Johdon tietoturvakoulutus 16.12.2024

Marko Buuri

talous hallinnon koulutukset

1

Järjestömme noudattaa kilpailulakia

talous hallinto liitto

Kilpailulaki kieltää sellaiset sopimukset, päätökset sekä yhdenmukaistetut menettelytavat, joiden tarkoituksena on merkittävästi estää, rajoittaa tai vääristää kilpailua tai joista seuraa, että kilpailu merkittävästi estyy, rajoittuu tai vääristyy.

Mikäli keskustelu liittyy kiellettyyn teemaan, kaikkien osallistujien tehtävä on lopettaa keskustelu. Emme keskustele seuraavista teemoista, jotka sisältävät jäsenen luottamuksellista tietoa:

- Yksityiskohtaiset sopimusehdot
- Toimittajat, asiakkaat
- Tarjoukset
- Tuotantomäärät
- Laajentumissuunnitelmat, jotka eivät vielä julkisia
- Muut tulevaisuudensuunnitelmat (esim. T&K-panostukset, tuotantoseisokit)

- Alan yleinen hintataso ja siihen vaikuttaminen
- Hinnoittelukäytännöt ja –mekanismit
- Osto- ja myyntihinnat
- Markkinaosuudet
- Kustannukset
- Kannattavuus
- Yhteiset boikotit

24.10.2023

talous hallinto liitto

Huoltovarmuuskeskus

Kysymys-vastausklinikka: Tietoturvahäiriöt ja poikkeamatilanteiden hallinta

2024

Tervetuloa taloushallintoalan johdon tietoturva- ja tietosuojakoulutukseen!

talous hallinto liitto

Huoltovarmuuskeskus

- Webinaarit
  - 8.11.2024 Ajankohtaiskatsaus: Kyberturvallisuuden tämän hetken trendit ja uhkakenttä
    Kysymys-vastausklinikka: Turvallisuusjohtaminen
  - 2.12.2024 Ajankohtaiskatsaus: Tekoäly ja taloushallinto
    Kysymys-vastausklinikka: Toimittajahallinta
  - 16.12.2024 Kysymys-vastausklinikka: Tietoturvahäiriöt ja poikkeamatilanteiden hallinta + TALk-keskustelu

Agenda

Kysymys-vastausklinikka: Tietoturvahäiriöt ja poikkeamatilanteiden hallinta

- Miten PK-yritys voi varautua tietoturvapoikkeamiin?
- Miten PK-yrityksen tulisi toimia tietoturvapoikkeamissa?
- Miten PK-yritys voi ennaltaehkäistä tietoturvapoikkeamia?

11.12.2024 ©Taloushallintoliitto

Tietoturvapoikkeamien vaikutukset yrityksen toimintaan

talous hallinto liitto

Huoltovarmuuskeskus

Tietoturvapoikkeama on tilanne, jossa tietoturva on oikeasti vaarantunut, kuten tietojärjestelmien tai tietojen luvaton käyttö tai tuhoaminen.

Tietoturvapoikkeamat voivat

- aiheuttaa operatiivisia häiriöitä yrityksen toiminnassa.
- aiheuttaa suoria taloudellisia menetyksiä, kuten tietojen palautuskustannuksia, korjaus- ja jälleenrakennuskuluja sekä mahdollisia sakkoja ja oikeudenkäyntikuluja.
- heikentää yrityksen mainetta asiakkaiden, yhteistyökumppaneiden ja sijoittajien silmissä.

©Taloushallintoliitto

Tietoturvapoikkeamiin varautuminen

talous hallinto liitto

Huoltovarmuuskeskus

Tietoturvapoikkeamien olosuhteet ja piirteet hankaloittavat niiden hallintaa:

- Onnistuneiden kyberhyökkäysten ajankohtaa ei voi ennakoida.
- Poikkeaman tunnistaminen voi olla vaikeaa; se voi näyttäytyä henkilöstölle esimerkiksi tietojärjestelmän hitautena, muuttuneina sisältöinä, tai muuna IT-toimintahäiriönä.
- Poikkeaman analysointi vaatii usein teknistä erityisosaamista.

Näistä syistä varautumisessa tavoitellaan kolmea asiaa:

1. Toimintamalli poikkeamien hallintaan tulee rakentaa ennalta ja olla tarvittavien osapuolten tiedossa.
2. Hyödynnetään teknisiä ratkaisuja poikkeamien havaitsemiseksi.
3. Henkilöstöllä ja soveltuvin osin kumppeneilla tulisi olla ohjeet tietoturvapoikkeamien tunnistamiseksi, ja niiden eskaloimiseksi sovituille avainhenkilöille.
4. On olemassa suunnitelma siitä, miten tarvittava asiantuntija-apu on saatavilla poikkeamatilanteessa.

11.12.2024 ©Taloushallintoliitto

Tietoturvapoikkeamiin varautuminen

talous hallinto liitto

Huoltovarmuuskeskus

1. Havaitseminen ja arviointi
2. Ensimmäiset kriittiset toimet
3. Selvitys ja toimenpiteet
4. Toipuminen ja palautuminen
5. Tilanteesta oppiminen

On yleistä, että tietomurto havaitaan niin myöhään, että merkittävää vahinkoa on jo syntynyt.

Esimerkkejä:

- Helsingin kaupungin tietomurto 2024 havaittiin tuoreeltaan epätyypillisestä tietoliikenteestä.
- Lemonsoftin tietomurto 2023 tuli ilmi, kun palvelimia meni lukkoon.
- Vastaamon tietomurto tuli ilmi 2020, kun hyökkääjä julkaisi kiristysviestin. Tietokanta oli viety jo yli vuotta aiemmin.
- Erään pääomasijoitusyhtiön tietomurto tuli ilmi, kun työntekijä havaitsi lähetetyissä sähköposteissaan ylimääräisen viestin.

Tietoturvapoikkeaman havaitseminen

talous hallinto liitto

Huoltovarmuuskeskus

1. Identiteetit kuten Active Directory, Entra, Google
2. Päätelaitteiden käyttöjärjestelmät, sovellukset, tietoturvaohjelmistot
3. Yrityksen omien palvelinten käyttö-järjestelmät, sovellukset, tietoturvaohjelmistot
4. Yrityksen omat verkot, palomuurit, nimipalvelut (DNS) ja etäkäyttöpalvelut (VPN)
5. Pilvipalvelualustat ja -sovellukset

Tietoturvalokit eli tekniset tapahtumatiedot

Automaattinen valvonta ja hälytykset

Manuaalinen valvonta

11.12.202 4 ©Taloushallintoliitto

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Huoltovarmuuskeskus

talous hallinto liitto

Opas tietomurtojen havaitsemiseen

Traficomin opas tietomurtojen havaitsemiseen vuodelta 2020 on kattava katsaus asiaan.

Parhaan hyödyn oppaasta saavat tekniset asiantuntijat.

Varautumisen mahdollisia toimia

talous hallinto liitto

Huoltovarmuuskeskus

Hallinnolliset toimet

- Tunne pilvipalvelusi
- Suunnittele ja dokumentoi poikkeamanhallintatoimet
- Määrittele roolit ja vastuut

Ote Kyberturvallisuuskeskuksen ohjeesta “Toimintaohje – Pilviympäristöjen poikkeamanhallinta”

Tekniset toimet

- Suunnittele pilviympäristö huolella
- Noudata palveluntarjoajien ohjeistamia käytäntöjä
- Varmista kehitys- ja tuotantoympäristöjen turvallisuus
- Pienennä hyökkäyspinta-alaa
- Aseta resurssien käytölle kulubudjetti
- Varmista pääsy palveluihin hätätilanteessa
- Varmista riittävät varmuuskopiointi- ja toipumismenettelyt
- Määrittele ja toteuta lokitus
- Monitoroi ympäristöjä ja havaitse poikkeamat
- Suunnittele poikkeamatilanteen selvityksen tekninen toteutus

Tietoturvapoikkeamiin varautuminen: Roolit ja vastuut

talous hallinto liitto

Huoltovarmuuskeskus

1. Havaitseminen ja arviointi
2. Ensimmäiset kriittiset toimet
3. Selvitys ja toimenpiteet
4. Toipuminen ja palautuminen
5. Tilanteesta oppiminen

Kuka tekee ja mitä?

Tehtäviä ainakin:
- Tilanteen johtaminen
- Juridinen analyysi
- Viestintä (ulkoinen ja sisäinen)
- Tekninen juurisyyanalyysi
- IT-palveluiden palauttaminen

Oman henkilöstön rooli?

IT-palvelu-tuottajan rooli?

Sovellus-palvelu-tuottajan rooli?

Poikkeamiin erikoistuneet konsultit?

Tietoturvapoikkeaman käsittelyn vaiheet

talous hallinto liitto

Huoltovarmuuskeskus

1. Havaitseminen ja arviointi

2. Ensimmäiset kriittiset toimet

3. Selvitys ja toimenpiteet

4. Toipuminen ja palautuminen

5. Tilanteesta oppiminen

Poikkeaman havaitseminen
Käytä valvontatyökaluja ja järjestelmiä, jotka tunnistavat poikkeavan toiminnan ja ilmoittavat havainnoista.

Ensivaiheen arviointi
Arvioi nopeasti poikkeaman laajuus ja vakavuus. Selvitä, mitkä tiedot tai järjestelmät ovat mahdollisesti vaarantuneet ja kuinka laaja poikkeama on.

Pohdi:
Edellä keskustelimme poikkeamiin varautumisesta. Mistä ensimmäinen havainto tai signaali tulee? Kuka sen käsittelee? Kuka arvioi onko kyseessä poikkeama vai ei?

Tietoturvapoikkeaman käsittelyn vaiheet

talous hallinto liitto

Huoltovarmuuskeskus

1. Havaitseminen ja arviointi

2. Ensimmäiset kriittiset toimet

3. Selvitys ja toimenpiteet

4. Toipuminen ja palautuminen

5. Tilanteesta oppiminen

Vaikutusten rajoittaminen
Toteuta toimenpiteitä, jotka rajoittavat poikkeaman aiheuttamia vahinkoja. Esimerkiksi, jos epäilette joidenkin tunnusten väärinkäyttöä, sulkekaa tunnukset käytöstä. Saastuneeksi epäilty tietokone tulee irrottaa internetyhteydestä ja säilyttää muutoin tutkintaa varten mahdollisimman muuttumattomana.

Eskaloi tarvittaville tahoille
Raportoi poikkeama välittömästi niille tahoille, jotka liittyvät asian selvittämiseen.

Pohdi:
Ketkä osapuolet organisoituvat? Mitkä tilit tai pääsyt täytyy sulkea? Miten näihin kysymyksiin vaikuttaa se, koskeeko poikkeama vaikka PC-tietokoneita tai käyttämäänne pilvipalvelua?

Tietoturvapoikkeaman käsittelyn vaiheet

talous hallinto liitto

Huoltovarmuuskeskus

1. Havaitseminen ja arviointi
2. Ensimmäiset kriittiset toimet
3. Selvitys ja toimenpiteet
4. Toipuminen ja palautuminen
5. Tilanteesta oppiminen

Selvitä mistä on kyse ja tee tarvittavat toimet
Selvitä mahdollisimman tarkoin mitä tilanteessa on tapahtunut. Hyvä tilannekuva on olennaista oikeista toimenpiteistä päättämiseksi. Määritelkää selvitystyön johtamisen vastuut.

Ilmoita viranomaisille
Mahdollisen henkilötietojen tietoturvaloukkauksen tapauksessa ilmoita asiasta tietosuojavaltuutetulle toimiessasi rekisterinpitäjänä. Epäiltäessä rikosta, tee ilmoitus poliisille. Traficomin Kyberturvallisuuskeskus ottaa vastaan ilmoituksia kaikista tietoturvapoikkeamista.

Pohdi:
Kuka johtaa tilannetta?
Kuka viestii asiakkaille ja yhteistyökumppaneille?
Kuka viestii viranomaisille?

Tietoturvapoikkeaman käsittelyn vaiheet

talous hallinto liitto

Huoltovarmuuskeskus

1. Havaitseminen ja arviointi
2. Ensimmäiset kriittiset toimet
3. Selvitys ja toimenpiteet
4. Toipuminen ja palautuminen
5. Tilanteesta oppiminen

Pohdi:
Onko yrityksen omissa tietokoneissa ja palvelimilla olevia tietoja varmuuskopioitu? Jos käyttämänne pilvipalvelun tietoja tuhottiin, tiedättekö pystyykö palveluntuottaja ne palauttamaan ja millä aikataululla?

Tietojen ja sovellusten palauttaminen
Palauta tiedot, tunnukset ja sovellukset toimintaan vaiheittain, varmistaen, että ne ovat täysin turvallisia ja että kaikki haavoittuvuudet on korjattu ennen palauttamista.

Tietoturvapoikkeaman käsittelyn vaiheet

1. Havaitseminen ja arviointi
2. Ensimmäiset kriittiset toimet
3. Selvitys ja toimenpiteet
4. Toipuminen ja palautuminen
5. Tilanteesta oppiminen

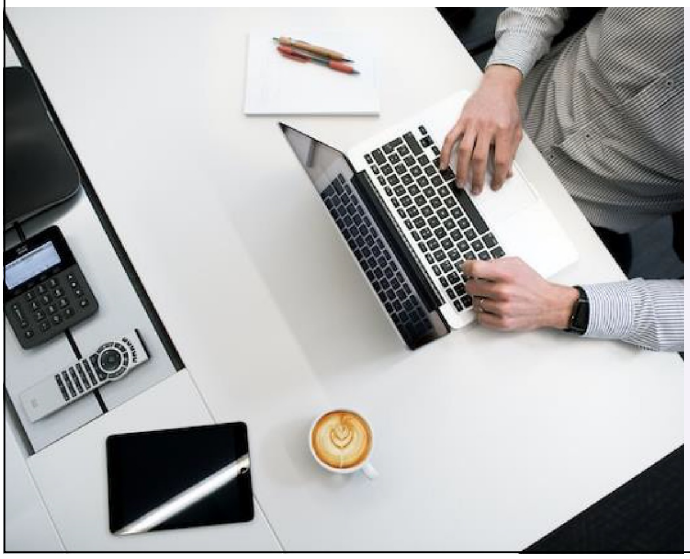
Muista kerätä opit ja tarvittaessa harjoitella vastaavien tilanteiden varalta.

Oppiminen ja parantaminen
Suorita poikkeaman jälkeinen analyysi ymmärtääksesi, miten ja miksi poikkeama tapahtui. Käytä näitä tietoja parantaaksesi yrityksen tietoturvakäytäntöjä.

Muista myös viranomaiset

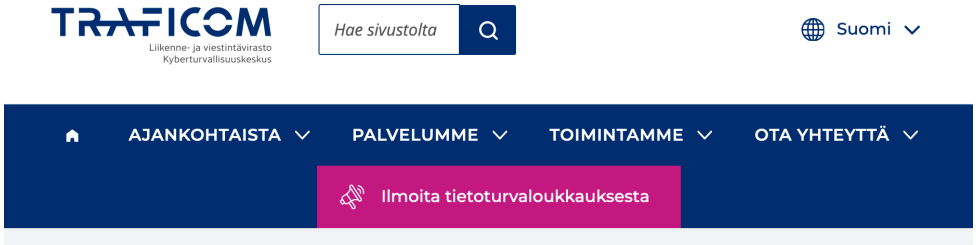
- **Kyberturvallisuuskeskukselle** voi ilmoittaa vapaaehtoisesti tietoturvapoikkeamista. Tämä auttaa heitä tilastoimaan ja muodostamaan tilannekuvaa kyberturvallisuudesta.
- Jos epäilet rikosta, asiasta on syytä ilmoittaa **poliisille**. Tietotekniikkaan ja tietoverkkoihin kohdistuvia rikoksia ovat esimerkiksi tietomurrot, luottokorttitietojen tai pankkitunnusten kalastelu, haittaohjelmien avulla tehdyt tietojen kaappaukset tai erilaiset verkkohyökkäykset.
- Henkilötietojen tietoturvaloukkauksesta on ilmoitettava **tietosuojavaltuutetun toimistolle** ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa.

Henkilötietojen tietoturvaloukkaukset



Esimerkkejä:

- Henkilötietoja lähetetään väärälle vastaanottajalle.
- Henkilötietoja tuhotaan tai muutetaan vahingossa.
- Luvaton taho pääsee käsiksi pilvipalveluun ja vie henkilötietoja.
- Yrityksen työntekijä tarkastelee henkilötietoja ilman työhön liittyvää syytä, esimerkiksi uteliaisuudesta.
- Henkilötietoja sisältävä tietokone, jonka sisältöä ei ole suojattu salaamalla ja pääsykoodilla, varastetaan.



TIETOTURVA NYT!

Toimi näin, jos havaitset tietoturvapoikkeaman

Julkaistu 21.04.2020 13:38

Murtauduttiinko sähköpostiisi, saitko oudon linkin tekstiviestillä, tuliko koneellesi haittaohjelma? Kun tietoturvapoikkeama osuu kohdalle, siitä on hyvä ilmoittaa sekä viranomaisille että omalle IT-tuelle. Neuvomme, kuinka teet ilmoituksen eri viranomaisille.

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toimi-nain-jos-havaitset-tietoturvapoikkeaman

Yritys voi rajoittaa tietoturvapoikkeamien mahdollisuutta merkittävästi muutamalla perustoimenpiteellä

talous hallinto liitto

Huoltovarmuuskeskus

1. Käyttäjätunnukset ovat tärkein puolustuslinja. Pidä huolta siitä, että kaikissa laitteissa ja palveluissa on vain luvallisten käyttäjien tunnuksia, käytössä on monivaiheinen tunnistaminen aina kun mahdollista, ja silloin kuin ei ole, salasanat on suojattu hyvin.
2. Pidä huoli siitä, että kaikkien verkkoon liitettyjen laitteiden ohjelmistot päivitetään säännöllisesti. Verkkorikolliset osaavat hyödyntää päivityksissä korjattuja vikoja pian niiden julkaisun jälkeen.
3. Päätelaitteiden tulisi sisältää suojausohjelmisto, joka lähettää tietoturvahälytyksiä automaattisesti.
4. Työntekijöillä ei tulisi olla mahdollisuutta asentaa sovelluksia omalla käyttäjätunnuksella.
5. Kouluta työntekijät varovaisuuteen sähköisten palveluiden ja luottamuksellisten tietojen käsittelyssä.


Kiitos!
Marko Buuri
talous
hallinto
liitto
Huoltovarmuuskeskus