Kyber- ja hybridiuhkien torjumisen muistilista lappilaisille yrityksille

LAPIN
KAUPPAKAMARI

ESIPUHE

Venäjän hyökkäyssota ja Suomen Natokeskustelu ovat kiihdyttäneet uhkia kyberturvallisuuden ja hybridivaikuttamisen rintamilla.

Kyberturvallisuudella tarkoitetaan esimerkiksi hyökkäyksiä yrityksen tietoverkkoihin, tietojenkalastelua, haittaohjelmia tai kiristyshaittaohjelmia. Kyberturvallisuudesta huolehtiminen on myös tapa varautua hybridivaikuttamisen uhkiin.

Hybridiuhilla tarkoitetaan pahantahoista vaikuttamista, jossa ulkopuolinen valtiollinen toimija pyrkii vaikuttamaan kohdemaahan. Hybridivaikuttamisen keinot voivat olla niin taloudellisia, poliittisia kuin sotilaallisia. Myös yritykset voivat olla väline hybridivaikuttamisen toteuttamiseen.

Tämän muistilistan tarkoitus on muistuttaa toimialariippumattomasti **erilaisten kyber- ja hybridiuhkien torjunnan tärkeydestä.** Muistilista on ensimmäinen askel yritysten häiriötilanteisiin varautumisen kehittämistä.

Ovatko yrityksesi ohjeistukset kunnossa?

- Pelastus- ja turvallisuus-suunnitelma
- Työterveyssuunnitelma
- Tietoturva
- Vakuutukset
- Rahoitussuunnitelma
- Riskienhallintasuunnitelma
- Henkilöstösuunnitelma
- Varautumissuunnitelma
- Kriisiviestintäsuunnitelma

Riskienhallinta varautumisen keskeisimpänä keinona

Käy läpi yritystoimintasi erilaiset skenaariot:

- Mitä jos liiketoimintani keskeisiin prosesseihin (henkilöstö, tietoliikenne, tietojärjestelmät, infra, omaisuus, varasto jne.) tulee häiriö?

Kun häiriötilanne on päällä, nopea toiminta ja selkeät toimintatavat voivat pelastaa paljon.

- Miten toimin häiriötilanteessa: mihin yllä olevista skenaarioista voin varautua etukäteen?
- Missä ovat liiketoiminnassa tarvittavat yhteystiedot tai varmuuskopiot tietojärjestelmistä?
- Onko henkilökuntani koulutettu häiriötilanteiden varalle?
- Onko yritykseni riippuvainen yhden henkilön tietotaidosta ja ns. hiljaisesta tiedosta?
- Miten yritykseni viestii kriiseissä?

Kaikkiin riskeihin on mahdotonta varautua etukäteen. Valmiusasteen nosto kriisien hallinnassa voi kuitenkin auttaa yritystä toipumaan kriiseistä nopeammin, kuin tilanteessa, jossa minkäänlaiseen kriisiskenaarioon ei olisi etukäteen valmistauduttu.

KYBERTURVALLISUUS

Kyberturvallisuuskeskus on listannut huhtikuussa 2022 suurimmat kyberturvallisuudet uhat.

Uhissa mainitaan esimerkiksi nopeasti muuttuva poliittinen ja taloudellinen toimintaympäristö, joka vaikuttaa suoraan kyberturvallisuuteen. Kyberrikoksissa käytetään hyväksi tietojärjestelmien haavoittuvuuksia. Henkilökunnan taidot ja tietojärjestelmien käyttöoikeudet nostetaan kyberuhkien kärkeen.

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen. Ilmiöt voivat näkyä digitaalisessa toimintaympäristössä nopeasti ja aiheuttaa vaikeasti ennakoitavia tapahtumia kyberturvallisuudessa.

2

Johtaminen ja riskienhallinta. Toimintaympäristön nopeat muutokset koettelevat organisaatioiden riskienhallintaa kyberturvallisuudessa. Johdon vastuulla on varmistaa riskienhallinnan vaikuttavuus.

3

Päivittämättömät haavoittuvuudet avaavat rikollisille reitin organisaatioon. Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

Symbolit

Uusi

Päivitetty

4

Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille! Tarve kyberturvallisuuden osaajille monipuolistuu uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta osaajille.

5

Käyttöoikeudet ovat avaimet organisaatioon. Käyttöoikeuksien kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle tunnusten ollessa väärissä käsissä.

Lähde: Kyberturvallisuuskeskus, maaliskuun 2022 Kybersää

Muistilista kyberturvallisuuteen

- Tunnista mitä digivälineitä yritykseni käyttää?
  - Puhelin, tietokone, maksupääte, muut laitteet ja ohjelmistot, kodinkoneet
- Verkon tietoturva ja päätelaitteen tietoturva kuntoon > huomioi molemmat
- Henkilöstön osaaminen ajan tasalle
- Ajantasaiset tietoturvaohjelmat sähköisiin laitteisiin
- Käytä vain luotettuja langattomia verkkoja
- Ota käyttöön tunnistautumisen kaksivaiheinen todennus myös sosiaalisessa mediassa
- Vaihda salasanat säännöllisesti, myös henkilöstön vaihtuessa
- Pidä järjestelmien käyttöoikeuksien hallinta ajan tasalla, poista käyttöoikeudet henkilöiltä, jotka eivät ole enää yrityksessä töissä, tai joiden tehtävänkuva ei vaadi pääsyä järjestelmiin
- Opi tunnistamaan huijaus- ja kalasteluviestit
- Suojaa muistikirjat ja tietokoneet ulkopuolisilta
- Tutustu GDPR asetukseen ja opi soveltamaan sitä
- Ota tietojärjestelmistä säännöllisesti varmuuskopiot
- Varmista, että häiriötilanteessa varmuuskopiot on helposti käyttöönotettavissa
- Pilvipalveluiden tietoturva: kysy palveluntarjoajalta minkälainen käyttämäsi pilvipalvelun tietoturva on
- Tarkista tarvitsetko vakuutusyhtiön tarjoamaa tietoturvavakuutusta
- Opi laitteiden etätyhjentäminen esimerkiksi varkauksien varalta
- Sulje luottokortit katoamistapauksissa
- Aseta kaikkiin laitteisiin pääsykoodi

Lisätietoja: Pienyritysten kyberturvallisuusopas

Muistilista hybridiuhkien torjuntaan

**Hybridiruhkien torjunta on yritysten näkökulmasta haastavampi kokonaisuus.
On kuitenkin tunnistettu, että yrityksiä voidaan käyttää hybridivaikuttamisen välineinä.
Hybridivaikuttamisen muodot ovat moninaisia.**

- Anna aikaa riskienhallinnalle ja varautumisen suunnittelulle, tunnista yrityksesi kriittiset toiminnot ja analysoi riskienhallinnan nykytila
- Mitkä yrityksen toiminnot ovat yrityksen jatkuvuuden kannalta keskeisiä?
- Tunnista informaatiovaikuttaminen, lue lisää:
  Vinkkejä informaatiovaikuttamisen tunnistamiseksi – Ole tarkkana ja toimi vastuullisesti
- Keneltä tilaan palveluita: toimiiko yhteistyöverkostoni ammattimaisesti, keneen olen yhteydessä erilaisissa häiriötilanteissa?
- Ota tietojärjestelmien kopiot saataville, muista että kopio muodostaa oman henkilörekisterin, josta on tehtävä rekisteriseloste
- Henkilöriskien hallinta: mistä yrityksen keskeiset tiedot, laitteet, salasanat löytyvät – miten järjestämme varahenkilötoiminnan
- Dokumentoi toimintaa osana jatkuvuuden varmistamista
- Tunnista urkkiminen, estä jututtaminen

Urkkimiseen varautuminen

❶ **Tiedä** mitä tietoja yrityksestä ei pidä jakaa. Tämä koskee myös henkilökohtaisia tietojasi, perhettäsi ja kollegojasi.

❷ **Torju** kohteliaasti epäasialliset keskustelunaiheet. Ohjaa julkisiin tietolähteisiin.

❸ **Ohita** epäasialliset kysymykset ja kannanotot tai vaihda suoraan aihetta.

Lähde: Helsingin seudun Kauppakamari.
Lisätietoja: Yritysturvallisuus2021-tiedon-urkkiminen.pdf

Huomioi myös

» Varaudu palveluestohyökkäyksiin ja nojaa asiantuntijapalveluihin. Tarjolla on esimerkiksi “tietoliikennepesureita” vähentämään verkkosivujen haittaliikennettä.

» Osallistu Keskuskauppakamarin Lujat –hankkeen tilaisuuksiin: kauppakamari.fi/vaikuttaminen/yritysturvallisuus

» Ohje poikkeustilanteiden henkilövarauksiin: puolustusvoimat.fi/asiointi/henkilovaraukset

LAPIN KAUPPAKAMARI