Hjælp til implementering af NIS 2-kravene med vejledninger og ISO/IEC 27001

Webinar 13. juni 2025

Dagens program

13:00 **Velkommen**

13:05 **Præsentation af de nye NIS 2-vejledninger – særligt med fokus på vejledningen om foranstaltninger**
Morten Rosted Vang, Styrelsen for Samfundssikkerhed

13:35 **Værdien af at lægge sig op ad ISO/IEC 27001 ift. NIS 2-implementeringen**
Søren Koefoed-Hansen, Dansk Standard

14:05 **Spørgsmål og afrunding**

14:30 **Tak for i dag**

Om Fonden Dansk Standard

Hvem er Dansk Standard

- Danmarks officielle standardiseringsorganisation
- Erhvervsdrivende fond med et almennyttigt formål, som skal bidrage til et stærkt erhvervsliv og et trygt samfund
- Grundlagt i 1926
- Ca. 200 medarbejdere
- Erhvervspolitisk partnerskab med Erhvervsministeriet

Vi er medlem af:

En stærk platform af solide brands:

Dansk Standards udvalg for cyber- og informationssikkerhed er med til at skrive fremtidens standarder

DANSK STANDARD

Udvalget består af 50+ medlemmer fra store danske virksomheder, smv'er, konsulenthuse, offentlige myndigheder, NGO'er, brancheorganisationer mm.

- Adgang til unik viden
- Et bredt, fagligt fællesskab
- En stemme, der bliver hørt - beslutter den danske holdning
- Åbent for alle interesserede
- Bidrager til at definere fremtidens markedskrav

Aktuelle temaer

- Fokus på udviklingen og implementeringen af relevant lovgivning på cyberområdet samt udviklingen af eventuelle standarder; fx Cyber Resilience Act, Cyber Security Act, Radioudstyrsdirektivet og NIS 2.
- Eventuelle revisioner af ISO/IEC 27000 serien

Læs mere om udvalget på ds.dk/s-441

Styrelsen for Samfundssikkerhed

NIS 2

MORTEN ROSTED VANG, STYRELSEN FOR SAMFUNDSSIKKERHED

Dansk Standard, 13. juni 2025

ORGANISERING AF MINISTERIET FOR SAMFUNDSSIKKERHED OG BEREDSKAB

DEPARTEMENTET

Departementschef:
Lisbet Zilmer-Johns

STYRELSEN FOR SAMFUNDSSIKKERHED

Direktør:
Laila Reenberg

BEREDSKABSSTYRELSEN

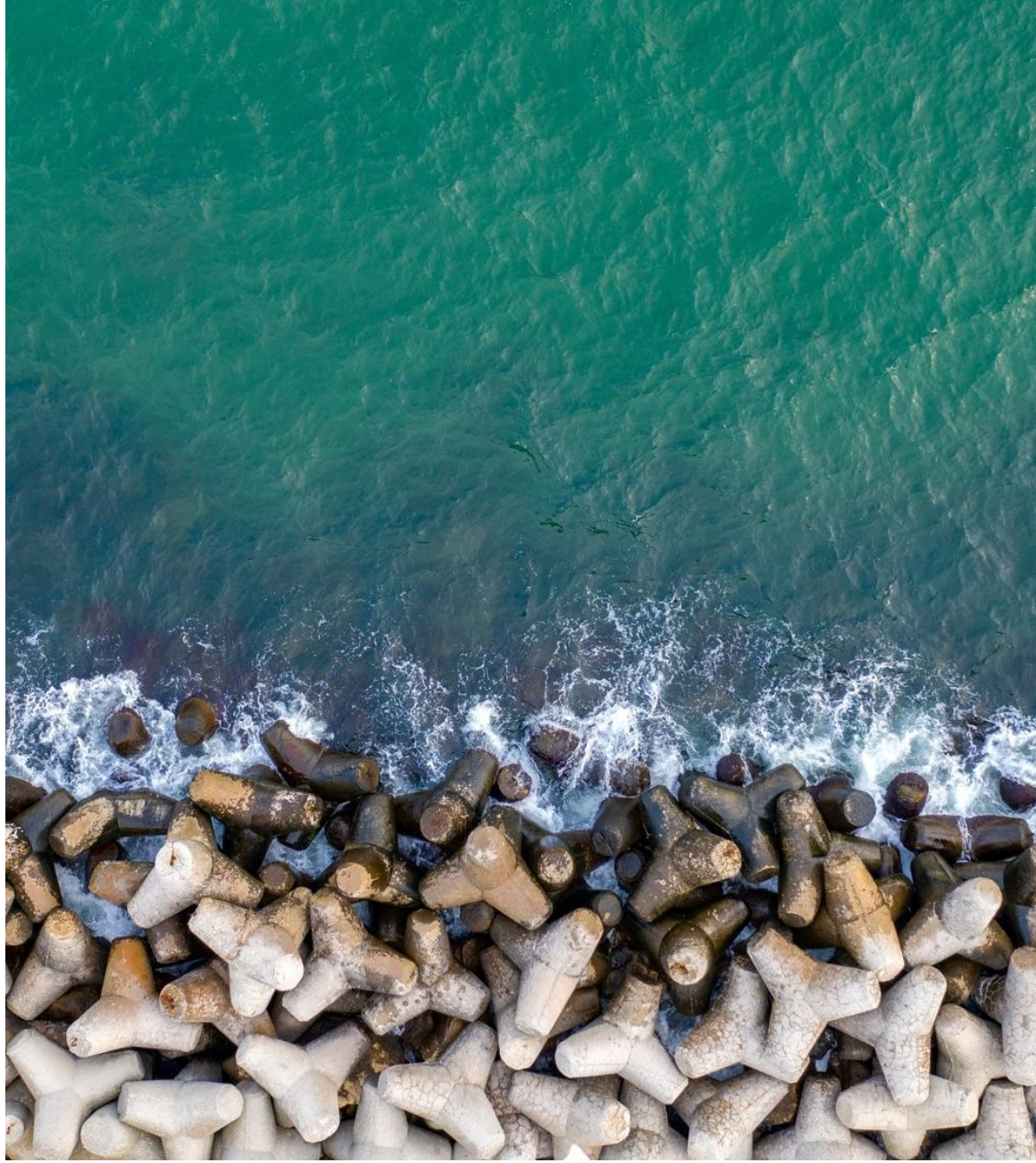
Fg. direktør:
Christine Engel Christensen

HVAD ER SAMSIK'S OPGAVE?

- Styrelsen for Samfundssikkerhed arbejder for at gøre Danmark mere **robust og sikkert** over for de trusler og risici, som samfundet står overfor.
- Vi er sat i verden for at styrke samfundets evne til at **forebygge, modstå og håndtere kriser**.
- Vi arbejder på tværs af sektorer og i tæt samarbejde med myndigheder og erhvervsliv.
- Under kriser skaber vi rammerne, der gør det muligt for myndigheder at løse deres opgaver effektivt.

FORMÅL MED NIS 2

- NIS 2 skal udbedre udfordringerne fra NIS 1 bl.a. inkonsistent implementering på tværs af medlemslandene
- Målet er at øge cybersikkerheden og modstandsdygtigen generelt for kritisk infrastruktur på tværs af sektorer i EU



HVILKE SEKTORER ER OMFATTET AF NIS 2?

SÆRLIGT KRITISKE SEKTORER

ENERGI	
TRANSPORT	
BANKVIRKSOMHED	
FINANSIELLE MARKEDSINFRASTRUKTUR	
SUNDHED	
DRIKKEVAND	
SPILDEVAND	●
DIGITAL INFRASTRUKTUR	
FORVALTNING AF IKT-TJENESTER	●
OFFENTLIG FORVALTNING	●
RUMMET	●

KRITISKE SEKTORER

POST- OG KURERTJENESTER	●
AFFALDSHÅNDTERING	●
FREMSTILLING, PRODUKTION OG DISTRIBUTION AF KEMIKALIER	●
PRODUKTION, TILVIRKNING OG DISTRIBUTION AF FØDEVARER	●
FREMSTILLING	●
DIGITALE UDBYDERE	
FORSKNING	●

● Nye sektorer i NIS 2

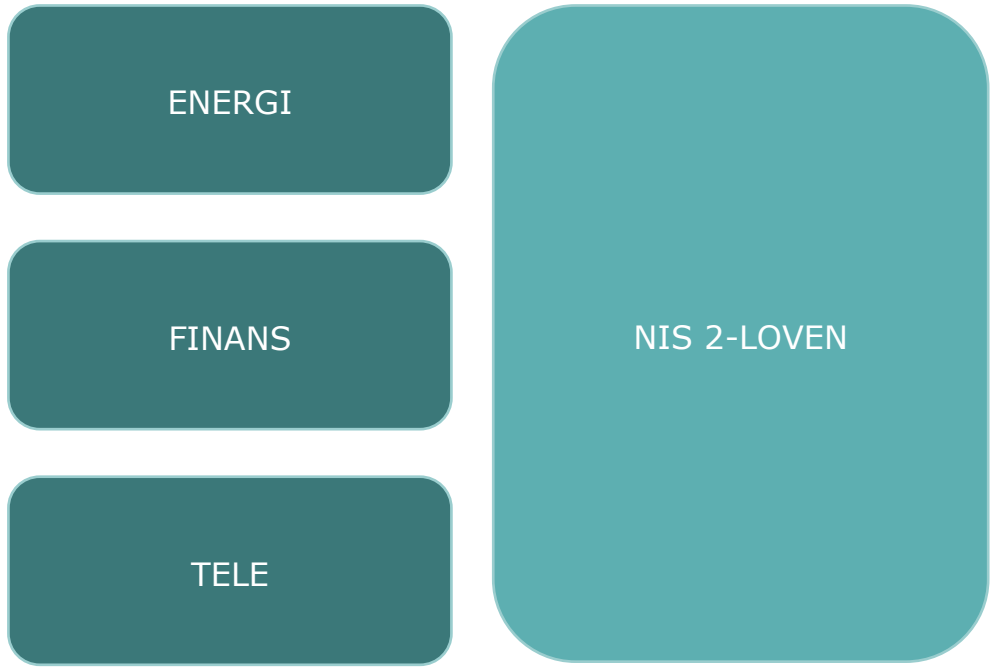
HVEM ER OMFATTET AF NIS 2?

Tre kriterier afgør, om en virksomhed er omfattet af NIS 2-loven:

- Virksomheden hører til en af de omfattede sektorer
- Virksomhedens størrelse kategoriseres som mellemstor eller stor
- Virksomheden er omfattet uanset størrelse eller særlig vigtig fra et samfundsperspektiv.

IMPLEMENTERING AF NIS 2 I DK

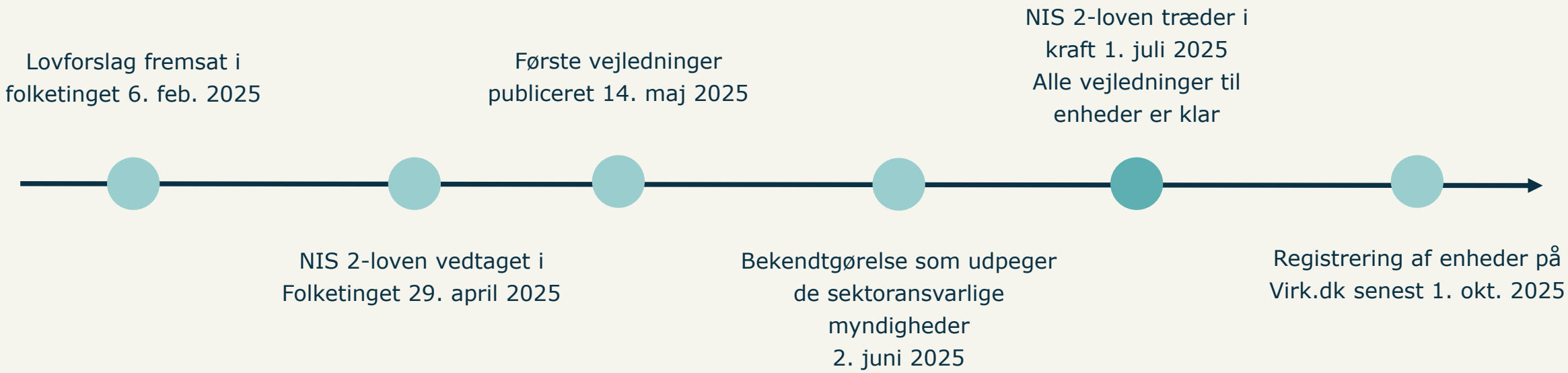
- Implementering bygger på sektoransvar
- Særlovgivning for tele-, energi- og finanssektoren
- Hovedlov for øvrige sektorer (NIS 2-loven)
- Bekendtgørelse til NIS 2-loven som udpeger de sektoransvarlige myndigheder
- Mulighed for, at de sektoransvarlige myndigheder i særlige tilfælde kan udarbejde en sektorbekendtgørelse



MSSB/SAMSIK'S ROLLER

- Koordinerende myndighed for implementeringen af NIS 2 i DK
- Centralt kontaktpunkt i forhold til EU og repræsenterer DK i NIS Samarbejdsgruppen
- Ansvar for NIS 2-loven og særlovgivningen på teleområdet
- Sektoransvarlig myndighed for tele, statslige myndigheder, kommuner, skibstrafiktjenester, fremstilling og kemi
- National CSIRT (på sigt)

TIDSLINJE NIS 2-LOVEN



SAMARBEJDE OG INTERESSENTINDDRAGELSE

- Bred interessentinddragelse i arbejdet med at udarbejde tværgående vejledninger til NIS 2-loven
- NIS 2-interessentgruppe bestående af erhvervs- og brancheorganisationer bl.a. Dansk Industri, Dansk Erhverv, KL og Danske Regioner
- NIS 2-følgegruppe i regi af Cybersikkerhedsrådet
- NIS 2-koordinationsgruppe – forum for samarbejde mellem relevante myndigheder

VEJLEDNINGSINDSATS

TVÆRGÅENDE VEJLEDNINGER
Udarbejdes af SAMSIK.
Centrale krav og begreber i NIS2-loven.

Virksomheder og myndigheder (enheder)

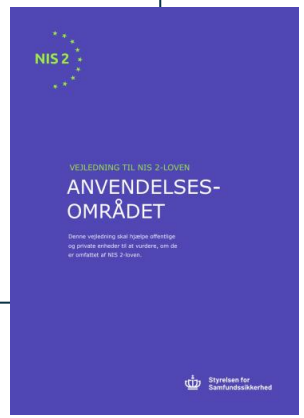
Ledelsesorganer

- ANVENDELSES-OMRÅDET
- IMPLEMENTERING AF CYBERSIKKERHEDS-FORANSTALTNINGER
- HÆNDELSES-UNDERRETNING
- LEDELSENS ROLLE OG OPGAVER

SEKTORVEJLEDNINGER
Udarbejdes af de sektoransvarlige myndigheder
Afgræsning af sektorer, sektornære forhold og eksempler, tilsynspraksis m.m.

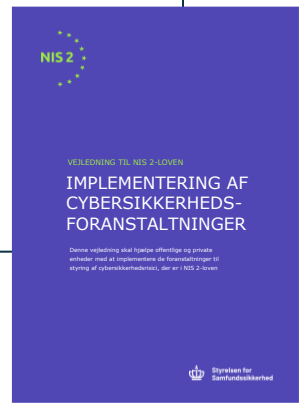
TVÆRGÅENDE NIS 2-VEJLEDNINGER 1/2

- Skal understøtte enheder i at vurdere, om de er omfattet af NIS 2-loven eller ej
- NIS 2-lovens definition af en ”enhed” samt forskellen på ”væsentlige” og ”vigtige enheder”
- Størrelseskriterierne og hvordan man beregner sin størrelse
- Jurisdiktionsbestemmelser
  - relevant for virksomheder som har aktiviteter i flere EU-lande



TVÆRGÅENDE NIS 2-VEJLEDNINGER 2/2

- Krav til foranstaltninger:
  - ✓ Politikker for informationssystemsikkerhed og risikostyring
  - ✓ Håndtering af hændelser, logning og monitorering
  - ✓ Driftskontinuitet, backup, redundans og krisestyring
  - ✓ Forsyningskædesikkerhed
  - ✓ Erhvervelse, udvikling og vedligeholdelse
  - ✓ Effektivitet af foranstaltninger
  - ✓ Cyberhygiejne og cybersikkerhedsuddannelse
  - ✓ Kryptografi
  - ✓ Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
  - ✓ Multifaktorautentificering og nødkommunikationssystemer
- Mapning til relevante internationale standarder



- Obligatorisk underretning om væsentlige hændelser
- Hvad er en væsentlig hændelse
- Proces for underretning
  <24 timer, <72 timer, <1 måned
- Frivillig underretning

På vej

Styrelsen for Samfundssikkerhed

FORANSTALTNINGSVEJLEDNING 1/2

- Udfolder krav til cybersikkerhedsforanstaltninger i NIS 2-lovens § 6
- Krav gælder både når, enheden selv driver sine net- og informationssystemer og ved outsourcing
- Net- og informationssystemer kan eksempelvis være it-systemer, OT-systemer, IoT-enheder og it-infrastrukturkomponenter
- Bygger på fortolkningsbidrag fra ENISA
- Mapping til relevante internationale standarder

FORANSTALTNINGSVEJLEDNING 2/2

- Vejledningen skelner mellem foranstaltninger som *skal* (krav), *bør* (anbefaling) og *kan* (eksempler) implementeres.
- Risikobaseret tilgang inkl. samfundsmæssig betydning
- All-hazards approach
- Bred definition af formkrav til dokumentation og politikker

EKSEMPEL PÅ FORANSTALTNING - FORSYNINGSKÆDESIKKERHED

- Risikobaseret tilgang
- Procedurer og aftaler/kontrakter
- Enheden bør anvende en risikobaseret tilgang, hvor kravene til den enkelte leverandør eller tjenesteudbyder er proportional med den specifikke leverances betydning for enhedens forsynings- og cybersikkerhed
- Forsyningskædesikkerhed er i fokus på tværs af EU-medlemsstater
- Vi vil løbende se på behov for vejledning

”Enheden skal implementere procedurer for leverandørstyring, der sikrer både forsyningssikkerhed og cybersikkerhed i samarbejdet med direkte leverandører eller tjenesteudbydere - i det omfang deres ydelser kan påvirke sikkerheden i forhold til den eller de ydelser, som gør, at enheden er omfattet af NIS 2.”

SAMARBEJDE OG KOORDINATION AF TILSYN

- Samarbejde om tilsyn i regi af NIS 2-koordinationsgruppen – forum for samarbejde mellem relevante myndigheder.
- De sektoransvarlige myndigheder samarbejder bl.a. omkring tilgange til tilsyn og håndtering af enheder, som har aktiviteter i flere sektorer
- MSSB udarbejder vejledning til de sektoransvarlige myndigheder

REGISTRERING PÅ VIRK.DK

- Virksomheder skal selv vurdere om de er omfattet af NIS 2.

