TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Toimintaohje – Tietomurto

Traficomin julkaisuja
24/2022

Sisällysluettelo

1 Johdanto

1.1 Ohjeen tarkoitus

Tämän Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen laatiman ohjeen tarkoituksena on neuvoa organisaatioita tilanteissa, joissa epäillään tietomurtoa. 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 tietomurto

Tietomurto tarkoittaa luvatonta tunkeutumista tietojärjestelmään, palveluun tai laitteeseen tai sovelluksen luvatonta käyttöä haltuun saatujen tunnusten avulla. Usein tietomurrolla pyritään saamaan taloudellista hyötyä esimerkiksi varastamalla tietoja, joita voidaan myydä eteenpäin. Joskus murtautuja ei itse varasta mitään, vaan myy pääsyn palvelimelle jollekin toiselle rikolliselle. Murrettua ympäristöä voidaan käyttää myös haitallisen materiaalin jakamiseen tai murretun ympäristön toiminta voidaan lamauttaa kiristyshaittaohjelmilla. Hyökkääjä voi käyttää murtamaansa ympäristöä osana muita hyökkäyksiä esimerkiksi palvelunestohyökkäyksissä.

Tietomurrot aiheuttavat taloudellisia tappioita ja mainetappioita kohteena olevalle organisaatiolle. Lisäksi organisaation normaali toiminta voi estyä pidemmäksikin aikaa korjauksista tai ympäristön uudelleenasennuksista johtuen. Tietomurtoja käytetään myös laskutuspetoksiin (engl. Business email compromise), joissa taloudelliset menetykset voivat olla merkittäviä. Tietomurron kohteeksi joutuneen organisaation tapauksessa väärennetty lasku lähetetään tavallisista toimitusjohtajahuijauksista poiketen organisaation sisältä, ja siksi se hyväksytään todennäköisemmin.

Joskus tietomurron hyväksikäyttö voi tapahtua kauan itse murtautumisen jälkeen. Tässä tapauksessa organisaatiolla ei välttämättä ole enää käytössä lokitietoja murtautumisen ajalta, mikä vaikeuttaa loukkauksen selvitystä huomattavasti.

2 Varautuminen

Varautuminen poikkeamiin on keskeinen tapa vähentää poikkeamien vakavuutta ja mahdollistaa nopea toipuminen ja liiketoiminnan jatkuminen. Organisaatio voi arvioida omaa valmiuttaan käyttämällä hyväksi esimerkiksi Kyberturvallisuuskeskuksen Kybermittaria.[1] Etukäteen laadittu poikkeamanhallintasuunnitelma antaa hyvät lähtökohdat toimia, kun poikkeamatilanne tapahtuu. Organisaation tulee myös varmistaa, että toimet kuten käyttäjätunnusten lukitseminen, palvelinten ja päätelaitteiden eristäminen verkosta, sekä verkkoliikenteen rajoittaminen haitallisiin IP-osoitteisiin tai verkkotunnuksiin on teknisesti mahdollista ja henkilöstöltä löytyy tähän myös osaaminen.

Lokitietojen kerääminen, kokoaminen ja monitorointi on tärkeää poikkeaman havaitsemiseksi ajoissa. Lokitiedot mahdollistavat myös poikkeaman perusteellisen tutkimisen ja täten nopeuttavat mahdollista ympäristön siivousta sekä palauttamista. Kyberturvallisuuskeskus on laatinut lokitietojen keräämisestä ja käyttämisestä oppaan.[2] Riippuen organisaation käyttämistä järjestelmistä, kattavaan havainnointiin vaaditaan tyypillisesti lisäksi verkko- ja järjestelmätason ratkaisuja.

2.1 Hallinnolliset toimet

- Laadi organisaatiollesi poikkeamanhallintasuunnitelma tietomurtoa varten.
- Kouluta henkilöstöä toimimaan tämän toimintaohjeen kaltaisen tietoturvaloukkauksen aikana.
- Selvitä etukäteen, miten voit ilmoittaa tietoturvaloukkauksesta Kyberturvallisuuskeskukselle.[3] Ota seurantaan Kyberturvallisuuskeskuksen ajankohtaiset tiedotteet.[4]
- Käy läpi hyökkäysskenaariot yrityksen johdon kanssa ja sovi käytännön toimet sekä johtovastuut ja -valtuudet tieturvaloukkaustilanteissa.
- Harjoittele[5] ja kehitä poikkeamanhallintasuunnitelmaa säännöllisesti kehysharjoitusten (engl. Tabletop Exercise) avulla, jossa vastuuhenkilöt ja sidosryhmät harjoittelevat tietoturvapoikkeaman käsittelyprosessia kuvitteellisessa skenaariossa.
- Ota käyttöön jatkuva haavoittuvuuksien ja päivitysten hallinta.
- Tunnista liiketoiminnan kannalta kriittiset komponentit ja luo sekä ylläpidä listoja suojattavista kohteista.
- 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.

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

- Testaa varmuuskopioiden toiminta säännöllisesti ja harjoittele varmuuskopioiden palauttamista vähintään kriittisten järjestelmien osalta.
- Hyödynnä verkkojen erottelua (engl. Network Segmentation), tietojen salausta sekä pääsyn rajausta varmistaaksesi, että yrityksesi hyökkäyspinta ja kerrallaan hyökkäykselle altistuva aineisto ovat mahdollisimman pieniä.
- Pyri havaitsemaan hyökkäykset mahdollisimman ajoissa erilaisilla keskitetyillä monitorointiratkaisuilla, joiden toiminnallisuutta myös testataan säännöllisesti.
- Asenna päätelaitteille haittaohjelmien torjuntaa varten ohjelmistot (engl. Endpoing Detection and Response, EDR), joiden avulla voidaan rajoittaa ohjelmien suorittamista, tutkia epäiltyjä tietoturvaloukkauksia sekä tarpeen vaatiessa eristää tietokone verkosta.
- Ota käyttöön mekanismeja haitallista sisältöä sisältävien sähköpostien, roskapostin ja ei-toivotun verkkoliikenteen suodattamiseksi.
- Ota käyttöön keskitetty lokienhallinta tehokkaan kyberuhkien havainnoinnin ja tutkinnan mahdollistamiseksi.

3 Tietoturvaloukkauksen havaitseminen

Hyökkäyksen havaitsemisen mahdollisuudet riippuvat suuresti tavasta, jolla hyökkääjä on päässyt tunkeutumaan järjestelmään. Tunkeutuminen on voinut tapahtua esimerkiksi hyödyntämällä palvelimella ollutta haavoittuvuutta, konfiguraatiovirhettä, sovelluksen haavoittuvuutta tai hyökkääjä on saattanut saada haltuunsa palvelimelle sopivat tunnukset esimerkiksi kalastelemalla.

Hyökkäys voidaan havaita esimerkiksi seuraavilla tavoilla:

- Järjestelmä lakkaa toimimasta tai ei ole saatavilla.
- Järjestelmässä on suoritettu odottamattomia toimenpiteitä, joita kukaan työntekijä ei usko tehneensä.
- Tietoturvatuote tai palveluntarjoaja tuottaa hälytyksen.
- Organisaatio saa ilmoituksen hyökkäyksestä organisaation ulkopuolelta esim. sosiaalisen median, asiakkaan, yhteistyökumppanin tai viranomaisten välityksellä.
- Järjestelmästä paljastuu vakava haavoittuvuus ja korjauksen yhteydessä havaitaan, että haavoittuvuutta on jo hyväksikäytetty.
- Hyökkääjä yrittää kiristää organisaatiota varastetuilla tiedoilla.

Ilmoita tietoturvaloukkauksesta Kyberturvallisuuskeskukselle.[6] Neuvomme teitä luottamuksellisesti ja maksutta vahinkojen rajoittamisessa, tapahtuman analysoinnissa sekä palautumistoimenpiteissä. Samalla tuette kansallisen tietoturvan tilannekuvaa ja mahdollistatte muiden mahdollisten uhrien varoittamisen ja auttamisen.

Tutustu Kyberturvallisuuskeskuksen oppaaseen tietomurtojen havaitsemisesta.[7]

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

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

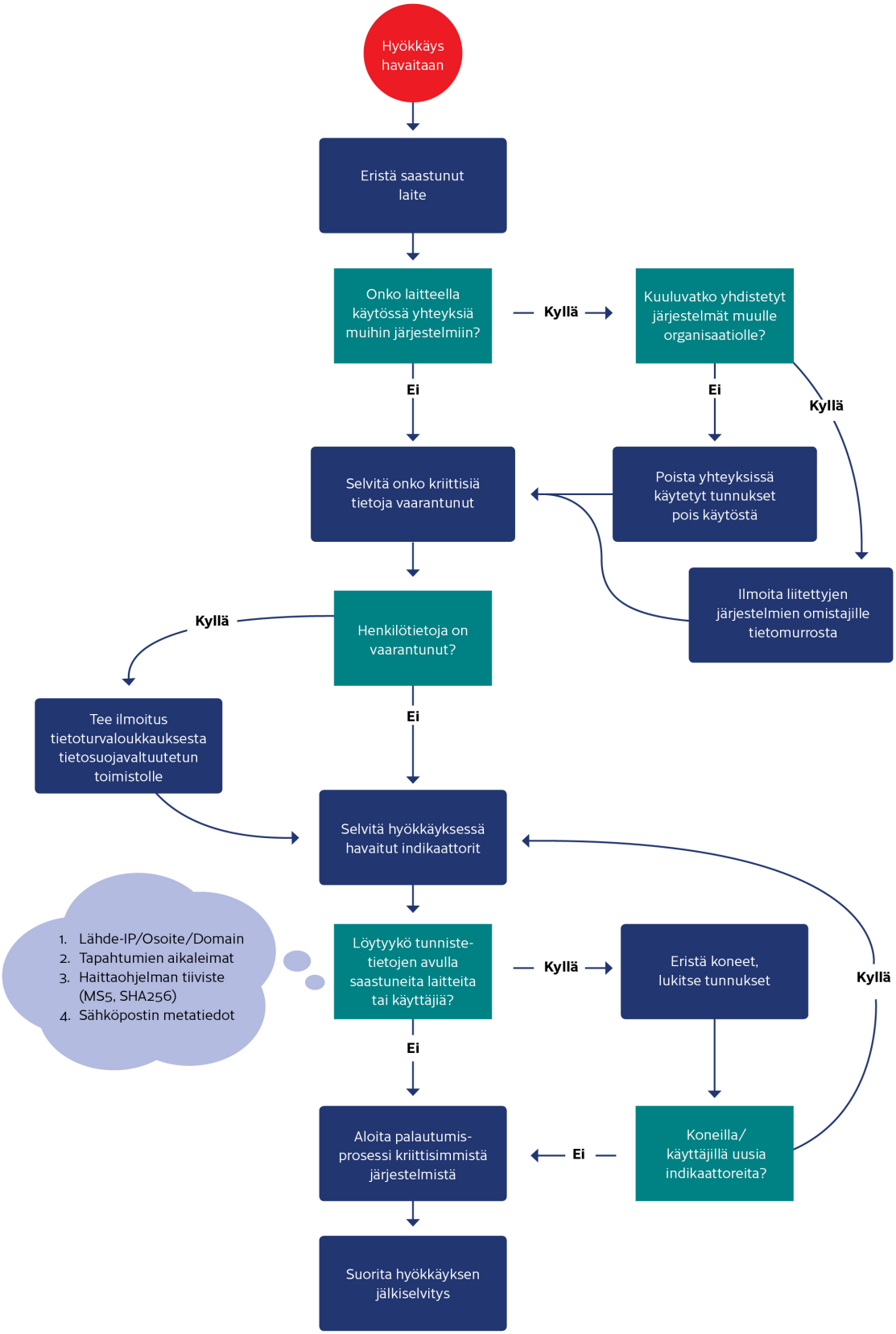
4 Toimintaohjeet

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

4.1 Tietoturvaloukkauksen selvityksen työnkulku

Alla oleva vuokaavio kuvaa toimia, joita noudattamalla loukkausta 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 tutkintaa sekä yhteistyötä poliisin ja tietoturvatutkijoiden kanssa merkittävästi.


Hyökkäys havaitaan
Eristä saastunut laite
Onko laitteella käytössä yhteyksiä muihin järjestelmiin?
Kyllä
Kuuluvatko yhdistetyt järjestelmät muulle organisaatiolle?
Ei
Kyllä
Ei
Kyllä
Selvitä onko kriittisiä tietoja vaarantunut
Poista yhteyksissä käytetyt tunnukset pois käytöstä
Ilmoita liitettyjen järjestelmien omistajille tietomurrosta
Kyllä
Henkilötietoja on vaarantunut?
Tee ilmoitus tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle
Ei
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
Kyllä
Ei
Aloita palautumis-prosessi kriittisimmistä järjestelmistä
Ei
Koneilla/ käyttäjillä uusia indikaattoreita?
Suorita hyökkäyksen jälkiselvitys

4.2 Välittömät toimenpiteet

Vaiheen tavoitteet	Toimenpiteiden tarkkuus ja nopeus ovat molemmat tärkeitä. Välittömien toimenpiteiden tavoite on suojata ympäristön kriittiset tiedot, pysäyttää haittaohjelman leviäminen, estää hyökkääjien jalansija verkossa sekä alustaa palautumisprosessin aloittaminen.

Vaihe	Tarkoitus	Toimenpiteet
Eristä saastunut laite	Eristämällä saastunut laite muista tietoverkoista pyritään estämään hyökkäyksen eteneminen sekä suojelemaan järjestelmän tietoja.	Eristä laite käyttämällä hyväksi keskitetyn päätelaitteiden valvonnan ominaisuuksia. Tarpeen vaatiessa irrota laitteen verkkoliitäntäkaapelit. Eristyksen pitää myös estää laitteen pääsy Internetiin, jotta voidaan estää hyökkääjän mahdollisuus varastaa palvelimelta tietoja.
Ota yhteyttä IT-palveluntarjoajaasi	Usein osa organisaation IT-infrastruktuurista on ulkoistettu palveluntarjoajalle. Osa tapauksen rajoittamiseen liittyvistä toimista voi vaatia apua palveluntarjoajilta.	Ota yhteyttä palveluntarjoajan kriisiyhteyshenkilöön. Voit joutua pyytämään muun muassa palveluntarjoajaasi irrottamaan palvelimiasi verkoista, palauttamaan niitä tai lähettämään niistä lokeja. IT-palveluntarjoajille on usein myös osaavaa henkilökuntaa, jotka voivat auttaa tilanteen ratkaisemisessa.
Selvitä palvelimella käytössä olleet yhteydet	Usein palvelimilla on käytössä yhteyksiä muihin järjestelmiin. Näitä voivat olla esimerkiksi tietokantayhteys tai erilaiset API-kutsut ja -avaimet. Yhdistettyjen järjestelmien eheys tulee varmistaa ensi tilassa, jotta voidaan ymmärtää tilanteen vakavuus.	Mikäli palvelimella on käytössä yhteyksiä muihin järjestelmiin, varmista tietojen eheys tarkastelemalla yhdistettyjen järjestelmien lokeja. Varmistettavia asioita voivat olla esimerkiksi tehtyjen tietokantahakujen koko tai rajapintakutsujen suuri määrä siltä ajalta, kun hyökkääjä on ollut palvelimella. Vaihda yhdistettyjen palveluiden tunnukset, kuten tietokantatunnus, joka oli käytössä saastuneella palvelimella ja rajapinta-avaimet sekä varmenteet, joita yhteyksiin on käytetty.
Ilmoita tietoturvaloukkauksesta niille yhteistyökumppaneille ja sidosryhmille, joihin tapaus voi vaikuttaa	Loukkaus voi aiheuttaa yhteistyökumppaneille, asiakkaille ja palveluntarjoajille riskejä tai ongelmia palveluiden saatavuudessa.	Ilmoita eri sidosryhmien kriisiyhteyshenkilöille tapauksesta, mikäli uskotte sen voivan vaikuttaa heidän palveluidensa saatavuuteen. Mikäli palvelimella on ollut käytössä yhteyksiä muihin organisaatioihin, ilmoita myös heille. Näin he voivat mitätöidä tunnukset, avaimet tai varmenteet, joita on ollut käytössä saastuneella palvelimella. On myös tärkeää, että he tarkastavat omien tietojensa eheyden.
Arvioi, tarvitsetko tietoturvaloukkauksen käsittelyyn ulkoista apua	Organisaatio voi tarvita apua teknisissä toimenpiteissä, poikkeaman hallinnassa ja toimenpiteiden organisoinnissa. Mikäli sisäisesti tai suoraan IT-palveluntarjoajilta ei löydy riittävää osaamista, tulee harkita ulkopuolisen avun tarvetta.	Tekniset toimet loukkauksen käsittelyssä voivat vaatia ulkopuolista osaamista. Ulkopuolista osaamista voivat vaatia esimerkiksi tunnistetietojen kerääminen ja uhan selvittäminen niiden perusteella. Ulkopuolinen apu voi myös esimerkiksi auttaa tarkastamaan, onko hyökkääjä saanut käsiinsä liiketoiminnan

		kannalta tärkeää dataa, ja jos on, niin mitä. Kyberturvallisuuskeskus voi auttaa organisaatioita erityisesti tapauksen ensivasteessa ja tarjoamalla lisätietoja vastaavista tapauksista Suomessa ja kansainvälisesti. Alaviitteessä listatuista resursseista löydät suomalaisia palveluntarjoajia.[8]
Tee ilmoitus tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle	Mikäli on uhkana, että henkilötietoja on päätynyt hyökkääjän käsiin osana tietomurtoa, on tapauksesta ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun organisaatio on saanut tietää tietoturvaloukkauksesta.	Tee välittömästi alustava ilmoitus henkilötietojen tietoturvaloukkauksesta, sillä ilmoitusta voi täydentää vielä myöhemmin. Rekisterinpitäjän täytyy arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu sen kohteena olleille henkilöille. Riskin taso määrittää ne toimenpiteet, joihin rekisterinpitäjän on myöhemmin ryhdyttävä. Dokumentoi kaikki henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet. Dokumentointivelvollisuuden piiriin kuuluvat myös tietojärjestelmään kohdistuneen tietoturvaloukkauksen osalta tapahtuma-ajan lokitiedot. Tietosuojavaltuutettu voi pyytää lokitietoja tietoturvaloukkausta koskevan ilmoituksen käsittelyä varten.
Raportoi poikkeama myös muille viranomaisille	Raportoi poikkeamasta viranomaistahoille. Organisaatiolla voi olla vastuu ilmoittaa poikkeamasta säädösten tai kybervakuutuksen ehtojen velvoittamana.	Tee tapauksesta rikosilmoitus Poliisille.[9] Ilmoita tapauksesta myös Kyberturvallisuuskeskukselle[10] tilannekuvan ylläpitämiseksi ja avun saamiseksi. EU:n verkko- ja tietoturvadirektiivin (ns. NIS-direktiivi) alaisten huoltovarmuuskriittisten toimijoiden ja palveluntarjoajien pitää ilmoittaa verkko- ja tietojärjestelmässä olevista tietoturvapoikkeamista viranomaisille.[11]

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

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

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

[11] 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. Perinpohjaisella tutkinnalla varmistetaan, että haittaohjelmat ja mahdolliset takaovet ovat siivottu 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-aika, kuten 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.
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 mahdollisuuden hakea laitteilta tapahtumia eri tunnisteilla. Mikäli organisaatiolla on käytössään myös keskitetty lokienhallinta, voidaan sen avulla tehokkaasti etsiä 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 vielä 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.
Selvitä onko kriittisiä tietoja vaarantunut	Osana tutkimusta tulee selvittää, onko hyökkääjä päässyt käsiksi organisaation tärkeisiin tietoihin, tai mahdollisesti asiakkaiden tai työntekijöiden henkilötietoihin.	Selvitä onko yhteyksissä käytetyillä tunnuksilla, varmenteilla tai avaimilla kirjauduttu muualta kuin palvelimelta, jolla niitä kuuluu käyttää. Selvitä onko hyökkääjä päässyt käsiksi tietoihin ja varastanut niitä tarkastelemalla tietokannan tai rajapinnan lokeja. Tehdyistä hauista tai kuormituksesta voit päätellä, onko hyökkääjä pyrkinyt noutamaan tietoja. Tarkista verkkolaitteiden lokeista onko saastuneen palvelimen liikenteessä poikkeamia. Poikkeuksellisen runsas liikenne voi viitata esimerkiksi siihen, että hyökkääjä on onnistunut varastamaan tietoja. Huomaa, että vaikka hyökkääjä ei olisi tuhonnut tai varastanut tietoja, hän on saattanut muokannut sitä. Hyökkääjä on saattanut myös varastaa kooltaan pientä, mutta merkityksellistä dataa, kuten tunnuksia.
Tallenna kaikki saatavilla olevat lokitiedostot sekä 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 rikosilmoituksen yhteydessä ja oikeuskäsittelyä varten. Jos organisaatiolla on kybervakuutus, voi myös vakuutusyhtiö vaatia poikkeamasta tarkempia tietoja ja todisteita tutkintaa varten.	Tallenna lokitiedostot, joista löytyy poikkeaman tutkinnan kannalta oleellista tietoa, verkosta eristetylle kovalevylle. 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.[12]

[12] 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 normaaliksi mahdollisimman pian, mutta vasta kun palautuminen voidaan toteuttaa turvallisesti.

Vaihe	Tarkoitus	Toimenpiteet
Palauta saastuneet järjestelmät varmuuskopioista	Pyritään palauttamaan järjestelmät takaisin toimintaan ja palaamaan normaalin toimintaan. Järjestelmien palautus pyritään suorittamaan 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 uudelleen. Huomioi myös edellisessä kappaleessa mainitut riskitekijät. Älä pyri puhdistamaan saastunutta järjestelmää automaattisilla työkaluilla tai haittaohjelman torjuntaohjelmistoilla, sillä ne eivät välttämättä kykene puhdistamaan järjestelmää täydellisesti. Tarkasta järjestelmät haittaohjelmien torjuntaohjelmistolla ennen niiden kytkemistä takaisin verkkoon.
Palauta saastuneet tunnukset ja varmenna järjestelmänvalvojatunnusten turvallisuus.	Varmistetaan, että kaikkien mahdollisesti saastuneiden tunnusten kirjautumistiedot vaihdetaan, jotta hyökkääjällä ei olisi enää pääsyä tunnusten avulla organisaation järjestelmiin. Kovennetaan käyttäjien kirjautumisvaatimuksia, mikäli 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.

Palauta saastuneet tietueet	Jos hyökkääjän epäillään muokanneen tietokannan sisältöä, tulee tietokanta palauttaa varmuuskopiosta hyökkääjän muutosten mitätöimiseksi, mikäli tietoja ei ole mahdollista puhdistaa.	Käytä hyväksesi tietokannan ja rajapintojen lokeja selvittääksesi, onko hyökkääjä muokannut tietueita. Jos lokien tarkkuus ei riitä muokkausten siivoamiseen, palauta tietokannan tiedot viimeisimpään turvalliseen varmuuskopioon. Mikäli hyökkääjä on varastanut tietoja, tulee kaikki varastetuissa tiedoissa olleet salasanat vaihtaa. Näin tulee myös toimia, vaikka salasanat olisikin säilötty vain tiivisteinä. Ilmoita henkilöille, joiden tiedot ovat vaarantuneet murron yhteydessä, jotta he voivat itse varautua tietojensa mahdolliseen väärinkäyttöön. Ilmoita myös, että tietoja on jouduttu palauttamaan vanhempaan versioon tietystä päivämäärästä alkaen, jotta asianomaiset voivat päivittää tietonsa ajan tasalle.

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.

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

kyberturvallisuuskeskus.fi

ISBN 978-952-311-816-4

HUOLTOVARMUUSKESKUS

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus