TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Toiminta kiristyshaittaohjelmatilanteessa - johdon ohje

Traficomin julkaisuja

12/2022

Sisällysluettelo

1 Mistä on kyse? 2

1.1 Hyökkäyksen vaikutukset 2

1.2 Miten hyökkäys voi alkaa? 3

1.3 Hyökkäyksen mahdollinen ilmeneminen 3

2 Mikäli pahin tapahtuu, toimi näin! 4

2.1 Anna lupa ja valtuudet rajoitustoimille 4

2.2 Kokoa kriisiryhmä 4

2.3 Kriisiryhmän tehtävät 4

2.3.1 Muodosta tilannekuva 4

2.3.2 Suunnittele ja aktivoi toipumissuunnitelma 5

2.3.3 Huolehdi sisäisestä ja ulkoisesta viestinnästä 6

2.3.4 Tee tarvittavat viranomaisilmoitukset 6

2.4 Tue toipumissuunnitelman toteuttamista 6

3 Kriisin jälkeiset toimet 7

4 Uhkaan varautuminen 8

4.1 Tiedosta 8

4.2 Suojaa 9

4.3 Havaitse 10

4.4 Reagoi 11

4.5 Palaudu 11

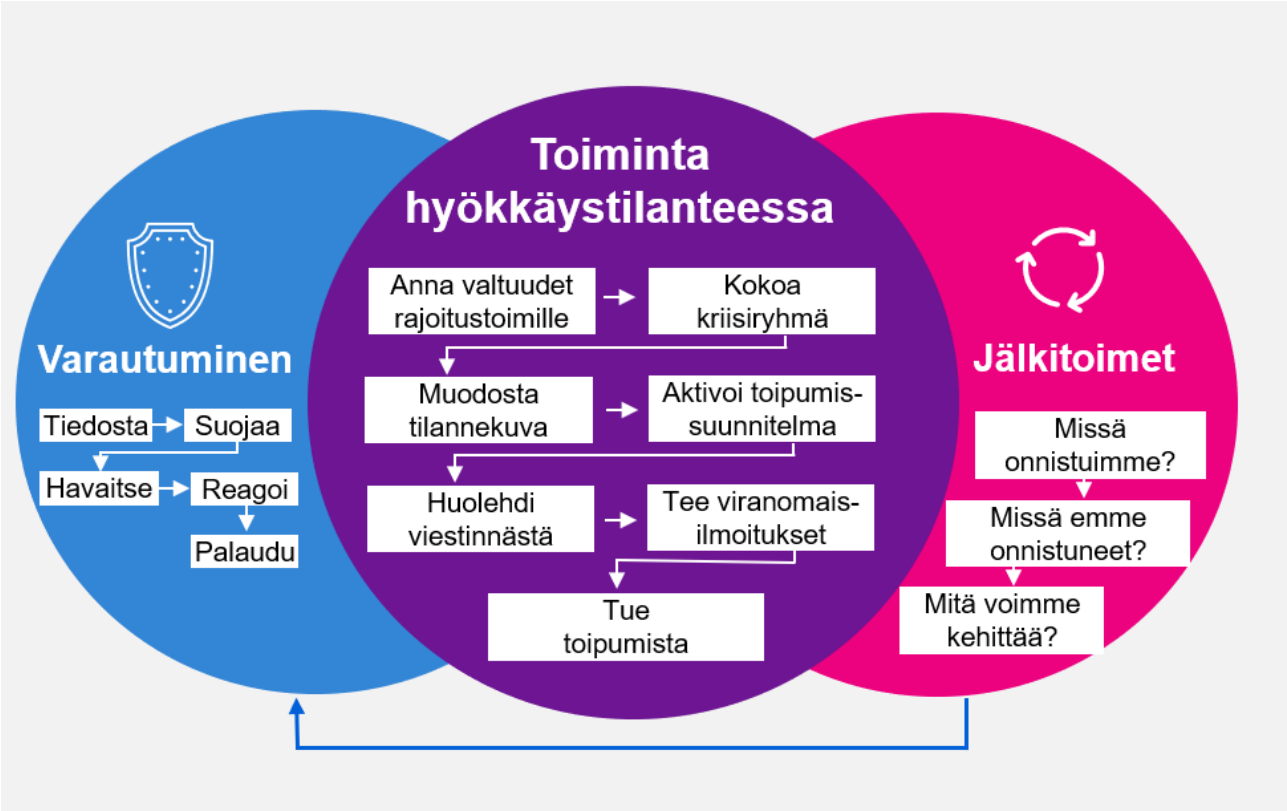
5 Lähteet ja lisäohjeet 13

1 Mistä on kyse?

Kiristyshaittaohjelma tai lunnastroijalainen (engl. ransomware) on kyberhyökkäys, jossa hyökkääjät pyrkivät salaamaan organisaation datan salausalgoritmilla ja vaativat lunnaita tietojen palauttamista vastaan. Rikolliset saattavat myös varastaa salaamansa tiedot ja kiristää organisaatiotanne tietovuodolla. Riski hyökkäyksen kohteeksi joutumiseksi on kasvanut viime aikoina merkittävästi: hyökkäysten määrä kasvoi vuodesta 2020 vuoteen 2021 noin 105 %.[1]

Kiristyshaittaohjelmat ovat osoittautuneet rikollisille tehokkaaksi tavaksi ansaita taloudellista hyötyä, sillä uhkaan varautumattomat organisaatiot ovat helppoja kohteita. Lunnaiden maksu ei kuitenkaan ole usein ratkaisu, sillä hyökkäys ja sitä kautta kiristäminen voi jatkua siitä huolimatta. Oikeaoppinen varautuminen kiristyshaittaohjelmahyökkäyksiin parantaa selvästi organisaatioiden tietoturvatasoa ja sietokykyä niin kiristyshaittaohjelmia kuin muitakin mahdollisia hyökkäyksiä vastaan. On hyvä huomioida, että osa hyökkäyksistä voidaan toteuttaa myös tiedon tuhoamistarkoituksessa.

Tämän ohjeen tavoitteena on antaa organisaatioiden ylimmälle johdolle opastusta kiristyshaittaohjelmatilanteessa toimimiselle. Tämän ohjeen lisäksi tarvitsette organisaation tietoturvasta tai ICT-ympäristöstä vastaaville henkilöille kohdennettuja teknisen tason ohjeita. Löydätte esimerkkejä teknisen tason ohjeista kappaleesta 5 (Lähteet ja lisäohjeet). Kuvassa 1 on tiivistetty ohjeen sisältö varautumisen ja hyökkäyksen hallinnan kokonaisuudeksi.



