IMPLEMENTERING AF NIS-DIREKTIVET:

NYE KRAV TIL SIKKERHEDEN I NET- OG INFORMATIONSSYSTEMER

Databeskyttelsesreglerne er ikke de eneste regler indført i maj 2018, der skærpede kravene til it-sikkerheden. Implementeringen af det såkaldte NIS-direktiv i dansk ret har indført en række forpligtelser i forhold til sikkerhed i net- og informationssystemerne, som navnlig forsyningsvirksomheder, offentlige myndigheder m.fl. i sundhedssektoren og andre operatører af væsentlige tjenester bør være opmærksomme på.

Den 6. juli 2016 vedtog EU-Parlamentet direktiv 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen. Formålet med direktivet, der ofte omtales som NIS-direktivet, er at harmonisere og skærpe reglerne om sikkerhed ved at stille nye krav til sikkerhed i net- og informationssystemer hos visse forsyningsvirksomheder og andre såkaldte operatører af væsentlige tjenester samt udbydere af digitale tjenester. Nu er NIS-direktivet implementeret i dansk ret.

IMPLEMENTERINGEN AF NIS-DIREKTIVET

Implementeringen af NIS-direktivet er gennemført via flere love og bekendtgørelser fra maj 2018 med forskellige administrerende myndigheder.

Det skyldes, at lovgiver har valgt at opdele administrationen af reglerne i forhold til de berørte sektorer på de forskellige relevante ministerier.

HVILKE ORGANISATIONER ER OMFATTET AF KRAVENE?

Formålet med den nye NIS-lovgivning er at harmonisere og skærpe medlemsstaternes regler om sikkerhed for kritisk infrastruktur i erkendelse af, at sikkerhedshændelser udgør en hyppig trussel for net- og informationssystemer, og at disse sikkerhedshændelser kan få afgørende økonomiske og samfundsmæssige konsekvenser.

Af denne årsag indfører NIS-lovgivningen specifikke forpligtelser for "operatører af væsentlige tjenester" og "udbydere af digitale tjenester". Begrebet *"operatører af væsentlige tjenester"* omfatter operatører, der leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter inden for sektorerne for drikkevandsforsyning og -distribution, energi (el, olie og gas), transport, bankvæsen, sundhed samt finansiel og digital infrastruktur.

Det er desuden et krav, at leveringen af tjenesten afhænger af net- og informationssystemer, og at en sikkerhedshændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Myndighederne vil mindst hvert andet år udpege de virksomheder i hver sektor og delsektor, der opfylder betingelserne for at være operatører af væsentlige tjenester.

Miljø- og Fødevareministeriet har meldt ud, at ingen vandforsyninger betragtes som "operatører af væsentlige tjenester", da drikkevand kan leveres uafhængigt af net- og informationssystemer. Denne vurdering tages op til revision senest i 2020.

For sundhedssektoren gælder, at alle operatører af væsentlige tjenester selv skal foretage anmeldelse af de væsentlige tjenester, som de er ansvarlige for, hos Sundhedsdatastyrelsen. Dermed vil det i første omgang være op til den enkelte organisation at vurdere, hvorvidt organisationen er omfattet af reglerne. Sundhedsdatastyrelsen har til dette formål udarbejdet en tilhørende vejledning til loven, hvoraf fremgår, at en operatør af en væsentlig tjeneste kan være kommuner, regioner, privatpraktiserende læger og speciallæger, apoteker og lignende.

Begrebet *"udbydere af digitale tjenester"* er afgrænset til udbydere af digitale tjenester af typen onlinemarkedspladser, onlinesøgemaskiner eller cloud computing-tjenester i Danmark. I modsætning til operatører af væsentlige tjenester, hvor myndighederne udpeger virksomhederne, er det i første omgang op til virksomhederne selv at vurdere, hvorvidt deres ydelser falder ind under disse typer af tjenester.

Udbydere af digitale tjenester, der beskæftiger under 50 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 10 millioner euro, er dog ikke omfattet af reglerne.

