NIS2 – Hvad betyder det for din virksomhed?

Nyt cyberdirektiv

Forbered din virksomhed på skærpede lovkrav til cyber- og informationssikkerhed.

Mentor it
- med dig i fremtiden

Hvad er NIS2-direktivet?

Europa-Parlamentet har vedtaget et nyt NIS2-direktiv, som indeholder skærpede lovkrav til cyber- og informationssikkerhed i udvalgte sektorer. Det nye direktiv bliver også gældende for danske virksomheder og organisationer.

Direktivet regulerer kravene til cybersikkerhed for at strømline sikkerhedsniveauet på tværs af medlemslandene.

Læs mere:
https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985

Gælder NIS2-direktivet for min virksomhed?

De omfattede virksomheder opdeles i to grupper: essentielle og vigtige sektorer. Forskellen på de to grupper ligger i tilsynsførelsen og bødeniveauet ved eventuelle overtrædelse af krav om sikkerhedsforanstaltninger samt anmeldelsespligt.

De omfattede sektorer er:
Energi, transport, finansielle virksomheder og markedsinfrastruktur, sundhed, drikkevand, spildevand, digital infrastruktur og udbydere, offentlig forvaltning, rumaktivitet, post, affaldshåndtering, kemikalier, fødevarer, uddannelse og forskning.

Sektor

Energi – forsyning, distribution, transmission og salg af energi	Essentiel
Transport via luft, jernbane, vej og sø	Essentiel
Finans - kredit, handel, marked og infrastruktur	Essentiel
Sundhed – forskning, produktion, udbydere og fremstillere af udstyr	Essentiel
Drikke- og spildevand	Essentiel
Digital infrastruktur – DNS, tillidstjenester, datacentertjenester, cloud computing, kommunikationstjenester (tele- og net), udbydere af managed services og managed security services	Essentiel
Offentlig administration, kommuner og regioner	Essentiel
Rumfart – software og services	Essentiel

Sektor

Post- og pakkeservice	Vigtig
Affaldshåndtering	Vigtig
Kemiske produkter – fremstilling og distribution	Vigtig
Fødevare - fremstilling, distribution og produktion	Vigtig
Fremstilling/produktion af pharma, elektronik, optisk udstyr, maskineri, køretøjer	Vigtig
Udbydere af online markedspladser, søgemaskiner, sociale platforme	Vigtig

Kilde: PwC Technology & Security

Hvilke krav stiller NIS2?

Det nye NIS2-direktiv fra Europa-Parlamentet skærper kravene til cyber- og informationssikkerhed til såkaldte essentielle og vigtige virksomheder.

NIS2 stiller nye krav inden for fire hovedområder:

- Virksomhedens ledelse skal være be-kendt med de nye krav i NIS2. Ledelsen kan desuden stilles til ansvar for indsatser vedrørende risikostyring, altså identificering og håndtering af cyberrisici.

- Der skal foreligge processer for rapportering til relevante myndigheder. Større hændelser skal rapporteres inden for 24 timer.

- De øgede krav til risikostyring omfatter blandt andet forebyggelse og redskaber til begrænsning af risiko og konsekvenser ved sikkerhedbrud. Minimumskravene er fx adgangskontrol, kryptering, netværkssikkerhed og sikring af forsyningskæder.

- Din virksomhed skal sikre driften af samfundskritiske aktiver i tilfælde af sikkerhedshændelser. Der skal foreligge procedurer for genopretning af systemer og etablering af en kriseorganisation.

Direktivet indfører syv nye minimumskrav til:

- politikker for risikoanalyse og informationssystemsikkerhed.

- håndtering af hændelser (forebyggelse, opdagelse og reaktion på hændelser).

- driftskontinuitet og krisestyring.

- sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.

- politikker og procedurer (test og revision) til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.

- brug af kryptografi og kryptering.

- forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forbindelserne mellem den enkelte enhed og dens leverandører eller tjenesteydere såsom leverandører af data-lagrings- og databehandlingstjenester eller forvaltede sikkerhedstjenester.

Kilde: Dansk Industri og PwC Technology & Security

Hvornår træder NIS2 i kraft?

Fra starten af 2024 er de omfattede virksomheder i medlemslandene forpligtet til at efterleve kravene. Det er derfor en fordel at komme i gang med at optimere dit IT-setup nu.

Virksomheder og organisationer i de omfattede sektorer er selv forpligtede til at være opmærksomme på retningslinjer og lovkrav i det nye direktiv.

Hos Mentor IT står vi klar til at hjælpe dig og din virksomhed med at blive klar i tide.

Hvordan håndhæves og sanktioneres NIS2?

Essentielle virksomheder risikerer bødestraf på op til 10 millioner euro eller 2 procent af den globale årlige omsætning.

Vigtige virksomheder risikerer bødestraf på op til 7 millioner euro eller 1,4 procent af den globale årlige omsætning.

Det nye direktiv understreger desuden, at ledelsen i en omfattet virksomhed kan stilles til ansvar for brud på sikkerheds- og anmeldelsespligten.

Ledelsen skal derfor gennemgå kurser for at kunne vurdere cybersikkerhedsrisici. Ledelsen skal samtidig opfordre og tilbyde alle medarbejdere lignende kurser regelmæssigt.

Trin for trin

Sådan bliver din virksomhed klar til nye lovkrav til cybersikkerhed

NIS2-direktivet udvider og skærper både krav og sanktionering af cybersikkerhed. Virksomheder i de omfattede sektorer skal nu forholde sig endnu mere til blandt andet risikostyring, kontrol og tilsyn.

Hvad skal du gøre? Og hvor skal du starte? Det kan virke som en uoverskuelig opgave at sætte sig ind i de nye lovkrav – og ikke mindst at lave de nødvendige risikovurderinger.

Men det behøver det slet ikke at være. Hos Mentor IT står vores IT-eksperter klar til at hjælpe. Først og fremmest har vi lavet en trin-for-trin-guide til dig lige her – men du er også altid velkommen til at kontakte os direkte på **70 122 123** eller **info@mentor-it.dk**.

1. Modenhedsvurdering

Trin 1 handler om jeres organisation. Hvad vil det kræve at efterleve de nye krav i NIS2? Vurderingen giver et konkret og samtidigt billede af, hvad der allerede efterleves, samt hvor din virksomhed skal i gang med at finde løsninger.

Hos Mentor IT anbefaler vi, at modenhedsvurderingen laves af eksterne konsulenter. Eksempelvis vores IT-eksperter.

Vurderingen beskriver de investeringer og kompetencer, som din virksomhed får brug for, hvis I skal i mål med implementeringen af de nye NIS2-krav.

2. Identificér driftskritiske aktiver

Formålet med NCIS2 er at beskytte den kritiske infrastruktur i EU-medlemslandene. Det gælder eksempelvis forsyningskæder og andre samfundsvigtige funktioner.

Direktivet omfatter driftskritiske processer, medarbejdere, teknologi og leverandører. Det er derfor et helt centralt trin i implementeringen.

3. Byg efter internationale standarder

NIS2-direktivet kræver, at virksomhederne implementerer et såkaldt ledelsessystem for cyber- og informationssikkerhed (fx. ISMS).

Når din virksomhed skal i gang med implementeringen af nye krav fra NIS2 – og måske større ændringer i jeres IT-setup, anbefaler vi, at I lader jer guide af internationale standarder. Lad eksempelvis ISO 27001, NIST eller IEC sætte rammerne.

Opbygningen af et effektivt ledelsessystem kræver opdaterede politikker for procedurer og processer. Og I skal desuden definere roller og ansvar, risiko og målsætninger.

4. Risikovurdering

Med det nye NIS2-direktiv skal din virksomhed fremadrettet arbejde mere risikobaseret, når det kommer til cyber- og informationssikkerhed.

I skal beskrive jeres risikoproces, og den bedste måde at komme i gang med den, er en grundig risikovurdering.

Vurderingen laves på de aktiver, som I tidligere i processen har defineret som driftskritiske.

Til risikovurderingen hører også risikohåndtering – og ikke mindst forebyggende tiltag i virksomheden som awareness-træning.