Kuva 1: Kiristyshaittaohjelmahyökkäyksen varautumisen ja hallinnan kokonaisuus

1.1 Hyökkäyksen vaikutukset

Onnistunut kiristyshaittaohjelmahyökkäys johtaa usein liiketoiminnan häiriintymiseen tai jopa sen täydelliseen keskeytymiseen. Tämä voi tarkoittaa merkittäviä taloudellisia tappioita organisaatiolle ja sen asiakkaille, mikäli toimintaa ei saada palautettua riittävän nopeasti. Haittaohjelma saattaa pahimmassa tapauksessa päätyä yhteisten palveluiden välityksellä myös tehdas- ja tuotantoympäristöihin sekä niiden toiminnanohjausjärjestelmiin.

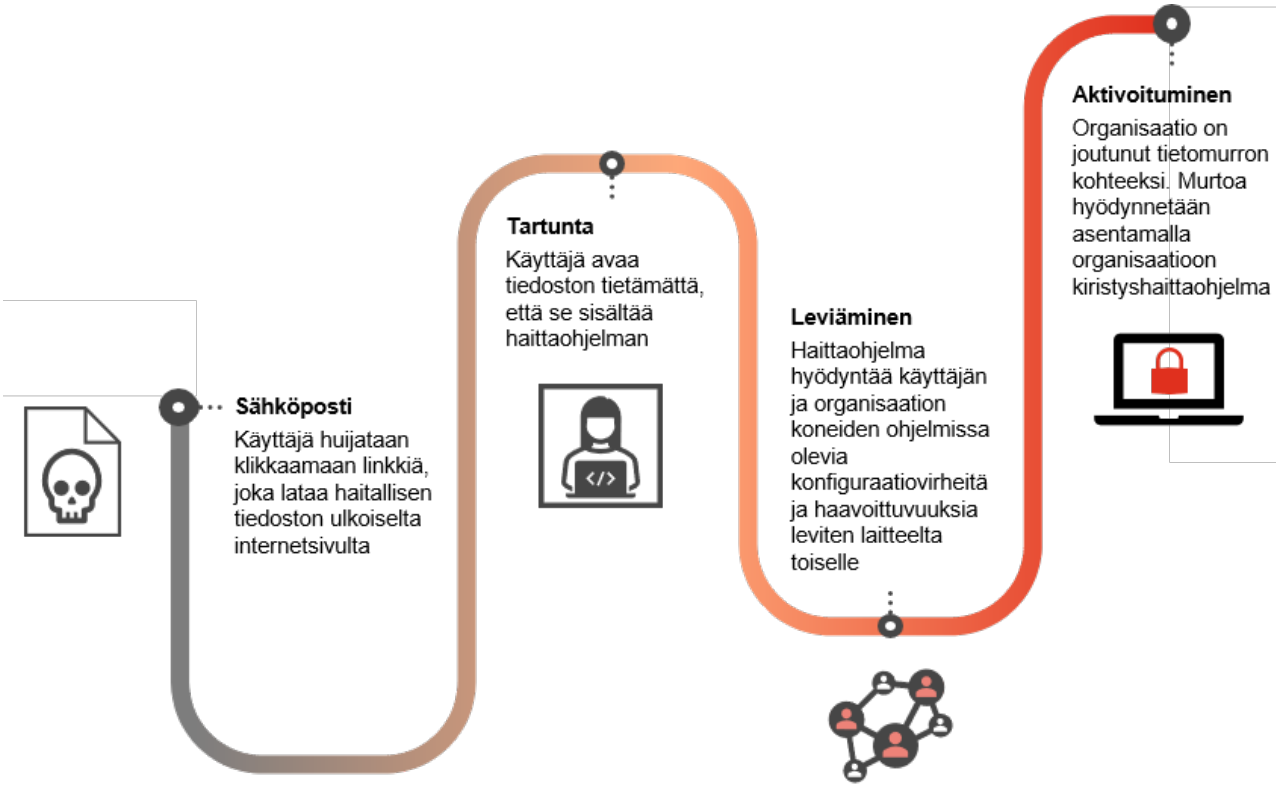
[1] Sonicwall, 2022 Sonicwall cyber threat report, https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf

Automaatioympäristöön päätynyt haittaohjelma saattaa pysäyttää tuotannon kokonaan tai pahimmassa tapauksessa muodostaa turvauhan ihmisille tai ympäristölle. Edellisten lisäksi myös erinäiset regulaatioon liittyvät sanktiot (ml. tietosuoja) voivat olla suuruusluokaltaan merkittäviä[2].

Kiristyshaittaohjelmahyökkäys on riski yhtiön maineelle, sillä tapaukset johtavat usein asian käsittelyyn julkisesti. Tämä voi vaikuttaa merkittävästi myös organisaation maineeseen, eri sidosryhmien luottamukseen sekä mahdollisesti yhtiön arvoon, ellei organisaatio ole varautunut hyökkäykseen tai hallinnut sitä asianmukaisesti.

1.2 Miten hyökkäys voi alkaa?

Kuvassa 2 esitellään yksi mahdollinen skenaario, miten hyökkääjät voivat toteuttaa kiristyshaittaohjelmahyökkäyksen. Hyökkäystapoja ja toteuttamiskeinoja on tämän lisäksi myös useita muita.



Kuva 2: Esimerkki kiristyshaittaohjelmahyökkäyksestä

1.3 Hyökkäyksen mahdollinen ilmeneminen

Kiristyshaittaohjelmahyökkäys voi ilmetä eri tavoin riippuen sen toteuttamistavasta. Parhaimmillaan hyökkäyksen kohteena oleva organisaatio kykenee havaitsemaan hyökkäyksen ensivaiheet nopeasti ja reagoimaan tilanteeseen asianmukaisesti estämällä sen leviämisen. Pahimmillaan hyökkäys havaitaan vasta silloin, kun haittaohjelma on levinnyt lähes koko organisaatioon. Hyökkääjä pyrkii usein toiminnallaan ajamaan kohdeorganisaation toivottamalta tuntumaan tilanteeseen ja näin hankaloittamaan hyökkäyksestä toipumista.

