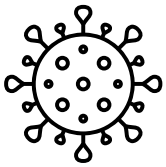
Sote-alan pienyrittäjän (1–9 työntekijää) kyberkriisiharjoitus



Harjoituksen tavoitteet:

- Parantaa pienyrittäjän kykyä tunnistaa ja vastata kyberhyökkäyksiin.
- Auttaa arvioimaan omaa ymmärrystä kyberuhkista ja kyberhyökkäyksistä.
- Auttaa arvioimaan yrityksen nykyisiä kyber- ja tietoturvasuunnitelmia ja ohjeita.
- Auttaa tutkimaan vaihtoehtoisia tapoja tietojen palauttamiseen
- Auttaa tunnistamaan tieto- ja kyberturva-aukot.

Harjoituksessa on suositeltavaa käyttää seuraavia dokumentteja:

- Tietoturvasuunnitelma
- Liiketoiminnan jatkuvuussuunnitelma
- Varmuuskopiointisuunnitelma

Osallistujat:

Tämä suunnitelma on laadittu siten, että voit toteuttaa sen yksin, kuten normaalistikin tekisit töitä tai mukana voi olla niin suuri tai pieni osa henkilökunnasta kuin haluat, eikä kenenkään harjoitukseen osallistuvan tarvitse olla tietoturva-asiantuntija.

Skenaario:

Työntekijän lapsi on sairaana kotona ja hän tekee etätyötä muutaman päivän. Päivän aikana työntekijä soittaa ja kertoo sinulle tietokoneongelmista. Seuravana päivänä huomaat, että tietokoneesi on hitaampi ja muutama tiedosto on virheellinen.

CyberCare Kymi -hanke
Rahoituksen myöntänyt Kymenlaakson liitto, Euroopan Unionin osarahoittamana.
https://www.xamk.fi/cybercare

Harjoituksen kulku

Häiriötilanteen alku:

Hengitä syvään.

- Pystytkö eristämään koneet verkosta?
- Pystytkö sammuttamaan verkon kokonaan?
- Määritä mitkä tiedot ovat virheellisiä ja miten kriittisiä ne ovat yrityksellesi.
- Jos työpaikalla on useampia tietokoneita, selvitä kuinka laajalle häiriö on levinnyt.

Ensitoimet:

- Päätä välittömistä toimista. Mikäli sinulla on olemassa suunnitelma tällaisen tilanteen varalta, ota se esiin. Onko tätä tilannetta kuvattu tietoturvasuunnitelmassa? Onko näitä riskejä otettu huomioon riskianalyysissä? Mikäli sinulla ei ole tällaista suunnitelmaa, jatka seuraavaan kohtaan.
- Mieti, keneen verkostossasi tai yhteisössäsi voit ottaa yhteyttä avun ja neuvojen saamiseksi.
- Miten voit selvittää, mikä tietokoneessa voisi olla vikana? Löytyykö koneista virustorjuntaohjelmaa? Onko se käytössä ja ovatko sen päivitykset ajan tasalla? Tiedätkö miten voit käyttää ohjelmaa tietokoneen tarkistamiseen?
- Arvioi täysin järjestelmiesi sulkemisen ja niiden toiminnassa pitämisen riskit ja hyödyt.

Viestintä:

- Viestintäsuunnitelma. Onko sitä olemassa? Päätä, miten tiedotat asiakkaitasi tapahtuneesta.
- Tunnista, mitä tietoja on jaettava asiakkaille ja miten voit vähentää paniikkia varmistaen samalla potilastietojen yksityisyyden.
- Miten viestit asiasta työntekijöillesi?
- Mikäli sinulla on valmiina kriisiviestintäpohjia, ota ne käyttöön. Mikäli niitä ei ole, etsi internetistä malliaineistoa esimerkiksi hakusanalla kriisiviestintä. Tässä vaiheessa valmiit peruspohjat viestintää varten voivat säästää sinulta paljon kallista aikaa.

CyberCare Kymi -hanke
Rahoituksen myöntänyt Kymenlaakson liitto, Euroopan Unionin osarahoittamana.
https://www.xamk.fi/cybercare

Liiketoiminnan jatkuvuus:

- Mieti valmiiksi keinot, kuinka varmistat asiakashoidon tilanteessa, jossa sinulla ei ole pääsyä sähköisiin asiakastietoihin tai muihin kriittisiin tietoihin.
- Mitä tietoja sinulla on paperilla? Kuinka näihin papereihin pääsee käsiksi? Voivatko mahdolliset paperiarkistot toimia tilapäisesti toiminnan jatkamiseksi.
- Mitä eri tapoja tai kanavia sinulla on tavoittaa asiakkaasi ja järjestääksesi toimintasi uudelleen?
- Mitä välittömiä taloudellisia vaikutuksia liiketoimintasi pysähtymisellä tai häiriintymisellä on sinulle?

Tietojen palautus:

- Kehitä suunnitelma tietojen ja järjestelmän palauttamiseksi. Selvitä, onko sinulla riittävät varmuuskopiot, ovatko ne palautettavissa ja turvallisia?
- Mille laitteelle voit palauttaa tiedot? Onko tietokonetta turvallista käyttää?
- Toteuta toimenpiteitä tulevien kyberuhkien estämiseksi, kuten tietoturvaprotokollien parantaminen, yhteistyön lisääminen asiantuntijoiden kanssa ja oman osaamisen kehittäminen.
- Keskustele palautumisaikataulusta ja mahdollisista vaikutuksista palveluiden tuottamiseen palautusprosessin aikana.

Häiriötilanteen jälkianalyysi:

- Tunnista vahvuudet ja heikkoudet varautumisessa ja kyberhäiriön aikaisissa ja sitä seuranneissa toimenpiteissä.
- Keskustele opituista asioista ja parannusalueista tietoturvakäytännöissä ja tapahtumien vastausmenettelyissä.
- Dokumentoi opitut asiat sekä suunnitellut seuraavat askeleet.
- Miten olisit voinut estää tartunnan?
- Oliko yrityksellä riittävät resurssit ja osaaminen tietoturvapoikkeaman hallintaan?
- Miten viestintä sujui tilanteen aikana?

CyberCare Kymi -hanke
Rahoituksen myöntänyt Kymenlaakson liitto, Euroopan Unionin osarahoittamana.
https://www.xamk.fi/cybercare

Jatkotoimenpiteet:

- Kehitä suunnitelmiasi harjoituksessa tunnistettujen parannustarpeiden mukaan.
- Aseta aikataulut ja tarkistuskohteet jatkotoimenpiteiden suorittamiselle.
- Aikatauluta säännölliset tarkistukset ja päivitykset varmistaaksesi jatkuvan valmistautumisen ja kyvyn selviytyä kyberuhkista.
- Testaa varmuuskopioita säännöllisesti. Varmista että ne ovat ajan tasalla, toimivat, ja osaat palauttaa tarvitsemasi tiedot niiden avulla.
- Dokumentoi harjoituksen löydökset ja kehityskohteet.

Tärkeimmät verkkosivut ja puhelinnumerot:

- Tietosuojavaltuutetun toimisto: https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta
- Poliisi: https://poliisi.fi/tee-rikosilmoitus (arkisin klo 8 – 16.15 0295 419 800)
- Kyberturvallisuuskeskus: https://www.kyberturvallisuuskeskus.fi/ – Tietoturvaloukkaus-lomake: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita (029 534 5630)
- Valvira: https://valvira.fi/sahkoinen-asiointi (jos potilas- ja/tai asiakasturvallisuus vaarassa)

CyberCare Kymi -hanke
Rahoituksen myöntänyt Kymenlaakson liitto, Euroopan Unionin osarahoittamana.
https://www.xamk.fi/cybercare