SIKKERHEDSKRAV

Den nye lovgivning styrker beskyttelsen af kritisk infrastruktur og tvinger en række organisationer, herunder visse forsyningsvirksomheder, til at have større fokus på it-sikkerheden. Det indebærer således også, at risikostyring skal tænkes bedre ind i organisationernes forretningsgange.

En operatør af væsentlige tjenester har navnlig pligt til at træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i de net- og informationssystemer, som anvendes til aktiviteterne. Under hensyntagen til teknologiens aktuelle stade skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står mål med risikoen.

Til dette formål stiller de fleste myndigheder krav om, at organisationen gennemfører en risikovurdering, der skal tage stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i de væsentlige tjenester, samt udarbejder en ledelsesgodkendt net- og sikkerhedspolitik med udgangspunkt i en anerkendt international standard.

For udbydere af digitale tjenester gælder i hovedtræk samme regler, men de påkrævede sikkerhedsforanstaltninger er lempeligere end for operatører af væsentlige tjenester.

Kravene til sikkerhedsniveauet afspejler, at lovgiver har vurderet, at graden af risiko, som tjenesterne udsættes for, er lavere ved digitale tjenester end ved de tjenester, som er af væsentlig betydning for opretholdelsen af vigtige økonomiske og samfundsmæssige aktiviteter.

UNDERRETNINGSPLIGT

Både operatører af væsentlige tjenester og udbydere af digitale tjenester har desuden pligt til hurtigst muligt at underrette den relevante myndighed og Center for Cybersikkerhed om visse hændelser.

Operatører af væsentlige tjenester skal underrette om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer, hvorimod udbydere af digitale tjenester skal underrette om hændelser med betydelige konsekvenser for leveringen af deres tjenester.

De enkelte regler indeholder nærmere information om, hvornår underretningspligten skal iagttages, og hvilken information der skal videregives. Underretningen af hændelser skal ske via virk.dk.

AFLEDTE KONSEKVENSER FOR ANDRE ORGANISATIONER

Ansvaret for at sikre sikkerheden i net- og informationssystemer er placeret hos selve operatøren eller udbyderen, men også andre organisationer kan ikke undgå at blive påvirket af reglerne.

Operatøren eller udbyderen skal således også sikre, at deres leverandører opretholder en tilsvarende sikkerhed i forhold til driftsleverancer. Det er samtidig nødvendigt, at operatøren eller udbyderen forholder sig til hele forsyningskæden, inklusive sikkerheden i forbindelse med tredjepartsleverandører og underkontrahenter for at sikre et tilstrækkeligt sikkerhedsniveau. De nye krav i NIS-lovgivningen bliver derfor også relevante for aktører, der leverer ydelser til organisationer omfattet af reglerne.

Tilsvarende er det relevant for offentlige og private aktører at vide, om deres leverandører af f.eks. cloud-tjenester er underlagt NIS-lovgivningen. Ved udbud og indgåelse af kontrakter bør de offentlige og private aktører forholde sig til, om og i givet fald hvordan der bør tages højde for dette.

SAMMENHÆNGEN MED DATABESKYTTELSESREGLERNE

NIS-lovgivningen har tæt sammenhæng med databeskyttelsesreglerne, der stiller lignende krav om underretning ved sikkerhedsbrud, risikoanalyse og indførelse af passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risiciene for personoplysningerne. Kravene i NIS-lovgivningen går dog videre end kravene i databeskyttelseslovgivningen, idet kravene også skal iagttages, selvom de berørte net- og informationssystemer ikke benyttes til at behandle personoplysninger.

Overtrædelser af reglerne i NIS-lovgivningen kan straffes med bøde ■

Mads Nygaard Madsen
Advokat, partner
mnm@horten.dk

Charlotte Kunckel
Specialistadvokat
cku@horten.dk

Maria Pilh Arendsdorf Bengtsen
Advokatfuldmægtig
mpB@horten.dk