



# **NIS 2 e-bogen for topledelsen**

Af

[Cyber Security Innovation ApS](#)

*NIS 2 e-bogen 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

<b>Introduktion til e-bogen .....</b>	<b>3</b>
Udbytte og materiale .....	4
Hvad er NIS 2-loven? .....	5
E-bogens opdeling.....	6
<b>Anvendelsesområdet.....</b>	<b>6</b>
Hvad er en enhed? .....	7
<i>Hvor stor en del af enheden er omfattet?.....</i>	<i>8</i>
<i>Jurisdiktion.....</i>	<i>8</i>
Hvilke sektorer er omfattet? .....	8
<i>Hvad er væsentlige og vigtige enheder?.....</i>	<i>9</i>
Hvordan beregner I en enheds størrelse? .....	10
<i>Partnervirksomheder og tilknyttede virksomheder .....</i>	<i>10</i>
Enheder af særlig betydning uanset størrelse.....	10
Digitale enheder og jurisdiktion .....	11
Kort om registreringspligt .....	11
Kort om leverandører til enheder omfattet af NIS 2-loven.....	12
NIS 2 tjek.....	13
<b>Ledelsens rolle og opgaver.....</b>	<b>13</b>
Introduktion.....	14
Hvordan er ledelsesbegrebet defineret i NIS 2-loven? .....	15
<i>Private virksomheder/organisationer.....</i>	<i>15</i>
Kan ledelsen uddelegere sin opgaver? .....	16
Hvilke krav er der til ledelsens styring af cybersikkerhedsrisici? .....	16
Hvordan skal ledelsen føre tilsyn med cybersikkerheden? .....	17
Hvilke krav stiller NIS 2-loven til ledelsens kompetencer? .....	17
Hvilken rolle spiller ledelsen ift. uddannelse af medarbejdere? .....	18
Kan ledelsen sanktioneres? .....	19
<b>Implementering af cybersikkerhedsforanstaltninger .....</b>	<b>20</b>

Introduktion.....	21
Krav og anbefalinger .....	22
Standarder.....	23
Politik for risikostyring og informationssystemssikkerhed.....	24
<i>Politik for informationssystemssikkerhed</i> .....	25
<i>Politik for risikostyring</i> .....	26
Håndtering af hændelser .....	26
<i>Håndtering af hændelser</i> .....	27
<i>Logning og monitorering</i> .....	27
Driftskontinuitet.....	29
<i>Driftskontinuitet</i> .....	29
<i>Backup</i> .....	30
<i>Redundans</i> .....	30
<i>Krisestyring</i> .....	30
Forsyningskædesikkerhed .....	31
Erhvervelse, udvikling og vedligeholdelse .....	33
<i>Erhvervelse, udvikling og vedligeholdelse</i> .....	33
<i>Håndtering af sårbarheder</i> .....	34
Effektivitet af foranstaltninger .....	34
<i>Vurdering af effektiviteten af de implementerede foranstaltninger</i> .....	35
<i>Tekniske tests</i> .....	35
Cyberhygiejne og cybersikkerhedsuddannelse .....	36
<i>Cyberhygiejnepraksisser</i> .....	37
<i>Cybersikkerhedsuddannelse</i> .....	38
Kryptografi .....	38
Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver .....	40
<i>Personalesikkerhed</i> .....	40
<i>Adgangskontrol</i> .....	41
<i>Forvaltning af aktiver</i> .....	41

Multifaktorautentificering og nødkommunikationssystemer .....	42
<i>Multifaktorautentificering</i> .....	43
<i>Nødkommunikationssystemer</i> .....	43
<b>Hændelsesunderretning</b> .....	<b>44</b>
Introduktion.....	45
Hvilke hændelser skal der underrettes om?.....	46
<i>Alvorlig driftsforstyrrelse af en af de leverede tjenester</i> .....	47
<i>Økonomiske tab for den pågældende enhed</i> .....	47
<i>Betydelig materiel, fysisk eller ikke-fysisk skade på andre fysiske eller juridiske personer</i> .....	48
Hvis vedligeholdelse af net- og informationssystemer er outsourcet.....	49
Hvordan skal du underrette? .....	50
Obligatoriske underretninger.....	51
Særligt for tillidstjenesteudbydere .....	52
Frivillig underretning .....	53
<b>Ordliste til e-bogen</b> .....	<b>53</b>

# Introduktion til e-bogen

Velkommen til ”NIS 2 e-bogen for topledelsen”.

E-bogen her er skrevet ud fra [NIS 2-vejledningerne fra Styrelsen for Samfundssikkerhed](#), men med specifikt fokus på topledelsen og simplificering, så du som læser får lige præcis det, du har brug for at vide og ikke mere.

Vi har kun udvalgt de relevante emner til dig, som er en del af direktionen eller bestyrelsen. Ordet ”leder” bruges igennem denne e-bog for at beskrive din rolle.

Formålet med denne e-bog er at hjælpe dig med at sikre din organisations efterlevelse af den danske NIS 2-lovs krav, ved at give dig den nødvendige viden for, at du kan lede ansvarligt.

Vi har tilføjet en række links, der viser dig videre til relevant information. Samt udarbejdet en **ordliste** med definitioner af ord og begreber, der hjælper dig med at forstå de tekniske og juridiske termer.

E-bogen kan læses som en selvstændig e-bog eller bruges som et opslagsværk, men er også udarbejdet som understøttende materiale til vores kursus: [NIS 2 e-læring for topledelsen](#).

Det er vigtigt at understrege, NIS 2-loven kræver, at du som leder har taget relevante kurser og har tilegnet dig tilstrækkelig viden inden for cybersikkerhed.

## Udbytte og materiale

E-bogen giver dig følgende udbytte.

- Indsigt i om din virksomhed er underlagt NIS 2-loven
- Kendskab til dit ansvar som en del af ledelsesorganet
- Forståelse af hvilke foranstaltninger du skal sikre, bliver implementeret
- Viden om hvad du skal gøre, hvis uheldet er ude

Det supplerende [NIS 2 e-læring for topledelsen-kursus](#) giver dig følgende:

- Et kursusbevis, der dokumenterer, du har gennemført den lovpligtige træning
- Viden til at gennemgå multiple choice spørgsmål og svar
- Hjælpeværktøjer og dokumentation, som du kan bruge i din hverdag

## Hvad er NIS 2-loven?

Inden vi går i gang, så lad os dykke dybere ned i [NIS 2-loven](#), da det er grundlaget for e-bogen.

[NIS 2-direktivet](#), som ligger til grund for NIS 2-loven er en videreudvikling af NIS-direktivet (et tidligere EU-direktiv ved navn “Direktiv (EU) 2016/1148”), og som fokuserede på at forøge Unionens cyberrobusthed og omhandlede netværks- og informationssystemer.

NIS 2-direktivet strømliner Unionens cybersikkerhed og dermed forsøger EU at undgå fragmentering blandt medlemslandenes cybersikkerhedsniveau.

NIS 2-loven er med andre ord den danske (nationale) implementering af det europæiske direktiv.

## E-bogens opdeling

Vi har delt e-bogen op i fire kapitler, der belyser NIS 2-loven fra forskellige vinkler, som alle er relevante for dig og dine kollegaer i ledelsesorganet.

### **ANVENDELSESOMRÅDET**

*Hvilke enheder er omfattet af NIS 2-loven, vigtige opmærksomhedspunkter, samt hvad en enhed er*

### **LEDELSENS ROLLE OG OPGAVER**

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

### **IMPLEMENTERING AF CYBERSIKKERHEDSFORANSTALTNINGER**

*Hvordan du som ledelsesorgan kan styre implementering af de cybersikkerhedsforanstaltninger, der kræves, og hvad cybersikkerhedsforanstaltningerne er*

### **HÆNDELSESUNDERRETNING**

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

# Anvendelsesområdet

1. Hvad er en enhed?
2. Hvilke sektorer er omfattet?
3. Hvordan beregner I en enheds størrelse?
4. Enheder af særlig betydning uanset størrelse
5. Digitale enheder og jurisdiktion
6. Kort om registreringspligt
7. Kort om leverandører til enheder omfattet af NIS 2-loven
8. NIS 2 tjek

## Hvad er en enhed?

En enhed er i følge NIS 2-loven en virksomhed, forening, organisation eller offentlig myndighed med videre (juridisk person), som er tildelt et CVR-nummer.

Et selskab med et underliggende datterselskab udgør to separate enheder, forudsat at de har fået tildelt hver deres CVR-nummer.

Enheden er derfor den organisation du er ansvarlig for, og som du skal sikre efterlever NIS 2-loven.

## Hvor stor en del af enheden er omfattet?

Hvis en enhed er omfattet af NIS 2-loven, vil hele enheden høre under loven. Det betyder, at enheden skal forholde sig til alle de net- og informationssystemer, som enheden anvender til sine operationer eller til at levere sine tjenester.

## Jurisdiktion

For at være omfattet af den danske NIS 2-lov, skal I som enhed være inden for dansk jurisdiktion. Som udgangspunkt vil enheder, der er etableret i Danmark med et dansk CVR-nummer, være omfattet af NIS 2-loven.

