FOCUS ADVOKATER

Webinar om NIS2

Jesper Løffler Nielsen, den 18. februar 2026

Dagsorden

- **Landskabet for regulering af cybersikkerhed**
- **Introduktion til NIS2**

(Pause)

- **NIS2's krav til awareness og uddannelse**

Om oplægsholderen

Jesper Løffler Nielsen

Associeret partner, advokat, ph.d. v. Focus Advokater P/S

Profil

- Certificeret IT-advokat og associeret partner hos Focus Advokater P/S
- Leder af Tech Teamet – specialister i digital regulering

Forskning og undervisning

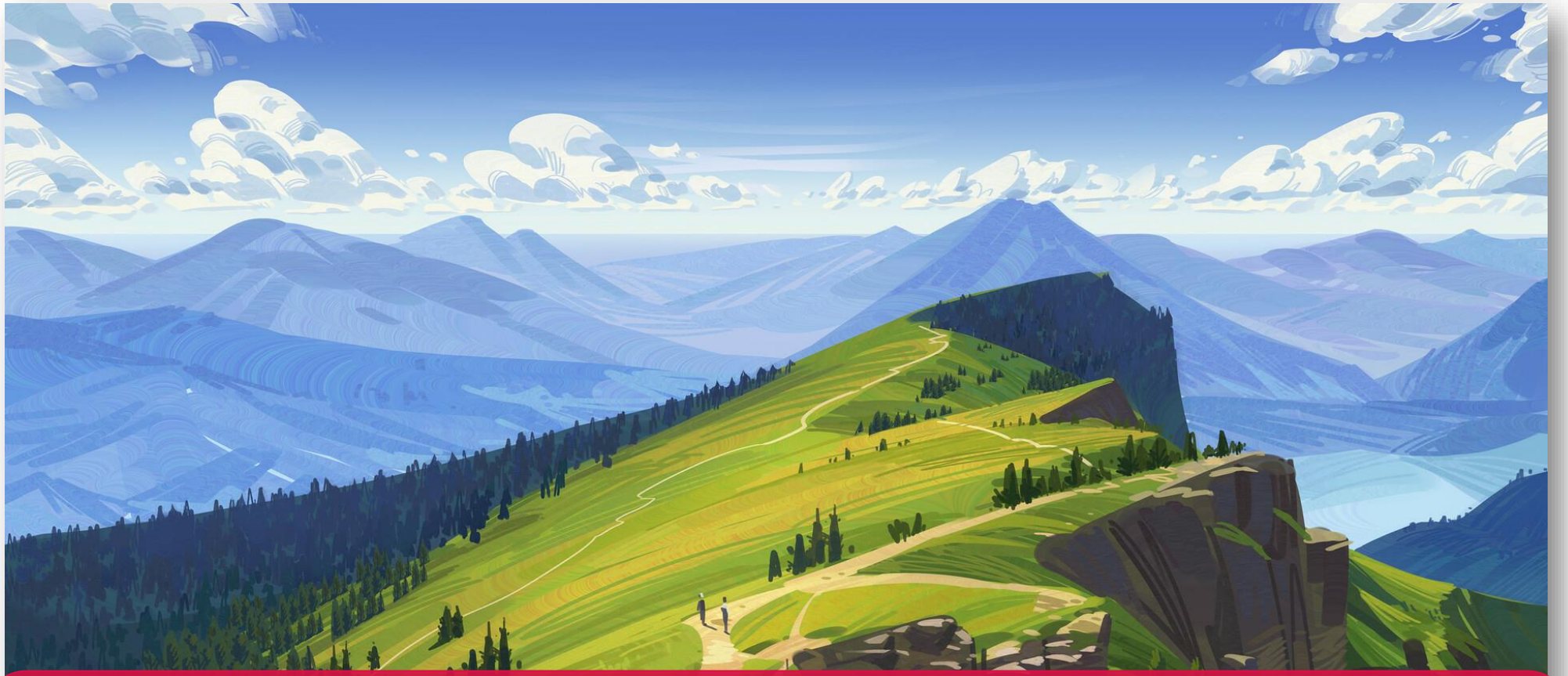
- Erhvervs-PhD i IT-ret (2013 – 2016)
- Ekstern lektor i IT-ret, Persondataret mv. (2010 -)
- Underviser på IT Vest's Master IT-fagpakke: *"Cybersikkerhed, Privacy og Regulering"*

Andet

- Bestyrelsesmedlem i Danske IT-Advokater
- Netværksleder for Technology Denmarks netværk: *"Innovation & Compliance"*
- Udpeget til EDPB "Pool of Experts" ift. digitale teknologier
- Medlem af Dansk Standards AI-udvalg

Kontakt: E-mail: jln@focus-advokater.dk LinkedIn

FOCUS ADVOKATER

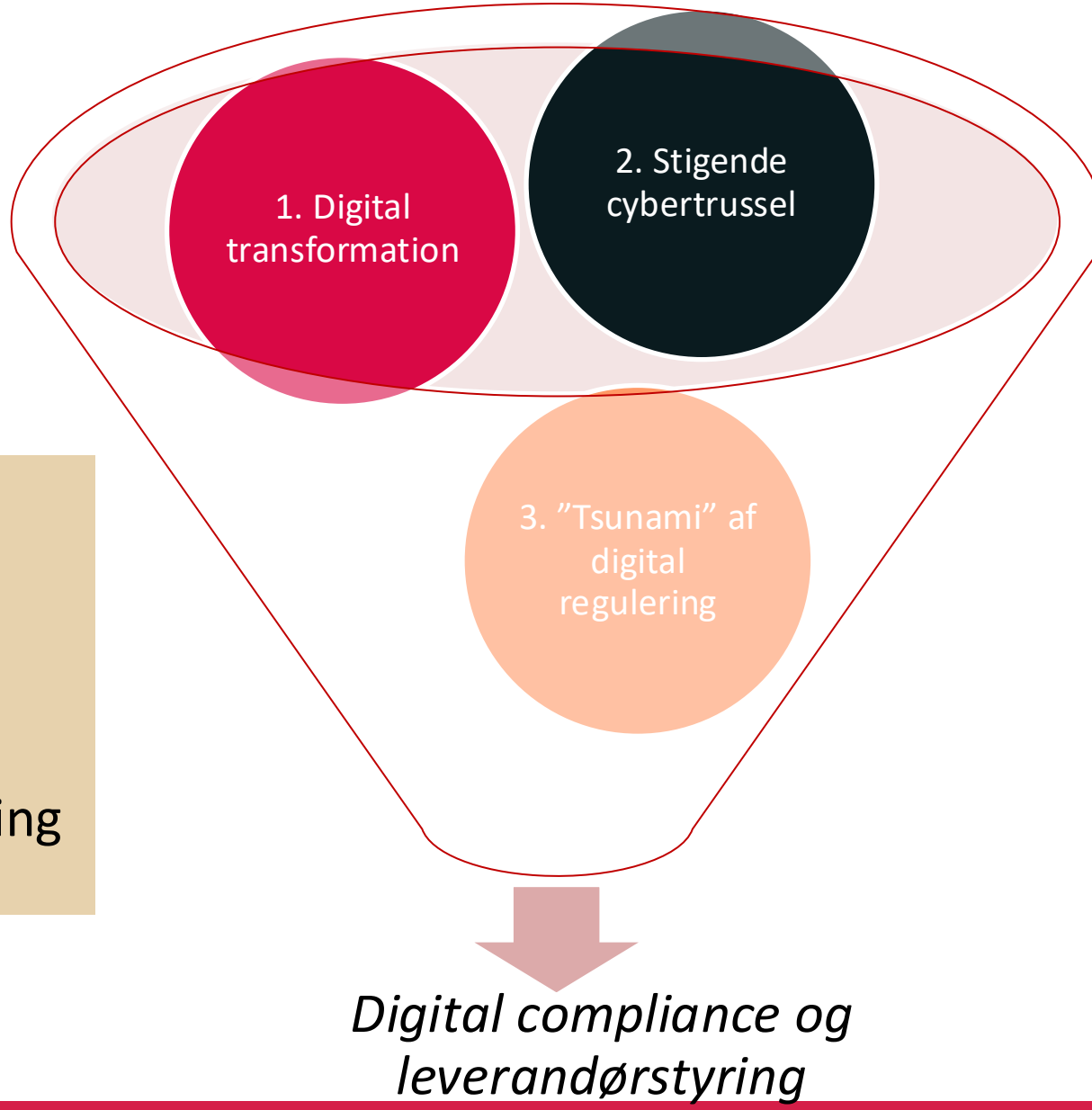


Landskabet for regulering af cybersikkerhed

FOCUS ADVOKATER

Stigende krav til digital compliance og leverandørstyring

1. Trend nr. 1: Digital transformation
2. Trend nr. 2: Stigende cybertrussel
3. Trend nr. 3: En ”tsunami” af digital regulering



