LAKIASIAINTOIMISTO VIVID OY

Riskienhallintaa tietoturvasopimuksin

24.4.2026

Noora Petäkoski
Lakiasiaintoimisto Vivid Oy

Ohjelma

- Tietoturvan rooli toimitusketjun riskienhallinnassa
- Riskien tunnistaminen ja arviointi
- Toimitusketjun riskienhallinnan sopimukselliset työkalut
- Mistä asioista on hyvä sopia toimitusketjussa?
- Hyvän toimittajahallinnan peruspilarit
- Kysymyksiä?

Tietoturvan rooli toimitusketjun riskienhallinnassa

Mitä tarkoittaa toimitusketjuhyökkäys?

Toimitusketjuhyökkäyksessä organisaation tietojärjestelmiin murtaudutaan sen käyttämien verkostojen, palveluiden, tuotteiden tai avoimen lähdekoodin projektien kautta. Hyökkäyksessä hyväksikäytetään organisaatioiden luottamusta toimittajiinsa. Hyökkäyksen reittinä voivat olla yhteistyökumppanit, palveluntarjoajat, ohjelmistot tai laitteet.

Toimitusketjuhyökkäyksen tavoitteena on jalansijan saavuttaminen eri organisaatioissa toimitusketjun varrella. Kun jalansija on varmistettu, voidaan sitä käyttää erilaisiin jatkohyökkäyksiin, kuten tietomurtoihin ja kiristyshaittaohjelmahyökkäyksiin.

Lähde: Traficom
ToimitusketjuhyökkäysToimintaohje.pdf

Tietoturvan rooli toimitusketjun riskienhallinnassa

NIS 2-direktiivi
Kyberturvallisuuslaki (124/2025)

Luokka	Esimerkkejä toimialoista
Erittäin kriittiset	Energia, liikenne, pankkitoiminta, terveydenhuolto, juomavesi, digitaalinen infrastruktuuri.
Muut kriittiset	Posti- ja kuriiripalvelut, jätehuolto, elintarvikkeiden tuotanto ja jakelu, kemikaalit, digitaaliset palveluntarjoajat.

7 §
Riskienhallinta

Toimijan on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuutta koskevalla riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin.

Toimijan on toteutettava riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin ja viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta.

Lähde: Finlex, kyberturvallisuuslaki

Tietoturvan rooli toimitusketjun riskienhallinnassa

•**Toimitusketjun turvallisuus:** Yritysten on varmistettava omien palveluntarjoajiensa ja alihankkijoidensa tietoturvan taso.

•**Kyberturvallisuuslaki 9 §, 4. kohta:** Toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on otettava huomioon ja pidettävä yllä ajantasaisesti ainakin:

”toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;”

• Yrityksen johto on suoraan vastuussa tietoturvatoimenpiteiden toteuttamisesta ja valvonnasta.

Riskien tunnistaminen ja arviointi

- **Kartoita toimitusketju ja järjestelmäriippuvuudet**
  - Missä data liikkuu?
  - Kenellä on pääsy dataan?
  - Mitä tietoa liikkuu?

- **Tunnista keskeiset uhat, joihin tulisi varautua:**
  - Luvaton pääsy ja tietovuodot
  - Palvelun keskeytykset
  - Lainsäädännön vastainen toiminta (esim. tietosuojarikkomukset)

- **Kyberuhat aiheuttavat toimitusketjuille merkittäviä riskejä, jotka voivat johtaa vakaviin toimintahäiriöihin, taloudellisiin tappioihin ja turvallisuusongelmiin.**