  ➡ SAMSIK har lanceret et værktøj NIS 2-tjek som hjælp NIS 2-tjek

- Registrering åbner 1. juli 2025
- Mere info på www.samsik.dk/nis2 (snart)
- Vejledning hos de sektoransvarlige myndigheder

KOM GODT I GANG MED NIS 2

1

VURDER OM I ER OMFATTET AF NIS 2

- NIS 2-tjek
- Vejledning om anvendelsesområdet

2

INVOLVER LEDELSEN

- Vejledning om ledelsens rolle og opgaver

3

IMPLEMENTER CYBERSIKKERHEDS-FORANSSTALTNINGER

- Vejledning om implementering af cybersikkerheds-foranstaltninger

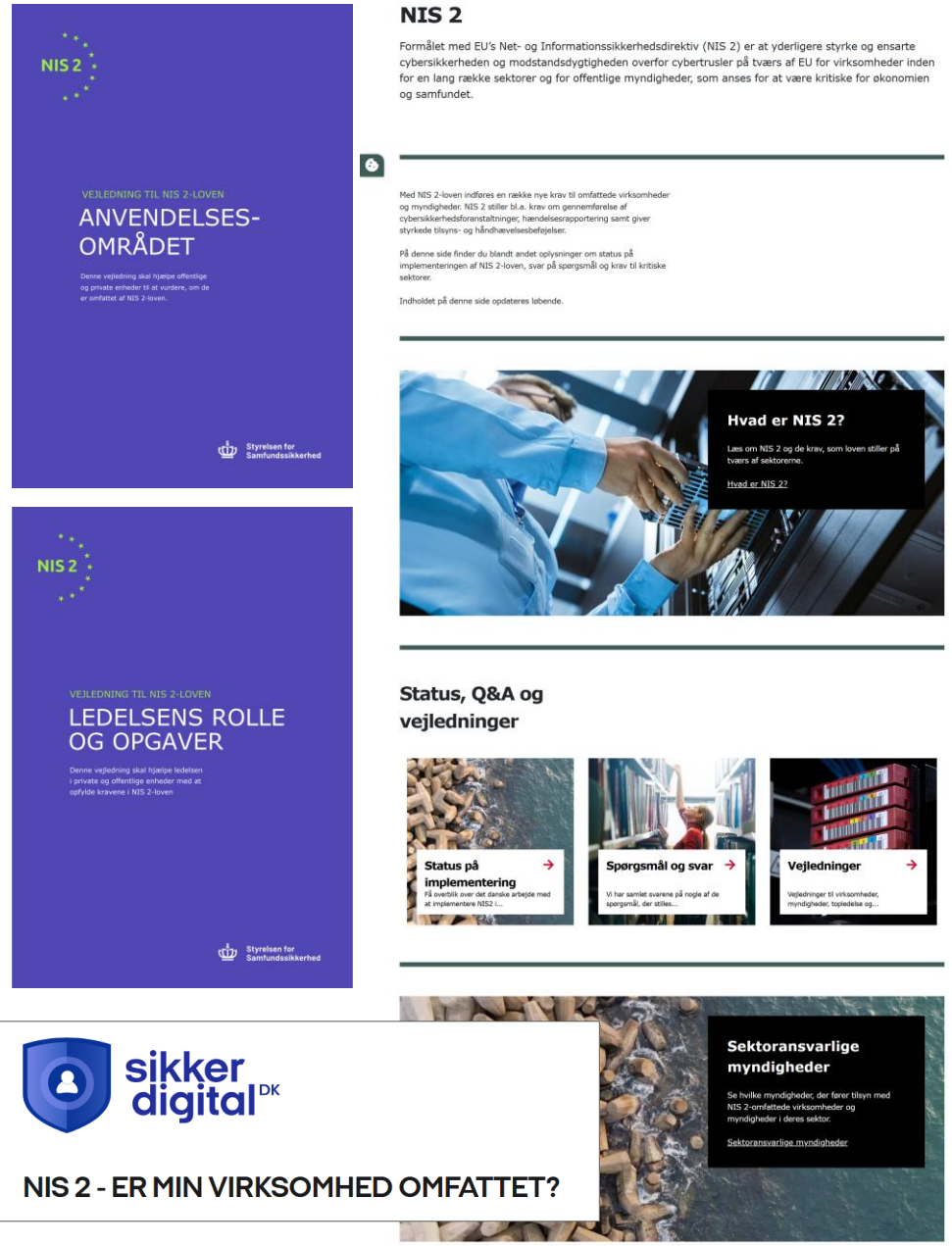
4

RAPPORTER VÆSENTLIGE HÆNDELSER

- Vejledning om hændelsesunderretning

FIND MERE INFORMATION OM NIS 2

- Vejledninger, info om sektoransvarlige myndigheder, spørgsmål og svar om NIS 2 m.m. på www.samsik.dk/nis2
- NIS 2-tjek - værktøj som hjælper virksomheder med at vurdere, om de er omfattet af NIS 2 på NIS 2-tjek
- Kontakt den relevante sektoransvarlige myndighed for vejledning og sektorspecifik information
- Kontakt SAMSIK nis2@samsik.dk



Styrelsen for Samfundssikkerhed

SPØRGSMÅL?

samsik.dk

Styrelsen for Samfundssikkerhed

@samfundssikker

NIS 2 og ISO/IEC 27001
Et perfekt par

Søren Koefoed

- Seniorkonsulent hos Dansk Standard
- Underviser og rådgiver inden for ISO/IEC 27000 serien
- Med i S-441 - udvalget for Cyber- og Informationssikkerhed hos Dansk Standard, hvor bl.a. nye versioner af 27000-seriens sikkerhedsstandarder udvikles.
- Med i S-852 Online Gambling

Baggrund:

- IT-master med speciale i IT-sikkerhed
- Underviser IT-governance UCL og SDU
- Spilmyndigheden
- Hosting branchen
- Uddannet i finanssektoren men ansvar for beredskab i handelsområdet

Program

- Mapning mellem NIS 2 og ISO/IEC 27001/2
- Afrapportering til CSIRT/myndighederne
- Spørgsmål

CASE:

Cyberkriminalitet – hvor alvorligt er det egenligt?

Hostingfirma lukker helt ned efter hackerangreb

Hosting-firmaet IT-hotellet ser sig nødsaget til at dreje nøglen om efter et alvorligt hackerangreb.

Foto: Steve Marcus

Kilde: https://watchmedier.dk/nyheder/resultater/article17179585.ece

Kære kunde hos IT-hotellet,

Dubex A/S har siden fredag assisteret IT-hotellet med et alvorligt cyberangreb. Thomas Vandsted Nielsen har i denne forbindelse bedt os dele nedenstående meddelelse med jer.

Kære Kunde,
IT-hotellet konstaterede fredag den 31. maj 2024 at vores systemer er blevet ramt af et alvorligt cyberangreb.