I skal være opmærksomme på, at hvis en enhed opererer i andre EU-lande, er det enhedens eget ansvar at undersøge, om denne enhed også er omfattet af de lokale landes implementering af NIS 2-direktivet.

## Hvilke sektorer er omfattet?

For at være omfattet af NIS 2-loven skal I være omfattet af de sektorer, der er beskrevet i NIS 2-loven [Bilag 1](#) og [Bilag 2](#).

Bilag 1 viser de "Særligt kritiske sektorer" såsom elektricitet, luft, sundhed og rummet

Bilag 2 viser de "Andre kritiske sektorer" såsom produktion og distribution af kemikalier eller håndtering af post.

NIS 2-loven lister omfattede sektorer i form af aktiviteter og tjenesteydelser. Og som enhed skal du derfor analysere jeres aktiviteter og tjenesteydelser for at kunne vurdere, om I er omfattet af loven.

Der er nogle sektorer, der er underlagt yderligere love end NIS 2-lovgivningen såsom energi og drikkevand. Disse har deres egne specifikke love, samtidig med at de er underlagt NIS 2-loven. Disse sektorer har deres egne love og indgår ikke i denne e-bog.

Men inden vi forlader dem, får du en kort introduktion til dem. På denne måde kan du bedre forstå, hvad det handler om. Formålet med sektor-specifik lovgivning er følgende:

1. **Differentieret risikoprofil** – Hver sektor har unikke trusselsbilleder (eksempelvis sabotage mod energinet vs. DDoS mod tele) og kræver derfor tilpassede regler. [\[shoosmiths.com\]](#), [\[enisa.europa.eu\]](#)
2. **Beskytte kritisk infrastruktur** – Sektorer som tele, energi og finans understøtter essentielle samfunksfunktioner, og deres kompromittering kan have vidtrækkende konsekvenser for national sikkerhed og offentlig orden. [\[berrec.europa.eu\]](#), [\[enisa.europa.eu\]](#)
3. **Styrket håndhævelse og ansvarlighed** – Med sektor-specifik lovgivning sikres klare retningslinjer og sanktionsmuligheder, herunder personligt ansvar for ledelsen, hvilket giver håndhævede incitament for compliance. [\[berrec.europa.eu\]](#), [\[eurolawhub.com\]](#)

Opsummering af sektor-specifik implementering af NIS 2 i Danmark:

- **Energi (Lov / Bekendtgørelse), Tele og Finans** har særskilt sektorlovgivning, der implementerer eller supplerer NIS 2-kravene.
- **Alle andre sektorer** følger den generelle NIS 2-lov.
- Kontakt altid din sektoransvarlige myndighed for at få præcis vejledning om gældende lovgivning for netop din sektor.

## Hvad er væsentlige og vigtige enheder?

NIS 2-loven opdeler omfattede enheder i væsentlige og vigtige enheder alt efter deres kritiske betydning og størrelse.

Inddelingen har betydning for, hvilket tilsyn enhederne er underlagt, samt hvilke håndhævelsesforanstaltninger og sanktioner de kan blive pålagt.

- *Væsentlige enheder* er NIS 2-omfattede enheder inden for sektorer af særligt kritisk betydning (lovens Bilag 1), som overskrider tærsklen for mellemstore virksomheder.
- *Vigtige enheder* er derimod omfattede enheder, der ikke opfylder kriterierne for at være væsentlige, men stadig har 50 ansatte eller derover *eller* har en årlig omsætning på over 10 mio. EUR og en årlig samlet balance på over 10 mio. EUR.

I kan som enheder få vejledning om de specifikke kriterier hos jeres sektoransvarlige myndighed.

Derudover kan de sektoransvarlige myndigheder via bekendtgørelser også fastsætte nærmere kriterier for, hvornår enheder i deres sektor vil være omfattet af kriterierne.

## Hvordan beregner I en enheds størrelse?

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

Når I skal beregne jeres enheds størrelse, skal I beregne for hele enheden.

En enhed anses for at være mellemstor, hvis den beskæftiger mindst 50 årsværk eller har en årlig omsætning og en årlig samlet balance på over 10 mio. EUR. Det skal være minimum 2 regnskabsår i træk, for at undgå at en lille virksomhed fejlagtigt glider ind under eller ud af NIS 2-loven.

Du kan anvende [EU-kommissionens definitioner](#) eller denne [brugervejledning til definitioner af små og mellemstore virksomheder \(SMV'er\)](#).

## Partnervirksomheder og tilknyttede virksomheder

Du skal også være opmærksomme på partnerskaber. Fordi hvis din enhed har partnervirksomheder og/eller tilknyttede virksomheder, kan disse også have betydning for, hvad der skal regnes med i enhedens størrelse.

## Enheder af særlig betydning uanset størrelse

Enheder kan være omfattet af NIS 2-loven uanset deres størrelse i visse tilfælde. Det gælder for enheder under f.eks. følgende kategorier

1. Tillidstjenesteudbydere og topdomænenavnsadministratorer samt DNStjenesteudbydere.
2. Offentlige forvaltningsenheder under den centrale forvaltning.
3. Enheder der er identificeret som kritiske enheder i henhold til lov om kritiske enheders modstandsdygtighed (CER-loven).

Den fulde liste findes i vejledningen under [Afsnit 4 "Enheder af særlig betydning uanset størrelse"](#).

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

I kan også få vejledning om de specifikke kriterier hos jeres sektoransvarlige myndighed.

## Digitale enheder og jurisdiktion

Der gælder særlige jurisdiktionsregler for en række digitale enheder omfattet af NIS 2-loven.

De gælder blandt andet for:

- DNS-tjenesteudbydere
- Topdomænenavneadministratorer (TLD)
- Enheder, der leverer domænenavnsregistreringstjenester
- Udbydere af cloudcomputing-tjenester (CC)

Den fulde liste findes i vejledningen under [Afsnit 1 "Hvad er en enhed?"](#).

Hvis sådanne enheder har aktiviteter på tværs af grænser, vil de kun være omfattet af nationale implementeringer af NIS 2-direktivet i ét EU-land ('hovedforretningsreglen').

Men det er et forholdsvis kompliceret spørgsmål alligevel, fordi der kan være undtagelser. For eksempel hvis enheden fungerer gennem mange sektorer.

Derfor anbefaler vi dig at undersøge dette nærmere med f.eks. en advokat, der kan vurdere ud fra jeres enheds konkrete situation.

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

## Kort om registreringspligt

Hvis man er omfattet af NIS 2-loven, skal man registrere sig på på [Virk.dk](#). Portalen vil blive tilgængelig samtidig med lovens ikrafttræden. Derfor er en tilgængelig nu.

Enheder har selv pligt til at vurdere, om de er omfattet af NIS 2-loven, og i givet fald skal registrere sig. I udgangspunktet er det sådan, at enheder skal registrere sig senest to uger efter, at enheden bliver omfattet af loven.

For digitale enheder er det senest tre måneder efter.

## Kort om leverandører til enheder omfattet af NIS 2-loven

Virksomheder, der ikke er omfattet af NIS 2-loven, kan blive mødt med krav til sikkerhedsforanstaltninger, fordi de leverer tjenester eller varer til en enhed, der er omfattet af NIS 2-loven.

Enheder omfattet af NIS 2 skal vurdere de risici, som den modtagne leverance udgør for den NIS 2-omfattede enheds net- og informationssystemer.

Denne vurdering kan medføre, at enheden stiller forholdsmæssige krav til sin leverandør, om at denne implementerer de nødvendige foranstaltninger.

## NIS 2 tjek

Vi anbefaler at bruge følgende [NIS 2-tjek fra sikkerdigital.dk](https://sikkerdigital.dk) for at få en ide om enheden er underlagt NIS 2-loven.

# Ledelsens rolle og opgaver

1. Introduktion
2. Hvordan er ledelsesbegrebet defineret i NIS 2-loven?
3. Kan ledelsen uddelegere sine opgaver?
4. Hvilke krav er der til ledelsens styring af cybersikkerhedsrisici?
5. Hvordan skal ledelsen føre tilsyn med cybersikkerheden?
6. Hvilke krav stiller NIS 2-loven til ledelsens kompetencer?
7. Hvilken rolle spiller ledelsen ift. uddannelse af medarbejdere?
8. Kan ledelsen sanktioneres?

## Introduktion

NIS 2-loven har følgende områder du som leder skal være særligt opmærksom på, fordi cybersikkerhed er topledelsens ansvar. Du skal derfor 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?

Ifølge NIS 2-loven § 3. 20) defineres *ledelsesorganet*:

- a) For virksomheder omfattet af selskabsloven er ledelsesorganet
  - i) bestyrelsen i selskaber, der har en direktion og en bestyrelse,
  - ii) direktionen i selskaber, der alene har en direktion, og
  - iii) direktionen i selskaber, der både har en direktion og et tilsynsråd.
  
- b) For virksomheder omfattet af lov om visse erhvervsdrivende virksomheder er ledelsesorganet
  - i) bestyrelsen i selskaber, der har en direktion og en bestyrelse,
  - ii) direktionen i selskaber, der alene har en direktion, og
  - iii) for de selskaber, der hverken har en bestyrelse eller en direktion, det ledelsesorgan, der har en kompetence, der svarer til den almindelige opfattelse af den kompetence, der tilkommer en bestyrelse eller en direktion.

