NIS 2

VEJLEDNING TIL NIS 2-LOVEN

LEDELSENS ROLLE OG OPGAVER

Denne vejledning skal hjælpe ledelsen i private og offentlige enheder med at opfylde kravene i NIS 2-loven

Styrelsen for Samfundssikkerhed

NIS 2-VEJLEDNING

Denne vejledning er udarbejdet af Styrelsen for Samfundssikkerhed. Vejledningen er generel og henvender sig til enheder i alle omfattede sektorer. Den kan suppleres af mere sektorspecifik vejledning ved den relevante sektoransvarlige myndighed. Det er i alle tilfælde den relevante sektoransvarlige myndighed, der vurderer, om en enhed lever op til forpligtelserne i NIS 2-loven.

Datavej 20
3460 Birkerød
Telefon: +45 4516 1666
E-mail: nis2@samsik.dk

1. udgave maj 2025.

Styrelsen for Samfundssikkerhed

INDHOLD

ORDLISTE

CYBERSIKKERHED
De aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler.

ENHED
En enhed er en virksomhed, forening, organisation eller offentlig myndighed mv. (juridisk person), som er tildelt et CVR-nummer.

CYBERSIKKERHEDSFORANSTALTNINGER
Tiltag, der fastholder og/eller ændrer en risiko. Omfatter både tekniske, operationelle og organisatoriske foranstaltninger. Bruges i vejledningen om de foranstaltninger, som en væsentlig eller vigtig enhed har truffet i medfør af § 6 i NIS 2-loven.

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 net-elementer, 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, elkabel-systemer, 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-systemer, IoT-enheder og it-infrastrukturkomponenter.

SEKTORANSVARLIGE MYNDIGHEDER
Begrebet beskriver den myndighed, der har ansvaret for de specifikke sektorer. De sektoransvarlige myndigheder udpeges pr. bekendtgørelse, inden NIS 2-loven træder i kraft. I NIS 2-loven bruges begrebet ”kompetente myndigheder”.

FORMÅL MED VEJLEDNINGEN

Cybersikkerhed er ledelsens ansvar. *Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau* (NIS 2-loven) stiller krav til medlemmer af ledelsesorganer i de enheder, som er omfattet af loven. Det er derfor vigtigt, at ledelsen[1] tager ejerskab for cybersikkerheden i deres organisation. Denne vejledning beskriver ledelsens opgaver og ansvar ift. styring af cybersikkerhedsrisici, krav til uddannelse samt de personlige sanktioner, som ledelsen i særlige tilfælde kan pådrage sig.

MÅLGRUPPE

Målgruppen for vejledningen er medlemmer af en bestyrelse og/eller en direktion i de virksomheder, organisationer og myndigheder (enheder), som er omfattet af NIS 2-loven.

LÆSEVEJLEDNING

Denne vejledning omhandler NIS 2-loven og beskriver således ikke sektorspecifikke forhold. Den forholder sig ikke til tele-, energi- og finanssektorerne, som har deres egen NIS 2-lovgivning. Vejledningen uddyber kravene til ledelsen i NIS 2-lovens § 7 og de særlige muligheder, der er for at sanktionere ledelsen efter NIS 2-lovens § 23. De sektoransvarlige myndigheder har ansvaret for at vejlede enheder inden for deres respektive sektorer og fører tilsyn med, at ledelsen i de relevante enheder lever op til lovens forpligtelser.

Vejledningen beskriver ikke ansvarsnormen eller praksis for håndhævelsen af ledelsesansvaret under dansk ret, som følger af selskabsretten, dansk rets uskrevne grundsætninger og god skik-regler formuleret af bl.a. Komitéen for God Selskabsledelse.

[1] Ledelsen, medlemmer af ledelsesorganet og ledelsesorganet bruges i denne vejledning som ensbetydende begreber.

1. HVORDAN ER LEDELSESBEGREBET DEFINERET I NIS 2-LOVEN?

Det siger NIS 2-loven:

§ 3, nr. 20 *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.

c) *For offentlige myndigheder er ledelsesorganet den øverste administrative ledelse i myndigheden.*

NIS 2-loven stiller krav til "ledelsesorganet" i væsentlige og vigtige enheder. Hvem der udgør ledelsesorganet afhænger af, om der er tale om en privat virksomhed/organisation eller en offentlig myndighed.

I PRIVATE VIRKSOMHEDER/ORGANISATIONER

I private virksomheder/organisationer er ledelsesorganet i NIS 2-loven defineret i overensstemmelse med definitionerne af henholdsvis det "centrale ledelsesorgan" i § 5, nr. 4 i *Lov om aktie- og anpartsselskaber, jf. lovbekendtgørelse nr. 1168 af 1. september 2023* (selskabsloven) og "ledelsen" i § 4 a, nr. 2 i *Lov om visse erhvervsdrivende virksomheder, jf. lovbekendtgørelse nr. 249 af 1. februar 2021* (LEV-loven).

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 af enhedens selskabsform. Selskabsloven finder alene anvendelse for aktie- og anpartsselskaber, 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 den enkelte enhed at vurdere deres virksomhedskonstruktion ift. selskabsloven eller LEV-loven.

I OFFENTLIGE MYNDIGHEDER

I offentlige myndigheder er ledelsesorganet den øverste administrative ledelse i myndigheden. Dette vil være direktionen for myndigheden eller andet ledelsesorgan på tilsvarende niveau.

I statslige myndigheder vil ledelsesorganet f.eks. være en direktion, hvis myndigheden har en direktion. I et departement, som ikke har en direktion, vil ledelsesorganet være departementschefen og vicedirektører/afdelingschefer. I en styrelse vil ledelsesorganet være direktionen. I regioner vil ledelsesorganet være koncerndirektionen eller tilsvarende. I kommuner vil ledelsesorganet være direktionen eller tilsvarende.

2. KAN LEDELSEN UDDELEGERE SINE OPGAVER?

Nogle virksomheder, organisationer og myndigheder har som en del af deres organisering etableret et cyber- og informationssikkerhedsudvalg, revisionsudvalg eller lignende med repræsentanter fra ledelsesorganet. Typisk varetager udvalgene opgaver vedr. styring og kontrol med enhedens cybersikkerhed. Ledelsesorganet kan uddelegere sine opgaver til denne type udvalg, 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 kravene til ledelsesorganet. Ledelsesorganet bør derfor overvåge og påse, at udvalget udfører opgaverne.

3. HVILKE KRAV ER DER TIL LEDELSENS STYRING AF CYBERSIKKERHEDSRISICI?

Det siger 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.

Ledelsesorganet har ansvaret for styringen af cybersikkerhedsrisici i deres virksomhed, organisation eller myndighed. Ansvaret skal ses i forlængelse af de opgaver, bestyrelsen har for risikostyring ifølge selskabslovens § 115, og kan sammenlignes med den opgave, bestyrelsen i øvrigt har ift. finansielle risici samt ikke-finansielle risici (f.eks. operationel risiko, teknologisk risiko m.m.). Ledelsesorganets opgaver ift. cybersikkerhed er således 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 bl.a., at ledelsen på et overordnet og strategisk niveau skal træffe beslutning om, hvilke foranstaltninger organisationen skal have, og hvornår beskyttelsen er tilstrækkelig.

For mere information om kravene til cybersikkerhedsforanstaltninger i NIS 2-loven, se vejledning om implementering af cybersikkerhedsforanstaltninger.

4. HVORDAN SKAL LEDELSEN FØRE TILSYN MED CYBERSIKKERHEDEN?

Ledelsesorganet i enheden skal føre tilsyn med, at de godkendte cybersikkerheds-foranstaltninger gennemføres og sikre, at foranstaltningerne har den fornødne effekt ift. de identificerede risici. Ledelsen skal derfor følge op på og føre kontrol med, at de sikkerhedstiltag, ledelsen 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. Ledelses-organet kan også føre tilsyn ved at etablere processer for intern revision, som rapporterer til ledelsen eller ved gennemførelse af ekstern revision af NIS 2-kravene, som rapporterer deres resultater til ledelsen.

EKSEMPEL

En direktion (ledelsesorganet) i en privat virksomhed modtager halvårligt ledelsesrapportering om virksomhedens arbejde med cyber- og informations-sikkerhed. I forbindelse med fremlæggelsen af rapporten tager ledelsen stilling til, hvorvidt der skal ske justeringer og evt. igangsættelse af yderligere tiltag med henblik på at styrke styringen af cyber- og informations-sikkerheden i virksomheden. Ledelsesrapporteringen indeholder en opfølgning på virksomhedens strategiske målsætninger og handleplaner for cyber- og informationssikkerhed samt aktuel status på en række målepunkter og indikatorer, som direktionen har besluttet at følge. Dette inkluderer bl.a. antallet af væsentlige hændelser i virksomheden og måltal for håndteringen af kritiske sårbarheder i enhedens net- og informationssytemer.

5. HVILKE KRAV STILLER NIS 2-LOVEN TIL LEDELSENS KOMPETENCER?

Det siger NIS 2-loven:

§ 7, 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 indholdskrav til kurserne, men uddannelseskravet 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. Det er ikke et krav, at alle eller et bestemt antal medlemmer af ledelsesorganet skal have gennemført kurser. Men ledelses-organet skal som kollektiv have de fornødne kompetencer til at styre cybersikkerheden i enheden.

Relevante kurser kan for eksempel være generelle kurser om cyber- og informations-sikkerhed, ledelseskurser og workshops om styring af cyber- og informationssikkerhedsrisici, kurser og certificeringer i anerkendte europæiske og internationale sikkerhedsstandarder eller enhedens egne internt tilrettelagte kurser og seminarer om cyber- og informationssikkerhed målrettet ledelsen. Uddannelsesaktiviteterne skal kunne dokumenteres f.eks. i form af kursusbevis eller bekræftelse på deltagelse i kursus.

LEDELSEN SKAL:

- Godkende foranstaltninger til styring af cybersikkerhedsrisici
- Føre tilsyn med implementeringen af foranstaltninger i enheden
- Gennemføre kurser med henblik på at have tilstrækkelig viden og kompetencer til styre enhedens cybersikkerhedsrisici
- Tilskynde til, at enheden tilbyder kurser til sine ansatte
- Tage ansvar for enhedens overholdelse af NIS 2-loven

6. HVILKEN ROLLE SPILLER LEDELSEN IFT. UDDANNELSE AF MEDARBEJDERE?

Ledelsen spiller en vigtig rolle for medarbejdernes kompetencer og adfærd. Ifølge § 7, stk. 2 i NIS 2-loven skal ledelsesorganet tilskynde til, at ansatte tilbydes kurser, svarende til dem, ledelsen selv gennemfører. 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. Politikken efter § 6. stk. 1, nr. 7 skal sikre, at medarbejderne har viden og færdigheder om cyber- og informationssikkerhed, som er passende i forhold til deres rolle og ansvar. Kravet om, at ledelsen skal tilskynde til, at ansatte tilbydes kurser, skal således ikke anses som et krav, der går videre end lovens § 6, stk. 1, nr. 7, men blot en understegning af, at medarbejdernes kompetencer og viden inden for cybersikkerhed er ledelsens ansvar.

For mere information om krav til uddannelse af medarbejdere, se vejledning om implementering af cybersikkerhedsforanstaltninger.

EKSEMPLER

1. I bestyrelsen (ledelsesorganet) for et privat selskab har to af medlemmerne viden om strategisk ledelse af cyber- og informationssikkerhed. Et af medlemmerne har gennemført en bestyrelsesuddannelse med fokus på styring af cybersikkerhedsrisici. Det andet bestyrelsesmedlem har en certificering i en relevant sikkerhedsstandard.

2. I en offentlig myndighed afholdes der en gang årligt et halvdages seminar for medlemmerne af myndighedens cyber- og informations-sikkerhedsudvalg, som inkluderer repræsentanter fra direktionen (ledelsesorganet). Myndigheden har selv tilrettelagt seminaret, som har fokus på trusselsbilledet, risikostyring og strategisk ledelse af cyber- og informationssikkerhed i offentlige myndigheder.

7. KAN LEDELSEN SANKTIONERES?

Det siger NIS 2-loven:

§ 23, stk.1 *Har én eller flere af 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.

Ledelsen skal være opmærksom på, at de 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. Denne sanktionsmulighed gælder ikke for ledelsen i offentlige myndigheder.

ANDRE RELEVANTE MATERIALER

Nedenfor fremgår en række vejlednings- og kommunikationsmaterialer, som kan være relevante i forhold til ledelsens rolle og opgaver. Materialet er til inspiration og er ikke udviklet med henblik på at opfylde specifikke lovkrav.

Sikkerdigital.dk
På sikkerdigital.dk kan virksomheder og myndigheder finde viden, vejledning og konkrete værktøjer til deres arbejde med cyber- og informationssikkerhed.

Bestyrelsesforeningen
Bestyrelsesforeningens Center for Cyberkompetencer har udarbejdet vejledning, anbefalinger og uddannelsestilbud målrettet bestyrelser og direktioners strategiske arbejde med cybersikkerhed.