Rådet for
Digital Sikkerhed

22. august 2024

Forsvarsministeriet
fmn@fmn.dk med kopi til jhb@fmn.dk
Sagsnummer 2024/004461

Svar på høring om forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (implementering af EU's NIS2-direktiv i dansk ret)

Rådet for Digital Sikkerhed takker for muligheden for at afgive bemærkninger til implementeringen af NIS2 i dansk ret. Selvom Forsvarsministeriet i høringsudkastet understreger, at det kommende lovforslag vil læne sig meget tæt af NIS2-direktivets systematik og definitioner, skal Rådet takke for et gennemarbejdet udkast, hvor navnlig lovbemærkningerne giver et oplysende overblik.

Rådet bakker fuldt op om NIS2-direktivets og udkastets hensigt om at højne cybersikkerhedsniveauet i Danmark og EU, herunder de retlige tiltag, der er lagt op til for at ensarte indsatsen på tværs af de samfundskritiske sektorer og landegrænserne. Det er i den forbindelse vigtigt, at der er fokus på en harmoniseret implementering på tværs af EU-landene – for det første af hensyn til konkurrencen, for det andet af hensyn til gensidig tillid mellem aktørerne, og for det tredje fordi den digitale integration ikke er mere sikker end det svageste led i leverandør- og samarbejdskæderne.

Rådet bemærker forventningen om, at direktivet og den kommende danske lov vil omfatte ca. 2000 virksomheder, myndigheder og organisationer, hvilket er markant flere end de ca. 150 enheder, der var omfattet af NIS1-direktivet. Implementeringsomkostningerne i offentligt regi forventes i størrelsesordenen 260-500 mio. kr., mens de erhvervsøkonomiske konsekvenser ventes at være 2,6-3 mia. kr.

Tallene indikerer, at implementeringsopgaven er stor, hvilket tydeliggør det store behov for åbenhed og vejledning i implementeringsfasen. Rådet deltager gerne i denne proces, og skal opfordre til, at Forsvarsministeriet, Center for Cybersikkerhed og andre centrale myndigheder allerede parallelt med Folketingets beslutningsproces inviterer til dialog med centrale aktører på feltet. Rådet bidrager gerne til denne proces. Implementeringslovens ikrafttræden ventes 1. marts 2025, godt 4 måneder efter direktivets frist, så jo før, jo bedre.

Rådet bemærker, at der i Danmark lægges op til en delvis decentral governance-struktur, hvor bekendtgørelser med sektorspecifikke bestemmelser om blandt andet foranstaltninger til styring af cybersikkerhedsrisici skal forhandles af vedkommende ressortministerium med Forsvarsministeriets Center for Cybersikkerhed for at sikre ensartethed og koordination på tværs af sektorer. Rådet skal opfordre til at der afsættes passende ressourcer til dette arbejde, og at navnlig denne del af implementeringsfasen sker i åben dialog, jf. ovenfor.

Herudover vil Rådet fremhæve følgende opmærksomhedspunkter i tilknytning til implementeringen mv.:

Lovgivningsmæssig usikkerhed
NIS2-lovgivningen, tilgrænsende lovgivning og de uddybende bekendtgørelser rummer betydelige risici for uensartethed og dermed uklarhed på tværs af de berørte sektorer. Rådet skal derfor opfordre til, at man fra regeringens side sikrer, at tilgrænsende lovgivning behandles i en koordineret beslutningsproces i Folketinget.

Rådet er således opmærksom på, at NIS2-direktivets implementering i dansk lov fra Forsvarsministeriets side er udsendt i høring samtidigt med implementeringen af CER-direktivet om kritiske enheders modstandsdygtighed. På Klima-, Energi- og Forsyningsministerens område implementeres NIS2- og CER-direktiverne særskilt via et lovforslag, som er udarbejdet i Energistyrelsen. For at sikre størst mulig ensartethed mellem lovteksterne og de kommende forpligtelser for de berørte virksomheder, skal Rådet opfordre til, at lovbehandlingen af de i alt 3 lovforslag i Folketinget koordineres i videst mulige omfang. Særligt i forhold til de samfundskritiske virksomheders leverandørkæder kan arbejdet med at sikre implementeringen af overlappende lovgivning i kontraktstyringen og det konkrete samarbejde blive kompleks og unødig omkostningsfuld.

Rådet skal i denne forbindelse bemærke, at vedtagelsen af L 122 (maj 2024), der blandt andet gennemførte EU-regulering på cybersikkerhedsområdet i den finansielle sektor (den såkaldte DORA-forordning), selvsagt ikke er omfattet af bemærkningen ovenfor. Derimod bør en eventuel kommende ændring af telelovgivningen, som følge af NIS2-direktivet, ske med fokus på at skabe størst mulighed ensartethed og klarhed på tværs af de berørte sektorer.

Usikkerhed i forhold til om en virksomhed er omfattet af lovgivningen
Direktivet og lovforslaget har detaljerede bestemmelser om sektorer, virksomhedstyper og aktiviteter, der omfattes af reglerne. Som led i udformningen af bekendtgørelserne samt den forestående vejledningsopgave, bør det overvejes at etablere en mulighed for navnlig mindre virksomheder at få vurderet, om deres service er omfattet af reglerne og det kommende tilsyn. Der kan fx være tale om virksomheder, der varetager kritiske funktioner eller underleverandører til virksomheder, der tydeligt er omfattet, hvor der kan være grobund for tvivl om, hvorvidt den pågældende leverance så også er omfattet.

I den forbindelse vurderer Rådet, at den foreslåede selvregistreringsordning kan vise sig at fungere uhensigtsmæssigt med risiko for unødig tvivl og bureaukrati hos mange virksomheder såvel som de kompetente myndigheder, navnlig på grund af de upræcise branchedefinitioner mv. i lovudkastet. Rådet anbefaler derfor, at der i udarbejdes mere præcise branchedefinitioner og vejledninger, samt at der etableres mulighed for, at virksomheder kan henvende sig til relevante sektormyndigheder for at få afklaring af, hvorvidt de er omfattet af reglerne.

Etablering af forhåndsgodkendelse af sikkerhedsforanstaltninger
I lyset af, at ca. 2000 virksomheder vil blive omfattet af de detaljerede krav om ledelsesansvar, risikovurdering og etablering af sikkerhedsforanstaltninger, bør det overvejes om der kan etableres en form for forhåndsgodkendelse eller proaktivt sikkerhedseftersyn efter forespørgsel. Rådet er selvsagt opmærksom på, at en sådan ordning ikke kan fritage en virksomhed for efterfølgende ansvarspådragelse, hvis det viser sig, at den ikke lever op til sin egen sikkerhedspolitik, -organisation og -foranstaltninger, men omvendt vil en 'foreløbig' forhåndsgodkendelse skabe afklaring i forhold til, om virksomheden i det hele

taget er omfattet af reglerne. Det skal således understreges, at der bør være vandtætte skotter mellem den foreslåede forhåndsgodkendelse og det egentlige tilsyn.

Rådet vurderer, at en form for forhåndsgodkendelse samlet set forbedre sikkerhedsberedskabet, lette virksomhedernes usikkerhed og administrative byrde samt ikke mindst reducere behovet for reaktive tilsyn. Også for de virksomheder, hvor det viser sig, at de ikke er omfattet af NIS2-reglerne, vil ordningen have en positiv betydning for beredskabet. I tråd med bemærkningerne nedenfor om koordineret tilsyn, bør en sådan ordning koordineres på tværs såvel horisontalt som vertikalt.

Kommunerne bør som udgangspunkt være omfattet af reglerne
Det fremgår af lovudkastet, at det ikke er intentionen, at kommunerne som helhed omfattes af den kommende lov. Der lægges dog op til, at visse kommunale forvaltningsaktiviteter vil være omfattet (fx på sundheds- og forsyningsområdet). Det er Rådets vurdering, at kommunerne som udgangspunkt bør være omfattet, ikke mindst for at sikre ensartethed i sikkerhedsberedskabet på tværs af kommuner, regioner og staten og for at minimere risikoen for unødige fortolkningsudfordringer. Omvendt er Rådet indstillet på, at visse kommunale aktiviteter kan undtages fra bestemmelserne, hvis det er åbenlyst, at de beredskabsmæssigt ikke har indvirkning på den samlede offentlige digitale infrastruktur.

Det kommende tilsyn med de berørte enheder
Høringsudkastet betoner, at der skal være tæt koordination mellem de kompetente myndigheder i forbindelse med tilrettelæggelse af tilsynsarbejdet, således, at der i videst mulige omfang anlægges en fælles tilgang. Rådet er i den forbindelse enig i bemærkningen om, at det er særlig relevant for tilsynet med enheder, der måtte indgå i flere forskellige sektorer, og hvor der kan være flere kompetente myndigheder, som skal føre tilsyn med samme enhed. Her lægger høringsudkastet op til, at der kan gennemføres fælles tilsynsbesøg og samarbejde om tilsynsressourcer, eksempelvis i form af et fælles sekretariat.

Rådet skal her opfordre til, at man i stor udstrækning forfølger denne tankegang og at de kompetente myndigheder forpligter sig på at koordinere tilsynsopgaven – både det løbende tilsyn med såkaldt 'væsentlige' virksomheder og det reaktive tilsyn med såkaldt 'vigtige' virksomheder. Denne koordination bør ikke kun udstrække sig til samme enhed (horisontalt), der måtte operere i forskellige sektorer, men også vertikalt i forhold til virksomheder og deres underleverandører.

Hændelsesunderretning
Rådet kan fuldt ud tilslutte sig bemærkningen om, at det - henset til underretningskravenes kvalitative og skønsmæssige karakter – vil være hensigtsmæssigt, at der fastsættes nærmere regler om, hvornår en hændelse anses for at være væsentlig, herunder ved fastsættelse af objektive kriterier om varighed og skadens omfang. Rådet anser det således som væsentligt, at hændelsesunderretningen ikke blot sker som led i det øjeblikkelige beredskab, men også som grundlag for videndeling og den fortsatte udbygning af sikkerhedsberedskabet centralt og for de enkelte sektorer.

Rådet anbefaler desuden, at det fx i bekendtgørelsesform præciseres, hvornår en given it-leverandør har ansvaret for den relevante hændelsesrapportering.

Endvidere ønsker Rådet at enhederne kan rapportere hændelserne via én kanal til en flerhed af myndigheder, som det kendes fra Virk.dk i dag, i stedet for at skulle lave de samme indberetninger til forskellige myndigheder.

Endelig bør det sikres, at de kompetente myndigheder i EU-landene koordinerer hændelsesrapporteringen, således, at virksomheder, der opererer i flere medlemslande, kun skal rapportere til en myndighed i et enkelt land.

Konkretisering af foranstaltninger
Rådet har noteret sig EU Kommissionens implementeringsforordning og særlig det bilag, som uddyber forventningerne til udformningen af og rapporteringen fra de tekniske og organisatoriske foranstaltninger, der skal implementeres fsva. NIS2. Rådet er glad for, at der kommer så forholdsvis konkrete krav til, hvad der forventes og vil opfordre til, at der kommer tilsvarende konkrete krav til forventningerne til de øvrige væsentlige og vigtige enheder. En konkret beskrivelse af disse krav må gerne blive udarbejdet så hurtigt som muligt, for de tager tid for enhederne at finde de rette foranstaltninger i markedet, at finde kompetencer til implementering og anvendelse af foranstaltningerne og at finde den fornødne ledelsesmæssige opbakning, herunder budgetmæssigt.

Med venlig hilsen

Henning Mortensen
Formand

Anne Dorte Bach
Næstformand