|  |
| --- |
| **Palvelunestohyökkäys organisaation verkkosivuille tai sähköisiin asiointipalveluihin**  |
| **Vahti-ohje 8/2017 LIITE 6. Esimerkki poikkeamatilanneohjeistuksesta** **Poikkeaman yksilöinti**Palvelunestohyökkäys organisaation verkkosivuille tai sähköisiin asiointipalveluihin**Poikkeaman kuvaus** Tahallisella ulkoisella kuormituksella tukitaan tai häiritään organisaation verkkosivuja tai sähköisiä asiointipalveluita siten, etteivät ne ole käytössä tai ne toimivat hitaasti tai virheellisesti yli neljän tunnin ajan. Kuormitus voi olla virheellistä tai oikeanlaista liikennettäja johtaa verkko- tai alustakapasiteetin loppumiseen tai palvelun kaatumiseen virheellisen toiminnon takia. |
| **Tietoturvapoikkeamien käsittelyryhmä** ICT-tietoturvapäällikkö Turvallisuuspäällikkö Tuotantopäällikkö Verkkoarkkitehti Käyttöpalvelutoimittajan tietoturvavastaava Palvelutoimittajan verkkovastaava Palvelutiimin vetäjä  | Tarpeen mukaan Viestintäasiantuntija Tuotantoryhmän vetäjä Palvelutoimittajan tietoturvavastaava  |
| **Sidosryhmät** Viestintäviraston Kyberturvallisuuskeskus Poliisi Käyttöpalvelutoimittaja Operaattori  |
| **Viestintä** Turvallisuuspäällikkö tiedottaa viraston johtoa sähköpostilla kahdesti päivässä. Vastaavasti päivitettävä tiedote julkaistaan int­ranetissä ja sidosryhmille lähetetään häiriötiedote. Jos kyseessä on vakava häiriö, viestintäasiantuntija valmistelee mediatiedot­teen, joka julkaistaan lisäksi organisaation nettisivuilla ja sosiaalisen median kanavissa (Facebook, Twitter). Tilannepäivityksiä julkaistaan näissä kahdesti päivässä. Medialle ja ulkoisiin kyselyihin vastaa tietohallintojohtaja tai turvallisuuspäällikkö.  |
| **Tapahtumalokin ylläpito** Päätetään kirjuri ja kirjataan tehdyt päätökset sekä oleelliset tapahtumat ja havainnot ajankohtineen.  |
| **Toimet** 1. Häiriönhallintaprosessista otetaan yhteyttä tietoturvapäällikköön ja tuotantopäällikköön.
2. Tietoturvapäällikkö ja / tai tuotantopäällikkö arvioivat, onko kyseessä todellinen palvelunestohyökkäys ja minkä tahojen palveluihin hyökkäys kohdistuu.
3. Tapauksesta tiedotetaan sähköpostilla / tekstiviestillä turvallisuuspäällikköä, tietohallintojohtajaa, palvelun ICT-omistajaa, palvelutiimin vetäjää sekä palvelutoimittajan tietoturvavastaavaa.
4. ICT-tietoturvapäällikkö tai tuotantopäällikkö kutsuu kriisiryhmän kokoon kriisinjohtokeskukseen (tarkoitukseen soveltuva neuvotteluhuone tms.) sekä avaa viestintäkanavat.
5. Arvioidaan hyökkäyksen laajuus, vaikutukset ja tyyppi
	* Mikä on liikenteen määrä ja lähde (kotimaa / ulkomaat) ja tyyppi
	* Mitkä ovat häiriön vaikutukset? Vaikuttaako organisaation kriittisiin sovelluksiin?
	* Onko kyseessä hajautettu palvelunestohyökkäys? Mihin kuormitus kohdistuu?
	* Onko viitteitä kiristyksestä tai aiemmasta uhkauksesta?
	* Hyödyntääkö hyökkäys haavoittuvuutta vai pelkkää resurssien ylikuormitusta?
	* Voidaanko poikkeava liikenne tunnistaa?
6. Tiedotetaan tarpeen mukaan viraston johtoa, henkilöstöä ja sidosryhmiä (häiriötiedote) sekä otetaan viestintäyksikkö mu­kaan ulkoiseen tiedottamiseen (mediatiedote, sosiaalinen media).
7. Jos tapaukseen liittyy kiristystä, vaateisiin tai viesteihin ei vastata.
8. Otetaan yhteyttä Viestintäviraston Kyberturvallisuuskeskuksen päivystäjään (ICT-tietoturvapäällikkö) sekä poliisiin asian­tuntija-avun saamiseksi. Asianomistaja tekee asiasta rikosilmoituksen.
 |