FOCUS
ADVOKATER

Webinar om NIS 2

Jesper Løffler Nielsen, den 13. marts 2026

Dagsorden

- **Introduktion til NIS 2**
  - NIS 2's rolle i det samlede landskab for lovkrav til cybersikkerhed
  - Overblik over national og EU-regulering, herunder sektorregulering
  - Hvornår er man direkte og indirekte omfattet?
  - Sanktioner

- **NIS 2's krav og organisatorisk forankring**
  - Overblik over kravene i NIS 2
  - Krav til dokumentation
  - Ansvarsfordeling i en organisation
  - Uddybning af krav til ledelsen
  - Uddybning af krav til uddannelse og cyberhygiejnepraksisser, og behovet for hhv. teknisk og juridisk viden

Dagens hovedbudskab

Kilde: ChatGPT

FOCUS ADVOKATER

Hvad er NIS 2?

FOCUS ADVOKATER

Cybersikkerhed bliver i stigende krav et juridisk anliggende

Generelle krav

- Databeskyttelsesreglerne,
  inkl. en række sikkerhedsrelaterede krav

Sektor- og produktspecifikke krav

- Krav om/anbefaling i forhold til offentlige myndigheders efterlevelse af informationssikkerhedsstandarden ISO 27001
- 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

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 ledelsen i 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.

NIS 2-regulering i Danmark

NIS 2-direktivet

Direktiv 2022/2055 (link)

EU-Kommissionens gennemførelsesforordninger, retningslinjer og øvrige retsakter

Gennemførelsesforordning (EU) 2024/26[illegible]0 (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

Sektorspecifikke regler og vejledninger

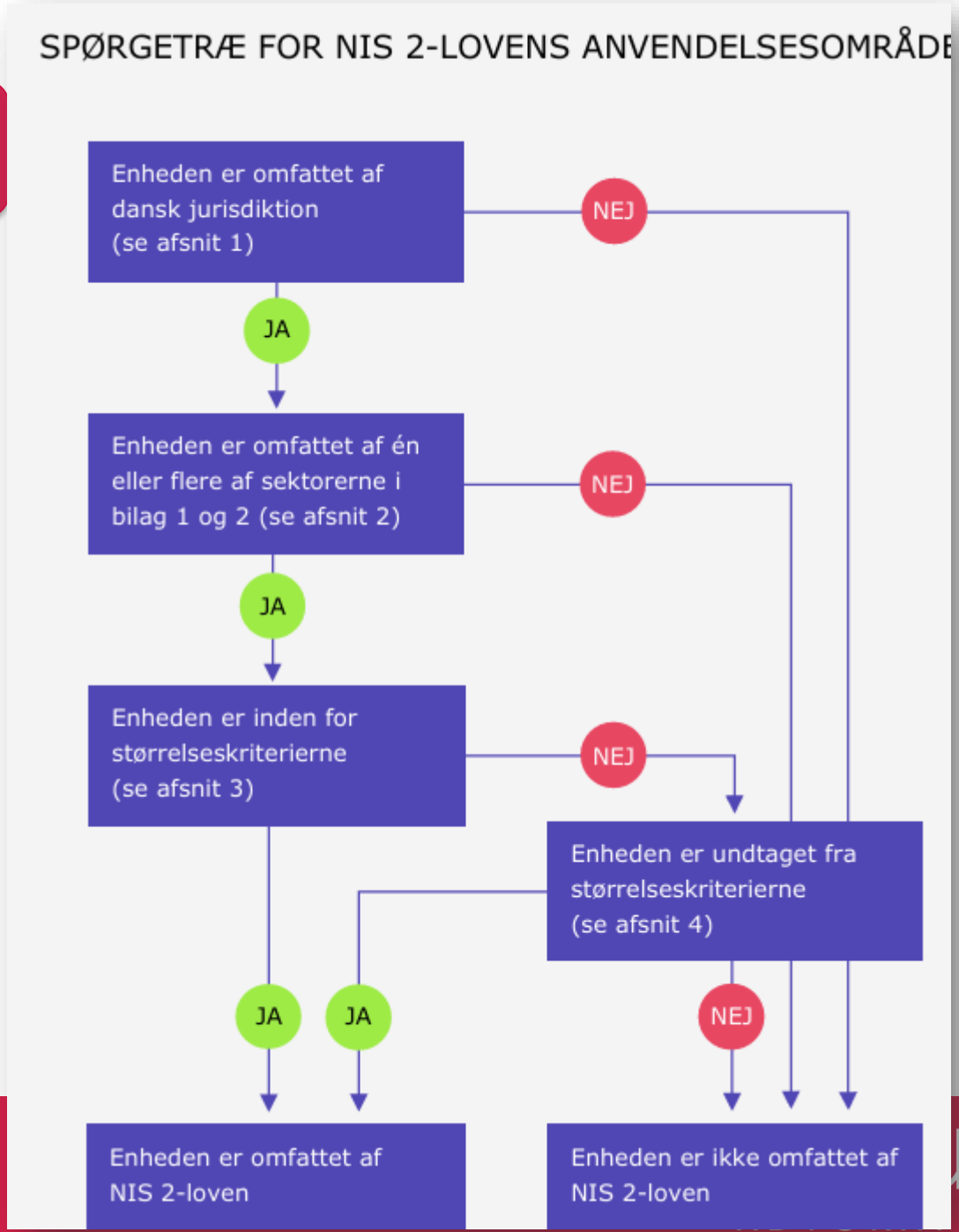
- Danmark følger det såkaldte ”**sektoransvarsprincip**”
- **Energi, tele og finans** er underlagt egne love og bekendtgørelser
- Den **digitale sektor** er underlagt en særskilt gennemførelsesforordning fra EU-Kommissionen, samt uddybende vejledning fra ENISA
- Fælles for alle sektorer er, at de skal fortolkes **direktivkonformt**, dvs. minimumskravene i direktivet altid skal opfyldes

