Webinar:
Vejen til robust NIS2-implementering i pharma og life science

Februar 2026

Agenda

1. Velkommen
2. Perspektiv fra myndighederne:
   NIS2 og sundheds- & life science sektoren
   v. Søren Bank Greenfield, Sundhedsdatastyrelsen
3. PwC NIS2 Cybersikkerhed og Q&A
4. Afrunding og tak for i dag

Den stadig stigende digitalisering af samfundets kritiske infrastruktur bærer en lang række fordele med sig, men øger også behovet for at styrke cybersikkerheden i virksomheder og organisationer.

NIS2 styrker det generelle niveau af cybersikkerhed i EU ved at skærpe kravene til cybersikkerhed.

Kort fortalt

- NIS2-loven **trådte i kraft pr. 1. juli 2025.**
- **Selvvurdering**: Organisationer er ansvarlige for at vurdere, om de er omfattet af NIS2. Registrere sig hos kompetente myndighed **senest d. 1. oktober 2025.**
- **Sundhed** er sektor af **særlig kritisk betydning**, herunder sundhedsudbydere, forskningslaboratorier, farmaceutiske virksomheder og producenter af medicinsk udstyr m.fl.
- NIS2 **påvirker hele forsyningskæden**, som skal sikres.
- **Passende og forholdsmæssige** sikkerhedsforanstaltninger baseret på **konkrete risikovurderinger**
- **10 centrale minimumsforanstaltninger** for cybersikkerhed, herunder sikre løsninger og teknologiske krav, dokumentere og sikre forsyningskæder, hændelseshåndtering og forretningskontinuitet
- Den **øverste ledelse** har fået en fremtrædende og central rolle. Bestyrelsen kan ifalde **individuelt og personligt ansvar**.

2

Perspektiv fra myndighederne:

NIS2 og sundheds- & life science sektoren

v. Søren Bank Greenfield, Sundhedsdatastyrelsen

NIS2

Søren Bank Greenfield

2026

SUNDHEDSDATA-
STYRELSEN

Baggrund for NIS

Bygger videre på NIS1 direktivet fra 2016

Det er et direktiv fra EU fra 2022

- Implementeret ved lov som blev vedtaget den 26. april 2025
- **Trådte i kraft den 1. juli 2025 i DK**

Formål

- At sikre et højt cybersikkerhedsniveau på tværs af medlemslandene
- At gøre samfundet mere robust

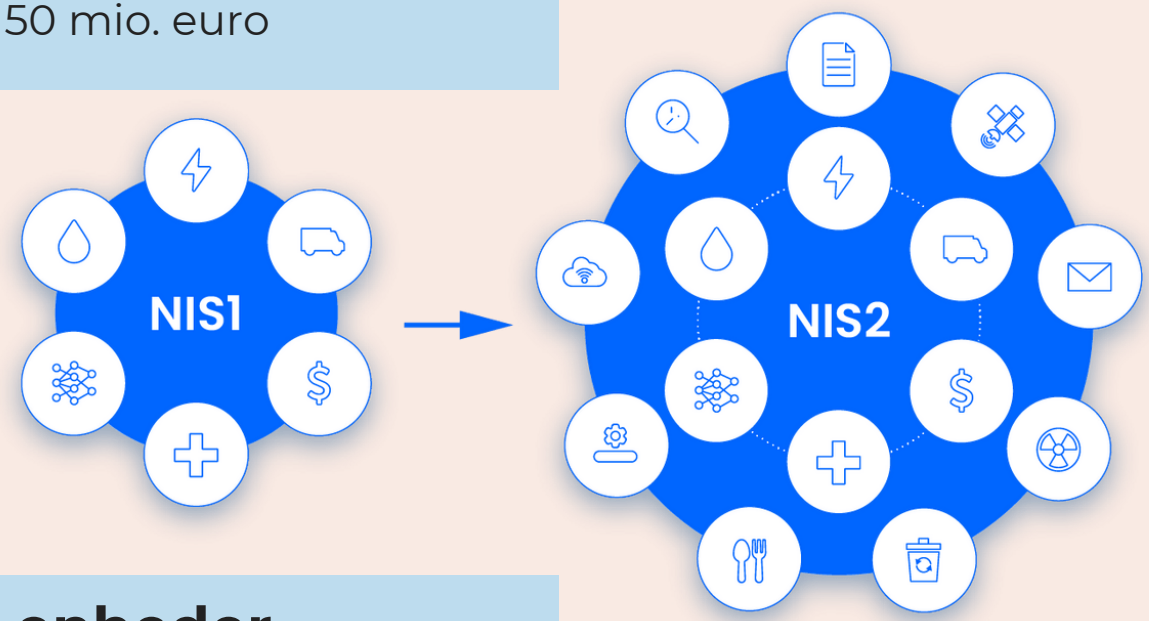
Hedder i dansk lov:
Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2 loven)

Hvad er nyt?

- Udvider anvendelsesområde
  - Nye kritiske sektorer
  - Fra 7 til 18 kritiske sektorer
- Fastlægger nye rammer
  - Indfører minimumsikkerheds-foranstaltninger og ledelsesansvar
  - Indfører skærpede krav om hændelsesrapportering
  - Bødestraf for private
    - Ikke offentlige myndigheder

Væsentlige enheder

- Enheder der beskæftiger 250 personer eller derover
- Enheder med årlig omsætning på over 50 mio. euro



Vigtige enheder

- Enheder der beskæftiger 50 personer eller derover
- Enheder der har en årlig omsætning på over 10 mio. euro

Hvem er omfattet i øvrigt?

Væsentlige enheder

- Den centrale forvaltning
- Regioner og kommuner
- Enheder omfattet af CER
- Enheder omfattet af NIS1

Vigtige enheder

- Enheder udpeget som vigtig af tilsynsmyndighed

Eksempler for sundhedsområdet

Kategori	> 250 ansatte	50-250 ansatte	< 50 ansatte
Sundhedstjenesteydere	**Regioner (Hospitaler), Kommuner og andre "aktører i sundhedsvæsenet, der yder sundhed"**	**Privathospitaler, fertilitetsklinikker, store sundheds- og lægehuse, ambulancetjenester**	
EU reference laboratorier	Udpegede EU-reference laboratorier	Udpegede eu-reference laboratorier	
Enheder, der udfører forsknings- og udviklingsaktiviteter vedrørende lægemidler	Medicinalproducenter	Forskningsenheder	
Enheder, der fremstiller farmaceutiske råvarer og farmaceutiske præparater	Medicinalproducenter	Medicinalproducenter; produktion af råvarer, som anvendes i lægemidler	
Enheder, som fremstiller medicinsk udstyr, som den anser for at være kritisk i en folkesundhedsmæssig krisesituation	Medicoproducenter	Medicoproducenter, mundbinds eller håndsprits producenter	
Fremstilling af medicinsk udstyr og medicinsk udstyr til in vitro-diagnostik	Medicoproducenter, dentale instrumenter	Medicoproducenter, dentale instrumenter	

Hvad betyder det så for en omfattet enhed (SDS)?

SUNDHEDSDATA-
STYRELSEN

Så hvad skal man gøre?

0. Lav en ”omfattelsesvurdering” med begrundelse for hvilken sektorer man er omfattet af

Registrer organisation på Virk.dk (inden 1. oktober 2025)
Det kan dog nås endnu ☺ En enhed skal registrere sig to uger efter den bliver omfattet af loven

1. Konsekvensvurder processer i forhold til ”det man er omfattet på baggrund af” (er det NIS2 tjenester eller aktiviteter?)

2. For ”NIS2 tjenester eller aktiviteter”
– Risikovurdér underliggende NIS infrastruktur ift. autenticitet (+FIT)

3. For NIS2 infrastruktur
– implementér passende foranstaltninger

4. For NIS tjenester og aktiviteter””
– ledelsesrapporter og ansvarstagen for foranstaltninger

Certificér i ISO27001?

8. Cyberspecifikt uddannelse af Ledelse (og medarbejdere)

Fast få NIS2 specifikt revisions erklæringer fra leverandører?

7. Udarbejd proces for og udfør tilsyn med leverandører i ”første led”

6. Lav aftaler med alle leverandører omkring hændelseshåndtering, rapportering og tilsyn

Beslut:
Hvem skal indmelde hændelserne på virk.dk?

5. Udarbejd proces og skaf bemanding for hændelseshåndtering og rapportering:
- Tidlig advarsel **inden for 24 timer.**
- Indberetning om hændelsen **senest efter 72 timer.**
- En endelig rapport senest **én måned med RCA.**

Bemærk: Indmelding for ”de NIS systemer der ***kan*** påvirke enhedens evne til at ***levere*** de ydelser, som gør, at enheden er **omfattet af** NIS2-loven”.

Hvad er vigtig for topledelsen?

1. Man skal kende de ””ydelser” (Tjenester og aktiviteter) organisationen udfører for sektoren/sektorerne og som er kritiske for forretningen.
2. Man skal kende den overordnede cybertrussel og have cyber- området med i prioriteten af indsatser.
3. **Allervigtigst: Man skal kende til udfordringer eller områder, der kunne være problematiske for de ”ydelserne” organisationen yder for sektoren.**

Status på NIS2

- Er trådt i kraft 1. juli og alle skal indmelde hændelser (24/72/1 måned)
- Alle skal have indmeldt sig 1. okt. 2025.
- Myndighederne er ved at gennemgå listerne og ”minder” virksomhederne om det.
- Myndigheder laver vurderinger om der mangler nogen.
- 25 april melder myndigheder til EU – hvem er omfattet i hvert land.

Spørgsmål

Kan også rettes til:

NIS2sundhedssektoren@sundhedsdata.dk

SUNDHEDSDATA-
STYRELSEN

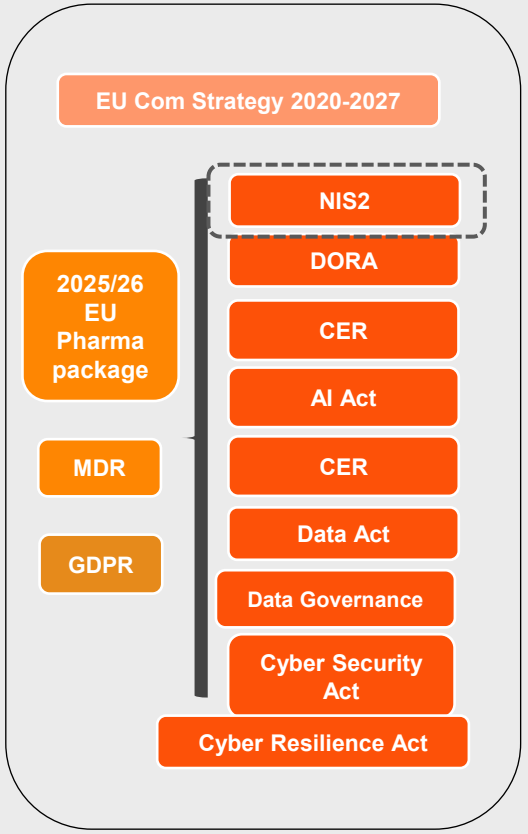
3

PwC NIS2 Cybersikkerhed og Q&A

Cybersikkerhed trends NIS2 anno 2026

3. februar 2026

Regulatory security compliance-by-design

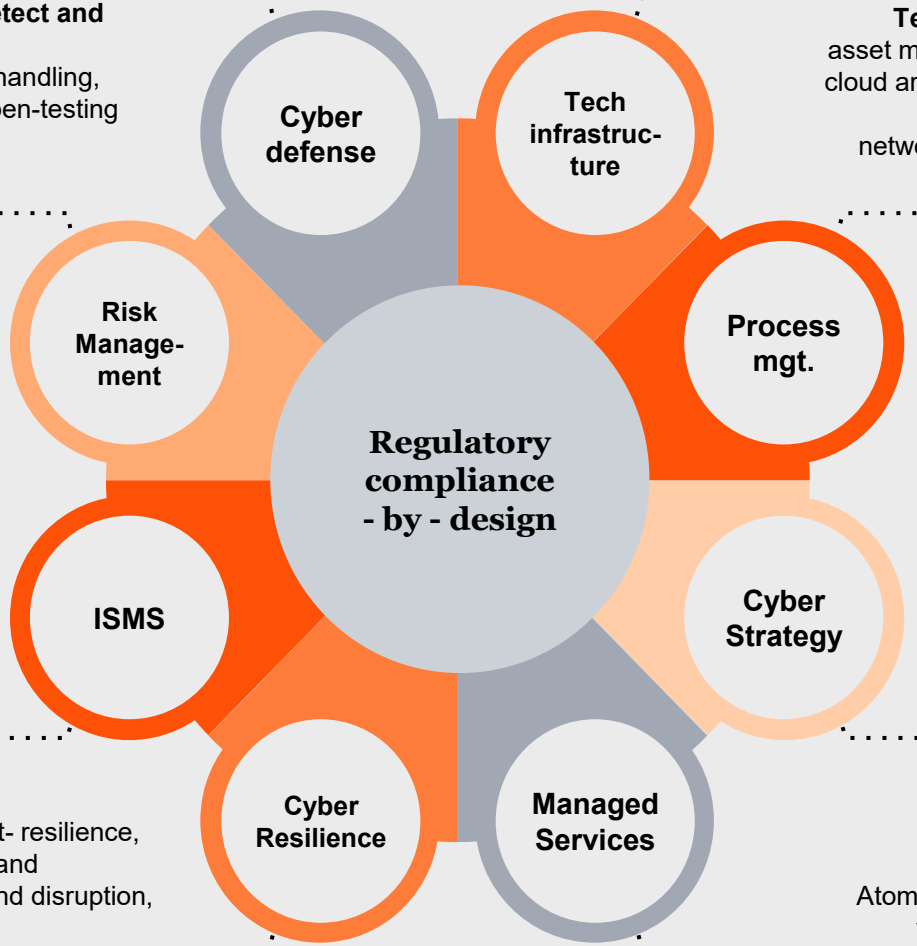


Cyber Defence, detect and response
,incident response handling, disaster recovery, pen-testing

Risk mgt.
Incl.. security risks and threats, ERM BIA, DPIA, TPRM, vendor risk mgt, Supply Chain

ISMS
incl. ISO/NIST, ENISA and industry standards, security compliance, benchmark and governance, cyber controls alignment

Cyber Resilience
incl BCM, crisis mgt- resilience, testing of recovery and emergency plans and disruption, wargaming



Tech infrastructure incl. asset mgt, encryption, SSLCD, cloud architects solution end-to -end, network security, network segmentation, SOC services, IAM, PAM

Process mgt. incl SOP, process and policies

Cyber Strategy and TOM – Zero Trust Architecture and infrastructure, cost of compliance

Managed Services,
Atomate and oprate, Tech vendors, agentic Ai,..

Cybercrime survey 2025: Cybertrusler

86 %

af virksomhederne med en øget bekymring for cybertrusler relaterer denne til den geo-politiske situation.

76 %

af virksomhedernes bestyrelser har cyber-sikkerhed som en fast del af deres årshjul.

