

KOM GODT I GANG MED NIS2

NIS2 har fokus på cybersikkerhed, og indgår som en væsentlig forudsætning for at kunne opretholde kvalitet og leverancesikkerhed for produkter og serviceydelser. NIS2 er relevant for alle, der måles på leveringssikkerhed, sporbarhed og kundetilfredshed. Di-rektivet løfter cybersikkerhed op på ledelsesniveau og kobler det til det, virksomheder allerede gør i kvalitetsledelsen: risikovurdering, forebyggelse og løbende forbedring. Læs med og få inspiration til hvordan virksomheder kan omsætte kravene til praksis, uden at gøre det tungere end nødvendigt.

Af **Mikkel Lundstrøm**, Virksomhedskonsulent i Unik Consult

INTRODUKTION OG BAGGRUND

NIS2-loven (Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau) trådte i kraft d. 1. juli 2025 i Danmark:
[Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau \(NIS 2-loven\)](#)

NIS2 (Network and Information Security Directive 2) er et EU-direktiv, der blev vedtaget af EU i oktober 2022. Der er således gået næsten 3 år fra vedtagelsen af NIS2-direktivet til det bliver implementeret i Danmark. NIS2 afløser det oprindelige NIS-direktiv fra 2016 som var mere begrænset i forhold til omfattede brancher og virksomheder, samt krav, der skulle opfyldes.

Manglende efterlevelse af kravene i NIS2-loven kan føre til virksomhedsbøder op til 10 mio. EUR eller 2 % af global omsætning, ledelsesmæssige sanktioner for bestyrelse/direktion samt øget tilsyn fra nationale myndigheder.

Formålet med NIS2 er at styrke cybersikkerheden i EU-landene ved at øge modstandsdygtigheden i samfundskritiske sektorer, øge beredskabet mod cyberangreb, skabe ensartede sikkerhedskrav på tværs af medlemslandene, samt forbedre samarbejdet mellem medlemslandenes myndigheder.

Styrelsen for Samfundssikkerhed har udgivet en række vejledninger til NIS 2-loven med henblik på at understøtte myndigheder og virksomheders arbejde med implementeringen af de nye og skærpede krav til cybersikkerheden.

Desuden har Styrelsen for Samfundssikkerhed lanceret værktøjet ”NIS 2-tjek”, som guider brugere igennem en vurdering af, om virksomheden er omfattet af NIS2-loven: [NIS 2-tjek](#)

Folketinget har – parallelt med NIS2-loven – også vedtaget 2 andre love, som relaterer sig til NIS2, men som ikke behandles yderligere i denne artikel:



For det første *CER-loven* (*CER står for Critical Entities Resilience*) der stiller krav til modstandsdygtighed for virksomheder indenfor kritisk infrastruktur, som implementerer CER-direktivet og stiller krav til fysisk sikkerhed hos kritiske enheder: *Lov om kritiske enheders modstandsdygtighed (CER-loven)*.

For det andet *Lov om sikkerhed og beredskab i telesektoren*, som implementerer NIS2-direktivet for telesektoren: *Lov om sikkerhed og beredskab i telesektoren*.

NIS2 OMFATTEDE ENHEDER

NIS2 opdeler enheder i 2 hovedkategorier: *Væsentlige enheder* og *vigtige enheder* afhængigt af deres samfundskritiske betydning. Omfang af sikkerhedskrav, tilsyn og sanktioner kan variere mellem væsentlige og vigtige enheder.

Styrelsen for Samfundssikkerhed har udarbejdet en vejledning om hvilke enheder, der er omfattet af NIS2: *Vejledning om anvendelsesområdet*

VÆSENTLIGE ENHEDER

En enhed anses for væsentlig hvis den beskæftiger 250 personer eller derover,

samt at enheden har en årlig omsætning på over 50 mio. euro og en årlig samlet balance på over 43 mio. euro.

Væsentlige enheder omfatter:

1. Energi – El, olie, gas, fjernvarme
2. Transport – Luftfart, jernbane, søfart, vejtransport
3. Finans – Banksektoren, kreditinstitutter
4. Sundhed – Hospitaler, private og offentlige sundhedsudbydere, biotekvirksomheder
5. Drikkevand og spildevand
6. Digital infrastruktur, internetknodepunkter (IXP), DNS-tjenester, topdomæneoperatører, cloud-, hosting- og datacentre
7. Offentlig administration – Stat og regioner (i visse tilfælde også kommuner)
8. Rumfart – Operatører af satellittjenester og -infrastruktur

Kommuner og regioner anses som væsentlige enheder, såfremt de med et kommercielt formål udfører opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kom-

munikationstjenester og opfylder mindst en af følgende betingelser: Enheden beskæftiger 50 personer eller derover, samt at enheden har en årlig omsætning på over 10 mio. euro og en årlig samlet balance på over 10 mio. euro.

VIGTIGE ENHEDER

En enhed anses for vigtig, hvis enheden beskæftiger 50 personer eller derover, samt at enheden har en årlig omsætning på over 10 mio. euro og en årlig samlet balance på over 10 mio. euro.

Vigtige enheder omfatter:

1. Post- og kurertjenester
2. Affaldshåndtering
3. Fødevarerproduktion – Produktion, forarbejdning og distribution af fødevarer
4. Fremstilling af kritiske produkter – Medicin og medicinsk udstyr, computer- og elektronikudstyr, elektrisk udstyr, maskiner og køretøjer
5. Digitalt indhold og tjenester – Online markedspladser, søgetjenester, sociale medier
6. Forskning – Særligt forskningsinstitutioner med kritisk viden eller infrastruktur





» REGISTRERING

NIS2-omfattede virksomheder skal gennemføre registrering inden d. 1/10-25.

Det er virksomhedernes eget ansvar at vurdere, om de falder ind under NIS2's kriterier. Manglende eller fejlagtig registrering kan medføre bøder, tilsyn og påbud, samt øget opmærksomhed fra myndighederne.

Registreringen foregår digitalt via [VIRK.dk](#) ved hjælp af en registreringsblanket, som virksomhederne skal udfylde, omfattende en række basisoplysninger – [Introduktion – Registrering af virksomhed efter NIS2 | Virk](#)

Foruden virksomheder kan også kommuner være omfattet af NIS2-loven: [Vejledning til kommuner om NIS 2-loven](#)

NIS2-LOVENS KRAVOMRÅDER

Sikkerhedsforanstaltninger

Væsentlige og vigtige enheder skal træffe 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.

Foranstaltningerne kan ses som udtryk for en god praksis for styring af cyber- og informationssikkerhedsrisici.

Styrelsen for samfundssikkerhed har udarbejdet en vejledning der skal hjælpe offentlige og private enheder med at implementere cybersikkerhedsforanstaltninger, som NIS2-loven kræver: [Vejledning til implementering af NIS 2-lovens cybersikkerhedsforanstaltninger](#)

Foranstaltningerne skal som minimum omfatte følgende:

1. Politikker for risikoanalyse og informationssystemsikkerhed
2. Håndtering af hændelser
3. Driftskontinuitet, backupstyring og reetablering efter en katastrofe og krisestyring
4. Forsyningskædesikkerhed
5. Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer
6. Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici
7. Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse
8. Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering

9. Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
10. Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant

Hændelsesunderretning

I henhold til NIS2-loven forestår der en opgave for væsentlige og vigtige enheder med at foretage hændelsesunderretning. Det gælder både væsentlige hændelser, der er omfattet af underretningspligten og om frivillige underretninger.

En hændelse skal forstås som en begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare.

Styrelsen for samfundssikkerhed har udarbejdet en vejledning, der skal hjælpe offentlige og private enheder til at efterleve deres forpligtelse til at underrette om væsentlige hændelser: [Vejledning til NIS 2-loven: Hændelsesunderretning](#)



VEJLEDNINGENS
OVERORDNEDE
BUDSKAB ER AT
CYBERSIKKERHED ER
LEDELSENS ANSVAR



Obligatoriske hændelsesunderretninger vedrører de net- og informationssystemer, som kan påvirke enhedens evne til at levere de ydelser, som gør, at enheden er omfattet af NIS 2-loven.

I henhold til NIS2-loven skal alle EU-lande etablere et nationalt CSIRT (*Computer Security Incident Response Team*). CSIRT'en varetages i Danmark af CFCS (Center for Cybersikkerhed), som er en del af Styrelsen for Samfundssikkerhed. CFCS hjælper danske myndigheder og virksomheder med at forebygge, imødegå og beskytte sig mod cyberangreb.

Væsentlige og vigtige enheder skal underrette myndigheder om væsentlige hændelser. Alle underretninger skal indgives gennem via Virk.dk. Når man underretter via Virk.dk, bliver underretningen automatisk sendt til relevante myndigheder. Der er desuden mulighed for at krydse af om Datatilsynet skal underrettes om brud på persondatasikkerheden i samme underretning.

Ledelsens rolle og opgaver

Styrelsen for samfundssikkerhed har udarbejdet en vejledning, som hjælper ledere i private og offentlige enheder med at opfylde kravene i NIS 2-loven: [Vejledning](#)

til NIS 2-loven: Ledelsens rolle og opgaver

Vejledningens overordnede budskab er at *cybersikkerhed er ledelsens ansvar*. For NIS2-omfattede virksomheder omfatter ledelsesansvaret en række punkter, herunder følgende:

- Ledelsen skal tage ejerskab for cybersikkerheden i deres organisation, herunder opgaver og ansvar ift. styring af cybersikkerhedsrisici, og krav til uddannelse.
- Ledelsen har ansvar for styringen af cybersikkerhedsrisici i deres virksomhed, organisation eller myndighed. Manglende opfyldelse af NIS2-lovens krav kan medføre personlige sanktioner for de ansvarlige ledere.
- Ledelsen skal godkende cybersikkerhedsforanstaltninger, herunder tekniske, operationelle og organisatoriske sikkerhedstiltag.
- Ledelsen skal føre tilsyn med, at de godkendte cybersikkerhedsforanstaltninger gennemføres og sikre, at foranstaltningerne har den fornødne effekt ift. de identificerede risici.
- Ledelsen skal deltage i relevante kurser om styring af cybersikkerhedsrisici.

Uddannelsesaktiviteterne skal kunne dokumenteres f.eks. i form af kursusbevis eller bekræftelse på deltagelse i kursus.

- Ledelsen spiller en vigtig rolle for medarbejdernes kompetencer og adfærd. Ledelsen skal tilskynde til, at ansatte tilbydes kurser, svarende til dem, ledelsen selv gennemfører.

IMPLEMENTERING AF NIS2

Det overordnede mål for virksomheden er at sikre en solid planlægning med henblik på effektiv implementering af kravgrundlaget i NIS2.



RELEVANTE LINKS

Alle de fremhævede links i artiklen finder du på vores hjemmeside, <https://dfk.dk/faglig-viden/> eller ved at scanne QR-koden her:





Som udgangspunkt kan virksomheder, der er omfattet af NIS2-loven, med fordel overveje at starte med en *gap-analyse*, som viser aktuel status for opfyldelse af NIS2-lovens kravpunkter. Med afsæt i gap-analysen kan virksomheden udarbejde en samlet plan for de implementeringsudfordringer, der forestår, uanset om målet er et D-mærke, en ISO 27001-certificering eller anden dokumentation for overholdelse af kravgrundlaget.

ISO/IEC 27001 understøtter implementeringen af NIS2-direktivet ved at give en internationalt anerkendt standard for opbygning og vedligeholdelse af et informationssikkerhedsledelsessystem (ISMS). Det hjælper organisationer med at opfylde mange af de centrale krav i NIS2 – både teknisk, organisatorisk og ledelsesmæssigt.

ISO 27001 er et dokumenteret værktøj til at implementere NIS2 på en struktureret, målbar og internationalt anerkendt måde. Mange organisationer bruger ISO-standarder som grundlag for deres compliance-arbejde, da ISO også kan understøtte virksomhed på andre områder.

Find oplysninger om ISO/IEC 27001 og NIS2: [NIS2-direktivet – skærpede krav](#)

D-mærket understøtter implementeringen af NIS2-loven ved at give virksomheder og organisationer et konkret og anerkendt rammeværk for at arbejde systematisk med informationssikkerhed og ansvarlig dataanvendelse: D-mærket fungerer som en praktisk ramme for danske organisationer, der vil styrke deres cybersikkerhed og dokumentere efterlevelse af NIS2 i dansk kontekst. Især for mange SMV'ere, som måske ikke har egne compliance-afdelinger, kan D-mærket være en attraktiv løsning.

Find oplysninger om D-mærket og NIS2: [Bliv klar til NIS2 med D-mærket](#)

At gennemføre NIS2-implementering kan anbefales tilrettelagt som et projekt med alt hvad det indebærer af stillingtagen til ledelsesinvolvering, projektorganisering, medarbejderinddragelse og beredskabshåndtering.

Ledelsesinvolvering stiller krav til ledelsen om at indtænke NIS2 i virksomhedens strategi og mål for informations- og cybersikkerhed, samt løbende opfølgning på status for arbejdet. Desuden skal ledelsen afsætte de fornødne ressourcer til at gennemføre projektaktiviteter og efterfølgende driftsaktiviteter, der skal sikre at virksomheden lever op til NIS2-kravene i praksis.

Projektorganisering indebærer at NIS2-implementeringen iværksættes som et projekt med alt hvad det indebærer i forhold til udpegnings af en projektgruppe, udarbejdelse af planer og gennemførelse af opgaver inden for fastlagte tidsfrister, rettidig håndtering af risici som kan forstyrre og forsinke processen, udvikling af kompetencer for relevante medarbejdere etc.

Medarbejderinddragelse er et vigtigt omdrejningspunkt for informations- og cybersikkerhed, og dermed for efterlevelse af NIS2-kravene. Det er vigtigt at styrke sikkerheden ved at gennemføre rutiner og kontroller. Erfaringsmæssigt er det tilsvarende vigtigt at styrke sikkerheden via fokus på medarbejdernes sikkerhedsmæssige adfærd som omdrejningspunkt til at leve op til NIS2-kravene.

Beredskabshåndtering er et centralt fokusområde for virksomheder, der rammes af informations- og cybersikkerhedsrisici.

Spørgsmålet er hvordan en ramt virksomhed kan genskabe en situation med normal drift eller nøddrift. Det kan forekomme uoverskueligt at gennemføre en sådan planlægning, men det er en nødvendig forudsætning for virksomhedens videre overlevelse.

Samlet set handler implementering af NIS2 om at skabe en helt ny kultur i virksomheden for håndtering af informations- og cybersikkerhed. Denne kultur omfatter både ledelsesmæssige, organisatoriske, adfærdsmæssige, fysiske og teknologiske elementer. ●



MIKKEL
LUNDSTRØM

virksomhedskonsulent i Unik Consult.
Læs mere på www.unikconsult.dk

Som konsulent løser Mikkel auditopgaver for MONTHE Certificering ApS. med særlig fokus på ISO 27001 certificering Læs mere på www.monthe-c.dk

MONTHE Certificering har kunder inden for informationssikkerhed i bl.a. software-, produktions-, entreprenør- og advokatbranchen. Virksomheden samarbejder med C1 Certification AB, som er akkrediteret af Swedac til at udstede certifikater [læs mere på c1cert.se].

Ved behov for ekstra personressourcer til den enkelte auditopgave inddrages auditorer fra C1.