NIS 2-implementering

Morten Rosted Vang, fagleder for cybersikkerhed og digital ansvarlighed

morv@di.dk

NIS 2 – det kommende nye net- og informationssikkerhedsdirektiv

- Status
  - Endelig afstemning, ikrafttræden efter 21 måneder
- Minimumskrav
  - 10 områder nævnes
- Rapporteringspligt
  - 24 timer, 72 timer, 1 måned
- Krav til ledelsen
  - Kompetencer og ansvarlighed (både overordnet og i forhold til proces) plus risiko for forbud mod at varetage ledelsesfunktioner
- Sanktioner/bøder
  - Række af sanktioner, påbud og bøder op til 2% af global omsætning eller 10 mio euro plus pålægge organisationen at offentliggøre manglende overholdelse af deres forpligtelser

Digital

NIS 2 – hvem gælder det for?

- Hvem er omfattet?

  - **Væsentlige enheder**; energi, transport, banker og finansiel infrastruktur, sundhed, drikkevand, spildevand, digital infrastruktur, it-service B2B, offentlig administration og rum-sektoren
  - **Vigtige enheder**; post og kurerservices, affald, kemi, fødevarer, produktion indenfor hospitalsudstyr, computer, optisk og elektronisk udstyr, digitale udbydere, forskning
  - **Leverandører** til vigtige og væsentlige enheder skal overholde kundens krav i NIS2 og være kontraktlig forpligtet til at overholde dem. Leverandører har også rapporteringspligt til kunden.
  - **Undtagelser** ift. størrelse, omsætning, samfundsfunktion etc.

  - Væsentlig eller vigtig har betydning for tilsyn og bødestørrelser og formentlig ekstra sikkerhedskriterier
  - Mapping

NIS 2 – national implementering

- Hvem er omfattet igen igen?
- Minimumskrav kontra sektorspecifikke krav
- Sektoransvarsprincippet eller ej
  - CSIRT, national kompetent myndighed, kontaktpunkt, tilsynsenheder,
  - Gennemskuelighed og forudsigelighed, koordination og kompetencer

Risikovurderingsprincip!

Risikostyring

Risici identificeres, vurderes og styres gennem ledelsestilsyn

Ledelsesbeslutning om risikoaccept, risikoundgåelse eller risikomitigering

Ledelsesgodkendelse af sikkerhedsforanstaltninger, der mitigerer risici til et acceptabelt niveau

Implementering gennem politikker, procedurer, teknologi og dokumentation

Digital

Rapporteringsforpligtelser

Hurtigst muligt og inden 24 timer: ”Early warning”

Hurtigst muligt og inden 72 timer: ”Initial assessment”

Inden 30 dage: Udførlig rapport

Hvad er omfattet:

Væsentlige sikkerhedshændelser der har forårsaget *eller potentielt kan forårsage* væsentlige driftsforstyrrelser, økonomiske tab eller påvirke andre ved at forårsage betydelige materielle eller immaterielle tab

Den endelige udførlige rapport skal indeholde:

- Detaljeret beskrivelse af hændelsen, dens alvorlighed og indvirkning
- Type trussel eller grundlæggende årsag, der sandsynligvis udløste hændelsen
- Anvendte og igangværende afbødende foranstaltninger.
- Og hvor det er relevant tillige hændelsens grænseoverskridende virkning

D I Digital

Minimumskrav til foranstaltninger

- POLITIKKER FOR RISIKOANALYSE OG INFORMATIONSSIKKERHED
- HÅNDTERING AF HÆNDELSER
- DRIFTSKONTINUITET OG KRISESTYRING
- FORSYNINGSKÆDESIKKERHED
- SIKKERHED VED ERHVERVELSE, UDVIKLING OG VEDLIGEHOLDELSE AF NET- OG INFORMATIONSSYSTEMER
- POLITIKKER OG PROCEDURER TIL VURDERING AF EFFEKTIVITETEN AF DE PÅGÆLDENDE FORANSTALTNINGER
- GRUNDLÆGGENDE COMPUTERHYGIEJNE OG UDDANNELSE I CYBERSIKKERHED
- POLITIKKER OG PROCEDURER RELATERET TIL KRYPTOGRAFI OG KRYPTERING
- HR-SIKKERHED, ADGANGSSTYRING OG AKTIVSTYRING
- ANVENDELSE AF MULTIFAKTORAUTENTIFIKATION ELLER ”KONTINUERLIGE AUTENTIFIKATIONSLØSNINGER” MV., ”HVOR RELEVANT”

Digital

Brug af standarder

NIS2 tilskynder til brug af europæiske eller internationalt accepterede sikkerhedsstandarder

CIS Controls

Digital

FORMÅL

D-mærket skal skabe digital tryghed hos kunder og forbrugere og digital ansvarlighed hos virksomhederne …

digital tryghed

1. **… ved at give dansk erhvervsliv et solidt løft for it-sikkerhed og ansvarlig dataanvendelse**
2. **… ved at give forretningsværdi for den enkelte virksomhed**
3. **… ved at skabe tryghed hos virksomhedernes kunder og samarbejdspartnere**
4. **… ved at gøre it-sikkerhed og ansvarlig dataanvendelse til en dansk styrkeposition**

D-mærkets 8 kriterier

1

KRITERIE 1

Styring og forankring i ledelsen

2

KRITERIE 2

Awareness og sikker adfærd

3

KRITERIE 3

Teknisk it-sikkerhed

4

KRITERIE 4

Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse

5

KRITERIE 5

Transparens & kontrol med data

6

KRITERIE 6

Privacy & security by design & default

7

KRITERIE 7

Pålidelige algoritmer & AI

8

KRITERIE 8

Dataetik

Kilde: https://d-maerket.dk/kriterier/

Tre gode råd lige nu - udover at tage D-mærket

1. **Gå allerede i gang nu**, hvis du tror, at din virksomhed er omfattet. God anledning til at få styr på din virksomheds it-sikkerhed.
2. Få et **overblik** over processer, systemer, leverandørkontrakter, (og kunder, der potentielt er omfattet af NIS2) og ikke mindst krisestyring og beredskab.
3. **Involver ledelsen fra start** – ikke bare fordi det er et krav i NIS2, men også fordi at NIS2 går på tværs af jura, it-teknik og forretningen.

Indsatser

VEJLEDNING

KOMMUNIKATION
OG PRESSE

MYNDIGHEDER
OG POLITIKERE

EU