Lainsäädännöstä yrityksille tulevat vastuut

Laki (esitys) kyberturvallisuuden riskienhallinnasta… ja muu sääntely…

30.11.2023 Jaakko Wallenius

DIGITALISAATIOLLA
KESTÄVÄ
TULEVAISUUS

Vastuullisuus, vaatimukset ja liiketoiminta

Asiakastarpeet
Asiakkaan tahto

Liiketoiminnan
tarpeet ja riskit
Oma tahto

Sääntely ja
vaatimukset
Yhteiskunnan tahto

Esimerkki toimialalta

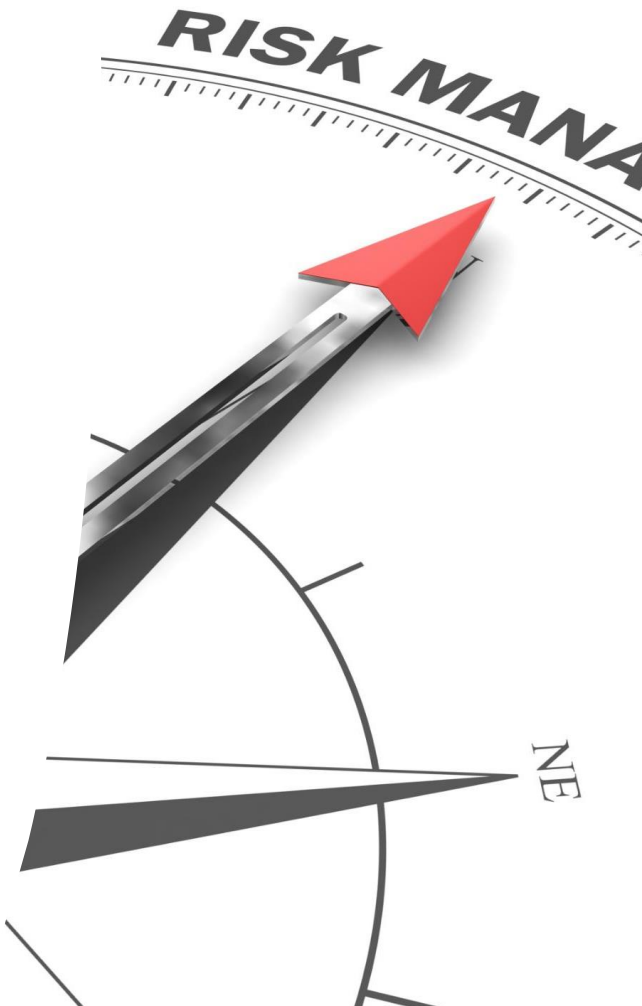
Lainsäädäntö, määräykset ja standardit osaltaan määrittävät teleyritysten turvallisuutta ja varautumista

- Laki sähköisen viestinnän palveluista:
  - 29L Laatuvaatimukset ja turvallisuus, ml. verkon kriittinen osa, verkkoturvallisuuden neuvottelukunta
  - 33L Tietoturvan ja häiriöiden hallinta sekä häiriöistä ilmoittaminen
  - 35L Varautuminen
- *Laki kyberturvallisuuden riskienhallinnasta*
- Valmiuslaki
- EU lainsäädäntö: GDPR, eEvidence, CER, CRA…
- Liikenne- ja viestintäviraston määräykset ja suositukset
- Kansainväliset standardit: 3GPP, GSMA, ETSI, IETF…
- Asiakkaiden kanssa erikseen sovitut järjestelyt
- Yhteistoiminta ja harjoittelu

Tuleva laki kyberturvallisuuden riskienhallinnasta

- Yritysten kannalta:
  - “vanhat ja uudet” toimialat ja kohteet
    - Keskeinen: keskisuuri tai suuri yritys, tai CER-kriittinen
    - Tärkeä: pienempi, erillinen määritelmä
  - Vaatimuksia mm:
    - Riskienhallinta
    - Järjestelmien tietoturvapolitiikat
    - Toimittajahallinta
    - Tietoturvatapahtumien käsittely ja poikkeamailmoitukset
    - Jatkuvuussuunnittelu
    - Kyberhygieniakäytännöt
    - Henkilöstöturvallisuus
    - Tietoturvakoulutukset
  - Valvonta
  - Johdon korostunut rooli ja sanktiointi
  - Yhtenäiset vaatimukset

  - DORA finanssialalla



Uusia toimialoja aiempien jatkoksi

Keskeisiä toimijoita toimialan mukaan ovat

- Energian **(vety- ja latauspisteiden palveluiden tarjoajat)**,
- liikenteen,
- pankkitoiminnan,
- finanssimarkkinoiden infrastruktuurit,
- terveydenhuollon,
- juomaveden,
- **jäteveden**,
- digitaalisen infrastruktuurin,
- **tieto- ja viestintätekniikka (TVT)-palvelun hallinnan,**
- **julkisen hallinnon ja**
- **avaruusteollisuuden organisaatiot.**

Tärkeitä toimijoita toimialan mukaan ovat

- **posti- ja kuriiripalvelut**
- **jätehuolto**
- **kemikaalien tuotanto ja jakelu**
- **elintarviketuotanto, jalostus ja jakelu**
- digitaalisen palvelun tarjoajat
- **valmistuksen organisaatiot**
- **tutkimustoiminta**

Johdon vastuut määritelty

- Johto: hallitus, hallintoneuvosto, toimitusjohtaja, tai rinnastettavassa asemassa oleva, sekä toimitusjohtajan välittömään alaisuuteen kuuluva ylin johto
- Johdon hyväksyttävä kyberturvallisuusriskien hallintatoimenpiteet ja valvottava täytäntöönpanoa.
- Johdon velvollisuus velvollisuus osallistua koulutukseen
- Johto voidaan saattaa henkilökohtaiseen vastuuseen rikkomuksista
  - Kielto toimia johtotehtävissä