## Private virksomheder/organisationer

For virksomheder omfattet af [selskabsloven](#) er ledelsesorganet:

- 1) Bestyrelsen i selskaber, der har en direktion og en bestyrelse
- 2) Direktionen i selskaber, der alene har en direktion
- 3) Direktionen i selskaber, der både har en direktion og et tilsynsråd

For virksomheder omfattet af [LEV-loven](#) er ledelsesorganet:

- 1) Bestyrelsen i selskaber, der har en direktion og en bestyrelse
- 2) Direktionen i selskaber, der alene har en direktion
- 3) For de selskaber, der hverken har en bestyrelse eller en direktion, det ledelsesorgan, der har en kompetence, der svarer til den almindelige opfattelse af den kompetence, der tilkommer en bestyrelse eller en direktion.

Den relevante definition afhænger derfor af enhedens selskabsform.

1. *Selskabsloven* finder alene anvendelse for aktie- og anpartsselskaber,
2. mens *LEV-loven* gælder for erhvervsdrivende virksomheder, der ikke er omfattet af selskabsloven f.eks. enkeltmandsvirksomheder, interessentskaber, kommanditselskaber, andelsselskaber og fonde eller foreninger med erhvervsmæssig aktivitet.

Det vil være op til dig/jer i den enkelte enhed at vurdere jeres virksomhedskonstruktion i forhold til selskabsloven eller LEV-loven.

## Kan ledelsen uddelegere sin opgaver?

Ledelsesorganet kan uddelegere sine opgaver, men det vil fortsat være det samlede ledelsesorgan, der kollektivt har ansvaret for, at enheden lever op til forpligtelserne i NIS 2-loven. Dette inkluderer også kravene til ledelsesorganet.

Ledelsesorganet bør derfor overvåge og påse, at evt. udvalg eller driftsansvarlige personer udfører opgaverne.

## Hvilke krav er der til ledelsens styring af cybersikkerhedsrisici?

[Ifølge NIS 2-loven § 7, stk. 1.:](#)

*De foranstaltninger, som en væsentlig eller vigtig enhed træffer på baggrund af § 6, stk. 1 og 2, og regler fastsat i medfør af § 6, stk. 3, skal være godkendt af enhedens ledelsesorgan. Ledelsesorganet fører tilsyn med foranstaltningernes gennemførelse.*

Som ledelsesorganet har du ansvaret for styringen af cybersikkerhedsrisici i jeres virksomhed, organisation eller myndighed.

Ledelsesorganets opgaver i forhold til cybersikkerhed er ikke anderledes end andre risikostyringsområder, hvor ledelsen skal vurdere og føre kontrol med virksomheden, organisationen eller myndighedens risici.

Ledelsesorganet skal godkende cybersikkerhedsforanstaltningerne. Det vil sige de tekniske, operationelle og organisatoriske sikkerhedstiltag, som enheden træffer på baggrund af forpligtelserne i NIS 2-loven.

Ledelsen skal derfor forholde sig til, hvad der udgør et passende sikkerhedsniveau for enhedens net- og informationssystemer set i forhold til enhedens risikoeksponering og den samfundsmæssige betydning af de tjenester og services, som enheden leverer.

Det betyder blandt andet at ledelsen på et overordnet og strategisk niveau skal træffe beslutning om, hvilke foranstaltninger organisationen skal have, og hvornår beskyttelsen er tilstrækkelig.

Mere information om kravene til cybersikkerhedsforanstaltninger i NIS 2-loven, kommer vi til senere i kurset om implementering af cybersikkerhedsforanstaltninger.

## Hvordan skal ledelsen føre tilsyn med cybersikkerheden?

Ledelsesorganet i enheden skal føre tilsyn med, at de godkendte cybersikkerhedsforanstaltninger gennemføres og sikre, at foranstaltningerne har den forventede effekt ift. de identificerede risici.

I som ledelsen skal derfor følge op på og føre kontrol med, at de sikkerhedstiltag, I har iværksat, realiseres og har den ønskede virkning.

Tilsynet kan ske på forskellige måder, eksempelvis gennem:

- *Periodiske ledelsesrapporter*, hvor ledelsesorganet får status på de strategiske målsætninger, handleplaner samt udvalgte nøgletal og kontrolmål for enhedens arbejde med cyber- og informationssikkerhed.
- *Processer for intern revision* kan ledelsesorganet også etablere for at føre tilsyn, som rapporterer til ledelsen eller ved gennemførelse af ekstern revision af NIS 2-kravene, som rapporterer deres resultater til ledelsen.

## Hvilke krav stiller NIS 2-loven til ledelsens kompetencer?

[Ifølge NIS 2-loven §7, stk. 2.:](#)

*De foranstaltninger, som en væsentlig eller vigtig enhed træffer på baggrund af § 6, stk. 1 og 2, og regler fastsat i medfør af § 6, stk. 3, skal være godkendt af enhedens ledelsesorgan. Ledelsesorganet fører tilsyn med foranstaltningernes gennemførelse.*

*Stk. 2. Medlemmerne af en væsentlig eller vigtig enheds ledelsesorgan skal deltage i relevante kurser om styring af cybersikkerhedsrisici og tilskynde til, at tilsvarende kurser tilbydes til enhedens øvrige ansatte.*

NIS 2-loven stiller krav om, at medlemmerne af et ledelsesorgan skal deltage i relevante kurser om styring af cybersikkerhedsrisici.

Der er ikke et specifikt form- og indholds krav til kurserne, men uddannelseskrauet skal ses i lyset af den rolle og de opgaver, ledelsesorganet har for cybersikkerheden i deres virksomhed eller myndighed efter NIS 2-lovens § 7, stk. 1.

Kurserne skal således gøre ledelsen i stand til at vurdere risici og kunne træffe beslutning om og følge op på enhedens cybersikkerhedsforanstaltninger. Fordi ledelsesorganet skal som kollektiv have de fornødne kompetencer til at styre cybersikkerheden i enheden.

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

## Hvilken rolle spiller ledelsen ift. uddannelse af medarbejdere?

Som ledelse spiller du en vigtig rolle for medarbejdernes kompetencer og adfærd. Og ifølge § 7, stk. 2 i NIS 2-loven skal ledelsesorganet tilskynde til, at ansatte tilbydes kurser, svarende til dem, ledelsen selv gennemfører.

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:

*7) Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.*

Politikken efter skal altså sikre, at medarbejderne har viden og færdigheder om cyber- og informationssikkerhed, som er passende i forhold til deres rolle og ansvar.

## Kan ledelsen sanktioneres?

Ifølge NIS 2-loven §23, stk.1, og 2):

*Har en eller flere af de håndhævelsesforanstaltninger, der er pålagt i medfør af § 22, nr. 1-4, vist sig at være utilstrækkelige, kan den kompetente myndighed fastsætte en frist, inden for hvilken den væsentlige enhed skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde den kompetente myndigheds krav. Er tiltagene ikke foretaget inden for den fastsatte frist, kan den kompetente myndighed træffe afgørelse om følgende, jf. dog stk. 4:*

*2) Midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos enheden at udøve ledelsesfunktioner i den pågældende enhed.*

Som ledelse skal du være særligt opmærksomme på, at du i særlige tilfælde kan gøres personligt ansvarlige for efterlevelsen af NIS 2-loven i deres organisation.

Den relevante tilsynsmyndighed kan ifølge NIS 2-lovens § 23, stk. 1 midlertidigt forbyde personer med ledelsesansvar på niveau med som minimum en administrerende direktør (eller den juridiske repræsentant, hvis virksomheden har sådan en) i at udøve ledelsesfunktioner i den pågældende enhed.

En forudsætning for denne sanktion er, at alle andre håndhævelsesforanstaltninger har vist sig at være utilstrækkelige, og den vil derfor kun blive anvendt som en sidste udvej.

Forbuddet skal være proportionalt med omstændighederne og overtrædelsens alvor. Forbuddet er midlertidigt og kan kun anvendes, indtil enheden afhjælper de mangler, eller opfylder de krav, som ligger til grund for forbuddet.

# Implementering af cybersikkerhedsforanstaltninger

1. Introduktion
2. Krav og anbefalinger
3. Standarder
4. Politik for risikostyring og informationssystemsikkerhed
5. Håndtering af hændelser
6. Driftskontinuitet
7. Forsyningskædesikkerhed
8. Erhvervelse, udvikling og vedligeholdelse
9. Effektivitet af foranstaltninger
10. Cyberhygiejne og cybersikkerhedsuddannelse
11. Kryptografi
12. Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
13. Multifaktorautentificering og nødkommunikationssystemer

## Introduktion

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

Det vil blive klart, hvad der er dit ansvar, og hvad du kan uddelegere til driftsorganisationen og medarbejderne.

Vi har tilføjet en række links fra sikkerdigital.dk, der i samarbejde med Styrelsen for Samfundssikkerhed og bestyrelsesforeningen har udarbejdet en række Vejledninger og anbefalinger.

[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.

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

## Krav og anbefalinger

I dette kapitel skelnes der mellem:

1. de dele af foranstaltningerne, der **skal** implementeres (et krav),
2. de dele af foranstaltningerne der **bør** implementeres (en anbefaling); og
3. de foranstaltninger, der **kan** implementeres (et forslag eller eksemplificering).

Enheder skal forelægge dokumentation for de foranstaltninger, der **skal** implementeres.

Hvis foranstaltninger der **bør** implementeres, ikke er implementeret, skal enheden forklare og dokumentere over for den relevante tilsynsførende myndighed, hvorfor disse er fravalgt.

Denne vurdering skal tage hensyn til den teknologiske situation, implementeringsomkostninger og risici, herunder samfundsmæssige og økonomiske konsekvenser.

For de dele af foranstaltningerne, der **kan** implementeres, kan enheden betragte dem som en mulig måde at implementere foranstaltninger i NIS 2-loven (§ 6).

Når enhederne bliver underlagt tilsyn, vil de sektoransvarlige myndigheder vurdere:

1. om anbefalingerne i denne [vejledning om implementering af cybersikkerhedsforanstaltninger](#) fra Styrelsen for Samfundssikkerhed er fulgt.
2. eller om enheden har foretaget en risikovurdering, vurderet om risikohåndteringen er tilstrækkelig og ikke mindst dokumenteret både vurdering og håndtering.

Disse cybersikkerhedsforanstaltninger er god praksis for styring af cyber- og informationssikkerhedsrisici og er i mange tilfælde allerede implementeret helt eller delvist. NIS 2-implementeringen er en god anledning til, at enhederne genbesøger deres risikostyring, samtidig med at de implementerer processer for indberetning af hændelser og sårbarheder.

## 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.

Hvis en enhed allerede anvender en standard, vil enheden nemmere kunne kortlægge sit eksisterende cyber- og informationssikkerhedsarbejde i forhold til NIS 2-loven.

Enheder der ikke anvender standarder, vil kunne finde uddybende hjælp til måder at arbejde med NIS 2-lovens foranstaltninger på i standarder.

Standardernes uddybninger er ikke med i denne e-bog, da det er op til enhederne selv at vurdere hvilke de vil anvende. Men for mere information om standarder se link nedenfor.

Det at følge en standard er en hjælp til efterlevelse, men er ikke en sikkerhed for, at du opfylder NIS 2-kravene.

Til din hjælp og overblik: De standarder, du med fordel kan støtte dig op af, er:

- **DS/EN ISO/IEC 27001:2023** Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Ledelsessystemer for informationssikkerhed – Krav
- **NIST CSF 2.0** National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0
- **DS/IEC 62443-2-1:2011** Industrielle kommunikationsnetværk – Netværks- og systemsikkerhed – Del 2-1: Etablering af et sikkerhedsprogram til industrielle automations- og styringssystemer
- **DS/EN IEC 62443-3-3:2019** Industrielle kommunikationsnetværk – Netværks- og systemsikkerhed – Del 3-3: Systemsikkerhedskrav og sikkerhedsniveauer
- **EECC** - Guideline on security measures under the EECC, 4th Edition, 2021

- **ETSI EN 319 401** Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers V2.3.1, May 2021

# Politik for risikostyring og informationssystemssikkerhed

Ifølge NIS 2-loven § 6, stk. 1, nr. 1.:

*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 skal som minimum omfatte følgende:*

*1) Politikker for risikoanalyse og informationssystemssikkerhed.*

## Lovbemærkninger:

Det foreslås i *nr. 1*, at foranstaltningerne skal omfatte politikker for risikoanalyse og informationssystemssikkerhed.

Dette vil bl.a. indebære, at enheden skal udarbejde en politik for informationssystemssikkerhed, der fastlægger den overordnede ramme for implementering af foranstaltninger, jf. § 6, stk. 1, nr. 1-10, som understøtter sikkerheden i enhedens net- og informationssystemer.

Enheder skal endvidere udarbejde en politik for risikostyring, som indeholder metoder til at identificere og adressere eventuelle risici.

## Politik for informationssystemssikkerhed

En politik for informationssystemssikkerhed sætter retningen for hvordan enheden styrer informationssystemssikkerhed og dens implementering, inklusiv tekniske, operationelle og organisatoriske aspekter = cybersikkerhedsforanstaltninger.

Enheden skal udarbejde og implementere en politik for informationssystemssikkerhed i net- og informationssystemer. Politikken skal ud fra en risikobaseret tilgang sikre et passende sikkerhedsniveau i forhold til enhedens formål. Risikovurderingen skal tage hensyn til det aktuelle tekniske niveau, implementeringsomkostninger og risici mod sikkerheden i enhedens net- og informationssystemer – Med fokus på, hvad der kan forvolde skade på data og tjenester af samfundsmæssig betydning.

Politikken for informationssystemssikkerhed bør ajourføres årligt og ved væsentlige ændringer af enhedens forretningsmæssige mål og i trusselsbilledet.

Politikken for informationssystemssikkerhed skal være godkendt af enhedens ledelsesorgan. Eventuelle specifikke politikker bør gennemgås af den relevante ledelse,

og resultatet af gennemgang og eventuelle tilretninger rapporteres til enhedens ledelsesorgan.

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

## Politik for risikostyring

Enheden skal udarbejde, dokumentere og kommunikere en politik for risikostyring inklusiv metoder til identifikation, analyse, evaluering og håndtering af risici. Politikker og metoder sikrer en ensartet og målrettet risikostyring på tværs af enheden.

Enheden skal etablere og vedligeholde en politik for passende risikostyring for at identificere og adressere alle de relevante risici, der er i forhold til sikkerheden i enhedens net- og informationssystemer. Enheden skal gennemføre og dokumentere risikovurderinger og implementere og regelmæssigt revurdere risikohåndteringsplanen.

Resultatet af risikovurdering, risikohåndtering og niveauet af tilbageværende risici, skal accepteres af risikoejeren. Primært i relation til samfundsrisici. Og der skal være passende rapportering til enhedens ledelsesorgan.

Politikker for risikostyring bør ajourføres med planlagte intervaller og ved væsentlige ændringer af enhedens forretningsmæssige virksomhed og ændringer i enhedens sårbarheder og trusselsbillede. Politikken for risikostyring skal være dokumenteret og godkendt af enhedens relevante ledelse.

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

## Håndtering af hændelser

Ifølge NIS 2-loven §6, stk 1, nr.2:

*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 skal som minimum omfatte følgende:*

*2) Håndtering af hændelser.*

Lovbemærkning:

*Det følger af det foreslåede nr. 2, at foranstaltningerne skal omfatte håndtering af hændelser.*

*Dette vil bl.a. indebære, at enheder skal udarbejde procedurer for håndtering af hændelser. Enheder skal i fornødent omfang implementere logning og monitorering af uregelmæssigheder i enhedens net- og informationssystemer med henblik på at kunne identificere hændelser. Logdata skal derudover sikres mod manipulation og beskyttes mod uautoriseret adgang.*

## Håndtering af hændelser

Enheden skal reagere hensigtsmæssigt på væsentlige hændelser for at minimere konsekvenserne. Det indebærer at begrænse skader på net- og informationssystemer samt kritiske tjenester, så trusslens indvirkning begrænses. Og at enhedens almindelige drift bliver genoprettet hurtigst muligt.

Enheden skal udarbejde og implementere procedurer for at kunne identificere, opdage, analysere og reagere på hændelser, herunder for at kunne genoprette sikker stabil drift samt håndtere underrettningsforpligtelser ved væsentlige hændelser.

Procedure for håndtering af hændelser bør ajourføres med planlagte intervaller og ved væsentlige ændringer af enhedens forretningsmæssige mål og ændringer i enhedens og trusselsbillede. Procedure for håndtering af hændelser skal være dokumenteret og godkendt af den relevante ledelse.

## Logning og monitorering

Enheden skal være i stand til at opdage hændelser, der kan bringe data i fare, og reagere passende og derved i videst mulige omfang afværge skadesvirkningen af hændelsen. Logs anvendes også til at undersøge hændelsen efterfølgende.

Enheden skal i nødvendigt omfang have processer og bruge værktøjer til at monitorere og logge samt reagere på aktiviteter på deres netværk og i deres informationssystemer. Hermed bliver enheden i stand til at opdage eventuelle hændelser og reagere i overensstemmelse hermed for at afbøde virkningerne. Monitorering bør så vidt muligt være automatiseret (f.eks. Intrusion Detection Systems) og kan udføres enten i realtid eller med regelmæssige intervaller, afhængigt af virksomhedens muligheder.

Procedurerne for logning og monitorering, samt listen over aktiver eller hændelser, der logges, bør gennemgås med planlagte intervaller, og når der sker ændringer, blandt andet i trusselsbilledet og ved kendte sårbarheder, eller i tilfælde af væsentlige hændelser. Der bør føres dokumentation for, at gennemgangen af procedurerne finder sted på det planlagte tidspunkt.

## Driftskontinuitet

[Ifølge NIS 2-loven §6, stk 1, nr.3:](#)

*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 skal som minimum omfatte følgende:*

*3) Driftskontinuitet, herunder backup-styring og reetablering efter en katastrofe og krisestyring.*

[Lovbemærkninger:](#)

Det foreslås i nr. 3, at foranstaltningerne skal omfatte driftskontinuitet, herunder backup-styring og reetablering efter en katastrofe og krisestyring.

Dette vil indebære, at enheder skal udarbejde procedurer til sikring af driftskontinuitet i tilfælde af en hændelse. På grundlag af enhedernes risikostyring, jf. nr. 2, og driftskontinuitets-procedure, skal enheder således udarbejde procedurer for backupstyring og gendannelse af data.

Enheder skal foretage en vurdering af behovet for at udarbejde en beredskabsplan for krisestyring og reetablering efter en katastrofe. Enheder skal foretage en vurdering af, om der er behov for at etablere redundans, nødstrømsforsyning, understøttende forsyning eller anden sikring med tilsvarende virkning for enhedens net- og informationssystemer.

## Driftskontinuitet

Enheden skal sikre at driften kan opretholdes, og at cybersikkerheden bevares i tilfælde af en væsentlig hændelse eller krise, og at normal-drift kan genetableres, når hændelsen eller krisen er overstået.

Enheden skal udarbejde og vedligeholde procedurer, der sikrer driftskontinuitet i tilfælde af en sikkerhedshændelse, eksempelvis en plan for fortsat drift og en plan for genopretning efter en krise.

Planer for opretholdelse af driften bør gennemgås og testes med regelmæssige planlagte mellemrum samt efter væsentlige hændelser og større ændringer i driftsmiljøet eller ændring i risici. Her bør det vurderes, om planerne virker efter

hensigten og er tilstrækkelige og tidssvarende i forhold til enhedens aktuelle forhold. Ændringer i planerne bør dokumenteres.

## Backup

Der skal tages backup af enhedens relevante data, så data kan gendannes i tilfælde af tab, beskadigelse eller anden form for forstyrrelse af enhedens data.

Enheden skal etablere procedurer, der sikrer, at der tages backup af alle enhedens relevante data, herunder konfigurationsdata, i det omfang som enheden finder det nødvendigt for at opretholde sine tjenester.

Enheden bør dokumentere, at den med jævne mellemrum tester, at dennes backup, eller alternative gendannelsesmetoder, er fuldstændig og tilgængelig i forhold til det, der er beskrevet i procedurer for backup, og at backuppen har den fornødne integritet, også selvom det ser ud til, at backup er fuldstændig. Resultatet af tests bør dokumenteres og godkendes af den relevante ledelse.

## Redundans

Enheden skal sikre adgang til tilstrækkelige ressourcer, herunder faciliteter, personale, net- og informationssystemer og komponenter, når det er nødvendigt.

Enheden skal vurdere, om der er behov for at etablere redundans ved eksempelvis at have it-udstyr eller alternative lokationer i reserve. Vurderingen bør tage udgangspunkt i enhedens politikker for informationssystemsikkerhed og risikostyring samt kontinuitetsplan.

Enheden bør med regelmæssige planlagte mellemrum vurdere sit behov for redundans af hardware, software, tjenester, faciliteter mv. for at sikre, at de passende ressourcer er til stede i tilfælde af driftsforstyrrelser.

Anvendelse af enhedens redundante ressourcer bør være dokumenteret, så relevante medarbejdere har kendskab til, hvordan de ekstra ressourcer kan tilgås.

## Krisestyring

Enheden skal have processer på plads til at håndtere kriser i tilfælde af en eller flere samtidige væsentlige hændelser.

Foranstaltning Enheden skal foretage en vurdering af behovet for at udarbejde en beredskabsplan med procedurer for krisestyring. Hvis enheden vurderer, at der er

behov, bør enheden etablere og dokumentere de relevante procedurer til at håndtere særligt væsentlige hændelser.

Den dokumenterede plan for krisestyring bør gennemgås med regelmæssige planlagte mellemrum, hvor det bør vurderes, om planen er tilstrækkelig og tidssvarende i forhold til enhedens aktuelle forhold.

Der bør regelmæssigt gennemføres øvelser, der kan belyse, om planen for krisestyring virker efter hensigten, og efterfølgende bør de ændringer til planen, der findes nødvendige, implementeres og dokumenteres.

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

## Forsyningskædesikkerhed

[Ifølge NIS 2-loven § 6, stk. 1, nr. 4:](#)

*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 skal som minimum omfatte følgende:*

*4) Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.*

### [Lovbemærkninger:](#)

Det foreslås i nr. 4, at foranstaltninger skal omfatte forsyningsikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.

Dette vil indebære, at enheder skal udarbejde procedurer for leverandørstyring for at sikre passende forsyningskædesikkerhed. [...]

Enheden skal sikre, at leverandører og tjenesteudbydere opfylder enhedens behov for forsyningsikkerhed og krav til cybersikkerhed, så enheden og enhedens produkter eller

tjenester ikke påvirkes negativt af sårbarheder eller hændelser hos enhedens leverandører eller i deres produkter/tjenester.

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. Det gælder både ved levering af it-produkter og tjenester samt andre kritiske leverancer som strøm, teknisk bistand med mere.

Procedurerne skal gøre enheden i stand til at identificere og vurdere risici ved specifikke leverandører og indgå aftaler, der sikrer overholdelse af enhedens krav til forsynings- og cybersikkerhed. For at undgå unødigt høje krav bør enheden anvende en risikobaseret tilgang, hvor kravene til den enkelte leverandør eller tjenesteudbyder er proportionelt med den specifikke leverances betydning for enhedens forsynings- og cybersikkerhed.

Enheden bør gennemgå procedurer til leverandørstyring og monitorere, gennemgå, evaluere og styre ændringer, der måtte opstå i de direkte leverandørers eller tjenesteudbyderes cybersikkerhedspraksis, med planlagte intervaller eller i tilfælde af en hændelse, der har eller kan påvirke cybersikkerheden i enhedens net- og informationssystemer. Observationer fra disse gennemgange, monitoreringer, evalueringer mv. bør dokumenteres.

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

## Erhvervelse, udvikling og vedligeholdelse

Ifølge NIS 2-loven §6, stk. 1, nr. 5:

*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 skal som minimum omfatte følgende:*

*5) Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.*

### Løvbemærkninger:

*Det foreslås i nr. 5, at foranstaltninger skal omfatte sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.*

*Dette vil indebære, at enheder skal udarbejde procedurer for sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af enhedens net- og informationssystemer, med udgangspunkt i politikken for informationssystemssikkerhed. Enheder skal endvidere udarbejde procedurer for håndtering af sårbarheder, der kan have indvirkning på enhedens net- og informationssystemer.*

## Erhvervelse, udvikling og vedligeholdelse

Enheden skal planlægge, implementere og vedligeholde cybersikkerheden i hele et net- og informationssystemets levetid – gennem hele livcyklussen (anskaffelse, implementering/indfasning, drift, udfasning og terminering/bortskaffelse) for de enkelte komponenter.

Enheden skal udarbejde dokumenterede procedurer for cybersikkerhed:

- ved anskaffelse af it-produkter eller tjenester fra tredje part.
- ved udvikling af net- og informationssystemer.
- ved vedligeholdelse af net- og informationssystemer.
- ved afvikling/bortskaffelse af net- og informationssystemer.

Procedurerne skal tage udgangspunkt i enhedens politik for informationssystemssikkerhed og bør være koblet til enhedens politik og metoder for risikostyring samt procedurer for leverandørstyring.

Enheden bør gennemgå deres processer for styring af livscyklus for indkøbte og selvudviklede it-tjenester, it-systemer eller it-produkter med regelmæssige planlagte mellemrum eller ved væsentlige hændelser. Observationer fra gennemgangen bør dokumenteres.

## Håndtering af sårbarheder

Enheden skal være orienteret om eventuelle sårbarheder og skal implementere passende foranstaltninger, der nedsætter sandsynligheden for, at sårbarhederne kan udnyttes. Derudover kan videregivelse af informationer om sårbarheder hjælpe andre til at blive opmærksomme på eventuelle sårbarheder i deres net- og informationssystemer.

Enheden skal udarbejde procedurer for håndtering af sårbarheder, der kan have indvirkning på enhedens net- og informationssystemer. Procedurene skal gøre enheden i stand til at indhente oplysninger om tekniske sårbarheder i sine net- og informationssystemer, evaluere enhedens eksponering for sådanne sårbarheder og træffe passende foranstaltninger til at håndtere sårbarhederne.

Enheden bør gennemføre sårbarhedsscanninger og indsamle observationer med regelmæssige planlagte mellemrum og ved større ændringer eller sikkerhedshændelser. Scanninger, observationer og håndtering bør dokumenteres. Enheden bør monitorere sine kilder til sårbarhedsinformationer med planlagte mellemrum og dokumentere de sårbarheder, der er relevante for enheden.

## Effektivitet af foranstaltninger

Ifølge NIS 2-loven §6, stk. 1, nr. 6:

*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 skal som minimum omfatte følgende:*

*6) Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.*

Lovbemærkninger:

*Det foreslås med nr. 6, at foranstaltninger skal omfatte politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.*

*Dette vil indebære, at enheder skal udarbejde en politik og procedurer med henblik på at vurdere effektiviteten af de implementerede foranstaltninger samt for vurdering af behov for tekniske tests for potentielle sårbarheder, herunder f.eks. i form af sårbarheds-scanninger eller penetrationstests.*

### Vurdering af effektiviteten af de implementerede foranstaltninger

Enheden skal sikre, at de foranstaltninger, enheden implementerer, er tilstrækkelige i forhold til de risici, enheden står overfor. Foranstaltningerne skal være proportionale med både trusselsbilledet og de ressourcer, der er afsat til området.

Enheden skal udarbejde en politik for, hvordan man løbende vurderer enhedens implementerede foranstaltninger. Vurderingen skal undersøge, om foranstaltningerne er tilstrækkelige til fortsat at beskytte mod relevante risici samt vurdere, om enhedens politik for informationssystemsikkerhed er i overensstemmelse med både enhedens egne krav, gældende lovgivning og relevante gennemførelsesforordninger.

Politik og procedure for vurdering af effektiviteten af de implementerede foranstaltninger bør ajourføres med planlagte intervaller og ved væsentlige ændringer af enhedens forretningsmæssige mål og ændringer i enhedens sårbarheder og trusselsbillede. Det kan eksempelvis være forud for den fastlagte gennemgang af enhedens politik for informationssystemsikkerhed.

## Tekniske tests

Ved hjælp af tekniske tests er det muligt at teste for eventuelle sårbarheder og derved undersøge effektiviteten af de foranstaltninger, som enheden har implementeret.

Enheden skal løbende vurdere behovet for tekniske tests som led i evalueringen af, hvor effektivt de implementerede foranstaltninger fungerer.

Test bør gennemføres med passende planlagte mellemrum og ved større ændringer eller væsentlige hændelser. Dokumentation fra tests bør gennemgås af relevant personale med passende planlagte mellemrum, og resultater bør rapporteres til relevant ledelse.

## Cyberhygiejne og cybersikkerhedsuddannelse

[Ifølge NIS 2-loven §6, stk. 1, nr. 7:](#)

*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 skal som minimum omfatte følgende:*

*7) Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.*

[Lovbemærkninger:](#)

*Det foreslås i nr. 7, at foranstaltninger skal omfatte grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.*

*Dette vil bl.a. indebære, at enheder skal implementere relevante grundlæggende cyberhygiejnepraksisser med udgangspunkt i deres politik for informationssikkerhed, herunder f.eks. gennem brug af passwords og sikker brug af e-mails. Endvidere skal enheder udarbejde en politik for uddannelse af relevante medarbejdere for at sikre, at medarbejderne har relevant viden og færdigheder om informationssikkerhed.*

## Cyberhygiejnepraksisser

Enheden skal opretholde et passende niveau af cybersikkerhed gennem implementering af fundamentale foranstaltninger.

Enheden skal implementere relevante grundlæggende cyberhygiejnepraksisser med udgangspunkt i enhedens politik for informationssystemssikkerhed. Cyberhygiejne dækker over de grundlæggende foranstaltninger og daglige sikkerhedsvaner, praksisser og procedurer, som beskytter netværk, systemer og data mod almindelige trusler. Dette indebærer blandt andet implementeringen af en række fundamentale foranstaltninger.

Der henvises til relevant dokumentation beskrevet i de andre afsnit om de pågældende foranstaltninger.

## Cybersikkerhedsuddannelse

Enheden skal sikre, at medarbejdere på alle niveauer er opmærksomme på, og er uddannet og trænet til at håndtere, relevante sikkerhedsrisici, samt kender og anvender almindelige cyberhygiejnepraksisser (se afsnittet overfor).

Enheden skal udarbejde en politik for uddannelse af medarbejdere for at sikre, at de modtager net- og informationssikkerhedstræning og uddannelse, der klæder medarbejderne på til at håndtere relevante sikkerhedsrisici og beskytte net- og informationssystemer. Uddannelse og træning skal etableres i overensstemmelse med enhedens politik for informationssystemssikkerhed, eventuelle emnespecifikke politikker og relevante procedurer for net- og informationssikkerhed.

Uddannelses- og træningsprogram bør opdateres og gennemføres med regelmæssige mellemrum under hensyntagen til gældende politikker og regler, tildelte roller, ansvarsområder samt kendte trusler og teknologisk udvikling.

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

# Kryptografi

[Ifølge NIS 2-loven §6, stk. 1, nr. 8:](#)

*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 skal som minimum omfatte følgende:*

*8) Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.*

[Lovbemærkninger:](#)

*Det foreslås med nr. 8, at foranstaltninger skal omfatte politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.*

*Dette vil bl.a. indebære, at enheder skal udarbejde en politik og procedurer for brug af kryptografi og, hvor det er relevant, kryptering for at beskytte deres net- og informationssystemer. Politikken og procedurerne skal være passende i forhold til det aktuelle teknologiske stade.*

Enheden skal sikre tilstrækkelig og effektiv brug af kryptografi til at beskytte informationens fortrolighed, autenticitet og/eller integritet.

Enheden skal udarbejde og implementere en politik og procedurer vedrørende kryptografi med henblik på at sikre tilstrækkelig og effektiv brug af kryptografi til at beskytte informationens fortrolighed, autenticitet og/eller integritet i overensstemmelse med aktivernes klassifikationsniveau og resultaterne af risikovurderingen.

Politikken og procedurerne skal være passende i forhold til det aktuelle teknologiske stade. Kryptografi kan bruges til forskellige formål, eksempelvis til opbevaring af password, sikker identifikation af data og dens validitet, samt beskyttelse af datas fortrolighed.

Alle relevante medarbejdere i enheden bør have adgang til politikker og procedurer for brug af kryptografi og kryptering i enheden. Politikken og procedurerne for kryptografi bør gennemgås med planlagte intervaller samt ved erkendte sårbarheder eller teknologiske fremskridt, der kan påvirke sikkerheden i den anvendte kryptografi. Det

kan eksempelvis være en algoritme, der bliver brudt, eller at behovet for nøgkel længde øges som følge af øget computerkraft hos angribere.

Hvis en gennemgang af politikker eller procedurer afdækker sårbarheder, skal dokumentationen og de tekniske løsninger opdateres, og ændringerne skal kommunikeres til relevante parter.

## Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

Ifølge NIS 2-loven §6, stk. 1, nr. 9:

*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 skal som minimum omfatte følgende:*

*9) Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.*

Lovbemærkninger:

*Det foreslås i nr. 9, at foranstaltninger skal omfatte personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.*

*Dette vil bl.a. indebære, at enhederne skal implementere foranstaltninger til personalesikkerhed, der skal sikre, at den enkelte medarbejder forstår, udviser og forpligter sig til at leve op til deres ansvar for informationssikkerhed.*

*Enheder skal derudover udarbejde en politik for adgangskontrol for at beskytte mod uautoriseret adgang til enhedens net- og informationssystemer. Politikken skal som minimum identificere og vurdere risici i forhold til logisk og fysisk adgangskontrol og indeholde procedurer for styring af adgangsrettigheder.*

*Enheder skal fastlægge hvordan den forvalter aktiver, der vil kunne påvirke sikkerheden i enhedens net- og informationssystemer.*

## Personalesikkerhed

Enheden skal sikre, at ansatte, samarbejdspartnere, og hvor relevant leverandører, forstår og forpligter sig til deres sikkerhedsansvar i overensstemmelse med enhedens politik for informationssystemsikkerhed.

Enheden skal sikre, at medarbejdere og – hvor relevant – leverandører eller tjenesteudbydere er bekendt med og lever op til deres ansvar for enhedens net- og informationssystemssikkerhed. Dette skal ske i forhold til de tjenester, enheden udbyder, og i overensstemmelse med enhedens politik for informationssystemsikkerhed.

Enheden kan sikre sig, at der i medarbejdernes ansættelsesaftaler anføres, at medarbejderen er forpligtet til at gennemføre den nødvendige uddannelse og træning i den net- og informationssikkerhed enheden definerer. Samt at medarbejderen er bekendt med deres ansvar for at efterleve enhedens politikker og procedurer for net- og informationssikkerhed.

Medarbejderens nærmeste leder bør godkende medarbejderes kompetencer og retskaffenhed. Dokumentation kan være i form af nedskrevne politikker og procedurer for, hvordan enheden eksempelvis gennemfører baggrundskontrol og aftrædelsessamtaler. Politikker og procedurer bør gennemgås med passende planlagte mellemrum.

## Adgangskontrol

Enheden skal beskytte fysiske og ikke fysiske aktiver imod tab af fortrolighed, integritet og tilgængelighed ved at beskytte dem mod uautoriseret adgang.

Enheden skal udarbejde en politik for at administrere tildeling, ændring og fjernelse af adgangsrettigheder til net- og informationssystemer i overensstemmelse med enhedens politik for informationssystemsikkerhed.

Dokumentation kan være i form af nedskrevne politikker og procedurer vedrørende tildeling af, ændring i og fratagelse af adgang til enhedens lokaler og net- og informationssystemer. Politikker og procedurer bør gennemgås med passende planlagte mellemrum.

## Forvaltning af aktiver

Enheden skal sikre en passende beskyttelse af det enkelte aktiv eller typer af aktiver. Forvaltning af aktiver sikrer, at enheden får indsigt i hvilke aktiver, enheden skal beskytte, og hvilket beskyttelsesniveau der er passende for de enkelte aktiver.

Enheden skal fastlægge, hvordan enheden forvalter aktiver, der vil kunne påvirke enhedens net- og informationssikkerhed. Enheden bør derfor udarbejde procedurer for forvaltning af alle enhedens aktiver, herunder net- og informationssystemer, tilhørende komponenter samt kritiske afhængigheder mellem disse og eventuelle samarbejdspartnere. Der bør defineres et passende beskyttelsesniveau for de aktiver, der er omfattet af enhedens net- og informationssystemer. Eksempelvis har mobile enheder ofte et andet beskyttelsesbehov end stationære servere.

Dokumentation kan være i form af nedskrevne procedurer vedrørende håndtering af aktiver, samt dokumentation for, hvordan disse kommunikeres til relevante parter. Procedurerne bør gennemgås med planlagte intervaller.

## Multifaktorautentificering og nødkommunikationssystemer

Ifølge NIS 2-loven § 6, stk. 1, nr. 10:

*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 skal som minimum omfatte følgende:*

*10) Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant.*

Lovbemærkninger:

*Det foreslås med nr. 10, at foranstaltninger skal omfatte brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant.*

*Dette vil bl.a. indebære, at enheder skal anvende multifaktorautentifikation eller kontinuerlig autentifikation ved adgang til net- og informationssystemer i overensstemmelse med enhedens politik for adgangskontrol.*

*Enheder skal endvidere anvende sikret tale-, video- og tekstkommunikation i overensstemmelse med politikken for brug af kryptografi og kryptering og under hensyntagen til kommunikationsmidlernes tilgængelighed, også i en nødsituation.*

## Multifaktorautentificering

Enheden skal styrke adgangskontrollen og reducere risikoen for uautoriseret adgang ved at kombinere flere autentifikationsfaktorer og løbende vurdere adfærd og kontekst.

Enhedens brugere, it-komponenter og andre aktiver skal, hvor det vurderes relevant, autentificeres ved hjælp af multifaktorautentifikation (MFA) og/eller kontinuerlige autentifikationsmekanismer ved adgang til enhedens net- og informationssystemer. Autentifikationskravene bør fastlægges med udgangspunkt i en risikovurdering og matche aktivets klassifikationsniveau (ud fra fortrolighed, integritet og tilgængelighed). Autentifikationen skal være i overensstemmelse med enhedens adgangskontrolpolitikker.

Enheden skal med regelmæssige planlagte mellemrum, eller ved større ændringer og sikkerhedshændelser, gennemgå politikken for adgangskontrol og i den forbindelse gennemgå og vurdere enhedens brug af MFA og/eller kontinuerlig autentifikation. Gennemgangen skal dokumenteres.

## Nødkommunikationssystemer

Enheden skal sikre, at enheden altid har mulighed for at anvende tale-, video- og tekstkommunikation, hvor og når det er relevant, herunder i tilfælde af hændelser. Kommunikationskanalerne skal sikre den nødvendige fortrolighed, integritet og tilgængelighed internt hos enheden.

Enheden bør vurdere deres behov for kommunikationskanaler, inklusiv enhedens behov for at beskytte fortrolighed ved brug af kryptering eller behov for redundante kommunikationsløsninger. Disse kommunikationsløsninger bør også indgå i enhedens risikovurdering samt i enhedens procedurer for driftskontinuitet, hændeshåndtering og krisestyring. Der bør fastlægges foranstaltninger på grundlag heraf.

Nødkommunikationssystemer bør testes regelmæssigt og kan indgå som en del af en årlig krisestyringsøvelse. Resultatet af tests og øvelserne bør dokumenteres for at sikre, at der samles op på de fejl, man finder, og den læring øvelserne tilvejebringer.

# Hændelsesunderretning

1. Introduktion
2. Hvilke hændelser skal der underrettes om?
3. Hvis vedligeholdelse af net- og informationssystemer er outsourcet
4. Hvordan skal du underrette?
5. Obligatoriske underretninger
6. Særligt for tillidstjenesteudbydere
7. Eksempler
8. Frivillig underretning

## Introduktion

Nu er vi nået til fjerde og sidste kapitel i e-bogen. I dette kapitel samler vi trådene og sætter fokus på hændelsesunderretning, hvor vi hjælper dig i ledelsesorganet med hændeshåndtering i forhold til NIS 2-loven.

På denne måde ved du *hvad* (og *hvornår*) du skal gøre, hvis uheldet skulle være 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.

Det vil sige, at hændelsen skal påvirke net- og informationssystemer, der understøtter leveringen af en eller flere af samfundskritiske ydelser, før der skal ske underretning.

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

Derudover skal påvirkningen af hændelsen jf. [§ 12, stk. 2](#) være betydelig, dvs. forårsage eller være i stand til at medføre mindst én af disse tre situationer:

1. alvorlig driftsforstyrrelse af en af de leverede tjenester (i de sektorer eller undersektorer, der er anført i Bilag 1 og 2 til NIS 2-loven)
2. betydelige økonomiske tab for den pågældende enheds betydelige materiel, fysisk eller ikke-fysisk skade som påvirker andre fysiske eller juridiske personer.
3. betydeligt materiel, fysisk eller ikke-fysisk skade som påvirker andre fysiske eller juridiske personer.

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.

Nedenfor bliver *de tre situationer* uddybet med konkrete eksempler på hændelser, der kan betragtes som væsentlige. Eksemplerne skal ses som illustrative og ikke dækkende for alle mulige scenarier.

## Alvorlig driftsforstyrrelse af en af de leverede tjenester

### [Lovbemærkninger til §12:](#)

*Med alvorlige driftsforstyrrelser forstås en hændelse, som kompromitterer tjenesterne fortrolighed, integritet, autenticitet og/eller tilgængelighed.*

Hændelser, der kompromitterer eller er i stand til at kompromittere **fortrolighed, integritet og/eller autenticitet** af data i enhedens net- og informationssystemer, kan eksempelvis være:

- uberettiget adgang til kritiske net- og informationssystemer - nogen har fået mere omfattende adgang end nødvendigt til netværk, systemer eller informationer, der understøtter leveringen af enhedens tjenester.
- uberettiget eller utilsigtet konfiguration af et kritisk net- og informationssystem, som understøtter leveringen af enhedens tjenester - et kritisk net- og informationssikkerhedssystem er blevet eller kan blive konfigureret af en person, som ikke burde have rettigheder til at konfigurere enhedens system eller netværk.

### **EKSEMPEL – På driftsforstyrrelser**

Hvis en trusselsaktør placerer sig i en enheds net- og informationssystemer med henblik på at forårsage afbrydelser af dens tjenester i fremtiden, bør hændelsen anses for at være væsentlig.

## Økonomiske tab for den pågældende enhed

### [Lovbemærkninger til §12:](#)

*Med økonomiske tab forstås betydelige tab og/eller omkostninger som følge af hændelse. Tab eller udbredelse af intellektuel ejendom, der kan bringe enhedens fremtidige indtægt eller omsætning i fare, medregnes ligeledes som økonomisk tab.*

En hændelse betragtes altid som væsentlig, hvis den forårsager:

- et betydeligt økonomisk tab eller en omkostning (eller en kombination af begge), eller en forventning om samme

- tab eller udbredelse af intellektuel ejendom på en måde, som sandsynligvis kan bringe enhedens fremtidige indtægter eller omsætning i fare
- eksfiltrering af forretningshemmeligheder fra den pågældende enhed i henhold til § 2, pkt. 1 i Lov nr. 309 af 25/04/2018 (Lov om forretningshemmeligheder).

### **EKSEMPEL - Betydeligt økonomisk tab**

En stor produktionsvirksomhed udsættes for et cyberangreb, der krypterer centrale systemer og produktionsmaskiner i tre dage. Nedlukningen forårsager produktionsstop og forsinkede leverancer, hvilket resulterer i bøder fra kunder samt tabte ordrer. Samlet set overstiger det økonomiske tab 1% af enhedens årlige omsætning, hvilket i virksomhedens risikovurdering er den foruddefinerede tærskel for et betydeligt tab.

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

### Lovbemærkninger til §12:

*En hændelse anses altid for væsentlig, hvis den forårsager hel eller delvis ødelæggelse af kritiske tredje parts fysiske eller digitale aktiver. Ligeledes anses en hændelse altid for at være væsentlig, hvis den forårsager død, eller skader der kræver hospitalsindlæggelse eller behandling.*

En hændelse anses altid for væsentlig, hvis konsekvenserne for tredjepart omfatter mindst én af følgende fysisk eller ikke-fysisk skade:

- delvis eller fuldstændig ødelæggelse af kritiske fysiske eller digitale aktiver
- skader på fysisk infrastruktur, der forårsager en forsinkelse i leveringen af produkter eller tjenester ud over kontraktligt garanterede leveringstider
- skader såsom dødsfald, hospitalsindlæggelse, kvæstelser eller invaliditet
- væsentlige økonomiske konsekvenser.

Tredjepart kan for eksempel være brugere, leverandører, samarbejdspartnere, databehandlere eller andre aktører.

## 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 [CSIRT](#) og de relevante sektoransvarlige myndigheder ([Lovbemærkninger til §12](#)).

Alle omfattede enheder har underretningspligt. Dette udelukker dog ikke, at en enhed kan indgå en aftale om, at den virksomhed, der f.eks. driver enhedens net- og informationssystemer, skal foretage underretninger på vegne af enheden.

Ansvar for, at der sker en rettidig hændelsesunderretning, påhviler dog altid enheden.

## 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>.

Når man underretter via Virk.dk, bliver underretningen automatisk sendt til både den relevante sektoransvarlige myndighed og til CSIRT'en. Det vil også være muligt at krydse af, om Datatilsynet skal underrettes om brud på persondatasikkerheden i samme underretning.

Hvis en enhed, der kun er etableret i Danmark, oplever en hændelse, og den vurderes at kunne have grænseoverskridende konsekvenser, skal enheden i forbindelse med hændelsesunderretningen via Virk.dk oplyse, at hændelsen kan have grænseoverskridende konsekvenser.

CSIRT'en og/eller det centrale kontaktpunkt vil herefter orientere den/de relevante CSIRT'er og/eller centrale kontaktpunkter i andre relevante medlemsstater.

Hvis en enhed, der er etableret i mere end en medlemsstat, oplever en hændelse, skal enheden underrette de relevante myndigheder i alle de medlemsstater, hvor den er etableret.

## Obligatoriske underretninger

Ifølge NIS 2-loven §12, stk. 1:

*Væsentlige og vigtige enheder skal underrette den relevante kompetente myndighed og Computer Security Incident Response Team (CSIRT) om enhver væsentlig hændelse.*

*En underretning skal indeholde oplysninger, der gør det muligt at fastslå eventuelle grænseoverskridende virkninger af hændelsen.*

Når en enhed har opdaget en mistænkelig hændelse, eller efter en potentiel hændelse er blevet bragt til dens opmærksomhed fra en tredjepart (såsom en person, en kunde, en enhed, en myndighed, en medieorganisation eller en anden kilde), skal den relevante enhed rettidigt vurdere den mistænkelige hændelse for at afgøre, om den udgør en væsentlig hændelse og i givet fald bestemme dens art og alvor.

## Særligt for tillidstjenesteudbydere

Ifølge NIS 2-loven §13, stk. 2:

*Tillidstjenesteudbydere skal i tilfælde af væsentlige hændelser afgive underretningen efter stk. 1, nr. 2, uden unødigt ophold og senest inden for 24 timer efter at være blevet bekendt med den væsentlige hændelse.*

For udbydere af tillidstjenester gælder det, at **både** den tidlige varslings og hændelsesunderretningen vil skulle sendes senest inden for *24 timer*, efter at enheden har fået kendskab til hændelsen.

Nedenstående er eksempel på en hændelse, hvor underretning skal ske. Vi har taget det med, fordi det vil give dig en bedre forståelse af processen.

### **EKSEMPEL - På ransomwareangreb på en virksomhed**

En virksomhed bliver ramt af en hændelse, som kunne være et ransomwareangreb. Virksomheden kan ikke få adgang til sine data, og den indledende undersøgelse viser, at data er krypteret. Angrebet påvirker både fortroligheden og tilgængeligheden af kritiske data, hvilket resulterer i alvorlige driftsforstyrrelser.

Indvirkning:

Afbrydelsen medfører, at virksomheden ikke kan levere sine tjenester eller produkter som normalt, hvilket skaber forsinkelser og potentielt økonomiske tab. Desuden kan der være risiko for, at følsomme data kompromitteres, hvilket kan føre til yderligere skade for kunder og samarbejdspartnere.

Anmeldelseskrav:

Virksomheden skal underrette hændelsen via [virksomheden.dk](https://virksomheden.dk) til sektoransvarlig myndighed og CSIRT inden for 24 timer med den første vurdering af hændelsen og dens konsekvenser.

## Frivillig underretning

[Ifølge NIS 2-loven §14, stk. 1:](#)

*Offentlige og private enheder kan, uanset at de ikke er omfattet af lovens anvendelsesområde, underrette CSIRT'en om hændelser, nærvedhændelser og cybertrusler*

Offentlige og private enheder har mulighed for at foretage frivillig underretning til CSIRT'en vedrørende hændelser, nærvedhændelser og cybertrusler, uanset om de er omfattet af NIS 2-loven.

Dette kan gøres gennem [Virksomheden.dk](https://virksomheden.dk), hvor der vil være en formular til dette.

Væsentlige og vigtige enheder, der er underlagt NIS 2-loven, kan ligeledes vælge at underrette ikke væsentlige hændelser, cybertrusler og nærvedhændelser frivilligt gennem [Virksomheden.dk](https://virksomheden.dk)

## Ordliste til e-bogen

**AUTENTICITET** Autenticitet betyder, at en person eller et system er, hvad den eller det forgiver at være.

**CSIRT** (Computer Security Incident Response Team) En national eller sektorbaseret enhed, udpeget eller oprettet af en medlemsstat i EU i henhold til artikel 10 i NIS 2-direktivet, med ansvar for at forebygge, detektere og håndtere cybersikkerhedshændelser. I Danmark er CSIRT'en en national enhed. CSIRT'ens opgaver omfatter bl.a. hændelseshåndtering, varsling og koordinering med relevante myndigheder og private aktører. CSIRT'en er en central aktør i både den nationale cybersikkerhedsstruktur og i det europæiske CSIRT-netværk, jf. artikel 15 i NIS 2-direktivet med fokus på samarbejde og informationsdeling på tværs af medlemsstaterne.

**CYBERTRUSSEL** Potentiel omstændighed, begivenhed eller handling, som kan skade, forstyrre eller på anden måde have en negativ indvirkning på net- og informationssystemer, brugerne af sådanne systemer, kunder, partnere (§ 3, nr. 4).

**FORTROLIGHED** Fortrolighed betyder, at information kun er tilgængelig for de personer, enheder eller systemer, der har de rette autorisationer. Det handler om at beskytte information mod uautoriseret adgang.

**HÆNDELSE** 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 (§ 3, nr. 12). På engelsk ofte benævnt "incident".

**HÅNDBLING AF HÆNDELSER** Enhver handling og procedure, der tager sigte på at forebygge, opdage, analysere og inddæmme eller at reagere på og reetablere sig efter en hændelse (§ 3, nr. 13).

**INTEGRITET** Integritet betyder, at information er nøjagtig, komplet, pålidelig og uændret, medmindre det er godkendt af de rette personer. Det sikrer, at data ikke er blevet ændret, slettet eller manipuleret på en uautoriseret måde.

**NET- OG INFORMATIONSSYSTEM** Et net- og informationssystem er i NIS 2-loven defineret som:

a) Et elektronisk kommunikationsnet, hvorved forstås transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer,

i det omfang de anvendes til transmission af signaler, net, som anvendes til radio og tv-spredning, samt kabel-tv-net, uanset hvilken type information der overføres.

b) Enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data.

c) Digitale data som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.

Eksempler på dette kan være it-systemer, OT (Operational Technology) -systemer, IoT (Internet of Things) -enheder og it-infrastrukturkomponenter.

**NÆRVEDHÆNDELSE** En begivenhed, der kunne have bragt 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, men som det lykkedes at forhindre (§ 3, nr. 22).

**SEKTORANSVARLIGE MYNDIGHEDER** Begrebet beskriver den myndighed, der har ansvaret for og fører tilsyn med de specifikke sektorer. De sektoransvarlige myndigheder udpeges ved en bekendtgørelse, inden NIS 2-loven træder i kraft. I NIS 2-loven bruges begrebet ”kompetente myndigheder”. De to betegnelser har samme betydning og skal forstås på samme måde.

**SÅRBARHED** En svaghed, modtagelighed eller fejl ved IKT-produkter eller -tjenester, som kan udnyttes af en cybertrussel (§ 3, nr. 29). IKT-produkter eller -tjenester dækker over it-tjenester, it-systemer eller it-produkter.

**TILLIDSTJENESTE** En elektronisk tjeneste, der normalt udføres mod betaling, og som består af: a) generering, kontrol og validering af elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler eller elektroniske registrerede leveringstjenester og certifikater relateret til tjenester, eller b) generering, kontrol og validering af certifikater for webstedsautentifikation, eller c) bevaring af elektroniske signaturer, segl eller certifikater relateret til disse tjenester (§ 3, nr. 30).

**TILLIDSTJENESTEUDBYDER** En fysisk eller juridisk person, der udbyder en eller flere tillidstjenester, enten som en kvalificeret eller ikke-kvalificeret tillidstjenesteudbyder (§ 3, nr. 31).

**TILGÆNGELIGHED** Tilgængelighed betyder, at information og systemer er tilgængelige og operationelle, når de er nødvendige. Det indebærer, at systemer og data skal være beskyttet mod forstyrrelser, og at de skal kunne genoprettes hurtigt i tilfælde af nedbrud.