ja epäsuorat kustannukset, kuten taloudelliset tappiot, maineen menetykset ja oikeudelliset seuraukset, muistuttavat yrityksiä ennaltaehkäisyn merkityksestä nykypäivän monimutkaisessa uhkakentässä. (Muniandy ym., 2024.)

Mcintoshin ym., (2024) tutkimus korostaa, että datan eksfiltraatio on noussut merkittäväksi osaksi kiristysohjelmien toimintatapaa, mikä on muuttanut hyökkäysten luonnetta ja uhrien kohtaamia riskejä. Perinteisesti kiristysohjelmat keskittyvät tiedostojen salaamiseen ja niiden vapauttamisen ehtona on lunnasrahojen maksaminen. Nykyään yhä useammat hyökkäykset yhdistävät tiedostojen salaamisen lisäksi datan varastamisen, tai keskittyvät pelkästään eksfiltraatioon ilman salausta. Datan eksfiltraatio tarjoaa hyökkääjille monipuolisempia painostuskeinoja. Uhria voidaan uhata esimerkiksi luottamuksellisten tietojen julkaisemisella, myymisellä kolmansille osapuolille tai väärinkäytöllä. Näillä keinoilla hyökkääjät pyrkivät maksimoimaan lunnaiden maksamisen todennäköisyyden ja mahdollisen rahallisen hyödyn. Datan eksfiltraatioon liittyvä kehys heijastaa hyökkääjien liiketoimintamallin muutosta. Koska organisaatiot ovat parantaneet varmuuskopiointistrategioitaan ja vähentäneet halukkuutta maksaa lunnaita, hyökkääjät ovat alkaneet painottaa tapoja, joilla voidaan lisätä uhreihin kohdistuvaa painetta ilman, että he pystyvät välttämään lunnaiden maksamista pelkästään palauttamalla tiedot varmuuskopioista. (Mcintosh ym., 2024.)

3 Akateemisessa kirjallisuudessa käsitellyt ransomware-hyökkäysten ennaltaehkäisymenetelmät

Tässä luvussa käsitellään akateemisessa kirjallisuudessa esiteltyjä menetelmiä ransomware-hyökkäysten ennaltaehkäisyyn. Menetelmät on ryhmitelty teknisiin ja ei-teknisiin lähestymistapoihin. Teknisten menetelmien tavoitteena on suojata järjestelmät haittaohjelmilta, tunnistaa epäilyttävä toiminta ja estää hyökkäysten eteneminen organisaation sisällä. Ei-tekniset menetelmät puolestaan painottavat inhimillisten virheiden vähentämistä ja tietoturvakulttuurin kehittämistä organisaatioissa. Ransomware-hyökkäysten ennaltaehkäisymenetelmiä tarkastellaan tässä luvussa erityisesti yritysnäkökulmasta, vertaillen niitä menetelmien vahvuuksien, heikkouksien, kustannustehokkuuden ja soveltuvuuden perusteella. Arvioinnin tueksi on laadittu kaksi taulukkoa; toinen käsittelee teknisiä menetelmiä ja toinen ei-teknisiä ennaltaehkäisymenetelmiä. Taulukot tarjoavat tiivistetyn esityksen eri menetelmien hyödyistä ja rajoitteista yritysympäristössä. Lisäksi taulukot täydentävät analyysia, joka esitetään yksityiskohtaisemmin taulukoiden alapuolella.

Luvussa tarkastellut ennaltaehkäisymenetelmät on valittu akateemisen kirjallisuuden perusteella. Valintakriteerinä on menetelmien relevanssi yritysmaailmassa sekä niiden toimivuuden ja soveltuvuuden arviointi kirjallisuuden pohjalta. Kirjallisuudesta valittiin erityisesti sellaisia tutkimuksia, joissa esiteltyjä menetelmiä voidaan soveltaa ransomware-hyökkäysten ennaltaehkäisyyn, ja tarkastelussa painotettiin näiden menetelmien analysointia ja vertailua yritysympäristössä. Valintaprosessissa hyödynnettiin keskeisiä tutkimuksia, kuten Mcintosh ym., (2024), Mcintosh ym., (2021), Pagán & Khaled (2021), Alshaikh ym., (2020), Silva ym., (2019), Al-Rimy ym., (2018), Tailor & Patel (2018) sekä Luo & Liao, (2007).

3.1 Tekniset ennaltaehkäisymenetelmät ja niiden tarkastelu yritysnäkökulmasta

Menetelmä	**Vahvuudet**	**Heikkoudet**	**Kustannus-tehokkuus**	**Soveltuvuus yritysympäristössä**	**Lähteet**
Pääsynhallinta	Estää valtuuttamattoman käytön; joustavat asetukset	Tehoton ilman säännöllistä auditoimista	Kustannustehokas, mutta auditointi vaatii resursseja	Soveltuu hyvin tiedostosuojausta vaativille yrityksille	(Ami ym., 2018) (Parkinson, 2017)

					(Kim & Lee, 2020)
Palomuurit	Estää tunnetut haitalliset IP-osoitteet ja liikenteen	Ei tunnista uusia tai hyvin naamioituja uhkia	Kohtuullinen, mutta vaatii ylläpitoa	Soveltuva osana monikerroksista puolustusta	(Pagán & Khaled, 2021)
Zero Trust -arkkitehtuuri	Mikrosegmentointi estää etenemisen; jatkuva valvonta	kallis käyttöönotto ja infrastruktuurin muutos	Pitkällä aikavälillä kustannustehokas	Hyvä soveltuvuus kriittistä tietoturvaa vaativille yrityksille	(Adahman ym., 2022) (Kindervag, 2010)
Houkuttelu-tiedostot	Havaitsee ja estää nopeasti uusia hyökkäyksiä	Ei estä alkuperästä hyökkäystä	Kustannustehokas lisä suojausstrategioihin	Soveltuu yrityksille, joissa kriittistä dataa ja nopeaa reagointia tarvitaan	(Lin & Lee, 2023) (Wang ym., 2018)
Itse-konfiguroitava ehkäisymekanismi IoMT-ympäristöihin	Automaatio vähentää manuaalista työtä; skaalautuva	Rajoittunut testaus ja uusia variantteja vaikea tunnistaa	Pienet ylläpitokustannukset avoimen lähdekoodin ansiosta	Soveltuu suurille IoT- ja IoMT-ympäristöille	(Tariq ym., 2022)
Säännölliset varmuuskopiot	Palauttaa tiedot ilman lunnaita; offline-suojaus tehokas	Vanhentuneet varmuuskopiot tehottomia	Pitkällä aikavälillä kustannustehokas	Keskeinen osa yritysten tietoturvaa	(Luo & Liao, 2007) (Al-Rimy ym., 2018)
Tietoturva-päivitykset ja -korjaukset	Sulkevat tunnetut haavoittuvuudet	Ei suojaa nollapäivähyökkäyksiltä	Kustannustehokas, jos automatisoitu	Soveltuva kaikenkokoisille yrityksille	(Al-Rimy ym., 2018) (Herrera Silva ym., 2019)
Päätelaitteiden tunnistus- ja	Reaaliaikainen uhkien tunnistus;	Monimutkainen käyttöönotto; mahdolliset väärät	Tehokas, mutta käyttöönotto voi olla kallista	Sopii monikerroksiseen suojaukseen	(Cappello, 2024)

reagointimenetelmä	automatisoitu toiminta	positiiviset hälytykset			
Verkon segmentointi	Rajoittaa hyökkäyksen leviämisen verkossa ja suojaa kriittisiä resursseja	Ei estä alkuperäistä hyökkäystä; vaatii huolellista suunnittelua	Kohtuullinen; riippuu verkon koosta ja monimutkaisuudesta	Erityisen hyödyllinen kriittisen infrastruktuurin suojaamiseen	(Zhanhui & Rahman, 2017) (Zimba & Rahman, 2017)
Monivaiheinen tunnistautuminen	Vahva suojaus varastettuja tunnuksia vastaan	Voi hidastaa käyttöä; haastava ottaa käyttöön vanhoissa järjestelmissä	Hyvä; erityisesti pilvipohjaisilla ratkaisuilla	Tärkeä kriittisten järjestelmien suojaukseen	(Takeuchi ym., 2023)
Kerrostettu suojaus	Yhdistää useita tehokkaita suojakeinoja	Ei havaitse kaikkia variantteja; monimutkaisuus	Kallis, mutta vähentää tietojen menetyksen riskiä ja tarjoaa kattavan suojan	Sopii suurille yrityksille, joissa kriittistä dataa	(Shaukat & Ribeiro, 2018)

Taulukko 1 Tekniset ennaltaehkäisymenetelmät

3.1.1 Pääsynhallinta

Pääsynhallinta ennaltaehkäisymenetelmänä rajoittaa tiedostoihin kohdistuvia muokkaus- ja poistotoimenpiteitä valtuuttamattomilta ohjelmilta ja prosesseilta. Se perustuu käyttäjien tai sovellusten autentikointiin ja valtuuttamiseen ennen tiedosto-operaatioiden sallimista, mikä vähentää haittaohjelmien mahdollisuutta päästä käsiksi suojattuihin tiedostoihin. (Ami ym., 2018.) Parkinson (2017) korostaa periaatetta, jossa käyttäjien oikeudet rajoitetaan vain välttämättömään. Tämä estää ransomwarea käyttämästä ylimääräisiä käyttöoikeuksia tiedostojen salaukseen tai poistamiseen. (Parkinson, 2017.) Kim ja Lee (2020) taas ehdottavat tutkimuksessaan sallintalistaan perustuvaa pääsynhallintaa, jossa vain tietyn listan mukaiset ohjelmat saavat pääsyn tiedostotyyppeihin. Tämä estää ransomwarea pääsemästä tiedostoihin, vaikka ohjelma olisi uusi tai tuntematon. (Kim & Lee, 2020.)