Vi involverede umiddelbart det eksterne sikkerhedsfirma Dubex A/S der er eksperter i håndtering af cyberangreb og har siden arbejdet på at få overblik over og inddæmme angrebet. Efter vi har fået gennemgået de enkelte systemer og fået et overblik over angrebets omfang, er det blevet tydeligt for os, at angrebet er langt mere omfattende end først vurderet og har ramt så mange systemer at det ikke umiddelbart kan inddæmmes. Vi har således konstateret at angriberne har installeret bagdøre på hovedparten af vores og vores kunders systemer. Vi vurderer desuden, at hvis vi forsøger at inddæmme angrebet yderligere, er der en overhængende risiko for at angriberne opdager dette og låser data med ransomware, hvorefter data vil være utilgængelige. Derfor har vi her til aften, den 6. juni 2024 besluttet at lukke alle kundesystemer ned for at begrænse konsekvenser af angrebet mest muligt.

Vi har desværre også måtte erkende at IT-hotellet hverken har de nødvendige interne ressourcer eller økonomiske mulighed for at gennemføre den oprydning der skal til for at reetablerer alle systemer til en sikker tilstand. Det er derfor også vores forventning af IT-hotellet lukker eller går konkurs som følge af dette angreb.

Vi vil gerne takke for den tillid I som kunder har vist os, ligesom det er med dyb beklagelse at vi er havnet i denne dybt ulykkelige situation. Vi har et stort ønske om hjælpe jer bedst muligt videre, og har derfor arrangeret at Dubex i den kommende periode fortsat vil have adgang til vores systemer. IT-hotellet har i den nuværende situation ikke mulighed for at afholde omkostningerne til yderligere håndtering af cyberangrebet, hvorfor I som kunde selv er nødt til at lave en aftale direkte med Dubex A/S. I vil efterfølgende kunne rejse et krav mod IT-hotellets eller vores konkursbo og derigennem vores forsikringsselskab, og derved måske kunne få dækket nogen af jeres omkostninger og tab.

Dubex A/S vil kunne hjælpe med reetablering af de enkelte systemer, udtræk af data fra serverne, udlevering af enkelte servere og efterforskning af evt. datakompromittering. Du kan kontakte Dubex A/S for den videre dialog eller udlevering af jeres data på e-mail support@dubex.dk eller via telefonnummer 3160 5800.

Med stor beklagelse og venlig hilsen,
Thomas Vandsted Nielsen
Direktør, IT-hotellet

Spørgsmål og svar

Hvornår kan jeg få mine data?
Der foregår ikke systematisk arbejde med at reetablere alle systemerne hos IT-Hotellet, hvorfor data ikke automatisk bliver tilgængeligt for kunderne på et givet tidspunkt. For at du som kunde kan få adgang til data, skal du rette henvendelse til support@dubex.dk. For at vi kan behandle din anmodning om adgang til, eller udlevering af data, skal du angive virksomhedens navn, CVR-nummer, kontaktperson, telefon nummer og navnet på den/de tegningsberittiget I virksomheden, så vi kan verificere din identitet inden udlevering af data. Hvis du allerede ved hvilke data der er vigtigst for dig, må du meget gerne notere det.

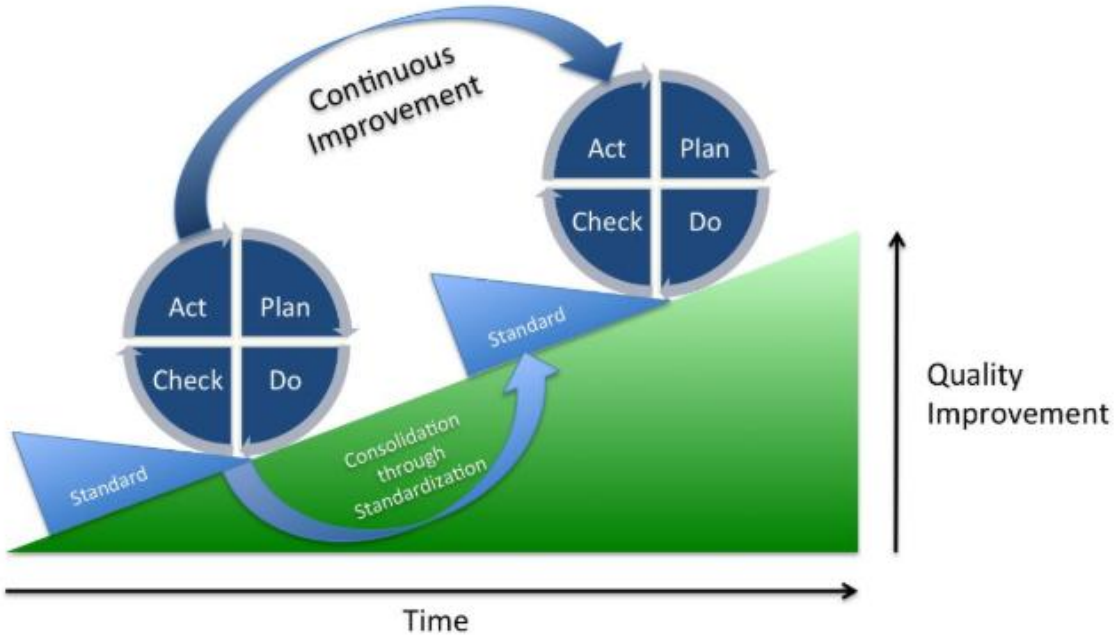
Introduktion til standarder og ISO/IEC 27001

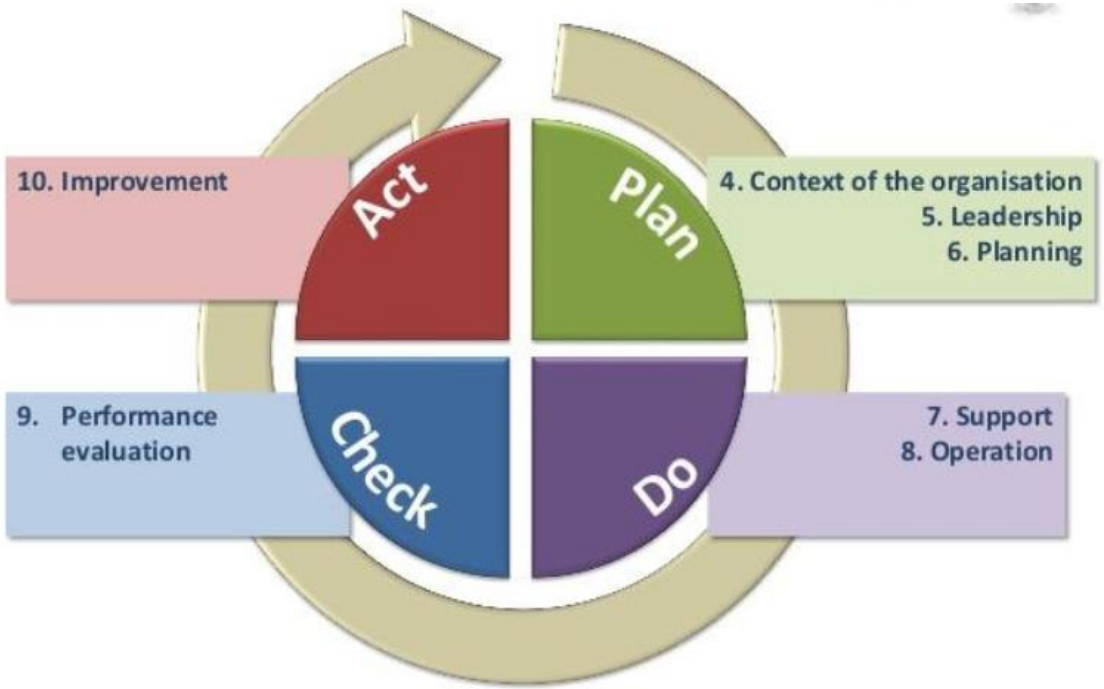
NIS 2 direktiv
Artikel 25

Standardisering

For at sikre en samordnet gennemførelse af artikel 21, stk. 1 og 2, tilskynder medlemsstaterne til at benytte **europæiske og internationale standarder** og tekniske specifikationer, der er relevante for sikkerheden i net- og informationssystemer, uden at de påtvinger eller forskelsbehandler til fordel for anvendelse af en bestemt type teknologi

ISO-principper for ledelsesstandarder





ISO/IEC 27001, Anneks A

Risikovurdering, muligheder for risikohåndtering og kriterier for risikoaccept.

Overholdelse af lovgivning, aftaler eller brancherelaterede krav.

Effekten af samspillet mellem forskellige foranstaltninger.

Kapitel 5. Organisatorisk
- alt det andet

Kapitel 6. Personrelateret
- personer: ansatte og eksterne

Kapitel 7. Fysisk
- de fysiske rammer og enheder

Kapitel 8. Teknologisk
- tekniske tiltag

NIS 2

Ledelsesansvar

Artikel 20

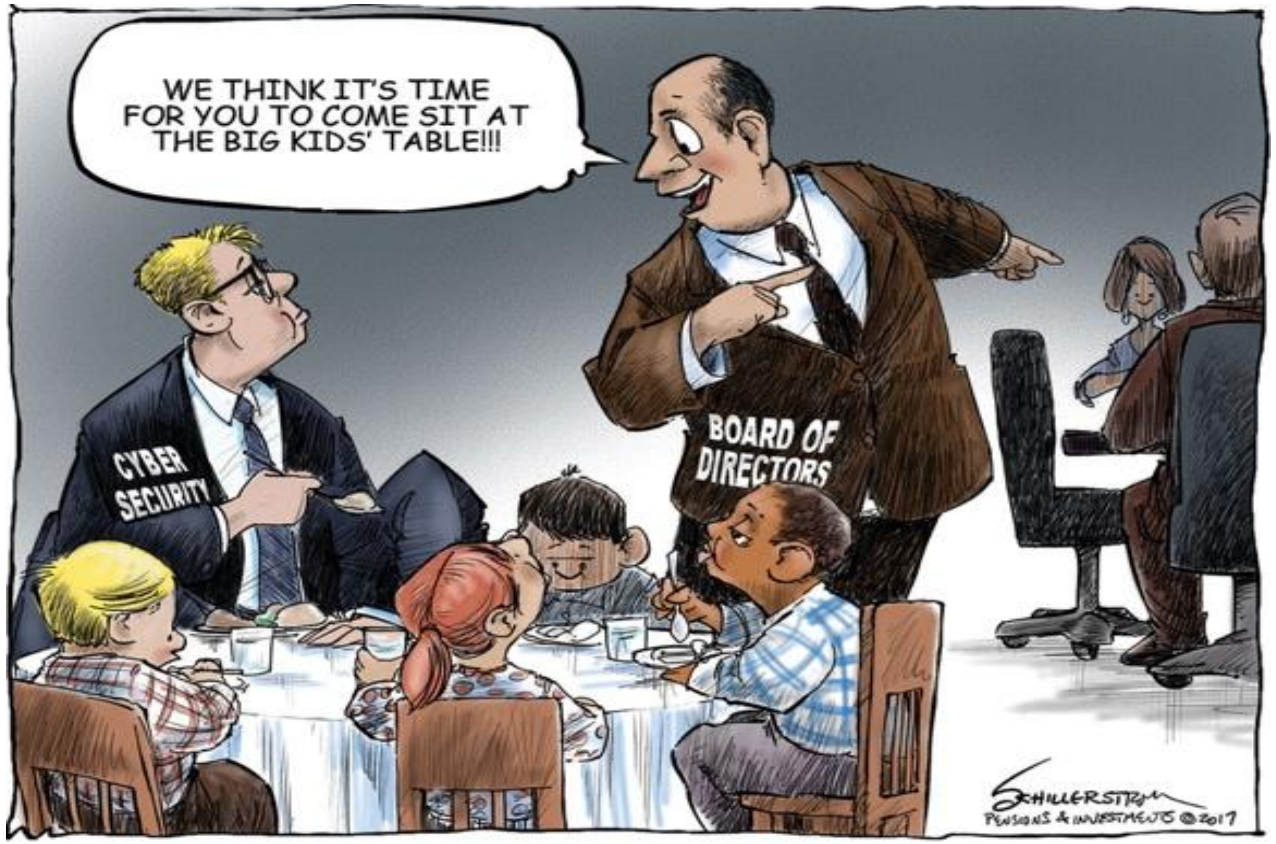
Styring

1. Medlemsstaterne sikrer, at de væsentlige og vigtige enheders 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.
Anvendelsen af dette stykke berører ikke national ret for så vidt angår de ansvarsregler, der gælder for offentlige institutioner, samt ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv.

2. Medlemsstaterne sikrer, at 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.

Ledelsens engagement

- ISO/IEC 27001 5.1 Lederskab og engagement
- ISO/IEC 27001 9.3 Ledelsens gennemgang



Strafferamme og sanktionsmuligheder

- Direktivet opdeler virksomheder i 'væsentlige' og 'vigtige', hvor der er en forskel i bødeniveau for at overtræde kravene om sikkerhedsforanstaltninger og anmeldelsespligten.
- Væsentlige virksomheder risikerer en bøde på op til 10 millioner euro eller 2 procent af den globale årlige omsætning, hvor vigtige virksomheder risikerer bøder på op til 7 millioner euro eller 1,4 procent af den globale årlige omsætning.
- Ledelse og bestyrelse kan stilles personligt til ansvar for manglende compliance

Grundlæggende risikovurdering

NIS 2 artikel 21.1

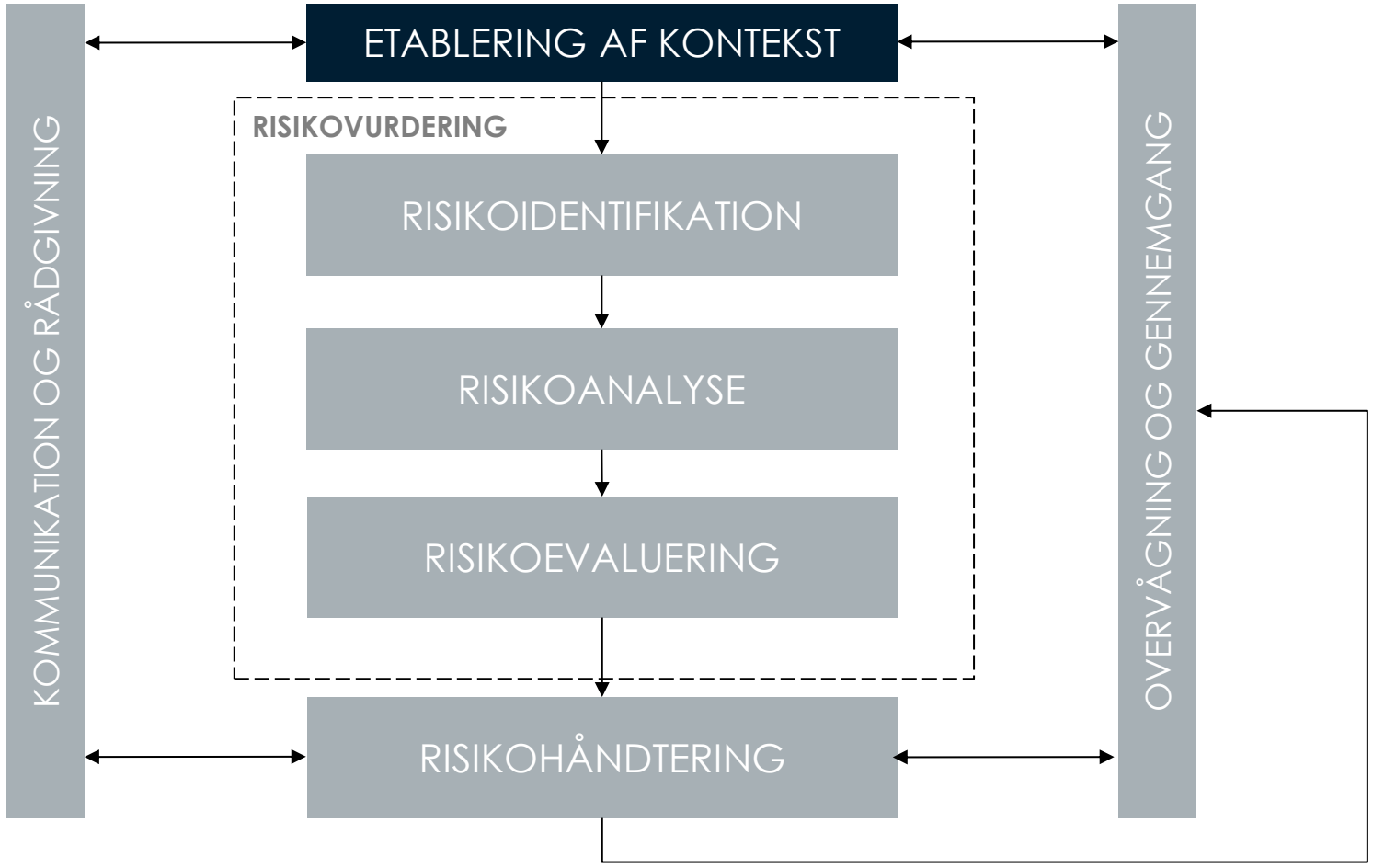
Artikel 21

Foranstaltninger til styring af cybersikkerhedsricisi

1. Medlemsstaterne sikrer, at væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

Under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne skal de i første afsnit omhandlede foranstaltninger tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.

Risikostyringsprocessen



Foranstaltninger
Artikel 21

Politikker for informationssikkerhed

NIS 2

Foranstaltninger til styring af cybersikkerhedsricisi

Artikel 21, stk. 2
De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:

a) politikker for risikoanalyse og informationssystemsikkerhed

ISO

DANSK STANDARD

ISO/IEC 27001

- ISO/IEC 27001 5.2 Politik
- ISO/IEC 27001 6.1 Handlinger til håndtering af risici og muligheder

ISO/IEC 27001 Annex A

- 5.1 Politikker for informationssikkerhed

Håndtering af hændelser

NIS 2

Foranstaltninger til styring af cybersikkerhedsricisi

Artikel 21, stk. 2

De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:

b) håndtering af hændelser

ISO

DANSK STANDARD

- **ISO/IEC 27001 Annex A**
- 5.24 Planlægning og forberedelse af incidenthåndtering ved sikkerhedsincidents
- 5.25 Vurdering af og beslutning om informationssikkerhedshændelser
- 5.26 Håndtering af informationssikkerhedsincidents
- 5.27 Læring fra informationssikkerhedsincidents
- 5.28 Indsamling af bevismateriale
- 6.8 Indrapportering af informationssikkerhedshændelser

Driftskontinuitet

NIS 2

Foranstaltninger til styring af cybersikkerhedsricisi

Artikel 21, stk. 2

De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:

c) driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring

ISO

DANSK STANDARD

ISO/IEC 27001 Annex A:

- 5.29 Informationssikkerhed under driftsforstyrrelse
- 5.30 IKT-Parathed til understøttelse af business continuity
- 8.13 Backup af information

Netværkssikkerhed

NIS 2

Foranstaltninger til styring af cybersikkerhedsricisi

Artikel 21, stk. 2

De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:

e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

ISO

DS DANSK STANDARD

ISO/IEC 27001 Annex A:

- 5.7 Underretning om trusler
- 8.20 Netværkssikkerhed
- 8.21 Sikring af netværkstjenester
- 8.25 Sikker udviklingslivscyklus
- 8.26 Krav til applikationssikkerhed
- 8.27 Sikker systemarkitektur og udviklingsprincipper
- 8.28 Sikker programmering
- 8.29 Sikkerhedstest under udvikling og godkendelse

Effektivitet, Awareness, Kryptografi

NIS 2

Foranstaltninger til styring af cybersikkerhedsricisi

Artikel 21, stk. 2

De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:

f) politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici

g) grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse

h) politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering

ISO

DANSK STANDARD

(fsva. f) ISO/IEC 27001

- 9.1 Overvågning, Måling, analyse og evaluering

(fsva. g) ISO/IEC 27001 Annex A

- 6.3 Awareness, uddannelse og træning vedrørende informationssikkerhed

(fsva. h) ISO/IEC 27001 Annex A

- 8.24 Use of cryptography

Personrelateret sikkerhed

NIS 2

Foranstaltninger til styring af cybersikkerhedsricisi

Artikel 21, stk. 2

De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:

i) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

ISO

DANSK STANDARD

ISO/IEC 27001 Annex A:

- 6.1-6.8 Personrelaterede foranstaltninger
- 5.1 Politikker for informationssikkerhed *(Emnespecfikke jf, 27002:2022: administration af adgange, styring af aktiver)*
- 5.15 Administration af adgang
- 5.9 Fortegnelse over information og understøttende aktiver.
- 5.10 Acceptabel brug af information og understøttende aktiver.
- 5.11 Returnering af aktiver
- 8.15 Logning

Multifaktorgodkendelse

NIS 2

Foranstaltninger til styring af cybersikkerhedsricisi

Artikel 21, stk. 2

De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:

j) brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

ISO

DANSK STANDARD

ISO/IEC 27001 Annex A

- 5.15 Administration af adgang *(Dataadgangspolitik kan kræve MFA eller andre former for sikker identifikation/godkendelse, herunder kontinuerlig godkendelse - ikke kun ved login, men kontinuerligt gennem hele sessionen jf, ISO/IEC 27002:2022 5.15)*
- 5.30 IKT parathed til understøttelse af business continuity.

Afrapportering

Artikel 23

Rapporteringsforpligtelser

1. Hver medlemsstat sikrer, at væsentlige og vigtige enheder uden unødigt ophold underretter dens CSIRT eller i givet fald dens kompetente myndighed i overensstemmelse med stk. 4 om enhver hændelse, der har en væsentlig indvirkning på leveringen af deres tjenester som omhandlet i stk. 3 (væsentlig hændelse). Hvor det er relevant, underretter de pågældende enheder uden unødigt ophold modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af disse tjenester negativt. Hver medlemsstat sikrer, at disse enheder indberetter bl.a. alle oplysninger, der gør det muligt for CSIRT'en, eller i givet fald den kompetente myndighed, at fastslå eventuelle grænseoverskridende virkninger af hændelsen. Underretningen i sig selv medfører ikke et øget ansvar for den underrettende enhed.

Anmeldelse af sikkerhedshændelser til myndighederne

3. **En hændelse anses for at være væsentlig, hvis:**

a) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed

b) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade

Kurser fra Dansk Standard

NIS 2 i praksis
NIS 2 for kommunerne
NIS 2 for ledelsen

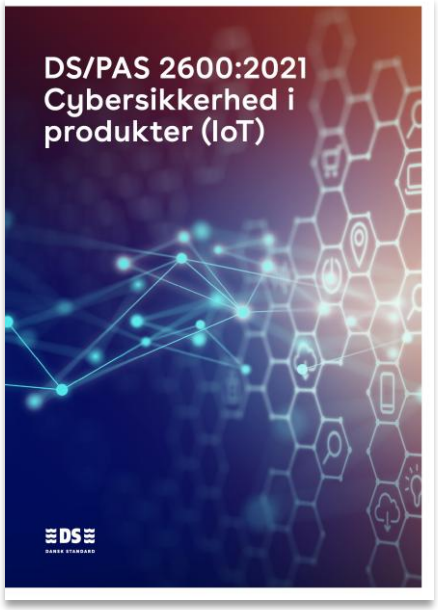
Se alle Dansk Standards kurser i informationssikkerhed og NIS 2:
https://www.ds.dk/da/kurser-og-arrangementer/kurser/informationssikkerhed

Spørgsmål

Tak for i dag

Søren Koefoed-Hansen
Tlf.: 2234 6279
E-mail: skh@ds.dk

Udgivelser fra Dansk Standard der kan hjælpe virksomheder og organisationer i gang



https://www.ds.dk/da/download/ds-pas-2600-2021

https://www.ds.dk/da/om-standarder/viden/cyber-og-informationssikkerhedsstandarder/guide-til-risikostyring

https://www.ds.dk/da/download/ds-inf-21007-2024

Koblingen mellem lovgivning på det digitale område og standarder

Cyber Resilience Act

Cyber Resilience Act er en ny EU-forordning som stiller fælleseuropæiske cybersikkerhedskrav til produkter med digitale elementer. Med forordningen følger en række standarder, der skal hjælpe virksomhederne med at leve op til de horisonale cybersikkerhedskrav.

Cyber Security Act

Den europæiske forordning om cybersikkerhed har til formål at etablere en fælles europæisk ramme for certificering inden for cybersikkerhed, som forventes at bygge på eksisterende standarder.

Data Act

Dataforordningen (Data Act) skal skabe harmoniserede regler om fair adgang til og anvendelse af data og gøre det lettere for europæiske virksomheder at dele og anvende data.

AI Act

Forordningen om kunstig intelligens (AI Act) skal sikre fælles spilleregler for brugen og udviklingen af kunstig intelligens. Med forordningen følger en række standarder, der skal hjælpe virksomhederne med at leve op til kravene om kunstig intelligens, som forordningen stiller.

Data Governance Act

Datastyringsforordningen (Data Governance Act) har til formål at skabe tillid til datadeling til gavn for samfundet, og der skal bl.a. prioriteres tværsektorielle standarder for datadeling og interoperabilitet.

GDPR

Databeskyttelsesforordningen (GDPR) fastlægger fælleseuropæiske retningslinjer for håndteringen af personoplysninger for virksomheder, organisationer, myndigheder mm.

NIS2-direktivet

NIS2-direktivet indeholder skærpede krav til cyber- og informationssikkerhed i forhold til kritisk infrastruktur. Direktivet opfordrer til at anvende internationale, anerkendte standarder.

https://www.ds.dk/da/i-fokus/lovgivning/lovgivning-paa-det-digitale-omraade-og-standarder

DS Cyberdag

1. oktober 2025

Programmet er under udarbejdelse.

DS CYBERDAG

Spørgsmål?

DANSK STANDARD