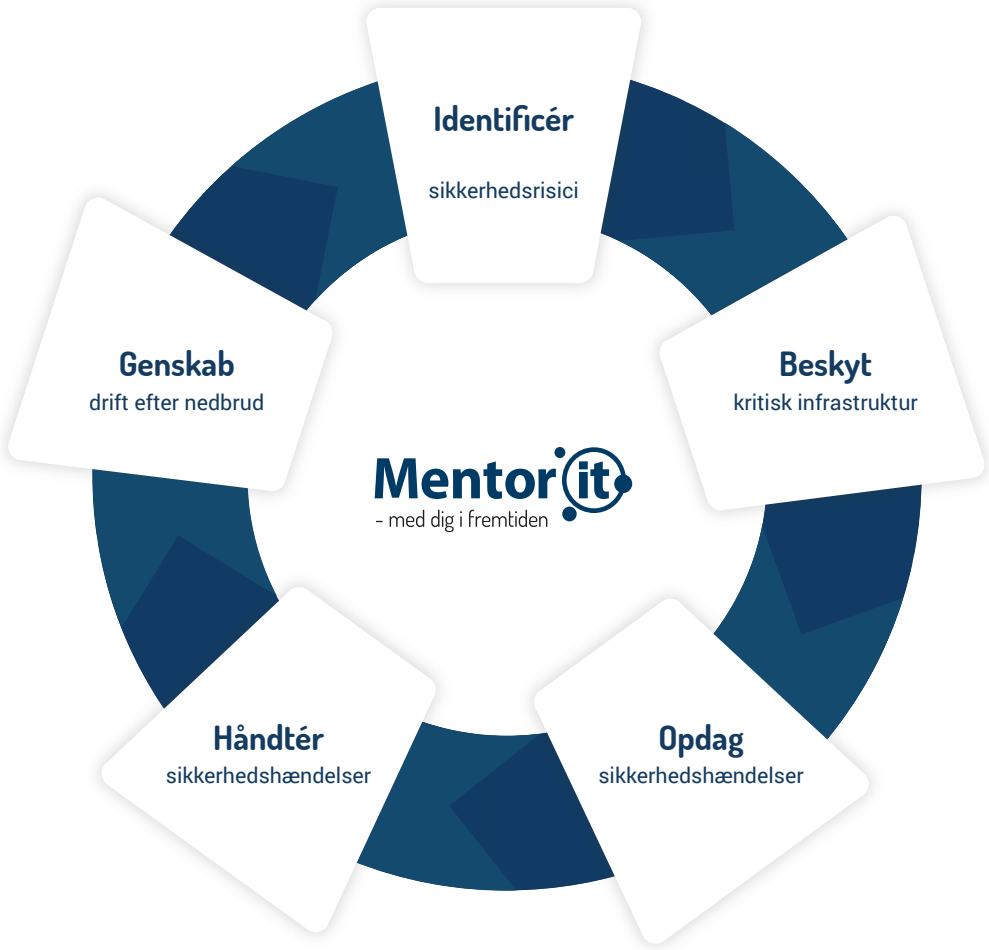
5. Rapportering

Ifølge det nye direktiv har du som virksomhed anmeldelsespligt. Hvis din virksomhed oplever en væsentlig sikkerhedshændelse, skal den rapporteres til en relevant myndighed eller CSIRT, som etableres af medlemslandene, inden for 24 timer.
Herudover skal den relevante myndighed eller CSIRT opdateres med en vurdering af hændelsen og eventuel kompromittering.

6. Gør det hele igen – og igen

Fremadrettet skal du og din virksomhed tænke på cyber- og informationssikkerhed som en mere cirkulær proces. Cybertruslerne er i kontant forandring – og det bør dit risikoberedskab derfor også være.

Gentag jævnligt jeres vurderinger af modenhed og risiko. Hvor er I udsatte? Er der kommet nye og måske bedre løsninger? Eller nye trusler?



“Det væsentligste er at få styr på sin virksomheds mange procedurer og håndteringen af disse. Lav et overblik – hvilke procedurer har I, og hvilke lægger NIS2 op til. Er der mangler, bør der laves en plan, så hullerne lukkes”

- Jesper Ungermann Christensen,
Quality Assurance & Compliance Manager hos Mentor IT

5 gode råd

1. Få sikret, at udførende af givne procedurer kender til, at de findes og er uddannet i udførelse.
2. Udfør test af de mest væsentlige procedurer. Fx beredskabsprocedure/Major Incident procedure.
3. Kortlæg risici og udarbejd risikovurdering på hver enkelt risiko.
4. Hold styr på hvem, der (udefra) forsøger på hvad og evt. hvilke sårbarheder, der findes på netværket.
5. Vær opmærksom på, hvilke sårbarheder/trusler der er i omløb og hvordan disse kan ramme jer.


Mentor it

I tvivl?

Har du spørgsmål, eller du det mindste i tvivl om, hvordan du og dine kollegaer bedst navigerer rundt i det nye direktiv, så sig endelig til. Vi hjælper gerne med at gøre din virksomhed klar til NIS2.

God fornøjelse!

Mentor IT Esbjerg
Mentor IT Kolding
Mentor IT København
Mentor IT Aarhus

Telefon 70 122 123
E-mail info@mentor-it.dk

Mentor it
- med dig i fremtiden