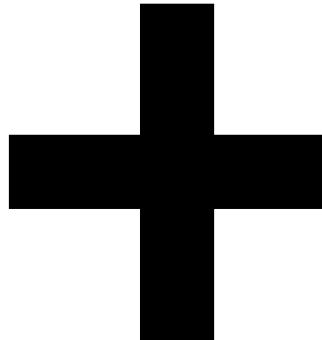


PressurePrevention

Data Privacy
Incident Response



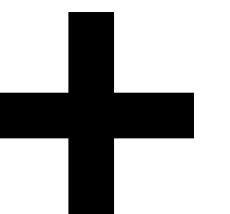
Skenaario

PressurePrevention on terveysteknologiayritys, joka tarjoaa tuotteen korkean verenpaineen ennaltaehkäisemiseen.

12.3.2025 klo 9:30 yritys sai tiedon tietomurrosta. Kolme asiantuntijaa aloittivat heti asian selvittämisen ja korjaamisen.

Ryhmään kuului:

- Data Protection Officer / Compliance Manager
- Data Engineer
- Communications Officer



Päivän kulku D+0

Tietomurrossa yrityksen työntekijä oli vuotanut EU-alueella ja USA:ssa asuvien asiakkaiden henkilötietoja sekä EU-alueella asuvien asiakkaiden terveystietoja tahallisesti.

09:30-10:30

- Tieto tietoturvatapaturmasta /tietovuodosta.
- Vastuutettiin oikeat henkilöt (Teknologia, viestintä, juridinen puoli).
- Sisäisesti tiedotettu asiasta, ja lakiosaston kanssa pohdittu, mitä tietoja voidaan antaa mahdollisissa asiakaskyselyissä.
- Avattu keskusteluyhteys lainoppineiden ja vakuutuksista vastaavien kanssa.
- Aloitettu raportointi ja listattu tahot, joille laki velvoittaa tiedottamisen, sekä aikarajat ja laajuus.
- Lähdetty tunnistamaan tietovuotoa ja ehkäisemään lisävahinkoja.

10:31-11:15

- Vuoto sisältää terveysdataa EU-alueelta, ja tiedot rikollisten kässissä.
- Viranomaisiin otettu yhteyttä välittömästi.
- Viestintä aloittaa asiakastiedotteen valmistelun. Lisätty uusi puhelinnumero asiakaspalveluun tapausta varten.
- Valmistellaan tiedote nettisivulle ja medialle.
- Aloitettu juridisten seuraamusten arviointi ja mitigointi. Verrataan verkossa olevia tietoja sisäisiin tietokanavoihin.
- Pyydetty analysointiapua (mm. Europol, CERT-FI, Traficom ja muut paikalliset DPA:t).

11:16-13:00

- Selvitetty, että tuotekehityksessä ollut henkilö on vuotanut tiedot, ja ne ovat usean rikollisen tahon hallussa.
- Johtoryhmälle kysymys, vaikuttaako tilanne yrityksen osakkeilla kaupankäyntiin
- Työntekijän pääsy yrityksen tietoihin poistettu, laitteet takavarikoitu ja sähköpostit sekä someviestit tutkitaan.
- Selvitetään, voiko tapaukseen liittyä muita työntekijöitä tai ex-työntekijöitä.
- Listataan "reasonable security measures" ja pyritään osoittamaan raportoinnissa, ettei tietosuojavelvoitteita ole laiminlyöty (vaikuttaa sakon suuruuteen).
- Esitetään DMCA-takedown-pyyntö, jos tiedot eivät ole dark webistä.

13:01-14:00

- Tieto, että murron kohteena on yli 50 000 henkilöä.
- Tämä vaikuttaa riskitasoon ja tiedottamisen laajuuteen

14:01 -

- Tieto, että murron tekijä on kytköksissä terroristijärjestöön.
- Osakkeenomistajille ja hallitukselle aletaan valmistelemaan raportteja.
- Johtoryhmä osallistuu asiointiin osakkeenomistajien kanssa.
- Suojelupoliisi otetaan mukaan tekniseen tutkintaan.
- Varaudutaan viranomaisten lisätoimiin ja mahdollisiin oikeudellisiin toimiin terroristiyhteyksien vuoksi.
- Päivitetään asiakastiedotteet ja valmistellaan laajempi tiedottaminen julkisuuteen.
- Selvitetään, onko kyseessä mahdollinen jatkuva uhka, nostetaan uhkatasoa tarpeen mukaan ja suunnitellaan jatkotoimenpiteet.

+ Viestinnän tehtävät

- Sisäiset palaverit IT:n ja Data Protection Officerin/Compliance Managerin kanssa pitkin päivää
- Viranomaisille ilmoitukset tietomurrosta (esim. poliisi, SUPO, EU Data Protection Authorities ja US state regulators)
- Poliisille rikosilmoitus tietomurron tehneestä työntekijästä
- Viestintäsuunnitelma; keitä kaikkia tulee tiedottaa ja millä aikataululla
 - Pitää huomioida lainsäädännöt tiedotuksissa (mitä voi tiedottaa)
- Tiedotteiden ja ohjeistusten laatiminen ja toimittaminen tarvittaville sidosryhmille
 - Lisäksi tiedotteiden päivitys, mikäli uutta tietoa tilanteeseen liittyen ilmenee
- Asiakaspalveluun oman linjan avaaminen tietomurtoon liittyville kysymyksille
- Somessa kommenttien seuraaminen tilanteeseen liittyen ja niihin reagointi
- Listan kerääminen asiakkaista, joiden tiedot ovat vuotaneet ja suunnitelma henkilökohtaisista yhteydenotoista lisäämään luottamusta yritystä kohtaan



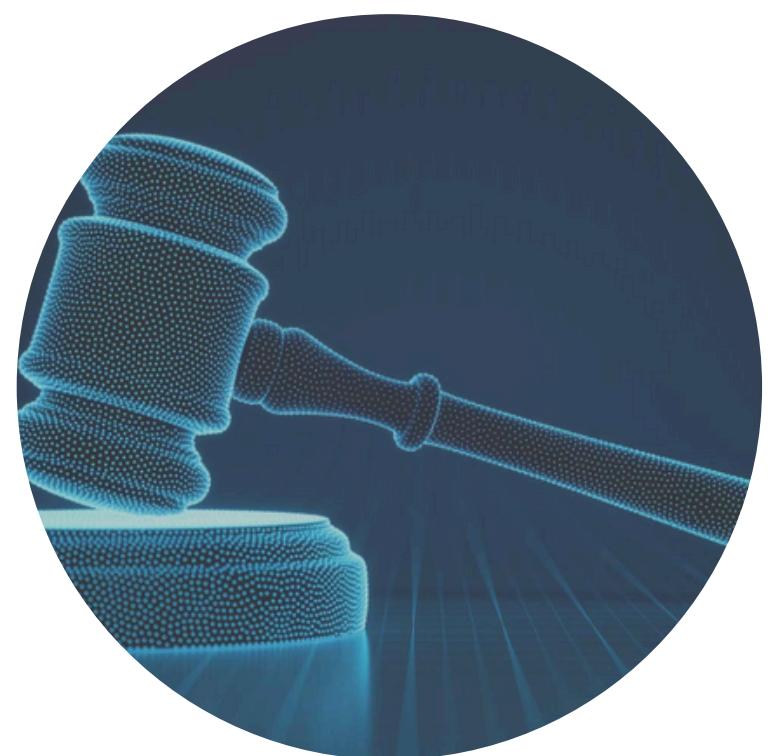
+ Tekninen reagointi

- Vaihe 1: Havaitseminen ja tunnistaminen (murron lähteen ja ajankohdan selvitys, vaikutuksen arvointi, eristetään vaarantuneet järjestelmät)
- Vaihe 2: Eristetään ja poistetaan haittoja (vahingoittuneiden järjestelmien suojaaminen, forensiikkatutkinta)
- Vaihe 3: Viestintä (sisäisesti lakiimille viestinnälle johdolle, ulkoisesti viranomaiset ja muu apu)
- Vaihe 4: Korjaavat toimenpiteet ja ehkäisy (turvatoimien vahvistaminen, haavoittuvuustestit, riskien arvointi, dokumentointi ja koulutus)
- Vaihe 5: Jälkiseuranta ja jatkuva valvonta (lokit, tietomurron lopullinen vahvistus, auditointi, pitkän aikavälin turvallisuusparannukset)



+ Lailliset velvollisuudet

- Yhteydenpito lailliseen edustukseen ja vakuutustahoihin:
Valmistaudutaan asiakkaiden nostamiin oikeustapauksiin ja selvitetään
vakuutsuyhtiön korvausvelvollisuus.
- Viestinnän ja raportoinnin oikeellisuus:
Pidettävä huolta, että lailliset viestintävelvoitteet toteutuvat ja riittävät
tiedot toimitetaan oikeille tahoille
- Vahingon mitigointi: Pyritään osoittamaan raporteilla ja
toimintakuvauksilla, että ei olla laiminlyöty velvoitteita. Jos
laiminlyöntejä ilmenee, voivat ne vaikuttaa negatiivisten
vaikutusten suuruksiin
- Dokumentointi ja riskinarvointi:
Riskitasoa ja vaikutuksia on jatkuvasti arvioitava. Aiheutuuko yksityishenkilöiden
vapaauksille tai oikeuksille haittaa. Kaikki dokumentit pitää voida toimittaa
viranomaisille pyynnöstä.
- GDPR:n noudattaminen eli Compliance:
Varmistetaan GDPR:n mukaiset toimet tapauksen käsitelyn jokaisessa vaiheessa ja
tulevaisuudessa. Valmistellaan dokumentti jossa käydään läpi GDPR:n vaatumat
kohtuulliset tietoturvatoimenpiteet



Turvallisuusselvitykset (SUPO)

Viranomaisen tekemä taustatarkistus, jolla arvioidaan uuden työntekijän luotettavuutta ja soveltuvuutta tehtävään, erityisesti silloin, kun työ liittyy kansalliseen turvallisuuteen tai arkaluontoiseen tietoon. Selvitys voi sisältää esimerkiksi rikosrekisteritietojen ja taloudellisen tilanteen tarkastelun.

Jatkuva valvonta

Järjestelmien, verkkojen ja käyttäjätoiminnan reaalialaista seurantaa uhkien, poikkeamien ja haavoittuvuuksien havaitsemiseksi. Sen tavoitteena on nopea reagointi ja riskien minimointi.

RBAC

RBAC (Role-Based Access Control) on käyttöoikeuksien hallintamalli, jossa käyttöoikeudet myönnetään roolien perusteella eikä yksittäisille käyttäjille. Käyttäjät saavat oikeuksia heidän rooliensa mukaan, mikä parantaa turvallisuutta ja helpottaa hallinnointia.



Varautuminen tulevaan

Kitos!



Linda
Tomi
Tuukka

+

