





Agenda

- Hvorfor nu lige NIS2?
- Hvem dækker NIS2?
- Ledelsesansvar
- Hvad siger jeres kollegaer
- Cyber awareness certificering fra GoLearn
- Afrundning og spørgsmål

Flemming Serritzlew



Head of
Customer Success, GoLearn

Kontakt på:



fs@golearn.dk



[linkedin.com/in/flemming-serritzlew](https://www.linkedin.com/in/flemming-serritzlew)

Det startede med NIS 1

“Direktiv om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen”

- **Det første direktiv blev vedtaget i 2016**

- Trådte i kraft omkring samme tid som GDPR i maj 2018
- Men det blev måske lidt glemt
- Stiller krav til (risikobaseret) sikkerhed hos udvalgte sektorer, der leverer kritisk infrastruktur (f.eks. forsyning, transport, tele- og internet, mv.)
- **Formål:** At sikre et højt niveau af cybersikkerhed på tværs af medlemsstaterne
- **I praksis:** Er blevet implementeret og håndhævet (meget!) forskelligt på tværs af EU-lande og en rimelig vag tilgang i Danmark

NIS 2

Primære formål

- Harmonisering!
- Udvidelse af omfattede sektorer (dog undtagelse for små virksomheder)
- Flere og mere konkrete (sikkerheds)krav
- Mere håndhævelse, herunder bøder og ledelsesansvar

Væsentlige enheder



Energi – forsyning, distribution, transmission og salg af energi (el, fjernvarme og -køling, olie, gas og brint)



Digital infrastruktur – internetudvekslingspunkter, DNS-udbydere, TLD-navnregistre, cloudcomputing, datacentertjenester, tillidstjenesteudbydere, mfl.



Transport – sø og luftfart, jernbane og vejtransport



IKT-tjenester (B2B) – udbydere af administrerende tjenester og sikkerhedstjenester



Bank og finansiell markedsinfrastruktur – bankvæsen, finansielle markedsinfrastrukturer, handel og børser



Offentlig forvaltning – statslige og regionale forvaltninger



Sundhed – forskning, produktion, udbydere og fremstillere af medicinsk udstyr



Rummet – infrastruktur til rumtjenester



Drikkevand og spildevand – primærleverandører og -distributører

Vigtige enheder



Post- og kurerservice – postvæsen og kurer-tjenester



Digitale udbydere – online markedspladser, søgemaskiner og SoMe



Affaldshåndtering



Forskning - forskningsorganisationer



Kemiske produkter – fremstilling, produktion og distribution



Fødevarer – produktion, forarbejdning og distribution



Fremstilling og produktion – medicinsk udstyr, computere, elektronik, optisk udstyr, elektrisk udstyr, maskineri, køretøjer, transportudstyr, mv.



1 RISIKOVURDERINGER: ALL HAZARD APPROACH

Alle farer inkl. fysiske

2 LEVERANDØRSTYRING

Forsyningskæde-
sikkerhed samt sikkerhed
ved erhvervelse og
udvikling IT-systemer.

3 TEKNISKE LØSNINGER

Brug af f.eks. multifaktor
autentifikation, kryptografi
og kryptering. Hertil
medfølgende politikker.

4 UDDANNELSE AF PERSONALE

Personalesikkerhed,
grundlæggende
cyberhygiejne, politikker
og uddannelse

5 HÅNDTERING AF HÆNDELSER

Omfatter både
hændeshåndtering og
f.eks. Driftskontinuitet efter
hændelser.

6 POLITIKKER, STRATEGIER & EVALUERING

Risikoanalyse,
informationssikkerhed,
samt effektiviteten af
foranstaltninger

1

RISIKOVURDERINGER: ALL HAZARD APPROACH

Alle farer inkl. fysiske



2

LEVERANDØRSTYRING

sikkerhe

v

udvil

Hvad NIS2 kræver af den direkte omfattede virksomhed

Den NIS2-omfattede virksomhed skal sikre:

- Personalesikkerhed
- **Grundlæggende cyberhygiejne**
- **Dokumenteret Awareness-træning**
- Relevante politikker og procedurer
- Ledelsesansvar for cybersikkerhed

Det gælder deres egne medarbejdere – men de skal også håndtere **risici i forsyningskæden**.

3

TEKNIS

Brug af

autentifik

og

medfo

UDDANNELSE AF PERSONALE

Personalesikkerhed,
grundlæggende
cyberhygiejne, politikker
og uddannelse

4

HÅNDTERING AF HÆNDELSER

mfatter både
ændelseshåndtering og
eks. Driftskontinuitet efter
ændelser.

5

POLITIKKER, STRATEGIER EVALUERING

isikoanalyse,
formationssikkerhed,
amt effektiviteten af
ranstaltninger

6

1

RISIKOVURDERINGER: ALL HAZARD APPROACH

Alle farer inkl. fysiske



2

LEVERANDØRSTYRING

sikkerhe

v

udvil

Hvad NIS2 kræver af den direkte omfattede virksomhed

Den NIS2-omfattede virksomhed

- Personalesikkerhed
- **Grundlæggende cybersikkerhed**
- **Dokumenteret Awareness**
- Relevante politikker og procedurer
- Ledelsesansvar for cybersikkerhed

Det gælder deres egne medarbejdere og leverandører
håndtere **risici i forsyningskæden**

3

TEKNISKE

Brug af

autentifik

og

medfø



4 UDDANNELSE AF PERSONALE

Personalesikkerhed,
grundlæggende
cyberhygiejne, politikker
og uddannelse

4

5 HÅNDTERING AF HÆNDELSER

mfatter både

5

Praktisk anbefaling som leverandør

Hvis du leverer til NIS2-omfattede virksomheder, bør du som minimum have:

- **En årlig dokumenteret awareness-træning**
- En informationssikkerhedspolitik
- Rollebaseret træning for tekniske medarbejdere
- En simpel incident-procedure
- Dokumentation klar til kundeaudit

Det behøver ikke være tung ISO-certificering – men det skal være struktureret og dokumenterbart.

Ledelsesforankring og -ansvar

Ledelsen skal:

- Godkende foranstaltninger til styring af Cyber sikkerhed
- Føre tilsyn med implementering i alle enheder
- Gennemføre kurser med henblik på at have tilstrækkelig viden og kompetencer til at styre Cybersikkerheds risici
- Sørge for at der er tilbudt kurser til alle ansatte*
- Tag ansvar for at NIS2-loven overholdes

Kort sagt:

Cybersikkerhed er ikke kun et IT-anliggende – det er et ledelsesansvar. NIS2 forpligter ledelsen til aktivt at sikre de rette kompetencer i organisationen.

*Ifølge § 7, stk. 2 i NIS 2-loven skal ledelsen aktivt tilskynde til, at medarbejdere tilbydes relevante kurser. Ledelsen skal også selv gennemføre relevant uddannelse.



Hvad siger vores kunder

Undersøgelse fra 18. februar

- **ca. 2 ud af 3** arbejder i dag **ikke** struktureret og dokumenterbar med awareness-træning.
- **Over halvdelen** peger på *manglende tid, ressourcer eller kompetencer* som den største barriere for at arbejde mere systematisk med IT-sikkerhed.
- **Mange organisationer er enten direkte eller indirekte omfattet af NIS2** – men en betydelig del er stadig i tvivl om deres konkrete rolle og ansvar.
- Mange organisationer er stadig i en **tidlig modenhedsfase**.
- Fokus på IT-sikkerhed drives især af **lovkrav, bestyrelse og reelle hændelser** – ikke af overskud eller god tid.

A man with a grey beard and glasses is looking down. He is wearing a blue and white checkered shirt over a grey t-shirt. The background is dark with blue light streaks. A large white 'NIS2' text is overlaid on his face. In the top right corner, there is a graphic consisting of a teal arc and an orange swirl.

NIS2



HVAD INDEHOLDER CERTIFICERINGEN?



Reducér menneskelige fejl og dokumentér I lever op til NIS2 awareness træningskravet

NIS2-certificeringen er et introducerende awareness-forløb, der klæder medarbejdere på til at forstå deres rolle i organisationens cybersikkerhed.

Det er ikke et teknisk kursus – Det er et dømmekraftskursus

NIS2

HVORDAN SER DET UD?

Skabt i samarbejde med Dansk IT

En quiz inspireret rejse mod IT-sikkerhed

- En underholdende læringsrejse
- Korte videoer der Fanger modtagerens opmærksomhed
- Baseret på NIS2 kravene til træning
- Øvelser baseret på tvivlssituationer og digitale henvendelser
- Refleksionsopgaver
- Ekspertindslag, der gør stoffet levende og troværdigt

Vært **Mette Walsted**

Tidligere nyhedsvært på DR P1 morgen og TVAVISEN



Kursets opbygning

1. Hvad er NIS2 – og hvorfor er det relevant for dig?
2. NIS2's grundprincipper
3. Hvad betyder cybersikkerhed i din hverdag på jobbet?
4. Genkend risici og trusler
5. Hændelser: Når noget går galt – hvad gør du?
6. NIS2-tjekliste & dit certifikat

Dvs. dækker NIS2 direktivets krav
(Artikel 20(2) – om Awareness og træning)

Ekspert: Steen Smidt

Senior IT-
og cybersikkerhedsspecialist hos Infinigate



Målgruppen er “alle”

Men særligt relevant for:

- Administrative funktioner
- Projektledere
- Nye medarbejdere
- Ikke-tekniske teams

Launch webinar

 17. marts | kl. 10 | Online

Du kan forvente eksperter som bl.a.

- Steen Smidt, Senior IT- og cybersikkerhedsspecialist hos Infinigate
- Mette Kaagaard, Adm. Direktør hos Microsoft
- Mette Walsted, Journalist og vært