Amin ym., (2018) esittämä Antibotics on autentikointiin perustuva pääsynhallintajärjestelmä, joka suojaa tiedostoja ransomware-hyökkäyksiltä. Se hyödyntää biometrisiä tunnistusmenetelmiä, kuten sormenjälkitunnistusta, ja CAPTCHA-tehtäviä varmistaakseen, että tiedostojen muokkaus- ja poistoyritykset ovat luvallisia. Järjestelmä toimii tiedostojärjestelmän suodatinajurina, joka tarkistaa tiedosto-operaatioiden pyynnöt ja asettaa haasteita ennen tiedostojen muokkausta.

Järjestelmänvalvoja voi määrittää suojatut tiedostot, haasteiden tyypit ja voimassaoloajat, mikä mahdollistaa käyttäjäkokemuksen ja turvallisuuden tasapainottamisen. Sen vahvuutena on kyky estää täysin suojattujen tiedostojen luvaton käyttö, mikä tekee menetelmästä tehokkaan myös nykyisiä ransomware-hyökkäyksiä vastaan. Ohjelma on testattu vain Windows-käyttöjärjestelmässä, eikä sen tehokkuutta tulevaisuuden kehittynyttä ransomwarea vastaan voida siten taata. (Ami ym., 2018.)

Parkinson (2017) ehdottaa tutkimuksessaan käyttäjien käyttöoikeuksien rajoittamista hierarkisesti, mikä estää ransomwarea pääsemästä tiedostojärjestelmien tärkeimpiin osiin. Roolipohjainen käyttöoikeuksien hallinta voi vähentää vahinkoa ja estää ransomwarea toimimasta kohdekoneessa laajasti. (Parkinson, 2017.) Genç ym., (2018) ehdottivat menetelmää, joka estää ransomwarea käyttämästä järjestelmän satunnaislukugeneraattoreita (PRNG) avainten luomiseen, mikä pysäytti 94 % testatuista ransomware-näytteistä. Tämä menetelmä ei kuitenkaan pysty estämään ransomwarea, joka ei tunkeudu PRGN-funktioihin, mikä rajoittaa sen sovellettavuutta. (Genç ym., 2018.) Tiedostojen käyttöoikeuksia suositellaan rajoitettavaksi niin korkealle hakemistorakenteessa kuin mahdollista, mutta tämän menetelmän tehokkuus riippuu siitä, kuinka hyvin se on toteutettu. Pääsynhallintamenetelmien tehokkuus voi heiketä, jos käyttöoikeuksien ja roolien auditointeja ei suoriteta säännöllisesti, mikä puolestaan jättää aukkoja järjestelmän suojausmekanismeihin. (Beaman ym., 2021.)

3.1.2 Palomuurit

Palomuurit ovat keskeinen osa monikerroksista puolustusta, ja niiden tehtävänä on tarkastaa ja suodattaa verkkoliikennettä, estää tunnetut haitalliset IP-osoitteet, maantieteelliset alueet ja portit sekä käyttää tunkeutumisen havaitsemis- ja estojärjestelmiä liikenteen analysointiin. Palomuurit on tarkoitettu estämään haitallinen liikenne jo ennen kuin se saavuttaa verkon sisäiset resurssit. Tämä voi sisältää eston haitallisten verkkosivujen tai tunnettuja haitallisia verkkokohteita käyttäen. Pagánin & Khaledin (2021) tutkimuksessa korostetaan palomuurin sääntöjen tarkkaa määrittelyä, kuten bit torrent -porttien estoa ja yrityksen toimintaan liittyvien tarpeettomien IP-osoitteiden ja alueiden estämistä. Palomuureilla pyritään katkaisemaan hyökkäyksen ennen kuin haittaohjelmat pääsevät leviämään verkkoon. (Pagán & Khaled, 2021.)

Palomuurien tehokkuus riippuu oikeiden sääntöjen luomisesta ja soveltamisesta. Tämä vaatii asiantuntemusta ja jatkuvaa ylläpitoa, mikä voi olla haastavaa rajallisten resurssien omaaville organisaatioille. Vaikka palomuurit voivat estää tunnettuja haitallisia IP-osoitteita ja liikennettä, ne eivät välttämättä pysty havaitsemaan uusia tai hyvin naamioituja hyökkäyksiä, kuten

nollapäivähaavoittuvuuksia. Palomuurit tarvitsevat toimiakseen myös jatkuvaa ylläpitoa ja sääntöjen päivittämistä. Yksittäin menetelmä ei riitä estämän ransomware-hyökkäyksiä, vaan ne toimivat osana laajempaa monikerroksista puolustusta. (Pagán & Khaled, 2021.)

3.1.3 Zero Trust -arkkitehtuuri

Zero Trust -arkkitehtuuri on tietoturvamalli, joka perustuu periaatteeseen ”ei koskaan luoteta, aina tarkistetaan”. Tämä lähestymistapa poistaa oletetun luottamuksen organisaation sisä- ja ulkopuolella, varmistaen, että jokainen käyttöoikeuspyyntö todennetaan jatkuvasti käyttäjän identiteetin, laitteen tilan ja organisaation tietoturvapolitiikkojen mukaisesti. (Kindervag, 2010.) Zero Trust -arkkitehtuurin toiminta perustuu käyttäjien ja laitteiden tarkkaan todennukseen ja pääsynvalvontaan, jossa käyttö rajoitetaan vain pyydettyihin resursseihin, sekä jatkuvaan verkon valvontaan ja lokitukseen, joiden avulla epäilyttävät toimet voidaan havaita nopeasti. Tämä arkkitehtuuri estää haittaohjelmien etenemisen verkossa ja suojaa organisaation resursseja. (Adahman ym., 2022.) Zero Trust tarjoaa myös monitasoisen suojauksen kaikille digitaalisessa ympäristössä oleville resursseille, kuten pilvipalveluille (Kindervag, 2010).

Zero Trust -arkkitehtuuri on tehokas lähestymistapa ransomwaren ennaltaehkäisyyn, sillä sen perusperiaate käsitellä kaikkea liikennettä epäluotettavana parantaa yrityksen tietoturvaa. Mikrosegmentoinnin avulla estetään haittaohjelmien leviäminen järjestelmän sisällä, ja tarkasti määritellyt pääsynhallintasäännöt varmistavat, että vain valtuutettu liikenne hyväksytään. Jatkuva valvonta ja kattava lokitietojen analysointi mahdollistavat nopean reagoinnin poikkeamiin ja haitalliseen toimintaan. (Adahman ym., 2022; Kindervag ym., 2022.) Vaikka käyttöönotto voi olla kustannuksiltaan korkea ja vaatia infrastruktuurimuutoksia, Zero Trust tarjoaa hyvän soveltuvuuden yritysympäristöihin, joissa tietoturvan ylläpito on kriittistä.

3.1.4 Houkuttelutiedostot

Houkuttelutiedosto on tietoturvamenetelmässä käytettävä tiedosto, joka toimii syöttinä ransomware-hyökkäysten havaitsemiseksi ja estämiseksi. Tiedosto sijoitetaan strategisesti järjestelmään, ja sen avulla pyritään huijaamaan ransomwarea käsittelemään ensin juuri tätä tiedostoa. Kun ransomware salaa tai vahingoittaa houkuttelutiedostoa, järjestelmä tunnistaa hyökkäyksen ja aktivoi suojamekanismin. Järjestelmä käyttää valvontaohjelmaa, joka tarkkailee jatkuvasti houkuttelutiedoston tilaa. Jos tiedosto vahingoittuu, tietokone sammutetaan välittömästi estääkseen ransomwarea salaamasta muita tiedostoja. Tämä mekanismi minimoi vahingot ja suojaa käyttäjän

dataa. Tiedoston valvontaprosessi tarkistaa sen sisällön esiasetetun tunnistusavaimen avulla varmistaakseen, ettei ransomware ole muuttanut tiedostoa. (Lin & Lee, 2023.)

Wang ym., (2018) esittelemä menetelmä kuuluu kyberturvallisuuteen perustuvan harhautusteknologian (eng. cyber deception technology) sovelluksiin. Se on erityisesti suunnattu RDP-pohjaisten ransomware-hyökkäysten havaitsemiseen ja torjuntaan. Menetelmä käyttää harhautusteknologiaa, joka houkuttelee hyökkääjät ansaan suojaten tärkeitä järjestelmiä kohdennetuilta ransomware-hyökkäyksiltä. Lisäksi se hyödyntää luonnollisen kielen käsittelyä ja koneoppimista, joita käytetään hyökkäyksen jäljittämiseen ja alkuperäisten hyökkäyslähteiden tunnistamiseen. Menetelmä on erikoistunut RDP-protokollaa hyödyntävien hyökkäysten estämiseen ja haittaohjelmien jäljittämiseen, eli sen sovellettavuus rajoittuu nimenomaan tähän hyökkäystyyppiin. (Wang ym., 2018; Alshaikh ym., 2020.)