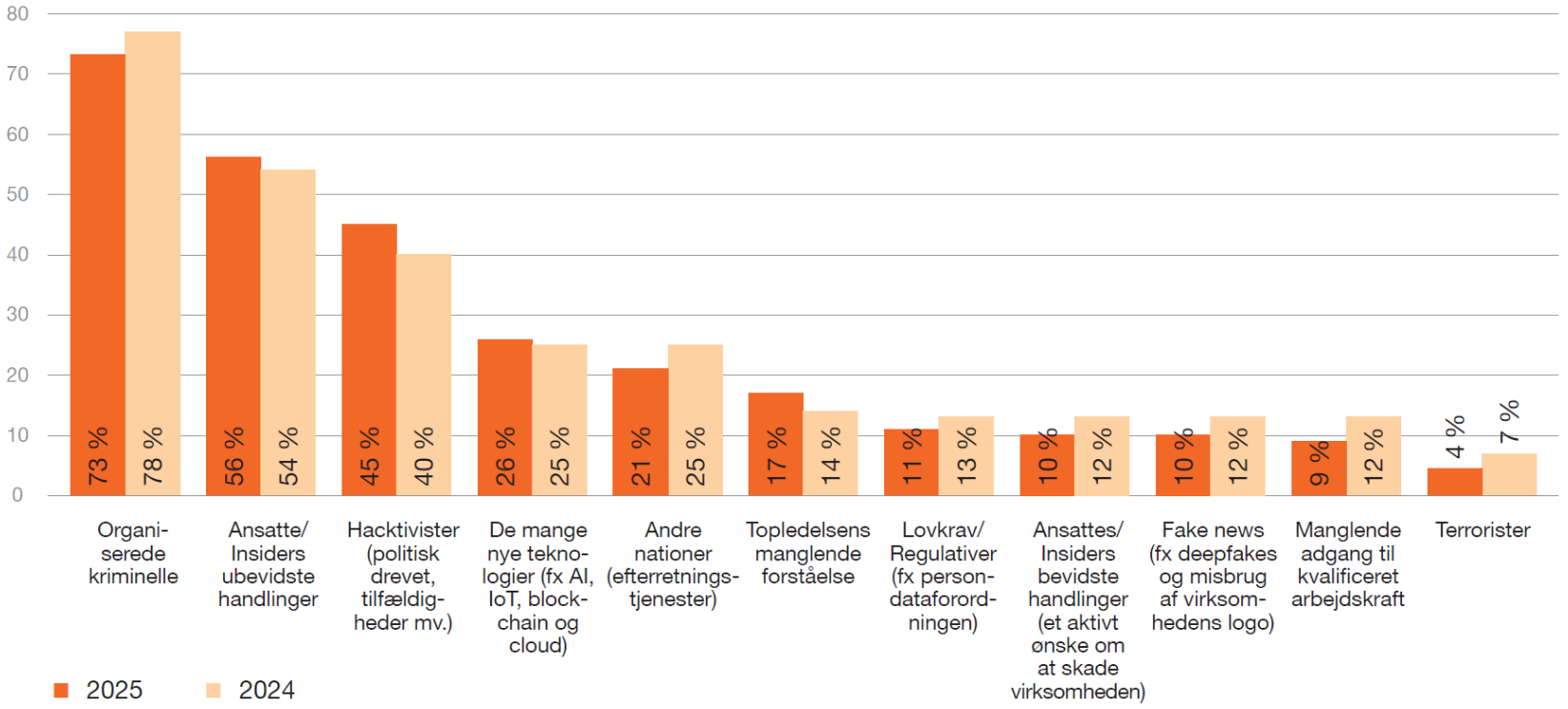
50 %

af virksomhederne op-lever, at manglende over-blik over tredjeparter og leverandører er den største barriere for at leve op til de nye sikkerheds-

64 %

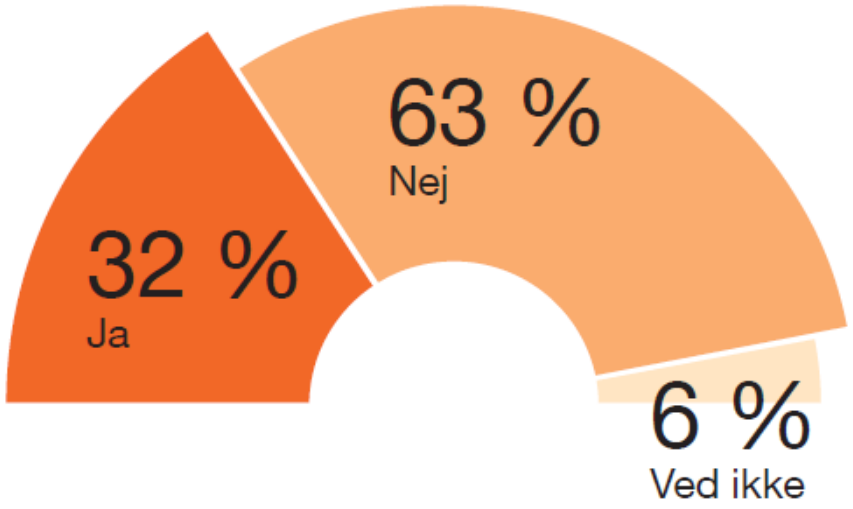
af respondenterne forventer, at deres virksomheds cyber- og informations-sikkerhedsbudget vil vokse inden for de

Hvad udgør de største trusler for din virksomhed i relation til cyber- og informationssikkerhed?

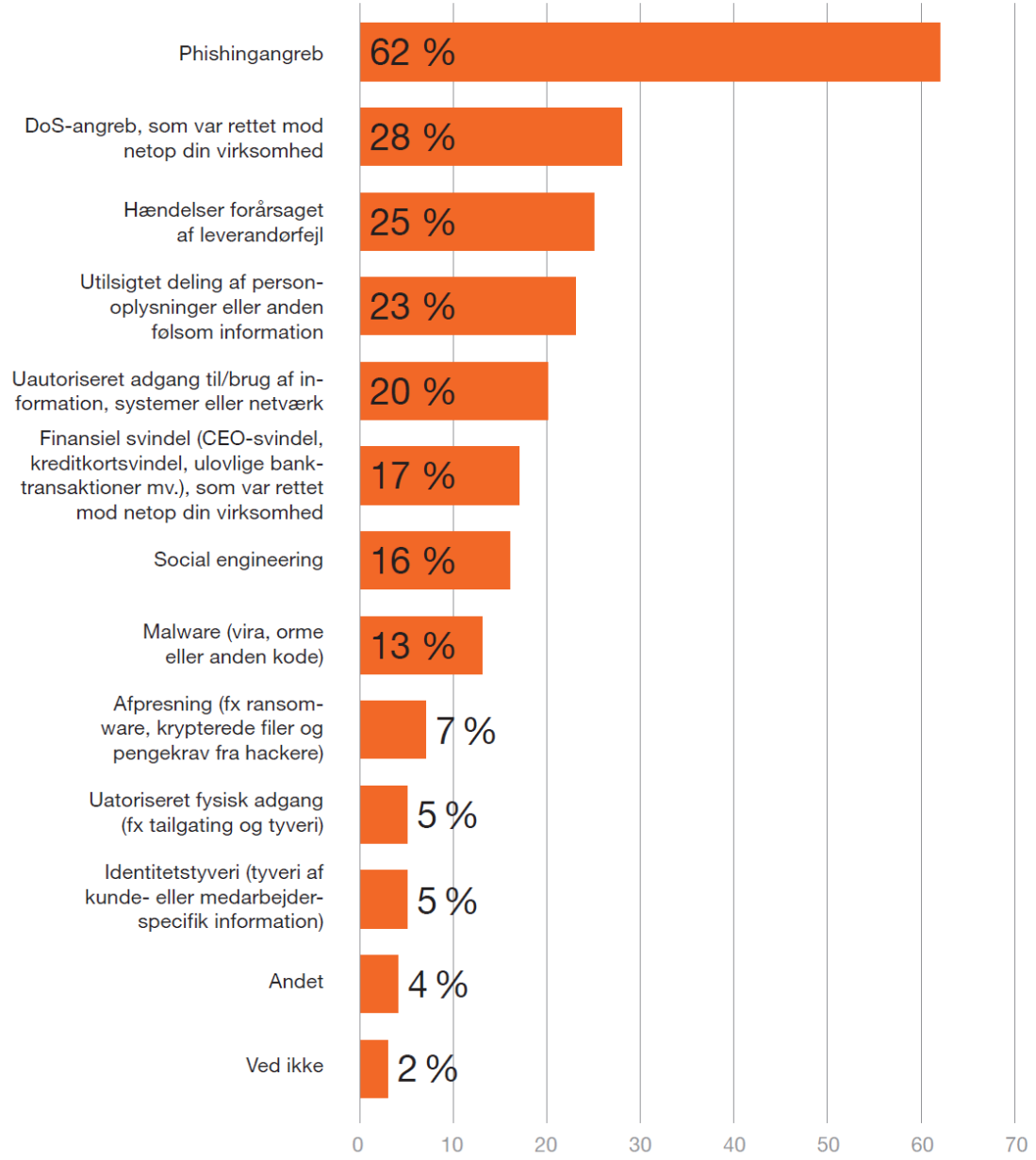


Cybercrime survey 2025: Sikkerhedshændelser

Har din virksomhed været udsat for en sikkerhedshændelse inden for de seneste 12 måneder?

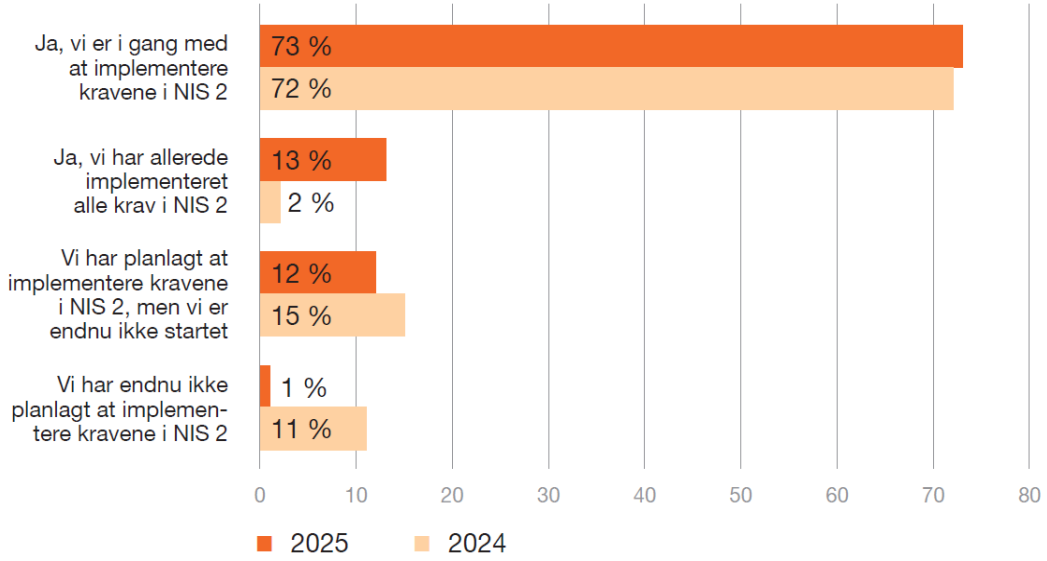


Hvilken type sikkerhedshændelse(r) var der tale om?



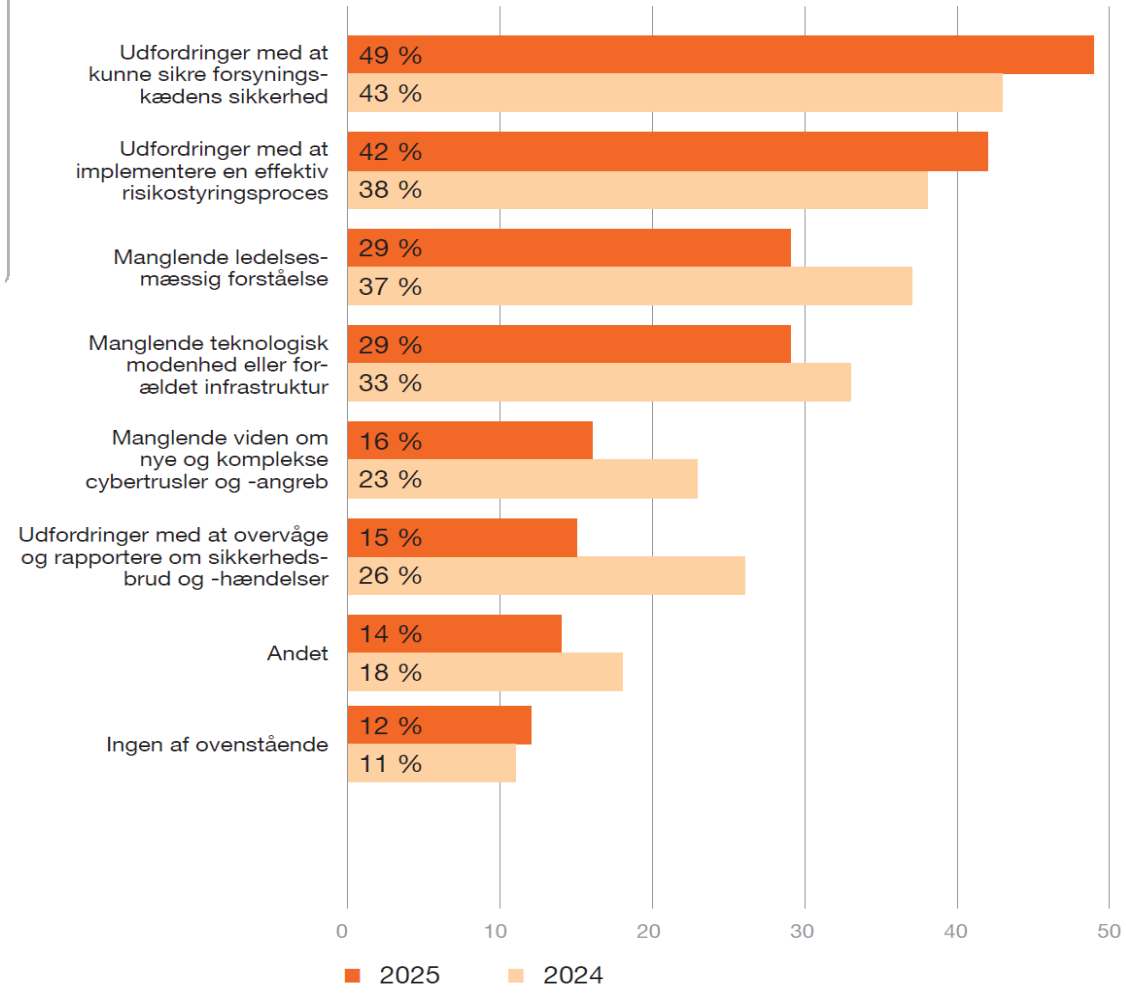
Cybercrime survey 2025: NIS2-direktivet

Har din virksomhed* en plan for, hvordan I vil imødekomme/implementere kravene i NIS 2-direktivet?



*) Kun virksomheder, der har angivet, at de er omfattet af NIS 2.

Hvilke af følgende ser du som barrierer for, at din virksomhed* kan leve op til kravene i NIS 2-direktivet?



*) Kun virksomheder, der har angivet, at de er omfattet af NIS 2.

4

Afrunding

Tak for i dag og på gensyn

Webinar: Sådan sikrer I, at ledelsen har de rette kompetencer til at efterleve NIS2

Onsdag den 18. februar 2026
Kl. 15.00-16.00

På webinaret får du en klar gennemgang af de vigtigste ledelseskrav i NIS2: ansvar, dokumentation, risikostyring og den praktiske gennemførsel af træningen. Du får konkrete værktøjer til, hvordan ledelsen kan styrke virksomhedens robusthed og sikre en effektiv efterlevelse.

Læs mere og tilmeld dig via QR-koden: