



NIS 2 referencekatalog for topledelsen

Af

[Cyber Security Innovation ApS](#)

NIS 2 referencekatalog for topledelsen

er udgivet af Cyber Security Innovation ApS

© 2025 Cyber Security Innovation ApS, <https://cybersecurityinnovation.dk/>,
Lejrvej 17, 3500, Værløse, Danmark

Alle rettigheder forbeholdes

Indhold

Introduktion til referencekataloget	3
Referencekatalogets opdeling	4
Hvad er NIS 2-loven?	4
Anvendelsesområdet	5
Introduktion.....	5
Hvad er en enhed?	5
Hvilke sektorer er omfattet?	5
Hvordan beregner I en enheds størrelse?	6
Enheder af særlig betydning uanset størrelse.....	6
Digitale enheder og jurisdiktion	6
Kort om registreringspligt	6
NIS 2 tjek 7	
Ledelsens rolle og opgaver	7
Introduktion.....	7
Hvordan er ledelsesbegrebet defineret i NIS 2-loven?	7
Hvilke krav er der til ledelsens styring af cybersikkerhedsrisici?	7
Hvilke krav stiller NIS 2-loven til ledelsens kompetencer?	8
Hvilken rolle spiller ledelsen ift. uddannelse af medarbejdere?	8
Kan ledelsen sanktioneres?	8
Implementering af cybersikkerhedsforanstaltninger	8
Introduktion.....	9
Standarder	9
Politik for risikostyring og informationssystemssikkerhed	9
Håndtering af hændelser	10
Driftskontinuitet.....	10
Forsyningskædesikkerhed	10
Erhvervelse, udvikling og vedligeholdelse	11
Effektivitet af foranstaltninger	11

Cyberhygiejne og cybersikkerhedsuddannelse	11
Kryptografi	12
Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver	12
Multifaktorautentificering og nødkommunikationssystemer	12
Hændelsesunderretning.....	12
Introduktion.....	13
Hvilke hændelser skal der underrettes om?.....	13
Hvis vedligeholdelse af net- og informationssystemer er outsourcet.....	14
Hvordan skal du underrette?	14
Obligatoriske underretninger.....	14
Særligt for tillidstjenesteudbydere	14
Frivillig underretning.....	15

Introduktion til referencekataloget

Vi har samlet de mest relevante referencer for dig der sidder i bestyrelsen eller direktion og ønsker at vide mere om hvordan du og din organisation skal forholde jer til NIS 2-loven.

Kataloget er delt fire hovedkapitler, på samme måde som “[NIS 2 e-bogen for topledelsen](#)”, dette e-læringskursus “[NIS 2 e-læring for topledelsen](#)” og [NIS 2-vejledningerne fra Styrelsen for Samfundssikkerhed](#).

Vi har udarbejdet dette materiale fordi, NIS 2-loven beskriver, at du som en del af bestyrelsen og direktion har et fået nyt ansvar, hvor du skal tage relevante kurser og tilegne dig tilstrækkelig viden inden for cybersikkerhed.

Dette referencekatalog indeholder kun information, der er relevant for dig i topledelsen og ikke andet.

Referencekatalogets opdeling

De fire kapitler belyser NIS 2-loven fra forskellige vinkler, som alle er relevante for dig og dine kollegaer i ledelsesorganet.

1. ANVENDELSESOMRÅDET

Hvilke enheder er omfattet af NIS 2-loven, samt hvad en enhed er.

2. LEDELSENS ROLLE OG OPGAVER

Hvilke krav er der til ledelsesorganet i følge NIS 2-loven og hvilke opgaver og ansvar medfører det.

3. IMPLEMENTERING AF CYBERSIKKERHEDSFORANSTALTNINGER

Hvordan styre du implementering af de cybersikkerhedsforanstaltninger, der kræves, og hvad er cybersikkerhedsforanstaltninger.

4. HÆNDELSESUNDERRETNING

Hvordan og hvornår skal du underrette myndigheder, når uheldet er ude, og i rammes af en cybersikkerhedshændelse

Hvad er NIS 2-loven?