Lenin ja Leen (2023) tutkimuksessa simuloitiin kolmen erityyppisen ransomware-hyökkäyksen käyttäytymistä. Ehdotettu menetelmä saavutti 98,82 %:n suojauksen tiedostoille ja 100 %:n suojauksen, jos tiedostoja ei ollut tallennettu C-asemaan. Houkuttelutiedostojen käyttö osoittautui tehokkaaksi menetelmäksi uusien ja tuntemattomien ransomware-hyökkäysten estämisessä. Houkuttelutiedostoja hyödyntävä menetelmä ei korvaa antivirus-ohjelmistoja, mutta se voi täydentää niiden suojauskykyä uusien ja tuntemattomien ransomware-hyökkäysten osalta. (Lin & Lee, 2023.) Houkuttelutiedostot ovat käytännöllinen ja tehokas lisä organisaatioiden tietoturvastrategioihin ransomwarea vastaan. Ne auttavat havaitsemaan hyökkäykset ajoissa ja minimoimaan vahingot.

3.1.5 Itsekonfiguroituva ransomware-ehkäisymenetelmä

Itsekonfiguroituva ransomware-ehkäisymekanismi on menetelmä, joka on suunniteltu suojaamaan erityisesti IoMT-ympäristöjä ransomware-hyökkäyksiltä. Mekanismi hyödyntää automaatiota ja avoimen lähdekoodin työkaluja, kuten OpenSSL ja Cuckoo Sandbox. Mekanismin toimintaperiaate perustuu reaaliaikaiseen analyysiin ja poikkeavan käyttäytymisen tunnistamiseen. Esimerkkinä menetelmän soveltamisesta toimii Tizen-käyttöjärjestelmän content screening and reputation (CSR) -kehys, joka valvoo tiedostojen käyttöä ja tarkastaa tiedostopyynnöt kryptografisten työkalujen avulla. Järjestelmä rajoittaa pääsyä tiedostoihin ja järjestelmäresursseihin käyttäjäkohtaisesti sekä estää haitalliset tapahtumakutsut automaattisesti. Dynaamisen valvonnan ansiosta mekanismi pystyy havaitsemaan ja estämään ransomware-hyökkäykset jo varhaisessa vaiheessa, mikä parantaa erityisesti IoMT-ympäristöjen turvallisuutta. (Tariq ym., 2022.)

Itsekonfiguroituva ransomware-ehkäisymekanismi IoMT-ympäristöihin havaitsee ja estää staattiset ja dynaamiset hyökkäykset jopa 95 % tarkkuudella. Menetelmä on skaalautuva, automatisoitu ja kustannustehokas, sillä se hyödyntää avoimen lähdekoodin työkaluja, kuten Cuckoo Sandoxia, mikä pienentää aloitus- ja ylläpitokustannuksia. Se tarjoaa kattavan suojan IoMT-laitteille ja minimoi manuaalisen työn tarpeen. Rajoitteena on kuitenkin rajallinen testaus muihin kuin Tizen-pohjaisiin järjestelmiin sekä haasteet uusien ransomware-varianttien reaaliaikaisessa tunnistamisessa. (Tariq ym., 2022.) Mekanismi soveltuu erityisesti suurille yrityksille, joilla on laajoja IoT- tai IoMT-verkostoja, kuten terveysteknologian ja finanssialan toimijoille, joissa tietojen eheys ja käytettävyys ovat kriittisiä. Pienemmille yrityksille investointi voi olla kuitenkin tarpeettoman raskas.

3.1.6 Säännölliset varmuuskopiot

Säännölliset varmuuskopiot ovat keskeinen osa ransomware-hyökkäysten ennaltaehkäisyä ja niiden vaikutusten minimointia. Varmuuskopiot tarjoavat mahdollisuuden palauttaa menetetyt tiedot ilman, että organisaation täytyy maksaa lunnaita. Tehokas varmuuskopiointistrategia, kuten 3–2–1-malli, jossa säilytetään vähintään kolme kopiota tiedostoista ja yksi niistä offline-tilassa, voi vähentää merkittävästi hyökkäysten aiheuttamia vahinkoja. Varmuuskopioiden suojaaminen hyökkäyksiltä edellyttää verkon ulkopuolisten tallennusvälineiden käyttöä ja järjestelmällistä varmuuskopioiden hallintaa. (Luo & Liao, 2007; Al-Rimy ym., 2018.) Modernien kiristysohjelmien, kuten WannaCry, kyky saastuttaa myös online-varmuuskopiot korostaa offline-varmuuskopioiden merkitystä järjestelmien palauttamisessa (Zimba & Chishimba, 2019a).

Säännölliset varmuuskopiot ovat tärkeä menetelmä ransomware-hyökkäysten ennaltaehkäisyssä erityisesti yrityksille, joiden liiketoiminta riippuu vahvasti tiedon jatkuvasta saatavuudesta. Menetelmän vahvuuksiin kuuluu mahdollisuus palauttaa tiedot ilman lunnaita, mikä vähentää hyökkäysten taloudellisia vaikutuksia. Toisaalta heikkoutena on, että varmuuskopiot vaativat jatkuvaa hallintaa ja päivittämistä ollakseen tehokkaita. Myös hyökkääjät voivat pyrkiä kohdistamaan iskunsa varmuuskopioihin, mikä lisää offline-säilytyksen ja eristettyjen järjestelmien merkitystä. (Al-Rimy ym., 2018; Luo & Liao, 2007.) Menetelmä on pitkällä aikavälillä kustannustehokas estäen mahdollisia taloudellisia menetyksiä. Säännölliset varmuuskopiot soveltuvat parhaiten keskisuurille ja suurille yrityksille, jotka pystyvät investoimaan laadukkaisiin varmuuskopiointijärjestelmiin ja niiden hallintaan. Pienemmille organisaatioille ratkaisu voi olla haastavampi, mutta yksinkertaistetut mallit, kuten 3–2–1-strategia, voivat tarjota riittävän suojan. Kokonaisuutena varmuuskopiointi on suositeltava osa ransomwaren ennaltaehkäisyä ja monikerroksista tietoturvastrategiaa.

3.1.7 Tietoturvapäivitykset ja -korjaukset

Tietoturvapäivitykset ja -korjaukset ovat keskeinen keino ransomware-hyökkäysten ennaltaehkäisyssä. Päivitykset sulkevat tunnetut ohjelmistohaavoittuvuudet, joita hyökkääjät usein hyödyntävät. Esimerkiksi WannaCry-hyökkäyksessä käytettiin Microsoftin SMB-protokollan haavoittuvuutta, joka olisi voitu estää ajantasaisilla päivityksillä. Al-Rimyn ym., (2018) tutkimuksessa suositellaan erityisesti automaattisten päivitysten käyttöä, sillä ne vähentävät inhimillisten virheiden riskiä ja varmistavat, että järjestelmät pysyvät ajan tasalla. Päivitykset ovat erityisen tärkeitä liiketoimintakriittisten järjestelmien suojaamisessa. (Al-Rimy ym., 2018.)

Tietoturvapäivitykset ovat tehokas ja kustannustehokas keino ehkäistä ransomware-hyökkäyksiä, koska ne sulkevat hyökkäysten yleisiä väyliä, kuten ohjelmistohaavoittuvuuksia (Al-Rimy ym., 2018). Ne sopivat erityisesti yrityksille, joissa automaattiset päivitykset voivat vähentää hallinnollista taakkaa ja minimoida virheitä. Päivitykset eivät kuitenkaan suojaa nollapäivähaavoittuvuuksilta, eikä niitä voida pitää yksinään riittävänä turvakeinona (Al-Rimy ym., 2018). Lisäksi manuaaliset päivitykset vaativat resursseja, mikä voi olla haaste pienemmille organisaatioille.

3.1.8 Päätelaitteiden tunnistus- ja reagointi

Päätelaitteiden tunnistus- ja reagointimenetelmä (eng. endpoint detection and response, EDR) yhdistää päätelaitteiden jatkuvan seurannan, epäilyttävien toimintojen tunnistamisen ja automatisoidut reagointitoimenpiteet. EDR eroaa perinteisistä suojausteknologioista, kuten virustorjuntaohjelmista, kyvyllään tarjota syvällistä näkyvyyttä päätelaitteiden käyttäytymiseen ja analysoida reaaliaikaisesti uhkien toimintaa. EDR:n keskeinen ominaisuus on sen kyky tunnistaa epäilyttävät toiminnot reaaliajassa, kuten tiedostojen salausyritykset, joita ransomware-hyökkäyksissä tyypillisesti käytetään. Ransomware hyödyntää usein monimutkaisia ja innovatiivisia menetelmiä, kuten polymorfisia uhkia ja tiedostottomia hyökkäyksiä, jotka voivat jäädä perinteisiltä suojausjärjestelmiltä havaitsematta. EDR:n käyttäytymisanalyysiin ja koneoppimismalleihin perustuvat algoritmit voivat tunnistaa tällaiset poikkeamat ja merkitä ne haitallisiksi ennen kuin ne aiheuttavat laajempaa vahinkoa. (Cappello, 2024.)

Kun EDR-järjestelmä havaitsee ransomware-uhkaan viittaavia toimintoja, se voi toteuttaa automatisoituja toimenpiteitä, kuten tartunnan saaneen laitteen eristämisen verkosta hyökkäyksen leviämisen estämiseksi. Menetelmä keskeyttää haitallisen prosessin, kuten tiedostojen salaamisen, ennen kuin ne aiheuttavat merkittäviä vahinkoja. Menetelmä lähettää reaaliaikaiset ilmoitukset

tietoturvatiimille, jotta uhkaan voidaan reagoida nopeasti. EDR-järjestelmät analysoivat päätelaitteiden toimintaa hyödyntäen heuristiikkaa ja käyttäytymismalleja. Tämä mahdollistaa uhkien tunnistamisen, vaikka ne eivät vastaisi tunnettuja haittaohjelmien allekirjoituksia. Tämä lähestymistapa on tehokas myös kehittyneitä ja tuntemattomia uhkia vastaan. Sen tehokkuus riippuu kuitenkin järjestelmän oikeasti konfiguroinnista ja analyysimallien tarkkuudesta. Menetelmä ei ole yksittäinen ratkaisu, vaan se toimii tehokkaammin osana kokonaisvaltaista suojautumista. Integroimalla EDR muiden suojaustyökalujen kanssa organisaatiot voivat luoda monikerroksisen puolustuksen ransomwarea vastaan. (Cappello, 2024.)

3.1.9 Verkon segmentointi

Verkon segmentointi on ransomwaren ennaltaehkäisymenetelmä, joka keskittyy hyökkäyksen leviämisen rajoittamiseen organisaation sisällä. Segmentoinnissa verkko jaetaan pienempiin osiin eli segmentteihin, mikä rajoittaa hyökkääjän pääsyä kriittisiin resursseihin ja estää ransomwarea leviämästä vapaasti koko organisaatiossa. Tämä on tärkeää, sillä ransomware tyypillisesti leviää päälaitteesta palvelimelle, ja ilman segmentointia hyökkäys voi vaarantaa koko organisaation verkon. Segmentoitu verkko mahdollistaa sen, että eri osastot ja toiminnallisuudet ovat erillään toisistaan. Tämä hidastaa ransomware-hyökkäysten leviämistä ja antaa organisaatiolle aikaa ryhtyä vastatoimiin vähentäen syntyvää riskiä. Kriittiset laitteet ja sovellukset tulisi sijoittaa erillisiin verkkosegmentteihin, jotta niiden suojaus vahvistuu ja hyökkäyksen vaikutusalue pienenee. Segmentoinnilla voidaan estää ransomwarea leviämästä niihin verkon osiin, joihin sillä ei ole pääsyä, ja siten minimoida hyökkäyksen aiheuttamat vahingot. (Zhanhui & Rahman, 2017.)

Zimba ym., (2017) suosittelevat tutkimuksessaan kaskadimallista verkon segmentointia, jossa verkot jaetaan loogisiin osiin eri toimintojen ja suojaustarpeiden mukaan. Tuotantoverkkojen suojaamisen tulisi olla ensisijainen tavoite. Tämä voidaan saavuttaa hyödyntämällä demilitarisoituja vyöhykkeitä vähentämään verkkolaitteiden altistumista suorille hyökkäyksille julkisista verkoista. Tutkimuksen mukaan myös kriittisen infrastruktuurin turvallisuus tulisi priorisoida suhteessa muihin verkon osiin. Tämä tarkoittaa, että verkon segmentointia painotetaan kriittisillä alueilla, joilla tietojen saatavuus ja eheys ovat keskeisiä. Verkon segmentoinnin avulla voidaan vähentää ransomware-hyökkäysten onnistumisen todennäköisyyttä ja minimoida niiden vaikutusta kriittisiin järjestelmiin. Menetelmä on tärkeä järjestelmissä, joissa kriittinen infrastruktuuri on yhdistetty julkisiin verkkoihin. (Zimba ym., 2017.)

3.1.10 Monivaiheinen tunnistautuminen

Monivaiheinen tunnistautuminen (eng. multi-factor authentication, MFA) toimii ylimääräisenä suojakerroksena, joka vaatii käyttäjiä todistamaan henkilöllisyytensä useammalla kuin yhdellä tavalla, kuten salasanalla, biometrisellä tunnistuksella tai kertakäyttöisellä koodilla. Tämä vaikeuttaa luvattomien käyttäjien pääsyä järjestelmään, vaikka heillä olisi esimerkiksi salasana tiedossaan. Järjestelmä soveltaa tiukempia tunnistautumisvaatimuksia korkeampiriskisissä tilanteissa, kuten kriittisten tietojen käsittelyssä. MFA-järjestelmä integroi biometrisiä tunnistusmenetelmiä, kuten sormenjälki- tai kasvojentunnistusta. Näin varmistetaan, että tunnistautuminen perustuu yksilöllisiin fyysisiin ominaisuuksiin, joita on vaikea väärentää. MFA vähentää riskiä, että hyökkääjä voisi käyttää varastettuja tunnistustietoja päästäkseen järjestelmään ja levittääkseen ransomwarea. Tämä auttaa erityisesti suojaamaan järjestelmän kriittisiä osia, kuten pääkäyttäjätilejä ja arkaluonteisia tietoja. (Takeuchi ym., 2023.)

3.1.11 Kerrostettu suojaus

Kerrostettu suojaus on menetelmä, joka yhdistää useita erilaisia suojaustekniikoita ja -kerroksia hyökkäysten torjumiseksi. Sen keskeinen idea on, että yksittäiset suojatoimet eivät riitä kattavaan puolustukseen, mutta niiden yhdistäminen tarjoaa monipuolisen ja vahvemman suojan. Kerrostettu suojaus, tässä tapauksessa Shaukatin ym., (2018) kehittämä RansomWall -järjestelmä, joka suojaa organisaatioita crypto-ransomware-hyökkäyksiltä yhdistämällä staattisen ja dynaamisen analyysin, hunajatiedostot, koneoppimisen ja varmuuskopioinnin. Järjestelmä tunnistaa ransomwarelle tyypillisen käyttäytymisen, kuten tiedostojen salaamisen ja järjestelmän muokkausyritykset. Epäilyttävät prosessit havaitaan varhaisessa vaiheessa, ja niiden muuttamat tiedostot varmuuskopioidaan. Koneoppimismalli luokittelee prosessin haitalliseksi tai harmittomaksi. Jos prosessi todetaan haitalliseksi, tiedostot palautetaan ja prosessi keskeytetään. Menetelmä toimii myös nollapäivähyökkäysten tunnistamisessa ja tarjoaa reaaliaikaista suojaa. (Shaukat & Ribeiro, 2018.)

RansomWall -järjestelmä tunnistaa uhkia jo varhaisessa vaiheessa seuraamalla tiedostojärjestelmän toimintaa ja hyödyntämällä hunajatiedostoja haitallisen käytöksen havaitsemiseksi. Koneoppimismallit, kuten gradient tree boosting, tarjoavat korkean havaitsemistarkkuuden, ja tiedostojen reaaliaikainen varmuuskopiointi varmistaa tietojen palauttamisen hyökkäyksen jälkeen. Sen vahvuutena on monitasoinen lähestymistapa ja tehokkuus nollapäivähyökkäyksiä vastaan. Heikkouksina ovat järjestelmän monimutkaisuus, korkeat laskentatarpeet ja riippuvuus

oppimismallien päivittämisestä. (Shaukat & Ribeiro, 2018.) Vaikka kustannukset voivat olla korkeat, menetelmä on erityisen sopiva suurille ja keskisuurille yrityksille, jotka tarvitsevat kattavaa suojaa kriittisiä tietoja vastaan.

Raudin ym., (2021) tutkimus tukee kerrostetun suojauksen merkitystä osana järjestelmien monikerroksista tietoturvaa. Sisäisten käyttöliittymien diversifiointi nähdään proaktiivisena ohjelmistoturvallisuusmenetelmänä, jolla pyritään estämään haittaohjelmien hyödyntämästä käyttöjärjestelmän keskeisiä resursseja. Tämä toteutetaan muuttamalla käyttöjärjestelmän sisäisiä rajapintoja, kuten järjestelmäkutsuja, kirjastoja ja komentotulkkeja, uniikiksi niin, että vain luotetut ohjelmat voivat käyttää niitä. Diversifiointimenetelmät tarjoavat lisäturvaa yhdistettynä perinteisiin suojakeinoihin, kuten salaukseen ja tunkeutumisen havaitsemisjärjestelmiin. Menetelmä soveltuu erityisesti järjestelmiin, joissa koodimäärä on pieni ja päivityksiä tehdään harvemmin. Testien mukaan diversifioinnilla on vain minimaalinen vaikutus järjestelmien suorituskykyyn. Täysi automaatio ei ole aina mahdollinen, ja ongelmalliset tapaukset saattavat vaatia manuaalista puuttumista. Diversifioitujen rajapintojen ylläpito ja päivittäminen voivat olla haastavia erityisesti suurissa järjestelmissä. Sisäisten rajapintojen diversifiointi voi tehokkaasti lisätä järjestelmien kerrostettua tietoturvaa ja vaikeuttaa haittaohjelmien toimintaa. Näin se toimii osana kokonaisvaltaista tietoturvastrategiaa. (Rauti ym., 2021.)

3.2 Ei-tekniset ennaltaehkäisymenetelmät ja niiden tarkastelu yritysnäkökulmasta

Ransomware-hyökkäysten ennaltaehkäisyssä ei-tekniset toimenpiteet ovat tärkeä osa kokonaisvaltaista suojautumista. Lévesque ym., (2018) osoittavat, että haittaohjelmien menestyminen riippuu paitsi teknologisesta suojauksesta myös käyttäjien toimista ja asenteista. Ransomware-hyökkäyksissä käytetyt taktiikat, kuten sähköpostien houkuttelevat otsikot, perustuvat vahvasti sosiaaliseen manipulointiin ja hyödyntävät kiireellisyyden tunnetta tai auktoriteettia (Ferreira, 2018). Lévesquen ym., (2018) tutkimuksen mukaan jopa parhaat turvamekanismit voivat epäonnistua, jos käyttäjät eivät tunnista riskejä tai toimivat huolimattomasti. Siksi tehokas ennaltaehkäisy edellyttää teknisten toimenpiteiden lisäksi käyttäjien koulutusta ja tietoisuuden lisäämistä inhimillisten virheiden minimoimiseksi.

Menetelmä	**Vahvuudet**	**Heikkoudet**	**Kustannus-tehokkuus**	**Soveltuvuus yritysympäristössä**	**Lähteet**

Käyttäjä-koulutus ja tietoisuuden lisääminen	Vähentää inhimillisiä virheitä; kasvattaa valmiuksia	Työntekijöiden motivaatio ja tiedon unohtaminen	Pitkällä aikavälillä kustannustehokas	Soveltuu kaikille organisaatioille, erityisesti räätälöitynä	(Ibrahim & Ade, 2023) (Lika ym., 2018) (Mcintosh, ym 2021)
Tietoturva-politiikat ja -prosessit	Yhtenäistää toimintatapoja ja vähentää virheitä	Riippuvainen henkilöstön sitoutumisesta	Kustannustehokas dokumentoinnin ja koulutuksen jälkeen	Erityisesti suurille ja keskisuurille organisaatioille	(Luo & Liao, 2007)
Turvallisuus-kulttuurin kehittäminen	Parantaa reaktio- ja tunnistuskykyä; sitouttaa työntekijöitä	Haastava kehittää ja ylläpitää pitkällä aikavälillä	Pitkällä aikavälillä kustannustehokas	Soveltuu kaikenkokoisille organisaatioille	(Ibrahim & Ade, 2023)

Taulukko 2 Ei-tekniset ennaltaehkäisymenetelmät

3.2.1 Käyttäjäkoulutus ja tietoisuuden lisääminen

Käyttäjäkoulutus ja tietoisuuden lisääminen ovat järjestelmällisiä prosesseja, joissa työntekijöille tarjotaan tietoa kyberturvallisuuden riskeistä, tässä tapauksessa erityisesti kiristysohjelmahyökkäyksistä, sekä keinoista tunnistaa ja välttää näitä uhkia. Koulutus voi sisältää esimerkiksi työpajoja, simulaatioita, e-oppimista ja roolikohtaista opetusta. Tavoitteena on varmistaa työntekijät tarvittavilla tiedoilla, kuten phishing-viestien tunnistamisella. Hyvä koulutusohjelma sisältää jatkuvia päivityksiä ja toistuvaa harjoittelua, jotta tiedot pysyvät ajan tasalla ja työntekijöiden tietoisuus säilyy läpi uudistusten. (Ibrahim & Ade, 2023.)

Bekkers ym., (2023) korostavat käyttäjäkoulutuksen merkitystä ransomware-hyökkäysten ennaltaehkäisyssä, erityisesti yrittäjien näkökulmasta. Tutkimuksen mukaan tietoisuuden lisääminen auttaa yrittäjiä paremmin arvioimaan organisaatioidensa haavoittuvuuksia ja motivoi ryhtymään ennaltaehkäiseviin toimiin. Tietoisuuden lisäämisessä ei ole kyse vain uhkien tunnistamisesta, vaan myös kyvystä ymmärtää ja toteuttaa tehokkaita suojaustoimenpiteitä. Yrittäjät saattavat usein yliarvioida nykyisten suojausmenetelmien tehokkuuden, mikä voi johtaa uhkien aliarvioimiseen. Tämä korostaa realistisen ja jatkuvan koulutuksen merkitystä. Lisäksi tunneperäiset tekijät, kuten huoli organisaation turvallisuudesta, voivat lisätä osallistumismotivaatiota ja tukea ennaltaehkäisevien toimenpiteiden käyttöönottoa. (Bekkers ym., 2023.)

Lika ym., (2018) korostavat käyttäjäkoulutuksen kehittämistä hyödyntämällä pelillistämistä tietoisuuden lisäämiseen ransomware-hyökkäyksistä. Pelillistämisen avulla oppiminen voidaan tehdä vuorovaikutteisemmaksi ja sitouttavammaksi, mikä voi puolestaan parantaa työntekijöiden motivaatiota ja oppimistuloksia. Heidän tutkimuksessaan ei tarjota yksityiskohtaista ratkaisua kiristysohjelmatartuntojen ehkäisyyn tai havaitsemiseen, jonka lisäksi he vahvistavat ”perfc”-tiedoston tehokkuuden vain NotPetya-kiristysohjelman torjumisessa. Pelillistämisen hyödyntäminen voi lisätä oppimisen mielekkyyttä ja tukea tietoisuuden kasvattamista, mutta sen tehokkuus riippuu toteutuksen laadusta ja siitä, kuinka hyvin työntekijät sitoutuvat ohjelmaan. (Lika ym., 2018.)

Käyttäjäkoulutuksen vahvuuksiin kuuluu sen kyky vähentää inhimillisiä virheitä ja kasvattaa työntekijöiden valmiuksia torjua kiristysohjelmia. Se myös edistää organisaation turvallisuuskulttuuria ja parantaa tietoisuuttaa uusista uhkista. Heikkouksiin kuuluu kuitenkin työntekijöiden mahdollinen motivaation puute koulutuksia kohtaan, tiedon unohtaminen ajan myötä sekä koulutuksen säännöllisen päivittämisen tarve. (Ibrahim & Ade, 2023.) Koulutus on kustannustehokas pitkällä aikavälillä, mutta vaatii aluksi investointeja ohjelmien kehittämiseen ja ylläpitoon. Yritysympäristössä menetelmä on soveltuva kaikille organisaatioille, etenkin jos sisältö räätälöidään työntekijöiden roolien mukaisesti.

3.2.2 Tietoturvapolitiikat

Tietoturvapolitiikat ja ohjeet muodostavat keskeisen osan organisaation tietoturvastrategiaa. Ne sisältävät yksityiskohtaisia sääntöjä ja käytäntöjä, joilla pyritään suojaamaan yrityksen tietoja ja järjestelmiä ulkoisilta ja sisäisiltä uhkilta. Tietoturvapolitiikat voivat ohjeistaa esimerkiksi järjestelmien säännöllisistä päivityksistä, tietojen varmuuskopiointikäytännöistä ja työntekijöiden koulutuksesta tietoturvauhkiin liittyen. Ohjeet tarjoavat myös selkeät toimintamallit mahdollisten tietoturvaloukkausten varalta, kuten raportointiprosessit ja järjestelmäeristämiskäytännöt. Tavoitteena on yhtenäistää työntekijöiden toimintatapoja ja vähentää inhimillisten virheiden riskiä. (Luo & Liao, 2007.)

Menetelmä on kustannustehokas, sillä sen toteuttaminen vaatii lähinnä resursseja dokumentointiin ja henkilöstön kouluttamiseen. Toisaalta menetelmän heikkous on sen riippuvuus henkilöstön sitoutumisesta, reaaliaikaisesta kehittämisestä ja jatkuvasta koulutuksesta. Jos ohjeita ei noudata tai niitä ei päivitetä, niiden tehokkuus voi heikentyä merkittävästi. Yritysympäristössä menetelmä on soveltuva erityisesti suurille ja keskisuurille organisaatioille, joilla on riittävät resurssit implementointiin ja valvontaan. (Luo & Liao, 2007.)

3.2.3 Turvallisuuskulttuuri

Työntekijöiden tietoisuuden lisäämisen ei tarvitse rajoittua vain uhkien tunnistamiseen, vaan siihen kuuluu myös oikeanlaisten turvallisuuskäytäntöjen omaksuminen. Esimerkkinä yksi tärkeistä suosituksista on, että organisaatiot sisällyttävät turvallisuuskulttuurin luomisen ja toteuttamisen osaksi päivittäistä työtä. Koulutuksen tulisi keskittyä paitsi uhkien tunnistamiseen, myös siihen, miten työntekijät voivat toimia, jos he epäilevät jotakin tai huomaavat epäilyttävää toimintaa. Koulutuksen ja tietoisuuden lisäämisen rinnalla on myös tärkeää, että organisaatiot luovat ympäristön, jossa kyberturvallisuus on kaikkien vastuulla. Tämä tarkoittaa, että työntekijöiden on tiedettävä, että heidän toimillaan on suuri vaikutus organisaation tietoturvatasoon, ja heitä tulee kannustaa aktiivisesti raportointiin ja epäilyttävän toiminnan tarkasteluun. (Ibrahim, Ade 2023.)

