Nye krav inden for cyber- og informationssikkerhed

Hvilken betydning har NIS2 for din virksomhed?

TD-K White Paper

TD-K white paper: *Nye krav inden for cyber- og informationssikkerhed - Hvilken betydning har NIS2 for din virksomhed,* © februar 2024

Hvad er NIS2-direktivet, og bliver din virksomhed omfattet af det?

Den 10. november 2022 vedtog Europa-Parlamentet NIS2-direktivet, som sigter mod at sikre et højt fælles niveau for net- og informationssikkerhed i Europa. Direktivet er rettet mod virksomheder og organisationer, der spiller en afgørende rolle i samfundets funktion og leverer tjenester, som er vitale for vores dagligdag.

De omfattede virksomheder opdeles i to grupper: *Væsentlige enheder** og *vigtige enheder**. Forskellen mellem de to grupper afspejler sig i tilsynsførelsen og sanktionsniveauet ved overtrædelse af kravene.

Download direktivet

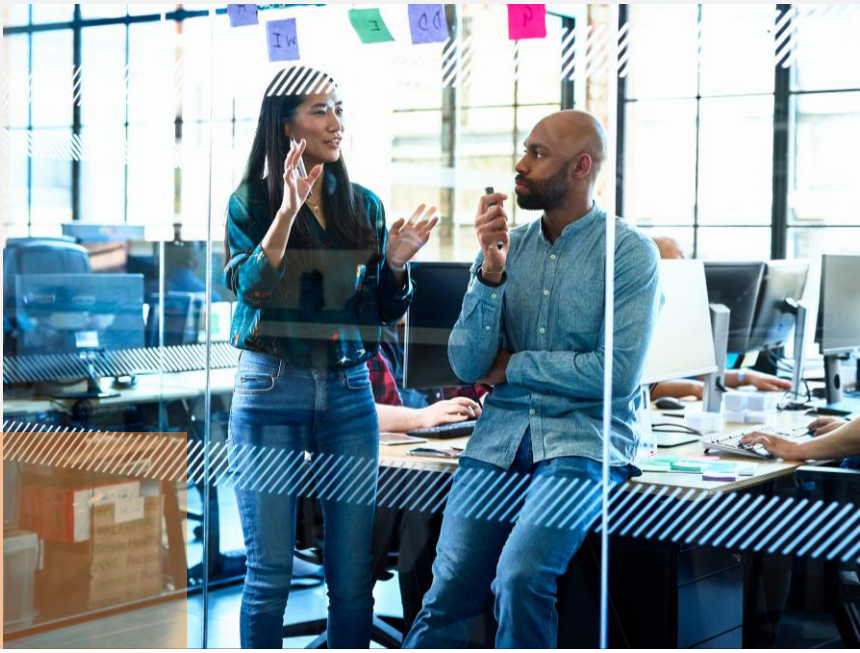
*Væsentlige enheder = særligt kritiske sektorer

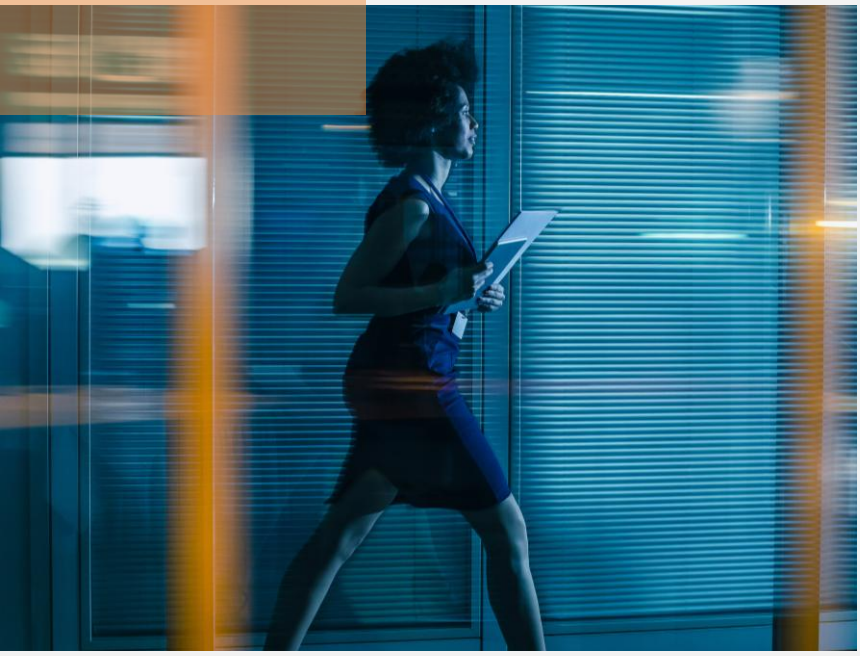
Vigtige enheder = kritiske sektorer

Væsentlige enheder

Energi	Væsentlig
Transport	Væsentlig
Bankvirksomhed	Væsentlig
Finansielle markedsinfrastruktur	Væsentlig
Sundhedssektoren	Væsentlig
Drikke- og spildevand	Væsentlig
Digital infrastruktur	Væsentlig
Informations- og kommunikationstjenesteudbydere	Væsentlig
Offentlig forvaltning	Væsentlig
Rummet	Væsentlig
Udbydere af Managed Services & Managed Security Services	Væsentlig

Se detaljeret liste





Vigtige enheder

Post- og kurertjenester	Vigtig
Affaldshåndtering	Vigtig
Forskning	Vigtig
Fremstilling, produktion og distribution af kemikalier	Vigtig
Fremstilling, bearbejdning og distribution af fødevarer	Vigtig
Udbydere af visse digitale tjenester	Vigtig
Fremstilling af bl.a. elektronik, maskiner og motorkøretøjer	Vigtig

Se detaljeret liste

Krav til sikkerhed i NIS2-direktivet

Med implementeringen af NIS2, vil ledelsen være forpligtet til at deltage i ansvaret for sikkerheden, og der vil være krav om implementering af tiltag som risikovurderinger, beredskabsplaner og awareness-træning af medarbejderne. Virksomheder skal desuden kunne dokumentere, at de nye tiltag gennemføres, og de har fremover pligt til at indberette kritiske hændelser, ligesom det er tilfældet med GDPR i dag, men under mere skærpede forhold. Sidst men ikke mindst skal virksomhederne kunne dokumentere, at de opfylder alle kravene i praksis. Disse dokumentationskrav vil kræve en ny tilgang til sikkerhedsstruktur for mange af de berørte virksomheder.

De vigtigste krav

Figur: Overblik over de vigtigste NIS2-krav

Hvilke krav stiller NIS2?

NIS2 stiller omfattende krav til ledelse, risikostyring, forretningskontinuitet og rapportering:

1. Ledelsen skal være bekendt med kravene og har direkte ansvar for håndtering af cyberrisici og overholdelse af NIS2-kravene.

2. Øgede krav til risikostyring og implementering af skadesforebyggende og -begrænsende foranstaltninger for at der reducerer risici og konsekvenser.

3. Forretningskontinuitet skal sikres gennem genoprettelsesprocedurer, nødprocedurer og etablering af en kriseorganisation.

4. Korrekt rapportering til myndighederne. Der stilles blandt andet krav til, at større hændelser rapporteres inden for 24 timer.

Tilsyn og sanktioner under NIS2-direktivet

Med implementeringen af NIS2 udvides myndighedernes tilsyn både i dybden og bredden. Virksomheder, der hører under *væsentlige enheder*, kan forvente løbende tilsyn og peer reviews. Virksomheder, der hører under *vigtige enheder* kan forvente tilsyn og tvungne revisioner ved mistanke om kravovertrædelser. Sanktioner kan omfatte bøder, tvungne revisioner og sanktionering af ledelse.

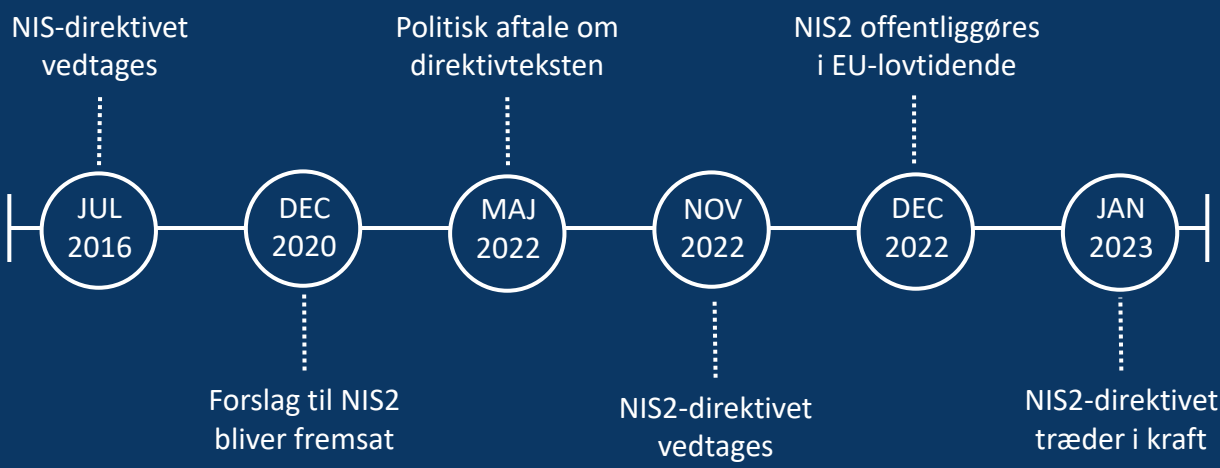
- **Væsentlige enheder** kan blive pålagt bøder på op til 10 mio. euro eller 2% af den globale årlige omsætning.

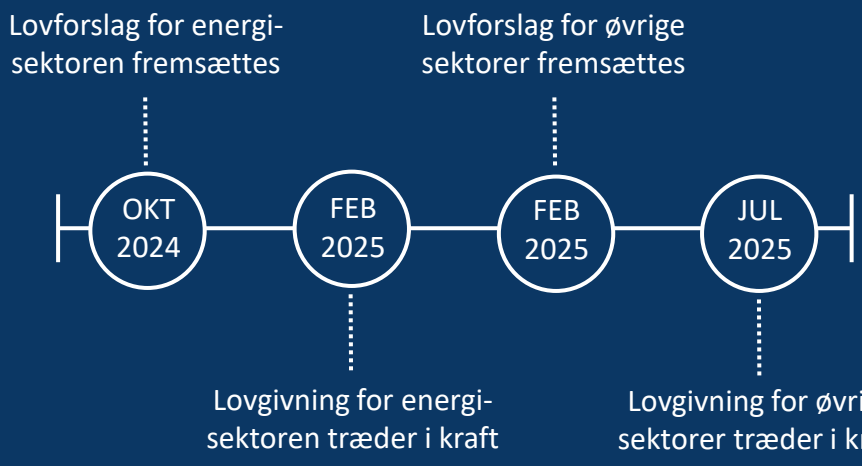
- **Vigtige enheder** kan få bøder på op til 7 mio. euro eller 1,4% af den globale årlige omsætning.

Hvornår træder NIS2 i kraft?

NIS2-direktivet blev formelt vedtaget den 10. november 2022 og blev annonceret i EU-tidende den 27. december 2022. Det betyder, at direktivet trådte i kraft den 18. januar 2023 (20 dage efter annonceringen). Fra denne dato har EU-landene en frist på 18 måneder til at få NIS2-implementeret i deres lovgivning. Den danske lovgivning skulle således senest træde i kraft den 18. oktober 2024, men Forsvarsministeriet har oplyst, at den danske lovgivning bliver forsinket, og at EU's implementeringsfrist dermed overskrides.

NIS2-tidslinje





Ifølge Ministeriet for Samfundssikkerhed og Beredskab forventes lovgivningen at træde i kraft den 1. juli 2025. En særskilt lov for energisektoren, som har til formål at implementere NIS2- og CER-direktiverne samt styrke beredskabet i energisektoren, blev dog fremsat i oktober 2024. Dette betyder, at lovgivningen for energisektoren træder i kraft den 1. februar 2025.

Hvad kan I gøre nu?

Indtil myndighederne får styr på den danske lovgivning, anbefaler vi at I går i gang med minimumskravene i NIS2. Vi ved allerede nu, at nedenstående krav, som minimum skal implementeres i dansk lovgivning:

- **Risikovurdering:** Udfør en grundig risikovurdering af jeres IT- og OT-miljøer. Udform en plan for at håndtere og minimere de identificerede risici.
- **Beredskabsplan:** Udarbejd en beredskabsplan, så I har styr på proceduren ved tilfælde af en sikkerhedshændelse.
- **Netværkssikkerhed:** Udarbejd sikkerhedsprocedurer for jeres netværk, herunder opdatering og patching.
- **Sikring af forsyningskæden:** Undersøg og sikr, at jeres leverandører op til NIS2-kravene.
- **Politikker for kryptering**: Etabler retningslinjer der styrer, hvordan I skal anvende kryptering for at beskytte jer mod uautoriseret adgang og misbrug.

- **Forretningskontinuitet:** Få styr på backup og genskabelse af data
- **Multifaktor brugeridentifikation:** Implementer MFA, så jeres medarbejdere skal bekræfte deres identitet ved hjælp af mindst to forskellige metoder.
- **Styring af brugerrettigheder:** Udarbejd procedurer for hvem der må få adgang til hvilke netværksressourcer.
- **Asset Management:** Lav en liste over alt jeres hardware som PC'er, servere og netværksenheder, softwareapplikationer m.m.
- **Basal sikkerhedshygiejne:** Opgaver som at opdatere software regelmæssigt, awarenes-træning af medarbejdere m.m.
- **Kontinuerlig revision og forbedring**: Gennemgå og revider jeres NIS2-overholdelse regelmæssigt for at sikre, at I fortsat opfylder direktivets krav.

For en vellykket NIS2-implementering anbefaler vi, at I tager udgangspunkt i internationale standarder som f.eks. CIS V8. En sådan standard kan fungere som en solid retningslinje for at opbygge et robust sikkerhedssystem. Samtidig, hvis jeres virksomhed ikke har tilstrækkelige ressourcer eller ekspertise til at arbejde med NIS2 internt, anbefaler vi at udlicitere arbejdet til en ekstern NIS2-leverandør for at sikre en gnidningsløs og effektiv implementering af direktivets krav.

Governance

Betegnelsen *governance* eller *IT-styring* i NIS2 refererer til den proces, hvormed organisationer bliver styret, ledet og administreret for at opnå deres mål. Det omfatter de strukturer, politikker, procedurer og praksisser, der skal være på plads for at sikre, at organisationen fungerer effektivt, overholder lovgivningen og opretholder et højt niveau af ansvarlighed over for sine interessenter. NIS2-direktivet kræver en solid integration både i organisationens ledelse og i dens daglige drift.

I NIS2-direktivet er det ledelsens ansvar, at der etableres passende strategier, politikker og ressourcer til at beskytte organisationens netværk og informationssystemer. Dette opnås gennem udarbejdelse og implementering af IT-strategien gennem en lang række obligatoriske dokumenter. Dokumenterne bør udarbejdes i henhold til kendte IT-sikkerhedsstandarder som CISv8, ISO27001 eller IEC62443.

Effektiv NIS2-dokumentation

Til højre ses en liste over de nødvendige dokumenter, der skal udarbejdes i forbindelse med en NIS2-revision. Dette er en omfattende opgave, der kræver betydelige ressourcer. Derfor har TD-K udviklet en intuitiv dokumentationsplatform, der indeholder skabeloner til alle relevante NIS2-dokumenter. Virksomheden kan selv udfylde skabelonerne, eller TD-K kan bistå med denne opgave. Med TD-Ks dokumentationsmodul kan virksomheden samle, organisere og administrere al NIS2-relateret dokumentation ét centralt sted.

Dokumentationsbehov

IT-sikkerhedspolitik Krav til IT-sikkerheden, gyldighedsområde og mål.	**Håndtering og anmeldelse** Procedure inkl. ansvar, kontaktlister m.m.
IT-sikkerhedshåndbog Krav til konfiguration, drift og anvendelse.	**Ansættelsesprocedure** Procedure for sikkerhedsforskrifter- og uddannelse.
Risikopolitik Håndtering af risici og definition af risikovillighed.	**Afskedigelsesprocedure** Procedure for orientering om fortsat fortrolighed.
Risikovurdering Vurdering af alle kritiske IT-systemer og trusler.	**Godkendelsesprocedure** Procedure for f.eks. adgange, rettigheder m.m.
Risiko handlingsplan Udførlig plan med tiltag for at mindske risici.	**Procedure for sletning af data** Procedure for sikker sletning af data.
Sårbarhedsanalyse Teknisk IT-gennemgang for kendte sårbarheder.	**Uddannelse af medarbejdere i IT-sikkerhed** Procedure for løbende videreuddannelse.
Beredskabsstrategi Kravene til et IT-beredskab, defineret af ledelsen.	**Registre** Række af procedurer til sikring af sikkerhedsniveau.
Beredskabsplan Konkret plan for indsatsen ved et cyberangreb.	**CMDB** Alle HW SW og data aktiver inkl. ejerskab/ansvar.
Leverandørpolitik Sikkerhedskrav til leverandører.	**Leverandørregister** Register over vigtige leverandører inkl. serviceaftale.
Sikkerhedskrav til applikationer Sikkerhedskrav ved anskaffelse af applikationer.	**Risikoregister** Register over alle identificerede risici.
Personalehåndbog Tilretning med krav til IT-sikkerhed/fortrolighed.	**Brugeradgange** Register over brugeradgange til alle applikationer.
Ansættelseskontrakter Tilretning omkring IT-sikkerhed/fortrolighed.	**Kontaktliste for hændelsesstyring** Liste over alle interne/eksterne kontaktpersoner.
Procedurer Procedurer til sikring af defineret sikkerhedsniveau.	**Årshjul** Kalender med aktiviteter der skal udføres periodisk.

Vælg den rigtige samarbejdspartner til jeres NIS2-kontrol

Det rette valg af samarbejdspartner til jeres NIS2-kontrol kan være afgørende for jeres virksomheds evne til at overleve et potentielt cyberangreb. Det handler ikke kun om at opfylde kravene på papiret, men også om at sikre, at jeres IT- og OT-miljøer er effektivt beskyttet i praksis. Før I indgår en aftale med en NIS2-kontrolvirksomhed, er der flere vigtige faktorer, I bør overveje nøje for at sikre det bedst mulige samarbejde og beskyttelse af jeres forretningskritiske systemer og data.

Tre essentielle spørgsmål, I bør stille jeres NIS2-leverandør, før I indgår et samarbejde

1. Sker der en reel kontrol af IT- og OT-udstyr?

   Eller er det blot en informationsindsamling fra jer selv og jeres leverandører? At sende et spørgeskema til en nuværende leverandør svarer til at bede dem læse korrektur på en tekst, de selv har skrevet. Vælg derfor en NIS2-leverandør, der kan undersøge jeres IT-/OT-infrastruktur, herunder servere, netværksudstyr, adgange og andre enheder – med andre ord, en leverandør, der udfører en ægte audit.

2. Er der indbygget automatiserede sårbarhedsscannere og teknisk audit i virksomhedens compliance-værktøj?

   For at imødekomme NIS2-kravene er det nødvendigt med en kontinuerlig overvågning, kontrol og scanning af alle tilknyttede kritiske enheder i IT- og OT-netværket, herunder de interne procedurer der knytter sig til disse.

3. Er kontrolvirksomheden uvildig?

   Det er vigtigt, at kontrollen er så transparant og uvildig som muligt i forhold til kontroller og analyser. En kontrolvirksomhed kan samarbejde med IT- og OT-leverandører, men bør ikke have økonomiske incitamentsaftaler med dem.

NIS2-direktivet er kompliceret.

Lad TD-K gøre det enkelt!

Jeres IT- og OT-miljø skal være i stand til at modstå et reelt cyberangreb i praksis, og ikke kun på papiret. Vores NIS2-kontrol er udviklet netop med fokus på at tilføje den afgørende tekniske dimension, der giver jer de bedste forudsætninger for at modstå et cyberangreb. Samtidig får I omfattende dokumentation for, at I overholder NIS2-direktivet. Vi påtager os hele opgaven med NIS2 og friholder derfor jer og jeres leverandører for at udføre NIS2-kontroller på egne systemer.

Figur: TD-K's NIS2-process

Processen

Sådan hjælper TD-K jer gennem NIS2

1. **Discovery:** Grundig gennemgang af jeres IT- og OT-infrastruktur for at identificere trusler og risici.

2. **Due Diligence:** Undersøgelse af de eksisterende sikkerhedsforanstaltninger baseret på opdagelser i Discovery-fasen.

3. **GAP-analyse:** Der udfærdiges en rapport af TD-K's teknikere, der beskriver, hvordan NIS2-kravene opfyldes.

4. **Mitigering:** Iværksættelse af foranstaltninger baseret på GAP-analysen for at imødekomme NIS2-kravene.

5. **NIS2-audit:** TD-K kontrollerer efterfølgende systemerne igen for at sikre, at alle punkter fra GAP-analysen nu opfyldes.

6. **NIS2-rapport:** Udarbejdelse af en uvildig rapport, der dokumenterer og bekræfter fuld NIS2-overholdelse.

Kraftfuldt værktøj: Compliance Manager

Vi forstår udfordringen ved at navigere gennem det komplekse landskab af krav og retningslinjer i NIS2. TD-Ks Compliance Manager er designet med netop dette for øje! Compliance Manager er et værktøj og online portal, som sikrer, at I altid er opdateret med de seneste regler og regulativer, så I kan fokusere på jeres kerneforretning. En af de mest kraftfulde funktioner i Compliance Manager er evnen til at generere omfattende rapporter og dokumentation. Dette er afgørende, når I skal rapportere til myndighederne eller vise overholdelsesstatus til interessenter.

Via Compliance Managers brugervenlige dashboard får I øjeblikkelig indsigt i, hvor jeres virksomhed befinder sig i forhold til kravene. I kan hurtigt identificere områder, der kræver opmærksomhed og træffe de nødvendige foranstaltninger for at forblive i overensstemmelse med lovgivningen. Compliance Manager har indbygget sårbarhedsscanning, så I hurtigt kan foretage en risikovurdering.

Brug også Compliance Manager til overholdelse af GDPR

I kan også bruge Compliance Manager til at sikre overholdelse af GDPR. Med vores omfattende værktøj kan I håndtere GDPR-kravene på en struktureret og effektiv måde. Compliance Manager giver jer mulighed for at identificere og adressere potentielle compliance-problemer i forhold til GDPR og tage de nødvendige skridt for at sikre overholdelse af databeskyttelsesreglerne.

Billede: Compliance Manager giver et fuldt overblik over jeres NIS2-status

Mitigering

Under en NIS2-revision vil der typisk blive identificeret sårbarheder, som det er virksomhedens eget ansvar at implementere foranstaltninger imod. Dette kaldes også mitigering. Hos TD-K adskiller vi os fra andre NIS2-leverandører i landet, da vi besidder de nødvendige tekniske kompetencer inden for både IT, OT og dokumentation, hvilket også gør os i stand til at hjælpe jer med denne del af NIS2-arbejdet. Hvis I har ekspertisen internt, kan I naturligvis selv udføre denne opgave, eller alternativt kan TD-K hjælpe jer enten helt eller delvist. Et samarbejde med TD-K bringer jer således helt i mål med jeres NIS2-efterlevelse.

Hovedkontor

Rugbjergvej 10, 4623 Lille Skensved

Afdeling Sydsjælland

Køgevej 18, 4700 Næstved

Afdeling Vestsjælland

Norvangen 3D, 4220 Korsør

Afdeling Jylland

Hjulmagervej 4A, 7100 Vejle

Telefon
+45 70 26 69 00

Mail
info@td-k.dk