Cybersikkerhed bliver i stigende krav et juridisk anliggende

Generelle krav

- Databeskyttelsesreglerne,
  inkl. en række sikkerhedsrelaterede krav

Sektor- og produktspecifikke krav

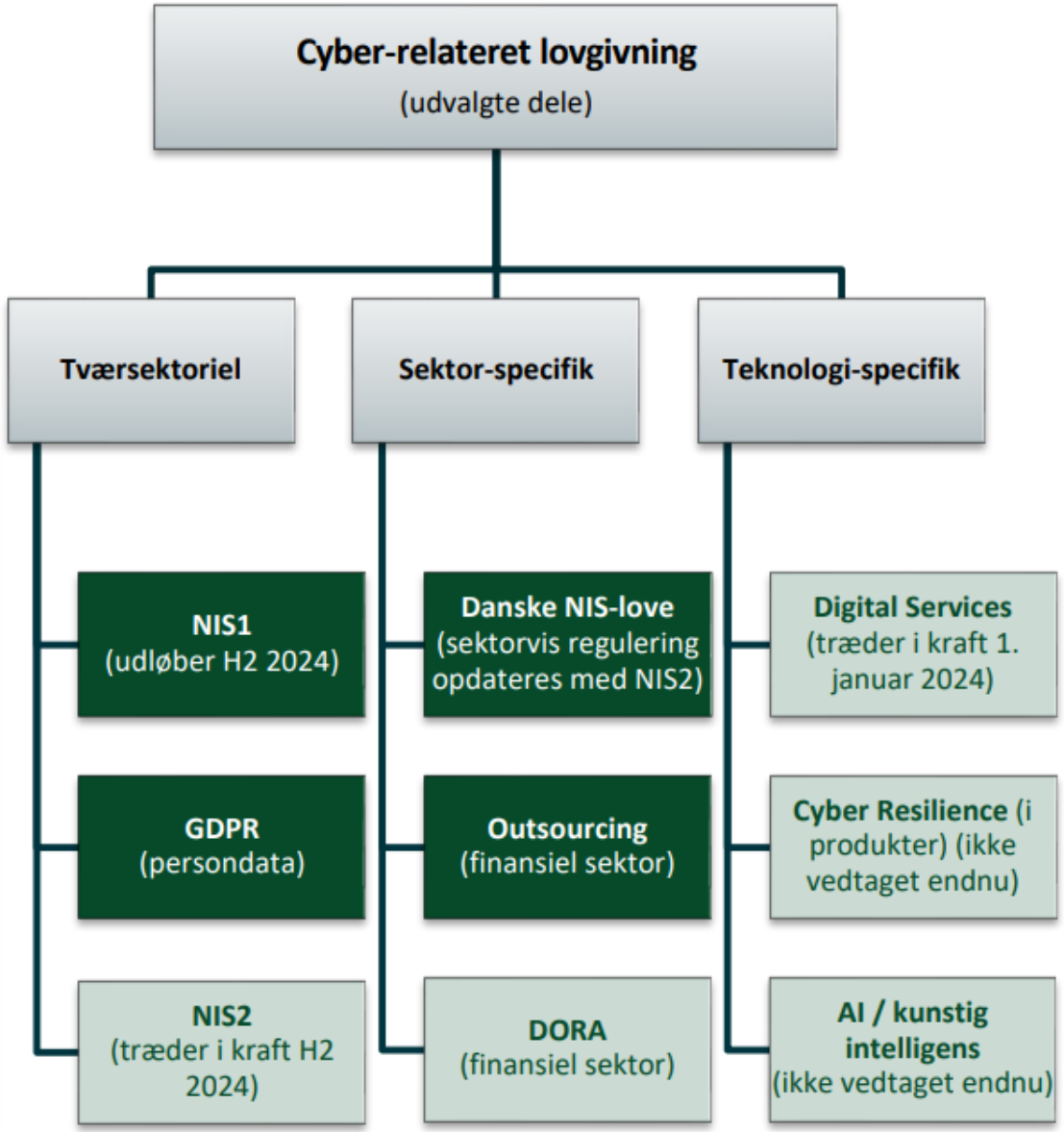
- Krav om/anbefaling ift. offentlige myndigheders efterlevelse af informationssikkerhedsstandarden ISO 2700X
- En række særregler for visse sektorer (NIS 2, DORA, mv.)
- Stigende lovkrav til cybersikkerhed i produkter og software (GPSR, CRA mv)

Indirekte "krav" ift. sikkerhed

- IT-sikkerhed er (i stigende grad) et ledelsesanliggende, også juridisk set
  - F.eks. selskabslovens §115, nr. 2: *"sikre en forsvarlig organisation… etableret de fornødne procedurer for risikostyring og interne kontroller"*
- Kun beskyttelse af forretningshemmeligheder, hvis tilstrækkelig sikkerhed
  - Lov om forretningshemmeligheder § 2, nr. 1, litra c

FOCUS ADVOKATER

Regulering



FOCUS ADVOKATER

Hvad er NIS 2?

FOCUS ADVOKATER

Om NIS 1

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

- **Det første direktiv ("NIS 1") blev vedtaget i 2016**
  - Trådte i kraft omkring samme tid som GDPR i maj 2018
  - 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

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

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 hændelseshåndtering og f.eks. Driftskontinuitet efter hændelser.

6 POLITIKKER, STRATEGIER & EVALUERING

Risikoanalyse, informationssikkerhed, samt effektiviteten af foranstaltninger

FOCUS ADVOKATER

Væsentlige enheder

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

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

Transport – sø og luftfart, jernbane og vejtransport

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

Bank og finansiel 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 kurertjenester

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.

FOCUS ADVOKATER

NIS 2-regulering i Danmark

NIS 2-direktivet

Direktiv 2022/2055 (link)

EU-Kommissionens gennemførelsesforordninger, retningslinjer og øvrige retsakter

Gennemførelsesforordning (EU) 2024/2690 (link) og retningslinjer for anvendelsen af artikel 4, stk. 1 og 2 (link)

(**NB**: flere retsakter er på vej, jf. "Cybersecurity Package" fra 20.1.2026)

Hovedlov	Sektorspecifikke love		
NIS 2-loven (link)	**Lov nr. 258 om styrket beredskab i energisektoren** (link)	**Lov nr. 435 om sikkerhed og beredskab i telesektoren** (link)	**Lov nr. 481 om ændring af lov om finansiel virksomhed, mv.** (link)
Bekendtgørelse nr. 620 (link) **Bekendtgørelse nr. 653 (link)**	**Bekendtgørelse nr. 260** (link) **Bekendtgørelse nr. 840** (link) **Bekendtgørelse nr. 1075** (link) **Bekendtgørelse nr. 1809** (link)	**Bekendtgørelse nr. 621** (link) **Bekendtgørelse nr. 622** (link) **Bekendtgørelse nr. 963** (link) **Bekendtgørelse nr. 1069** (link)	**Bekendtgørelse nr. 1323** (link)

Generelle vejledninger fra SAMSIK (link), sektoransvarlige myndigheder, og ENISA (link) (link)

FOCUS ADVOKATER

Vejledninger fra SAMSIK

Maj 2025

Vejledning om anvendelsesområdet

Denne vejledning skal hjælpe offentlige og private enheder til at vurdere, om deer omfattet af NIS 2-loven.

Maj 2025

Vejledning om ledelsens rolle og opgaver

Denne vejledning skal hjælpe ledelser private og offentlige enheder med at opfylde kravene i NIS 2-loven.

Juni 2025

Vejledning om foranstaltninger

Denne vejledning skal hjælpe offentlige og private enheder med implementering af NIS 2-lovens cybersikkerhedsforanstaltninger.

Juni 2025

Vejledning om hændelsesunderretning

Denne vejledning skal hjælpe offentlige og private enheder til at efterleve deres forpligtelse til at underrette om væsentlige hændelser.

GoLearn spørgeskema

FOCUS ADVOKATER

NIS2's krav til awareness og uddannelse

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 hændelseshåndtering og f.eks. Driftskontinuitet efter hændelser.

6 POLITIKKER, STRATEGIER & EVALUERING

Risikoanalyse, informationssikkerhed, samt effektiviteten af foranstaltninger

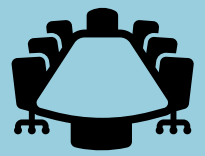
FOCUS ADVOKATER

Risikobaseret tilgang

Fra SAMSIK's vejledning om foranstaltninger (side 10):

"NIS 2-loven understreger, at enhederne skal anlægge en risikobaseret tilgang til sikkerhedsarbejdet, da de ikke alle er risikoeksponeret i samme grad. Det vil sige, at enheden skal implementere de foranstaltninger (tekniske, operationelle og organisatoriske), der vurderes nødvendige for at opnå et passende niveau af sikkerhed i forhold til levering af den eller de ydelser, som gør, at enheden er omfattet af NIS 2-loven. Enhedens foranstaltninger skal dog som minimum omfatte de foranstaltninger, der er beskrevet i NIS 2-loven. Derudover skal enheden, hvor det er relevant, implementere foranstaltninger, der reducerer risikoen for hændelser eller minimerer deres skadevirkning på eventuelle modtagere af deres tjenester og på eventuelle andre tjenester."

Fordeling af ansvaret

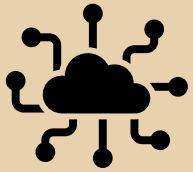


Ledelsen

- Overordnet strategi
- Kulturen-fra-toppen
- Godkend politikker om sikkerhed

HR

- Sikre on- og offboarding
- Procedure for træning og opfølgning
- Dokumenta-tion for uddannelse



IT

- Overblik over systemer og foranstalt-ninger
- Ajourføre IT-politikker

IT-sikkerhed

- Risiko-vurderinger
- Bidrage til awareness om sikkerhed
- Ajourføre sikkerhed-politikker

FOCUS ADVOKATER

Ledelsesforankring og -ansvar

Artikel 20

Styring [*Governance*, eng.]

1. *…**ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici**, som disse enheder har truffet med henblik på at overholde artikel 21, **fører tilsyn med** dens gennemførelse og **kan gøres ansvarlige** for enhedernes overtrædelser af forpligtelserne i nævnte artikel.*

2. *… medlemmerne af væsentlige og vigtige enheders **ledelsesorganer** er **forpligtet til at følge kurser**, og skal **tilskynde** væsentlige og vigtige enheder til **løbende at tilbyde tilsvarende kurser til deres ansatte**, således at de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, der leveres af enheden.*

Bestemmelser om uddannelse og cyberhygiejnepraksisser

NIS 2-direktivet	NIS 2-loven	Lov om styrket beredskab i energisektoren	Bekendtgørelse om modstands-dygtighed og beredskab i energisektoren	Lov om finansiel virksomhed	Lov om sikkerhed og beredskab i telesektoren
Artikel 21, stk. 2, litra g) og i)	§ 6, stk. 1, nr. 7 og 9	§ 6, stk. 2, nr. 9 og 10	§§ 24, 25 og 26	§§ 333 a, stk. 3, nr. 7 og 333 b, stk. 7	§ 5, stk. 1, nr. 7 og 9

"grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse"

"Øvelsesplanlægning, herunder afholdelse af øvelser og træning af beredskabsforanstaltninger"

"Beredskabstræning, cybersikkerhedsadfærds- og sikkerhedsuddannelse af ansatte i virksomheden"

"Medlemmer af en virksomheds ledelsesorgan skal deltage i relevante kurser eller undervisning om organisatoriske beredskab, fysiske sikring og cybersikkerhed"

FOCUS ADVOKATER

Ledelsesforankring og -ansvar

LEDELSEN SKAL:

- Godkende foranstaltninger til styring af cybersikkerhedsrisici
- Føre tilsyn med implementeringen af foranstaltninger i enheden
- Gennemføre kurser med henblik på at have tilstrækkelig viden og kompetencer til styre enhedens cybersikkerhedsrisici
- Tilskynde til, at enheden tilbyder kurser til sine ansatte
- Tage ansvar for enhedens overholdelse af NIS 2-loven

HVILKEN ROLLE SPILLER LEDELSEN IFT. UDDANNELSE AF MEDARBEJDERE?

Ledelsen spiller en vigtig rolle for medarbejdernes kompetencer og adfærd. Ifølge § 7, stk. 2 i NIS 2-loven skal ledelsesorganet tilskynde til, at ansatte tilbydes kurser, svarende til dem, ledelsen selv gennemfører. Bestemmelsen skal ses i sammenhæng med § 6, stk. 1, nr. 7 i NIS 2-loven, som stiller krav om, at enheden skal have en politik for uddannelse af relevante medarbejdere. Politikken efter § 6. stk. 1, nr. 7 skal sikre, at medarbejderne har viden og færdigheder om cyber- og informationssikkerhed, som er passende i forhold til deres rolle og ansvar. Kravet om, at ledelsen skal tilskynde til, at ansatte tilbydes kurser, skal således ikke anses som et krav, der går videre end lovens § 6, stk. 1, nr. 7, men blot en understegning af, at medarbejdernes kompetencer og viden inden for cybersikkerhed er ledelsens ansvar.

For mere information om krav til uddannelse af medarbejdere, se vejledning om implementering af cybersikkerhedsforanstaltninger.

EKSEMPLER

1. I bestyrelsen (ledelsesorganet) for et privat selskab har to af medlemmerne viden om strategisk ledelse af cyber- og informationssikkerhed. Et af medlemmerne har gennemført en bestyrelsesuddannelse med fokus på styring af cybersikkerhedsrisici. Det andet bestyrelsesmedlem har en certificering i en relevant sikkerhedsstandard.

2. I en offentlig myndighed afholdes der en gang årligt et halvdages seminar for medlemmerne af myndighedens cyber- og informations-sikkerhedsudvalg, som inkluderer repræsentanter fra direktionen (ledelsesorganet). Myndigheden har selv tilrettelagt seminaret, som har fokus på trusselsbilledet, risikostyring og strategisk ledelse af cyber- og informationssikkerhed i offentlige myndigheder.

FOCUS ADVOKATER

Uddannelse og cyberhygiejnepraksisser

Politik for uddannelse af medarbejdere

- Net- og informationssikkerhedstræning
- Håndtere relevante sikkerhedsrisici

- Kan f.eks. indeholde:
  - Konkretisering af, hvilke roller der kræver specifikke sikkerhedsrelevante færdigheder
  - Etablering af egentlig uddannelses- og træningsprogram
  - Instruktioner i og træning af gængse cyberhygiejnepraksisser, såsom adgangsstyring, håndtering af opdatering af f.eks. mobile enheder, brug af passwords, mv.
  - Løbende orientering om kendte trusler, f.eks. om forskellige angrebsmetoder eller menneskelige sårbarheder, og tilpas orienteringen til medarbejdernes roller
  - Uddannelse og træning i, hvad medarbejdere skal gøre, når der indtræffer hændelser

- *"Relevante kurser kan for eksempel være generelle kurser om cyber- og informations-sikkerhed, workshops om styring af cyber- og informationssikkerhedsrisici, kurser og certificeringer i anerkendte europæiske og internationale sikkerhedsstandarder eller enhedens egne internt tilrettelagte kurser og seminarer om cyber- og informationssikkerhed"*, jf. side 45

- Cybersikkerhedsuddannelse bør ske regelmæssigt, både for nye medarbejdere og for dem, der overgår til nye stillinger eller roller med væsentligt anderledes krav til net- og informationssikkerhed

FOCUS ADVOKATER

Teknisk og juridisk viden

- **Teknisk viden**
  - Fx om konkrete løsninger, usecases, integration til øvrige IT-systemer, bagvedliggende modeller, datagrundlag, cybersikkerhed, potentielle bias mv.
- **Juridisk viden**
  - Fx om AI Act, GDPR, NIS2, sektorregulering, relevante standarder, officielle vejledninger, kontraktmæssige krav mv
- **Brobygning!**

Spørgsmål fra deltagerne