13. januar 2025

Att: Ministeriet for Samfundssikkerhed og Beredskab
Sagsnr.:2024-13723
mssb@mssb.dk

Høringssvar: Udkast til forslag til lov om sikkerhed og beredskab i telesektoren

Dansk Industri Digital og Rådet for Digital Sikkerhed takker for muligheden for at komme med bemærkninger til Ministeriet for Samfundssikkerhed og Beredskabs udkast til forslag til lov om sikkerhed og beredskab i telesektoren.

I lyset af det aktuelle trusselsniveau anerkender vi nødvendigheden og behovet for at styrke sikkerheden og modstandsdygtigheden i samfundet. Vi hilser derfor ambitionen om at sikre et højt cybersikkerhedsniveau og beredskab i Danmark såvel som på tværs i EU velkomment. En robust og fremtidssikret digital infrastruktur er netop central for vores konkurrenceevne, velfærd, vækst og samfundets stabilitet.

Vores høringssvar vil hovedsageligt bestå af generelle bemærkninger med enkelte nedslag. Nærværende høringssvar skal i øvrigt ses i relation til vores fælles høringssvar, der er udarbejdet sammen med Teleindustrien, IT-branchen, Dansk Erhverv, samt i relation til Dansk Industri Digitals høringssvar den 21. august til udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau[1]. Nærværende høringssvar vil være supplerende i forhold til ovenstående høringssvar, men vil ligeledes frembringe nogle af de samme bemærkninger for at understrege betydningen af disse.

1. Bemærkninger

Overordnet fremstår lovforslaget gennemarbejdet. Der stilles krav til tekniske, operationelle og organisatoriske foranstaltninger, som er vigtige skridt i retning af at sikre bedre beredskab og cybersikkerhed. Det er ligeledes formålstjenstligt, at ministeriet samtænker nærværende lovforslag med lov om leverandørsikkerhed i den kritiske teleinfrastruktur og lov om sikkerhed i net og tjenester, hvoraf sidstnævnte ophæves.

At lov om sikkerhed og beredskab i telesektoren forventeligt fremsættes parallelt med loven om foranstaltninger til sikring af et højt cybersikkerhedsniveau, finder vi ligeledes formålstjenstligt med henblik på at understøtte muligheden for at skabe koordination og ensartethed på tværs af sektorer.

[1] https://www.danskindustri.dk/globalassets/brancher/di-digital/2024/di-horingssvar-vedr.-forslag-til-lov-om-foranstaltninger-til-sikring-af-et-hojt-cybersikkerhedsniveau.pdf

Kort høringsfrist
En tæt involvering af de virksomheder, som omfattes af NIS2-lovgivningen, er essentiel for en vellykket implementering. Vi vil i den henseende påpege ministeriets korte frist – tilmed i en ferieperiode - på nærværende omfangsrige lovforslag som problematisk herfor.

Implementering
Med lovens ikrafttrædelse den 1. juli 2025, mener vi, at der efter ikrafttrædelsen bør være en passende implementeringsperiode. Dette vil give virksomhederne mulighed for at opfylde de nye krav, inden tilsyn indledes. Vi anbefaler, at virksomhederne skal have 12 måneder eller som minimum seks måneder til at efterleve kravene. Det er vores bekymring, at en kort implementeringsperiode vil føre til mere fokus på compliance end reelle forandringer, der styrker sikkerheden og beredskabet.

Derudover mener vi, at harmonisering på EU-niveau er afgørende for et konkurrencedygtigt indre marked. Virksomheder, der opererer på tværs af landegrænser, skal i videst muligt omfang reguleres af ensartede krav. Vi vil derfor opfordre til, at regeringen deltager aktivt i EU Kommissionens arbejde med henblik på at sikre, at reglerne bliver ensartede på tværs af EU.

Uklarhed om kommende rammer
Det fremgår af lovforslaget, at dele af den konkrete regulering på området efterfølgende vil blive udmøntet i bekendtgørelser, hvor lovforslaget herunder indeholder en række ministerbemyndigelser med mulighed for at "*fastsætte nærmere regler".* Dette sikrer naturligvis en vis fleksibilitet hos myndighederne, men gør det ligeledes svært at gennemskue omfanget, rækkevidden og proportionaliteten af krav og forpligtelser, som herved skaber usikkerhed for virksomheder i telesektoren. I og med, at bekendtgørelserne ikke er tilgængelige samtidig med nærværende lovforslag, vil vi opfordre til, at interessenter fra branchen involveres i udarbejdelsen af disse samt at der planlægges en tilstrækkelig lang frist når disse sendes i høring.

Økonomiske og administrative byrder
Ministeriet har ikke foretaget en kvantificering af de erhvervsøkonomiske og administrative konsekvenser for erhvervslivet som lovforslaget medfører, men en foreløbig vurdering. Med krav til tekniske, operationelle og organisatoriske foranstaltninger, herunder implementeringsomkostninger og potentielle økonomiske sanktioner, er der tale om betydelige økonomiske og administrative byrder.. Vi vil derfor understrege vigtigheden af at implementere de sektorspecifikke regler om sikkerhed og beredskab på en måde, der ikke øger byrderne for virksomheder i telesektoren, og henlede til at ministeriet tager højde for teleaftalen af den 21. december 2021, om at "*telepolitikken skal fremme, at rammerne for private investeringer på teleområdet er enkle, klare og forudsigelige, samtidig med at barrierer og byrder for private investeringer i den digitale infrastruktur reduceres*".

Derudover vil vi henlede til § 9 i lovforslagets kapitel 3 "Oplysnings- og underretningspligter mv.", der stiller krav til, *"at teleudbydere skal uden unødigt ophold underrette Center for Cybersikkerhed og CSIRT'en om enhver væsentlig hændelse",* medfører unødige administrative byrder, da teleudbydere skal underrette flere instanser. I tilfælde af væsentlige hændelser, der netop har karakter af kritiske samfundssituationer, er det ikke effektivt at skulle bruge tid på at underrette flere steder, men derimod at allokere virksomhedens ressourcer til at bidrage til at løse den pågældende situationen. Vi ser derfor, at underretningerne til Center for Cybersikkerhed og CSIRT'en sker via én fælles digital indgang, som sikrer, at virksomheden kun skal foretage én samlet underretning, som derefter fordeles til relevante myndigheder.

Proportionalitet i krav
Det er positivt, at loven understreger princippet om proportionalitet med en risikobaseret tilgang ved, at *"væsentlige og vigtige teleudbydere skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer…"*. Vi mener, at krav til sikkerhed og beredskab bør stå i rimelig forhold til den faktiske trussel, til virksomhedernes størrelse og til deres kapacitet. Det for blandt andet at sikre, at små og mellemstore virksomheder ikke pålægges uforholdsmæssigt store krav eller unødvendige byrder.

Afklaring og yderligere vejledning
Klarhed, tydelighed og forudsigelighed i de krav der stilles medvirker til, at virksomheder i telesektoren har de rette forudsætninger for implementering af lovforslaget. I lovforslaget er der en række definitioner, som på nuværende tidspunkt synes uklare, hvorfor der vil være behov for yderligere afklaring samt vejledning eller lignende. I nedenstående fremhæves nogle af disse eksempler:

Foranstaltninger til styring af sikkerhedsrisici mv. – Kapitel 2 § 6.; Lovforslaget stiller krav til, at foranstaltninger godkendes af teleudbyderens ledelsesorgan, og i *§ 6. Stk. 2* krav til, at ledelsesorganet skal *"deltage i relevante kurser om styring af informationssikkerhedsrisici og tilskynde til at tilsvarende kurser tilbydes til udbyderens øvrige ansatte".* Det præciserer ikke yderligere, hvilken enhed eller personkreds begrebet *ledelsesorgan* dækker over.

Oplysnings- og underretningspligt – Kapitel 3 § 8 pkt 2.; stiller krav til, at teleudbyder underretter Center for Cybersikkehed om påtænkt indgåelse af aftaler om leverancer, der *"vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf"*. Hvornår noget defineres som *"væsentlige dele"* kan være udfordrende for virksomhederne at vurdere, hvorfor vi ser et behov for, at der udarbejdes vejledninger eller lignende, der kan støtte teleudbyderne i fortolkningen.

Sikkerhedsgodkendelser – Kapitel 6 § 17. stk. 1; stiller krav til sikkerhedsgodkendelse foretaget af Center for Cybersikkerhed, når *"det er nødvendigt i forhold til den pågældendes adgang til klassificeret information eller til de funktioner, som den pågældende skal varetage"*. Vi finder det uklart, hvem der er omfattet, herunder om der er krav til, at leverandører ligeledes skal godkendes.

Vi ser derudover et generelt behov for, at sikkerhedsgodkendelser behandles effektivt med kort sagsbehandlingstid.

2. Opsummering

Dansk Industri Digital og Rådet for Digital Sikkerhed støtter lovforslagets formål om at styrke cybersikkerheden og beredskabet i telesektoren. For tilstrækkelig at kunne indfri lovforslagets ambitioner ser vi generelt et behov for klare definitioner, vejledning, en rimelig implementeringsfrist samt tæt inddragelse af branchen i arbejdet med de kommende bekendtgørelser, herunder for at sikre at implementeringen ikke øger byrderne for virksomheder i telesektoren

Vi står naturligvis til rådighed for en uddybning af høringssvaret og besvarelse af eventuelle spørgsmål.