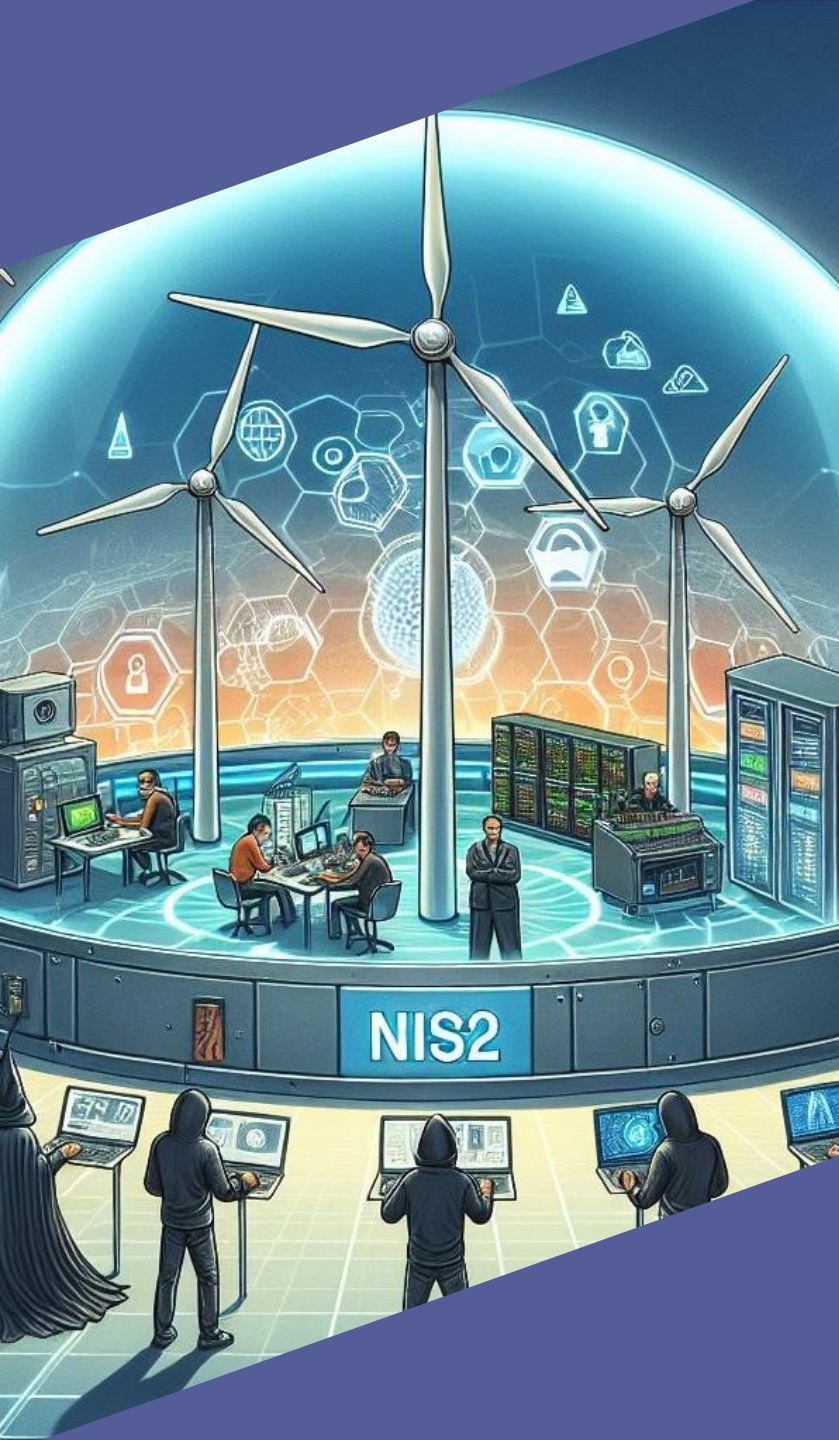


NIS2, konkreettisilla toimilla direktiivi hyötykäyttöön

Marita Harju, Senior Consultant
Security & Modern Work, Netox Oy
marita.harju@netox.fi



Energia-ala ja NIS2

Kriittinen infrastruktuuri on elintärkeässä roolissa yhteiskunnan toimivuuden kannalta.

NIS2 auttaa yrityksiä katsomaan omaa toimintaansa kyberturvallisuuden näkökulmasta ja asettaa vaatimuksia joiden avulla asioita tehdään jatkossa hallitummin ja turvallisemmin.

NIS2 ei ole mörkö tai EU:n pakkopulla. Se vaatii enimmäkseen asioita, jotka kaikilla yrityksillä tulisi olla kunnossa.

Don't Panic, vaan ota NIS2 ilolla vastaan!



Miten NIS2 auttaa puolustautumisessa?



NIS2 direktiivin ja pian hyväksyttävän kansallisen kyberturvallisuuslain tavoitteena on parantaa kyberturvallisuuden tasoa ja nopeuttaa tapahtumiin reagointia EU:n laajuisesti



Yritysten kyberturvallisuuden tasoa parannetaan laittamalla lakisääteisesti kyberperustukset kuntoon ja siten nostetaan yritysten ja kriittisten toimialojen puolustus- ja palautumiskykyä



Kun perustukset ovat NIS2:sen myötä kunnossa ja tiedetään omat vahvuudet, heikkoudet ja uhat, voidaan keskittää resurssit sinne missä niitä oikeasti tarvitaan

Konkreettiset stepit onnistuneeseen NIS2 projektiin:

1. Ymmärrä, miksi NIS2 on tärkeää juuri teille

- Kun tehdään asioita joiden merkitys ymmärretään, lopputulos on parempi ja asiat on helpompi saada myös pysymään kunnossa pitkällä tähtäimellä

2. Tee tilannekuva ja vertaa sitä NIS2 vaatimukseen

- Selvitä mitkä asiat on kunnossa ja mitkä ei, tee itse tai palkkaa apujoukkoja
 - Tiedät miten asioita tehdään nyt, ymmärrät mitä sinulla on, missä se on ja mikä siitä on oikeasti tärkeää
 - Hyödynnä esim. oman toimialasi valvovan viranomaisen (Energiavirasto) tarjoamia materiaaleja, FISC:in NIS2 opasta ja Traficomin materiaaleja

3. Laadi To Do –lista asioista mitkä eivät vastaa NIS2 vaatimuksia, priorisoi listan työt ja ala hommiin

- Osa asioista vie aikaa, osa on nopeita tehdä vaikka samanaikaisesti
- Priorisoi korkealle omaan liiketoimintaan oleellisesti vaikuttavat asiat (esim. mikä riski toteutuessaan estäisi liiketoiminnan)

Asioita mitkä tulee laittaa kuntoon

Riskienhallinta ja vastuiden määrittely

- kaikki riskit, MYÖS kyberriskit haltuun, vastuut määritetty ja säännölliset läpikäynnit
- johdon osallistuminen ja vastuu todennettavissa = dokumentointi (kokousmuistiot jne.)
- hallintatoimenpiteiden tehokkuuden seuranta (kartoitukset, auditoinnit, mittarointi jne.)

Poikkeamien tunnistaminen ja ilmoittaminen

- kyvykkyys tunnistaa poikkeamia ja reagoida niihin (lokiin hallinta, SIEM, SOC tms.)
- kriittisten poikkeamien ilmoittaminen ja raportointi viranomaisille aikarajojen puitteissa

Jatkuvuuden hallinta

- jatkuvuussuunnitelmat, varmuuskopiointi ja palautumissuunnittelu
- kriisinhallinta, vastuut

Toimitusketjun turvallisuus (omat toimittajat), järjestelmien hankinnan ja ylläpidon turvallisuus

- hankittujen/hankittavien järjestelmien säännölliset tietoturvapäivitykset
- toimittajan vakavaraisuus, luotettavuus ja NIS2 vaatimusten täyttyminen

Lisää asioita mitkä tulee laittaa kuntoon

Kyberhygienia

- politiikat, ohjeet, haavoittuvuuksien hallinta, päivitykset
- päätelaitteiden ja palvelinten suojaus
- verkon turvallisuus (segmentointi, verkonvalvonta jne.)
- henkilökunnan pakolliset, säännölliset koulutukset

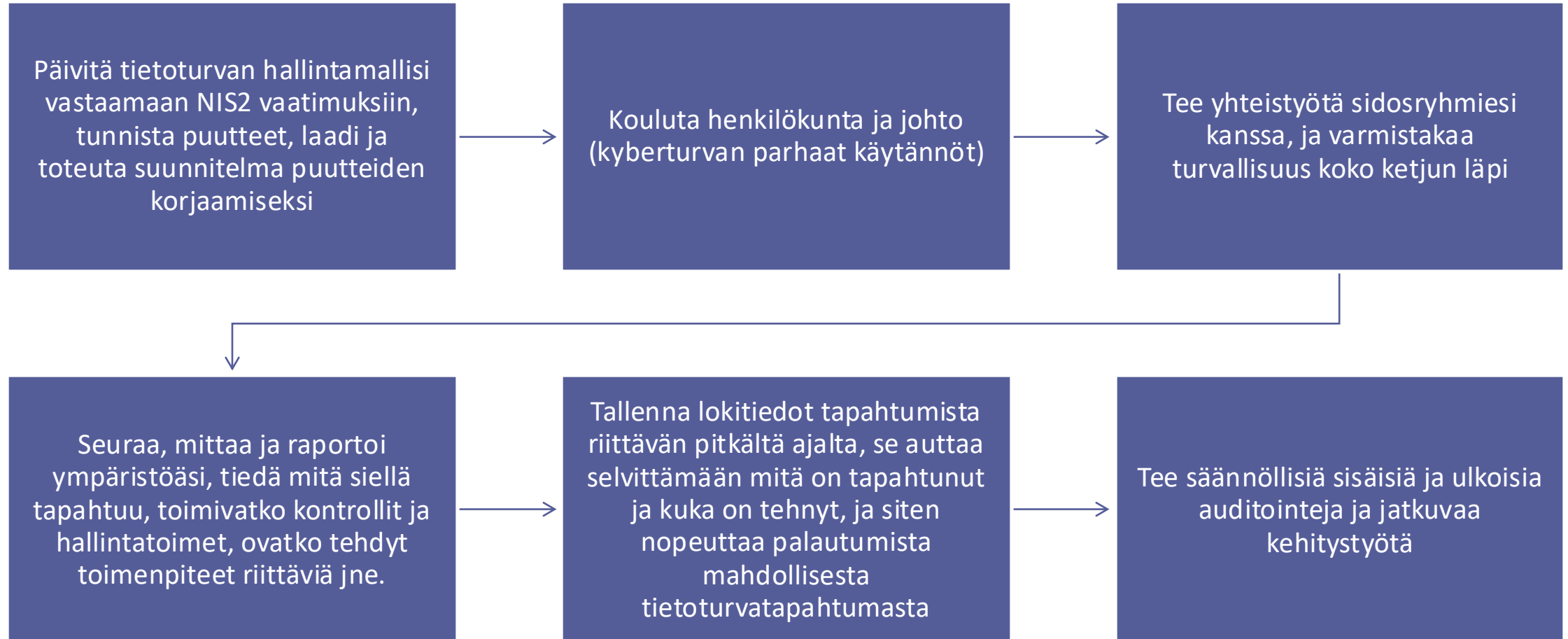
Pääsynhallinta, monivaiheinen tunnistautuminen, omaisuudenhallinta jne.

- omaisuus: tieto-omaisuus, laitteet, puhelimet, ajoneuvot jne.
- Zero-Trust, identiteetinhallinta, pääsynhallinta, turvallisuusselvitykset jne.
- autentikointi (tunnistus) politiikka
- tiedonsiirtopolitiikka
- turvallisen kommunikoinnin politiikka
- kryptografia, salaus tekniikat

Dokumentteja mitä tulisi olla:

- tietoturvapoliitiikka
- tietosuojapolitiikka
- jatkuvuussuunnitelmat
- jatkuvuussuunnitelmien testaukset
- varmistussuunnitelma
- DRP (disaster recovery plan)
- kriisinhallintasuunnitelma
- poikkeamienhallinnan prosessi
- toimittajien arviointi kriteeristö
- tietojärjestelmävaatimukset/tietoturva vaatimukset toimittajille
- henkilöstön koulutussuunnitelma
- pääsynhallinnan dokumentti
- riskienhallinnan ohjeistus
- omaisuudenhallinnan politiikka
- johdon katselmoinnin prosessi

Näillä eväillä pääsee jo pitkälle



A group of diverse professionals in business attire are smiling and working at their desks with multiple computer monitors. A bright, glowing light emanates from the center of the group. Overlaid on the top left of the image is the text 'NIS2' in large, white, sans-serif font, with a digital, circuit-like background effect.

NIS2

Kun ensimmäinen kierros on tehty..

..aloitetaan seuraava. NIS2 on jatkossa osa arkea, se ei ole projekti joka päättyy. Hyvä ja tuloksekas ensimmäinen kierros helpottaa elämää!

Kiitos! Kysymyksiä?

Contact us

Netox Oy

Krouvintie 4, 90400 Oulu

Ilmalanlinna, Ilmalantori 4, 00240 Helsinki