Organisaatioiden omaksuma turvallisuuskulttuuri vahvistaa työntekijöiden valmiuksia havaita ja estää uhkia. Sitouttamalla kaikki organisaation jäsenet yhteiseen tavoitteeseen turvallisuuskulttuuri auttaa torjumaan inhimillisiä virheitä, jotka ovat merkittävä tekijä ransomware-hyökkäysten onnistumisessa. Turvallisuuskulttuurin tuomat käytännöt, kuten aktiivinen raportointi ja turvallisuuskäytäntöjen omaksuminen, parantavat organisaation kykyä reagoida uhkiin. Menetelmä korostaa työntekijöiden aktiivista osallistumista kyberturvallisuuden etulinjassa, mikä parantaa organisaatioiden valmiuksia. Haasteena turvallisuuskulttuurin luomisessa voi kuitenkin olla työntekijöiden motivoinnin ja sitouttamisen vaikeus. Lisäksi kulttuurin kehittäminen vaatii aluksi investointeja koulutukseen ja käytäntöjen jalkauttamiseen, vaikka se onkin pitkällä aikavälillä kustannustehokas. Myös tiedon unohtaminen on riski, sillä koulutuksen ja tietoisuuden vaikutukset voivat heikentyä ajan myötä, ellei turvallisuuskulttuuria jatkuvasti ylläpidetä ja päivitetä. (Ibrahim & Ade, 2023.)

4 Yhteenveto ja johtopäätökset

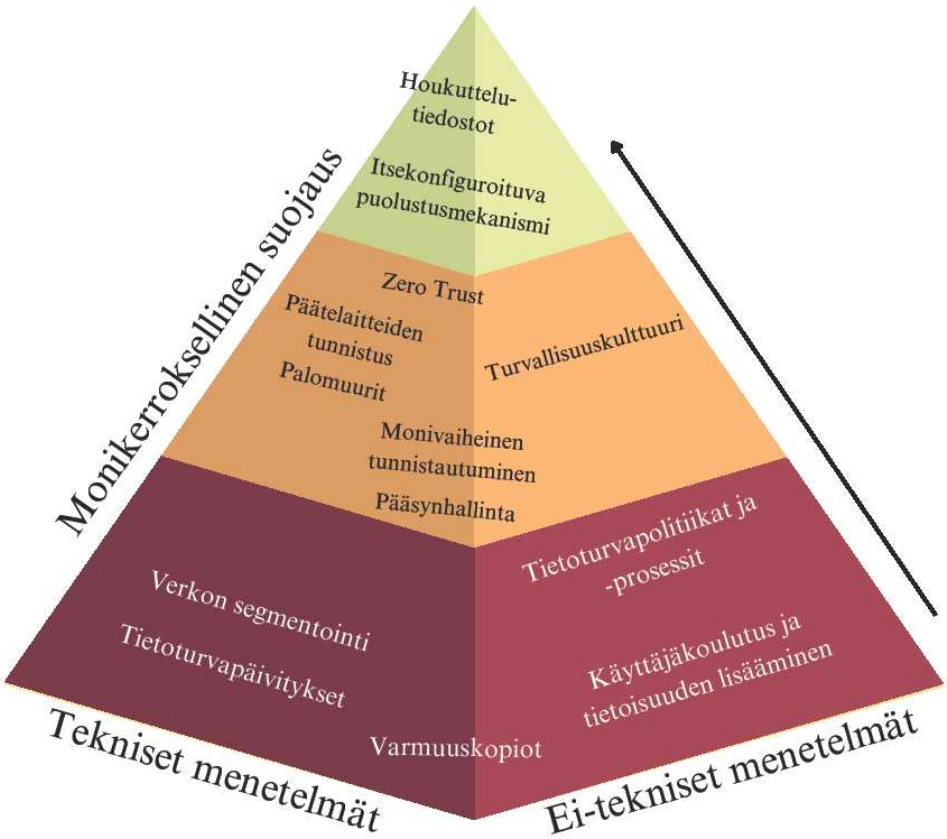
Tämä kandidaatintutkielma tarjoaa kattavan tarkastelun ransomware-hyökkäysten ennaltaehkäisyyn, painottaen teknisten ja ei-teknisten menetelmien yhdistämisen merkitystä sekä kokonaisvaltaista suojautumista. Ransomware-hyökkäykset ovat monimuotoistuneet ja sisältävät nykyisin enemmän hybridimalleja, jotka yhdistelevät useampia eri hyökkäystekniikoita, mikä vaikeuttaa hyökkäysten havaitsemista ja ennaltaehkäisyä perinteisin menetelmin. Hyökkääjät mukautuvat uusiin puolustustekniikoihin ja kehittävät entistä monimutkaisempia hyökkäysstrategioita. Tämä edellyttää yrityksiltä ja organisaatioilta ennakoivaa lähestymistapaa, jossa uhkiin varaudutaan ennaltaehkäisevin toimenpitein ja suojaukset päivitetään reaaliaikaisesti. Mcintosh ym., (2021) painottavat tutkimuksessaan, ettei yksittäisiin menetelmiin keskittyvät strategiat ole riittäviä. Ransomware-uhkien torjunta vaatii teknisten ja ei-teknisten menetelmien yhdistämistä, jotka yhdessä vastaavat organisaation kykyä estää hyökkäyksiä.

Datan eksfiltraation yleistyminen on muuttanut myös organisaatioiden tarpeita kyberturvallisuuden osalta. Perinteiset varmuuskopiointimenetelmät, jotka ovat tehokkaita pelkän salauksen torjumiseen, eivät yksinään riitä. Organisaatioiden on nyt keskityttävä myös esimerkiksi datan suojaamiseen ja tiedonhallintaan, jotta tiedot eivät päädy hyökkääjien käsiin. Tämä sisältää muun muassa tietoliikenteen tarkkailun, tietojen salaamisen myös niiden ollessa siirrettävissä, pääsynhallinnan tiukentamisen sekä käyttäjien koulutuksen. (Mcintosh ym., 2024.) Kiristysohjelmien torjunnan tulisi olla osa organisaation laajempaa kyberturvallisuuden riskienhallintaa, joka sisältää teknologian, prosessien ja ihmisten yhteistyön (Mcintosh ym., 2021).

Organisaation sisällä on tärkeää määritellä selkeästi vastuualueet. Ransomware-hyökkäysten ennaltaehkäisyssä organisaation IT-osasto vastaa teknisistä toimenpiteistä, kuten ohjelmistopäivityksistä, verkon segmentoinnista ja varmuuskopioiden hallinnasta. Johto huolehtii resurssien ja koulutusten järjestämisestä sekä tietoturvakulttuurin vahvistamisesta. Henkilöstön vastuulla on tunnistaa esimerkiksi phishing-yritykset ja toimia ensimmäisenä puolustuslinjana. (Christopher, 2023.) Raj ym., (2024) esittävät kolmitasoisen lähestymistavan modernien ransomware-mallien torjuntaan, jossa politiikka-, verkko- ja käyttäjätason toimenpiteet täydentävät toisiaan. Politiikkatasolla organisaation johto vastaa tietoturvapolitiikkojen laatimisesta ja toimeenpanosta, kuten tietoturvakoulutusten järjestämisestä ja järjestelmien säännöllisestä koventamisesta. Johdon tehtävänä on myös varmistaa, että organisaation tietoturvakäytännöt kattavat kaikki keskeiset osa-alueet. Verkkotasolla IT-tiimi vastaa teknisistä toimenpiteistä, kuten verkon segmentoinnista ja pääsynhallinnasta. Resurssirajoitteiset organisaatiot voivat ulkoistaa

nämä toiminnot kolmannen osapuolen tarjoajille. Käyttäjätasolla jokaisen työntekijän rooli on tärkeä ja työntekijöiden koulutus ransomware-uhkien tunnistamisessa on keskeistä. Johto vastaa siitä, että raportointikäytännöt ovat selkeitä ja henkilöstö tietoinen toimintatavoista. (Raj ym., 2024.)

4.1 Ohjeistus yrityksille ransomware-hyökkäysten ennaltaehkäisyyn



Kuva 2 Monikerroksellinen suojaus ransomwarea vastaan

Kuvion 2 pyramidi kuvaa monikerroksista suojausmallia, jossa yhdistetään tekniset ja ei-tekniset menetelmät ransomware-hyökkäysten ennaltaehkäisemiseksi. Pyramidin alin taso on kriittisin muodostaen suojauksen perustan. Ylemmät tasot puolestaan laajentavat ja vahvistavat suojausta tuomalla mukaan kehittyneempiä menetelmiä. Pohjatasolla painopiste on perusmenetelmissä, jotka ovat kriittisiä hyökkäysten estämiseksi ja niiden vaikutusten minimoimiseksi. Tähän tasoon kuuluvat esimerkiksi varmuuskopiointi, tietoturvapäivitykset, käyttäjäkoulutus ja tietoturvapolitiikat (Pagán & Khaled, 2021). Tekniset menetelmät, kuten varmuuskopiot, verkon segmentointi ja päivitysten hallinta, muodostavat perustan ransomware-hyökkäysten estämiselle, kun taas ei-tekniset menetelmät, kuten turvallisuustietoisuuden koulutus ja tietoturvapolitiikat, vähentävät

ihmisten aiheuttamia tietoturvapoikkeamia (Seng ym., 2024). Keskimmäinen taso vahvistaa suojaa lisäämällä edistyneempiä menetelmiä, kuten palomuurit, päätelaitteiden suojauksen ja Zero Trust -arkkitehtuurin. Ei-tekniset menetelmät, kuten turvallisuuskulttuurin edistäminen, varmistavat, että tietoturva integroituu osaksi organisaation päivittäistä toimintaa ja päätöksentekoa. Pyramidin huipulla ovat kehittyneimmät menetelmät, kuten houkuttelutiedostot, jotka täydentävät alempia tasoja ja lisäävät suojan kattavuutta.

Ransomwaren ennaltaehkäisyyn tarvitaan toisiaan täydentäviä kerroksia, jotka tarjoavat suojan useammilla tasoilla. Kerrokset täydentävät toisiaan, ja koko järjestelmä muodostaa kattavan ja tehokkaan suojauksen ransomware-hyökkäyksiä vastaan. Kerrosten avulla hyökkäykset voidaan pysäyttää eri vaiheissa, ja jos ne onnistuvat, varmuuskopiointi mahdollistaa nopean palautumisen. Tämä lähestymistapa painottaa, että yksittäinen menetelmä ei riitä, vaan tarvitaan kokonaisvaltainen ja kerroksellinen strategia. (Pagán & Khaled, 2021.) Pyramidin (kuvio 2) rakenne havainnollistaa, että tehokas suojautuminen ransomware-hyökkäyksiä vastaan edellyttää eri menetelmien yhdistämistä. Tekniset ja ei-tekniset menetelmät tukevat ja täydentävät toisiaan, muodostaen kattavan puolustusstrategian. Pyramidin alin taso tarjoaa kriittisen perustan suojaukselle, kun taas ylemmät tasot lisäävät resilienssiä ja laajentavat puolustuskykyä.

Alla on esitetty käytännön ohjeistus yrityksille ransomware-hyökkäysten tehokkaaseen ennaltaehkäisyyn:

1. **Kriittisen tason teknisten menetelmien käyttöönotto**

    - **Varmuuskopiot**: Ota käyttöön säännöllinen ja automatisoitu varmuuskopiointijärjestelmä, joka tallentaa kriittiset tiedot myös offline-tilassa. Testaa varmuuskopioiden palauttamista säännöllisesti ja säilytä useita kopioita eri sijainneissa.

    - **Tietoturvapäivitykset**: Ota käyttöön automatisoitu päivitystenhallinta, joka varmistaa, että käyttöjärjestelmät, ohjelmistot ja laitteistot pysyvät ajan tasalla. Suorita säännöllisiä tietoturvaskannauksia, jotta haavoittuvuudet havaitaan ja korjataan nopeasti.

    - **Verkon segmentointi**: Jaa verkko pienempiin aliverkkoihin, jolloin pääsy kriittisiin järjestelmiin ja tietoihin on rajattu vain tarpeellisille käyttäjille ja palveluille. Käytä esimerkiksi palomuureja ja vahvoja käyttäjäkontrolleja estämään haittaohjelmien liikkuminen verkon sisällä.

2. **Kriittisen tason ei-teknisten menetelmien käyttöönotto**

- **Käyttäjäkoulutus**: Järjestä säännöllisiä koulutuksia henkilöstön tietoturvataitojen parantamiseksi. Korosta turvallisia käytäntöjä, kuten phishing-viestien tunnistamista.
- **Tietoturvapolitiikat**: Laadi selkeät tietoturvapolitiikat, jotka kattavat käyttöoikeuksien hallinnan ja toimintaohjeet ransomware-uhkien varalta. Päivitä politiikat säännöllisesti ja varmista niiden noudattaminen esimerkiksi auditointien ja seurannan avulla.

3. **Lisämenetelmien käyttöönotto**

- Hyödynnä organisaation resursseihin ja tarpeisiin sopivia lisämenetelmiä pyramidin (kuvio 2) ylemmiltä tasoilta, kuten pääsynhallintaa, päätelaitteiden suojausta, monivaiheista tunnistautumista, Zero Trust -arkkitehtuuria ja turvallisuuskulttuurin kehittämistä. Räätälöi tietoturvaratkaisut organisaation riskienhallintasuunnitelman ja kriittisten toimintojen mukaisesti.

Ransomware-hyökkäysten torjunnassa organisaation kyky sietää, hallita ja palautua hyökkäyksistä on keskeisessä asemassa. Tässä tutkielmassa tarkastellut ennaltaehkäisymenetelmät tukevat tätä tavoitetta monitasoisen puolustuksen, proaktiivisten toimintatapojen ja nopean palautumiskyvyn kannalta. Monitasoinen puolustus, kuten pääsynhallinnan, varmuuskopioiden ja käyttäjäkoulutuksen yhdistäminen, luo kattavan suojan ja vähentää hyökkäysten vaikutuksia. Proaktiiviset toimet, kuten tietoturvapäivitykset ja turvallisuuskulttuurin kehittäminen, vahvistavat organisaation kykyä tunnistaa ja estää uhkia ennen niiden toteutumista. Lisäksi palautumiskyky, erityisesti offline-varmuuskopioiden avulla, mahdollistaa kriittisten tietojen palauttamisen ilman lunnaiden maksamista. Resilienssin kehittäminen on olennainen osa ransomware-hyökkäysten ehkäisyä ja hallintaa. Se vaatii teknologisten ratkaisujen ja inhimillisten tekijöiden yhdistämistä sekä jatkuvaa sopeutumista ransomware-uhkien kehittymiseen.

4.2 Työn rajoitukset ja suuntaukset tulevaisuuden tutkimukselle

Tutkimus pohjautuu akateemisesta kirjallisuudesta löytyviin ransomware-uhkien ennaltaehkäisymenetelmiin, mikä tarjoaa kattavan teoreettisen näkökulman, mutta ei välttämättä heijasta kaikkia käytännön liiketoimintaympäristössä esiintyviä haasteita. Monien teknisten ja ei-teknisten menetelmien tehokkuutta on vaikea verrata suoraan, koska tutkimukset käsittelevät niitä eri näkökulmista ja erilaisissa ympäristöissä. Lisäksi tutkimusten menetelmät ja mittarit vaihtelevat, mikä rajoittaa tulosten keskinäistä vertailtavuutta. Monet tutkimukset käyttävät vanhentuneita oletuksia, vanhoja tai tarkastamattomia näytteitä ja keskittyvät liikaa crypto-ransomwaren

salausmekanismeihin (Mcintosh ym., 2024). Kyberturvallisuuden ja ransomware-uhkien nopeasti muuttuva luonne voi tehdä joistakin tämän tutkimuksen havainnoista vanhentuneita tulevaisuudessa. Esimerkiksi uusien hyökkäystekniikoiden tai kehittyneempien suojausmekanismien ilmaantuminen voi vaikuttaa suositeltujen menetelmien relevanssiin. Tutkimus ei myöskään ota riittävästi huomioon organisaatioiden resursseja, kuten budjettia, teknologista osaamista tai henkilöstökapasiteettia. Tämä voi rajoittaa joidenkin menetelmien soveltuvuutta.

Tulevaisuuden tutkimuksessa olisi tärkeää keskittyä hybridimenetelmien tarkasteluun. Näin voidaan luoda entistä tehokkaampia ja mukautuvampia ratkaisuja ransomware-hyökkäysten ennaltaehkäisyyn. Yhdistämällä teknologiset innovaatiot ja inhimilliset lähestymistavat organisaatiot voivat rakentaa kattavia ja kestäviä suojarakenteita tämän jatkuvasti kehittyvän uhan torjumiseksi. Mclintoshin ym., (2024) tutkimuksen mukaan tulevaisuuden tutkimuksen tulisi siirtää painopisteensä crypto-ransomwaren salauksesta data eksfiltraation tarkasteluun ja keskittyä kehittämään ratkaisuja, jotka ovat paremmin sovellettavissa liiketoimintaympäristössä. Olisi hyödyllistä keskittyä menetelmien käytännön toteutukseen organisaatioissa, analysoida kustannushyötysuhteita eri kokoisille yrityksille ja tehdä empiiristä tutkimusta, jotka täydentävät akateemista lähestymistapaa. Tämä lisäisi tutkimuksen yleistettävyyttä ja auttaisi organisaatioita tekemään paremmin informoituja päätöksiä ransomwaren kehittyvässä uhkakentässä.

Lähteet

Adahman, Z., Malik, A. W., & Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational securit*y. Computers & Security, Vol 122(102911).* https://www.sciencedirect.com/science/article/pii/S0167404822003042

Ahn, G., Jang, J., Choi, S., & Shin, D. (2024). Research on Improving Cyber Resilience by Integrating the Zero Trust Security Model With the MITRE ATT&CK Matrix. *IEEE Access*, Vol *12*, 89291–89309. https://doi.org/10.1109/ACCESS.2024.3417182

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 and Security*, Vol *74*, 144–166. https://doi.org/10.1016/j.cose.2018.01.001

Alshaikh, H., Ramadan, N., Hefny, H. A. (2020). Ransomware Prevention and Mitigation Techniques. *International Journal of Computer Applications*, Vol 177(40), 31-39.

Alwashali, A. A. M. A., Rahman, N. A. A., & Ismail, N. (2021). A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack. *2021 14th International Conference on Developments in eSystems Engineering (DeSE)*, 92–96. https://doi.org/10.1109/DeSE54285.2021.9719456

Ami, O., Elovici, Y., & Hendler, D. (2018). Ransomware prevention using application authentication-based file access control. *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 1610-1619. https://dl.acm.org/doi/abs/10.1145/3167132.3167304

Anghel, M., & Racautanu, A. (2019). A note on different types of ransomware attacks. *IACR Cryptology ePrint Archieve* (No. 2019/605). https://eprint.iacr.org/2019/605

Beaman, C., Barkworth, A., Akade, T. D., Hakak, S., Khan, . K. (2021) Ransomware Recent advances, analysis, challenges and future research directions. *Computers & Security*, Vol 111(2021), 102490. DOI: https://doi.org/10.1016/j.cose.2021.102490

Bekkers, L., Goede, S. V. H., Huurne, E. M., Houten, Y. V., Spithoven, R., Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protections motivation theory model. *Computers & Security,* Vol 127(2023), 103099. DOI: https://doi.org/10.1016/j.cose.2023.103099

Cappello, M. (2024). A comprehensive analysis of EDR (Endpoint Detection & Response), EPP (Endpoint Protection Platform), and antivirus security technologies. *Master Thesis.* DOI: http://dx.doi.org/10.26267/unipi_dione/4173

Chen, Q., & Bridges, R. A. (2017). Automated Behavioral Analysis of Malware: A Case Study of Wannacry Ransomware. *IEEE International Conference on Machine Learning and Applications 2017*, Vol 16. https://doi.org/10.1109/ICMLA.2017.0-119

Christopher, J. (2023) Building Ransomware Resilience: Proactive Prevention and Effective Response Frameworks for Organizations. *Revista De Inteligencia Artificial en Medicina,* Vol 14(1).

Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, Vol *6*(1). https://doi.org/10.1093/cybsec/tyaa023

Djenna, A., Belaoued, M., & Lifa, N. (2024). Top Cyber Threats: The Rise of Ransomware. *Information Security Theory and Practice*, Vol *14625*, 80–95. https://doi.org/10.1007/978-3-031-60391-4_6

Ferreira, A. (2018) Why Ransomware Needs A Human Touch. 2018 International Carnahan Conference on Security Technology (ICCST). 10.1109/CCST.2018.8585650

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, Vol *22*(1), 105–117. https://doi.org/10.1016/j.eij.2020.05.003

Ibrahim, A., & Ade, M. (2023). Impact of Employee Awareness Programs on Ransomware Prevention.

Kim, D. Y., Lee, J. (2020). Blacklist vs. Whitelist-Based Ransomware Solutions. *IEEE Consumer Electronics Magazin*e, Vol 9(3), 22-28. DOI: https://doi.org/10.1109/MCE.2019.2956192

Kindervag, J. (2010). *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*. Forrester Research

Kovács, A. M. (2024). Ransomware: A comprehensive study of the exponentially increasing cybersecurity threat. *Insights into Regional Development,* Vol 4(2), 96-104. https://doi.org/10.9770/IRD.2022.4.2(8)

Lévesque, F. L., Chiasson, S., Somayaji, A. & Fernandez, J. M. (2018) Technological and Human Factors of Malware Attacks: A Computer Security Clinical Trial Approach. *ACM Transactions on Privacy and Security (TOPS),* Vol 21(4), 1-30. https://dl.acm.org/doi/10.1145/3210311

Lika, R. A., Murugiah, D., Brohi, S. N., Ramasamy, D. (2018) NotPetya: Cyber Attack Prevention through Awareness via Gamification. *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*. 2018:1-6. DOI: https://doi.org/10.1109/ICSCEE.2018.8538431

Lin, Y. S., & Lee, C. F. (2023) Ransomware Detection and Prevention through Strategically Hidden Decoy File. *International Journal of Network Security,* Vol 35(2), 212-220. DOI: 10.6633/IJNS.202303 25(2).04

Luo, X., & Liao, Q. (2007). Awareness Education as the Key to Ransomware Prevention. *Information Systems Security*, Vol *16*(4), 195–202. https://doi.org/10.1080/10658980701576412

Mcintosh, T., Kayes, A. S. M., Chen, Y. P. P., NG, A. (2021) Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. *ACM Computer Service*, Vol 54(9) Article 197. DOI: https://doi.org/10.1145/3479393

Mcintosh, T., Susnjak, T., Liu, T., Xu, D., Watters, P., Liu, D., Hao, Y., Ng, A., Halgamuge, M. (2024) Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration. *ACM Computer Survey*, Vol 57(18). DOI: https://doi.org/10.1145/3691340

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science,* Vol 8(5), 1938-1940.

Muniandy, M., Ismail, N. A., Al-Nahari, A. Y. Y., Yao, D. N. L. (2024) Evolution and Impact of Ransomware: Patterns, Prevention, and Recommendations for Organizational Resilience. *International Academic Research in Business & Social Science*s, Vol 14(1), 585-599. DOI:10.6007/IJARBSS/v14-i1/19803

Nadir, I., & Bakhshi, T. (2018). Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques. *IEEE* 2018, 1–7. https://doi.org/10.1109/ICOMET.2018.8346329

Nguyen, D. D. A., Alain, P., Autrel, F., Bouabdallah, A., François, J., & Doyen, G. (2024). How Fast Does Malware Leveraging EternalBlue Propagate? The case of WannaCry and NotPetya. *2024 IEEE 10th International Conference on Network Softwarization (NetSoft)*, 399–404. https://doi.org/10.1109/NetSoft60951.2024.10588886

Pagán, A. J., & Khaled, E. (2021) A Multi-Layered Defense Approach to Safeguard Against Ransomware. *2021 IEEE 11th Annual Computing and Communications Workshop and Conference (CCWC)*. DOI: http://dx.doi.org/10.1109/CCWC51732.2021.9375988

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity*, Vol *5*(1), 1–11. https://doi.org/10.1093/cybsec/tyz003

Parkinson, S. (2017). Use of access control to minimise ransomware impact. *Network Security*, Vol 2017(7), 5-8. DOI: https://doi.org/10.1016/S1353-4858(17)30069-7

Prasad, K. P., & Kumar, P. (2024). A Systematic Study on Ransomware Attack: Types, Phases and Recent Variants. *2024 5th International Conference on Intelligent Communication*

Technologies and Virtual Mobile Networks (ICICV), 661–668. https://doi.org/10.1109/ICICV62344.2024.00110

Raj, A., Narayan, V., Muskan, V., Sani, A., Sharma, P., Sarma, S. S. (2024) Modern ransomware: Evolution, methodology, attack model, prevention and mitigation using multi-tiered approach. *Security and Privacy,* Vol 7(6). DOI: https://doi.org/10.1002/spy2.436

Rauti, S., Laurén, S., Mäki, P., Uitto, J., Laato, S., Leppänen, V. (2021) Internal interface diverdification as a method against malware. *Journal of Cyber Security Technology,* Vol 5(1), 15-40. DOI: https://doi.org/10.1080/23742917.2020.1813397

Sakib, S., Raiaan, M. A. K., Fahad, N. M., Mukta, M. S. H., Al Mamun, A., & Chowdhury, S. (2023). A Review of the Evaluation of Ransomware: Human Error or Technical Failure? *2023 International Conference on Information and Communication Technology for Sustainable Development.* 393–397. https://doi.org/10.1109/ICICT4SD59951.2023.10303580

Shaukat, S. K., & Ribeiro, V. J. (2018). RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning. *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*, 356–363. https://doi.org/10.1109/COMSNETS.2018.8328219

Silva, J. A H., López, L. I. B., Caraguay, Á. L. V., Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks - Detection and Prevention Parameters. *Remote Sensing*, Vol 11(10), 1168. DOI: http://dx.doi.org/10.3390/rs11101168

Tailor, J. P., Patel, A. D. (2017). A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control. *International Journal of Research and Scientific Innovation (IJRSI)*, Vol IV(VIS), 2321-2705.

Takeuchi, K., Kumamoto, T., Yoshida, Y., Fujima, H. (2023) Decentralized Identity Verification System for Data Access to Prevent Data Exfiltration Ransomware. *Journal of Preprints*. DOI: 10.36227/techrxiv.24732729.v1

Tariq, U., Ullah, I., Yousuf Uddin, M., & Kwon, S. J. (2022). An Effective Self-Configurable Ransomware Prevention Technique for IoMT. *Sensors*, Vol *22*(21), 8516. https://doi.org/10.3390/s22218516

Teichmann, F. M., & Boticiu, S. R. (2024). The most impactful ransomware attacks in 2023 and their business implications. *International Cybersecurity Law Review*, Vol *5*(2), 301–311. https://doi.org/10.1365/s43439-024-00115-3

Wang, Z., Cui, X., Su, S., Giu, J., Liu, C., Tian, Z. (2018). Automatically Traceback RDP-Based Targeted Ransomware Attacks. *Wireless Communications and Mobile Computing,* 2018:1-13.

Zhanhui, L., Rahman, N. A. A. (2017) A Review on Ransomware Trend of Attacks and Prevention. International Journal of Applied Engineering Research ISSSN, Vol 12(16), 6201-6210). DOI: http://www.ripublication.com

Zimba, A., & Chishimba, M. (2019a). On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. *European Journal for Security Research*, Vol *4*(1), 3–31. https://doi.org/10.1007/s41125-019-00039-8

Zimba, A., & Chishimba, M. (2019b). Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures. *International Journal of Computer Network and Information Security*, Vol *11*(1), 26–39. https://doi.org/10.5815/ijcnis.2019.01.03

Zimba, A., Wang, Z., Chen, H. (2017). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express,* Vol 4(2018), 14-18. DOI: https://doi.org/10.1016/j.icte.2017.12.007