Toimitusketjun riskienhallinnan sopimukselliset työkalut

Uudet hankinnat
Nykyiset järjestelmät ja palvelut

- **NDA (Non-Disclosure Agreement):** Salassapitosopimus luottamuksellisen tiedon käsittelystä
- **Tietoturvavaatimukset:** Erilliset riskiarviointiin perustuvat vaatimukset palvelulle/järjestelmälle määrittäen vaaditut kontrollit (esim. salaus, lokitus, pääsynhallinta)
- **Tietoturvasopimus:** Sopimus tietoturvan osalta. Määrittää tietoturvan tason ja tietoturvatoimenpiteet palvelun tuottamisessa
- **DPA (Data Processing Agreement):** Tietosuoja-asetuksen vaatima sopimus henkilötietojen käsittelystä
- **SLA (Service Level Agreement):** Palvelutasosopimus varmistaa saatavuuden ja vasteajat
- **Jatkuvuussuunnitelma:** Suunnitelma sen varalta, että toiminta voi jatkua mahdollisimman häiriöttömästi, vaikka tapahtuisi jotain odottamatonta

Mistä asioista on hyvä sopia toimitusketjussa tietoturvan osalta?

”Tämän sopimuksen tavoitteena on varmistaa Pääsopimuksella hankittavien tuotteiden ja Palveluiden elinkaaren kattava tietoturvallisuus, Toimittajan toiminnan vaatimustenmukaisuus ja palvelutuotannon jatkuvuus erilaisissa häiriötilanteissa. Tavoitteena on lisäksi varmistaa Tilaajan aineiston luottamuksellisuus, eheys ja saatavuus.”

Mistä asioista on hyvä sopia toimitusketjussa tietoturvan osalta?

- **Kumppanin riittävä tietoturvan taso**
  - **Mitä tarkoittaa:** Kumppanin on osoitettava, että sen omat prosessit (esim. suojatut toimitilat, työntekijöiden koulutus, palomuurit) ovat riittävällä tasolla
  - **Käytännössä:** Voidaan mm. vaatia tiettyä sertifikaattia (kuten ISO 27001) tai vastaavan tasoista toimintaa, henkilökunnan perehdyttämistä jne.

- **Auditointioikeus**
  - **Mitä tarkoittaa:** Yritykselläsi (tai valitsemallasi kolmannella osapuolella) on oikeus auditoida kumppani, sen toiminta ja järjestelmät
  - **Käytännössä:** Vuotuinen tarkastus tai pistokoe kriittisissä palveluissa

Mistä asioista on hyvä sopia toimitusketjussa tietoturvan osalta?

- **Alihankkijoiden käyttö ja hallinta**
  - **Mitä tarkoittaa:** Kumppanilla on usein omia alihankkijoita. Yrityksesi on tiedettävä, ketä nämä ovat, ja kumppani vastaa siitä, että myös alihankkijat noudattavat asetettuja vaatimuksia
  - **Käytännössä:** Kumppani ilmoittaa käyttämänsä alihankkijat, eikä se saa vaihtaa alihankkijaa ilman yrityksesi hyväksyntää

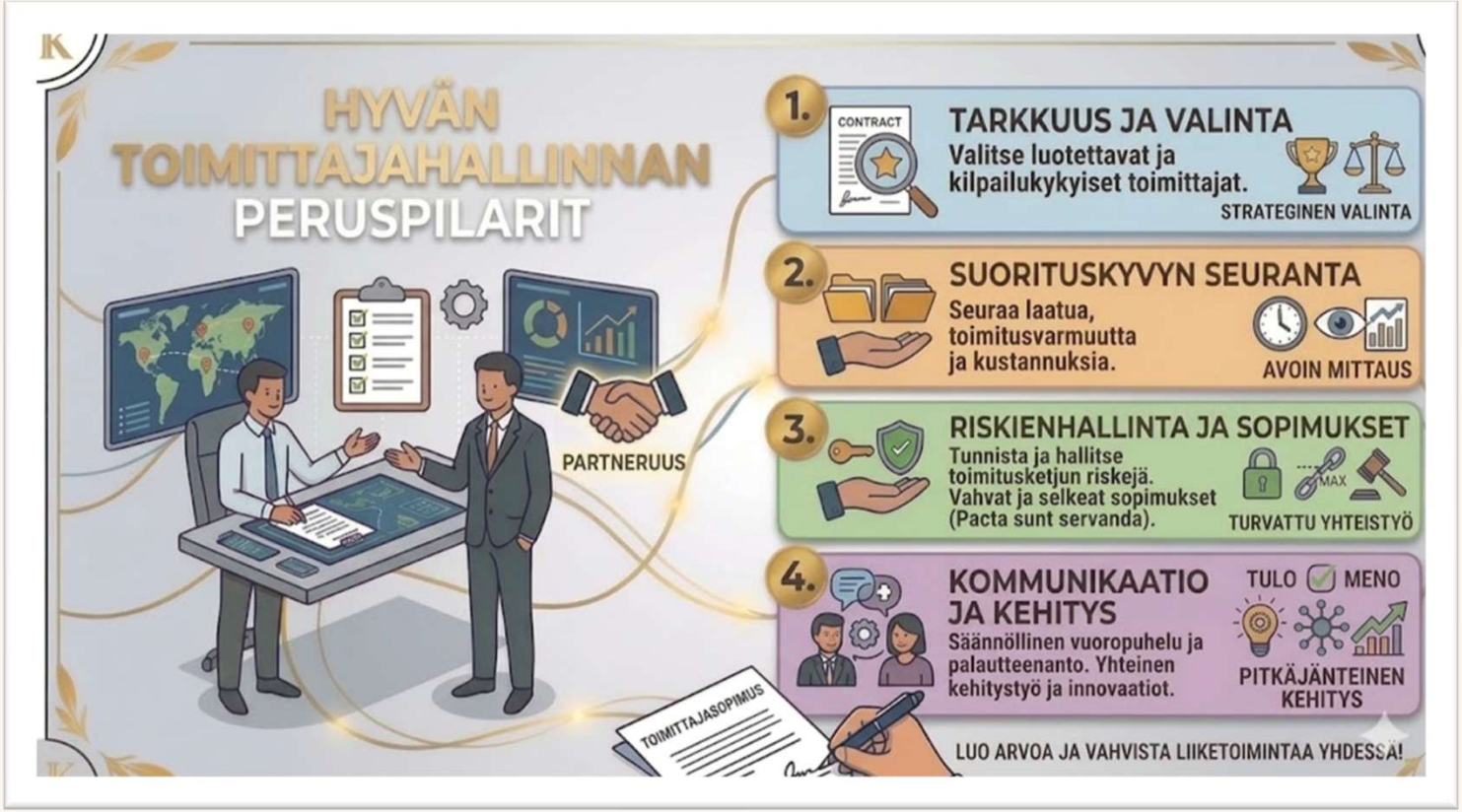
- **Poikkeamista ilmoittaminen** **(kyberturvallisuuslaki 11 §:** Ensi-ilmoitus on tehtävä 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta ja jatkoilmoitus 72 tunnin kuluessa merkittävän poikkeaman havaitsemisesta.)
- → **Mitä tarkoittaa**: Jos kumppaniin kohdistuu tietomurto tai tekninen häiriö, sen on ilmoitettava siitä yrityksellesi
  - **Käytännössä:** Sopimuksessa määritellään aikaraja ja kanava, jota pitkin tiedon on kuljettava

Mistä asioista on hyvä sopia toimitusketjussa tietoturvan osalta?

- **Roolien ja vastuiden määrittely**
  - **Mitä tarkoittaa:** Varmistetaan, että jokainen mukana oleva taho ymmärtää oman osuutensa turvallisuuden ylläpitämisessä
  - **Käytännössä:** Selkeät viestintä- ja yhteistyölinjat toimitusketjuverkostojensa sisällä

- **Sopimussakot ja vahingonkorvaukset**
  - **Mitä tarkoittaa:** Jos kumppanin toiminnassa on laiminlyöntejä tai toiminta aiheuttaa sinulle vahinkoa, kumppani on velvoitettu sopimussakkoihin tai korvaamaan aiheutuneen vahingon
  - **Käytännössä:** Sovitaan, mitkä ja mihin määrään vahingot korvataan

Hyvän toimittajahallinnan peruspilarit



Kysymyksiä?