Organisaation johdon on usein mahdotonta itse hallita tai tunnistaa hyökkäyksen eri ilmenemismuotoja, mutta johdon on hyvä ymmärtää, milloin organisaatio on mahdollisesti kiristyshaittaohjelmahyökkäyksen kohteena. Seuraavat havainnot voivat olla merkkejä onnistuneesta kiristyshaittaohjelmahyökkäyksestä:

[2] GDPR.EU, What are the GDPR fines? 2022, https://gdpr.eu/fines/

- Hyökkääjä lähettää kohdeorganisaatiolle kiristysviestin tai sellainen ilmestyy työaseman näytölle.
- Organisaatio saa ilmoituksen hyökkäyksestä organisaation ulkopuolelta esim. sosiaalisen median, asiakkaan, yhteistyökumppanin tai viranomaisten välityksellä.
- Organisaation tiedostoja ei saa auki esim. verkkolevyltä tai ne ovat muutoin korruptoituneita.
- Tehdas- tai tuotantoympäristön laitteisto lakkaa toimimasta ilman näkyvää tai tunnistettavaa syytä.

2 Mikäli pahin tapahtuu, toimi näin!

2.1 Anna lupa ja valtuudet rajoitustoimille

Kun kiristyshaittaohjelmahyökkäys iskee, johdolta tarvitaan ripeää ja päättäväistä toimintaa, sillä organisaatio siirtyy normaalista johtamisesta kriisijohtamiseen. Tämä tarkoittaa samalla akuuttien rajoitustoimien toteuttamiseen liittyvien toimivaltuuksien siirtoa normaalien valtuutusprosessien sijaan ICT- tai tietoturvahenkilöstölle.

Ensimmäiset minuutit kiristyshaittaohjelmahyökkäyksen vaikutuksien rajaamisessa ovat merkittävimmät. ICT- tai tietoturvahenkilöstö voi joutua tekemään kovia ratkaisuja, kuten ajamaan joitain palveluita alas tai irrottamaan niitä verkosta. On tärkeää valtuuttaa heidät suorittamaan tarvittavia rajoitustoimia itsenäisesti, sillä kriittisessä tilanteessa toimenpiteiden valtuuttaminen yksi kerrallaan voi viedä liikaa aikaa ja laajentaa ongelmaa entisestään. Organisaatio voi tarvita myös ulkoista asiantuntija-apua. Valtuudet ulkoisen asiantuntija-avun hankkimiseen tulee myös olla kunnossa.

Organisaation johdon on hyvä tiedostaa, että asiantuntijat pyrkivät tekemään kaiken tarvittavan ja heille on hyvin tärkeää antaa työrauha sekä turvata heidän toimintaedellytyksensä koko hyökkäystilanteen ajan.

2.2 Kokoa kriisiryhmä

Hyökkäyksen iskiessä on tärkeää koota kriisiryhmä. Kriisiryhmän tehtävänä on koordinoida ja vastuuttaa tarvittavat organisaatiotasoiset toimet sekä huolehtia myös sovittujen rajoitus- tai ratkaisutoimien toteuttamisen ja niiden tehokkuuden seurannasta.

Kriisiryhmä voi olla esimerkiksi organisaation laajennettu johtoryhmä, mutta sen olisi hyvä koostua seuraavista henkilöistä tai rooleista:

- Toimitusjohtaja
- Liike- tai ydintoiminnoista vastaavat
- Tietoturvavastaava
- ICT-vastaava
- Viestintävastaava
- Lakiasioista ja/tai tietosuojasta vastaava.

2.3 Kriisiryhmän tehtävät

2.3.1 Muodosta tilannekuva

Kun ICT- tai tietoturvahenkilöstönne on saanut välittömät rajoitustoimet käyntiin ja tiedottanut organisaation johtoa tilanteesta, kriisiryhmän tulee laatia käytössä olevien tietojen perusteella tilannekuva hyökkäyksen vaikutuksista.

Ottakaa huomioon seuraavat asiat muodostaessanne organisaatiotasoista tilannekuvaa:

- Mikä on hyökkäyksessä menetetyn tiedon merkitys ja suora vaikutus organisaationne sekä asiakkaidenne ydin-, liike- tai tukitoiminnoille?
- Mitä taloudellisia seurauksia suoraan tai välillisesti tilanteesta syntyy ja onko organisaatiollanne riittävästi käytössä olevia varoja?
- Keille tulisi ensi tilassa kommunikoida hyökkäyksestä (työntekijät, hallitus, asiakkaat, sidosryhmät)?
- Tunnistakaa myös mahdolliset muut hyökkäyksestä juontuvat skenaariot ja niiden todennäköisyys, esimerkiksi onko organisaatio kenties joutunut tietomurron kohteeksi tai millaisia seuraamuksia hyökkäyksen yhteydessä varastettujen tietojen julkaisemisella olisi teille tai asiakkaillenne?
- Kriisiryhmän tulee huolehtia tapahtumapäiväkirjan (tapahtumaloki) ylläpidosta. Dokumentoikaa huolellisesti hyökkäyksen ja siitä palautumisen jokainen vaihe aikajanamuotoon. Tarkka dokumentaatio on erittäin keskeistä palautumisen, tapahtumasta oppimisen, oman oikeusturvan ja viranomaisyhteistyön kannalta.

Kriisiryhmän tehtävänä on myös huolehtia siitä, että tilannekuvaa pidetään jatkuvasti ajan tasalla, jotta tilanteen johtaminen ja siitä tiedottaminen olisi mahdollista.

2.3.2 Suunnittele ja aktivoi toipumissuunnitelma

Jos organisaatiollanne on jo olemassa suunnitelma kiristyshaittaohjelmatilanteesta toipumiselle, nyt on aika käynnistää ohjeen mukainen toiminta.

Jos organisaatiollanne ei ole olemassa olevaa suunnitelmaa, keskittykää seuraaviin asioihin:

- Miten rajaamme hyökkääjän toiminnan ja leviämisen tietojärjestelmissämme?
- Ennen kuin aloitamme palauttamisen, onko hyökkääjän yhteydet järjestelmiimme katkaistu ja onko sinne asennetut haittaohjelmat poistettu?
- Miten palautamme ydinpalvelumme ja liiketoimintamme sekä näiden tarvitsemat resurssit normaalitilaan ja varmistamme niiden tietoturvallisuuden?
- Mitä resursseja (sisäiset ja ulkoiset) tähän tarvitsemme? Huolehdi, että ICT- tai tietoturvahenkilöstö saa tarvitsemansa tuen järjestelmien palauttamisprosessissa, kuten varmuuskopioiden tarkastamisessa ja palauttamisessa.
- Mikäli organisaatiollanne on kybervakuutus, niin huolehtikaa, että organisaatio ottaa yhteyttä vakuutusyhtiöön. Osa kybervakuutuksista voi sisältää palveluelementtejä, kuten tarvittavaa asiantuntijatukea, josta voi olla tilanteen ratkaisemisessa apua.

Älkää maksako lunnaita! Aluksi voi näyttää siltä, että lunnaiden maksamisesta koituvat kustannukset olisivat pienempiä kuin kriisin ratkaiseminen itsenäisesti. Lunnaita ei kuitenkaan tule missään tapauksessa maksaa, sillä:

- Rikollisen sanaan ei voi luottaa, eikä heidän tarjoamiensa salauksen purkuavaimien toiminnasta ole mitään takeita.
- Toimivienkin avaimien kanssa toipuminen voi olla hidasta ja kallista.
- Lunnaiden maksaminen rahoittaa rikollista toimintaa ja tukee sen kehitystä.

- Kiristys voi olla myös hämäystä, ja haittaohjelma tuhoaakin tiedostot niiden salaamisen sijaan.[3]

- Lunnaiden maksu voi olla pakotesääntelyn tai jonkin maksun vastaanottavan maan kansallisen säädännön vastaista eli lunnaiden maksun läpimenoon voi liittyä myös epävarmuuksia.

2.3.3 Huolehdi sisäisestä ja ulkoisesta viestinnästä

Suunnitelkaa, miten tilanteesta ja palautumisprosessista sekä sen edistymisestä tiedotetaan yhtiön hallitukselle, asiakkaille, yhteistyökumppaneille sekä tarvittaessa viranomaisille. Raportoikaa ja päivittäkää tilannekuvaa sidosryhmille myös tilanteen edetessä.

Sopikaa, kuka toimii organisaation virallisena kasvona julkisuuteen ja kuka ottaa yhteyttä asiakkaisiin tai muihin tarvittaviin sidosryhmiin. Välttäkää tilannetta, jossa ratkaisun kannalta merkittävimmät henkilöt (kuten tekniset asiantuntijat tai tietoturvavastaava) toimisivat organisaation tiedottajina. Heille tulee antaa täysi työrauha itse tilanteesta palautumiseen liittyviin tehtäviin.

2.3.4 Tee tarvittavat viranomaisilmoitukset

Ilmoittakaa hyökkäyksestä Kyberturvallisuuskeskukselle. Meiltä saa apua hyökkäyksen selvittämisessä ja ilmoituksenne auttaa muita mahdollisen hyökkäyksen kohteeksi joutuvia organisaatioita. Voitte tehdä ilmoituksen sähköpostitse osoitteeseen cert@traficom.fi tai lomakkeella (https://www.kyberturvallisuuskeskus.fi/fi/ilmoita). Varautukaa myös Kyberturvallisuuskeskuksen yhteydenottoon.

Tehkää hyökkäyksestä rikosilmoitus poliisille osoitteessa https://asiointi.poliisi.fi/. Tämä kannattaa tehdä hyökkäyksen teknisen selvittämisen yhteydessä, sillä ilmoitukseen tulee liittää todisteita. Saatte opastusta poliisilta todistusaineiston asianmukaiseen taltioimiseen. Jos hyökkäystilanne vaarantaa yleisen turvallisuuden (esim. turvauhka[4]), hengen tai terveyden, tehkää ilmoitus suoraan hätänumeroon 112.

Mikäli rikolliset ovat saaneet haltuunsa henkilötietoja, tietosuojavaltuutetun toimistolle on ilmoitettava 72 tunnin kuluessa tietoturvaloukkauksen havaitsemisesta osoitteessa https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta. Tämän ensisijaisena tarkoituksena on rekisteröidyn oikeuksien turvaaminen. Voitte tarvittaessa tehdä ilmoituksen vaiheittain: tee ensin alustava ilmoitus ja täydennä ilmoitusta myöhemmin. [5]

Jos organisaationne toimii huoltovarmuuskriittisellä alalla, ilmoittakaa hyökkäyksestä myös oman toimialanne valvovalle viranomaiselle, eli tässä tapauksessa ns. NIS-viranomaiselle: https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx?langid=fi&RetUrl=https%3A//www.traficom.fi/fi/asioi-kanssamme. Lisätietoa NIS-direktiivin sääntelystä löydätte täältä: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/digitaaliset-palvelut-ja-infrastruktuuri

2.4 Tue toipumissuunnitelman toteuttamista

Kun välittömät hyökkäyksen ratkaisutoimet ovat käynnistyneet, tulisi organisaation johdon keskittyä siihen, että toipumista toteutetaan tarvittavin keinoin. Organisaation johto voi tukea tätä olemalla helposti avainhenkilöiden tavoitettavissa sekä tukemalla toipumisen kannalta keskeisten henkilöiden työskentelyä pitämällä mm. yllä rauhallista ja eteenpäin katsovaa ilmapiiriä. On hyvä muistaa, että tässä kohden ei ole syytä keskittyä siihen, mitä kukin oli ehkä tehnyt väärin tai oli jättänyt tekemättä.

[3] https://www.bleepingcomputer.com/news/security/beware-onyx-ransomware-destroys-files-instead-of-encrypting-them/

[4] Turvauhka kemikaalien käsittelyssä: https://tukes.fi/turvauhkiin-varautuminen-vaarallisten-kemikaalien-kasittelyssa-ja-varastoinnissa

[5] https://www.suomi.fi/oppaat/tietomurto/akuutit-toimet/ilmoita-viranomaisille

Yleisesti ottaen hyökkäyksestä aiheutuneisiin toipumiskustannuksiin tai menetettyyn aikaan ei tulisi tässä kohden keskittyä liikaa. Tärkeintä on yrittää toipua hyökkäyksestä organisaationa mahdollisimman tehokkaasti, jotta organisaatio voisi palata takaisin normaalitilaan niin pian kuin mahdollista.

3 Kriisin jälkeiset toimet

Kriisin päätyttyä ja liiketoimintojen normalisoiduttua on tärkeää käynnistää hyökkäyksen jälkiselvitys ja oppia tapahtuneesta mahdollisimman paljon. Tämän yhteydessä on hyvä arvioida hyökkäyksen näkökulmasta missä olimme onnistuneet, missä emme ja miten voimme parantaa turvallisuustasoamme, jotta vastaavilta tilanteilta vältyttäisiin jatkossa.

Ensisijaisesti organisaationne tulisi kuitenkin selvittää mitä kautta hyökkääjät pääsivät sisään tietojärjestelmäympäristöönne ja miten he siellä etenivät. Nämä hyökkäyksen mahdollistaneet aukot tai puutteelliset turvallisuustoteutukset tulee paikata viipymättä, jotta samanlainen hyökkäys ei toistuisi. Selvitystyön apuna on hyvä käyttää kohdassa 2.3.1 kuvattua tapahtumapäiväkirjaa, jota on täydennetty tutkinnan ja palautumisen edetessä.

Seuraavaksi tulisi kartoittaa organisaationne havainnointikykyä hyökkäykseen liittyen. Pyrkikää etsimään vastauksia alla oleviin kysymyksiin yhdessä asiantuntijoidenne tai palvelutarjoajienne kanssa. Johdon tulisi tarkastella vastausten perusteella organisaation havainnointi- ja reagointisuunnitelmia sekä prosesseja ja pyrkiä kehittämään niitä tehokkaammiksi.

- Ovatko hyökkäyksien havaitsemiseen liittyvät kontrollimme riittäviä?
- Aiheuttivatko hyökkääjän toimet hälytyksiä? Millaisia hälytyksiä?
- Välittyikö tieto hälytyksistä oikeille henkilöille?
- Miten näihin hälytyksiin reagoitiin, jos reagoitiin?

Palautumisprosessin tehokkuutta tulee myös arvioida seuraavien kysymysten avulla:

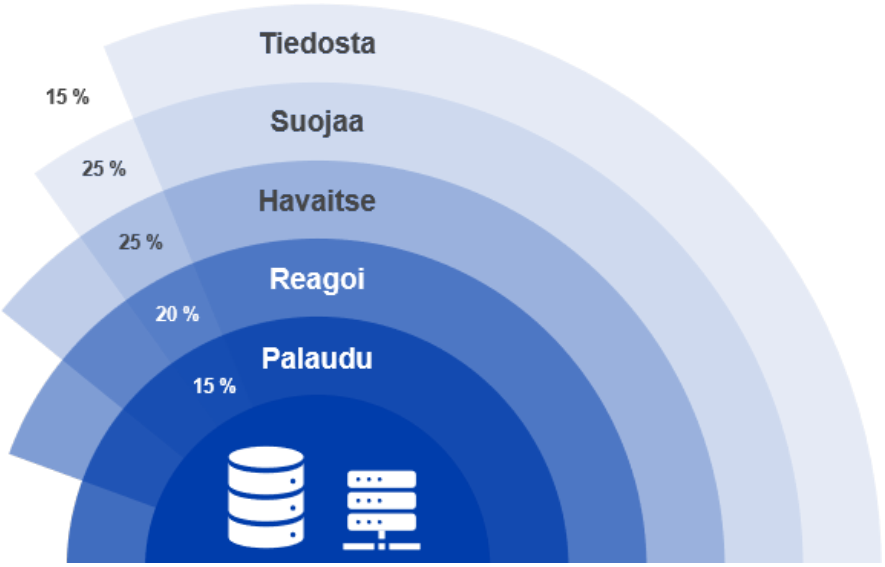
- Jaettiinko kriisiryhmän vastuut oikeille henkilöille? Miten kyseiset henkilöt suoriutuivat tehtävistään?
- Miten IT-henkilöstö onnistui palautumisessa? Saatiinko palvelut riittävän nopeasti jälleen toimintakuntoon ja riittivätkö resurssit?
- Onnistuiko kriisiryhmä viestimään oikeat asiat, oikeille henkilöille ja oikeaan aikaan?
- Sisältääkö dokumentointi kaikki tapauksen kannalta merkittävät tapahtumat ja ovatko aikaleimat oikein?
- Oliko tapauksen tekninen tutkinta riittävää?
- Toimiko yhtiön johto itse tilanteessa tai siihen varautumisessa riittävän kokonaisvaltaisesti?

Vaikka kiristyshaittaohjelmahyökkäys on aina vakava tilanne, voi niitä myös estää hallita. Tämä ei kuitenkaan onnistu ilman asianmukaista varautumista sekä jatkuvaa työtä kyberturvallisuuden varmistamiseksi.

4 Uhkaan varautuminen

Hyökkäysmenetelmät kehittyvät jatkuvasti, joten hyökkäyksiin varautumiseen liittyvän työn on oltava jatkuvaa ja perustuttava systemaattiseen toimintaan sekä puolustuksen kerroksellisuuteen. Organisaation johdon on osoitettava kiristyshaittaohjelmahyökkäyksiä varten tarvittavat resurssit, jotta organisaation käytössä olevan tietoverkko- ja palveluympäristön turvallisuudesta voidaan huolehtia. Resurssien riittävyyttä sekä varautumistoimien käytännön tehokkuutta tulee myös mitata kehityksen mahdollistamiseksi.

Kyberturvallisuuden tulee keskittyä puolustukselliseen syvyyteen ja varautumiskyvykkyyteen eri kontrollitasoilla. Mikäli yksi puolustuskerros pettää, muut kerrokset tarjoavat lisäsuojaa. Kiristyshaittaohjelmaan varautuminen voidaan jakaa viiteen eri kerrokseen, jotka yhdistettyinä parantavat suojautumista huomattavasti. Kuvassa 3 on myös ilmaistu prosentein kunkin kerroksen viitteellinen merkittävyys koko varautumisprosessissa. On tärkeää ymmärtää, että asianmukainen kybervarautuminen onnistuu vain tällaisessa muodossa ja että yksittäinen suojaava kerros ei yksinomaan useinkaan riitä.[6]



Kuva 3: Uhkaan varautuminen ja osa-alueiden merkittävyys varautumisprosessissa

4.1 Tiedosta

Jokainen organisaatio on potentiaalinen kiristyshaittaohjelmahyökkäyksen kohde joko suoraan tai osana kriittistä toimitusketjua. Rikolliset osaavat myös muokata hyökkäyksiään ja lunnasvaatimuksiaan kohdeorganisaatiokohtaisesti hyvinkin tarkasti tuottonsa maksimoimiseksi. Suhtautukaa siis uhkaan vakavasti.

Tunnistakaa toimintanne kannalta elintärkeät palvelut ja arvioikaa mitä tapahtuisi, mikäli jokin tai kaikki näistä palveluista ei olisi käytettävissä. Kartoittakaa tämän jälkeen yhteistyössä ICT-asiantuntijoidenne kanssa organisaationne käytössä oleva IT-omaisuus, jota tarvitsette toimintanne kannalta keskeisten palveluiden tuottamiseen tai toteuttamiseen. Näitä ovat mm. työasemat, palvelimet, mobiililaitteet, tietokannat ja käyttäjärekisterit. Muistakaa, että ette voi suojata sellaista, jonka olemassaolosta ette ole tietoisia. Tämä auttaa organisaatiotanne myös poikkeamanhallinta- ja palautumissuunnitelmien laatimisessa.[7]

Luokaa seuraavaksi eri varautumisen kerroksien konteksti arvioimalla erityisesti kiristyshaittaohjelmahyökkäyksen mahdollisesti aiheuttama riski. Huomioikaa arvioinnissa olemassa olevat hallinnolliset ja tekniset kontrollit sekä henkilöstön tietoisuus. Muistakaa

[6] NIST Cybersecurity framework https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[7] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

käsitellä jäännösriskit ja peilata niitä organisaationne riskinottokykyyn ja -halukkuuteen. Keskustelkaa kiristyshaittaohjelmaan liittyvästä uhkasta sekä riskistä johtoryhmän ja hallituksen kokouksissa.

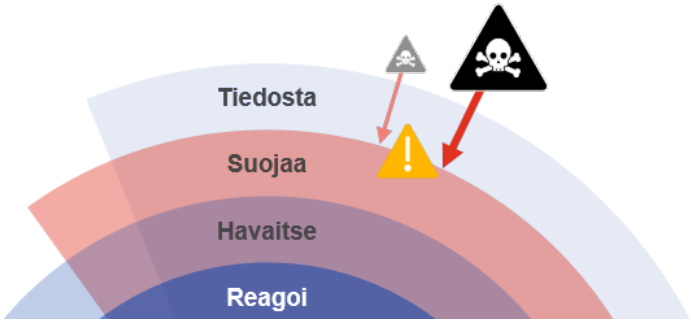
Varmistakaa sopimuksin ja vaatimuksin myös palveluntuottajien vastuut ja tehtävät.

Seuratkaa käytössä olevien varautumistoimienne tilaa ja organisaationne riskitasoa tätä varten luotujen mittareiden avulla.

Organisaation johdon on myös tärkeää huomioida, että kyberturvallisuudelle tulisi osoittaa budjetista sellainen osa, joka on riittävä tarvittavien varautumistoimien toteuttamiseksi. Voitte käyttää hyödyksi ajatusmallia, jossa arvioitte kuinka ison rahallisen menetyksen toteutettu turvallisuusinvestointi estää tulevaisuudessa. Toisin sanoen, kuinka paljon euromääräisesti mahdollinen onnistunut hyökkäys teille maksaisi? Tätä kautta pystytte myös arvioimaan organisaationne riskinottohalukkuutta.

4.2 Suojaa

Suojaustoimenpiteet tulee hoitaa huolellisesti, sillä internetistä lähtöisin olevia hyökkäysyrityksiä tapahtuu päivittäin. Osa näistä yrityksistä ei ole organisaationne verkon palveluiden kartoittamista kummempia, mutta joukossa voi olla myös hyvinkin vihamielisiä ja aggressiivisia hyökkäysyrityksiä. Organisaationne kykenee tehokkaalla suojautumisella torjumaan suurimman osan näistä hyökkäysyrityksistä, mutta tämä vaatii panostuksia kyberturvallisuuden ylläpitoon ja kehittämiseen.



Kuva 4: Jotkut hyökkäykset pysähtyvät suojaustoimien ansiosta

Organisaatiollanne tulisi tässä vaiheessa olla kattava lista kaikesta käytössä olevasta IT-omaisuudesta (ks. kohta 3.1), jotta niiden suojaamiseksi voidaan tehdä toimenpiteitä. Suojaamistoimenpiteissä tulisi ensisijaisesti keskittyä tunnistettuihin toimintanne kannalta elintärkeisiin palveluihin tai järjestelmiin.

Suojaustasoon vaikuttaa merkittävästi organisaationne hallinnollinen ja tekninen kypsyys. Mitä kyberkyvykkäämpi organisaationne on, sitä paremmin se on suojautunut myös kiristyshaittaohjelmahyökkäyksiltä.

Seuraavat kysymykset auttavat määrittämään organisaationne teknistä kypsyystasoa. Voitte myös täydentää kypsyystason arviointia käyttämällä kyberturvakeskuksen julkaisemaa Kybermittaria (https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari).

Käykää alla olevien kysymyksien tilanne tarkkaan läpi asiantuntijoidenne kanssa:[8] [9]

[8] Centre for cyber security Belgium: Incident management guide https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

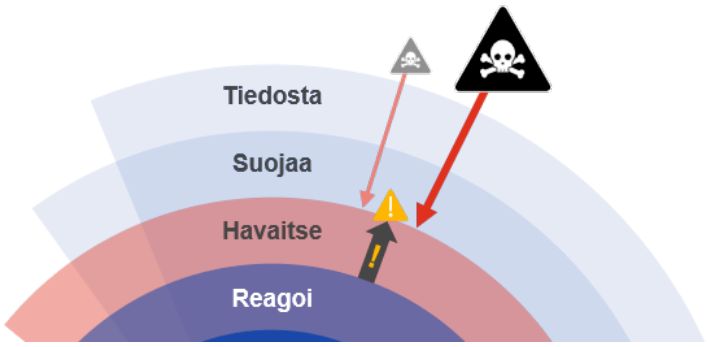
[9] CIS, 7 steps to help prevent & limit the impact of ransomware, 2022, https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

