Toimintaohjeet palvelunestohyökkäyksen kohteeksi joutuneelle

1 Havainto palvelunestohyökkäyksestä?

- Ilmoita tilanteesta sisäisesti ja yhteistyökumppaneille oman organisaatiosi ohjeistuksen mukaisesti.
- Jos hyökkäys on edelleen käynnissä, ota viipymättä yhteyttä Viestintävirastoon sähköpostilla (**cert@viestintavirasto.fi**) tai puhelimitse (**0295390230**), kun hyökkäyksen kohteesta on alustava käsitys.
- Alla on luettelo asioita, joita tullaan tarvitsemaan hyökkäyksen selvittelyssä. Välitä selville tulleet tiedot eteenpäin viivytyksettä.

1.1 Vaikutukset ja vakavuusarvio

- **Mikä organisaatio on hyökkäyksen kohteena?**
  - Mitkä ovat organisaatiosi yhteystiedot?
  - Mitkä ovat palvelun toteutukseen osallistuvat tahot (esimerkiksi internetoperaattorit tai palvelutoimittajat)? Mitkä ovat yhteystiedot? Onko niihin oltu jo tilanteesta yhteydessä?
- **Mihin palveluihin hyökkäys vaikuttaa?**
  - Mikä on hyökkäyksen kohteena oleva järjestelmä? Mitkä ovat palvelun keskeiset ohjelmistot (palvelinten käyttöjärjestelmä, www-palvelimen tyyppi, sisällönhallintajärjestelmä)?
  - **Kohdejärjestelmien IP-osoitteet tai osoitealueet,** mahdolliset **verkkotunnukset** joihin hyökkäys kohdistuu.
  - Palvelun / palveluiden **käyttäjämäärät?**
- **Minkä tyyppinen hyökkäys on?**
  - Onko kyseessä tietoliikenneyhteyksiä vai itse palvelimia kuormittava hyökkäys?
- Onko hyökkäysliikenteestä **näytteitä tai lokitietoa?**
  - Ensi vaiheessa on syytä varmistaa että lokitietoa kertyy ja lokit jäävät talteen.
  - Hyökkäysliikenteen **tyyppi**: esim. TCP SYN, HTTP GET, UDP?
  - **Mikä on liikenteen määrä?** Gbit/s tai pakettia/s
- **Onko hyökkäävä taho ottanut yhteyttä** (esim. sähköposti, sosiaalinen media)? Hyökkääjän motiivi? Voisitko olla sivullinen uhri?
- **Mikä vaarantuu** hyökkäyksen johdosta?
- Mikä on palveluiden **käytettävyysaste?**
- Onko hyökkäyksellä **seurannaisvaikutuksia** muihin palveluihin?

1.2 Hyökkäysliikenteen lähde

- Mahdollinen tieto hyökkäysliikenteen **lähdeosoitteista** ja **lukumäärästä** . Voivatko lähdeosoitteet olla **väärennettyjä?**
- Lähdeosoitteissa tulisi olla mukana aikaleima (ja aikaleiman aikavyöhyke), jotta lähdeosoitteiden haltijat voidaan jäljittää.

1.3 Aikajakso

- Milloin hyökkäys on **alkanut? Jatkuuko yhä?**
- Jos hyökkäys on jo **loppunut**, milloin loppui?
- Onko hyökkäys **toistoa** aiemmalle?
- Milloin hyökkäys tuli **tietoonne?**

1.4 Tarpeet toimenpiteille

- **Onko hyökkäystä pystytty torjumaan tai väistämään? Miten?**
- Onko internetoperaattoriin ja palveluntarjoajaan oltu yhteydessä?
- Tarvitaanko torjunnassa apua?
- **Onko tapauksesta tehty tai suunnitteilla tutkintapyyntö poliisille?**
- Voiko tapaus herättää kiinnostusta mediassa?

2 Jatkotoimenpiteet

2.1 Hyökkäyksen torjunta

- Vastuuhenkilöiden aktivointi ja toimintasuunnitelmien kertaaminen.
- Omat toimenpiteet: ruuhkasivu, palveluiden hallittu sammuttaminen, …
- Oman internetoperaattorin kanssa tehtävät toimenpiteet: suodatus, …

2.2 Rikosilmoituksen tekeminen poliisille

- Tee rikosilmoitus paikallispoliisille.
- Viestintävirasto voi luvallanne antaa tapauksen selvittämiseen teknistä tukea poliisille. Tutkintapyynnön tunnisteen antaminen Viestintävirastolle helpottaa tuen antamista.

2.3 Kriisiviestintä

- Omalle henkilöstölle.
- Tärkeimmille sidosryhmille
- Julkisuuteen, jos hyökkäys on julkisesti havaittavissa.

2.4 Tilanteen seuraaminen

- Torjuntatoimien vaikuttavuus.
- Hyökkäyksen muuttuminen
- Hyökkäyksen ja sen torjunnan kustannusten seuranta.
- Tilannekuvan jakaminen torjunta- ja selvitystoimiin osallistuville.

3 Jälkipyykki

3.1 Torjuntatoimien lopettaminen

- Mahdollisten liikennerajoitusten poistaminen ja palveluiden palauttaminen.
- Tiedottaminen tilanteen muutoksesta.

3.2 Tapauksesta oppiminen

- Oman ja yhteistyökumppaneiden toiminnan tarkastelu hyökkäyksiin varautumisen ja hyökkäyksen aikaisen toiminnan näkökulmista.
- Varautumisen ja toimintaohjeiden parantaminen.