Mitä EU:n kyberkestävyyssäädös merkitsee yrityksille?

Erityisasiantuntija Outi Slant
Liikenne- ja viestintäministeriö,
turvallisuusyksikkö

Kyberala murroksessa-seminaari
23.1.2023

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Mikä ihmeen kyberkestävyyssäädös?

- Kyberkestävyyssäädös eli CRA (Cyber Resilience Act) on kyberturvallisuuden vähimmäisvaatimukset asettava tuoteturvallisuusasetus.

- Ehdotuksen tavoitteena on
  - Parantaa markkinoilla olevien tuotteiden tietoturvaa
  - Tehdä tietoturvavaatimukset käyttäjille läpinäkyväksi
  - Asettaa velvoitteet tuotteiden haavoittuvuuksien hallinnalle

- Asetuksen neuvottelut saatiin päätökseen vuoden 2023 lopulla ja tuotteita koskevia vaatimuksia aletaan soveltaa arviolta vuonna 2027.

Mitä tuotteita vaatimukset koskevat?

- Digitaalisen elementin sisältävä **laite tai ohjelmisto**, joka on suoraan tai epäsuorasti liitettävissä toiseen laitteeseen tai verkkoon
  - ➢ Soveltamisala on erittäin laaja
  - ➢ Aikaisempaan nähden erityisesti ohjelmistojen sääntely täydentyy

- Asetusta ei sovelleta lääkinnällisiin laitteisiin, tiettyihin ajoneuvoihin ja lentokoneisiin. Lisäksi sitä ei sovelleta yksinomaan kansallisen turvallisuuden ja maanpuolustuksen käyttöön tarkoitettuihin tuotteisiin sekä yksinomaan salassa pidettävän aineiston käsittelyyn tarkoitettuihin
- Vaatimuksia tulee valmistajille, maahantuojille ja jakelijoille

Tuotteita koskevat vaatimukset

- Tuotteiden turvallisuusvaatimukset toteutetaan riskiperusteisesti
- Vaatimukset kohdistuvat
  - Tuotteiden kyberturvallisuusvaatimuksiin
  - Valmistajan haavoittuvuuksien hallintaan

- Tuotteisiin kohdistuvia vaatimuksia ovat mm.
  - Turvalliset oletusasetukset ja automaattiset turvallisuuspäivitykset
  - Luvattomalta pääsyltä estäminen
  - Datan luottamuksellinen säilyttäminen ja datan minimointi
  - Keskeisten toimintojen turvaaminen

Vaatimustenmukaisuuden arviointi ja osoittaminen

- Riskiperusteisesti vaatimustenmukaisuutta voidaan arvioida ja osoittaa eri tavoin
  - Itsearviointi
  - Standardien soveltaminen
  - EU:n tyyppihyväksyntämenettely
  - Ilmoitetun laitoksen tekemä tarkastus
  - Kyberturvallisuussertifikaatti

- Tuotteisiin kohdistetaan markkinavalvontaa vastaavalla tavoin kuin muidenkin tuoteturvallisuussäädösten perusteella

Mitä tapahtuu seuraavaksi?

- Käynnistetään kansallisia täytäntöönpanotoimia
  - Lainsäädännöllisiä toimenpiteitä täytyy kohdistaa erityisesti viranomaisroolien määrittelemiseen
  - Määritellään muut täytäntöönpanoa vaativat toimet ja luodaan prosesseja
  - Käydään sidosryhmäkeskusteluja eri täytäntöönpanon osa-alueista
- Arviointilaitoksien määrän lisäämiseen on kiinnitettävä erityistä huomiota
- Komissio lähettää standardointipyynnöt standardointijärjestöihin voimaantulon yhteydessä
  - Standardit ovat merkittävässä roolissa vaatimustenmukaisuuden toteuttamisen näkökulmasta
  - Tavoitteena on, että ne olisivat olemassa noin vuotta ennen soveltamisen aloittamista

Kiitos!

lvm.fi

LIIKENNE- JA VIESTINTÄMINISTERIÖ