- Olemmeko varmistaneet, että käytössämme on toimiva viestintäkanava kyberhyökkäyksen toteutuessa?
- Asennammeko tietoturva- tai ohjelmistopäivitykset säännöllisesti ja riittävän usein? Miten varmistumme siitä, että käytämme vain turvallisia ohjelmistoversioita?
- Käytämmekö kaksivaiheista tunnistautumista kaikissa Internettiin avoinna olevissa palveluissamme?
- Onko järjestelmämme ja palvelumme tietoturvatestattu ja niiden perusteella saadut havainnot korjattu?
- Onko organisaatiomme verkko suojattu asianmukaisesti palomuureilla ja päätelaitteet havainnointi- ja hyökkäyksien torjuntaohjelmistoilla? Käytämmekö myös virustorjuntaohjelmistoa sekä työasemakohtaisia palomuureja?
- Onko työntekijöillä vain ne käyttöoikeudet ja -valtuudet eri järjestelmiin ja palveluihin, joita he tarvitsevat jokapäiväisessä työssään?
- Käytämmekö työasemiamme vain käyttäjätason oikeuksin? Ylläpitäjän oikeudet laajentavat merkittävästi hyökkääjän mahdollisuuksia edetä järjestelmässä.
- Onko organisaatiomme tietoverkko jaettu eri osiin käyttötarkoitustensa mukaan? Tehokas segmentointi hidastaa hyökkäyksen leviämistä eri tietoverkon osiin ja siten myös järjestelmiin.
- Tallennammeko verkko-, järjestelmä- ja palvelukohtaisia tapahtumalokeja ja kuinka kauan niitä säilytetään? Toteutammeko lokienhallintaa säädösten mukaisesti?

4.3 Havaitse

Parhaimmat mahdolliset suojauksetkin voivat joskus pettää. Tämän vuoksi organisaationne palveluita, järjestelmiä sekä verkkoa tulisi valvoa jatkuvasti mahdollisten hyökkäysten havaitsemiseksi. Tehokas havainnointi mahdollistaa nopean reagoinnin, mikäli kohdan 4.2 suojaukset pettävät. Mitä nopeammin hyökkäys havaitaan, sitä paremmin sen aiheuttamia vahinkoja pystytään pienentämään ja ehkäisemään.

Organisaationne ICT-omaisuutta voidaan valvoa erilaisilla sensoreilla ja tietoturvaohjelmistoilla. Voitte myös hankkia organisaationne valvonnan tueksi esimerkiksi tietoturvavalvomopalvelun, joka vastaa koko organisaatioverkon valvonnasta ja tarjoaa palvelua usein myös kellon ympäri juhlapyhinä tai esim. lomakausina.



Kuva 5: Osa hyökkäyksistä voi läpäistä suojauskerroksen. Tällöin tarvitaan tehokasta havainnointia, jotta organisaationne pystyy reagoimaan hyökkäykseen.

Myös organisaationne henkilöstön tietoisuus hyökkäyksen uhasta on tärkeää. Huolehtikaa, että organisaatiossanne järjestetään säännöllisesti koulutuksia, joissa esitellään uhkia ja niiden realisoitumismekanismeja (ks. 1.2), opetetaan oikeita toimintamalleja ja hyvää kyberhygieniaa sekä käydään läpi hyökkäystilanteessa tarvittavia toimenpiteitä. Jokaisen organisaation

työntekijän olisi hyvä ymmärtää, miten toimia turvallisesti päivittäisessä työssään ja näin pienentää mahdollisen hyökkäyksen todennäköisyyttä.

Organisaation havaitsemiseen liittyviä kyvykkyyksiä voidaan myös kehittää ja niiden toimintaa varmistaa erilaisten teknisten arviointien ja testauksien avulla. Yksi parhaista keinoista tämän toteuttamiseen on testaaminen, jossa valitut tietoturva-asiantuntijat ”hyökkäävät” eri tietoverkon osia, järjestelmiä tai palveluita vastaan ja samalla organisaation omat sekä palvelukumppaneiden edustajat pyrkivät havainnoimaan hyökkäyksen eri vaiheita. Havainnointikyvykkyyttä tarkennetaan sitä mukaa, jos hyökkäystä ei kyetä havaitsemaan nostaen näin teknisten kontrollien tehokkuutta tai tietoturvahenkilöstön osaamistasoa.

4.4 Reagoi

Tehokkaan havainnoinnin lisäksi uhkiin täytyy reagoida asianmukaisesti. Tietoturvavalvomon tai havainnointi- ja reagointiohjelmiston tekemästä havainnosta ei ole juurikaan hyötyä, mikäli organisaationne ei osaa ryhtyä tarvittaviin toimenpiteisiin. Reagointi tulee myös aina osata suhteuttaa havaitun uhkan vakavuuteen, jotta liiketoimintaa ei häirittäisi tarpeettomasti tai kriittistä uhkaa vähäteltäisi.

Varmistakaa, että organisaatiollenne kehitetään suunnitelmia tietoturvapoikkeamien hallintaan ja että kiristyshaittaohjelma sisällytetään yhdeksi skenaarioksi. Varmistakaa, että nämä suunnitelmat ovat saatavilla myös ”offline”-versiona esimerkiksi paperisessa muodossa. Tällöin niihin pääsee käsiksi, vaikka kiristyshaittaohjelma olisikin salannut kaikki digitaaliset tiedostonne.

Varmistakaa sopimuksilla ja vaatimuksilla palveluntuottajien vastuu uhkiin reagoimisessa, sillä osa haittaohjelmista voi levitä myös kolmansien osapuolien kautta.

Sopikaa palveluntarjoajienne kanssa teknisen poikkeamatilanteen tukitoimista, kuten teknisestä tutkinnasta ja vahinkojen pienentämistoimista. Lisätkää nämä osaksi varautumissuunnitelmia.

Selvittäkää myös, tarvitseeko organisaationne kybervakuutusta ja mikäli päädytte sellaisen hankkimaan, liittäkää sen mahdolliset palveluelementit liittyvät myös osaksi palautumissuunnitelmia. Muistakaa pitää kybervakuutus tarkoin varjeltuna salaisuutena! Tiedon julkistaminen tekee organisaatiostasi potentiaalisen hyökkäyskohteen.

Huolehtikaa, että suunnitelmianne käydään säännöllisesti läpi harjoituksin ja että niitä kehitetään saamanne harjoitusdatan, palautteen ja teknisten metriikoiden tarjoaman tiedon perusteella. Kaikkien suunnitelmien osapuolten tulisi myös ymmärtää oma roolinsa ja osata toimia sen mukaisesti hyökkäystilanteessa.

4.5 Palaudu

Joskus kiristyshaittaohjelmahyökkäys onnistuu varautumistoimista huolimatta. Tähän voi olla erilaisia syitä, kuten esimerkiksi jonkin varautumisen kerroksen keskeneräisyys, teknisten kontrollien puutteet tai ns. 0-päivähaavoittuvuuden hyväksikäyttö (ohjelmistohaavoittuvuus, johon ei ole saatavilla korjausta).

Laaja-alaisesta kiristyshaittaohjelmahyökkäyksestä palautuminen on yleisesti mahdollista, jos hyökkäyksen kohteeksi joutuneella organisaatiolla on käytössään ajantasaiset ja riittävän kattavat varmuuskopiot. Jossain tapauksissa, joissa varmuuskopiot ovat myös saastuneet, tarvitaan myös suojakopioita.

Jotta palautuminen olisi tehokasta, on varautumisessa syytä kiinnittää huomiota myös tarvittavaan tekniseen arkkitehtuuriin ja kyvykkyyksiin. Näitä ovat muun muassa:

- Turvallinen tallennusympäristö, jossa varmistetaan säilytetyn tiedon eheys ja luottamuksellisuus.
- Lokienhallinta, jonka tarkoituksena on mahdollistaa ajantasaisen ja asianmukaisen varmuuskopioinnin seuranta.

- Mikäli organisaationne käyttää esim. virtuaalipalvelimia, varmistakaa, että nekin kuuluvat varmuuskopioinnin piiriin.
- Varmuuskopioiden palauttamisen testaus sekä niiden toimivuuden varmistaminen.
- Eristetty varmuuskopiointiympäristö, joka estää varmuuskopioiden manipuloinnin tai tuhoamisen.

Kohdassa 4.1 (Tiedosta) organisaatioiden tulisi tunnistaa toimintansa kannalta keskeiset järjestelmät ja palvelut. Kun tunnistaminen on tehty, tulisi niille suunnitella palvelu- ja järjestelmäkohtaiset toipumissuunnitelmat. Toipumissuunnittelun tavoitteena on ylläpitää tarvittavaa dokumentaatiota, toimintamallia sekä kyvykkyyksiä, joiden avulla palveluiden tai järjestelmien palauttaminen on mahdollista toteuttaa tehokkaasti ja turvallisesti. Näitä toipumissuunnitelmia tulisi säilyttää niin, että ne ovat käytettävissä siinäkin tapauksessa, että tiedostojärjestelmät eivät olisi saatavilla. Suunnitelmista voidaan tehdä esimerkiksi paperikopioita.

Muita palautumisessa ja siihen liittyvässä suunnittelussa huomioitavia seikkoja ovat muun muassa:

- Missä järjestyksessä järjestelmät tulee palauttaa? Väärä palauttamisjärjestys voi aiheuttaa ongelmia tai hidastaa kaikkien kriittisten palveluiden kokonaispalautumisprosessia.
- Onko palautumisprosessit ohjeineen huomioitu palveluntarjoajien ylläpitämien palveluiden tai järjestelmien osalta? Onko palauttamista harjoiteltu?
- Miten varmistamme, että palautetut palvelut ja järjestelmät ovat turvallisia? Jos varmuuskopioversiot, kuten suojakopiot, eivät ole ajantasaisia, voi niiden kautta tuotantoon päätyä turvattomia ohjelmistoversiota tai turvattomia konfiguraatioita.

5 Lähteet ja lisäohjeet

Ohjeita johdolle

1. **Kyberturvallisuuskeskus.** Selviytymisopas kiristyshaittaohjelmia vastaan. [Online] 2016. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf

2. **Kyberturvallisuuskeskus**. Pienyritysten kyberturvallisuusopas. [Online] 2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

3. **Suomi.fi.** Tietomurto: ilmoita viranomaisille. [Online] 2022. https://www.suomi.fi/oppaat/tietomurto/akuutit-toimet/ilmoita-viranomaisille

4. **Forbes.** Ransomware 2.0: How malware has evolved and where it's heading. [Online] 2021. https://www.forbes.com/sites/forbestechcouncil/2021/05/20/ransomware-20-how-malware-has-evolved-and-where-its-heading/

5. **NIST.** Getting started with Cybersecurity Risk Management | Ransomware. [Online] 2022. https://csrc.nist.gov/csrc/media/Publications/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final/documents/quick-start-guide--ransomware.pdf

6. **NIST.** Cybersecurity Framework. [Online] 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

7. **NIST**. Ransomware Risk Management: A Cybersecurity Framework Profile. [Online] 2022. https://csrc.nist.gov/publications/detail/nistir/8374/final

8. **GDPR.EU.** What are the GDPR fines? [Online] 2022. https://gdpr.eu/fines/

9. **Australian kyberturvallisuuskeskus.** Ransomware emergency response: one page guide. [Online] 2022 https://www.cyber.gov.au/sites/default/files/2021-10/ACSC-ransomware-emergency-response-one-page-guide.pdf

10. **Ransomware.org.** Everything you need to know about ransomware. [Online] 2022. https://ransomware.org/

Ohjeita ICT-asiantuntijoille

11. **NIST.** Recovering from Ransomware and Other Destructive Events. 2022**.** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-11.pdf

12. **CIS.** 7 steps to help prevent & limit the impact of ransomware. [Online] 2022. https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

13. **CISA.** Cyber security evaluation tool with ransomware readiness assessment module. [Online] 2022. https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

14. **Europol.** No more ransom. [Online] 2021. https://www.nomoreransom.org/en/index.html

15. **NIST.** Ransomware protection and response. [Online] 2022. https://csrc.nist.gov/projects/ransomware-protection-and-response

16. **Microsoft.** Ransomware and extortion, a collection of resources. [Online] 2022. https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware

17. **CIS.** 7 steps to help prevent & limit the impact of ransomware. [Online] 2022. https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

18. **CISA.** Cyber security evaluation tool with ransomware readiness assessment module. [Online] 2022. https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

19. **Europol.** No more ransom. [Online] 2021 https://www.nomoreransom.org/en/index.html

20. **NIST.** Ransomware protection and response. [Online] 2022. https://csrc.nist.gov/projects/ransomware-protection-and-response

21. **Microsoft.** Ransomware and extortion, a collection of resources. [Online] 2022 https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware

22. **Sonicwall.** 2022 Sonicwall cyber threat report. [Online] 2022. https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf

23. **NCSC-UK.** Mitigating malware and ransomware attacks. [Online] 2021. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

24. **NCSC-UK.** Mitigating malware and ransomware attacks. [Online] 2021. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus

PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-798-3
ISSN 2669-8757

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus