Rådet for Digital Sikkerhed

08.03.2021

Rådet for Digital Sikkerheds overblik over NIS 2 - Direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS2)

I 2018 blev den første EU-lovgivning om cyber- og informationssikkerhed vedtaget. Den – NIS2 – havde fokus på de samfundskritiske sektorer. Med NIS2 udvides de berørte sektorer væsentligt. Med direktivet følger en række krav til virksomhederne, herunder at tilsynsførende myndighed gennemfører revision og tilsyn med virksomhederne. Væsentlige bøder til virksomhederne kan følge i forlængelse i de tilfælde, hvor virksomhederne ikke lever op til de gældende krav.

Formålet med denne vejledning er at skabe et overblik over, hvem der er berørt af direktivet og informere de berørte virksomheder om, hvilke krav der følger, og som virksomhederne skal leve op til.

Baggrund og formål

EU-direktivet om sikkerhed i net- og informationssystemer, det såkaldte NIS-direktiv (NIS1) blev vedtaget i 2018. Formålet var at øge cyber- og informationssikkerheden på tværs af EU ved at stille en række tekniske og organisatoriske krav til virksomheder i de berørte sektorer og dermed også sikre en harmonisering af sikkerheden på tværs af EU.

Direktivet stiller krav om, at operatører af samfundskritiske tjenester (tele-, finans-, energi-, sundheds-, transport- og søfartssektoren) træffer foranstaltninger til at håndtere sikkerheden i de net- og informationssystemer, som de anvender ved levering af deres tjenester. Valget af disse sektorer skyldes, at der er store samfundsmæssige risici forbundet med angreb på særligt de kritiske samfundssektorer. Danmark er kommet langt med implementeringen af NIS-direktivet. Der er udarbejdet sektorstrategier og organisering af faste samarbejder mellem myndigheder og decentrale cyber- og informationssikkerhedsenheder (DCIS'er) i seks udpegede samfundskritiske sektorer. DCIS'er er ansvarlige for informationsudveksling og validering af information mellem sektorerne og Center for Cybersikkerhed samt vedligeholdelsen af risiko- og sårbarhedsvurderinger. Dette er en ressourcekrævende opgave for de berørte virksomheder. En væsentlig gevinst er deling af viden og erfaring omkring det aktuelle trusselsbillede og relevante foranstaltninger. NIS1 har herved bidraget til at øge cybersikkerheden i de samfundskritiske sektorer væsentligt

Med NIS2 ønsker man en yderligere harmonisering af cybersikkerheden på tværs af EU. NIS2 udvider antallet af berørte sektorer til at inkludere fx post- og kurertjenester, affaldshåndtering, fremstilling og distribution af fødevarer og kemikalier samt flere typer produktion og betydelige dele af den offentlige forvaltning. Langt flere virksomheder forpligtes til at indgå i samarbejder med myndighederne om indberetning af sikkerhedstrusler og -hændelser m.m. NIS 2 lægger sig desuden, på en række områder, metodisk op ad GDPR-lovgivningen. Direktivet forventes færdigbehandlet ved udgangen af 2021, hvorefter der vil være en 18 måneders implementeringsperiode.

Formålet med denne vejledning er at skabe et overblik over, hvem der er berørt af direktivet samt informere virksomheder i de berørte sektorer om, hvilke krav der følger, og som virksomhederne skal leve op til.

Hvilke sektorer berøres

Direktivet udvider omfanget af den nuværende NIS betydeligt, og langt flere sektorer og virksomheder berøreres. De nye sektorer er tilføjet baseret på deres kritiske betydning for økonomi og samfund.

Kritiske enheder	Vigtige enheder
Energi (elektricitet, fjernvarme, olie, gas og brint)	Post og kurertjenester
Transport (luft, jernbane, vand og vejtransport)	Affaldshåndtering
Bankvæsen og finansielle markedsinfrastrukturer	Fremstilling og distribution af kemikalier
Sundhed	Fremstilling (medicinsk udstyr, computere, elektrisk udstyr, motorkøretøjer, transportmidler)
Drikkevand og spildevand	Fødevareproduktion, forarbejdning og distribution
Digital infrastruktur (fx udbydere af internet, DNS, cloud, datacenter og indholdsleveringsnetværk)	Digitale udbydere (online markedspladser, søgemaskiner og sociale netværkstjenester)
Offentlig forvaltning rummet (centralregering, offentlig forvaltning) og rummet (operatører af jordbaseret infrastruktur).	

Tabel 1:Oversigt over berørte virksomheder – for nærmere information se bilag 1- Berørte virksomheder

Alle mellemstore- og store virksomheder[1] indenfor de ovenstående sektorer er berørt – det vil sige, hvis en virksomhed har over 50+ ansatte eller en omsætning på mere end EUR 10 millioner. Ligeledes kan nogle mikro-virksomheder også være omfattet, hvis de vurderes at have tilstrækkelig kritisk betydning for samfundet. Der kan være særregulering fx inden for finansområdet.

Det er et minimums direktiv, og der kan nationalt stilles større krav til virksomhederne.

Risikobaseret vurdering og ledelsens rolle

Et væsentligt skift fra tidligere er det stærke fokus på ledelsesansvar – cyber- og informationssikkerhed er ledelsens ansvar. Ledelsen skal godkende risikostyring og er ansvarlig for bl.a. at sikre den nødvendige uddannelse af medarbejdere.

[1] Mikrovirksomheder og små enheder som omhandlet i Kommissionens henstilling 2003/361/EF af 6. maj 2003 er udelukket fra direktivets anvendelsesområde, undtagen udbydere af elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, tillidstjenesteudbydere, topdomænenavneregistraturer og offentlig forvaltning samt visse andre enheder såsom den eneste udbyder af en tjeneste i en medlemsstat

Ledelsen af kritiske og vigtige enheder skal godkende foranstaltninger til styring af cybersikkerhedsrisiko. Ledelsen skal føre tilsyn med implementering af foranstaltningerne, og den er ligeledes ansvarlig for evt. manglende overholdelse. Ledelsen skal sikre sig tilstrækkelig viden og færdigheder til at forstå og vurdere risikostyring af cybersikkerhed og konsekvenserne for deres forretning og virksomhedens aktiviteter.

Ledelsen skal sikre en række risikobaserede foranstaltninger, der omfatter:

- risikoanalyse og ledelsessystem til styring af informationssikkerheden
- håndtering af hændelser (forebyggelse, afsløring og reaktion på hændelser)
- forretningskontinuitet og krisestyring
- forsyningskædesikkerhed inklusiv sikkerhedsrelaterede aspekter ifm. forholdet mellem hver enhed, dens leverandører eller tjenesteudbydere såsom udbydere af dataopbevaring, databehandling eller tjenester til håndtering af sikkerhed
- sikkerhed i netværks- og informationssystemer: udvikling og vedligeholdelse, herunder sårbarhedsvurderinger, håndtering og videregivelse
- politikker og procedurer (test og revision) til vurdering af, hvor effektiv indsatsen er
- kryptering

Rapporteringsforpligtelse

Virksomhederne der berøres af direktivet, skal underrette de relevante ansvarlige myndigheder om hændelser af væsentlig betydning for levering virksomhedens samfundskritiske tjenester inden for 24 timer. Ligeledes skal modtagerne af tjenesten informeres om enhver væsentlig hændelse. Man skal ligeledes informere sine kunder samt indsende en *endelig rapport* senest én måned efter anmeldelsen. Den skal indeholde:

1. en detaljeret beskrivelse af hændelsen, dens sværhedsgrad og indvirkning
2. den type trussel eller grundårsag, der sandsynligvis udløste hændelsen
3. anvendte og igangværende afbødende foranstaltninger

Bødestørrelse

NIS-bøder gælder for både kritiske og vigtige virksomheder og har EU-bredt basislinje på 10 mio. € eller 2% af den samlede omsætning. Ligeledes giver NIS2 den ansvarlige myndighed mulighed for midlertidigt at standse en virksomheds aktiviteter og endda fjerne en CEO fra sin stilling, hvis denne ikke har sikret, at virksomheden tilfredsstillende overholdelse af de krav der følger af NIS2.

Tilsyn med de berørte virksomheder:

Med NIS2 skrues der yderligere op for kontrollen, og igen vil der være fokus på en risiko baseret tilgang. For *de kritiske* enheder skal tilsynet sikre, at enheden har sikkerheden på plads. For *de vigtige* enheder kan tilsynet pålægge enheden at få styr på sin sikkerhed.

Tilsyn af de kritiske enheder indebærer:

- ”On site” inspektioner og off site tilsyn, herunder stikprøvekontrol
- regelmæssige revisioner - målrettede sikkerhedsrevisioner baseret på risikovurderinger eller risikorelaterede tilgængelige informationer
- sikkerhedsscanninger baseret på objektive og gennemsigtige risikovurderingskriterier
- anmodninger om oplysninger der er nødvendige for, at tilsynet kan vurdere de implementerede sikkerhedsforanstaltninger herunder dokumentere cybersikkerhedspolitikker, overholdelse af forpligtelsen til underrette;
- anmodninger om adgang til data, dokumenter eller alle nødvendige oplysninger til udførelse af deres tilsynsopgaver
- anmodninger om bevis for gennemførelsen af cybersikkerhedspolitikker fx resultater af sikkerhedsrevision foretaget af revisor og den respektive underliggende dokumentation

Tilsyn af de vigtige enheder indebærer efterfølgende tilsynsforanstaltninger:

- ”on site” inspektioner og efterfølgende opfølgning
- sikkerhedsrevisioner baseret på risikovurderinger/risikorelaterede tilgængelige informationer;
- sikkerhedsscanninger baseret på objektive og gennemsigtige risikovurderingskriterier
- anmodninger om alle nødvendige oplysninger til at vurdere efterfølgende sikkerhedsforanstaltninger, herunder dokumenteret cybersikkerhedspolitikker såvel overholdelse af meddelelsespligten overfor ENISA;
- anmodninger om adgang til data, dokumenter og / eller nødvendige oplysninger til udførelse af tilsynsopgaverne

Hvad er de næste skridt – hvornår rammer NIS2 virksomhederne?

EU-Kommissionen reviderer NIS direktiv (NIS2) i offentlig høring, som løber frem til den 18. marts. Herefter kommer de med deres endelige version. Herefter skal det vedtages af Kommissionen og offentliggøres i EU-tidende. Herefter har medlemslande 18 måneder til at implementere direktivet.