Det er vigtigt at læse NIS 2-loven og dens grundlag, derfor kan du læse både NIS-2 loven og NIS 2-direktivet, som ligger til grund for den danske NIS 2-lov: [NIS 2-loven](#) og [NIS 2-direktivet](#)

Anvendelsesområdet

Introduktion

Det er vigtigt at kende til grundbegreberne i NIS 2-loven samt om selve loven gælder for din enheds situation, så i dette kapitel får du de vigtigste referencer for at blive afklaret herom.

Hvad er en enhed?

En enhed er kort sagt en organisation med et CVR-nummer. Se [§3, 9\) i NIS 2-loven](#).

Hvilke sektorer er omfattet?

NIS 2-loven har defineret de sektorer der er omfattet NIS 2-loven. De kan findes her i [Bilag 1](#) og [Bilag 2](#).

Der findes sektor specifik lovgivning som har præcedens over NIS 2-loven, hvilket betyder, at hvis I rammer inden for disse sektorer, skal I følge disse love og ikke NIS 2-loven:

Energi: [Lov](#) / [Bekendtgørelse](#)

Tele: [Lov om sikkerhed og beredskab i telesektoren](#)

Finans: [EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV \(EU\) 2022/2555](#)

Hvordan beregner I en enheds størrelse?

Udover at være omfattet af NIS 2-lovens Bilag 1 og 2, skal en enhed i udgangspunktet være mellemstor eller stor, før den er omfattet af NIS 2-loven.

For at forstå om du er dette, kan du anvende [EU-kommissionens definitioner](#) eller denne [brugervejledning til definitioner af små og mellemstore virksomheder \(SMV'er\)](#).

Enheder af særlig betydning uanset størrelse

Enheder kan være omfattet af NIS 2-loven uanset deres størrelse i visse tilfælde. Den fulde liste findes i vejledningen under [Afsnit 4 "Enheder af særlig betydning uanset størrelse"](#).

Se også de officielle EU-Forordningskrav på [Gennemførelsesforordning - EU - 2024/2690 - EN - EUR-Lex](#).

Digitale enheder og jurisdiktion

Der gælder særlige jurisdiktionsregler for en række digitale enheder omfattet af NIS 2-loven, hvilket du skal være opmærksom på. Den fulde liste findes i vejledningen under [Afsnit 1 "Hvad er en enhed?"](#).

Kort om registreringspligt

Hvis man er omfattet af NIS 2-loven, skal man registrere sig på på [Virksomheden.dk](#). Portalen blev tilgængelig samtidig med lovens ikrafttræden.

NIS 2 tjek

Vi anbefaler at bruge følgende [NIS 2-tjek fra sikkerdigital.dk](#), for at få en ide om enheden er underlagt NIS 2-loven. Husk at dobbelttjekke med en specialist.

Ledelsens rolle og opgaver

Introduktion

NIS 2-loven har følgende områder du som leder skal være særligt opmærksom på, fordi cybersikkerhed er topledelsens ansvar. Derfor skal du som leder tage ejerskab for styring af cybersikkerheden i din organisation.

NIS 2-loven stiller klare krav til medlemmerne af ledelsesorganer, og dem gennemgår vi i dette kapitel, herunder også krav om uddannelse.

Hvordan er ledelsesbegrebet defineret i NIS 2-loven?

Se her hvordan [*NIS 2-loven § 3. 20\) definerer ledelsesorganet.*](#)

Private virksomheder/organisationer

Se ang. ledelsesorganet for virksomheder omfattet af [*selskabsloven.*](#)

Se ang. ledelsesorganet for virksomheder omfattet af [*LEV-loven.*](#)

Hvilke krav er der til ledelsens styring af cybersikkerhedsrisici?

For at forstå kravene bedre, se [*NIS 2-loven § 7, stk. 1*](#) ang. nærværende emne.

Hvilke krav stiller NIS 2-loven til ledelsens kompetencer?

Fordi NIS 2-loven stiller krav om, at medlemmerne af et ledelsesorgan skal deltage i relevante kurser om styring af cybersikkerhedsrisici: [*NIS 2-loven §7, stk 2.*](#)

Uddannelsesaktiviteterne skal kunne dokumenteres f.eks. i form af kursusbevis, hvilket du får ved gennemførelse af kurset: [*NIS 2 e-læringskursus for topledelsen.*](#)

Hvilken rolle spiller ledelsen ift. uddannelse af medarbejdere?

Medarbejdernees kompetencer og viden inden for cybersikkerhed er dit ansvar som ledelsen.

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.

Kan ledelsen sanktioneres?

Ifølge NIS 2-loven §23, stk. 1, og 2) skal du som ledelse være særligt opmærksomme på, at du i særlige tilfælde kan gøres personligt ansvarlige for efterlevelsen af NIS 2-loven i deres organisation.

Implementering af cybersikkerhedsforanstaltninger

Introduktion

I dette kapitel er fokus sat på referencer der hjælper dig med implementering af cybersikkerhedsforanstaltninger. Særligt hvor de vil hjælpe dig i ledelsesorganet med at styre implementering af de foranstaltninger der håndterer cybersikkerhedsrisici.

[Disse bestyrelsesvejledninger- og tjeklister](#) er direkte relevante for jer i bestyrelsen og de efterfølgende vejledninger i dette kapitel kan bruges som inspiration til at implementere de mest relevante cybersikkerhedsforanstaltninger.

Samt denne [NIS 2-vejledning fra Styrelsen fra Samfundssikkerhed](#), der indeholder relevant viden indenfor hvert område i dette kapitel. Du kan med fordel følge den parallelt.

For sektorspecifik vejledning skal man kontakte den sektoransvarlige myndighed: [Find oversigten her](#).

Standarder

For at sikre en ensartet gennemførelse af NIS 2-direktivet *tilskyndes medlemsstaterne til at basere sig på europæiske og internationale standarder og tekniske specifikationer*, der er relevante for sikkerheden i net- og informationssystemer.

I Styrelsen for Samfundssikkerheds vejledning “Implementering af cybersikkerhedsforanstaltninger” finder du en liste over relevante standarder (samt i vores e-bog), som kan hjælpe dig godt på vej: [Implementering af cybersikkerhedsforanstaltninger](#).

Politik for risikostyring og informationssystemssikkerhed

For mere viden om den relevante paragraf i loven ift. politik for risikostyring og informationssystemssikkerhed, se her: [Ifølge NIS 2-loven § 6, stk. 1, nr. 1.](#) og [Lovbemærkninger](#).

Politik for informationssystemssikkerhed

Du kan få vejledning og hjælp til at nedskrive en IT-sikkerhedspolitik ved at bruge [denne vejledning og skabelon fra sikkerdigital.dk](#).

Politik for risikostyring

Du kan få vejledning og hjælp til at lave en IT-risikovurdering ved at bruge [denne vejledning og skabelon fra sikkerdigital.dk](#).

Håndtering af hændelser

For mere viden om den relevante paragraf i loven ift. håndtering af hændelser, se her: [Ifølge NIS 2-loven §6, stk 1, nr.2](#) og [Lovbemærkning](#).

Driftskontinuitet

For mere viden om den relevante paragraf i loven ift. driftskontinuitet, se her: [Ifølge NIS 2-loven §6, stk 1, nr.3](#) og [Lovbemærkninger](#).

Du kan få vejledning og hjælp til at få lavet en beredskabsplan ved at bruge [denne vejledning og skabelon fra sikkerdigital.dk](#).

Forsyningskædesikkerhed

For mere viden om den relevante paragraf i loven ift. forsyningskædesikkerhed, se her: [Ifølge NIS 2-loven § 6, stk. 1, nr. 4](#) og [Lovbemærkninger](#).

Du kan få vejledning og hjælp til at lave en vurdering af din leverandør ved at bruge [denne vejledning og spørgeskema fra sikkerdigital.dk](#).

Erhvervelse, udvikling og vedligeholdelse

For mere viden om den relevante paragraf i loven ift. erhvervelse, udvikling og vedligeholdelse, se her: [Ifølge NIS 2-loven §6, stk. 1, nr. 5](#) og [Lovbemærkninger](#).

Effektivitet af foranstaltninger

For mere viden om den relevante paragraf i loven ift. effektivitet af foranstaltninger, se her: [Ifølge NIS 2-loven §6, stk. 1, nr. 6](#) og [Lovbemærkninger](#).

Cyberhygiejne og cybersikkerhedsuddannelse

For mere viden om den relevante paragraf i loven ift. cyberhygiejne og cybersikkerhedsuddannelse, se her: [Ifølge NIS 2-loven §6, stk. 1, nr. 7](#) og [Lovbemærkninger](#).

Du kan få vejledning og hjælp til at styrke medarbejdernes IT-sikkerhedsadfærd ved at bruge [dette materiale fra sikkerdigital.dk](#)

Kryptografi

For mere viden om den relevante paragraf i loven ift. kryptografi, se her: [Ifølge NIS 2-loven §6, stk. 1, nr. 8](#) og [Lovbemærkninger](#).

Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

For mere viden om den relevante paragraf i loven ift. personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver, se her: [Ifølge NIS 2-loven §6, stk. 1, nr. 9](#) og [Lovbemærkninger](#).

Multifaktorautentificering og nødkommunikationssystemer

For mere viden om den relevante paragraf i loven ift. multifaktorautentificering og nødkommunikationssystemer, se her: [Ifølge NIS 2-loven § 6, stk. 1, nr. 10](#) og [Lovbemærkninger](#).

Hændelsesunderretning

Introduktion

Nu er vi nået til fjerde og sidste kapitel i referencekataloget. I dette kapitel finder du referencer til håndtering af hændelsesunderretning, der hjælper dig i ledelsesorganet med hændeshåndtering i forhold til NIS 2-loven. Så du ved hvad du skal gøre, hvis uheldet er ude.

Hvilke hændelser skal der underrettes om?

Enheder skal underrette om hændelser, der ud fra en indledende vurdering har påvirket eller er i stand til at påvirke enhedens levering af ydelser. Derudover skal påvirkningen af hændelsen være betydelig, jf. [§ 12, stk. 2](#).

Vi anbefaler, at du ser på sektorer der er omfattet igen (ligesom i kapitel 1), dvs. [Bilag 1](#) og [Bilag 2](#), for at skabe et hurtigt overblik over de hændelser, der skal underrettes.

Alvorlig driftsforstyrrelse af en af de leverede tjenester

Se nærmere her: [Lovbemærkninger til §12.](#)

Økonomiske tab for den pågældende enhed

Se nærmere her: [Lovbemærkninger til §12.](#)

Betydelig materiel, fysisk eller ikke-fysisk skade på andre fysiske eller juridiske personer

Se nærmere her: [Lovbemærkninger til §12.](#)

Hvis vedligeholdelse af net- og informationssystemer er outsourcet

Hvis enheden køber eller outsourcer vedligeholdelse af deres net- og informationssystemer, er det ved tilfælde af en væsentlig hændelse, enhedens ansvar at underrette: 1) [CSIRT](#), og 2) de relevante sektoransvarlige myndigheder

[Lovbemærkninger til §12.](#)

Hvordan skal du underrette?

Væsentlige og vigtige enheder skal underrette de relevante sektoransvarlige myndigheder og CSIRT'en om væsentlige hændelser.

Alle underretninger skal indgives gennem en fælles digital indgang: <https://virk.dk>.

Obligatoriske underretninger

For mere viden om den relevante paragraf i loven ift. obligatoriske underretninger, se her: [Ifølge NIS 2-loven §12, stk. 1.](#)

Særligt for tillidstjenesteudbydere

For mere viden om den relevante paragraf i loven ift. særligt for tillidstjenesteudbydere, se her: [*Ifølge NIS 2-loven §13, stk. 2.*](#)

Frivillig underretning

For mere viden om den relevante paragraf i loven ift. frivillig underretning, se her: [*Ifølge NIS 2-loven §14, stk. 1.*](#)

Offentlige og private enheder har mulighed for at foretage frivillig underretning til CSIRT'en vedrørende hændelser, nærvædhændelser og cybertrusler, uanset om de er omfattet af NIS 2-loven. Dette kan gøres gennem [*Virk.dk*](#), hvor der er en formular til dette.