Verkkohyökkäyksien torjunta

Organisaatio tai yksityinen henkilö voi joutua verkkohyökkäyksen kohteeksi. Verkkohyökkäyksellä vihamielinen hyökkääjä voi pyrkiä lamauttamaan tietojärjestelmät, kaappaamaan tietotekniset laitteet hyökkääjän hallintaan, estämään tietoliikennettä tai varastamaan informaatiota kohteen järjestelmistä. Verkkohyökkäys voi pahimmillaan estää koko organisaation toiminnan, johtaa pitkiin selvitystöihin ja suuriin kustannuksiin. Seuraavilla toimenpiteillä voidaan pienentää verkkohyökkäyksen haittoja.

Ennakkoon - kartoitus

- Kartoita tietojärjestelmäsi. Mitä laitteita, ohjelmia ja palveluita käytät? Mitkä versiot näistä ovat käytössä?
- Arvioi eri järjestelmien, palvelujen ja tietojen kriittisyys toimintasi kannalta. Minkä palvelun tulee ehdottomasti toimia? Missä sijaitsee luottamuksellinen aineisto?

Ennakkoon – järjestelmien ylläpito

- Ylläpidä järjestelmiäsi. Käytä ohjelmista uusinta toimivaa versiota. Toimisto-ohjelmissa ja työasemien käyttöjärjestelmissä voit käyttää ohjelmien automaattista päivitysominaisuutta. Kriittisten järjestelmien ja palvelinsovellusten oikea toiminta tulee testata ennen niiden käyttöönottoa.
- Poista tai estä laitteilta palvelut, joita et tarvitse. Näin vaikeutat haittaohjelmien asentumista.
- Synkronoi kaikkien järjestelmien järjestelmäkellot, näin helpotat vianetsintää.
- Mitoita palvelukapasiteettisi niin suureksi, että vähäiset hyökkäykset eivät aiheuta kapasiteetin loppumista. Tee kapasiteetin laajennukset ajoissa, että voit harjoitella toimintaa.
- Huolehdi erityisesti web-sovellusten turvallisuudesta. Tarkasta kaikki syötteet. Rajaa pituudet ja poista syötteistä tarpeettomat erikoismerkit.
- Vaadi turvallisuutta myös verkkosivujen ylläpitäjiltä, alihankkijoilta ja sovellustoimittajilta.

Ennakkoon – verkko ja sen valvonta

- Käytä palomuuria. Sulje tarpeeton liikenne julkisiin verkkoihin ja julkisista verkoista sisäverkkoon.
- Segmentoi verkkoa pienempiin osiin palomuureilla tai VLAN-kytkimillä. Estä tarpeeton liikenne ja turhat protokollat verkon eri osien välillä.
- Kerää ja talleta lokeja palomuureista, järjestelmistä sekä verkon tapahtumista erilliselle lokipalvelimelle. Tilastoi aineisto saadaksesi käsitys normaalista verkkoliikenteestä.
- Asenna kaikille laitteistoille automaattisesti päivittyvä virustorjuntaohjelmisto.
- Vaihda järjestelmien, ohjelmien ja laitteistojen oletussalasanat. Pidä salasanat riittävän pitkinä (> 14 merkkiä) ja vaikeina arvata.
- Rajaa käyttäjien oikeudet vain työtehtävien kannalta tarvittaviin järjestelmiin ja hakemistoihin.

Ennakkoon – työkalut kuntoon

- Pyri yhtenäisiin työasemakokoonpanoihin, ja tee asennuspaketti (levyimage), joka yksinkertaistaa ohjelmien asennusta työasemien kiintolevyille.
- Tee vianselvitystä varten DVD:lle tai USB-tikulle virtuaalinen ”työkalupakki”, joka sisältää tärkeitä apuohjelmia laitteiden ja verkon vianmääritykseen.
- Järjestä verkon ylläpitäjälle varayhteys julkisiin verkkoihin ennakkoon työkalujen ja avun saantiin mahdollisessa verkkohyökkäysvaiheessa.

Ennakkoon – varmista, valmistu ja valista

- Varmista kriittiset tiedot säännöllisesti ja usein. Tee useita eriaikaisia varmistuksia ja säilytä ne turvallisesti eri paikassa kuin varsinainen järjestelmä. Testaa tietojen palautus.
- Jos mahdollista, pyri pitämään matalaa profiilia verkossa, älä elämöi turvallisuudellasi. Turvallisuudella uhoaminen houkuttelee hyökkääjiä.
- Seuraa tehostetusti verkon tapahtumia mahdollisen negatiivisen julkisuuden aikana (esim. irtisanomiset, ympäristövahingot, johdon väärinkäytökset).
- Tee toimintasuunnitelmat ja valmistelut mahdollisten verkkohyökkäysten varalta. Testaa ja kouluta ne.
- Informoi työntekijöitä haittaohjelmista ja verkon vaaroista sekä niiltä suojautumisesta.

Toiminta yksittäisen koneen saastuessa

- Yksittäisen koneen saastuessa, eristä saastunut kone verkosta esimerkiksi irrottamalla sen verkkokaapeli.
- Pyri dokumentoimaan tapahtuma esimerkiksi kuvaamalla digikameralla näytön tapahtumat. Kirjaa tapahtumat ja kellonajat ylös. Pyydä työtoveri todistajaksi.
- Sammuta saastunut laite irrottamalla sen virtajohto ja akku. Älä käytä virtakytkintä tai järjestelmien sulkemisnäppäimiä.
- Älä yritä käynnistää konetta uudelleen.
- Jos epäilet rikosta (tietomurtoa / yritysvakoilua / luvatonta käyttöä), tee asiasta rikosilmoitus ja noudata poliisin ohjeita todisteiden keruussa.
- Muussa tapauksessa toimita kone huoltoon.
- Pyri selvittämään tarttumistapa, arvioi vahingot ja käynnistä korjaustoimet (mm. tiedottaminen, verkon skannaus, salasanojen vaihto, ohjelmien päivitys, käyttöoikeuksien muutos).

Toiminta [hajautetussa] palvelunesto-hyökkäyksessä ([Distributed] Denial Of Service = [D]DOS)

- Ota yhteys internet-operaattoriisi, ilmoita tilanteesta ja pyydä apua hyökkäyksen torjuntaan.
- Ota käyttöön kevennetty julkinen verkkosivusto, poista tarpeettomat palvelut.
- Tarvittaessa rajoita organisaation internetliikennettä ja mahdollisuuksien mukaan sulje tilapäisesti julkisten palvelujen yhteydet ydinjärjestelmiin.
- Jos käytössäsi on vaihtoehtoinen www-osoite, joka ei ole hyökkäyskohde, vaihda toiminta tilapäisesti sille (esim. *yritys.com* → *yritys.fi*).
- Ilmoita hyökkäyksestä Viestintäviraston (Ficora) tietoturvatiimille (Cert-FI).

Tee ilmoitus poliisille.