TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Toimintaohje – Kiristyshaittaohjelma

Traficomin julkaisuja
23/2022

Sisällysluettelo

1 Johdanto 2
1.1 Ohjeen tarkoitus 2
1.2 Mitä tarkoittaa kiristyshaittaohjelma 2
2 Varautuminen 3
2.1 Hallinnolliset toimet 3
2.2 Tekniset toimet 4
2.3 Varautuminen ja harjoittelu käytännössä 4
3 Tietoturvaloukkauksen havaitseminen 6
4 Toimintaohjeet 7
4.1 Tietoturvaloukkauksen selvityksen työnkulku 7
4.2 Välittömät toimenpiteet 9
4.3 Tietoturvaloukkauksen selvitys 12
4.4 Palautuminen 14
5 Tietoturvaloukkauksen jälkiselvitys 16

1 Johdanto

1.1 Ohjeen tarkoitus

Tämän Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen laatiman ohjeen tarkoituksena on neuvoa organisaatioita tilanteissa, joissa epäillään kiristyshaittaohjelman aiheuttamaa hyökkäystä tai kiristyshaittaohjelma estää normaalin toiminnan. Ohje keskittyy tämän tietoturvallisuuden poikkeamatyypin erityispiirteiden käsittelyyn. Tilanteen ratkaisemiseksi kokonaisuudessaan organisaation on hyvä ylläpitää ja noudattaa laatimaansa hallintasuunnitelmaa tietoturvapoikkeamatilanteita varten (engl. Incident Response Plan).

Tämä ohje opastaa yleisellä tasolla tietoturvaloukkaustilanteessa toimimista ja siitä toipumista. On suositeltavaa, että organisaatio laatii itselleen erillisen oppaan, joka huomioi sen oman teknisen ja toiminnallisen ympäristön tarkemmalla tasolla. Projektin on rahoittanut Huoltovarmuuskeskus.

1.2 Mitä tarkoittaa kiristyshaittaohjelma

Kiristyshaittaohjelmia (engl. Ransomware) käytetään kyberhyökkäyksissä, joissa verkkorikolliset pyrkivät salaamaan organisaation datan salausalgoritmilla ja vaativat lunnaita tietojen palauttamista vastaan. Rikolliset usein myös varastavat luottamuksellisia tietoja ja voivat kiristää organisaatiota tietovuodoilla.

Kiristyshaittaohjelmat ovat osoittautuneet rikollisille tehokkaaksi tavaksi ansaita taloudellista hyötyä, sillä uhkaan varautumattomat organisaatiot ovat helppoja kohteita. Lunnaiden maksu tilanteen selvittämiseksi ei kuitenkaan ole oikea ratkaisu. Maksaminen ei välttämättä takaa tietojen palauttamista tai edes estä kiristyksen tai muiden hyökkäysten jatkumista. Hyökkääjän tavoitteena voi olla myös pelkkä tietojen tuhoaminen, jolloin kiristys on vain hämäystä. Tällöin dataa ei ole mahdollista palauttaa edes lunnaita maksamalla.

Oikeaoppinen varautuminen kiristyshaittaohjelmahyökkäyksiin parantaa selvästi organisaatioiden tietoturvatasoa ja sietokykyä niin kiristyshaittaohjelmia kuin muitakin mahdollisia hyökkäyksiä vastaan. Kyberturvallisuuskeskus on tämän ohjeen lisäksi julkaissut erityisesti johdolle suunnatun oppaan kiristyshaittaohjelmaloukkaustilanteissa toimimiseksi.[1]

[1] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/toiminta-kiristyshaittaohjelmatilanteessa-johdon-ohje

2 Varautuminen

Varautuminen poikkeamiin on hyvä tapa vähentää niiden vakavuutta ja mahdollistaa nopea toipuminen ja liiketoiminnan jatkuminen. Organisaatio voi arvioida omaa valmiuttaan käyttämällä hyväksi esimerkiksi Kyberturvallisuuskeskuksen Kybermittaria.[2] Etukäteen laadittu poikkeamanhallintasuunnitelma antaa hyvät lähtökohdat toimia, kun poikkeamatilanne tapahtuu. Organisaation tulee myös varmistaa, että toimet kuten käyttäjätunnusten lukitseminen, palvelinten ja päätelaitteiden eristäminen verkosta ja verkkoliikenteen rajoittaminen haitallisiin IP-osoitteisiin tai verkkotunnuksiin on teknisesti mahdollista ja henkilöstöltä löytyy tähän osaaminen.

Lokitietojen kerääminen, kokoaminen ja monitorointi on tärkeää poikkeaman havaitsemiseksi ajoissa. Lokitiedot mahdollistavat myös poikkeaman perusteellisen tutkimisen ja täten nopeuttavat ympäristön siivousta ja palauttamista. Kyberturvallisuuskeskus on laatinut lokitietojen keräämisestä ja käyttämisestä oppaan.[3] Riippuen organisaation käyttämistä järjestelmistä, kattavaan havainnointiin vaaditaan tyypillisesti lisäksi verkko- ja järjestelmätason ratkaisuja.

2.1 Hallinnolliset toimet

Välittömät toimet

- Laadi organisaatiollesi poikkeamanhallintasuunnitelma kiristyshaittaohjelmahyökkäystä varten.
- Kouluta henkilöstöä toimimaan tässä toimintaohjeessa kuvaillun poikkeaman aikana.
    - Tarjoa myös tavallisille työntekijöille perustason koulutus, jossa neuvotaan kuinka toimia kiristyshaittaohjelma iskiessä työntekijän omalle päätelaitteelle.
- Selvitä etukäteen, miten voit ilmoittaa tietoturvaloukkauksesta Kyberturvallisuuskeskukselle.[4] Ota seurantaan Kyberturvallisuuskeskuksen ajankohtaiset tiedotteet.[5]
- Käy läpi hyökkäysskenaariot yrityksen johdon kanssa ja sovi käytännön toimet, johtovastuut ja -valtuudet tieturvaloukkaustilanteissa.
- Harjoittele[6] ja kehitä poikkeamanhallintasuunnitelmaa säännöllisesti kehysharjoitusten (engl. Tabletop Exercise) avulla, jossa vastuuhenkilöt ja sidosryhmät harjoittelevat tietoturvapoikkeaman käsittelyprosessia kuvitteellisessa skenaariossa.
- Harkitse organisaatiollesi kybervakuutusta, joka voi kattaa kiristyshaittaohjelmahyökkäyksestä aiheutuneita vahinkoja. Keskustele lisätiedoista tarkemmin vakuutusyhtiöiden kanssa. Älä kuitenkaan missään tapauksessa kerro julkisesti, mikäli organisaatiollasi on kybervakuutus, sillä verkkorikolliset saattavat kohdentaa hyökkäyksiä näihin organisaatioihin toivoen todennäköisempää lunnaiden maksua.

Laajemmin kyberturvallisuutta tukevat toimet

- Tunnista liiketoiminnan kannalta kriittiset komponentit, luo ja ylläpidä listoja suojattavista kohteista.
- Varmista, että organisaatiossasi ja alihankkijoillasi on käytössä jatkuva haavoittuvuuksien ja päivitysten hallinta.

[2] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari
[3] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja
[4] https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

[5] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaiset

[6] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta

- Määrittele tarkasti tarvittavat käyttöoikeudet perustuen käyttäjien ja teknisten toiminnallisuuksien tarpeisiin.
- Harkitse tietoturvavalvomopalvelun perustamista tai vastaavan palvelun ostamista. Valvomotoiminnon tarkoituksena on nimensä mukaisesti valvoa yrityksesi verkkoliikennettä ja järjestelmien tietoturvatapahtumia.

2.2 Tekniset toimet

- Varmuuskopioi kriittiset järjestelmäsi säännöllisesti ja automaattisesti 3-2-1-sääntöä noudattaen. Eli säilytä vähintään kolmea kopiota kahdessa eri muodossa ja pidä yksi näistä kopioista täysin poissa verkosta.
- Testaa varmuuskopioiden toimintaa säännöllisesti ja harjoittele varmuuskopioiden palauttamista vähintään kriittisten järjestelmien osalta.
- Hyödynnä verkkojen erottelua (engl. Network Segmentation), tietojen salausta ja pääsyn rajausta varmistaaksesi, että yrityksesi hyökkäyspinta ja kerrallaan hyökkäykselle altistuva aineisto ovat mahdollisimman pieniä.
- Pyri havaitsemaan hyökkäykset mahdollisimman ajoissa erilaisilla keskitetyillä monitorointiratkaisuilla, joiden toiminallisuutta myös testataan säännöllisesti.
- Asenna päätelaitteille haittaohjelmien torjuntaohjelmistot, joiden avulla voidaan rajoittaa ohjelmien suorittamista, tutkia epäiltyjä tietoturvaloukkauksia, ja tarpeen vaatiessa eristää tietokone verkosta.
- Ota käyttöön mekanismeja haitallista sisältöä sisältävien sähköpostien, roskapostin ja eitoivotun verkkoliikenteen suodattamiseksi.

2.3 Varautuminen ja harjoittelu käytännössä

Tärkeä osa varautumista on myös uhkaskenaarioiden harjoittelu. Harjoittelemalla alla olevaa skenaariota etukäteen, voit varmistaa, että organisaatiosi on valmis kohtaamaan kuvatun kaltaisen tilanteen. Harjoittelemalla varmistuu muun muassa, että organisaation henkilöstö ymmärtää mitä toimintaohjeen työnkulku-vuokaaviossa ja tarkistuslistassa olevat kohdat tarkoittavat, ja että heiltä löytyy valmiudet toimia kuvattujen ohjeiden mukaisesti.

Esimerkiksi skenaariona tässä tapauksessa voisi olla tilanne, jossa kiristyshaittaohjelma on lukinnut toiminnan kannalta kriittisen järjestelmän tiedostot samalla estäen järjestelmän käytön ja toiminnan. Tämä ilmenee organisaatiolle niin, että järjestelmä lakkaa toimimasta. Hyökkääjät ovat tunkeutuneet organisaatioon kalasteluviestin avulla ja onnistuneet liikkumaan saastutetun työaseman kautta kriittiseen järjestelmään käyttäen hyväksi palvelimella ollutta haavoittuvuutta. Henkilöstö ja asiakkaat kuormittavat IT- ja asiakastukea, ja paine toiminnan palauttamiselle tai vaihtoehtoisten toimintatapojen löytämiselle kasvaa.

Kuinka organisaatiossanne toimittaisiin kuvatun kaltaisessa tilanteessa? Pyrkikää harjoittelun avulla vastuuttamaan ja resursoimaan riittävästi ripeän toipumisen kannalta keskeiset neljä rinnakkaista toimintalinjaa:

1. Toipuminen takaisin normaalitilaan (palautuminen)
2. Juurisyyn selvittäminen ja lisävahinkojen estäminen (tutkinta ja korjaavat toimenpiteet).
3. Toipumisen aikaiset tilapäisratkaisut ja niiden hallittu purkaminen toipumisen jälkeen (engl. Workarounds / Stopgap Measures).
4. Viestintä reagoivan tiimin, muun henkilöstön, sidosryhmien, johdon ja julkisuuden välillä, tiedottaminen ja koordinaatio (koordinaatio).

Harjoitelkaa ainakin seuraavat vaiheet tästä toimintaohjeesta:

- Poikkeamasta ilmoittaminen ja tilanteen eskalaatio.
- Välittömästi tunnistettujen laitteiden eristäminen verkosta.
- Saastuneiden tunnusten lukitseminen ja aktiivisten istuntojen katkaisu.
- Toiminnan jatkuvuuden varmistaminen tietoturvaloukkauksen aikana.
- Haittaohjelman tunnistetietojen kerääminen ja lokianalyysi.
    - Pystytäänkö selvittämään miten ja mistä haittaohjelma on tullut?
    - Keiden käyttäjätunnukset ovat vaarantuneet?
- Kerättyjen tunnistetietojen käyttäminen muiden palvelinten ja päätelaitteiden tarkastamiseksi saastumisen varalta.
- Kalasteluviestin vastaanottajien selvitys.
    - Ketkä ovat avanneet haitallisen liitetiedoston?
- Saastuneiden järjestelmien palautus.
    - Palvelimet ja päätelaitteet. Varmuuskopioiden käyttö.
- Poikkeaman loppututkinnan prosessi.

Kaikkien harjoiteltavien tehtävien ohessa tulee pitää mielessä, kuinka organisaatio johtaa poikkeaman hallintaa, kuinka sisäinen kommunikaatio toimii ja ketkä ovat missäkin aiheessa vastuuhenkilöitä ja heidän varahenkilöitään. On suositeltavaa tutustua myös Kyberturvallisuuskeskuksen materiaaleihin liittyen harjoitustoimintaan.[7]

[7] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta

3 Tietoturvaloukkauksen havaitseminen

Hyökkäyksiä on kahta tyyppiä: kiristyshyökkäys (ransomware) ja tuhoamishyökkäys (wiperware). Vaikutukset ovat kummassakin samat: et pääse käsiksi organisaatiosi toiminnan kannalta tärkeisiin tiedostoihin tai järjestelmiin. Hyökkäys voidaan havaita esimerkiksi seuraavilla tavoilla:

- 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 muulla tavoin käyttökelvottomia.
- Tehdas- tai tuotantoympäristön laitteisto lakkaa toimimasta ilman näkyvää tai tunnistettavaa syytä.
- Tietoturvatuote tai palveluntarjoaja tuottaa hälytyksen.

Ilmoita tietoturvaloukkauksesta Kyberturvallisuuskeskukselle.[8] Neuvomme teitä luottamuksellisesti ja maksutta vahinkojen rajoittamisessa, tapahtuman analysoinnissa ja palautumistoimenpiteissä. Samalla tuette kansallisen tietoturvan tilannekuvaa ja mahdollistatte muiden mahdollisten uhrien varoittamisen.

Tutustu Kyberturvallisuuskeskuksen oppaaseen tietomurtojen havaitsemisesta.[9]

[8] https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

[9] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

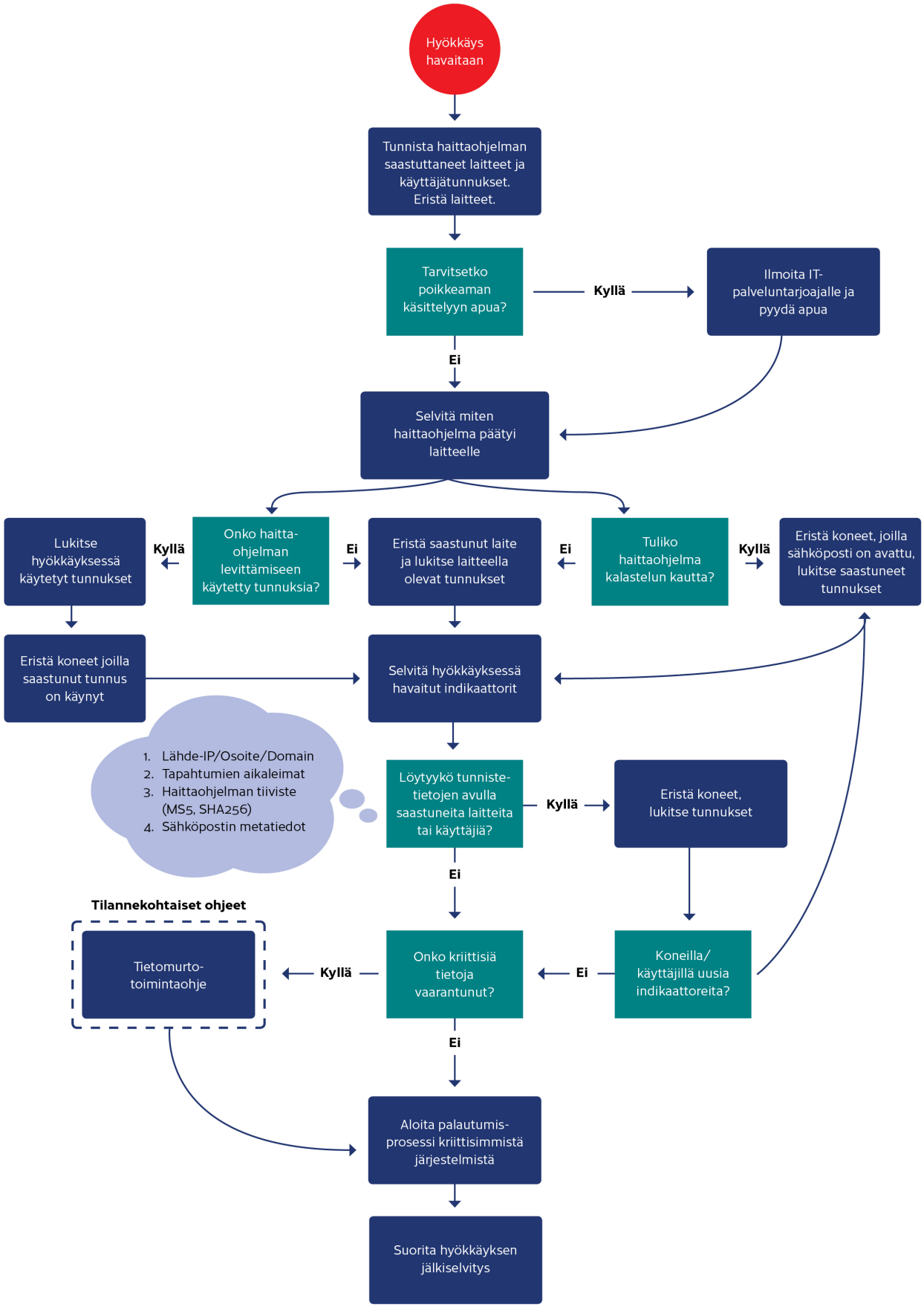
4 Toimintaohjeet

Käytä oheista toimenpiteiden tarkistuslistaa apuna, kun epäilet joutuneesi kiristyshaittaohjelman uhriksi. Tarkistuslista auttaa organisaatiota priorisoimaan ja vaiheistamaan toimintaa tietoturvapoikkeaman selvittämisessä.

4.1 Tietoturvaloukkauksen selvityksen työnkulku

Alla oleva vuokaavio kuvaa toimia, joita noudattamalla poikkeamaa voidaan selvittää oikeassa järjestyksessä. Vuokaavio tukee tarkistuslistan käyttöä. Tutkinnan aikana on myös ehdottoman tärkeää ylläpitää tarkkaa tapahtumalokia tehdyistä toimenpiteistä. Lokista tulisi käydä ilmi tehty toimenpide, aikaleima ja toimenpiteen suorittaja.

Myös mahdollinen todistusaineiston kerääminen on syytä dokumentoida huolellisesti. Ylös tulisi kirjata kuka keräsi, mitä aineistoa sekä mistä ja milloin se kerättiin. Huolellisesti laadittu tapahtumaloki helpottaa merkittävästi tutkintaa sekä yhteistyötä poliisin ja tietoturvatutkijoiden kanssa.


Hyökkäys havaitaan
Tunnista haittaohjelman saastuttaneet laitteet ja käyttäjätunnukset. Eristä laitteet.
Tarvitsetko poikkeaman käsittelyyn apua?
Kyllä
Ilmoita IT-palveluntarjoajalle ja pyydä apua
Ei
Selvitä miten haittaohjelma päätyi laitteelle
Lukitse hyökkäyksessä käytetyt tunnukset
Kyllä
Onko haitta-ohjelman levittämiseen käytetty tunnuksia?
Ei
Eristä saastunut laite ja lukitse laitteella olevat tunnukset
Ei
Tuliko haittaohjelma kalastelun kautta?
Kyllä
Eristä koneet, joilla sähköposti on avattu, lukitse saastuneet tunnukset
Eristä koneet joilla saastunut tunnus on käynyt
Selvitä hyökkäyksessä havaitut indikaattorit
1. Lähde-IP/Osoite/Domain
2. Tapahtumien aikaleimat
3. Haittaohjelman tiiviste (MS5, SHA256)
4. Sähköpostin metatiedot
Löytyykö tunniste-tietojen avulla saastuneita laitteita tai käyttäjiä?
Kyllä
Eristä koneet, lukitse tunnukset
Ei
Tilannekohtaiset ohjeet
Tietomurto-toimintaohje
Kyllä
Onko kriittisiä tietoja vaarantunut?
Ei
Koneilla/ käyttäjillä uusia indikaattoreita?
Ei
Aloita palautumis-prosessi kriittisimmistä järjestelmistä
Suorita hyökkäyksen jälkiselvitys

4.2 Välittömät toimenpiteet

Vaiheen tavoitteet	Toimenpiteiden tarkkuus ja nopeus ovat molemmat tärkeitä. Välittömien toimenpiteiden tavoite on pysäyttää haittaohjelman leviäminen, estää hyökkääjien jalansija verkossa ja alustaa palautumisprosessin aloittaminen. Älä alistu hyökkääjien kiristykseen. Lunnaiden maksaminen ei takaa, että tilanne raukeaa tai että tietoja saadaan palautettua.

Vaihe	Tarkoitus	Toimenpiteet
Tunnista saastuneet järjestelmät ja käyttäjätunnukset	Pyritään tunnistamaan kaikki palvelimet ja päätelaitteet, joille kiristyshaittaohjelma on ehtinyt levitä. Tämän lisäksi pyritään tunnistamaan myös käyttäjätunnukset, jotka ovat saattaneet päätyä hyökkääjän hallintaan.	Tunnistaaksesi saastuneet laitteet ja tunnukset, tarkista valvontatuotteistasi saastuneet tietokoneet. Tarkista käyttäjät, jotka ovat olleet kirjautuneina saastuneille laitteille, ja selvitä mihin muualle he ovat kirjautuneet. Voit tehdä tämän muun muassa Active Directoryn lokien perusteella, keskitetyn päätelaitteiden valvontatuotteen (engl. Endpoint Detection and Response) avulla, tai identiteetinhallinnan lokeista.
Eristä tunnistetut saastuneet laitteet	Tunnistettujen saastuneiden laitteiden eristämisellä kaikista tietoverkoista voidaan onnistua pysäyttämään hyökkäyksen leviäminen.	Eristä laitteet käyttämällä hyväksesi keskitetyn päätelaitteiden valvonnan ominaisuuksia. Tarpeen vaatiessa irrota laitteiden verkkoliitäntäkaapelit. Pidä laitteita päällä eristämisen jälkeen. Se mahdollistaa palauttamisen, mikäli kiristyshaittaohjelman käyttämät salausavaimet löytyvät edelleen muistista. Muistipohjainen tutkinta on myös tehokas tapa tietoturvaloukkausten selvittämiseksi.
Tunnista hyökkäyksessä käytetyt tunnukset	Usein haittaohjelmaa levitetään käyttämällä tunnuksia, joilla on laajat käyttöoikeudet (kuten ylläpitotunnukset)	Tutki päätelaitteiden valvonnasta tai saastuneiden laitteiden lokeista, miten haittaohjelma on päätynyt saastuneille laitteille. Kaikkia tunnuksia, jotka ovat kirjautuneina saastuneilla palvelimilla ja päätelaitteilla, tulee kohdella menetettyinä. Huomioi myös palvelinten ja päätelaitteiden paikalliset tunnukset ja palvelutunnukset (engl. Service Accounts), jotka ovat voineet päätyä hyökkääjän hallintaan. Hyökkääjät käyttävät usein työkaluja (esim. Mimikatz) laitteiden muistissa olevien tunnusten varastamiseksi. Nämäkin tunnukset kannattaa siis lukita.
Ota yhteyttä IT-palveluntarjoajaasi	Usein osa organisaation IT-infrastruktuurista on ulkoistettu palveluntarjoajalle. Tällöin osa tapauksen rajoittamiseen liittyvistä toimista voi vaatia apua palveluntarjoajilta.	Selvitä viimeistään tässä vaiheessa, mitä organisaatiosi IT-infrastruktuurista on ulkoistettu palveluntarjoajille. Ota yhteyttä palveluntarjoajan kriisiyhteyshenkilöön. Voit joutua pyytämään palveluntarjoajaasi muun muassa irrottamaan palvelimiasi verkoista, palauttamaan niitä tai lähettämään niistä lokeja.

		IT-palveluntarjoajilla on usein myös osaavaa henkilökuntaa, joka voi auttaa poikkeaman ratkaisussa.
Ilmoita tietoturvaloukkauksesta yhteistyökumppaneille ja sidosryhmille, joihin tapaus voi vaikuttaa	Loukkaus voi aiheuttaa yhteistyökumppaneille, asiakkaille ja palveluntarjoajille riskejä tai ongelmia palveluiden saatavuudessa. Hyökkäys toimitusketjuun voi myös vaarantaa kaikkien kumppaneiden turvallisuuden.	Ilmoita eri sidosryhmien kriisiyhteyshenkilöille tapauksesta, jos uskot että se voi vaikuttaa heidän tietoihinsa, palveluiden saatavuuteen, tai mikäli on olemassa mahdollisuus, että haittaohjelma voi levitä organisaatioiden välillä. Tapauksesta kannattaa viestiä aktiivisesti myös sisäisesti. Jos haittaohjelma on jo levinnyt laajalle, työntekijöitä voi olla hyvä ohjeistaa välttämään tietokoneidensa käynnistämistä jatkovahinkojen ehkäisemiseksi.
Arvioi tarvitsetko tietoturvaloukkauksen käsittelyyn ulkoista apua	Organisaatio voi tarvita apua toimenpiteiden organisoinnissa, loukkauksen hallinnassa ja teknisissä toimenpiteissä. Jos omasta organisaatiosta tai omalta IT-palveluntarjoajilta ei löydy riittävää osaamista, tulee harkita ulkopuolisen avun tarvetta.	Tekniset toimet poikkeaman käsittelyssä voivat vaatia ulkopuolista osaamista. Tällaisia toimia voivat olla muiden muassa tunnistetietojen kerääminen, uhan selvittäminen niiden perusteella, kiristyshaittaohjelman tyypin tunnistaminen ja saastuneiden koneiden muistianalyysi. Kyberturvallisuuskeskus voi auttaa organisaatioita erityisesti tapauksen ensivasteessa ja tarjoamalla lisätietoja vastaavista tapauksista Suomessa ja kansainvälisesti. Alaviitteessä listatuista resursseista löydät suomalaisia palveluntarjoajia.[10]
Raportoi tietoturvaloukkauksesta viranomaisille	Raportoi loukkauksesta viranomaistahoille. Organisaatiolla voi olla vastuu ilmoittaa loukkauksesta säädösten tai kybervakuutuksen velvoittamana.	Tee tapauksesta rikosilmoitus poliisille.[11] Ilmoita tapauksesta myös Kyberturvallisuuskeskukselle[12] tilannekuvan ylläpitämiseksi ja avun saamiseksi. Mikäli on uhkana, että henkilötietoja tai muita tietosuojalainsäädännön (GDPR) alaisia tietoja on päätynyt hyökkääjän käsiin, tee ilmoitus Tietosuojavaltuutetun toimistolle.[13] EU:n verkko- ja tietoturvadirektiivin (ns. NIS-direktiivi) alaisten huoltovarmuuskriittisten toimijoiden ja palveluntarjoajien tulee ilmoittaa verkko- ja tietojär-

[10] https://dfir.fi/
https://www.fisc.fi/fi
https://www.hansel.fi/yhteishankinnat/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/

[11] https://poliisi.fi/tee-rikosilmoitus

[12] https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

[13] https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta

		jestelmässä olevista tietoturva-poikkeamista valvontaviran-omaisille.[14]

[14] https://www.kyberturvallisuuskeskus.fi/fi/asioi-kanssamme/ilmoita-tietoturvapoikkeamasta-nis-ilmoitusvelvollisuus

4.3 Tietoturvaloukkauksen selvitys

Vaiheen tavoitteet	Loukkauksen selvityksen tavoitteena on selvittää hyökkäyksen laajuus ja vaikutus organisaatiossa. Huolellisella tutkinnalla varmistetaan, että haittaohjelmat, vääriin käsiin joutuneet käyttöoikeudet ja mahdolliset takaovet ovat poistettu ympäristöstä.

Vaihe	Tarkoitus	Toimenpiteet
Tunnista haitallinen toiminta ja kerää tunnistetiedot	Tunnistetietoja kerätään, jotta voidaan kartoittaa miten laajasti laitteet ovat saastuneet ja miten varastettuja käyttöoikeuksia on hyödynnetty. Jalansijan saatuaan hyökkääjä voi käyttää eri hyökkäysmenetelmiä. Tunnistetietoja tuleekin kerätä laajasti ja niiden käytön merkkejä tutkia huolellisesti, jotta ympäristön puhdistaminen voidaan tehdä luotettavasti. Vasta kun hyökkääjä on karkotettu ympäristöistä, voidaan palautuminen aloittaa.	Kerättäviä tunnistetietoja ovat muun muassa tapahtuma-ajat, esimerkiksi milloin palvelimelle on kirjauduttu, tai milloin tietty komento on ajettu palvelimella. Haittaohjelma kommunikoi usein hyökkääjän komentopalvelimen kanssa. Tarkastelemalla saastuneiden laitteiden verkkoliikennettä tai verkkotunnusten selvitystä (DNS-lokit), voidaan tunnistaa lähde-IP-osoitteet tai verkkotunnukset, joita hyökkääjä käyttää. Kun haitallisia tiedostoja tunnistetaan, voidaan niistä ottaa tiivisteet (MD5/SHA256), joiden avulla voidaan tunnistaa haitalliset tiedostot myös muilta laitteilta. Saastuneisiin laitteisiin kohdistuneista tunnistautumistapahtumista ja näihin liittyvillä käyttäjätileillä suoritetuista toimenpiteistä voidaan päätellä tunnukset, joilla haittaohjelmaa on levitetty. Keskitetystä päätelaitteiden valvonnasta löytyy usein ominaisuudet edellä mainittujen tunnistetietojen keräämiseen ja niiden käyttämiseen. Muussa tapauksessa toimet tulee tehdä käsin käyttämällä keskitettyä lokipalvelinta. Mikäli tätäkään ei ole saatavilla, tulee tutkia yksittäisten palvelinten ja päätelaitteiden lokeja. Mikäli haittaohjelma on alun perin toimitettu organisaatioon sähköpostin tai muun viestivälineen välityksellä, tulee viesteistä kerätä tunnistetietoja. Tärkeitä tietoja ovat viestien aikaleimat, aiheet, liitetiedostot, lähettäjät, vastaanottajat ja viestien sisällöt. Näiden tietojen avulla voidaan selvittää, ketkä kaikki ovat mahdollisesti vastaanottaneet haitallisen viestin ja saaneet sitä kautta haittaohjelman koneelleen.
Käytä tunnistetietoja avuksi tunnistamaan kaikki saastuneet järjestelmät	Kerättyjen tunnistetietojen avulla voidaan selvittää, kuinka laajalle hyökkääjä on päässyt tunkeutumaan organisaatiossa. Keräämällä tunnistetietoja ja hakemalla niitä kohdejärjestelmistä voidaan varmentaa, että kaikki saastuneet laitteet ja tunnukset löydetään ja siivotaan.	Tunnistetietojen avulla voidaan etsiä saastuneita laitteita, esimerkiksi käyttämällä keskitetyn päätelaitteiden valvonnan ominaisuuksia, jotka usein tarjoavat suoraan mahdollisuuden hakea eri tunnisteilla tapahtumia laitteilta. Jos organisaatiolla on käytössään myös keskitetty lokipalvelin, voidaan sieltä hakea tehokkaasti tunnisteiden perusteella tapahtumia useilta eri koneilta samanaikaisesti.

		Mikäli kumpikaan edellä mainituista ratkaisusta ei ole käytettävissä, tulee tunnisteita hakea erikseen kaikilta laitteilta. Tässä voidaan kuitenkin käyttää hyväksi erilaisia etähallintaratkaisuja, jotka usein mahdollistavat esimerkiksi PowerShell-komentojen ajamisen yhtäaikaisesti useammalla palvelimella. On olemassa riski, että hyökkääjä laitteelle päästyään on yrittänyt peittää jälkiään kytkemällä lokien keräämisen pois päältä. Tällöin laitteen lokeista ei välttämättä voida löytää kaikkia kerättyjä tunnistetietoja. Tämän vuoksi on tärkeää pyrkiä käyttämään laajaa kirjoa erilaisia tunnistetietoja ja tapahtumalähteitä.
Tallenna kaikki saatavilla olevat lokitiedostot ja muut todisteet verkosta eristetylle kovalevylle myöhempää tutkimusta varten	Todisteiden keräämisellä ja säilömisellä pyritään takaamaan laadukas tapauksen jälkitutkinta, jotta tapauksen juurisyyt saadaan selvitettyä. Todisteita voidaan tarvita rikostutkinnan yhteydessä ja oikeuskäsittelyä varten. Jos organisaatiolla on kybervakuutus, voi myös vakuutusyhtiö vaatia poikkeamasta tarkempia tietoja ja todisteita tutkintaa varten.	Tallenna verkosta eristetylle kovalevylle ne lokitiedostot, joista löytyy poikkeaman tutkinnan kannalta oleellista tietoa. Kerää myös talteen mahdolliset haitalliset sähköpostit ja muut viestit. Pyri säilyttämään todisteet, kuten kokonaiset levykuvat ja muistinäytteet, mahdollisimman eheinä. Ota niistä eheystiivisteet tämän varmistamiseksi. Pyri säilömään näytteet havaituista haittaohjelmista. Käsittelyssä tulee noudattaa suurta varovaisuutta. Turvallinen toteuttaminen vaatii usein ammattiosaamista. Lähetä näytteet Kyberturvallisuuskeskukselle.[15]

[15] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/sahkopostin-valittaminen-ja-naytteiden-lahettaminen-kyberturvallisuuskeskukselle

4.4 Palautuminen

Vaiheen tavoitteet	Aloita palautuminen liiketoiminnan kannalta kriittisimmistä järjestelmistä. Organisaation tulee pyrkiä palauttamaan liiketoiminta takaisin normaalitilaan mahdollisimman pian, mutta vasta kun palautuminen voidaan toteuttaa turvallisesti.

Vaihe	Tarkoitus	Toimenpiteet
Palauta saastuneet järjestelmät varmuuskopioista	Pyritään palauttamaan järjestelmät ja palaamaan normaalin toimintaan. Suoritetaan järjestelmien palautus mahdollisimman turvallisesti, jotta hyökkääjä ei pääsisi tunkeutumaan takaisin järjestelmiin.	Palauta järjestelmät varmuuskopioista. Ota huomioon myös riski, että aikaisemmat päiväkohtaiset (inkrementaaliset) varmuuskopiot voivat olla jo saastuneita. Palauttaessasi vanhoja varmuuskopioita ota huomioon, että varmuuskopio voi sisältää haavoittuvuuksia, joita hyökkääjä on hyväksikäyttänyt hyökkäyksessä. Riskiä voi yrittää välttää palauttamalla järjestelmät ilman verkkoyhteyksiä ja päivittämällä käyttöjärjestelmä ja sen sovellukset ennen verkkoon kytkemistä. Mikäli sopivaa varmuuskopiota ei ole saatavilla, asenna käyttöjärjestelmä ja sen sovellukset kokonaan alusta. Huomioi myös edellisessä kappaleessa mainitut riskitekijät. Älä pyri puhdistamaan saastunutta järjestelmää automaattisilla työkaluilla tai haittaohjelmien torjunnalla, sillä ei ole takeita, että ne kykenevät puhdistamaan järjestelmän täydellisesti. Säilytä salatut tiedostot tai kovalevyt siltä varalta, että myöhemmin löytyy keino avata ne. Tarkasta järjestelmät haittaohjelmien torjunnan työkaluilla ennen niiden kytkemistä takaisin verkkoon.
Palauta saastuneet tunnukset ja varmenna järjestelmänvalvojatunnusten turvallisuus.	Varmistetaan, että kaikkien saastuneiden tunnusten kirjautumistiedot vaihdetaan, jotta hyökkääjällä ei olisi enää pääsyä tunnusten avulla organisaation järjestelmiin. Vahvennetaan käyttäjien kirjautumisvaatimuksia, mikäli vain mahdollista.	Vaihda saastuneiden tunnusten salasanat ja ota tunnukset takaisin käyttöön. Vaihda varmuuden vuoksi ylläpitotunnusten ja palvelutunnusten salasanat siltä varalta, että osa niistä on joutunut hyökkääjien käsiin. Toimita uudet salasanat käyttäjille joko suullisesti, tekstiviestillä tai soittamalla. Älä käytä organisaation sähköpostia tai pikaviestimiä, sillä hyökkääjällä saattaa edelleen olla niihin pääsy. Harkitse kaksivaiheisen tunnistautumisen käyttöönottoa ylläpitotunnuksille sekä niille tunnuksille, joita oli hyväksikäytetty hyökkäyksen aikana. Valvo myös tarkemmin hyökkäyksessä käytettyjä tunnuksia palauttamisen jälkeen siltä varalta, että hyökkääjä saa ne uudelleen käsiinsä. Mikäli organisaatiolle jää epäselväksi, miten hyökkääjä oli saanut tietyt tunnukset käsiinsä, harkitse täysin uusien tunnusten luomista.

		Näin varmistut, että hyökkääjä ei saa tunnuksia uudelleen haltuunsa tällä tuntemattomaksi jääneellä tavalla. Mikäli organisaatiolla on käytössään Active Directory ja on epäilys, että hyökkääjä on jossakin vaiheessa saanut haltuunsa koko domainin, vaihda myös KRBTGT-tunnuksen salasana kahdesti ns. Golden Ticketin vanhentamisesi. Uudelleen provisioi myös Active Directoryn Varmennepalvelu (engl. Certificate Services), siltä varalta, että hyökkääjä on saanut haltuunsa varmennepalvelusta varmenteita, joita voidaan käyttää tunnistautumiseen.

5 Tietoturvaloukkauksen jälkiselvitys

Kriisin päätyttyä ja liiketoimintojen normalisoiduttua on tärkeää käynnistää hyökkäyksen jälkiselvitys ja oppia tapahtuneesta tulevaisuutta varten. Samalla kriisinhallintasuunnitelmat on syytä päivittää tehtyjen havaintojen mukaan. On mahdollista, että organisaatio joutuu uudelleen vastaavan hyökkäyksen uhriksi, mikäli tapahtuneen juurisyyt eivät selviä eikä tapauksesta oteta opiksi.

Jälkiselvityksessä (engl. Post Incident Review) tarkastellaan toimintaa kriisitilanteessa: mitkä toimet tehtiin hyvin, missä oli parantamisen varaa ja kuinka voidaan parantaa turvallisuustasoa ja -suunnitelmia. Jälkiselvityksestä on syytä laatia raportti, joka tarkastelee tapahtumien kulun lisäksi ainakin seuraavia kysymyksiä:

- Tapahtuman juurisyyt:
    - Mitkä tekniset tai toiminnalliset heikkoudet johtivat tilanteeseen?
- Oman suojauksen tehokkuus:
    - Olivatko hyökkäyksien havaitsemista varten käytetyt kontrollit riittäviä?
    - Aiheuttivatko hyökkääjän toimet hälytyksiä?
    - Miten hälytyksiin reagoitiin? Välittyikö tieto hälytyksistä oikeille vastuuhenkilöille?
- Toiminta kriisitilanteessa:
    - Noudatettiinko kriisisuunnitelmaa? Miten käyttökelpoinen se oli?
    - Jaettiinko kriisiryhmän vastuut oikeille henkilöille?
    - Miten hyökkäyksen rajaamisessa ja hyökkääjän karkottamisessa onnistuttiin?
    - Kuinka kriisiryhmän viestintä onnistui? Miten sidosryhmät huomioitiin?
- Palautuminen:
    - Miten kriittisten tietojen ja palveluiden palautuminen onnistui?
- Jälkiselvitys:
    - Onko tapahtumien kulku ja selvitystyö dokumentoitu?
    - Oliko tapauksen tekninen tutkinta riittävää? Onko esim. viranomaisten käyttöön voitu toimittaa riittävät aineistot hyökkäyksestä?
    - Arvioi palvelutoimittajien toimintaa. Oliko vasteaika ja sovitut palvelut riittäviä tapauksen selvittämistyötä varten?

Organisaation tulee päivittää omaa poikkeamanhallintasuunnitelmaansa ja tarkempia erilaisten poikkeamien torjuntaan suunniteltuja pelikirjoja tapahtuneen jälkeen. On myös suositeltavaa harjoitella eri skenaarioita säännöllisin väliajoin, jotta niiden hyöty kriisitilanteissa voidaan varmistaa.

Kyberturvallisuuskeskus toivoo, että yritykset ja organisaatiot jakaisivat sillekin tärkeimmät poikkeamasta saamansa opit. Tapausraporttien avulla Kyberturvallisuuskeskus voi auttaa muita organisaatioita Suomessa ja kansainvälisesti vastaavien tapauksen selvittämisessä. Palautumisesta saadut opit auttavat kehittämään kaikkien organisaatioiden varautumista.

HUOLTOVARMUUSKESKUS

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-815-7

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus