Sote-alan pienyrittäjän (1–9 työntekijää) kyberkriisiharjoitus

Harjoituksen tavoitteet:

- Parantaa yksinyrittäjän kykyä tunnistaa ja vastata kyberhyökkäyksiin.
- Auttaa arvioimaan yksinyrittäjän 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
- Viestintäsuunnitelma
- 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:

Pyörität omaa yritystäsi. Kirjauduit tietokoneellesi aloittaaksesi työpäiväsi. Mutta jotakin onkin vialla. Näytölle ei ilmesty tuttua työpöytää, vaan pelkkä outo teksti.

Tehtävä: Lue seuraavaksi kiristysviestin teksti, jossa löydät lopussa.

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

Harjoituksen kulku

Häiriötilanteen alku:

Hengitä syvään.

- Määritä, mitkä tiedot ovat tosiasiallisesti kyberhyökkääjän lukitsemia ja miten kriittisiä salatut tiedot ovat yrityksellesi.
- Mitkä ovat yrityksen tärkeimmät järjestelmät ja tiedot? Ovatko juuri ne tiedot lukittuina?
- Tunnista mahdolliset seuraukset tietovuodosta, esimerkiksi oikeudellisia seuraamuksia, mainehaittoja ja vaikutuksia potilashoitoon.
- Arvioi hyökkääjien antama aikataulu. Kuinka paljon aikaa sinulla on ennen kuin hän toteuttaa uhkauksensa?

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.
- Arvioi vaihtoehtosi: pidätkö kaikki järjestelmäsi suljettuina vai onko mahdollista esimerkiksi kirjautua toisilta täysin erillisiltä laitteilta joihinkin käyttämiisi ohjelmistoihin?
- Ota yhteyttä tietosuojavaltuutetun toimistoon, poliisiin (arkisin klo 8 - 16.15 0295 419 800), Kyberturvallisuuskeskukseen ja Valviraan (jos potilas- ja/tai asiakasturvallisuus vaarassa). Dokumentin lopussa löytyy linkit.

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

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.
- 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.

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?

Päätöksenteko:

- Arvioi lunnasvaatimusten maksamisen laillisuutta ja eettisyyttä. Mitkä ovat lunnasvaatimuksen kustannukset verrattuna siihen, että et maksa?
- Kannattaako vaadittuja lunnaita maksaa vai toimitko jollakin muulla tavalla? Konsultoi tarvittaessa lakimiehiä tai tietoturva-asiantuntijoita.
- Pohdi päätöksen pitkäaikaisia vaikutuksia liiketoiminnallesi.

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

Tietojen palautus:

- Tee suunnitelma tietojen ja järjestelmän palauttamiseksi. Selvitä, onko sinulla varmuuskopioita, miltä ajalta ne ovat ja ovatko ne turvallisia.
- Mitä kaikkea tarvitsee tehdä, mikäli lunnasvaatimukseen ei suostuta ja kaikki on rakennettava uudelleen alusta saakka? On myös mahdollista, ettei rikollisilla ole aikomustakaan palauttaa tietoja, vaikka maksaisit heille.
- Tämä myöhemmin: Keskustele palautumisaikataulusta kenen kanssa ja mahdollisista vaikutuksista potilashoitoon palautusprosessin aikana.

Häiriötilanteen jälkianalyysi:

- Pohdi, mitkä asiat menivät hyvin ja mitä heikkouksia löysit valmistautumisessasi sekä toiminnassasi tilanteen aikana. Tunnista vahvuudet ja heikkoudet valmistautumisessa ja reagoinnissa.
- Käy läpi tilannetta myös muiden kanssa. Keskustele opituista asioista ja parannusalueista tietoturvakäytännöissä ja tapahtumien vastausmenettelyissä.
- Dokumentoi opitut asiat ja päivitä dokumentaatiosi.

Jatkotoimet:

- Aikatauluta säännölliset kyber- ja tietoturvadokumentaatiosi ja -toimintatapojesi tarkistukset sekä päivitykset.
- Testaa varmuuskopioitasi säännöllisesti ja palauta niitä myös. Varmuuskopioiden säännöllinen testaaminen.
- Harjoittele.

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

Lunnasvaatimusviesti

Olemme salanneet asiakkaittesi terveystiedot vahvoilla salausalgoritmeilla, mikä tekee tietojen saamisesta mahdottoman ilman salauksen purkuavainta. Yritys purkaa tietoja ilman apuamme johtaa tiedostojesi peruuttamattomaan menetykseen.

Saadaksesi purkuavaimen ja uudelleen pääsyn tietoihisi, sinun on maksettava lunnaita **1 Bitcoin** osoitteeseen: **1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa**.

Jos et noudata vaatimuksiamme **48 tunnin** kuluessa, seurauksena on purkuavaimen peruuttamaton poistaminen, mikä tekee tietosi palauttamattomaksi. Lisäksi joudumme julkaisemaan arkaluontoiset potilastietosi verkossa yleisön saataville.

Aloittaaksesi maksun ja saadaksesi lisäohjeita, ota yhteyttä meihin osoitteeseen **ransom@ransom.fi**. Liitä sähköpostisi aihekenttään uniikki **tunniste 789456** varmennustarkoituksiin.

Älä ota yhteyttä lainvalvontaviranomaisiin tai tietoturvaviranomaisiin, koska he eivät kykene auttamaan sinua tässä asiassa. Kaikki yritykset jäljittää tai puuttua toimintaamme johtavat välittömään ja peruuttamattomaan tietojesi tuhoamiseen.

Ymmärrämme potilastietojesi tärkeyden ja olemme halukkaita tarjoamaan todisteita purkukyvystämme heti, kun lunnasmaksu on vastaanotettu. Luota siihen, että tarjoamme purkuavaimen välittömästi maksun vahvistamisen jälkeen.

Muista, että aikaa on rajallisesti. Toimi nopeasti estääksesi tietojesi peruuttamattoman menetyksen.

Pöytäharjoitus-Kiristäjät

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

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