TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Toimintaohje – Toimitusketjuhyökkäys

Traficomin julkaisuja
21/2022

Sisällysluettelo

1 Johdanto

1.1 Ohjeen tarkoitus

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

Toimitusketjuhyökkäyksessä organisaation tietojärjestelmiin murtaudutaan sen käyttämien verkostojen, palveluiden, tuotteiden tai avoimen lähdekoodin projektien kautta. Hyökkäyksessä hyväksikäytetään organisaatioiden luottamusta toimittajiinsa. Hyökkäyksen reittinä voivat olla yhteistyökumppanit, palveluntarjoajat, ohjelmistot tai laitteet. Hyökkääjä tunkeutuu toimittajan järjestelmiin ja saastuttaa toimitusketjussa käytetyn osan omalla haittakoodillaan, jonka jälkeen se leviää normaalia tuotteen jakelukanavaa pitkin yhteistyö- ja asiakasorganisaatioihin.

Toimitusketjuhyökkäyksen tavoitteena on jalansijan saavuttaminen eri organisaatioissa toimitusketjun varrella. Kun jalansija on varmistettu, voidaan sitä käyttää erilaisiin jatkohyökkäyksiin, kuten tietomurtoihin ja kiristyshaittaohjelmahyökkäyksiin.

Toimitusketjuhyökkäyksen havainnointi ja hallinta ovat tärkeitä, koska niillä on suuri merkitys organisaation maineelle ja luottamukselle verkostossa. Toimitusketjuhyökkäyksen uhrina ovat sekä toimittaja että asiakas. Tilanteen hallinta vaatii usein avoimuutta ja yhteistyötä osapuolilta.

2 Varautuminen

Varautuminen poikkeamiin on hyvä tapa vähentää poikkeaman 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 ja 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 ympäristön siivousta ja 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 toimitusketjuhyökkäystä varten.
- Kouluta henkilökuntaa toimimaan tämän toimintaohjeen kaltaisen poikkeaman 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 johto-vastuut 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, luo ja ylläpidä listoja suojattavista kohteista.
    - Ylläpidä kriittisimpien järjestelmien komponenttilistaa.
- Ylläpidä listaa organisaation käyttämistä lisensseistä, ohjelmistoista ja niiden versioista.
    - Seuraa niiden päivitysaikatauluja ja haavoittuvuuksia.
- Määrittele tarkasti tarvittavat käyttöoikeudet perustuen käyttäjien ja teknisten toiminnallisuuksien tarpeisiin.
- Arvioi toimittajien kyberturvallisuuden tila. Varmistaessasi, että jokainen toimittaja antaa täydellisen kuvauksen turvatoimistaan, saat käsityksen heidän tuotteidensa turvallisuudesta. Voit myös pyytää kyberturva-ammattilaista tutkimaan toimittajien antamat tiedot nähdäksesi, ovatko turvallisuusratkaisut asianmukaisia ja riittäviä.

[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

- 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 verkon segmentointia, tietojen salausta sekä pääsyn rajausta varmistaaksesi, että yrityksesi hyökkäyspinta on mahdollisimman pieni.
- Suojaa yhteistyökumppaneiden yhteydet vahvoilla salausasetuksilla ja ota monivaiheinen tunnistautuminen käyttöön.
- Pyri havaitsemaan hyökkäykset mahdollisimman ajoissa erilaisilla keskitetyillä monitorointiratkaisuilla, joiden toiminallisuutta myös testataan säännöllisesti.
- Asenna päätelaitteille haittaohjelmien torjuntaa varten ohjelmistot, 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.
- Keskitetty lokienhallinta tulee ottaa käyttöön tehokkaan kyberuhkien havainnoinnin ja tutkinnan mahdollistamiseksi.

3 Tietoturvaloukkauksen havaitseminen

Toimitusketjun kautta realisoituneen tietoturvaloukkauksen havaitseminen voi olla haastavaa, sillä hyökkääjä käyttää hyväkseen organisaation luottamusta yhteistyökumppaneihin. Usein tunkeutuminen tapahtuu käyttämällä yhteistyökumppaneiden yhteyksiä tai saastuttamalla heidän tarjoamansa sovelluksen. Tällöin hyökkääjä ei vielä tunkeutumisvaiheessa tee mitään epäilyttäväksi tai haitalliseksi tulkittavaa.

Hyökkäys voidaan havaita esimerkiksi seuraavilla tavoilla:

- Yhteistyökumppani ilmoittaa joutuneensa kyberhyökkäyksen uhriksi.
- Yhteistyökumppaneiden tunnuksilla pyritään kirjautumaan palveluihin, joihin he normaalisti eivät kirjautuisi.
- Tietoturvatuote tai palveluntarjoaja tuottaa hälytyksen, jonka aiheuttaa yleensä luotettu sovellus.
- Organisaatio saa ilmoituksen hyökkäyksestä organisaation ulkopuolelta esimerkiksi sosiaalisen median, asiakkaan, yhteistyökumppanin tai viranomaisten välityksellä.

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

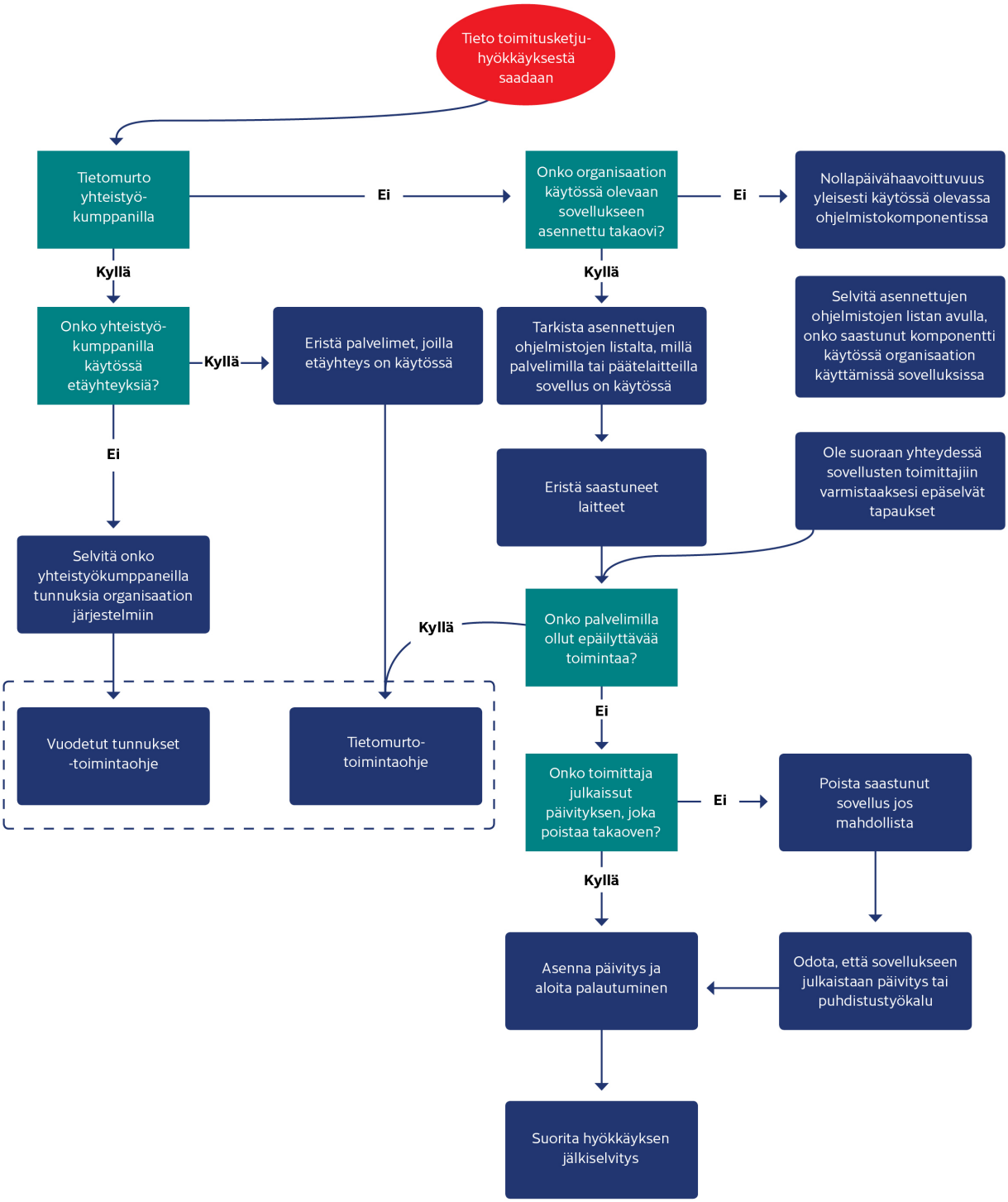
4 Toimintaohjeet

Käytä oheista toimenpiteiden tarkistuslistaa apuna, kun epäilet joutuneesi toimitusketjuhyökkäyksen 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. Selvityksen 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 tulee kirjata kuka keräsi, mitä aineistoa, mistä ja milloin se kerättiin. Huolellisesti laadittu tapahtumaloki helpottaa tutkintaa sekä yhteistyötä poliisin ja tietoturvatutkijoiden kanssa merkittävästi.


Tieto toimitusketju-hyökkäyksestä saadaan
Tietomurto yhteistyö-kumppanilla
Ei
Onko organisaation käytössä olevaan sovellukseen asennettu takaovi?
Ei
Nollapäivähaavoittuvuus yleisesti käytössä olevassa ohjelmistokomponentissa
Kyllä
Kyllä
Onko yhteistyö-kumppanilla käytössä etäyhteyksiä?
Kyllä
Eristä palvelimet, joilla etäyhteys on käytössä
Tarkista asennettujen ohjelmistojen listalta, millä palvelimilla tai päätelaitteilla sovellus on käytössä
Selvitä asennettujen ohjelmistojen listan avulla, onko saastunut komponentti käytössä organisaation käyttämissä sovelluksissa
Ei
Eristä saastuneet laitteet
Ole suoraan yhteydessä sovellusten toimittajiin varmistaaksesi epäselvät tapaukset
Selvitä onko yhteistyökumppaneilla tunnuksia organisaation järjestelmiin
Kyllä
Onko palvelimilla ollut epäilyttävää toimintaa?
Ei
Vuodetut tunnukset -toimintaohje
Tietomurto-toimintaohje
Onko toimittaja julkaissut päivityksen, joka poistaa takaoven?
Ei
Poista saastunut sovellus jos mahdollista
Kyllä
Asenna päivitys ja aloita palautuminen
Odota, että sovellukseen julkaistaan päivitys tai puhdistustyökalu
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 laitteet käyttämällä hyväksesi keskitetyn päätelaitteiden valvonnan ominaisuuksia. Tarpeen vaatiessa irrota laitteiden verkkoliitäntäkaapelit. Eristyksen pitää myös estää laitteen pääsy Internetiin, jotta voidaan estää hyökkääjän mahdollisuus varastaa palvelimelta tietoja.
Selvitä hyökkäyksessä käytetty yhteys tai komponentti	Toimitusketjuhyökkäyksessä voidaan käyttää monenlaisia yhteyksiä, kuten tiedonsiirto-, ohjelmistopäivitys-, järjestelmä- tai huoltoyhteyksiä. Hyökkäykset voidaan myös toteuttaa ohjelmistoja tai niiden komponentteja hyväksikäyttämällä.	Selvitä, onko hyökkäys toteutettu • yhteistyökumppanin etäyhteyden tai vuodettujen tunnuksien välityksellä tai • organisaatiosi käytössä olevaan sovellukseen asennetun takaoven avulla. Selvitä, ovatko saastuneella laitteella olevat ohjelmistot ja järjestelmät ajan tasalla. Seuraa myös Kyberturvallisuuskeskuksen tiedotteita, sillä hyökkäys on saattanut tapahtua uutta nollapäivähaavoittuvuutta hyväksikäyttäen.
Selvitä palvelimet ja työasemat, jotka ovat saattaneet saastua hyökkäyksessä	On kyettävä tunnistamaan nopeasti kaikki palvelimet ja päätelaitteet, joissa hyökkäyksessä käytetty yhteys tai komponentti on käytössä, jotta kaikki mahdollisesti saastuneet laitteet saadaan eristettyä.	Käytä hyväksesi listaa IT-omaisuudestasi sekä asennetuista ohjelmistoista saadaksesi nopeasti käsityksen siitä, missä saastunut sovellus tai komponentti on käytössä. Jos kyseessä on etähallintayhteys tai muu integraatio, tarkista dokumentaatiosta missä nämä ovat käytössä ja mihin niistä pääsee käsiksi. Jos kyseessä on esimerkiksi saastunut kirjasto, jota käytetään useissa eri järjestelmissä, tarkasta asennettujen ohjelmistojen listauksen avulla käytössä olevat sovellukset ja selvitä, onko kyseinen komponentti niissä käytössä. Tämä voi vaatia sen, että organisaatio on suoraan yhteydessä sovellustoimittajaan, jotta asiasta saadaan varmuus. Mikäli jokin toimenpiteistä ei onnistu ilman IT-palveluntarjoajan apua, siirry ohjeen seuraavaan kohtaan.
Ota yhteyttä IT-palveluntarjoajaasi	Usein osa organisaation IT-infrastruktuurista on ulkoistettu palveluntarjoajalle. 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 muun muassa palveluntarjoajaasi irrottamaan palvelimiasi verkoista, palauttamaan niitä tai lähettämään niistä lokeja. IT-palveluntarjoajille on usein myös osaavaa henkilökuntaa, joka voi auttaa enemmänkin poikkeaman ratkaisussa.
Ilmoita tietoturvaloukkauksesta yhteistyökumppaneille sekä sidosryhmille, joihin tapaus voi vaikuttaa	Loukkaus voi aiheuttaa yhteistyökumppaneille, asiakkaille ja palveluntarjoajille riskejä tai ongelmia palveluiden saatavuudessa. Myös kumppaneiden kyberturvallisuus voi vaarantua toimitusketjuun kohdistuvan hyökkäyksen seurauksena.	Ilmoita eri sidosryhmien kriisiyhteyshenkilöille tapauksesta, jos uskot että se voi vaikuttaa heidän palveluidensa saatavuuteen. Jos palvelimella on ollut käytössä yhteyksiä muihin organisaatioihin, ilmoita myös heille, jotta he voivat mitätöidä tunnukset, avaimet tai varmenteet, joita oli käytössä saastuneella palvelimella. On myös tärkeää, että he tarkastavat omien tietojensa eheyden. Ilmoita tapauksesta tarvittaessa myös toimitusketjun muille organisaatioille, kuten toimittajalle.
Arvioi, tarvitsetko tietoturvaloukkauksen käsittelyyn ulkoista apua	Organisaatio voi tarvita apua toimenpiteiden organisoinnissa, poikkeaman hallinnassa tai teknisissä toimenpiteissä. Mikäli sisäisesti tai suoraan IT-palveluntarjoajilta ei löydy riittävää osaamista, tulee harkita ulkopuolisen avun tarvetta.	Tekniset toimet poikkeaman käsittelyssä voivat vaatia ulkopuolista osaamista. Kuten esimerkiksi tunnistetietojen kerääminen ja niiden perusteella uhan selvittäminen. Ulkopuolinen apu voi myös 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. Lähdeluettelon linkkien takaa löydät suomalaisia palveluntarjoajia.[8]
Tee ilmoitus tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle	Mikäli henkilötietoja on saattanut 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 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

[8] https://dfir.fi/

https://www.fisc.fi/fi

https://www.hansel.fi/yhteishankinnat/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/

		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 tietoturvaloukkauksesta 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 tietoturvaloukkauksista viranomaisille[11].

[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. Huolellisella selvityksellä varmistetaan, että haittaohjelmat ja mahdolliset takaovet on siivottu ympäristöstä.

Vaihe	Tarkoitus	Toimenpiteet
Tunnista merkkejä haitallisesta aktiviteetista ja poimi 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. Palautuminen voidaan aloittaa vasta, kun hyökkääjä on karkotettu kaikista ympäristöistä.	Kerää seuraavia tunnistetietoja: • Milloin palvelimelle kirjauduttiin • Mistä IP-osoitteesta kirjautuminen suoritettiin • Mihin aikaan tietty komento suoritettiin palvelimella • Mitä kyseinen komento sai palvelimella aikaan Haittaohjelma kommunikoi usein hyökkääjän komentopalvelimen kanssa. Saastuneiden laitteiden verkkoliikennettä tai verkkotunnusten selvitystä (DNS-lokit) tarkastelemalla, voit tunnistaa lähde-IP-osoitteen tai verkkotunnuksen, jota hyökkääjä käyttää. Voit ottaa haitallisista tiedostoista tunnisteet (MD5/SHA256), joiden avulla voit tunnistaa ne myös muilla laitteilla. Saastuneisiin laitteisiin kohdistuneista tunnistautumistapahtumista ja näihin liittyvillä käyttäjätileillä suoritetuista toimenpiteistä voit päätellä tunnukset, joilla haittaohjelmaa on levitetty. Keskitetystä päätelaitteiden valvonnasta löytyy usein toiminnallisuus edellä mainittujen tunnistetietojen keräämiseen ja niiden käyttämiseen. Muussa tapauksessa toimet tulee tehdä käsin käyttämällä keskitettyä lokipalvelinta. Mikäli tätäkään ei ole saatavilla, voit tutkia yksittäisten palvelinten ja päätelaitteiden lokeja.
Käytä tunnistetietoja avuksi selvittääksesi 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.	Voit toteuttaa saastuneiden laitteiden etsintää tunnistetiedoilla esimerkiksi käyttämällä keskitetyn päätelaitteiden valvonnan ominaisuuksia, jotka usein tarjoavat suoraan mahdollisuuden hakea tapahtumia laitteilta eri tunnisteilla. Jos organisaatiollasi on käytössä myös keskitetty lokienhallinta, voit hakea sieltä hakea tapahtumia tunnisteiden perusteella useilta eri koneilta samanaikaisesti. Mikäli kumpikaan edellä mainituista ratkaisusta ei ole käytettävissä, hae tunnisteita erikseen kaikilta koneilta. Tässä voit kuitenkin käyttää hyväksi erilaisia etähallintaratkaisuja, jotka usein mahdollistavat esimerkiksi PowerShell-komentojen ajamisen yhtäaikaisesti useammalla palvelimella. On olemassa riski, että hyökkääjä on laitteelle päästyään kytkenyt lokien

		keräämisen pois päältä, jolloin hänen toimistaan ei ole jäänyt mitään jälkiä. Tämän vuoksi sinun tulee tarkastella kaikista eri lähteistä kerättyjä tunnistetietoja, ja niiden avulla pyrkiä muodostamaan kokonaiskuva hyökkääjän toimista.
Selvitä palvelimella käytössä olleet yhteydet	Usein palvelimilla on käytössä yhteyksiä muihin järjestelmiin. Näitä voivat olla esimerkiksi tietokantayhteys tai erilaiset API- kutsut ja -avaimet. Tilanteen vakavuuden kartoittamiseksi tulisi varmistaa ensi tilassa, onko myös näihin järjestelmiin murtauduttu. Selvitä mahdollisimman pian, onko myös yhdistettyihin järjestelmiin murtauduttu tarkastelemalla niiden lokeja. Näin saat kokonaiskuvan loukkauksen laajuudesta.	Mikäli palvelimella on käytössä yhteyksiä muihin järjestelmiin, selvitä onko myös niihin murtauduttu tarkastelemalla yhdistettyjen järjestelmien lokeja. Varmistettavia asioita voi olla muun muassa 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, rajapinta-avaimet ja varmenteet, joita yhteyksiin on käytetty.
Selvitä onko kriittisiä tietoja vaarantunut	Osana tukimusta tulee selvittää, ovatko hyökkääjät päässeet käsiksi organisaation tärkeisiin tietoihin, tai mahdollisesti asiakkaiden tai työntekijöiden henkilötietoihin.	Selvitä, onko yhteyksissä käytetyillä tunnuksilla, varmenteilla tai avaimilla kirjauduttu muualta kuin palvelimelta, jossa niitä kuuluu käyttää. Selvitä, ovatko hyökkääjät päässeet käsiksi tietoihin ja varastaneet ne. Tarkastelemalla tietokannan tai rajapinnan lokeja voi päätellä tehdyistä hauista tai rasitusasteesta, onko hyökkääjä pyrkinyt lataamaan tietoja. Tarkista verkkolaitteiden lokeilta, onko saastuneen palvelimen liikenteessä poikkeamia. Poikkeuksellisen raskas liikenne voi viitata esimerkiksi siihen, että hyökkääjä on varastanut tietoja. Huomaa, että hyökkääjä on saattanut tietojen tuhoamisen ja varastamisen lisäksi muokata niitä. Hän on myös saattanut viedä hyvin pieniä määriä tietoja, 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 rikostutkinnan yhteydessä ja oikeuskäsittelyä varten. Jos organisaatiolla on kybervakuutus, voi myös vakuutusyhtiö vaatia poikkeamasta tarkempia tietoja, sekä todisteita tutkintaa varten.	Tallenna lokitiedostot, joista löytyy poikkeaman tutkinnan kannalta oleellista tietoa, verkosta eristetylle kovalevylle. Kerää talteen myös mahdolliset haitalliset sähköpostit ja muut viestit. Pyri säilyttämään todisteet, kuten kokonaiset levykuvat ja muistinäytteet, mahdollisimman eheinä. Ota niistä eheystiivisteet tämän varmistamiseksi. Pyri ottamaan haittaohjelmista näytteet ja säilö ne. Käsittelyssä tulee noudattaa erityistä varovaisuutta. Säilömisen 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	Palautuminen aloitetaan liiketoiminnan kannalta kriittisimmistä järjestelmistä. Organisaation tulee pyrkiä palauttamaan liiketoiminta takaisin normaaliin mahdollisimman pian, mutta vasta silloin, kun se voidaan toteuttaa turvallisesti.

Vaihe	Tarkoitus	Toimenpiteet
Aktivoi yhteydet uudelleen ja käynnistä sovellukset	Pyritään palauttamaan liiketoiminnoissa tarvittavat kumppaneiden etäyhteydet tai ohjelmistot takaisin toimintaan.	Varmista ennen yhteyksien aktivointia, että ne ovat turvallisia ja että yhteistyökumppani on myös onnistunut puhdistamaan omat järjestelmänsä ja tunnuksensa. Varmista ennen ohjelmistojen aktivointia, että tarvittavat korjauspäivitykset on asennettu. Mikäli korjauspäivitystä ei ole saatavilla, älä ota ohjelmistoa käyttöön ja harkitse sen poistamista käytöstä kokonaan.
Palauta saastuneet järjestelmät varmuuskopioista	Pyritään palauttamaan järjestelmät takaisin toimintaan ja palaamaan normaalin toimintanaan. Suoritetaan järjestelmien palautus mahdollisimman turvallisesti, jotta hyökkääjä ei pääsisi tunkeutumaan takaisin järjestelmiin.	Palauta järjestelmät varmuuskopioista. Ota huomioon, että aikaisemmat päiväkohtaiset (inkrementaaliset) varmuuskopiot voivat olla jo saastuneet. Vanhoja varmuuskopioita palauttaessasi ota huomioon, että varmuuskopio saattaa sisältää haavoittuvuuksia, joita hyökkääjä on voinut hyväksikäyttänyt poikkeaman aikana. Pyri palauttamaan järjestelmät ilman verkkoyhteyksiä ja päivitä käyttöjärjestelmä ja sen sovellukset ennen verkkoon kytkemistä välttääksesi kyseiset riskit. 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 torjunnalla, sillä automaattiskannerit eivät välttämättä kykene puhdistamaan järjestelmiä täydellisesti. Tarkista järjestelmät haittaohjelmien torjunnan työkaluilla ennen niiden kytkemistä takaisin verkkoon.
Palauta saastuneet tunnukset ja varmenna järjestelmänvalvojan tunnusten 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, mutta älä sähköpostilla tai organisaation suosimilla pikaviestimillä, sillä hyökkääjällä saattaa edelleen olla pääsy niihin. Harkitse kaksivaiheisen tunnistautumisen käyttöönottoa ylläpitotunnuksille sekä niille tunnuksille, joita oli käytetty hyväksi hyökkäyksessä. Valvo myös hyökkäyksessä käytettyjä tunnuksia tarkemmin tunnusten palauttamisen jälkeen siltä varalta,

		että hyökkääjä saa ne uudelleen käsiinsä. Mikäli jää epäselväksi, miten hyökkääjä oli saanut tietyt tunnukset käsiinsä, harkitse niiden tuhoamista ja täysin uusien tunnusten luomista. Näin varmistat, että hyökkääjä ei saa tunnuksia haltuunsa uudelleen tällä tuntemattomalla tavalla.

5 Tietoturvaloukkauksen jälkiselvitys

Kriisin päätyttyä ja liiketoimintojen normalisoiduttua on tärkeää käynnistää loukkauksen jälkiselvitys ja oppia tapahtuneesta tulevaisuutta varten. Samalla kriisinhallintasuunnitelmat on syytä päivittää tehtyjen havaintojen mukaan. On mahdollista, että organisaatio joutuu uudelleen vastaavan loukkauksen 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 toimintaohjeita 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 978-952-311-813-3

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus