TRAFICOM
Liikenne- ja viestintävirasto

Näkökulmia ohjaukseen ja valvontaan

Olli Lehtilä, yksikönpäällikkö

NIS2-direktiivin mukaisten velvoitteiden ohjaus ja valvonta Kyberturvallisuuskeskuksessa

- Ohjauksen ja valvonnan kannalta keskeistä tunnistaa toimijat, jotka kuuluvat sääntelyn soveltamisalaan.
- Toimijoiden ilmoittautuminen toimijaluetteloon.
  - Toimivaltaiset viranomaiset auttavat ja opastavat tarpeen mukaan.
- Kyberturvallisuutta koskevan riskienhallinnan toimintamallin toteuttaminen.
- Merkittävistä poikkeamista ilmoittaminen uudessa NIS2-poikkemailmoitussovelluksessa.

Kyberturvallisuuskeskuksen valvomat toimialat

- Sektorikohtaiset valvovat viranomaiset valvovat lain, sen nojalla annettujen määräysten sekä NIS2-direktiivin nojalla annettujen säädösten, eli komission täytäntöönpanosäädösten noudattamista kunkin sektorin toimijoiden osalta.
- Kyberturvallisuuskeskus toimii valvovana viranomaisena seuraavilla sektoreilla:
  - Digitaalinen infrastruktuuri;
  - Digitaaliset palvelut;
  - TVT-palvelut;
  - Julkishallinto;
  - Tutkimus
- Kyberturvallisuuskeskus tukee muita valvovia viranomaisia tarpeen mukaan.

Kyberturvallisuuskeskus – Ohjaus ja valvonta

Toimintamme periaatteita ovat yhteistyö, avoimuus, luotettavuus ja tasapuolisuus

Suosimme ennaltaehkäisevää ja laajavaikutteista ohjausta

Panostamme perusluonteisten palvelujen toimivuuden ja tietoturvan ohjaukseen ja valvontaan

Valvonnan riskiperustaisuus - Kyberturvallisuuskeskuksen valvontatehtävät kasvussa

Sääntelyn mahdollistamat ohjaus- ja valvontakeinot

Ohjaus ja valvonta 2025-2026

- Kyberturvallisuuslaki voimaan huhtikuussa 2025.
  - Uuden sääntelyn sisäistäminen ja tarkentaminen niin valvovien viranomaisten kuin soveltamisalaan kuuluvien toimijoiden keskuudessa → Yhteistyön merkitys!
- Toimijaluettelon valmistuminen ja toimijoiden kontaktointi.
  - Yhteistyökeskustelut valvovan viranomaisen ja toimijoiden kesken yhteisen tilannekuvan muodostamiseksi.
- Valvontasuunnitelman sektorikohtainen laatiminen ja tarkentaminen.
  - Kyseessä KTK:n NIS2-valvontaa ja sen eri ohjaus- ja valvontatoimenpiteitä (ml. Tarkastustoiminta) koskeva suunnitelma.
- Valvonta- ja ohjaustoimenpiteet käynnistyneet heti lain voimaantultua.

TRAFICOM
Liikenne- ja viestintävirasto

Kokemukset NIS1-valvonnasta

Aleksi Hirvonen, erityisasiantuntija

Traficomin Kyberturvallisuuskeskuksen NIS1-valvonta

- NIS1-direktiivin (2016/1148) mukaiset valvontatehtävät kattoivat digitaalisen infrastruktuurin toimijat ja digitaalisen palvelun tarjoajat
- Digitaalisen infran kohdalla sovellettiin olemassa olevaa teleyrityssääntelyä
- Digitaalisen palvelun tarjoajien kohdalla NIS1 uutta sääntelyä
  - Päätoimipaikkaperustainen valvontamalli (”one-stop-shop”)
  - Vain jälkivalvonnan piirissä (ex post)

Jälkivalvontamenettely käytännössä

- Poikkeamailmoitus valvottavalta toimijalta tai ilmoitus toimijan asiakkaalta palvelua koskevasta häiriöstä
  - Poikkeama voi tulla ilmi myös median kautta
- Ilmoituksen tutkiminen
  - Jos kyse merkittävästä poikkeamasta, on todennäköisesti tarve arvioida, onko toimija noudattanut lakisääteisiä velvoitteitaan
- Lisäselvityksen pyytäminen tarvittaessa
- Pääsääntönä ollut asian selvittäminen kirjallisessa menettelyssä
- Arvioidaan tarve valvontapäätökselle
  - NIS2 myötä myös seuraamusmaksu mahdollinen

Case: Tunkeilija ylläpitoympäristössä 1/2

- Pilvipalveluntarjoajan verkonhallintaympäristössä havaittu haitallista liikennettä Q1/22
- Havainto haitallisesta liikenteestä tullut emoyhtiön tekemän erillisen tietoturvaskannauksen kautta.
  - Ei havaittu palvelun omissa valvontamekanismeissa
- Valvontamenettelyssä kiinnitetty huomiota yrityskauppojen myötä integroitujen palveluiden ja järjestelmien tietoturvakäytäntöihin
  - Kyseessä palvelu, joka hankittu yrityskaupan myötä
- Traficom antanut asiassa valvontapäätöksen Q3/22

Case: Tunkeilija ylläpitoympäristössä 2/2

- Valvontamenettelyssä kiinnitetty huomiota seuraaviin puutteisiin:
  - Hankittujen järjestelmien ja palveluiden integroimisessa uuteen yritykseen selviä puutteita tietoturvakäytäntöjen tarkastelun ja ylläpidon osalta.
- Yleisesti puutteita havaittu mm.
  - Ylläpitoympäristön palomuurikäytännöt
  - Ympäristön valvonta
  - Lokien hallinta ja -kattavuus
  - Päivityskäytännöt
  - Laitteiden elinkaarihallinta
  - Salasanapolitiikka
- Annettu velvoite korjata havaitut puutteet ja tarkastaa myös muut yrityskauppojen myötä hankitut palvelut

Valvonnassa esiin nousseita kysymyksiä ja havaintoja 1/2:

- Mihin loppuu pilvipalveluntarjoajan vastuu tietoturvakäytänteiden toteuttamisessa?
  - Eri sopimus- ja palvelutyyppien vaikutukset vastuunjakoon pilvipalveluiden kohdalla
    - Onko vastuunjako selvä molemmille osapuolille?
  - Pitäisikö tiettyjen palveluiden kuulua automaattisesti ns. perustasoiseen sopimukseen?
    - Esim. varmuuskopiot, laiteredundanssi...
- Yrityskauppojen tai organisaatiomuutosten aiheuttamat vaikutukset
  - Hankittujen järjestelmien tietoturvakäytänteiden ajantasaisuuden varmistaminen
- Sertifikaatit eivät takaa ”vapaudu vankilasta” –korttia velvoitteiden noudattamisen suhteen
  - Tapauskohtainen tarkastelu voi paljastaa puutteita käytännöissä
  - Inhimillinen tekijä on alati läsnä
  - Tapaus, jossa laitevikaa koskevaa tikettiä ei käsitelty ajoissa -> merkittävä palvelukatko (sertifikaatti ei estänyt virheiden syntymistä)

Valvonnassa esiin nousseita kysymyksiä ja havaintoja 2/2:

- Tuotanto- ja testausympäristöjen eriyttäminen tulisi toteuttaa niin, että niitä hallitaan omina kokonaisuuksinaan
  - Tapaus, jossa testausympäristössä tehty tietojen poisto aiheutti laajan häiriön myös tuotantoympäristössä
- Kuinka paljon työntekijään voi luottaa?
  - Suppeat (ns. nollaluottamus-periaate) vs. laajat ylläpito-oikeudet, kuinka rajata käyttöoikeuksia tarkoituksenmukaisesti ilman, että työnteko hankaloituu merkittävästi?
  - Yhteiskäyttöiset ylläpitotunnukset luovat suuren riskin ja vaikeuttavat jäljitettävyyttä
- Kv. standardien ja alan uusimman tekniikan huomiointi vaatimusten asettamisessa
  - Lakiteksti ja komission asetus jättävät valvovalle viranomaiselle tulkinnanvaraa

TRAFICOM
Liikenne- ja viestintävirasto

Kiitos

Nis.valvonta.ktk(a)traficom.fi