NIS2-direktiivi

Sidosryhmäjulkinen

Kimmo Iso-Ahola
Tietoturva-asiantuntija
Istekki, Tietoturvakonsultointi

Yleistä

- Tavoitteena vahvistaa ja yhdenmukaistaa EU:n yhteistä kyberturvallisuustasoa
- Kumoaa aiemman verkko- ja tietoturvadirektiivin (NIS1)
- Kansallisen täytäntöönpanon määräpäivä 17.10.2024, kansallinen soveltaminen alkaa 18.10.2024
- Direktiivi ei ota kantaa käytettäviin teknologioihin
- Sisältää velvoitteita ja seuraamuksia velvoitteiden laiminlyönneistä
- Direktiivi määrittää vähimmäistason
- Toimialakohtaiset tai kansalliset säädökset voivat olla direktiiviä tiukemmat
- Kansalliset vaatimukset ovat vielä työn alla

NIS2 toimialat

- Keskeiset toimijat:
  - Organisaatioita, joiden palveluksessa on yli 250 työntekijää, ja joiden vuosiliikevaihto on yli 50 milj. € tai joiden taseen loppusumma on yli 43 milj. €
  - Toimiala jokin seuraavista:
    - Energia
    - Liikenne
    - Pankkitoiminta
    - Finanssimarkkinat
    - Terveys
    - Juomavesi
    - Jätevesi
    - Tieto- ja viestintäteknologian hallinta
    - Julkishallinto
    - Avaruus
    - CER-direktiivin mukaiset keskeiset toimijat
    - Digitaalinen infrastruktuuri (DNS-palveluntarjoajat, luottamuspalvelun tarjoajat, aluetunnusrekisterit, yleisten sähköisten viestintäverkkojen tai –palveluiden tarjoajat jne.)

- Tärkeät toimijat:
  - Organisaatioita, joiden palveluksessa on yli 50 työntekijää, ja joiden vuosiliikevaihto on yli10 milj. € tai joiden taseen loppusumma on yli 10 milj. €
  - Toimiala jokin seuraavista:
    - Energia
    - Liikenne
    - Pankkitoiminta
    - Finanssimarkkinat
    - Terveys
    - Juomavesi
    - Jätevesi
    - Tieto- ja viestintäteknologian hallinta
    - Julkishallinto
    - Avaruus
    - Digitaalinen infrastruktuuri
    - Posti- ja kuriiripalvelut
    - Jätehuolto
    - Kemikaalien valmistus, tuotanto ja jakelu
    - Elintarvikkeiden valmistus, tuotanto ja jakelu
    - Valmistus
    - Digitaalisten palveluiden tarjoajat
    - Tutkimustoiminta

istekki

Hallinnon vastuu korostuu

Kyberturvallisuusriskien hallintatoimenpiteet

- Direktiivi velvoittaa asioiden käsittelyn hallintoelinten tasolla (esim. osakeyhtiöissä hallituksen tulee käsitellä ja hyväksyä toimenpiteet kyberturvallisuusriskien hallintaan)
- Johdon vastuu korostuu

1. Hallintoelinten tulee hyväksyä riskienhallintakäytännöt. Käytännöt tulee katselmoida ja hyväksyä uudelleen säännöllisin väliajoin. Esim. vuosikello tai kun tulee muutoksia käytäntöihin.
2. Hallintoelinten tulee hyväksyä tunnistetut riskit ja hallintatoimenpiteet säännöllisin väliajoin. Tästä tulee myös muodostaa kirjallinen dokumentaatio.
3. Hallintoelinten jäsenten tulee kouluttautua kyberturvallisuusriskien suhteen. Esim. verkkokoulutus, jonka suorittamisesta jää merkintä.

Artikla 21 - Kyberturvallisuusriskien hallintatoimenpiteet

- Riskienhallinta
- Tietojärjestelmien turvallisuus
- Poikkeaminen käsittely
- Jatkuvuudenhallinta
- Toimitusketjujen turvallisuus
- Hankintojen, kehittämisen ja ylläpidon turvallisuus
- Haavoittuvuuksienhallinta
- Kryptografian ja salauksen käyttö
- Henkilöstöturvallisuus
- Pääsynhallinta
- Omaisuudenhallinta
- Suojattujen viestintä- ja hätäviestijärjestelmien käyttö, tarvittaessa

ISTEKKI

Velvoitteet

- Kolmiportainen raportointivelvoite merkittävissä kyberpoikkeamissa
  - Ensi-ilmoitus 24 h kuluessa
  - Jatkoilmoitus 72 h kuluessa
  - (Mahdollinen väliraportti)
  - Loppuraportti 1 kk kuluessa
  - Myöskin valvovan viranomaisen on vastattava 24 h kuluessa ilmoitukseen ja annettava pyydettäessä ohjeita poikkeamatilanteeseen (yhdessä KTK kanssa)
- Riskienhallintavelvoitteet
  - Tavoitteena estää tai minimoida poikkeaminen vaikutus palveluihin
  - Riskianalyysit
  - Jatkuvuudenhallinta
  - Poikkeaminen käsittely ja havainnointi
- Toimijalla on velvollisuus tiedottaa palvelujensa vastaanottajia merkittävästä kyberuhkasta

ISTEKKI

Seuraamukset

- Keskeiset toimijat
  - Ennakkovalvonta
  - Jälkivalvonta
  - Seuraamusmaksut velvoitteiden laiminlyönnistä enintään 10 milj. € tai 2 % vuosittaisesta liikevaihdosta
- Tärkeät toimijat
  - Jälkivalvonta
  - Seuraamusmaksut velvoitteiden laiminlyönnistä enintään 7 milj. € tai 1,4 % vuosittaisesta liikevaihdosta

Miten Istekki voi auttaa NIS2 direktiivin vaatimusten täyttämisessä

- Konsultoinnin palvelut
  - GAP analyysi
  - Roadmap, jossa tarvittavat toimenpiteet GAP analyysin pohjalta
  - Tietoturvallisuuden hallintamalli
    - Asiakkaalle sopivalla laajuudella
    - Mahdollisuus peilata toimenpiteet ISO 27001 standardiin

Kysymyksiä?

Kiitos!