Mapping

NIS2 og D-mærket

Få overblik over NIS2's minimumskrav og relationen til D-mærkets kriterier

Version 1.0.4

Hvem er omfattet af NIS2-direktivet?

NIS2-direktivet gælder som udgangspunkt for virksomheder og organisationer, der arbejder indenfor "sektorer af særligt kritisk betydning" eller "andre kritiske sektorer", og som leverer ydelser eller afvikler deres aktiviteter indenfor EU.

Kategorien "sektorer af særligt kritisk betydning" omfatter offentlige og private organisationer inden for følgende sektorer[1]:

1. Energi (elektricitet, fjernvarme og fjernkøling, olie, gas og brint)
2. Transport (luft, jernbane, vand og vejtransport)
3. Bankvirksomhed (kreditinstitutter)
4. Finansielle markedsinfrastrukturer (markedspladser)
5. Sundhed (sundhedstjenesteydere, producenter af lægemidler, medicinsk udstyr mv.)
6. Drikkevand
7. Spildevand
8. Digital infrastruktur (bl.a. udbydere af cloud ydelser, datacentre, domænenavnssystemer (DNS), topdomæneregistre (TLD) og offentlige kommunikationsnet- og tjenester)
9. Forvaltning af IKT-tjenester (business-to-business)
10. Offentlig forvaltning (undtagen Folketinget, domstolene og Nationalbanken)
11. Rummet (operatører af jordbaseret infrastruktur).

Kategorien "andre kritiske sektorer" omfatter offentlige og private organisationer inden for[2]:

1. Post- og kurertjenester
2. Affaldshåndtering
3. Fremstilling, produktion og distribution af kemikalier
4. Produktion, tilvirkning og distribution af fødevarer
5. Fremstilling af bl.a. medicinsk udstyr, computere, elektroniske og optiske produkter, elektrisk udstyr, maskiner, motorkøretøjer og andre transportmidler
6. Digitale udbydere (onlinemarkedspladser og -søgemaskiner samt platforme for sociale netværkstjenester)
7. Forskning (forskningsinstitutioner)

Direktivet skelner mellem henholdsvis "væsentlige enheder" og "vigtige enheder". Denne skelnen omhandler i hvilket omfang virksomheder og organisationer er kritiske for så vidt angår deres sektor eller den type tjenester, de leverer, samt deres størrelse.[3] Bemærk at NIS2-direktivet lægger op til, at SMV'er med under 50 FTE og en omsætning eller balance på under 10 mio. EUR som udgangspunkt ikke skal leve op til direktivets krav[4], hvilket svarer til kategorien "Micro" og "Small" i EU's SMV-definition[5] eller virksomhedsgruppe I og II i D-mærket[6].

[1] Bilag I, Sektorer af særligt kritisk betydning
[2] Bilag II, Andre kritiske sektorer
[3] Artikel 3, Væsentlige og vigtige enheder
[4] Artikel 2, Anvendelsesområde
[5] Artikel 2, stk. 1, i bilaget til henstilling 2003/361/EF samt European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, User guide to the SME definition, Publications Office, 2020, https://data.europa.eu/doi/10.2873/255862
[6] Virksomhedsgrupper | it-sikkerhed og data | D-mærket (d-maerket.dk)

At blive defineret som en "væsentlig enhed" kræver bl.a. at virksomheden eller organisationen arbejder indenfor sektorer af særlig kritisk betydning og overskrider tærsklerne for mellemstore virksomheder, som det fremgår i tabel 1 nedenfor.

Denne skelnen er relevant, da tilsyns- og håndhævelsesordningerne for hhv. "væsentlige" og "vigtige" virksomheder og organisationer differentieres for at sikre en fair balance mellem risikobaserede krav og forpligtelser på den ene side og på den anden side de administrative byrder, der følger af tilsynet med overholdelsen[7]. Se oversigt over hhv. sektorer og enheder samt tilsyn og håndhævelse i tabel 1 nedenfor.

Tabel 1: Overblik over anvendelsesområde og sektorer (artikel 2), væsentlige og vigtige enheder (artikel 3) samt tilsyn og håndhævelse (artikel 32 og 33)

	Sektorer af særlig kritisk betydning *(reference til bilag I)*	**Andre kritiske sektorer** *(reference til bilag II)*	**Tilsyn og håndhævelse** *(ref. til artikel 32–33)*
Art. 3, stk. 1 **Væsentlige enheder**	*Art. 3, stk. 1, litra a)* >250 personer (FTE) og har en årlig omsætning på over 50 mio. EUR eller en årlig samlet balance på over 43 mio. EUR. Se litra b)–g) for yderligere kriterier	*Art. 3, stk. 1, litra e)* Alle andre enheder af en type omhandlet i bilag I eller II, som en medlemsstat har identificeret som væsentlige enheder i medfør af artikel 2, stk. 2, litra b)-e)	*Art. 32* Løbende myndighedstilsyn såsom revision, sikkerhedsscanninger, rapportering og peer reviews *Art. 34* Bøder op til 10 mio. EUR eller 2 % af årsomsætning
Art. 3, stk. 2 **Vigtige enheder**	*Art. 3, stk. 2* Enheder af en type omhandlet i bilag I eller II, der ikke opfylder kriterierne for at være væsentlige enheder i henhold til artikel 3, stk. 1. Dette indbefatter enheder, som medlemsstaterne har identificeret som vigtige enheder i medfør af artikel 2, stk. 2, litra b)-e) *Art. 2, stk. 1* >50 personer (FTE) og en omsætning og/eller balance på over 10 mio. EUR		*Art. 33* Reaktiv tilgang til myndighedstilsyn, hvor tvungen revision og rapportering kun påkræves, hvis der er mistanke om, at virksomheden eller organisationen ikke lever op til kravene *Art. 34* Bøder op til 7 mio. EUR eller 1,4 % af årsomsætning

Kilde: egen tilvirkning

Udover de virksomheder og organisationer, der bliver direkte omfattet af NIS2-direktivet, vil en lang række virksomheder blive indirekte omfattet af direktivet, fordi de er leverandører til virksomheder i sektorer af særlig kritisk betydning eller andre kritiske sektorer. Læs mere om dette under afsnittet "NIS2-krav får konsekvens for underleverandører" senere i dette dokument.

[7] Artikel 32, Tilsyns- og håndhævelsesforanstaltninger vedrørende væsentlige enheder og artikel 33, Tilsyns- og håndhævelsesforanstaltninger vedrørende vigtige enheder samt bemærkning 122

Hvad er de væsentligste elementer i NIS2-direktivet?

NIS2-direktivet omfatter krav til ledelsesmæssig styring og forankring, risikostyring og tilhørende sikkerhedsforanstaltninger samt underretningspligt og desuden krav til håndhævelse, tilsyn og tilhørende sanktioner ved mangelfuld efterlevelse.

Skærpede krav til styring og forankring i ledelsen[8]

Med de nye regler stilles der skærpede krav til styring og forankring i ledelsen. Ledelsen får ansvar for at godkende foranstaltninger til styring af cybersikkerhedsrisici, føre tilsyn med dens gennemførelse og er ansvarlig for manglende overholdelse af krav og regler i NIS2-direktivet.

For at sikre de tilstrækkelige kompetencer skal ledelsesmedlemmer regelmæssigt følge konkrete kurser for at opnå tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på driften.

Minimumskrav til styring af cybersikkerhedsrisici[9]

Virksomheden eller organisationen skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre cybersikkerhedsrisici og forhindre eller begrænse skaderne i tilfælde af en sikkerhedshændelse.

NIS2-direktivet anviser 10 overordnede minimumskrav, som virksomheder og organisationer skal leve op til:

a) Politikker for risikoanalyse og informationssystemsikkerhed
b) Håndtering af hændelser
c) Driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring
d) Forsyningskædesikkerhed, herunder leverandørstyring/-sikkerhed
e) Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder
f) Politikker og procedurer (test og revision) til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici
g) Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse
h) Politikker og procedurer vedrørende brug af kryptografi, og hvor relevant, kryptering
i) Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
j) Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering mv., hvor relevant

[8] Artikel 20, Styring
[9] Artikel 21, Foranstaltninger til styring af cybersikkerhedsrisici

Rapporteringsforpligtelser[10]
Virksomheder eller organisationer omfattet af NIS2-direktivet skal hurtigst muligt og indenfor 24 timer underrette den kompetente myndighed (forventeligt Center for Cybersikkerhed i Danmark) om væsentlige hændelser og cybertrusler. Dernæst skal der indenfor 72 timer forelægge en "hændelsesunderretning" og endelig skal der udarbejdes en endelig rapport efter én måned.

En hændelse anses som væsentlig, hvis hændelsen eller cybertruslen (i) har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for virksomheden eller organisationen, eller (ii) hændelsen har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelige materielle eller immaterielle tab.

Hvis offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende væsentlig hændelse, eller hvor offentliggørelse af den væsentlige hændelse på anden vis er i offentlighedens interesse, kan myndighederne informere offentligheden om den væsentlige hændelse eller kræve, at virksomheden eller organisationen gør det.

Tilsyn, håndhævelse og sanktioner
Med implementeringen af NIS2-direktivet skal myndighederne udvide tilsynet både i dybden og bredden. I dybden, fordi tilsynsmyndigheder er forpligtet til at håndhæve kravene i direktivet, og i bredden, fordi omfanget af direktivet er udvidet til at gælde flere sektorer.

Som det fremgik i tabel 1 ovenfor, kan "væsentlige" virksomheder eller organisationer[11] forvente løbende tilsyn såsom revision, sikkerhedsscanninger, rapportering og peer reviews[12], mens "vigtige" virksomheder og organisationer[13] kan forvente tilsyn, tvungen revision og rapportering, hvis der er mistanke om, at virksomheden eller organisationen ikke lever op til kravene.

NIS2-direktivet giver mulighed for at forbyde personer med ledelsesansvar på direktionsniveau eller som juridisk repræsentant i den pågældende væsentlige virksomhed eller organisation at udøve ledelsesfunktioner i den pågældende virksomhed eller organisation[14].

NIS2-direktivet giver myndighederne mulighed for at give store bøder ved overtrædelse. Direktivet skelner i den forbindelse igen mellem væsentlige og vigtige virksomheder eller organisationer[15].

Som det fremgik i tabel 1 ovenfor, kan "vigtige" virksomheder eller organisationer risikere at skulle betale op til 7 mio. EUR eller 1,4 % af den globale årsomsætning og "væsentlige" virksomheder eller organisationer kan potentielt få bøder på op til 10 mio. EUR eller 2 % procent af den globale omsætning[16].

[10] Artikel 23, Rapporteringsforpligtelser
[11] Artikel 32, Tilsyns- og håndhævelsesforanstaltninger vedrørende væsentlige enheder
[12] Artikel 19, Peerevalueringer
[13] Artikel 33, Tilsyns- og håndhævelsesforanstaltninger vedrørende vigtige enheder
[14] Artikel 32, stk. 5, litra b
[15] Artikel 3, Væsentlige og vigtige enheder
[16] Artikel 34, Generelle betingelser for pålæggelse af administrative bøder til væsentlige og vigtige enheder

Brug D-mærket som standard til at leve op til NIS2's krav til styring og forankring i ledelsen samt minimumskrav

NIS2-direktivet tilskynder til, at virksomheder og organisationer bruger europæiske eller internationalt accepterede sikkerhedsstandarder eller EU-landenes egne nationale standarder for at sikre, at direktivet efterleves[17]. Det stemmer overens med D-mærket, som bygger på europæiske og internationalt anerkendte standarder og rammeværker[18].

Der er god overensstemmelse mellem D-mærkets kriterier og krav og NIS2-direktivets krav til hhv. styring og forankring i ledelsen samt krav til risikostyring og sikkerhedsforanstaltninger.

I tabel 2 nedenfor er angivet de krav til styring og forankring i ledelsen, som væsentlige og vigtige virksomheder og organisationer skal leve op til i NIS2-direktivet.

Tabel 2: Mapping mellem NIS2-direktivet, artikel 20 og D-mærket

Styringskrav i NIS2 (artikel 20)		**Kriterie i D-mærket (niveau 2)**	
Stk. 1	Ledelsesgodkendelse af foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, fører tilsyn med dens gennemførelse og gøres ansvarlige for enhedernes overtrædelser af forpligtelser til styring.	1.3	• Risikostyring
Stk. 2	Ledelsen er forpligtet til at følge kurser, og skal løbende tilbyde tilsvarende kurser til deres ansatte, således at de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, der leveres af virksomheden eller organisationen.	1.1 2.1 2.2	• Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse • Træn bestyrelsen og den øverste ledelse i sikkerhed, databeskyttelse og dataetik • Awareness om og træning i it-sikkerhed

I tabel 3 nedenfor er angivet de ti minimumskrav, som virksomheder og organisationer skal leve op til i NIS2-direktivet og disse kravs relation til relevante kriterier i D-mærket.

Tabel 3: Mapping mellem NIS2-direktivet, artikel 21 og D-mærket

Minimumskrav i NIS2 (artikel 21, stk. 2)		**Kriterie i D-mærket (niveau 2)**	
(a)	Politikker for risikoanalyse og informationssystemsikkerhed	1.2 1.3 1.4	• Overblik over data og systemer • Risikostyring • Politik for it-sikkerhed
(b)	Håndtering af hændelser	1.1 1.5	• Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse • It-beredskabsplan

[17] Artikel 25, Standardisering
[18] D-mærkets mapping til andre rammeværker og lovgivning | D-mærket (d-maerket.dk)

(c)	Driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring	1.1 1.2 1.5 3.6 3.7	• Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse • Overblik over data og systemer • It-beredskabsplan • Beskyttelse mod tab af vigtige og fortrolige data • Overvågning af systemaktivitet gennem logning
(d)	Forsyningskædesikkerhed, herunder leverandørstyring/-sikkerhed	4.1 4.2	• Leverandørlivscyklus og risikovurdering • Krav til it-sikkerhed hos leverandører
(e)	Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder	1.7 3.2 3.5 4.1 4.2 6.1 6.2 6.3	• Udviklingsproces • Korrekt konfiguration • Kontinuerlig opdatering af software og styresystemer • Leverandørlivscyklus og risikovurdering • Krav til it-sikkerhed hos leverandører • Vurdering af risici og behov i forbindelse med udvikling af produkter og tjenester • Privacy by design & default • Security by design & default
(f)	Politikker og procedurer (test og revision) til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici	1.1 1.3 1.4 1.5	• Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse • Risikostyring • Politik for it-sikkerhed • It-beredskabsplan • Bestået tilsyn i D-mærket
(g)	Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse	3.4 2.1 2.2	• Beskyttelse mod malware • Træn bestyrelsen og den øverste ledelse i sikkerhed, databeskyttelse og dataetik • Awareness om og træning i it-sikkerhed
(h)	Politikker og procedurer relateret til kryptografi, og hvor relevant, kryptering	1.4 1.6 3.1 6.1 6.2 6.3	• Politik for it-sikkerhed • Politikker for ansvarlig dataanvendelse • Netværkssikkerhed og kryptering • Vurdering af risici og behov i forbindelse med udvikling af produkter og tjenester • Privacy by design & default • Security by design & default
(i)	Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver	1.2 2.1 2.2 3.3	• Overblik over data og systemer • Træn bestyrelsen og den øverste ledelse i sikkerhed, databeskyttelse og dataetik • Awareness om og træning i it-sikkerhed • Beskyttelse af administrative brugerkonti

(j)	Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering mv., hvor relevant	3.1 3.3	• Netværkssikkerhed og kryptering • Beskyttelse af administrative brugeradgange

D-mærket følger den kommende udmøntning af NIS2

D-mærket vil sikre, at virksomheder ved at blive D-mærket vil leve op til den kommende danske udmøntning af NIS2 – hvis de har behovet for det.

D-mærket vil sikre, at de virksomheder, som bliver omfattet af NIS2, vil falde i D-mærkets gruppe III og gruppe IV[19]. Virksomheder indplaceret her vil leve op til krav til styring og forankring i ledelsen samt minimumskravene i NIS2.

I takt med, at NIS2 implementeres i både EU og i Danmark, vil D-mærket løbende blive tilpasset, så virksomheder med behov for at leve op til den danske NIS2-udmøntning vil gøre det ved at være D-mærket.

Det vil ske gennem en kombination af dialog med relevante myndigheder om den danske udmøntning, et særskilt NIS2-modul i D-mærket, som sikrer opfyldelse af minimumskravene i NIS2 (artikel 20, 21 og 23) og den kommende danske udmøntning, samt tilpasning af D-mærkets kriterier.

D-mærkets digitale mapping-værktøj bliver løbende opdateret i takt med viden om den danske udmøntning af NIS2, så virksomhederne kun behøver at gå ét sted hen for at holde sig ajour. Her kan virksomheder se, hvordan D-mærket som samlet standard relaterer sig til NIS2, og hvordan virksomhedens egen gruppeindplacering og kriterietildeling i D-mærket relaterer sig til NIS2.

D-mærket vil desuden proaktivt oplyse virksomheder, for hvem NIS2 er relevant, om eventuelt behov for yderligere handling for at leve op til minimumskravene i NIS2. Det sker ved at gøre mapping-værktøjet til en integreret del af D-mærkets selvevalueringsværktøj og udvikle et særskilt NIS2-modul, som sikrer opfyldelse af minimumskravene i NIS2 og den kommende danske udmøntning – også hvis den bliver sektorspecifik.

Myndighederne forventes at føre løbende tilsyn med væsentlige virksomheder og organisationer

Som det fremgår i tabel 1 ovenfor, så forventes myndighederne at føre løbende tilsyn med de virksomheder og organisationer, der benævnes som væsentlige. Det indebærer at myndighederne vil fokusere deres tilsynsindsats på virksomheder over 250 personer (FTE) og en årlig omsætning på over 50 mio. EUR eller en årlig samlet balance på over 43 mio. som opererer i sektorer af særlig kritisk betydning.

D-mærket er særlig relevant for "vigtige enheder"

Som det fremgår i tabel 1 ovenfor, så forventes myndighederne at have en reaktiv tilgang til myndighedstilsyn overfor "vigtige enheder". D-mærket kan hermed udfylde en rolle, der kan bistå myndighederne i sikring af efterlevelse af NIS2 for

[19] Virksomhedsgrupper | D-mærket | it-sikkerhed og data (d-maerket.dk)

vigtige virksomheder og organisationer, og disse virksomheder og organisationer kan anvende D-mærket til proaktivt at differentiere sig i forhold til deres konkurrenter indenfor "vigtige enheder" ved at blive D-mærket.

NIS2-krav får konsekvens for underleverandører

Som det fremgår af tabel 3 ovenfor, er et af NIS2-direktivets minimumskrav Forsyningskædesikkerhed, herunder leverandørstyring/-sikkerhed. Herved bliver en lang række virksomheder indirekte omfattet af NIS2-direktivet, fordi de er leverandører til virksomheder i sektorer af særlig kritisk betydning eller andre kritiske sektorer, fx energi, transport, drikke- og spildevand, digital infrastruktur eller fødevarer.

D-mærket kan med fordel anvendes i denne kunde-leverandør-relation. Kunden kan bruge D-mærket som ramme for at stille krav til leverandøren, og leverandøren kan bruge D-mærket som bevis for, at de overholder krav til it-sikkerhed og ansvarlig dataanvendelse. Dermed kan D-mærket bidrage til at skabe en konkurrencefordel for leverandører til NIS2-omfattede virksomheder og samtidig øge trygheden hos den NIS2-omfattede kunde.

Kun myndighederne kan garantere efterlevelse ved NIS2-tilsyn

En garanti for efterlevelse ved tilsyn kan kun myndighederne stille – det gælder for NIS2 og for alle andre myndighedstilsyn. En virksomhed eller organisation kan altså ikke bestå et myndighedstilsyn alene ved at fremvise et D-mærke.

Hvad skal din virksomhed gøre for at forberede sig på NIS2?

1. Bliv oprettet i D-mærkets gratis selvevalueringsværktøj og få overblik over din virksomheds eller organisations udfordringer og nødvendige indsatsområder. Direkte link til oprettelse her og læs om processen her.
2. Skab opbakning fra ledelsen, så der bliver afsat de rette ressourcer og brug D-mærket som styringsramme gennem hele processen. Læs, hvordan det anbefales at organisere arbejdet med D-mærket.
3. Kom godt i gang og book gratis online opstarts- eller sparringsmøde her.
4. Brug processen i D-mærkets selvevaluering til at implementere nødvendige tiltag samt at få dokumenteret kriterier og krav.
5. Hold dig opdateret i sammenhængen mellem NIS2 og D-mærket i D-mærkets digitale mapping-værktøj.
6. Gå i tilsyn og få D-mærket, så I har en 3. parts vurdering af jeres it-sikkerhed og ansvarlige dataanvendelse.
7. Rapportér til Center for Cybersikkerhed ved relevante sikkerhedshændelser
8. Hold øje med nyheder på D-mærkets LinkedIn eller tilmeld dig D-mærkets nyhedsbrev i bunden af hjemmesiden, hvor vi løbende vil kommunikere om NIS2 i forhold til D-mærket.