Johdon tietoturva

Turvallisuusjohtaminen ja kyberturvallisuuden tämän hetken trendit ja uhkakenttä

talous
hallinnon
koulutukset

1

Järjestömme noudattaa kilpailulakia

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

Kyberturvallisuuden tämän hetken trendit ja uhkakenttä

Kysymys-vastausklinikka: Turvallisuusjohtaminen

Johdon livekoulutus 1

2024

2

Tervetuloa taloushallintoalan johdon tietoturva- ja tietosuojakoulutukseen!

talous hallinto liitto

Huoltovarmuuskeskus

- Kohderyhmä
- 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

4

Sisältö

talous hallinto liitto

Huoltovarmuuskeskus

Kyberturvallisuuden johtamisen ajankohtaisia trendejä

1. Generatiivinen tekoäly
2. Toimittajariskien hallinta ICT-palveluissa
3. Haavoittuvuuksien jatkuva monitorointi
4. Identiteettien ja pääsynhallinnan kehittäminen

Uhkaympäristön tapahtumia

- Akira- ja Lockbit-kiristyshaittaohjelmat

5.11.2024 ©Taloushallintoliitto

Generatiivinen tekoäly

- Generatiivinen tekoäly on yleisnimitys tekoälytuotteille, jotka luovat uutta sisältöä.
- Merkittävä hyöty tietotyön tehostamisessa (erilaiset Copilotit, ChatGPT jne.)
- Tulevaisuudessa esimerkiksi yhä tehokkaampaa ohjelmistokehitystä, robottiautomaatioita sekä BI-datan analysointia.
- Tärkeintä jokaisen yrityksen varmistaa nyt, että työpaikalla on sovittu pelisäännöt tekoälypalveluiden käytöstä. Näkökulmia:
  - Tulosten oikeellisuuden kanssa oltava tarkkana
  - Osa palveluista toimii EU:n ulkopuolella
  - Osa palveluista varaa oikeuden asiakkaan tietojen hyödyntämiseen.

Toimittajariskien hallinta ICT-palveluissa

- Yritysten IT-palvelut nojaavat yhä enemmän palveluhankintoihin omien järjestelmien sijaan.
- Maailmalla on tapahtunut ICT-palvelutoimittajien häiriöitä, joista on aiheutunut suuria vahinkoja heidän asiakkailleen.
  - Case: Tietoevry
  - Case: CrowdStrike
- Asiakkaan ja toimittajan vastuunjako.

7

Vastuunjako pilvipalveluissa

- Pienille yrityksille yleisin pilvipalveluiden hankintamalli on sovelluspalvelu eli SaaS. Esimerkkejä SaaS-palveluista ovat
  - Google Workplace-palvelut ja Microsoft 365-palvelut, jotka molemmat ovat helposti käyttöönotettavia sähköposti-, dokumentinhallinta-, ja yhteistyöpalveluita, sekä
  - asiakastiedonhallinnan, taloushallinnon, laskutuksen, ja henkilöstöhallinnon palvelut, jotka toimitetaan valmiina ratkaisuina ja joita käytetään selaimella.
- Joillakin palvelutuottajilla on heidän toiminnan laatua ja varmuutta kuvaavia sertifiointeja, kuten ISO 9001 (laatujärjestelmä) ja ISO 27001 (tietoturvajärjestelmä).
- SaaS-palveluissa asiakkaan vastuulla on aina palveluiden luvallisten käyttäjien määrittäminen, pitäen sisällään käyttäjät ja heidän roolinsa. Tämän lisäksi selvitettäviä palvelukohtaisia asioita ovat ainakin
  - millaisia asiakaskohtaisia valintoja tietoturvan suhteen on mahdollista tehdä, esimerkiksi asettaa hälytyksiä, turvarajoja, tai kirjautumiseen liittyviä kontrolleja,
  - muodostuuko palvelun käytöstä asiakkaan käyttäjien tunnuksilla sellaista audit-lokia, joka mahdollistaa epäiltyjen väärinkäytösten tutkinnan,
  - miltä osin palveluntuottaja varmuuskopioi tietoja, ja voiko asiakas valinnoillaan vaikuttaa tähän. Esimerkiksi, jos luvallinen käyttäjä vahingossa tuhoaa tietoja, ovatko ne palautettavissa?

5.11.2024

Haavoittuvuuksien jatkuva monitorointi

- Riittääkö haittaohjelmatorjunta ja säännölliset Windowsin tietoturvapäivitykset? Miten seurataan että nämä asentuvat ja toimivat kuten pitääkin?
- Yritykset panostavat yhä enemmän kyberturvallisuuden työkaluihin, jotka automatisoivat ja keskittävät järjestelmien ja palveluiden tietoturvallisuuden hallintaa. Samalla tekninen tietoturvatyö tehostuu.
- Markkinoilla on erilaisia yrityksille tarkoitettuja palveluita, jotka mahdollistavat päätelaitteiden ja muiden järjestelmien tietoturvatason seurannan.
  - Palveluiden ominaisuuksissa ja hinnoissa on valtavasti eroa.
  - Pienen yrityksen on suositeltavaa tiedustella asiasta omalta IT-palvelutuottajalta.

Identiteettien ja pääsynhallinnan kehittäminen

talous hallinto liitto

Huoltovarmuuskeskus

- IT on muuttumassa järjestelmistä palveluiksi, ja tämä on muuttanut identiteettien eli tunnusten hallinnan ja pääsynhallinnan roolia tietoturvassa.
- Esimerkiksi Googlen ja Microsoftin identiteettipalveluissa on kehittyneitä toimintoja, jotka tunnistavat mahdollisia väärinkäytöksiä analysoimalla esimerkiksi
  - käyttäjän toimintaa,
  - päätelaitteiden ominaisuuksia, ja
  - sijaintitietoja.
- Huomioi että vaikka nämä palvelut muodostavat audit-lokeja automaattisesti, lokit eivät ole oletuksena saatavilla kuin muutamia kuukausia. Pidempi säilytysaika edellyttää asiakaskohtaisia toimenpiteitä.

Akira- ja Lockbit-kiristyshaittaohjelmat

talous hallinto liitto

Huoltovarmuuskeskus

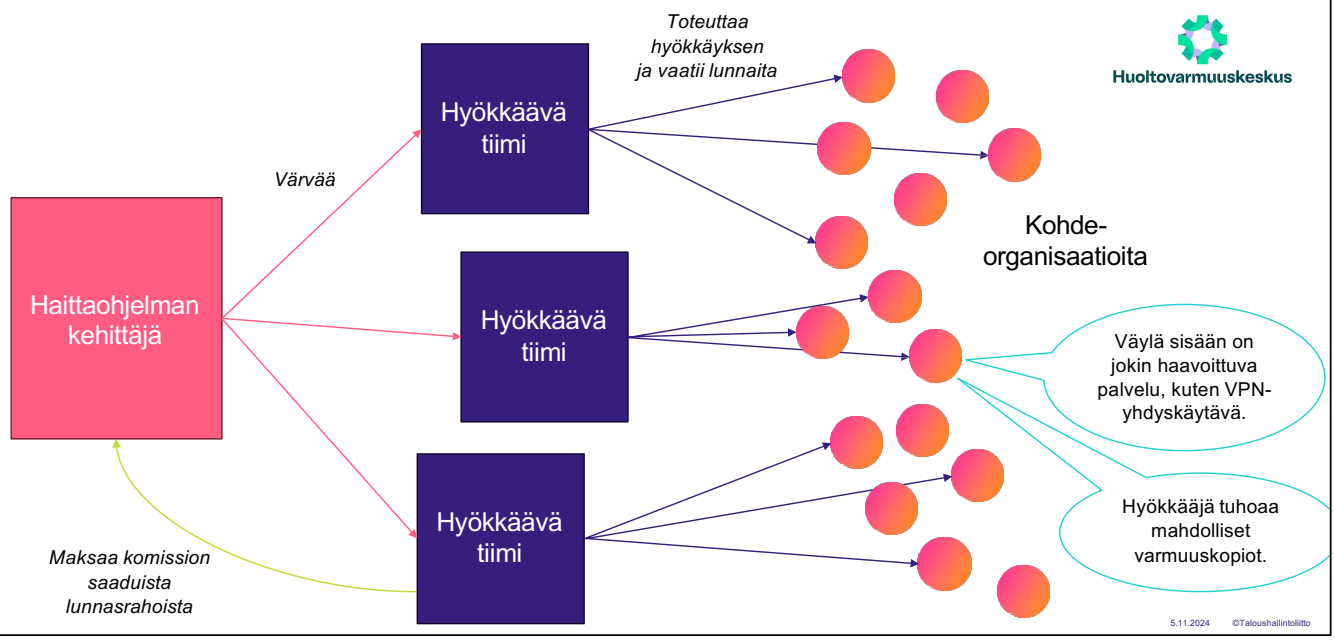
- Kyberturvallisuuskeskuksen mukaan kiristyshaittaohjelmat ovat yksi merkittävimmistä organisaatioihin kohdistuvista kyberuhista.
- Viime vuosina Suomessa havaituissa kiristyshaittaohjelmahyökkäyksissä ovat korostuneet Akira ja Lockbit.
- Kyse on järjestäytyneestä rikollisuudesta jonka tavoitteena on rahallinen hyöty.

12

Järjestäytyneen rikollisuuden toimintamalli

talous hallinto liitto

Huoltovarmuuskeskus



5.11.2024

14

Sisältö

talous hallinto liitto

Huoltovarmuuskeskus

Klinikka:

1. Mitä turvallisuusjohtaminen tarkoittaa ja mitä hyötyä siitä on PK-yritykselle?
2. Mitä PK-yrityksen pitäisi tehdä, että turvallisuusjohtamista tapahtuisi ja teema kehittyisi?
3. Miten vastuut PK-yrityksen turvallisuuden johtamisessa tulisi määritellä?

5.11.2024 ©Taloushallintoliitto

15 **EK:n malli**

talous hallinto liitto

Huoltovarmuuskeskus

16 **Asiaa sivuavia standardeja**

talous hallinto liitto

Huoltovarmuuskeskus

Laadunhallintajärjestelmä	ISO 9000
Riskienhallinta	ISO 31000, ISO 31010
Toimitusketjun turvallisuus	ISO 28000
Jatkuvuudenhallinta	ISO 22301
Ympäristöjohtaminen	ISO 14000
Tietoturvallisuuden hallinta	ISO/IEC 27000
Omaisuudenhallinta	ISO 55000
Työterveys- ja turvallisuusjohtaminen	ISO 45000, OHSAS 18000
Yhteiskuntavastuu	ISO 26000
Energianhallinta	ISO 50001

17

Tyypillinen tilanne PK-yrityksessä

talous hallinto liitto

Huoltovarmuuskeskus

Johdon fokus suuntautuu pääasiassa ulkoiseen toimintaympäristöön, eli liiketoiminnan kehittämiseen ja asiakashankintaan

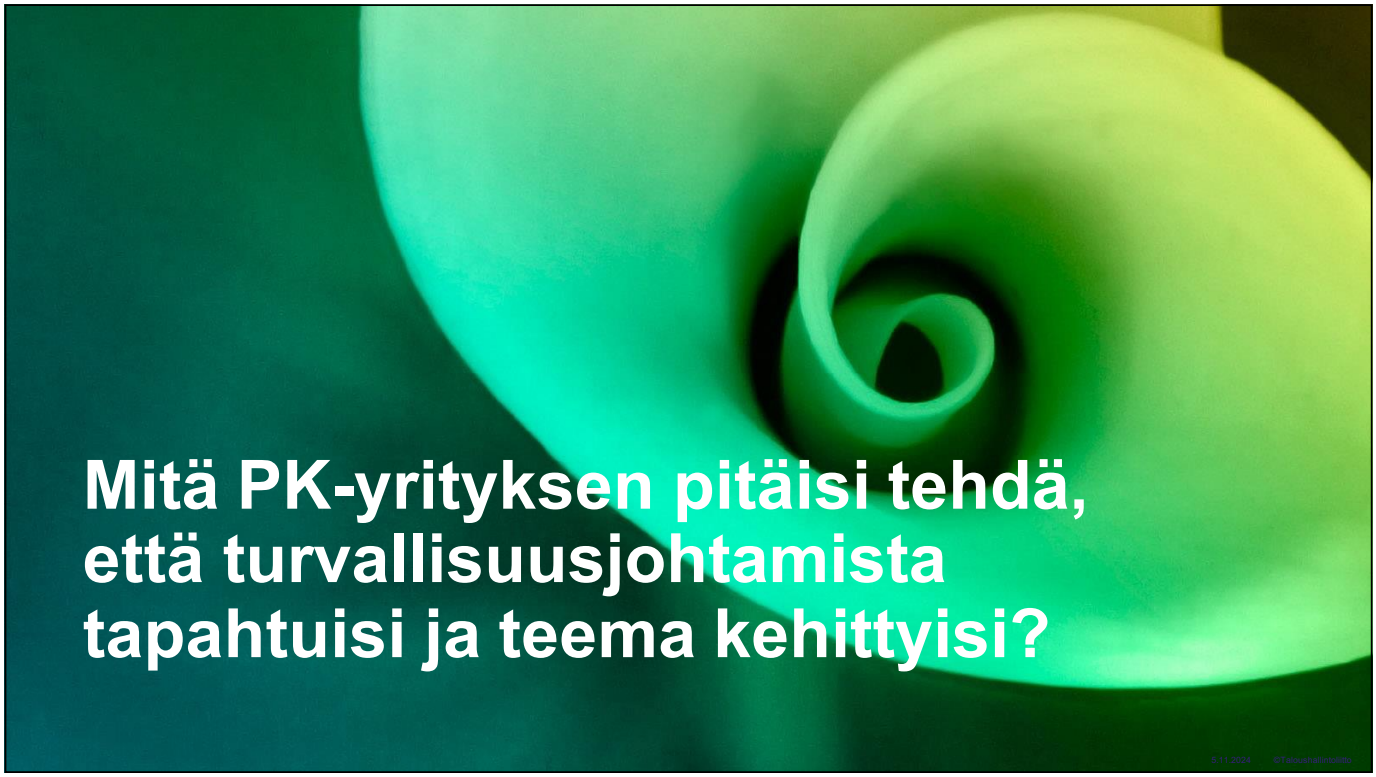
Turvallisuus on erityisosaamisalue, johon ei ole mahdollista palkata täysipäiväistä asiantuntijaa

Turvallisuusjärjestelyjen pitäisi olla riittävät, mutta ei hidastaa tai rajoittaa yrityksen toimintaa tai kehittämistä

Asiakkaille pitäisi olla jonkinlaista näyttöä auditointi- ja myyntitilanteissa

Toiminnan tulisi olla sääntelyn vaatimusten mukaista, esimerkiksi tietosuojakysymyksissä

5.11.2024 ©Taloushallintoliitto



19

Turvallisuusjohtamisen aloittaminen

Tärkeintä on johdon asennoituminen aiheeseen: **turvallisuusjohtaminen tarkoittaa samanlaista jatkuvaa tekemistä kuin mikä tahansa muu johtaminen**. Turvallisuus ei ole koskaan pysyvästi valmis, vaan sitä edistetään kulloinkin sopivalla tavalla ja resursseilla.

Sisäisen johtamisen malliin olisi hyvä tuoda turvallisuustekemisen työjono, jota seurataan säännöllisesti kuten mitä tahansa sisäisen kehittämisen työjonoa.

Lähestymistapa kurssilla

- Kurssilla esittelemme tietoturvallisuuden eri osa-alueita, ja annamme esimerkkejä niiden merkityksestä taloushallintoalalla.
- Tämän jälkeen ehdotamme kolmiportaisen “Tuumasta toimeen” kehittämismallin mukaisia toimenpiteitä: Aloita tästä → Kehitä → Paranna.
- Jokaisen yrityksen tulisi tehdä omakohtaista priorisointia siitä, mitä osa-alueita on tarkoituksen mukaista edistää kulloinkin. Yleensä tämä priorisointi on tarkoituksen mukaista kytkeä riskeihin, asiakasvaatimuksiin, tai regulaation vaatimuksiin.

5.11.2024 ©Taloushallintoliitto

20

Arviointimalleja

Erilaisia arviointimalleja voi hyödyntää sen arvioinnissa, millä tasolla oman yrityksen turvallisuusjohtaminen ja kontrollit ovat.

Tietoturvan arviointimalli tilitoimistoille	Kybermittari	Kansallinen turvallisuus-auditointi-kriteeristö Katakri	Pilviturvallisuuden arviointikriteeristö Pitukri
Tässä kokonaisuudessa kehitetään tietoturvan arviointimalli, joka soveltuu pienille ja keskisuurille tilitoimistoille. Tästä mallista tiedotetaan enemmän 2025 aikana.	Kybermittari on työkalu tietoturva-toiminnan kypsyyden mittaamiseen. Vaikka sen kohderyhmä ovat yhteiskunnan kriittiset toimijat, voi sitä soveltaa myös muihin toimijoihin.	Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset, kun käsitellään viranomaisten salassa pidettäväksi luokiteltuja tietoja.	Pitukri on tarkoitettu työkaluksi pilvipalvelujen turvallisuuden arviointiin. Sen sisältö perustuu viranomaisten salassa pidettäväksi luokiteltujen aineistojen vaatimuksiin.

5.11.2024 ©Taloushallintoliitto

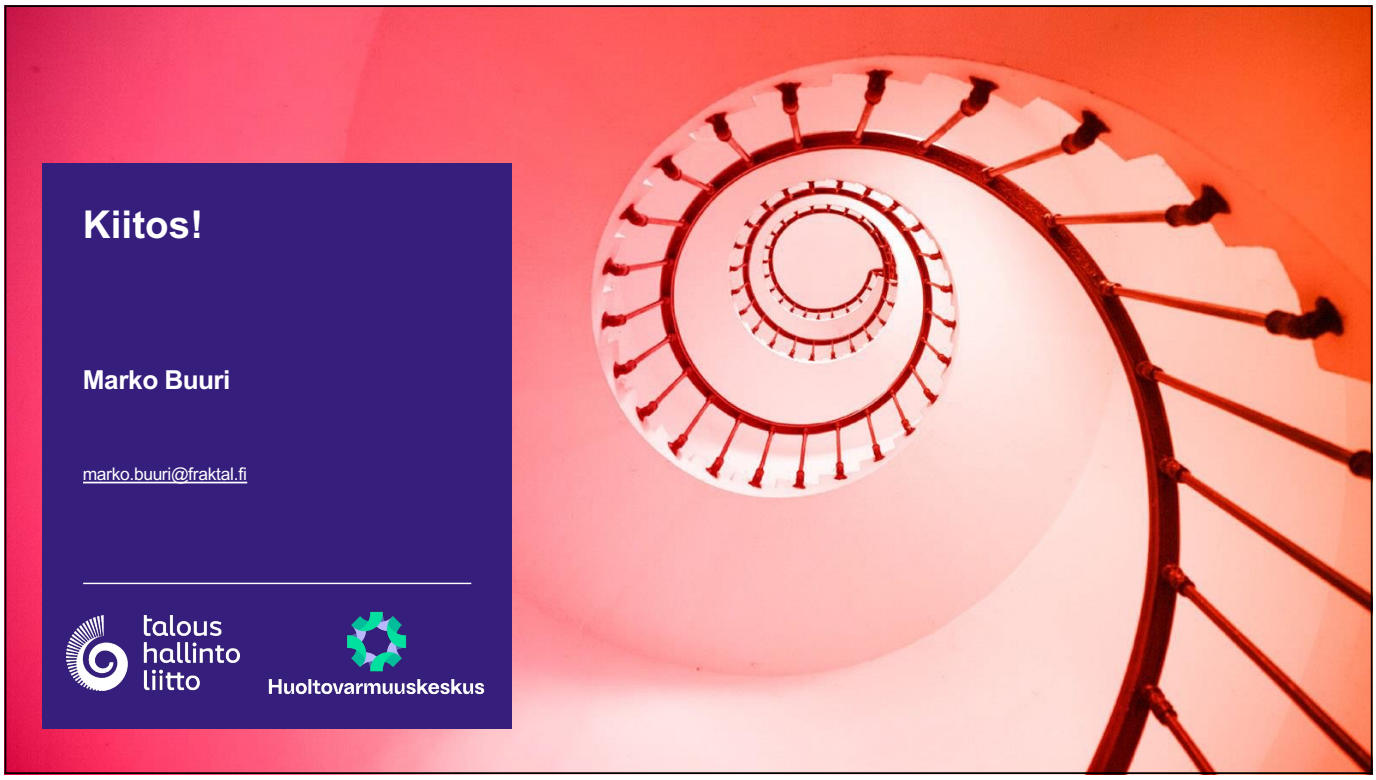
Miten vastuut PK-yrityksen turvallisuuden johtamisessa tulisi määritellä?

22 ## Vastuualueita

talous hallinto liitto

Huoltovarmuuskeskus

- Kuka vastaa myyntisopimuksista?
- Kuka vastaa operatiivisesta toiminnasta?
- Kuka vastaa ICT-laitteista ja –palveluista?
- Kuka vastaa työntekijöiden kouluttamisesta?


Kiitos!
Marko Buuri
marko.buuri@fraktal.fi
talous
hallinto
liitto
Huoltovarmuuskeskus