Vejledning om anvendelsesområdet

Maj 2025

Vejledning om anvendelsesområdet

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



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

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

Undtagne enheder og sektorer

Mikrovirksomheder og små virksomheder

- Mikrovirksomheder
  - Beskæftiger under 10 personer, og
  - årlig omsætning eller samlet årlig balance på ikke over EUR 2 mio.
- Små virksomheder
  - Beskæftiger under 50 personer, og
  - årlig omsætning eller samlet årlig balance på ikke over EUR 10 mio.
- **NB**: Undtagelser til undtagelserne

Specifikke enheder

- Medlemsstaterne kan undtage specifikke enheder fra kravene i artikel 21 eller 23 for så vidt angår enhedernes tjenester
- Navnlig inden for:
  - National sikkerhed
  - Offentlig sikkerhed
  - Forsvar, eller
  - Retshåndhævelse

Case-eksempler

Dansk SaaS-leverandør

- **Dansk jurisdiktion**: Ja
- **Omfattet af sektorer i bilag 1 og 2**: Ja (dog usikkerhed ift. definition på "*Cloud Computing Service*")
- **Indenfor størrelseskriterier:** Ja (ca. 70 ansatte, DKK 100 millioner i årlig omsætning og DKK 100 millioner i samlet årlig balance)
- → Omfattet af den danske NIS 2-lov, dog suppleret af EU-Kommissionens gennemførelsesforordning for digital sektor og ENISA's uddybende vejledning

International koncern, der producerer IoT-udstyr

- **Dansk jurisdiktion**: Ja, men også selskaber i andre EU-lande
- **Omfattet af sektorer i bilag 1 og 2**: Ja, da de producerer "*elektronisk udstyr*" omfattet af en af hovedgrupperne i NACE rev. 2
- **Indenfor størrelseskriterier:** Ja (+200 ansatte, DKK 1,5 milliarder i årlig omsætning og DKK 250 millioner i samlet årlig balance)
- → Omfattet af den danske NIS 2-lov, suppleret af SAMSIK's vejledninger

FOCUS ADVOKATER

Direkte eller indirekte omfattet?

Direkte og indirekte krav til NIS 2		
Emne / artikel	**Direkte omfattet**	**Indirekte omfattet**
Formelle krav		
Scope	Ja	Nej
Registreringspligt	Ja	Nej
Konkrete krav til cybersikkerhed		
Ledelsesforankring og lovmæssigt ansvar for ledelse	Ja	Nej (dog kan der være kontraktuelle krav, f.eks. i forhold til efterlevelse af ISO 27001)
Uddannelse af ledelse og medarbejdere	Ja	Nej
Implementering af cybersikkerhedsforanstaltninger	Ja	Ja (som følge af kundens krav til leverandørstyring)
Leverandørstyring / indkøb af nye systemer	Ja	Ja (som følge af kundens krav til leverandørstyring)
Hændelsesrapportering	Ja	Ja (til omfattede NIS 2-kunder)
Sanktioner og erstatning		
Tilsyn fra sektoransvarlige myndigheder	Ja	Nej
Sanktioner (bøde, påbud og forbud)	Ja	Nej
Erstatning	Ja (dog ikke reguleret i lovgivningen)	Ja (over for NIS 2-omfattede kunder på grund af kontraktbrud)

Sanktioner

Bøder

- Bøderammen for **væsentlige enheder** er EUR 10.000.000 eller 2% af samlede globale omsætning
- Bøderammen for **vigtige enheder** er EUR 7.000.000 eller 1,4% af samlede globale omsætning
- Visse offentlige myndigheder kan ikke blive pålagt bøder

Sanktioner for ledelsesorganet

- Midlertidigt forbud mod at udøve ledelsesfunktioner i organisationen
  - **NB**: kun for væsentlige enheder
  - "*Midlertidigt*" = indtil organisationen retter op på forholdet, der har medført nedlæggelse af forbuddet

GoLearn spørgeskema

FOCUS ADVOKATER

NIS 2’s krav og organisatorisk forankring

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

Vejledninger fra SAMSIK

Maj 2025

Vejledning om ledelsens rolle og opgaver

Denne vejledning skal hjælpe ledelsen i 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.

Krav om dokumentation

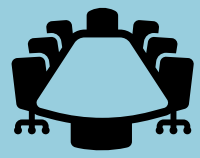
Fra SAMSIK's vejledning om foranstaltninger (side 5):

DOKUMENTATION

Dokumentation er nedskrevne politikker og procedurer, som alle relevante medarbejdere i enhederne har adgang til. Det kan eksempelvis være i form af papirdokumenter, sider på enhedernes intranet eller i en vidensdatabase. Enhederne kan benytte sig af den metode og form, de i forvejen anvender til at opbevare og formidle deres procedurer og lignende. I forbindelse med tilsyn kan dokumentation også antage andre former, som eksempelvis netværksovervågnings-logs, udskrift af adgangstilladelse, referater m.v. Dokumentationen skal under alle omstændigheder kunne gøres tilgængelig for tilsynet, der har behov for adgang til data, dokumenter og oplysninger, som er nødvendige for udførelsen af tilsynsopgaven.

FOCUS ADVOKATER

Fordeling af ansvaret af ansvaret i en organisation (eksempel!)



Ledelsen

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

Jura/compliance

- Fortolke relevante lovkrav
- Formidle viden til kolleger
- Politikker, procedure, kontrakter, mv.

IT

- Overblik over systemer og foranstaltninger
- Ajourføre IT-politikker

IT-sikkerhed

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

HR

- Sikre on- og offboarding
- Procedure for træning og opfølgning
- Dokumentation for uddannelse

FOCUS ADVOKATER

Ledelsesforankring og -ansvar

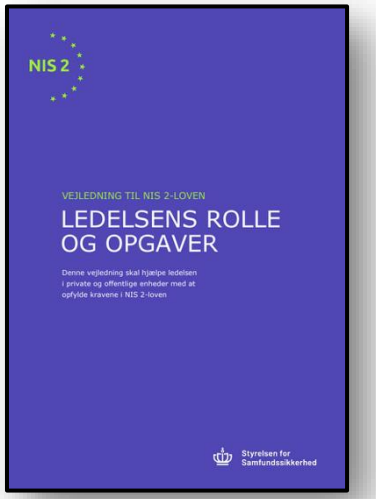
LEDELSEN SKAL:

- 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

Ledelsesforankring og -ansvar

- KL har lanceret to kapitler i deres en drejebog for NIS 2
- Det ene kapitel omhandler ledelsesansvar, hvor de bl.a. har mappet kravstyperne for ledelsen i den danske NIS 2 lov, NIS 2-direktivet og i vejledningen fra SAMSIK

Juridisk grundlag
Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-loven), vedtaget 29. april 2025, trådte i kraft 1. juli 2025. Gælder for kommunerne, der er identificeret som væsentlige enheder jf. § 2 og § 3 i loven.
Direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau (NIS2-direktivet) 2022/2555

Centrale paragraffer i NIS2-loven vedr. ledelsen

§	Krav	Kravstype	Indhold
§ 6, stk. 1, nr. 7	Enheden skal træffe foranstaltninger for uddannelse af relevante medarbejdere.	Skal	Ledelsen skal sikre, at der er cybersikkerhedsuddannelse til relevante medarbejdere.
§ 7, stk. 1	Ledelsesorganet skal godkende foranstaltninger til håndtering af cybersikkerhedsrisici.	Skal	Direktionen har ansvar for godkendelse af sikkerhedsforanstaltninger.
§ 7, stk. 2	Ledelsesorganet skal deltage i relevante kurser om cybersikkerhed og risikostyring.	Skal	Krav om kompetenceopbygning i direktionen.
§ 7, stk. 2	Ledelsesorganet skal tilskynde til uddannelse af medarbejdere.	Bør	Direktionen opfordres til at fremme awareness og træning.

Centrale ledelseskrav i NIS2-direktivet

Artikel	Krav	Kravstype	Indhold
Artikel 20, stk. 1	Ledelsesorganet i enheden skal godkende foranstaltninger til håndtering af cybersikkerhedsrisici og overvåge deres gennemførelse.	Skal	Strategisk og operationelt ansvar placeres direkte hos ledelsen.
Artikel 20, stk. 2	Medlemmer af ledelsesorganet skal have tilstrækkelig viden og kompetence til at vurdere cybersikkerhedsrisici og konsekvenser.	Skal	Krav om kompetenceopbygning og organisatorisk kapacitet i ledelsen.

Vejledningsbaserede krav (SAMSIK)

Kilde	Krav	Kravstype	Indhold
SAMSIK's Vejledning om ledelsens rolle og opgaver	Ledelsen bør etablere faste beslutningsfora for cybersikkerhed.	Bør	Governance-struktur med faste møder og rapportering.
SAMSIK's Vejledning om ledelsens rolle og opgaver	(Kommunen) skal have en politik for uddannelse af relevante medarbejdere	Skal	Politikken skal sikre, at medarbejderne har viden og færdigheder om cyber- og informationssikkerhed, som er passende ift. deres rolle og ansvar.
SAMSIK's Vejledning til Implementering af Cybersikkerhedsforanstaltninger	Ledelsen bør sikre, at leverandørstyring inkluderer NIS2-krav.	Bør	Leverandørkontrakter og kontrolmekanismer.

FOCUS ADVOKATER

Uddannelse og cyberhygiejnepraksisser

Politik for udarbejdelse 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**
  - F.eks. om konkrete løsninger, usecases, integration til øvrige IT-systemer, bagvedliggende modeller, datagrundlag, cybersikkerhed, potentielle bias, mv.
- **Juridisk viden**
  - F.eks. om AI Act, GDPR, NIS 2, sektorregulering, relevante standarder, officielle vejledninger, kontraktmæssige krav, mv.
- **Brobygning!**

Spørgsmål fra deltagerne

FOCUS ADVOKATER

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)
- Deltidslektor (20%) på SDU
- Underviser på IT Vest's Master IT-fagpakke: *"Cybersikkerhed, Privacy og Regulering"*

Andet

- Bestyrelsesmedlem i Danske IT-Advokater
- Medlem af Danske Advokaters fagudvalg for Teknologi
- Udpeget til EDPB "Pool of Experts" ift. digitale teknologier

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

FOCUS ADVOKATER