TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Toimintaohje – Palvelunestohyökkäys

Traficomin julkaisuja

**25/2022**

## Sisällysluettelo

# 1 Johdanto

## 1.1 Ohjeen tarkoitus

Tämän Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen laatiman ohjeen tavoitteena on neuvoa organisaatioita tilanteessa, jossa epäillään palvelunestohyökkäystä tai palvelunestohyökkäys 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 palvelunestohyökkäys

Palvelunestohyökkäys (eng. denial of service attack) on hyökkäys, jolla pahantahtoinen toimija pyrkii estämään verkkoresurssin tai palvelun käytön häiritsemällä sen toimintaa. Hyökkäys voidaan toteuttaa esimerkiksi kuormittamalla kohdepalvelu tai verkkoliikenne ylimääräisellä liikenteellä tai hyödyntämällä palvelussa tai verkkolaitteessa olevaa haavoittuvuutta. Nykyään suurin osa palvelunestohyökkäyksistä on hajautettuja, eli liikenne lähetetään kohteeseen useasta lähteestä samanaikaisesti. Hajautettujen hyökkäysten taustalla on usein hyökkääjän hallitsema bottiverkko, joka koostuu useista internetiin kytketyistä laitteista, jotka ovat kaapattu hyökkäyskäyttöön laitteiden omistajien tietämättä.

Palvelunestohyökkäykset tapahtuvat yleensä joko kuormittamalla kohde puhtaasti suurella liikennemäärällä tai vaihtoehtoisesti lähettämällä sellaista liikennettä, joka saa kohdelaitteen käyttämään normaalia enemmän muisti- tai laskentaresursseja liikenteen käsittelyyn, jolloin liikenteen määrän ei tarvitse olla erityisen suuri. Tämänkaltaiset hyökkäystyypit eivät välttämättä ilmene liikennemäärän poikkeavana kasvuna.

Sovellustason palvelunestohyökkäyksissä voidaan ottaa kohteeksi esimerkiksi sovelluksen taustalla pyörivä tietokanta, joka kuormitetaan lähettämällä suuria määriä kyselyitä itse sovelluksen kautta.

Palvelunestohyökkäys ei vaadi nykyaikana suurta teknistä osaamista, koska sellaisen voi ostaa esimerkiksi pimeästä verkosta edullisesti palveluna. Hyökkäyksiä käytetään usein kiristämiseen, kiusantekoon tai poliittiseen häirintään (ns. haktivismi), jolloin hyökkäyksen tilaaja ja toteuttaja ovat yleensä eri tahot.

Hyökkäyksen toteutustapoja on monia erilaisia, joiden kaikkien lopputulos on sama. Klassinen menetelmä on hajautetut TCP SYN -tulvahyökkäykset, joissa bottiverkko lähettää kohteeseen suuria määriä TCP SYN -paketteja, jättäen ACK-paketit lähettämättä. Tämä johtaa siihen, että kohteen TCP-pino täyttyy keskeneräisistä TCP-kättelyistä, eikä palvelin tai laite pysty enää vastaanottamaan uusia yhteydenottopyyntöjä. Varautuessa kannattaa keskittyä yleisimpien hyökkäystapojen torjuntaan.

# 2 Varautuminen

Yleisesti tietoliikennehäiriöiden korjausvastuu on IT-palveluntarjoajalla, joten nopea palautuminen häiriöstä edellyttää palvelutasosopimusta (engl. Service Level Agreement, SLA), joka velvoittaa palveluntarjoajan palauttamaan palvelutason nopealla aikataululla.

Palvelunestohyökkäyksen tapauksessa erillinen sopimus sen vaikutusten lieventämiseksi hyökkäyksen sattuessa voi olla tarpeellinen. Myös verkkolaitteiden ja palvelinten ohjelmistot ovat syytä pitää ajan tasalla, koska osa palvelunestohyökkäyksistä hyödyntää ohjelmistojen haavoittuvuuksia.

Sopimusten lisäksi on huolehdittava tietoliikenneyhteyksien kahdennuksesta, sekä mahdollisista varajärjestelmistä, riippuen miten kriittinen järjestelmä on kyseessä. Häiriön sattuessa on syytä tietää valmiiksi toimintamalli, joka takaa sujuvan kommunikaation yrityksen ja palveluntarjoajien välillä, sekä määritelmän tilannejohtamisesta ja tilanteen dokumentoinnista. Häiriön korjaamiseen osallistuvilla henkilöillä tulee olla selkeät roolit ja tutkintalinjojen pitää olla selkeät ja asianmukaiset.

Organisaatio voi arvioida omaa valmiuttaan käyttämällä hyväksi esimerkiksi Kyberturvallisuuskeskuksen Kybermittaria.[1] Kyberturvallisuuskeskus on myös julkaissut erillisen ohjeen vielä palvelunestohyökkäysten ehkäisyyn ja torjuntaan.[2]

## 2.1 Hallinnolliset toimet

- Laadi organisaatiollesi poikkeamanhallintasuunnitelma palvelunestohyökkäystä varten.
- Kouluta henkilökuntaa toimimaan pelikirjan kaltaisen poikkeaman aikana.
    - Tarjoa myös tavallisille työntekijöille perustason koulutuksia, joissa neuvotaan miten toimia, kun palvelunestohyökkäys rampauttaa yrityksen palveluita.
- 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 poikkeamanhallintasuunnitelma 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.
- Määrittele tarkasti tarvittavat käyttöoikeudet perustuen käyttäjien ja teknisten toiminnallisuuksien tarpeisiin.
- Harkitse tietoturvavalvomopalvelun (SOC) perustamista tai vastaavan palvelun ostamista. Valvomotoiminnon tarkoituksena on nimensä mukaisesti valvoa yrityksesi verkkoliikennettä ja järjestelmien tietoturvatapahtumia.

[1] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari
[2] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta_0.pdf

[3] https://www.kyberturvallisuuskeskus.fi/fi/ilmoita
[4] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaiset
[5] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta

- Varmista, että palveluntarjoajien kanssa tehdyt sopimukset kattavat palvelunestohyökkäysten torjunnan.

## 2.2 Tekniset toimet

- Pyri havaitsemaan hyökkäykset mahdollisimman ajoissa erilaisilla keskitetyillä monitorointiratkaisuilla, joiden toiminnallisuutta myös testataan aika-ajoin. Esimerkiksi IDS-ratkaisut (engl. Intrusion Detection System) havaitsevat hyökkäykset ja usein pyrkivät estämään ne automaattisesti.

- Pidä palvelinten ohjelmisto ajan tasalla ja tarkista, että konfiguraatiot ovat suositusten mukaiset. Oikeilla konfiguraatioilla voidaan heikentää palvelunestohyökkäysten vaikutuksia.

- Palvelunestohyökkäyksiä vaimentavat konfiguraatiot voivat sisältää esimerkiksi yksittäisten yhteyksien nopeusrajoituksia (engl. Rate Limiting), TCP-yhteyksien käsittelyjonon pidennyksiä (engl. Backlog Queue), keskeneräisten TCP-yhteyksien kierrätystä (engl. Half-Open Connection Recycling) tai SYN-evästeiden käyttöönoton (engl. SYN cookies). Selvitä mitkä näistä tekniikoista sopivat palvelinympäristöönne parhaiten ja ota niitä käyttöön tarpeen mukaan.

- Kyberturvallisuuskeskus on julkaissut teknisen oppaan palvelunestohyökkäyksen puolustukseen.[6]

## 2.3 Varautumisen ja harjoittelu käytännössä

Tärkeä osa varautumista on myös uhkaskenaarioiden harjoittelu. Harjoittelemalla tämän toimintaohjeen skenaarion etukäteen, organisaatio voi varmistaa, että se 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 palvelunestohyökkäys rampauttaa kriittisen tietojärjestelmän estäen täysin järjestelmän käytön ja toiminnan.

Kuinka organisaatiossanne toimittaisiin kuvatun kaltaisessa tietoturvaloukkaustilanteessa? Harjoitelkaa ainakin seuraavat vaiheet tästä pelikirjasta:

- Loukkauksesta ilmoittaminen ja tilanteen eskalaatio

- Ilmoittaminen tilanteesta olennaisille palveluntarjoajille ja muille sidosryhmille

- Varajärjestelmän käyttöönotto

- Poikkeaman loppututkinnan prosessi

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

[6] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_liite_1_Palvelunestohyokkaysten_tekniikkaa_puolustajille_0.pdf
[7] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta

# 3 Tietoturvaloukkauksen havaitseminen

Palvelunestohyökkäys havaitaan yleensä palveluiden toimimattomuuden perusteella. Myös kattava valvonta voi havaita hyökkäyksen ennen vaikutusta palveluiden saatavuuteen, esimerkiksi verkkoliikenteen nopean kasvun tai palvelimen nopean resurssien kulutuksen kasvun perusteella. Jotkin palvelunestohyökkäykset saattavat pyrkiä aiheuttamaan vikatilan yksittäisissä verkkolaitteissa, jolloin liikennemäärissä ei välttämättä näy suuria muutoksia. Siksi on tärkeää, että yksittäisten verkkolaitteiden toiminta on valvonnan piirissä.

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

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

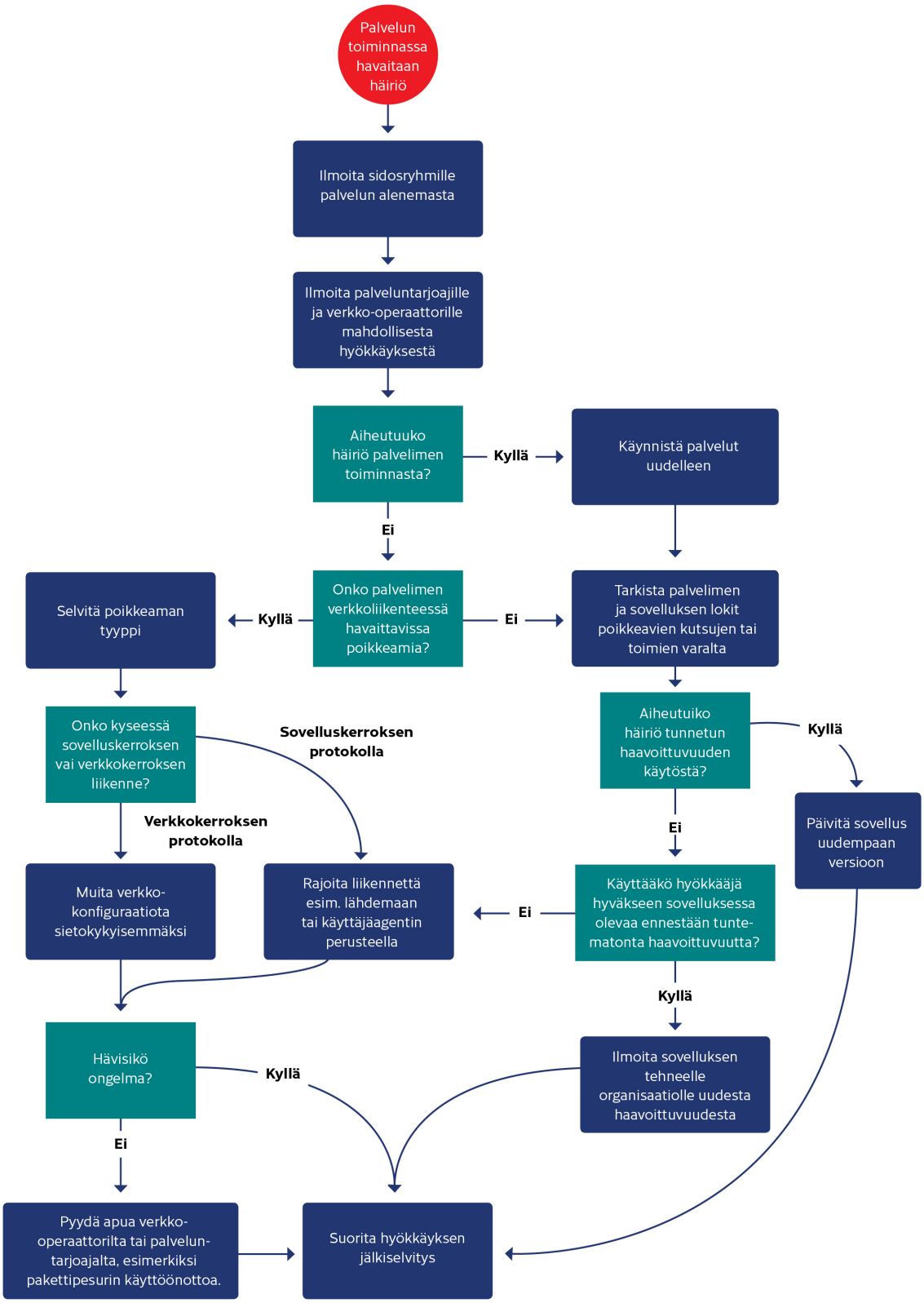
# 4 Toimintaohjeet

Käytä oheista toimenpiteiden tarkistuslistaa apuna, kun epäilet joutuneesi palvelunestohyökkäyksen kohteeksi. Tarkistuslista auttaa organisaatiotasi 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.


Palvelun toiminnassa havaitaan häiriö
Ilmoita sidosryhmille palvelun alenemasta
Ilmoita palveluntarjoajille ja verkko-operaattorille mahdollisesta hyökkäyksestä
Aiheutuuko häiriö palvelimen toiminnasta?
Kyllä
Käynnistä palvelut uudelleen
Ei
Onko palvelimen verkkoliikenteessä havaittavissa poikkeamia?
Kyllä
Selvitä poikkeaman tyyppi
Ei
Tarkista palvelimen ja sovelluksen lokit poikkeavien kutsujen tai toimien varalta
Onko kyseessä sovelluskerroksen vai verkkokerroksen liikenne?
Sovelluskerroksen protokolla
Verkkokerroksen protokolla
Aiheutuiko häiriö tunnetun haavoittuvuuden käytöstä?
Kyllä
Päivitä sovellus uudempaan versioon
Ei
Muita verkko-konfiguraatiota sietokykyisemmäksi
Rajoita liikennettä esim. lähdemaan tai käyttäjäagentin perusteella
Ei
Käyttääkö hyökkääjä hyväkseen sovelluksessa olevaa ennestään tuntematonta haavoittuvuutta?
Kyllä
Hävisikö ongelma?
Kyllä
Ilmoita sovelluksen tehneelle organisaatiolle uudesta haavoittuvuudesta
Ei
Pyydä apua verkko-operaattorilta tai palvelun-tarjoajalta, esimerkiksi pakettipesurin käyttöönottoa.
Suorita hyökkäyksen jälkiselvitys

## 4.2 Välittömät toimenpiteet

| | |
|---|---|
| **Vaiheen tavoitteet** | Toimenpiteiden tarkkuus ja nopeus ovat molemmat tärkeitä. Välittömien toimenpiteiden tavoite on rajata tietoliikennehäiriön syy ja käynnistää lieventävät tai korjaavat toimenpiteet mahdollisimman nopeasti. |

| Vaihe | Tarkoitus | Toimenpiteet |
|---|---|---|
| **Tarkista häiriön kohteena olevan palvelun palvelinten tilanne** | Häiriön syy pyritään rajaamaan mahdollisimman tarkasti. Jos esimerkiksi verkkosivuilla esiintyy häiriö, saattaa syynä olla vikatilanne jossakin sivuston taustapalvelimessa. Myös palvelunestohyökkäys saattaa aiheuttaa jonkin taustasovelluksen kaatumisen. | Pyydä sovelluspalvelimen ylläpitäjää tarkistamaan sovelluksen tila, lokit ja palvelimen resurssien käyttö. Mikäli sovellukseen liittyy taustapalveluita, esimerkiksi tietokantoja, tulee myös nämä tarkistaa erikseen. |
| **Tarkista häiriön kohteena olevan palvelun liikenne poikkeamien varalta ja tunnista hyökkäyksen tyyppi** | Palvelunestohyökkäys näkyy monissa tapauksissa liikennemäärän selvänä kasvuna. Siksi liikennemäärän kasvu yhdistettynä palvelun toimimattomuuteen voi olla merkki palvelunestohyökkäyksestä. Palvelunestohyökkäyksen tyyppi on myös tärkeä tunnistaa torjumisen helpottamiseksi. | Tarkista onko sovelluksen lokeihin tullut normaalia enemmän kyselyitä ja mistä kyselyt ovat peräisin. Kyselyiden äkillinen kasvu esimerkiksi ulkomaisista IP-osoitteista voi olla merkki palvelunestohyökkäyksestä.<br><br>Suurin osa palvelunestohyökkäyksistä tehdään nykyään TCP SYN tulvahyökkäys -tekniikalla. Nämä hyökkäykset ovat vaikeampia havaita, koska ne eivät näy verkkopalvelinten lokeissa. Ne voidaan kuitenkin havaita reaaliajassa palvelinten TCP-yhteyslistauksesta normaalia suurempana määränä 'SYN RECV' -rivejä.<br><br>Sovellustason hyökkäys näkyy yleensä erikoisina HTTP-kyselyinä web-palvelimen lokissa, tai vaihtoehtoisesti normaaleina kyselyinä, joita on poikkeuksellisen paljon. Tämä hyökkäys on teknisesti helpoin toteuttaa, mutta se aiheuttaa myös vähiten vahinkoa kohteelle.<br><br>Vahvistettu DNS-hyökkäys näkyy myös kasvaneina HTTP-kyselyinä lokeissa, mutta se aiheuttaa huomattavasti enemmän haittaa normaaliin sovellustason HTTP-hyökkäykseen verrattuna. Hyökkääjä toteuttaa sen lähettämällä usealle nimipalvelimelle DNS-kyselyitä, joiden lähettäjäosoite on väärennetty tulemaan hyökkäyksen kohteena olevasta organisaatiosta. Tällöin palvelimet palauttavat vastauksen hyökkäyksen kohteelle kuormittaen tätä. Hyökkäyksen tunnistaa lokeista HTTP-vastauksina, joille ei löydy vastaavaa lähetettyä kyselyä. |
| **Ota yhteyttä IT/ICT-palveluntarjoajaasi** | Usein osa organisaation IT-infrastruktuurista on ulkoistettu palveluntarjoajalle. Haitallinen liikenne menee lähes aina palveluntarjoajan verkon läpi, jolloin palveluntarjoajalla on mahdollisuus suodattaa liikennettä, mikäli asiasta on tehty ennakkoon sopimukset. | Tee poikkeamasta ilmoitus IT- tai ICT-palveluntarjoajallesi riippuen siitä, mikä palvelu on hyökkäyksen kohteena. Mikäli hyökkäys on ns. volumetrinen, eli perustuu suureen liikennemäärään, voi palveluntarjoaja auttaa hyökkäyksen pysäyttämisessä rajoittamalla palveluun |

| | | |
|---|---|---|
| | | kohdistuvaa liikennettä pakettipesurilla. |
| **Ilmoita tietoturvaloukkauksesta yhteistyökumppaneille sekä sidosryhmille joihin tapaus voi vaikuttaa** | Loukkaus voi aiheuttaa yhteistyökumppaneille, asiakkaille ja palveluntarjoajille riskejä tai ongelmia palveluiden saatavuudessa. | Ilmoita eri sidosryhmien kriisiyhteyshenkilöille tapauksesta, mikäli uskot että se voi vaikuttaa heidän palveluidensa saatavuuteen.<br><br>Hoida tapauksesta viestiminen myös sisäisesti, varsinkin jos hyökkäys rajoittaa myös sisäisten palveluiden saatavuutta. |
| **Arvioi tarvitsetko loukkauksen käsittelyyn ulkoista apua** | Organisaatio voi tarvita apua teknisissä toimenpiteissä, loukkauksen hallinnassa ja toimenpiteiden organisoinnissa. Mikäli sisäisesti tai käytetyiltä IT-palveluntarjoajilta ei löydy riittävää osaamista, ulkopuolisen avun tarvetta tulee harkita. | Tekniset toimet loukkauksen käsittelyssä voivat vaatia ulkopuolista osaamista. Tällaisia toimia voivat olla muiden muassa tunnistetietojen kerääminen ja uhan selvittäminen niiden perusteella.<br><br>Kyberturvallisuuskeskus voi auttaa organisaatioita erityisesti tapauksen ensivasteessa ja tarjoamalla lisätietoja vastaavista tapauksista Suomessa ja kansainvälisesti.<br><br>Alaviitteessä listatuista resursseista löydät suomalaisia palveluntarjoajia.[9] |
| **Raportoi tietoturvaloukkauksesta viranomaisille** | Raportoi loukkauksesta viranomaistahoille. Organisaatiolla voi olla vastuu ilmoittaa loukkauksesta säädösten tai kybervakuutuksen velvoittamana. | Tee tapauksesta rikosilmoitus Poliisille.[10] Ilmoita tapauksesta myös Kyberturvallisuuskeskukselle[11] tilannekuvan ylläpitämiseksi ja avun saamiseksi.<br><br>Huoltovarmuuskriittisten toimijoiden ja palveluntarjoajien pitää ilmoittaa verkko- ja tietojärjestelmässä olevista tietoturvapoikkeamista viranomaisille.[12] |

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

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

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

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

## 4.3 Tietoturvaloukkauksen selvitys

| | |
|---|---|
| **Vaiheen tavoitteet** | Loukkauksen selvityksen tavoitteena on selvittää, miten hyökkäys on aiheuttanut häiriön palvelussa ja saada sitä kautta tietoa miten vastaavalta hyökkäykseltä voidaan suojautua jatkossa. |

| Vaihe | Tarkoitus | Toimenpiteet |
|---|---|---|
| **Selvitä, mihin kohteisiin hyökkäys on kohdistunut** | On tärkeää tunnistaa mihin osaan infrastruktuuria palvelunestohyökkäys on kohdistunut. Esimerkiksi verkkopalvelun tapauksessa on oleellista selvittää, onko hyökkäys kohdistunut suoraan esimerkiksi verkkosivupalvelimeen vai siihen yhteydessä oleviin verkkolaitteisiin. | Tarkista hyökkäyksen kohteena olleen palvelimen lokitiedot. Jos kyseessä on verkkosivupalvelin, voi hyökkäys näkyä lisääntyneinä yhteydenottoina lokissa.<br><br>Jos kyse on TCP SYN -tulvahyökkäyksestä tai muusta alemman protokollan hyökkäyksestä, voi selvitystyö olla vaikeaa ilman IT-palveluntarjoajan apua. |
| **Selvitä hyökkäyksen tyyppi** | Hyökkäyksen tyyppi on tärkeä selvittää, jotta palvelu voidaan suojata jatkossa paremmin. Kyseessä voi olla sovelluskerroksen, kuten HTTP:n, tai verkkokerroksen protokollan hyökkäys, kuten TCP, tai hyökkääjä on voinut hyödyntää kohteessa olevaa ohjelmistohaavoittuvuutta. | Jos hyökkäys on toteutettu hyväksikäyttämällä haavoittuvuutta kohteessa, tulee kohdejärjestelmä päivittää haavoittuvuuden poistamiseksi. Mikäli kyseessä on organisaation muualta tilaama sovellus, tulee haavoittuvuuden korjaamiseksi olla yhteydessä sovelluksen toimittaneeseen tahoon.<br><br>Volumetrisissä hyökkäyksissä tehokkain tapa puolustautua on IT- tai ICT-palveluntarjoajan toteuttama liikenteen suodattaminen, joka vaatii erillisiä sopimuksia palveluntarjoajan kanssa.<br><br>Sovelluskerroksen protokollan, eli sovellustason hyökkäyksiä voi pyrkiä torjumaan itsenäisesti, esimerkiksi rajoittamalla yhteydenottoja perustuen IP-osoitteeseen, verkkotunnukseen, selaimen käyttäjäagenttiin tai IP:n geolokaatioon. |
| **Tallenna kaikki tapaukseen liittyvät lokit myöhempää tutkintaa varten** | Todisteiden keräämisellä ja säilömisellä pyritään takaamaan laadukas tapauksen jälkitutkinta, jotta tapauksen juurisyyt saadaan selvitettyä.<br><br>Todisteita voidaan tarvita rikosilmoituksen yhteydessä ja oikeuskannetta varten. | Tallenna verkosta eriytetylle kovalevylle kaikki lokitiedostot, joista löytyy loukkauksen tutkinnan kannalta oleellista tietoa. |

## 4.4 Palautuminen

| | |
|---|---|
| **Vaiheen tavoitteet** | Palvelunestohyökkäykset kestävät keskimäärin alle 15 minuuttia, mutta joskus ne voivat venyä useamman tunnin mittaisiksi. Palvelut palautuvat hyökkäyksen jälkeen yleensä itsestään takaisin toimintaan. |

| Vaihe | Tarkoitus | Toimenpiteet |
|---|---|---|
| **Tarkista kohteena olleet palvelun osat vikatilanteiden varalta** | Palvelunestohyökkäys on voinut saada kohteena olleen palvelimen tai verkkolaitteen vikatilaan, jolloin on hyvä tarkistaa, että palvelimet ja niiden päällä pyörivät sovellukset toimivat normaalisti. | Tarkista kohteena olleiden palvelinten ja verkkolaitteiden tila. Tarkista myös, että sovellukset toimivat normaalisti. |
| **Tarkista, että palvelinten ohjelmisto ja konfiguraatio on ajan tasalla** | Palvelunestohyökkäyksessä on saatettu hyödyntää haavoittuvuutta sovelluksessa tai palvelimessa, joten on syytä tarkistaa, että palvelimen päivitykset ovat ajan tasalla. | Käy läpi hyökkäyksen kohteena olleen palvelimen sovellusversiot ja päivitä tarvittaessa uudempaan.<br><br>Selvitä sovelluksen lokeilta millaisia kutsuja sovellus on vastaanottanut saadaksesi selville kutsut, joita on saatettu hyödyntää osana hyökkäystä. |

# 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 978-952-311-817-1

HUOLTOVARMUUSKESKUS

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus