Advokatrådet

KRONPRINSESSEGADE 28
1306 KØBENHAVN K
TLF.: 33 96 97 98

Forsvarsministeriet

DATO: 20. august 2024
SAGSNR.: 2024 - 2135
ID NR.: 1024024

fmn@fmn.dk
cc. jbh@fmn.dk

Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau - sagsnummer 2024/004461

Ved e-mail af 5. juli 2024 har Forsvarsministeriet anmodet om Advokatrådets bemærkninger til ovennævnte lovforslag.

Advokatrådet har følgende bemærkninger:

Generelle forhold

Det angives i lovforslaget, at Forsvarsministeriet har lagt afgørende vægt på, at gennemførelsen af NIS 2-direktivet sker i overensstemmelse med regeringens principper for implementering af erhvervsrettet EU-regulering, hvorefter den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen. Dette sker efter det anførte for at sikre, at danske virksomheder ikke pålægges flere byrder end andre europæiske virksomheder.

Advokatrådet støtter generelt hensigten om at sikre, at implementeringen af erhvervsrettet regulering i dansk ret ikke går videre, end hvad den relevante EU-regulering forudsætter. Hensynet til at sikre minimumsimplementering bør dog ikke hindre, at lovgivningen – herunder navnlig lovgivning underlagt så betydelig strafsanktionering, som det er tilfældet efter det foreliggende lovforslag – udformes på en måde, der gør det muligt for de omfattede virksomheder at fastlægge, hvilke retlige forpligtelser, de er underlagt, samt hvordan de konkret skal indrette sig for at efterleve reglerne og undgå strafsanktionering mv.

I den forbindelse bemærkes det, at hovedparten af lovforslagets krav rettet mod omfattede enheder indeholder bredt udformede krav, der ordret gennemfører NIS 2-direktivet. F.eks. indeholder lovforslaget 32 definitioner. Bemærkningerne til disse definitioner ses kun i begrænset omfang at indeholde fortolkningsbidrag, ud over henvisninger til den underliggende EU-regulering, der gør det muligt for omfattede enheder at anvende begreberne, og dermed lovforslaget, i praksis. En række af lovforslagets øvrige bestemmelser ses også alene at indeholde en ordret gengivelse af direktivets ordlyd, og indeholder kun i meget begrænset omfang bidrag, der kan understøtte de omfattede enheders konkrete fortolkning og afgrænsning af, hvilke forpligtelser de er underlagt.

Advokatrådet anerkender i sagens natur, at den danske stat som led i implementeringen af NIS 2-direktivet er EU-retligt forpligtet til at udforme ordlyden af de relevante bestemmelser i overensstemmelse med direktivets ordlyd. Ligesom det anerkendes, at et område af så dynamisk og omskiftelig karakter som cybersikkerhed til en vis grad må lovreguleres generelt og neutralt. Med henblik på at sikre de omfattede enheder en acceptabel grad af klarhed om, hvilke tiltag de er forpligtet til at implementere for at efterleve lovforslaget, finder Advokatrådet dog, at det er af afgørende betydning, at den direktivnære implementering ledsages med bemærkninger, der mere entydigt fastsætter de specifikke begreber og krav de omfattede enheder er underlagt. I fraværet af mere udbyggede lovbemærkninger overlades de enkelte enheder og kompetente myndigheder til selv at fastlægge deres forståelse af lovforslagets praktiske betydning.

Advokatrådet har i den forbindelse noteret, at der efter lovforslagets § 6, stk. 3, kan udstedes sektorspecifikke bekendtgørelser med mere konkretiserede krav til de foranstaltninger, som enhederne skal træffe i medfør af den foreslåede bestemmelse i stk. 1. Af bemærkningerne til bestemmelsen anføres det, at regler fastsat efter denne bestemmelse bl.a. vil skulle være i overensstemmelse med regeringens principper om minimumsimplementering.

Som anført finder Advokatrådet, at hensynet til alene at foretage en minimumsimplementering ikke bør hindre, at de i praksis meget relevante – og strafbelagte – krav i § 6, stk. 1, blot gentages i de sektorspecifikke bekendtgørelser. Advokatrådet tilskynder derfor til, at der i lovforslagets bemærkninger nærmere beskrives, hvilken grad af præcisering de regeludstedende myndigheder kan og bør sikre som led i udstedelsen af de sektorspecifikke bekendtgørelser. Derudover

bemærkes det, at såvel kravene i lovforslagets § 6, samt lovforslagets øvrige bestemmelser, der pålægger enheder forpligtelser, i praksis bør understøttes af konkret og handlingsanvisende vejledninger mv. fra de relevante myndigheder for også derigennem at sikre de omfattede enheder betryggende mulighed for at efterleve reglerne. Dette vurderes samtidig at ville lette de relevante myndigheders håndhævelse af og tilsyn med lovforslagets krav.

Advokatrådet opfordrer til, at udarbejdelsen af sådanne vejledninger mv. prioriteres højt af de relevante myndigheder og udstedes i rimelig tid inden reglerne finder anvendelse.

I forlængelse af ovenstående bemærkes det, at lovmodellen for implementering af NIS 2-direktivet forudsætter, at der udpeges en række kompetente myndigheder på tværs af de omfattede sektorer, der - for hver deres sektor - skal varetage tilsyns- og myndighedsopgaver. Det fremgår af lovforslagets bemærkninger, at det forudsættes, at der vil være en tæt koordination mellem de kompetente myndigheder i forbindelse med tilrettelæggelsen af tilsynsarbejdet, således at der i videst muligt omfang anlægges en fælles tilgang. Det er endvidere fastsat, at Center for Cybersikkerhed (CFCS) vil varetage funktionen som CSIRT i forhold til alle de af direktivet omfattede sektorer og forestå forhandlingen af bekendtgørelser efter lovforslagets § 6, stk. 3.

Advokatrådet tilslutter sig det anførte om, at denne model forudsætter en meget effektiv koordinering mellem de kompetente myndigheder. Advokatrådet bemærker i den forbindelse, at det – netop for at sikre en fælles tilgang og effektiv vejledning mv. af de berørte enheder – vil være af afgørende betydning, at myndighederne etablerer en ordning, der sikrer, at eventuelle uoverensstemmelser mellem kompetente myndigheders fortolkning, vurdering af trusselsbilledet mv. identificeres og udredes af myndighederne. Lovforslaget bør på den baggrund nærmere beskrive, hvordan det i praksis vil blive sikret, at f.eks. enheder, der har aktiviteter inden for flere omfattede sektorer, ikke mødes af divergerende krav, fortolkninger mv. fra to eller flere kompetente myndigheder.

Retssikkerhedsmæssige forhold

Lovens anvendelsesområde

Det fremgår af lovforslagets generelle bemærkninger, at lovforslaget vurderes at omfatte omkring 2.000 virksomheder. Lovforslagets § 1 fastsætter anvendelsesområdet med en generel henvisning til NIS 2-direktivets artikel 2. Samtidig indeholder lovforslagets bemærkninger – med henvisning til NIS 2-direktivet – flere opregninger af hvilke typer af enheder, der, alt efter deres størrelse og sektor, er omfattet af lovforslaget. Eksempelvis angives det, at følgende sektorer er omfattet udover de sektorer, der i dag er omfattet af NIS 1-reglerne: 1) Spildevand, 2) forvaltning af informations- og kommunikationstjenester (IKT-tjenester) (business-to-business), 3) offentlig forvaltning, 4) rummet, 5) post- og kurertjenester, 6) affaldshåndtering, 7) fremstilling, produktion og distribution af kemikalier, 8) produktion, tilvirkning og distribution af fødevarer, 9) forskning og 10) fremstilling med delsektorerne: a) Fremstilling af medicinsk udstyr og medicinsk udstyr til vitrodiagnostik, b) fremstilling af computere og elektroniske og optiske produkter, c) fremstilling af elektrisk udstyr, d) fremstilling af maskiner og udstyr ikke andetsteds nævnt, e) fremstilling af motorkøretøjer, påhængsvogne og sættevogne og f) fremstilling af andre transportmidler.

Endvidere opregnes der i bemærkningerne, de typer af enheder, som vil være omfattet af lovforslaget, uanset deres størrelse.

Det fremgår af bemærkningerne til § 1, at det efter den foreslåede bestemmelse vil være enhedernes ansvar at vurdere, om de er omfattet af lovens anvendelsesområde, idet enheder, der er omfattet af anvendelsesområdet i artikel 2 i NIS 2-direktivet, vil være umiddelbart omfattet af lovens anvendelsesområde. Enheder vil i overensstemmelse med forvaltningslovens § 7 i fornødent omfang kunne få vejledning og bistand fra de kompetente myndigheder.

Det anføres videre, at i en situation, hvor en enhed fejlagtigt måtte vurdere, at denne er eller ikke er omfattet af lovens anvendelsesområde, vil de kompetente myndigheder ved en forvaltningsakt kunne konstatere, hvorvidt enheden er omfattet af lovens anvendelsesområde.

Afgrænsningen af hvilke enheder, der anses for væsentlige, fremgår af lovforslagets § 4. I § 4, stk. 4, er der hjemmel til, at vedkommende minister inden for sit område kan fastsætte nærmere regler om kriterier for, hvornår enheder er omfattet af stk. 3, nr. 5. Det fremgår af bemærkningerne til stk. 4, at hjemlen til at fastsætte nærmere regler om hvilke enheder, der er omfattet af § 4, stk. 3, nr. 5, idet denne bestemmelse har et forholdsvist skønsmæssigt og kvalitativt præg, hvilket kan gøre det vanskeligt for de enkelte enheder at vurdere, om de betragtes som omfattet af lovens krav.

Advokatrådet finder, at ordningen for afgrænsning af hvilke enheder, der er omfattet af lovforslaget efter § 1, ligeledes efterlader en betydelig grad af usikkerhed om lovforslagets anvendelsesområde. Vurderingen af om en enhed – der møder lovforslagets øvrige krav – f.eks. er beskæftiget med "rummet" eller "fremstilling af elektronisk udstyr" giver ikke mulighed for entydigt at fastslå om, og hvorfor, aktivitet knyttet til et angivet område bevirker, at enheder er omfattet af lovforslagets krav. Hensynet anført i bemærkningerne til § 4, stk. 4, om at bestemmelsen i § 4, stk. 3, nr. 5, har et forholdsvist skønsmæssigt og kvalitativt præg synes således ligeledes at være aktuelt i forhold til afgrænsningen af dele af anvendelsesområdet fastsat i lovforslagets § 1. Den foreslåede ordning efter § 1, bør således, efter Advokatrådets vurdering, omfatte et egentligt retskrav for en enhed til, efter anmodning, at modtage en afgørelse fra den relevante sektorspecifikke myndighed om, hvorvidt den er omfattet eller ej. Alternativt bør der fastsættes en hjemmel svarende til bestemmelsen i § 4, stk. 4, hvorefter vedkommende minister inden for sit område kan fastsætte nærmere regler om kriterier for, hvornår enheder er omfattet af § 1.

Anvendelse af kriterier for omfattede enheders størrelse

Det fremgår af lovforslaget, at det – inden for de relevante sektorer – finder anvendelse for små virksomheder i kategorien SMV'er, der defineres som virksomheder, der beskæftiger under 50 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 10 mio. euro.

Advokatrådet anbefaler, at det præciseres fra hvilket tidspunkt SMV'er, der først efter lovens ikrafttræden opfylder disse betingelser, anses for omfattet af lovforslaget, herunder om tidspunktet fastsættes baseret på indeværende eller afsluttede regnskabsår. Endvidere bør der angives, hvad retsvirkningen er – og

hvornår den indtræffer – hvis en virksomhed ikke længere opfylder de angivne kriterier.

Leverandører

Det fremgår af lovforslagets § 6, stk. 1, nr. 4, at væsentlige og vigtige enheder som minimum skal tage højde for forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.

Af bemærkningerne til bestemmelsen fremgår det, med henvisning til direktivet, at enheder i den forbindelse skal tage hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder, og den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer.

Af NIS 2-direktivets præambelbetragtning 84-85 fremgår bl.a. følgende:

"Væsentlige og vigtige enheder bør navnlig tilskyndes til at indarbejde foranstaltninger til styring af cybersikkerhedsrisici i kontraktlige arrangementer med deres direkte leverandører og tjenesteudbydere. Disse enheder kunne overveje risici hidrørende fra leverandører og tjenesteudbydere i andre led.
Væsentlige og vigtige enheder bør derfor vurdere og tage hensyn til den generelle kvalitet og modstandsdygtighed af produkter og tjenester, de heri integrerede foranstaltninger til styring af cybersikkerhedsrisici og deres leverandørers og tjenesteudbyderes cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer. Væsentlige og vigtige enheder bør navnlig tilskyndes til at indarbejde foranstaltninger til styring af cybersikkerhedsrisici i kontraktlige arrangementer med deres direkte leverandører og tjenesteudbydere. Disse enheder kunne overveje risici hidrørende fra leverandører og tjenesteudbydere i andre led."

Advokatrådet bemærker, at omfattede enheder i vidt omfang benytter leverandører som led i driften og understøttelsen af net- og informationssystemer omfattet af § 6. I praksis er der således allerede forud for direktivets implementering stor fokus på disse spørgsmål blandt de enheder og leverandører, der forventer at være omfattet af lovforslaget. Henset til lovforslagets og NIS 2-direktivets generelle udformning, må der i praksis derfor forventes at opstå spørgsmål om det præcise omfang og karakteren, af de krav, enhederne skal stille

til deres leverandører. Herunder i hvilket omfang enheden skal påtage sig et nærmere ansvar for at føre tilsyn med leverandørers cybersikkerhedspraksis mv. Lovforslaget og NIS 2-direktivet ses kun i begrænset omfang at beskrive det nærmere omfang af såvel enhedernes, som leverandørers ansvar for forsyningskædesikkerhed mv., herunder hvordan konkrete krav nærmere afgrænses.

Advokatrådet opfordrer derfor til, at lovforslaget nærmere behandler den præcise afgrænsning af indholdet og ansvaret for forsyningskædesikkerhed mv., og beskriver hvilke forventninger de kompetente myndigheder har til "styring af cybersikkerhedsrisici i kontraktlige arrangementer", jf. NIS 2-direktivets præambel.

Strafbestemmelser mv.

Det følger af lovforslagets § 23, stk. 1, nr. 2, at den kompetente myndighed kan træffe afgørelse om midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos enheden at udøve ledelsesfunktioner i den pågældende enhed. Efter bestemmelsens stk. 2, kan midlertidige suspensioner eller forbud, som er pålagt i medfør af stk. 1, kun anvendes, indtil enheden træffer de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningerne blev anvendt.

Efter bestemmelsens stk. 3 kan en afgørelse efter stk. 1 forlanges indbragt for domstolene af enheden eller den fysiske person, afgørelsen vedrører. Den myndighed, som vedkommende minister bemyndiger hertil, anlægger i givet fald sag inden for rammerne af den civile retspleje mod den enhed eller person, som har forlangt sagen indbragt.

Det fremgår af lovforslagets bemærkninger, at Forsvarsministeriet har vurderet, at de eksisterende muligheder for rettighedsfrakendelse i straffeloven ikke er tilstrækkelige til at sikre korrekt og tilstrækkelig gennemførelse af den pågældende bestemmelse i direktivet. Det skyldes navnlig, at rettighedsfrakendelse i medfør af straffelovens § 79 alene kan ske i forbindelse med dom for strafbart forhold, og hvis det udviste forhold begrunder en nærliggende fare for misbrug af stillingen.

Advokatrådet finder, at den foreslåede særregel – som den danske stat er EU-retligt forpligtet til at indføre – om midlertidig frakendelse af retten til at udøve ledelsesfunktioner i den pågældende enhed, aktualiserer visse retssikkerhedsmæssige overvejelser.

Som lovforslaget er affattet, er adgangen til at forbyde en person at udøve ledelsesfunktioner ikke direkte knyttet til den pågældende persons egen adfærd, men fungerer som et middel til at foranledige den pågældende enhed til at træffe de nødvendige foranstaltninger til at afhjælpe manglerne eller opfylde den kompetente myndigheds krav.

Advokatrådet anbefaler, at det nærmere behandles i lovforslaget, om et forbud kan meddeles en person, uden at den pågældende konkret har foretaget dadelværdige forhold eller forsømmelser (objektivt ansvar) eller om anvendelsen af et forbud forudsætter, at den pågældende konkret har været vidende om eller deltaget i beslutninger, der vedrører de forhold, som forbuddet søger at adressere.

Advokatrådet finder det positivt – ud fra en retssikkerhedsmæssig betragtning – at en afgørelse om midlertidig frakendelse, kan forlanges indbragt for domstolene. Dette ses også at være i overensstemmelse med Justitsministeriets vejledning om lovkvalitet, jf. dennes afsnit 6.3. Det bemærkes i den forbindelse, at det fremgår af Justitsministeriets vejledning, at der normalt bør være adgang for den pågældende til, eventuelt inden for en vis frist, at forlange spørgsmålet indbragt for domstolene ved den administrative myndigheds foranstaltning. Henset til, at rettighedsfrakendelsen efter lovforslaget er midlertidig, og således alene kan anvendes indtil enheden træffer de nødvendige tiltag, vil adgangen til domstolsprøvelse – i lyset af domstolenes samlede sagsbehandlingstid for behandlingen af civile sager i 1. instans ofte er over ét år – imidlertid i praksis kun have reel betydning i tilfælde, hvor afhjælpningen af de relevante forhold hos enheden overstiger domstolens samlede sagsbehandlingstid. Adgangen til domstolsprøvelse vil således i de fleste – hvis ikke alle – tilfælde, alene have relevans for en prøvelse af en rettighedsfrakendelse, der efterfølgende er bortfaldet.

Endvidere bemærkes det, at lovforslaget ikke ses at fastsætte, at en begæring om, at en afgørelse om midlertidig frakendelse, indbringes for domstolene har opsættende virkning, medmindre retten bestemmer andet. Efter

Justitsministeriets vejledning om lovkvalitet, jf. ovenfor, bør dette ellers i almindelighed være tilfældet.

Advokatrådet antager, at fraværet af en bestemmelse om, at indbringelse for domstolene skal have opsættende virkning, skyldes, at der i lovforslaget alene er tale om en midlertidig frakendelse af retten til at udøve ledelsesfunktioner i den pågældende enhed, hvorfor opsættende virkningen i vidt omfang vil bevirke, at frakendelsen ikke når at få effekt, før forholdet er afhjulpet og frakendelsen derfor bortfalder. Da en midlertidig frakendelse i alle tilfælde vil være særdeles bebyrdende for de omfattede personer, og potentielt kunne have varige omdømmemæssige konsekvenser og påvirke den pågældendes adgang til senere at genindtræde i den samme eller tilsvarende stillinger, bør lovforslaget sikre en passende varetagelse af de berørte personers retssikkerhed.

På denne baggrund anbefaler Advokatrådet, at Forsvarsministeriet overvejer alternative måder at sikre de berørte personer og enheders retsstilling. Dette kunne være i form af en lovfastsat adgang for de berørte til at opnå prøvelse gennem administrativ rekurs inden for en passende kort frist, der henset til sagernes karakter, ikke bør overstige 3 uger.

Endvidere bør der – som et supplement til ovenstående – fastsættes en udvidet partshøringspligt i sager efter lovforslagets § 23, således at afgørelse alene kan træffes, når der er partshørt over såvel sagens faktum, myndighedens bevismæssige og retlige vurdering og den påtænkte sanktion.

Forholdet til anden lovgivning mv.

Forholdet til databeskyttelsesretten

Det anføres generelt i lovforslaget, at det er Forsvarsministeriets opfattelse, at behandling af almindelige personoplysninger i forbindelse med overholdelsen af registreringsforpligtelserne i §§ 9 og 10 og underretningsforpligtelserne i §§ 12 og 13, samt i forbindelse med myndighedernes anvendelse af tilsyns- og håndhævelsesforanstaltninger efter reglerne i kapitel 6 for private virksomheder vil kunne ske i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra c og e.

For så vidt angår spørgsmålet om videregivelse af personoplysninger til CSIRT'en og det centrale kontaktpunkt, fremgår det af lovforslaget, at private virksomheder vil kunne videregive almindelige personoplysninger efter databeskyttelsesforordningens artikel 6, stk. 1, litra f. Det anføres i den forbindelse, at det fremgår af databeskyttelsesforordningens præambelbetragtning 49, at behandling af personoplysninger – i det omfang, det er strengt nødvendigt og forholdsmæssigt for at sikre net- og informationssikkerheden – der foretages af eksempelvis Computer Emergency Response Teams (CERT'er), udgør en legitim interesse for den berørte dataansvarlige.

Efter Advokatrådets vurdering kan der rejses spørgsmål om, hvorvidt videregivelse af personoplysninger til CSIRT og det centrale kontaktpunkt navnlig efter lovforslagets § 19, i alle tilfælde kan baseres på interesseafvejningsreglen i databeskyttelsesforordningens artikel 6, stk. 1, litra f. Navnlig henset til, at det – som anført ovenfor – følger af databeskyttelsesforordningens præambelbetragtning nr. 49, at videregivelse forudsætter, at det er "strengt nødvendigt og forholdsmæssigt for at sikre net- og informationssikkerheden".

Den meget omfattende deling af oplysninger, der er en forudsætning for et effektivt samarbejde på tværs af omfattede enheder, vurderes således at omfatte deling af oplysninger – herunder personoplysninger – uden at det på forhånd kan fastlægges i hvilket omfang oplysningerne konkret har relevans for modtagerne, navnlig når formålet med delingen er at varsle fællesskaber af væsentlige og vigtige enheder og, hvor det er relevant, deres leverandører eller tjenesteudbydere, jf. bemærkningerne til lovforslagets § 19. Dette gælder f.eks. ved deling af oplysninger om nærved hændelser, kompromitteringsindikatorer, IP-adresser mv.

Endvidere bemærkes det, at det følger af lovforslagets § 1, stk. 6, at offentlige og private enheder kan, uanset om de er omfattet af lovens anvendelsesområde, give frivillig underretning til CSIRT'en efter § 14 og deltage i den frivillige udveksling af oplysninger mellem enheder i cybersikkerhedsfællesskaber efter § 19.

Efter de specielle bemærkninger til § 19 vil bestemmelsen kunne omfatte udveksling af relevante cybersikkerhedsoplysninger indbyrdes, herunder oplysninger om cybertrusler, nærved hændelser, sårbarheder, teknikker og procedurer, kompromitteringsindikatorer, fjendtlige taktikker, specifikke

oplysninger vedrørende trusselsaktører, cybersikkerhedsadvarsler og anbefalinger vedrørende konfiguration af cybersikkerhedsværktøjer til opdagelse af cyberangreb.

Det databeskyttelsesretlige grundlag for udveksling af oplysninger mellem enheder efter lovforslagets § 19, ses ikke nærmere behandlet i lovforslaget. Sådanne enheder vil efter Advokatrådets umiddelbare vurdering ikke kunne basere deres videregivelse af personoplysninger på databeskyttelsesforordningens artikel 6, stk. 1, litra c.

Advokatrådet anbefaler derfor, at der – for at sikre så klare og betryggende rammer som muligt for de berørte enheder – mere entydigt fastsættes i lovforslaget, at den ofte brede og omfattende videregivelse af oplysninger, herunder af personoplysninger i form af IP-adresser mv., som et effektivt samarbejde om cybersikkerhed forudsætter, kan finde sted til CSIRT'en og det centrale kontaktpunkt, og at lovforslaget i databeskyttelsesforordningens forstand fastsætter en retlig forpligtelse, jf. artikel 6, stk. 1, litra c, for alle enheder til at dele oplysninger, herunder enheder, der ellers ikke er omfattet af lovforslaget, jf. lovforslagets § 1, stk. 6.

Advokatrådet skal endvidere anbefale, at lovforslaget – under hensyntagen til de ovenfor anførte betragtninger om at sikre en betryggende ramme for udvekslingen af personoplysninger – tilføjes en redegørelse for hjemmelsgrundlaget for udveksling af personoplysninger efter § 19.

Håndtering af klassificerede oplysninger mv.

Lovforslagets §§ 12 og 13, fastsætter en række forpligtelser for omfattede enheder til at underrette den relevante kompetente myndighed og CSIRT'en om væsentlige hændelser.

Det fremgår bl.a. af lovforslagets bemærkninger, at der ved vurderingen af, om offentligheden skal informeres, skal sikres, at dette sker uden at kompromittere fortrolige oplysninger.

Advokatrådet bemærker, at underretninger – efter omstændighederne – kan vedrøre hændelser, der, med varierende grader af sikkerhed, kan attribueres til ondsindede tredjestatsaktører.

Lovforslaget ses dog ikke at behandle, hvordan enheder, der eventuelt på baggrund af oplysninger fra CSIRT'en, må lægge til grund, at en aktuel hændelse afdækker en tredjestatsaktørs forsøg på f.eks. at opnå adgang til, eller kompromittere, net- og informationssystemer, skal behandle nærmere oplysninger herom. Det bemærkes i den forbindelse, at såfremt CSIRT'en konkret vurderer, at oplysninger om den pågældende hændelse omfatter oplysninger, der er, eller bør være, klassificerede efter Justitsministeriets cirkulære nr. 10338 af 17. december 2014 (sikkerhedscirkulæret), vil hovedparten af de omfattede enheder ikke være omfattet af cirkulæret, og dermed ikke være forpligtet til at behandle oplysningerne i overensstemmelse hermed. Lovforslaget ses samtidig ikke at hjemle adgang for CSIRT'en eller de kompetente myndigheder, til at pålægge omfattede enheder eksempelvis tavshedspligt mv. i forhold til oplysninger om hændelsen.

Med henblik på at sikre, at der er klarhed om, hvordan omfattede enheder skal forholde sig ved underretninger om hændelser, der af myndighederne anses for at vedrøre klassificerede forhold mv., opfordrer Advokatrådet til, at det nærmere reguleres i lovforslaget, såfremt Forsvarsministeriet forventer, at der i konkrete tilfælde kan opstå behov for at underretninger og opfølgningen på hændelser behandles under iagttagelse af særlige foranstaltninger. Det bør i den forbindelse overvejes, om der bør fastsættes en adgang til, at CSIRT'en, eller den kompetente myndighed, kan beslutte, at navnlig forpligtelserne i lovforslagets §§ 12 og 13, konkret skal fraviges med henblik på at sikre, at særlige fortrolighedshensyn kan varetages inden for lovgivningens rammer.

Med venlig hilsen

Andrew Hjuler Crichton
Generalsekretær

Forsvarsministeriet
Sendt på mail til fmn@fmn.dk og jhb@fmn.dk

22. august 2024
Jeres ref.nr.: 2024/004461

ATP's svar på høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Vi vil indledningsvist takke for muligheden for at afgive bemærkninger til lovforslaget.

Udover varetagelsen af ATP Livslang Pension, yder ATP teknisk og administrativ bistand til en række ordninger, der på forskellig måde påvirkes af forslaget. ATP har på den baggrund følgende bemærkninger til lovforslaget:

ATP
Kongens Vænge 8,
3400 Hillerød

Tlf.: 70 11 12 13
Fax: 48 20 48 02

www.atp.dk

CVR-nr.: 43405810

Telefontid:
Mandag-Torsdag: 8.00-16.00
Fredag: 8.00-15.30

Lovens anvendelsesområde

Lovforslaget henviser i § 1, stk. 1, til anvendelsesområdet, som defineret i art. 2 i direktiv 2022/2555 (herefter NIS2-direktivet). I bemærkningerne præciseres det, at en enhed – udover fysiske personer – kan være virksomheder, foreninger, organisationer og offentlige myndigheder mv. (juridiske personer), der er tildelt et CVR-nummer. For ATP's vedkommende medfører dette, at ATP selv og de administrerede ordninger skal vurderes enkeltvist for at vurdere, hvorvidt de falder ind under lovens anvendelsesområde.

ATP og hovedparten af de administrerede ordninger er oprettet som selvejende institutioner, og de anses alle for at være offentlige myndigheder, men ikke for at indgå i centraladministrationen. Alle ordningerne falder ind under definitionen af "offentlige forvaltningsenheder", som fastsat i art. 6, nr. 35 i NIS2-direktivet, og dermed også af anvendelsesområdet for NIS2-direktivet, som fastlagt i art. 2, stk. 2, f) og direktivets bilag I.

På den baggrund vurderer ATP, at ATP Livslang Pension, Udbetaling Danmark, Lønmodtagernes Garantifond, Arbejdsmarkedets Fond for Udstationerede, Arbejdsgivernes Uddannelsesbidrag, Arbejdsmarkedets Erhvervssikring, Seniorpensionsenheden, FerieKonto og Barsel.dk er omfattet af lovforslagets § 1 og dermed af lovens anvendelsesområde.

Den daglige administration af Lønmodtagernes Feriemidler varetages af ATP, men enheden hører under LD Fonde. Afklaring af, hvorvidt fonden er omfattet af lovforslagets anvendelsesområde, afventer LD Fonde.

ATP hører gerne, hvis vedkommende minister, jf. lovforslagets § 1, eller Forsvarsministeriet vurderer anvendelsesområdet for ATP og de administrerede

ordninger anderledes.

Definition af CSIRT

Begrebet CSIRT anvendes gennem lovforslaget i betydningen ”enheder, der håndterer it-sikkerhedshændelser”, på samme måde som i direktivet. Det foreslås, at der indskrives en definition heraf i lovforslaget, fx i § 3.

Forsyningskædesikkerhed

Det foreslås i § 6, stk. 1, nr. 4, at enhederne bl.a. skal tage højde for forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere. ATP bemærker, at det dermed alene er direkte leverandører og ikke eventuelle underleverandører, som enhederne skal tage højde for. ATP kvitterer for denne begrænsning, da det som kunde er svært effektivt at kontrollere efterfølgende led i leverandørkæden.

I § 6, stk. 2, foreslås det, at omfattede enheder skal træffe mitigerende foranstaltninger ”uden unødigt ophold”. ATP bemærker, at det vil være nyttigt at få defineret tidsrummet yderligere, da det kan give anledning til fortolkningstvivl.

Endelig bemærkes det, at det fremgår af bemærkningerne s. 230, at når enhederne skal træffe passende foranstaltninger efter § 6, medfører det, at enhederne skal tage hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder, og at enhederne i den forbindelse tager højde for resultaterne af de koordinerede sikkerhedsrisikovurderinger, der skal udarbejdes efter NIS2-direktivets art. 22, stk. 1. ATP skal i den forbindelse opfordre til, at Center for Cybersikkerhed sikrer let adgang til disse risikovurderinger og gerne orienterer herom, når der kommer nye vurderinger, så det bliver enkelt for danske enheder at holde sig ajour med de europæiske vurderinger.

Ledelsesorgan

I udkastets § 7, stk. 1, foreslås det bl.a., at foranstaltninger skal være godkendt af ”enhedens ledelsesorgan”. Det er ikke nærmere defineret i lovforslaget eller NIS2-direktivet, hvad eller hvem, der udgør ledelsesorganet. ATP bemærker, at begrebet ”ledelsesorgan” også anvendes i DORA-forordningen om cybersikkerhed for finansielle virksomheder. Her defineres ledelsesorgan i art. 3, nr. 45 ved at henvise til definitioner i en række andre EU-retsakter, der på forskellig vis anvender begrebet ”ledelsesorgan” for enheder, der modsvarer bestyrelser. Definitionen i DORA-forordningen går derefter videre med følgende tilføjelse: ”eller dertil svarende personer, som varetager den faktiske drift af enheden eller nøglefunktioner i overensstemmelse med relevant EU-ret eller national ret”.

På denne baggrund lægger ATP til grund, at ”ledelsesorgan” i NIS2-lovens kontekst skal forstås som bestyrelse og direktion. Da NIS2-direktivet ikke regulerer

nøglepersoner, vurderer ATP ikke, at henvisningen til nøglepersoner i DORA-forordningen er relevant for gennemførelsen af NIS2. ATP lægger på den baggrund til grund, at godkendelse af enhedens ledelsesorgan kan ske enten på direktionsniveau eller på bestyrelsesniveau, afhængigt af beslutningens rækkevidde, jf. almindelige selskabsretlige regler.

Det foreslås videre i § 7, stk. 2, at medlemmerne af ledelsesorganet skal "deltage i relevante kurser". ATP skal foreslå, at ordet "kurser" erstattes med "uddannelse", hvilket bedre modsvarer brugen af det engelske ord "training" eller det svenske ord "utbildning" i hhv. den engelske og svenske udgave af direktivet. Brugen af ordet "kurser" signalerer, at den ønskede viden alene kan opnås ved køb af kurser fra 3. partsudbydere, mens uddannelse er bredere, og dermed også kan dække fx uddannelse internt i en enhed.

Registreringspligt

ATP forventer ikke at blive omfattet af den foreslåede § 9, men det forekommer uhensigtsmæssigt at fastsætte en frist for registrering i stk. 2, der ligger forud for lovens ikrafttrædelse.

Den foreslåede § 10 omhandler registrering for øvrige enheder. I stk. 1, nr. 2) foreslås det, at der skal oplyses adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre. ATP bemærker, at det vil være nyttigt med en præcisering af, hvem der ønskes kontaktoplysninger til, herunder om det er på ledelsesniveau, eller på teknisk niveau. For at lette den administrative byrde skal ATP foreslå, at registreringen så vidt muligt kobles op på den eksisterende enheds registrering i CVR-registret, så kontaktoplysninger efter den indledende registrering skal holdes ajour så få steder som muligt.

Adgang til oplysninger

Det foreslås i § 14, stk. 3, at frivillige underretninger undtages fra aktindsigt. Det præciseres i bemærkningerne s. 259, at undtagelsen alene gælder for frivillige indberetninger i medfør af § 14, og at obligatoriske indberetninger efter § 12 således ikke undtages. ATP skal opfordre til, at de obligatoriske indberetninger ligeledes undtages fra aktindsigt, på samme måde som alle tilsvarende indberetninger til Center for Cybersikkerhed undtages i dag efter lov om sikkerhed i net og tjenester[1], og bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester[2].

Særligt i lyset af den korte frist på 24 timer til den tidlige varsling, vil et krav om mulig efterfølgende udlevering medføre, at enheden allerede i forbindelse med den tidlige varsling skal tage stilling til, om der er oplysninger i varslingen, der fx kan udstille sårbarheder eller uhensigtsmæssigheder, der efterfølgende kan udnyttes af hackere eller andre kriminelle. Dette kan medføre, at oplysninger undlades eller alene gives i

[1] LBKG nr. 153 af 1. februar 2021
[2] BKG nr. 1414 af 30. november 2023

overordnet form, hvilket må formodes at skade det videre arbejde med at mitigere hændelsen.

I tillæg må adgang til oplysninger om varslinger mv. forventes at give et væsentligt ressourcetræk hos de kompetente myndigheder, da information om mulige angreb på samfundsinteressante enheder må forventes at have mediernes konstante interesse. Også hos de omfattede enheder forventes muligheden for at søge aktindsigt i underretninger at ville skabe et uhensigtsmæssigt træk på cybersikkerhedsressourcer, på tidspunkter, hvor disse personer forventes at have travlt med at mitigere en hændelse.

Det bemærkes, at en underretning efter § 12 og 13 må formodes at indeholde en række faktiske oplysninger, der som udgangspunkt vil være omfattet af ekstraheringspligt efter offentlighedsloven.

Det bemærkes videre, at hensynet til transparens er varetaget i lovforslagets § 15 og 16, der fastlægger i hvilke tilfælde offentligheden og modtagerne af tjenester skal underrettes. NIS2-direktivet fastlægger så vidt ses ikke krav om yderligere offentlighed, og det implicitte krav om offentlighed i underretninger efter § 12 vurderes dermed at gå videre end direktivet, og dermed være i strid med ønsket om minimumsimplementering.

Det foreslås i § 16, stk. 1, at den kompetente myndighed kan informere om en hændelse, bl.a. hvis offentliggørelsen er i offentlighedens interesse. Det fremgår af bemærkningerne s. 262, at en kompetent myndighed i givet fald skal afveje hensynet til den konkrete enhed overfor hensynet til orientering af offentligheden. ATP skal på den baggrund foreslå, at det i lovteksten præciseres, at der kan ske offentliggørelse, hvis denne er af *væsentlig* interesse for offentligheden. Dette vil sikre, at det EU-retlige proportionalitetsprincip, der gælder for fortolkningen af direktivet, også afspejles i den danske lovtekst.

CSIRT'ens opgaver

Det foreslås i § 18, at CSIRT'en sikrer, at der kan rapporteres anonymt om sårbarheder. Det er uklart, om det samme gælder for de underretninger, der omtales i § 14. Hvis det er tilfældet, kan det overvejes tydeliggjort med fx en henvisning til § 14.

Tilsyn

I § 21 foreslås der regler for tilsyn med området. I stk. 1, nr. 6), foreslås det, at kompetente myndigheder kan kræve at få udleveret oplysninger, der er nødvendige for udførelsen af tilsynsopgaven, herunder til afgørelse af om et forhold er omfattet af denne lov eller regler udstedt i medfør af loven. I stk. 3, foreslås det, at den kompetente myndighed kan stille nærmere krav til hvordan og i hvilken form oplysninger mv. skal afgives.

ATP bemærker, at det umiddelbart synes som en meget bred adgang for myndighederne til at kræve oplysninger uden nogen modsvarende rettigheder for de

berørte enheder. Særligt synes det vidtgående, at det kan kræves materiale på områder, som ikke nødvendigvis er omfattet af loven. Tilsvarende gælder for den foreslåede § 24 for vigtige enheder.

Det foreslås derfor at indsætte nogle begrænsninger for de kompetente myndigheder, fx at enhederne skal gives rimelige frister, eller at materiale skal udleveres i henhold til almindelige standarder på området. Ligeledes bør der være begrænsninger for hvor meget materiale, der kan kræves. Med de foreslåede regler vil en kompetent myndighed fx kunne anmode om, at der udarbejdes store mængder nyt materiale, hvilket ikke synes proportionalt.

I tillæg vil indsendelse af materiale til en kompetent myndighed kunne medføre, at ellers internt materiale i offentlige myndigheder underlægges aktindsigt. På samme måde vil materiale fra private virksomheder kunne blive underlagt aktindsigt. Det foreslås derfor, at det tydeliggøres, når den kompetente myndighed anmoder om materiale i medfør af sine tilsynsforpligtelser, og at sådant materiale undtages fra aktindsigt, jf. også ovenfor.

I § 22 foreslås en række konkrete håndhævelsesforanstaltninger. Det fremgår af bemærkningerne s. 284, at en kompetent myndighed ligeledes kan give advarsler i form af henstillinger, der ikke kan sanktioneres med bøde. ATP skal foreslå, at dette skrives ind i lovteksten.

På samme måde som ovenfor under tilsyn skal ATP foreslå, at der også i § 22 fastsættes nogle rettigheder for de berørte enheder, fx i form af rimelige frister eller proportionale foranstaltninger. ATP har noteret, at det i § 26 foreslås, at enhederne høres, inden der iværksættes håndhævelsesforanstaltninger efter §§ 22, 23 eller 25, og at enhederne skal have en rimelig frist til at fremsætte bemærkninger. ATP skal foreslå, at denne frist præciseres, fx til minimum 14 dage, medmindre der er tungtvejende grunde til at fravige fristen.

I § 23 foreslås yderligere håndhævelsesforanstaltninger, herunder i stk. 1. nr. 2, mulighed for at forbyde personer med ledelsesansvar på niveau med administrerende direktør af udøve ledelsesfunktioner i den pågældende enhed. ATP vil gerne kvittere for præciseringen til CEO-niveau. Dette vil samtidig tydeliggøre, at denne foranstaltning ikke kan anvendes over for fx bestyrelsesmedlemmer. I § 23, stk. 3, foreslås det, at afgørelser kan forlanges indbragt for domstolene. Det kan overvejes at tilføje, at denne type sager har opsættende virkning, da frakendelser efter stk. 1 vil være af meget alvorlig karakter for en enhed.

ATP bemærker tillige, at det foreslås i stk. 4, at bestemmelserne i § 23, stk. 1-3, ikke gælder for offentlige forvaltningsenheder. ATP og de administrerede ordninger vil dermed ikke være omfattet af de foreslåede bestemmelser.

Endelig skal ATP bemærke, at det er vigtigt, at de kompetente myndigheder koordinerer tilsynet med cybersikkerhed. ATP kan blive underlagt tilsyn af op mod fire forskellige tilsynsmyndigheder vedrørende cybersikkerhed, og der opfordres derfor til, at myndighederne samtænker og koordinerer tilsynsopgaver på området.

Digital kommunikation

Det foreslås i § 31, at der kan fastsættes regler om digital kommunikation mv. Det fremgår af bemærkningerne s. 314, at det bl.a. kan gøres obligatorisk at anvende bestemte internetløsninger. Det fremgår også af bemærkningerne, at hvis enheden ikke selv kan opfylde betingelserne på grund af nedbrud i systemer mv., må der fx indberettes via en rådgiver. ATP skal bemærke, at fx i forbindelse med underretninger, vil disse skulle ske i forbindelse med hændelser, hvor det er sandsynligt, at enhedens digitale muligheder er kompromitterede. Ligeledes kan de offentlige selvbetjeningsløsninger være nede, fx MitID eller lignende. Det kan derfor overvejes at give mulighed for indberetninger på anden vis, fx telefonisk, hvis det ikke er praktisk muligt at tilgå de offentlige løsninger.

Lovforslagets konsekvenser

Det er beskrevet i bemærkningerne s. 180 ff., at de økonomiske konsekvenser endnu ikke fuldt ud kan opgøres. Da de nærmere krav til cybersikkerhed først vil blive udmøntet i efterfølgende bekendtgørelser, kan der gå lang tid, før de økonomiske konsekvenser kan opgøres. ATP skal dog opfordre til, at der ved fastlæggelse af mere konkrete sektorspecifikke krav også ses på de økonomiske omkostninger forbundet hermed, så der lægges vægt på tiltag, der giver mest sikkerhed for pengene. Lovforslaget vil have implementeringsomkostninger for ATP, herunder til teknik, processer og uddannelse.

Endelig fremgår det af bemærkningerne s. 184, at lovforslaget ikke vurderes at påvirke bl.a. virksomheders muligheder for at teste, udvikle eller anvende nye teknologier og innovation. ATP skal bemærke, at de foreslåede regler kræver et øget fokus på cybersikkerhed, herunder til dokumentation, hvilket også vil gælde for udvikling, test og implementering, samt risikostyring og -vurdering heraf. Samtidig kan de berørte enheder ifalde bøder, hvis dette ikke efterleves, hvorfor enhederne må forventes at være mere tilbageholdende med at afprøve nye teknologier, indtil det er bevist, at de overholder krævede sikkerhedsstandarder.

Generelt skal ATP opfordre til, at forpligtelser og stillede krav konkretiseres i de efterfølgende sektorbekendtgørelser, da de foreslåede regler i lovforslaget og tilsvarende bestemmelser i direktivet er blødt formulerede. Uklare og upræcise regler gør det vanskeligt for de omfattede enheder at sikre korrekt efterlevelse.

ATP står naturligvis til rådighed, hvis høringssvaret giver anledning til spørgsmål. Henvendelse kan rettes til director Lone Knudsen på lku@atp.dk.

Venlig hilsen

Haktan Bulut
Koncerndirektør, CITO

Mona Frandsen
Chefjurist

Skatteministeriet
Holmens Kanal 9
1060 København K
Att.: fmn@fmn.dk

Biogas Danmark
Axeltorv 3
1609 København V

22. august 2024

Høring af udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Forsvarsministeriet har lagt høring af udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau på Høringsportalen, **J. nr. 2024/004461.**

Biogas Danmark har noteret, at det fremgår af udkastets §1. stk. 2, at loven ikke finder anvendelse på enheder i energisektoren. Biogas Danmark skal anmode om en præcisering af, at dette er tilfældet og at loven dermed ikke relaterer sig til produktion og anvendelse af biogas. I forhold til implementering af NIS2 og CER-direktiverne på energiområdet skal Biogas Danmark henvise til de afgivne bemærkninger i høringen af lovforslaget vedrørende styrket beredskab i energisektoren.

Af bilag II til direktivet (udkastets side 129) fremgår virksomheder inden for affaldshåndtering at høre til i gruppen af Andre kritiske virksomheder. Disse defineres som virksomheder, der varetager affaldshåndtering, som defineret i artikel 3, nr. 9), i Europa-Parlamentets og Rådets direktiv 2008/98/EF, bortset fra virksomheder, for hvilke affaldshåndtering ikke er deres vigtigste økonomiske aktivitet.

Biogasanlæg håndterer også affald som defineret af ovennævnte direktiv, men affaldshåndteringen er ikke den primære økonomiske aktivitet. Biogas Danmark skal anmode om en præcisering af, at biogasanlæg derfor heller ikke er omfattet af loven inden for denne kategori.

Biogas Danmark stiller sig til rådighed for en uddybning af ovennævnte bemærkninger og ser frem til en afklaring i forhold til ovennævnte bemærkninger.

Med venlig hilsen

Bruno Sander Nielsen
2724 5967
bsn@biogas.dk

C.c.: jhb@fmn.dk

DeiC
DANISH INFRASTRUCTURE CONSORTIUM

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Vedr. høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Kære Forsvarsministeriet

Tak for muligheden for at afgive høringssvar i forbindelse forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

Vedlagt er DeiC/DKCERTs høringssvar, som er koordineret med Danske Universiteter.

Venlig hilsen

Gitte Julin Kudsk
Direktør for DeiC

og

Jacob Steen Madsen
Chef for DKCERT

15. august 2024

Eskil Sørensen
93511103
Eskil.sorensen@deic.dk

DeiC
DTU
Produktionstorvet
Bygning 426
2800 Kgs. Lyngby
Danmark

35 88 82 02
sekretariat@deic.dk
cvr 30 06 09 46
ean 5798000430686

Bemærkninger til NIS2 lovforslag

Kapitel 1

§1 Lovforslagets anvendelsesområde

Der bemærkes en bekymring over, at det kan blive meget omfattende hvis alle dele af sektoren omfattes af lovgivningen.

§3 - 3)

Paragraf 3 bør indeholde en definition af informationssikkerhed.
Definitionen bør ikke afvige fra tidligere anvendte definitioner, fx fra den nationale cyber- og informationssikkerhedsstrategi 2015-16 (side 2) og gentaget i national strategi for 2018-21 (side 7). Her hedder det:

"Informationssikkerhed
Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed. I arbejdet indgår blandt andet organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer for behandling af data, styring af leverandører samt tekniske sikringsforanstaltninger."

Eller CFCSs ordforklaring på CFCSs hjemmeside.
"Informationssikkerhed
Informationssikkerhed er bevarelsen af informationers fortrolighed, integritet og tilgængelighed. Informationssikkerhed er inddelt i følgende typer foranstaltninger: organisatoriske, personrelaterede, fysiske og teknologiske."

Det bemærkes, at den nationale strategi 2015-16 og 2018-21 også indeholder en definition af "cybersikkerhed", som afviger fra lovforslagets §3 3).

"Cybersikkerhed
Cybersikkerhed omfatter beskyttelse imod de sikkerhedsbrud, der opstår som følge af angreb mod data eller systemer via en forbindelse til et eksternt net eller system. Arbejdet med cybersikkerhed fokuserer således på sårbarheder ved sammenkoblingen mellem systemer, herunder forbindelser til internettet."

Kilde: https://digst.dk/media/13813/national-strategi-for-cyber-og-informationssikkerhed-2015-2016.pdf og
https://digst.dk/media/16815/national_strategi_for_cyber-_og_informationssikkerhed_pdfa.pdf

Lovforslagets §3 3) definerer cybersikkerhed således:
"Cybersikkerhed: De aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler."

Det bemærkes, at der generelt ikke bør være denne divergens.

§3 – 4): Cybertrussel

Cybertrussel defineres i lovforslagets §3 - 4) som "..enhver potentiel omstændighed, begivenhed eller handling, som kan skade, forstyrre eller på anden måde have en negativ indvirkning på net- og informationssystemer, brugerne af sådanne systemer og andre personer."

Som teksten er formuleret i lovforslaget dækker den alle former for trusler, men bør kun dække trusler fra cyberangreb.

Definitionen afviger ligeledes fra CFCSs definition, som den fremgår af https://www.fmn.dk/da/arbejdsomraader/cybersikkerhed/om-cybersikkerhed

"Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) definerer cybertrusler som trusler fra cyberangreb, hvor en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester."
Der bør være en gennemgående og enslydende definition af begreberne i lovforslaget som korresponderer med definitionerne på de relevante platforme.

§ 3 – 12): Hændelse
Det bemærkes, at i definitionen af "hændelse" bringes et fjerde element, nemlig autenticitet ind ud over de sædvanlige fortrolighed, integritet og tilgængelighed, der anvendes i definitionen af informationssikkerhed. Det fremgår af NIS2-teksten, at "autenticitet" også anvendes her. Det giver anledning til en præcisering i den danske lovteksts bemærkninger, hvad der menes hermed. Det bør ligeledes præciseres, om der er tale om en definition af en cyber-, it-sikkerheds- eller informationssikkerhedshændelse.

Dette forhold går igen i kapitel 5 §17 under CSIRT'ens opgaver, hvor det hedder, at CSIRT'en håndterer "it-sikkerhedshændelser". En følge af dette er, at §3 bør indeholde en definition af den type hændelser, som CSIRT'en håndterer.

§3 – CSIRT
Paragraf 3 bør indeholde en begrebsbeskrivelse af en CSIRT. Det bør også nævnes fx i kapitel 5, at en CSIRT dækker et nærmere defineret sektorområde og at der således af lovteksten fremgår at der er flere flere CSIRT'er og ikke kun én (som det fremstår, når "CSIRT'en" nævnes i bestemt form).

§6 - 1) Politikker for risikoanalyse og informationssystemsikkerhed
Det fremgår af § 6, at foranstaltninger til styring af informationssikkerhedsrisici "..bør omfatte politikker for risikoanalyse og informationssystemsikkerhed". Det fremgår ikke, hvad "informationssystemsikkerhed" er. DKCERT er af den opfattelse, at "politikker for risikoanalyse og informationssystemsikkerhed" er en delmængde af politik for informationssikkerhed. Med en definition af informationssikkerhed i §3 vil det være tilstrækkeligt at stille krav om, at der skal være en politik for "informationssikkerhed".

§6 - 7) Cyberhygiejnepraktisser og cybersikkerhedsuddannelse
De to begreber kan med fordel skilles ad, da der ikke nødvendigvis er sammenhæng mellem uddannelse og hygiejne. Man kan sagtens iagttage god cyberhygiejnepraksis uden cybersikkerhedsuddannelse. Hvad der menes med uddannelse kan også med fordel præciseres.

§6 9) Personalesikkerhed
Det bør uddybes hvad der menes, fx om der er tale om fysisk sikkerhed af personalet eller om der fx er tale om det at screene personale.

§12 stk. 2:
Definitionen af en "væsentlig hændelse" synes meget lav.

§13 stk. 1 og 2:
Fristen for anmeldelse af hændelse er meget kort.

§17 CSIRT'ens opgaver
Der lægger op til mange flere opgaver, end hvad en traditionel CSIRT dækker. I den pågældende beskrivelse lyder det mere som en SOC og som forensic-arbejde.

Bemærkninger til bilag 1 EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU)
DKCERT bemærker til bilag 1 "EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU)", at der i afsnit 60) side 38 og fremefter anvendes begrebet "informationssikkerhedsforskere."

Dette begreb anvendes i forbindelse med en passus i teksten om behovet for fastlæggelse af en relevant national politik om offentliggørelse af sårbarheder. DKCERT bemærker, at "informationssikkerhedsforskere" formentlig er direkte oversat fra det engelsk/amerikanske udtryk "information security researcher". En "researcher" kan ganske vist direkte oversættes til "forsker" på dansk, men i denne kontekst har information security researcher / "informationssikkerhedsforsker" meget lidt at gøre med traditionel forskning, som udføres i uddannelses- og forskningssektoren.

De personer – informationssikkerhedsresearchere – der henvises til, som finder og i mange tilfælde lever af at finde sårbarheder i software og indmelde med til softwareproducenter under producenternes bug bounty-programmer, er typisk fritids eller professionelle softwareeksperter, white/gray/black hat hackere, "script kiddies" osv, der ikke udfører "forskning" i traditionel forstand.

Det vil derfor efter DKCERTs opfattelse være forkert at bruge betegnelsen "informationssikkerhedsforskere". Det kan føre til misforståelser ved introduktion af begreber, hvor oversættelsen ikke er velovervejet.

DKCERT opfordrer generelt myndighederne til at være meget varsom ved direkte oversættelser af engelsk/amerikanske begreber og foreslår nedsættelse af et udvalg med deltagelse af relevante eksperter, herunder sprogfolk, der en gang for alle etablerer et begrebsbibliotek med præcise og nøjagtige danske definitioner, der tager hensyn til en dansk tradition og kontekst.

Det er almindeligt anerkendt, at mange udfordringer med cyber- og informations-sikkerhed skyldes dårlig kommunikation og manglende forståelse mellem forskellige fagdiscipliner, der er involveret i arbejdet med informationssikkerhed. Med grundighed omkring introduktion af oversatte begreber, kan ikke alt, men noget af den manglende forståelse forhindres.

Danmarks Apotekerforening
Bredgade 54 · 1260 København K
Telefon 33 76 76 00 · Fax 33 76 76 99
apotekerforeningen@apotekerforeningen.dk · www.apotekerforeningen.dk

Forsvarsministeriet
Holmens Kanal 9
1060 København K

22-08-2024
MKA/623/00185

Svar på høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Forsvarsministeriet har den 5. juli 2024 sendt udkast til lovforslag om foranstaltninger til sikring af et højt cybersikkerhedsniveau i høring.

Danmarks Apotekerforening takker for muligheden for at kommentere lovudkastet og skal i den anledning fremkomme med nedenstående bemærkninger.

Lovforslaget er en delvis gennemførelse af Europa-Parlamentets og Rådets direktiv fra 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2-direktivet). Der synes efter Apotekerforeningens umiddelbare vurdering at være en tekstnær implementering af direktivet, herunder vedrørende for så vidt angår omfattede enheder, krav til de omfattede enheder og ikrafttrædelsesbestemmelser.

Der er tale om et ganske omfattende og forholdsvis "teknisk" materiale blandt andet i forhold til vurderingen af, hvilke konkrete enheder, der er omfattet af reguleringen samt de økonomiske konsekvenser heraf for erhvervslivet. Det fremgår således af bemærkninger til lovudkastet, at der ikke er fuldt overblik over, hvor mange danske virksomheder, der vil blive omfattet, ligesom det fremgår, at det på nuværende tidspunkt er vanskeligt at estimere de økonomiske konsekvenser for erhvervslivet.

I bilag til direktivet og lovforslaget er sundhed nævnt under sektorer af særligt kritisk betydning, og som – hvis der er tale om mellemstore virksomheder – vil være omfattet af direktivet. Herunder er blandt andet sundhedstjenesteydere som defineret i artikel 3, litra g, i EU-direktiv 2011/24/EU.

Apoteker er omfattet af definitionen "sundhedstjenesteydere" i artikel 3, litra g, i EU-direktiv 2011/24/EU.

Danmarks Apotekerforening lægger imidlertid til grund, at de enkelte apoteker – uanset størrelse og omsætning – ikke er direkte omfattet af direktivet, men at apotekernes IT-systemleverandører vil være omfattet.

Det skyldes, at en ”hændelse” på det enkelte apotek jf. definitionen i Artikel 2, stk. 2c ikke "*vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden*" og ikke vil forstyrre/hindre borgeres adgang til lægemidler. Der er således en relativ let tilgængelighed til receptekspederende enheder i hele landet, ligesom der findes mulighed for at bestille og få tilsendt lægemidler fra andre apoteker i et tilfælde, hvor et lokalt apotek på grund af en hændelse ikke måtte være i stand til at betjene borgerne.

Apoteker i Danmark har pligt til at holde åbent i et nærmere bestemt antal timer om ugen. Er apoteket af en udefra kommende årsag forhindret heri, kræver det underretning til og dispensation fra sundhedsmyndighederne. Apotekerne er herudover allerede i dag underlagt en række sektorspecifikke krav, som omfatter tyverisikring, temperaturkontrol, skadedyrsforebyggelse m.v.

I bilag 2 er også nævnt enheder, der fremstiller farmaceutiske råvarer og farmaceutiske præparater som omhandlet i hovedafdeling C, hovedgruppe 21, i NACE rev. 2.

I Danmark er der 2 private apoteker, som fremstiller såkaldte magistrelle lægemidler. Der er tale om lægemidler, som tilberedes på et apotek til den enkelte patient efter recept fra en læge.

Danmarks Apotekerforening lægger til grund, at disse apoteker heller ikke er omfattet af direktivet, idet Apotekerforeningen går ud fra, at NACE rev. 2 hovedafdeling C, hovedgruppe 21, omfatter større industriel fremstilling af farmaceutiske præparater mv. Apoteker, der fremstiller magistrelle lægemidler, udfører ikke industriel produktion af lægemidler i stor skala. Hertil kommer, at de danske sygehusapoteker kan fremstille magistrelle lægemidler og under visse betingelser forhandle disse til private apoteker med henblik på udlevering til borgerne.

Da hovedparten af apotekernes virksomhed er baseret på IT-systemer fra to systemleverandører, er det som nævnt ovenfor til gengæld Apotekerforeningens opfattelse, at disse IT-systemer være omfattet af direktivet.

Med venlig hilsen

Henrik Bruun

DANSK ERHVERV
Børsen
1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. + 45 3374 6000

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sagsnummer 2024/004555

Den 22. august 2024

Høringssvar til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Dansk Erhverv takker for muligheden for at give input til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

I lyset af det forhøjede trusselsniveau mod danske virksomheder fra cyberangreb som følge af den geopolitiske situation i Europa, af øget digitalisering og øget tilgængelighed af cybervåben, er det meget positivt, at reguleringen omkring virksomhedernes beredskab nu styrkes. Danmarks digitale sikkerhed er et vigtigt konkurrenceparameter og rammevilkår for danske virksomheder, og den er derfor afgørende at styrke i takt med den digitale udvikling.

På den korte bane er cybertruslen den mest konkrete og alvorlige trussel mod Danmark, og den hastige digitale udvikling åbner nye flanker for kriminelle og statslige aktører. Derfor er det godt, at myndighederne nu implementerer de fælleseuropæiske cybersikkerhedsregler med målsætningen om at styrke cybersikkerheden og øge modstandsdygtigheden i Danmark.

Generelle bemærkninger

Dansk Erhverv bakker op om lovforslagets risikobaserede tilgang, der tillader en metodefleksibilitet for de enheder, der skal kunne reagere på de aktuelle cybersikkerhedsricisi, som loven pålægger enhederne et ansvar for. Imidlertid er der en risiko for, at mangel på klare definitioner kan føre til ineffektiv, utilstrækkelig og uens implementering på tværs af sektorer, brancher og grænser. Det er derfor afgørende for implementeringen af de nye cybersikkerhedskrav, at denne lov snarest følges op med de anmeldte sektorspecifikke bekendtgørelser og konkret vejledning til virksomhederne.

Lovforslaget bemyndiger ressortministerier at fastsætte nærmere regler i bekendtgørelsesform. Disse beføjelsesrammer kan være fordelagtige for så vidt angår fundamentale forskelle mellem sektorer, såsom sektorernes digitale modenhed, systemiske risici (fx grænseoverskridende virkning) og enhedernes samfundskritiske karakter. Samtidig vækker beføjelsesrammerne bekymring for, at enheder kan blive ramt med forskellige krav og tilsynskoncept/-metode. Hvis de nationale ressortbetingede krav ikke er i overensstemmelse med direktivets risikobaserede tilgang, er det dertil en bekymring hos Dansk Erhverv, at de tiltag, som en enhed foretager i et land, ikke kan an-

ses for fyldestgørende for overholdelse af NIS2-krav i et andet land. Både bekendtgørelser og vejledninger bør i videst muligt omfang være ensartet på tværs af brancher og grænser. Det er således også nødvendigt for en effektiv og byrdefri implementering, at Danmark arbejder aktivt for harmonisering af NIS2-direktivets implementering på tværs af EU's medlemsstater.

Dansk Erhverv anbefaler i øvrigt, at Forsvarsministeriet eller Center for Cybersikkerhed snarest muligt fremlægger en detaljeret oversigt over de forskellige sektoransvarlige myndigheder, som omfattede enheder kan modtage vejledning fra og rette henvendelse til.

Erhvervspolitiske konsekvenser
Det bemærkes, at de nationalt sikkerhedsbetingede krav kan medføre øgede omkostninger. F.eks. kan kravene til sikkerhedsgodkendelser, baggrundstjek og datalokation være omkostningsdrivende for leverandører og producenter. Desuden virker det ikke til, at de erhvervsøkonomiske konsekvenser for virksomhedernes internationale aktiviteter er med i de beregnede konsekvenser.

Grundig lovteknisk gennemgang af lovforslaget
Der bør gennemføres en grundig lovteknisk gennemgang af lovforslaget. Gennemgangen skal bl.a. sikre, at tiltænkte virksomheder er omfattet af loven, samt at de anvendte begreber stemmer overens med anden gældende dansk lovgivning på området – bl.a. dansk implementeringslovgivning af samme direktiv i andre sektorer (tele, energi og finans). Gennemgangen skal yderligere sørge for, at lovforslagets bemærkninger giver en klar og entydig vejledning til fortolkning af loven og de dertilhørende bemyndigelser – der er forståelig for omfattede virksomheder.

Dansk Erhverv anbefaler dertil, at danske myndigheder lader sig inspirere af EU-Kommissionens gennemførelsesretsakter, hvor retsakterne følger direktivets risikobaserede tilgang, således at der i videst muligt omfang bliver implementeret ens på tværs af EU's medlemsstater.

Konkrete bemærkninger
Anvendelsesområdet
Det fremgår af lovforslaget, at væsentlige og vigtige enheder selv skal registrere sig hos den relevante, kompetente myndighed. Det er Dansk Erhvervs overbevisning, at det vil blive vanskeligt for mange danske enheder at vurdere, om de er omfattet af loven. Det er i den henseende vigtigt, at der tages højde for, hvad der er muligt i de respektive enheder. Registreringen skal være pragmatisk – bl.a. af hensyn til danske virksomheder med globale markeder, hvor fx kortlægning af netværk og IP kan være administrativt byrdefuldt at dokumentere. Af lovforslagets §9 stk. 2 fremgår det i øvrigt, at selvregistreringen skal ske senest d. 17. januar 2025. Dansk Erhverv anbefaler, at man i stedet skriver d. 17. april 2025 ligesom i §10, idet loven først træder i kraft den 1. marts 2025, og virksomheder dermed ikke kan forpligtes af loven inden.

For så vidt angår størrelseskravet/bagatelgrænsen i lovens anvendelsesområde forstår Dansk Erhverv artikel 2 i bilaget til henstilling 2003/361/EF således, at en enhed kun kan undtages fra lovens anvendelsesområde såfremt, enheden har under 50 ansatte *og* en årlig omsætning eller en samlet årlig balance på ikke over 10 mio. EUR. I flere sektorrelevante myndigheders vejledningsmateriale fremgår det imidlertid, at enhederne skal beskæftige mindst 50 personer og have en år-

lig omsætning eller en samlet årlig balance på over 10 mio. EUR. Når ordlyden i vejledningsmaterialet får omvendt (positivt) fortegn, vil færre enheder end hensigten i direktivet være omfattet af loven, da en enhed med fx 30 ansatte og en årlig omsætning på 3 mia. EUR ikke dækkes af vejledningsmaterialets ordlyd. Hvis myndighederne holder fast i denne formulering, bør de skrive, at "enheder skal beskæftige mindst 50 personer *eller* have en årlig omsætning eller en samlet årlig balance på over 10 mio. EUR."

Det er uklart, om virksomheder, der primært leverer telekommunikation, men som også har digitale tjenester, kan blive omfattet af både denne lov og lov om cybersikkerhed i telesektoren. For at undgå at selskaber underlægges to overlappende reguleringer med forskellige krav og myndigheder indenfor samme område, opfordrer Dansk Erhverv til, at virksomheden kun reguleres i én lov. Det er også uklart, om holdingselskaber, der er koncernforbundne med selskaber, som omfattes af nærværende lovforslag, også omfattes af lovens anvendelsesområde.

Der lægges i loven op til, at kommuner, der udfører aktiviteter i flere af de sektorer, der er omhandlet i direktivets bilag, kan blive omfattet som enten væsentlig eller vigtig enhed alt afhængig af kommunens aktivitet. Dansk Erhverv anbefaler imidlertid, at kommunerne utvetydigt omfattes af denne implementeringslov for at imødegå cybertruslen, i hvilken forbindelse de nye cybersikkerhedsregler i denne lov er en god mulighed for at løfte det generelle sikkerhedsniveau i Danmark. Det er i den forbindelse væsentligt, at loven præciserer i hvilket omfang, kommunerne er omfattet. Det er dertil uklart, hvornår kommuner har offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, og Dansk Erhverv anbefaler, at der gives eksempler herpå.

Håndhævelse og rapportering
En række af Dansk Erhvervs medlemmer efterspørger en afklaring om hændelsesrapportering for globale virksomheder. Der mangler bl.a. en afklaring på, i hvor mange lande, og hos hvor mange myndigheder, enheder skal hændelsesrapportere. Dansk Erhverv anbefaler, at enheder kun behøver at hændelsesrapportere hos én myndighed, og at det vil være op til myndighederne at koordinere og videndele.

For så vidt angår håndhævelsen af lovgivningen, har erfaringer fra energi- og telesektoren vist, at det vil lette den administrative byrde markant, hvis man følger samme tilsynskoncept/-metodik, hvis timingen for tilsyn koordineres mellem myndigheder, samt hvis man sammenlignet med håndhævelse under NIS-loven opnår en bedre sammenhæng og harmonisering af tilsyn mellem de forskellige tilsynsførende myndigheder. Tilsyn kan ses som et redskab til konstruktiv og proaktiv dialog og fungerer bedst i følgeskab med rådgivning i form af f.eks. operative risikovurderinger, vejledninger, kurser og standardhenvisninger. Den rolle har Energistyrelsen indtil nu udfyldt tilfredsstillende. Det er vigtigt, at hændelsesrapportering, tilsyn og håndhævelse ikke i sig selv kommer til at udgøre en stor administrativ belastning.

Det er ligeledes afgørende, at samtlige NIS2-relevante myndigheder sikrer klar og transparent adskillelse mellem det regulatoriske tilsyn og deres rådgivende funktion.

Sidst anbefaler Dansk Erhverv, at de sektorrelevante myndigheder fremlægger information om proces og format for tilsyn hurtigst muligt, så virksomhederne bedst muligt kan forberede sig. I den forbindelse er det afgørende, at myndighederne forholder sig til eventuelle overlap i deres andre typer af tilsyn med samme enheder.

Ledelsesansvar
Sidst vil Dansk Erhverv anføre, at omtalen af ledelsesansvar i bemærkningerne til lovforslaget er vidtgående, og særligt er der tvivl om, om der er den rigtige balance mellem det overordnede ledelsesansvar, der ligger hos direktion og bestyrelse og en specifik godkendelse af nogle meget detaljerede og tekniske risiko- og sårbarhedsvurderinger og beredskabsplaner mv. Den overordnede ledelses rolle bør i mere generelle vurderinger af sikkerhedsniveauet som eksempelvis en modenhedsanalyse af sikkerhedsberedskabet og af hensyn til ressourceallokering.

Standarder
Dansk Erhverv bakker op om, at medlemsstaterne i EU bør fremme væsentlige og vigtige enheders anvendelse af relevante europæiske og internationale standarder. Cybersikkerhed – og lovmedholdighed med nye cybersikkerhedsregler – er et "moving target"; det, der var passende sikkerhedsforanstaltninger forrige år, kan have ændret sig med det eskalerende trusselsbillede. Derfor er cybersikkerhed en praksis, som enhederne skal sætte i system, hvor de løbende skal evaluere og potentielt opjustere de foranstaltninger, de har implementeret. Mange virksomheder har imidlertid svært ved at vurdere deres risikoprofil og dermed implementere passende IT-sikkerhedsforanstaltninger. Mange har behov for en omkostningseffektiv og intuitiv løsning, der kan hjælpe dem med

1. at få overblik over deres nuværende niveau,
2. at komme i mål og leve op til lovens krav.

D-mærket som standard kan være et godt værktøj for virksomhederne til at skabe ensartede, tydelige og transparente krav til virksomhedernes cybersikkerhed. Dansk Erhverv anbefaler derfor, at regeringen og de sektorrelevante tilsynsmyndigheder anbefaler D-mærket som et af værktøjerne til at dokumentere NIS2-lovmedholdighed. Særligt ser vi D-mærket som en mulighed for, at små og mellemstore virksomheder kan komme i mål med cybersikkerheden.

Dansk Erhverv opfordrer generelt til grundig og konstruktiv markedsdialog om udmøntningen af lovgivningen i kommende bekendtgørelser.

Dansk Erhverv står selvfølgelig til rådighed i tilfælde af opfølgende spørgsmål.

Med venlig hilsen

Joen Magieres
Politisk konsulent

Dansk Industri

21. august 2024

Forsvarsministeriet
Sendt pr. mail til:
fmn@fmn.dk
jbh@fmn.dk (cc)
Sagsnummer: 2024/004461

Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Indledende bemærkninger

Dansk Industri (DI) vil gerne takke for muligheden for at afgive høringssvar på Forsvarsministeriets lovudkast om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-direktivet). Formålet med NIS2-direktivet er at sikre et højt fælles cybersikkerhedsniveau på tværs af EU, hvilket er både nødvendigt og rettidigt for at imødegå den voksende trussel fra cyberangreb.

DI vil gerne takke for et gennemarbejdet lovudkast, som indeholder flere gode aspekter. Vi støtter op om en tekstnær minimumsimplementering med henvisning til principperne i Justitsministeriets vejledning om lovkvalitet og Erhvervsstyrelsens vejledning om principper for implementering af erhvervsrettet EU-regulering. En sådan tilgang vil være med til at sikre, at erhvervslivet ikke pålægges unødvendige byrder, som kan stille virksomheder underlagt dansk regulering dårligere i den internationale konkurrence. Harmonisering på EU-niveau er afgørende for et konkurrencedygtigt indre marked. Virksomheder, der opererer på tværs af lande grænser og i flere sektorer, skal i videst muligt omfang rammes af ensartede krav. Derfor opfordrer DI til, at NIS2- og CER-direktiverne samt Klima-, Energi- og Forsyningsministeriets udkast til lovforslag om styrket beredskab i energisektoren, der implementerer NIS2- og CER-direktivet for energisektoren, behandles samtidig i Folketinget. Dette vil understøtte muligheden for at skabe koordination og ensartethed på tværs af sektorer, i det omfang der ikke er grundlag for særregler i lyset af særlige sektorvise forhold og trusler.

For at undgå en situation som var tilfældet med forgængeren NIS1, der blev implementeret forskelligt på tværs af medlemslandene, er det ligeledes afgørende, at regeringen deltager aktivt i EU-Kommissionens arbejde med henblik på at sikre, at reglerne bliver ensartet på tværs af EU, samt at udmøntningen af de danske krav baseres på anerkendte og anvendte standarder. Standarder kan bidrage til at sikre en ensrettet tilgang på tværs af medlemslandene og kan styrke det generelle cybersikkerhedsniveau på tværs af medlemslandene via en fælles tilgang.

H. C. Andersens Boulevard 18
1553 København V
Danmark

(+45) 3377 3377
di@di.dk
di.dk

CVR-nr.:16077593

Med et så omfattende lovforslag, der stiller en lang række organisatoriske og tekniske krav, samt håndhævelsesforanstaltningerne taget i betragtning, bør der være en rimelig implementeringsperiode efter ikrafttrædelsestidspunktet, så virksomhederne får mulighed for at implementere de nye omfattende krav, inden tilsynet begynder. Efterlevelse vil kræve mange ressourcer – såvel i tid som i omkostninger – og der skal ganske enkelt være rimelige rammer til dette. Således burde virksomhederne under normale omstændigheder have mindst 12-18 måneder til at tilpasse sig de nye krav. DI understreger samtidig, at vi står i en situation, hvor truslen mod vores digitale infrastruktur og virksomheder fortsat spidser til, og hvor det er vigtigt, at vi får løftet sikkerhedsniveauet på tværs af sektorer. Det er imidlertid DI's bekymring, at den korte implementeringshorisont mange steder vil føre til mere fokus på compliance snarere end reelle forandringer. Den nuværende korte periode er resultatet af en forsinket lovproces, og kan for virksomheder, der er omfattet af lovgivning, vise sig, at være urimeligt kort for at sikre overholdelse. Derfor mener DI, at virksomhederne skal have 12 måneder eller som minimum seks måneder til at efterleve kravene. Ikrafttrædelsesdatoen bør vel at mærke først ligge minimum seks 6-12 måneder efter, at indholdet i de sektorvise bekendtgørelser er kendt og vedtaget.

Lovudkastet er i høj grad en rammelovgivning, der indeholder en lang række ministerbemyndigelser, hvilket gør det vanskeligt at vurdere omfanget, rækkevidden og proportionaliteten af de krav og forpligtelser, som vil blive udmøntet i de kommende bekendtgørelser. Det er derfor afgørende, at de sektorvise bekendtgørelser sendes i høring med en rimelig hørings frist, så virksomhederne har mulighed for at gøre opmærksom på indbyrdes modsatrettede regler samt anvendte sektor-specifikke standarder og forhold**.** Dette høringssvar vil derfor fremhæve elementer i lovudkastet, der umiddelbart ikke fremstår tilstrækkeligt klare og afgrænsede samt betone principielle overvejelser, der bør vægtes i arbejdet med at fastsætte de konkrete bestemmelser.

Det er op til virksomhederne selv at registrere sig, formentlig via Virk.dk, hvis virksomhedens service er omfattet af reglerne og det kommende tilsyn. Selvom lovudkastet indeholder en række kriterier for, hvornår en virksomhed er omfattet, er der fortsat uklarheder og gråzoner, fx hvad angår virksomheder, der er omfattet uanset størrelse, samt virksomheder, der opererer i flere omfattede sektorer. Myndighederne bør derfor, som led i den forestående vejledningsopgave og i de sektorvise bestemmelser, etablere en mulighed for at virksomheder kan få afklaret, om deres service er omfattet af reglerne og det kommende tilsyn. Dertil bør myndighederne vejlede virksomhederne i forhold til at forstå, i hvilket omfang deres underleverandører er omfattet. Af lovudkastet fremgår det, at første led i leverandørkæden er omfattet, men det specificeres ikke nærmere i hvilke tilfælde underleverandører er omfattet, og om leverandører vil skulle efterleve samme krav som den direkte omfattede virksomhed. Til sidst vil DI indledningsvist fremhæve, at der er behov for vejledning omkring detaljeringsgraden for underretninger om væsentlige hændelser samt afklaring omkring tærsklen for, hvornår en hændelse reelt er væsentlig i et samfundsperspektiv.

Kapitel 1 Anvendelsesområde, jurisdiktion og definitioner

En enhed, der omfattes af lovens anvendelsesområde, skal selv identificere sig som omfattet og registrere sig på en fælles digital platform. Dette står i modsætning til NIS1-direktivet, hvor medlemsstaterne havde ansvaret for at identificere omfattede enheder. Denne ændring fra NIS1 stiller krav til en større vejledningsindsats, der skal gøre det klart og tydeligt for virksomheder, om de bliver omfattet. Det er for nuværende uklart for mange virksomheder, om de er underlagt NIS2-loven. Det skyldes fraværet af tydelig præcisering i lovbemærkningerne af, hvilke virksomheder der reelt er omfattet, herunder hvilke virksomheder der uanset direktivets størrelsesrelaterede minimumskriterier, vil være omfattet af lovens forpligtelser. DI opfordrer til, at de sektoransvarlige myndigheder prioriterer vejledningsindsatsen herom. Henset til, at det for mange virksomheder vil være administrativt byrdefuldt at implementere foranstaltningerne, og at der følger skrappe sanktioner med, hvis man er omfattet, men ikke følger direktivet, bør det være tydeligt for virksomheder, om de er underlagt direktivet.

§ 3 Definitioner

DI finder det positivt, at lovforslaget indeholder definitioner af centrale begreber, der afspejles af tilsvarende definitioner i NIS2- og CER-direktiverne. Vi ser dog en række centrale begreber, der ikke defineres i lovudkastet til CER-direktivet og eksempler på overlap i definitioner, hvilket skaber uklarhed. Det er vigtigt, at alle definitioner fra direktivet føres over fra direktivet til dansk lov. Det synes ikke at være tilfældet nu, da der definitioner af centrale begreber, der relaterer sig til cybersikkerhed, ensartes er 41 definitioner i direktivet, men kun 32 i lovudkastet. DI opfordrer til, at på tværs af direktiverne, da dette er med til at styrke forståelsen og skabe klarhed og konsistens. Det bør desuden sikres, at definitionerne er i overensstemmelse med definitionerne i andet eksisterende EU-lovgivning, såsom DSA'en, hvor fx "onlinemarkedsplads" og "Platform for sociale netværkstjenester" er defineret anderledes end i dette lovudkast. Dette kan skabe unødig forvirring i forbindelse med at identificere hvilke digitale tjenester, der er omfattet af lovgivningen.

§ 4, stk. 3, nr. 5, om virksomheder, der anses for at være væsentlige uanset størrelse

Det fremgår af ovennævnte paragraf, at visse typer af virksomheder vil blive anset for at være væsentlige uanset størrelse. DI understreger, at disse kvalitative kriterier bør defineres ud fra en risikobaseret tilgang og i tæt dialog med de pågældende virksomheder, så det sikres, at der ikke stilles uforholdsmæssigt høje krav i forbindelse med tilsyn for en række virksomheder, der reelt ikke bør anses som af særlig kritisk betydning for økonomien og samfundet.

Afgrænsningen mellem vigtige og væsentlige enheder

Der er mange virksomheder, der udøver aktiviteter i flere af de sektorer, der omtales i direktivets bilag, og vi vil se situationer, hvor virksomheder ud fra en vurdering i én sektor vil være betragtet som vigtige, mens samme virksomhed vil være betragtet som væsentlig ud fra en vurdering af aktiviteterne i en anden sektor. Det fremgår af Forsvarsministeriets bemærkninger, at en virksomhed i en sådan situation som helhed vil skulle anses for en væsentlig enhed, hvis virksomheden i én sektor lever op til kriterierne for at være en væsentlig enhed. Det er uklart, hvor stor en andel af virksomhedens aktiviteter der

skal vurderes som væsentlige, før hele virksomheden vil betragtes som væsentlig. For eksempel i tilfælde, hvor en virksomheds energiproduktion (fx fra solcelleanlæg) udgør mindre end 1% af dens samlede aktivitet, vil virksomheden da anses for at være en væsentlig enhed og derved underlægges krav for væsentlige enheder (NIS2- og CER-direktiverne)?

Grænsen for, hvornår en virksomhed betegnes som kritisk for energiforsyningen, er sat lav, og DI finder igen lejlighed til at fremhæve, at myndighederne, herunder Forsvarsministeriet og Klima-, Energi- og Forsyningsministeriet, der har ansvar for at implementere NIS2- og CER-direktiverne, i fællesskab og i dialog med repræsentanter fra de samfundskritiske sektorer skal afdække sektorernes gensidige afhængigheder og på den baggrund definere, hvad der reelt anses som samfundskritisk infrastruktur, og hvad der bør beskyttes som sådan. Det er afgørende, at der er en høj grad af proportionalitet mellem de pålagte regler og virksomhedens kritikalitet for økonomien og samfundet.

Kapitel 2 Foranstaltninger til styring af cybersikkerhedsrisici

Da der er tale om rammelovgivning, er det vanskeligt at vurdere omfanget, rækkevidden og proportionaliteten af de krav til foranstaltninger til styring af cybersikkerhedsrisici. Indledningsvist vil DI understrege, at der som følge af uklarhed omkring krav til underleverandører er risiko for, at direkte omfattede virksomheder vil skubbe alle krav ned i leverandørkæden for at sikre overholdelse. Dette kan medføre uforholdsmæssigt store byrder for leverandører, og der bør sikres en risikobaseret tilgang og vejledning omkring, i hvilket omfang leverandørers leverancer også er omfattet.

Ensartethed i basiskrav på nationalt og internationalt plan

DI efterspørger en ensartet linje på tværs af sektorer, hvad angår udformningen af §6, da flere virksomheder vil være omfattet af mere end én sektor, fx både telesektoren og energisektoren, i det omfang at der ikke er grundlag for særregler i lyset af særlige sektorvise forhold og trusler. Det er uhensigtsmæssigt, hvis man som virksomhed bliver stillet overfor forskellige detailkrav til styring af cybersikkerhedsrisici, og det er derfor vigtigt, at den ensartede baseline skabes ud fra laveste fællesnævner i stedet for højeste fællesnævner. Vi støtter en tekstnær minimumsimplementering og opfordrer til, at bestemmelserne til §6 vil følge denne tilgang. Det vil gøre virksomhederne i stand til, på baggrund af en konkret risikovurdering, at vurdere og implementere et passende niveau af foranstaltninger indenfor rammen af minimumskravene.

Der lægges op til en implementering, der følger sektoransvarsprincippet, og hvor bekendtgørelser med sektorspecifikke bestemmelser om foranstaltninger til styring af cybersikkerhedsrisici kan forhandles af vedkommende ressortministerium med CFCS for at sikre ensartethed og koordination på tværs af sektorer. DI opfordrer til, at der afsættes passende ressourcer til dette store arbejde med at skabe enartedhed på nationalt plan, og til at de kommende bekendtgørelser sendes i høring med en rimelig høringsfrist, så virksomheder i omfattede sektorer og branchefællesskaber har mulighed for at komme med input, gøre opmærksom på indbyrdes modsatrettede regler, sektorspecifikke forhold samt anvendte standarder, som kravene bør være i overensstemmelse med. Samtidig bør regeringen under-

søge, hvordan øvrige EU-lande implementerer direktivet med henblik på at sikre, at internationale virksomheder i Danmark ikke skal tilpasse sig 27 forskellige fortolkninger af samme lov, hvilket vil gøre det meget svært at navigere i de forskellige regelsæt med risiko for sanktioner.

Minimumsimplementering og overensstemmelse med standarder, ikke detailregulering
CFCS bør i modelbekendtgørelsen lægge op til at de sektorspecifikke bestemmelser om krav til foranstaltninger bør følge principperne om hensigtsmæssighed, proportionalitet og hensyntagen til implementeringsomkostningerne. Tiltag i den konkrete udmøntning, der mindsker den administrative byrde og som hjælper virksomheder med hurtigere at tilpasse sig og styrke samfundets modstandsdygtighed, er nødvendige. Det vil indebære vejledning, men også klare krav, der er hægtet op på anvendte og anerkendte internationale og europæiske standarder. Udgangspunktet for NIS2-direktivet er, at virksomhederne skal arbejde ud fra en risikobaseret tilgang og implementere "*passende planlægning og træffe passende cybersikkerhedsforanstaltninger*". Derfor anbefaler DI grundlæggende, at myndighederne undgår detailregulering, som løbende vil skulle justeres og tilpasses som følge af ændrede trusler, teknologi udviklingen, nye metoder og standarder, mv., hvilket vil være omkostningstungt. Eventuelle tekniske detailkrav vil risikere at begrænse den teknologiske udvikling og virksomhedernes optag af ny teknologi.

Standarder bidrager til at sikre en ensrettet tilgang på tværs af medlemslandene og kan styrke det generelle cybersikkerhedsniveau på tværs af medlemslandene via en fælles tilgang. Intentionen om, at der i nationale lovtekster bør henvises til internationale standarder, understreges flere steder i direktivet. I direktivets artikel 21 om foranstaltninger står der, at *"...foranstaltningerne, under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder* (...) *skal tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene"*. Udkastet til den danske lovtekst nævner ikke europæiske og internationale standarder, hvilket ikke er hensigtsmæssigt, da ambitionen med NIS2 er at have en fælles tilgang. Det bør derfor fremgå tydeligt i §6 stk. 3 at de nærmere regler om foranstaltninger bør henvise til internationale standarder såsom ISO/IEC 27001, ISO/IEC 27002 eller lignende standarder. På samme måde stiller DI sig kritiske overfor, at Forsvarsministeriet har valgt at udelade artikel 25 om standardisering, hvor det fremgår at medlemsstaterne tilskyndes "... *til at benytte europæiske og internationale standarder og tekniske specifikationer, der er er relevante for sikkerheden i net- og informationssystemer for at sikre en samordnet gennemførelse af artikel 21 stk. 1 og 2*". At udelade dette er ikke i overensstemmelse med tilgangen om en direktivnær minimumsimplementering. Andre medlemslande bibeholder desuden referencen til standarder, og derfor bør den danske lov også tydeligt henvise til international og europæiske standarder. Risikoen ved ikke at tydeligt henvise til standarder er, at danske virksomheder ikke bliver opfordret til at anvende de samme redskaber som andre europæiske virksomheder, hvilket potentielt kan stille dem ringere i en konkurrencemæssig situation. DI understreger behovet for metodefrihed i forhold til valg af standard, og derfor er det vigtigt, at lovteksten ikke refererer til konkrete standarder.

NIS2 ikke er en market access produktlovgivning, dog vil DI referere til 'New Legislative Framework' (vedtaget i 2008), der inkluderer principper om, at lovkrav ikke bør være overdrevent detaljerede og

tekniske, men derimod kun indeholde klare og væsentlige krav, og overlade de specifikke tekniske detaljer til frivillige tekniske standarder.

En sådan tilgang vil bidrage til at skabe klarhed og harmonisering, der er afgørende for virksomheder, og reducere de øgede administrative byrder, der er steget markant i de seneste år med de mange digitale lovpakker, der er vedtaget i EU. DI opfordrer til en tæt dialog mellem ressortmyndighederne og virksomhederne om, hvordan de nærmere regler om krav til foranstaltninger kan fastlægges, så vi sikrer, at de konkrete krav og tilsyn er hægtet på det allerede eksisterende sikkerhedsarbejde i sektorerne (se kapitel 6). Dertil bør myndighederne læne sig ind i det igangværende arbejde med at kortlægge og skabe klarhed omkring, hvordan overholdelse af standarder såsom ISO 27001 og IEC 62443 eller danske rammeværker såsom D-mærket kan bruges til at demonstrere overensstemmelse med krav til styring af cybersikkerhedsrisici. Klarhed omkring, hvilke standarder der er tilstrækkelige, vil give virksomhederne mulighed for at forberede sig på efterlevelse af kravene.

Selvom det vil bliver uddybet yderligere, hvordan man i de enkelte sektorer lever op til kravene om foranstaltninger, vil DI fremhæve et par punkter, hvor vi savner øget klarhed og afgrænsning;

Punkt 1 om politikker for risikoanalyse og informationssystemsikkerhed. Er det Forsvarsministeriets forventning, at virksomhederne skal etablere og opretholde et informationssikkerhedsledelsessystem (ISMS) i henhold til en anerkendt international standard i stil med ISO 27001 eller tilsvarende, herunder eventuelt krav om certificering?

Punkt 4 om forsyningskædesikkerhed og **punkt 1** om risikoanalyse. I hvilket omfang skal virksomheder føre kontrol med sikkerhedsrelaterede aspekter vedrørende forholdene mellem enheden og dens direkte leverandører eller tjenesteudbydere, og hvad er Forsvarsministeriets forventning til, hvor langt ud og ned i forsyningskæderne virksomhederne skal gå i risikoafdækning og risikoanalyse af forsyningskæder, samt myndighedernes forventninger til virksomhedernes mulighed for at føre tilsyn med globalt anerkendte leverandører, fx cloudleverandører?

Punkt 7 om grundlæggende cyberhygiejnepraksisser - hvad indeholder det?

Punkt 8 om politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering. Det vil være omfattende at gør brug af kryptering, nøgler og certifikater i alle typer af systemer og miljøer, som anvendes til virksomhedens tjenester. Prisen for disse ekstra funktionalitetet for nuværende er uforholdsmæssig høj. Virksomhedens tjenester kan opretholdes, og evt. risici vil kunne mitigeres billigere og på anden vis.

§7 Krav til enhedens ledelse

Der er adskillige problemer med udkastets udformning. Udkastet præciserer ikke om ”enhedens ledelsesorgan”/”ledelsesorganet” alene omfatter bestyrelsen eller direktionen, eller begge disse ledelsesorganer. Dette bør præciseres. DI bemærker, at direktivet anvender ”ledelsesorganer” uden at

præcisere det nærmere, og at direktivet derfor formentlig som udgangspunkt omfatter både bestyrelsen og direktionen i danske selskaber. Der er dog forskel på, hvilke opgaver og ansvar en direktion og en bestyrelse har i danske selskaber, jf. selskabsloven. Derfor er der også forskel på, hvad man rettelig kan forlange af medlemmer henholdsvis af en direktion, som har den daglige ledelse, og medlemmer af en bestyrelse, som har den overordnede ledelse.

Det er rimeligt, at både direktionen og bestyrelsen har ansvar for at føre tilsyn med foranstaltningernes gennemførelse, men ansvaret bør være et culpaansvar i overensstemmelse med ledelsesansvarsnormen i gældende dansk selskabsret, jf. selskabslovens § 361. Udkastet forholder sig imidlertid ikke til, om ansvaret er et culpaansvar. Tværtimod kunne formuleringen "[..] *og sikre, at foranstaltningerne har den fornødne effekt*" give anledning til tvivl om, hvorvidt der er tiltænkt et objektivt ansvar for ledelsesmedlemmerne. Et objektivt ansvar ville være meget byrdefuldt for ledelsesmedlemmerne, ville stride imod den gældende ledelsesansvarsnorm og ville derfor kræve meget klar lovhjemmel. Det ville endvidere være en overimplementering og derfor også stride imod tilkendegivelsen på udkastets s. 156 om, at "*Forsvarsministeriet har lagt vægt på, at gennemførelsen af NIS-2 direktivet sket i overensstemmelse med regeringens principper for minimumsregulering af erhvervsrettet EU-regulering*".

DI bemærker, at EU-direktivet ikke indeholder et krav om at ændre den gældende culpanorm for ledelsesansvaret i danske selskaber. Direktivets art. 20, som § 7 implementerer, indeholder ikke formuleringen "*og sikre, at foranstaltningerne har den fornødne effekt*". Derimod kræver art. 20, at vigtige enheders ledelsesorganer "*kan gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i [artikel 21]*", dvs. at ledelsen kan gøres ansvarlig for overtrædelser af forpligtelserne i udkastets § 6. EU-direktivet siger ikke noget om hvilken ansvarsnorm, der skal anlægges – og direktivet sætter heller ikke lighedstegn mellem effekt og ansvar.

Ledelsesansvarsgrundlaget i dansk selskabsret er individuelt og konkret, og forudsætter bl.a. et brud på den uagtsomhedsnorm som må forventes af ledelsesmedlemmer som befandt sig i den pågældendes sted under de pågældende omstændigheder (culpaansvaret). Dette er selvsagt ikke et objektivt ansvar. Et *selskabs* brud på en lovforpligtelse er derfor ikke nødvendigvis det samme som, at *ledelsen* ifalder et *personligt ansvar* for overtrædelsen. Sanktioner for selskabet (f.eks. bødestraf), omdømmerisiko og den gældende culpanorm for personligt ansvar vurderes således generelt fuldt ud tilstrækkeligt til at sikre, at ledelsen har fuld fokus på de pligter, som selskabet er underlagt.

I de sager, hvor danske domstole har idømt ledelsesmedlemmer et personligt ansvar, er der blevet taget stilling til hvert enkelt ledelsesmedlems individuelle ansvar. Personligt ansvar for det ene ledelsesmedlem betyder derfor ikke nødvendigvis, at det samme gælder et andet ledelsesmedlem. DI opfordrer derfor kraftigt til, at lovteksten tilpasses direktivteksten, og at det præciseres, at ledelsesansvarsnormen efter loven er den gældende culpanorm i selskabsloven både for direktions- og bestyrelsesmedlemmer.

DI finder det uklart, om krav om deltagelse i relevante kurser gælder samtlige medlemmer af både bestyrelsen og direktionen, eller kun nogle af medlemmerne, således at kursuskompetencerne er repræsenteret i det pågældende ledelsesorgan. Normalt har man ikke har lovkrav om specifik viden inden for et bestemt fagområde hos ledelsesmedlemmer i selskaber, da det er svært at sætte ledelsesegnethed på formel, og da hvert selskabs behov og organisation kan være forskelligt. For eksempel vil nogle selskaber prioritere at have visse kompetencer repræsenteret direkte i bestyrelsen og sikre den nødvendige viden på andre områder via viden fra andre dele af selskabets organisation eller fra eksterne rådgivere, mens andre selskaber vil prioritere anderledes. Da både bestyrelsen og direktionen er kollektive organer, vil man sædvanligvis også prioritere, at ledelsesmedlemmernes kompetencer supplerer hinanden. Såfremt kravet om kurser gælder alle ledelsesmedlemmer, bør dette derfor præciseres. DI finder det også uklart, hvor omfattende kravet er. Er der fx krav om løbende kursusdeltagelse, og hvilket niveau af (teknisk) viden inden for styring af risici, der relaterer sig til cybersikkerhed, krisestyring og sikkerhedskultur, skal kurserne svare til? Er der forskel på de kurser henholdsvis et direktionsmedlem og et bestyrelsesmedlem skal have? Efter DI's opfattelse, bør kravene afspejle, at direktionen varetager selskabets daglige ledelse, mens bestyrelsen varetager selskabets overordnede ledelse og føre tilsyn med direktionen.

Efter DI's opfattelse kan man ikke forvente, at bestyrelsesmedlemmer bliver eksperter i cybersecurity alene ved at tage nogle kurser – og bestyrelsen bør heller ikke nødvendigvis være eksperter cybersecurity. Der bør ligesom i dag være mulighed for inddrage egne, fagspecifikke medarbejdere, eksterne konsulenter mv., for at kunne foretage en ledelsesvurdering af, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der er egnede til styring af cybersikkerhedsrisici. Selvom man kan forvente mere af direktionen, bør der tilsvarende være grænser for, hvilke ekspertkrav man kan stille til direktionsmedlemmer, ellers vil ledelsesmedlemmers kompetencer blive uhensigtsmæssigt tiltet imod en enkelt kvalifikation – og fordelene ved at specialisering hos ansatte og eksterne konsulenter går tabt, hvis specialistviden også påkræves i direktionen

Kapitel 3 Registrerings- og underretningspligter

§ 9 Registreringsforpligtigelser for visse typer af digitale tjenester
Der vil være risiko for, at virksomheder registrerer sig uden at være omfattet af loven, da lovens anvendelsesområde er præget af en vis usikkerhed. Derfor er det vigtigt med hjælp til virksomhederne, så de kan vurdere, om de er omfattet og derfor bør registrere sig. Som nævnt indledningsvist skal der 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.

§ 10 Registreringsforpligtigelser for enheder, der levere domæneregistreringstjenester.
DI foreslår, at tidsrammen for ajourføring af disse oplysninger om enheder, der leverer domæneregistreringstjenester, gøres mere fleksibel, da to uger ikke er lang tid. Fristen kan med fordel være tre måneder, hvilket er tilfældet i § 9.

§ 12 Underretningspligter for væsentlig og vigtige enheder om væsentlige hændelser

Underretning via en fælles digital indgang

Det foreslås i §12, stk. 1, at væsentlige og vigtige enheder uden unødigt ophold skal underrette den relevante kompetente myndighed og CSIRT'en om enhver væsentlig hændelse. Såfremt enheden leverer tjenester i flere sektorer, som påvirkes af hændelsen, skal enheden underrette de kompetente myndigheder i de pågældende sektorer. I en potentiel krisesituation efter en hændelse, hvor hvert sekund tæller og opgaven med at håndtere hændelsen prioriteres højt, er det ikke hensigtsmæssigt, at virksomheden skal bruge ressourcer på at underrette op til flere myndigheder. Derfor understreger DI vigtigheden af, at underretningerne til myndighederne og CSIRT'en skal ske via én fælles digital indgang, da dette vil sikre, at den ramte virksomhed kun skal foretage én samlet underretning, som derefter fordeles til relevante myndigheder. DI noterer sig, at dette er Forsvarsministeriets hensigt. Da der kan være tale om forretningsmæssigt følsomme data, oplysninger om fremgangsmåder, driftsforhold og tekniske indretninger m.v., er det afgørende, at myndighederne kan garantere, at data og information beskyttes tilstrækkeligt og behandles fortroligt. Dertil opfordrer DI til, at sikkerhedsmyndighederne, fx PET og FE, inddrages i en risikovurdering af, hvilke data og informationer der skal behandles som fortrolige. Se bemærkninger til kapitel 8.

Tærsklen for, hvornår en hændelse anses for at være væsentlig

Vedkommende minister kan jf. stk. 3, efter forhandling med forsvarsministeren, fastsætte nærmere regler om, hvornår en hændelse anses for at være væsentlig. De sektoransvarlige myndigheder bør inddrage virksomhederne i arbejdet med at fastsætte nærmere sektorvise regler, der præciserer, hvornår en hændelse er væsentlig. Det skal sikre, at underretningerne bliver værdiskabende fremfor potentielt at blive en tung, administrativ byrde, der reelt ikke bidrager til at skabe højere sikkerhed. Derfor bør en hændelse kun betragtes som væsentlig, hvis to eller flere kriterier, der skal defineres nærmere efter stk. 2, er opfyldt, med særlig fokus på, om hændelsen påvirker den relevante enheds evne til at levere kritiske tjenester til sine direkte kunder, hvilket påvirker kundens forretningskritiske funktioner.

For mange virksomheder vil det på grund af den type tjeneste, de leverer (fx cloud-tjenester eller en fødevareprodukter, hvor brugere ofte kan substituere), ikke altid være muligt at beregne det præcise antal berørte brugere eller individer, der er påvirket af hændelsen, med det formål at vurdere, om hændelsen er væsentlig. Tjenesteudbyderen har ikke nødvendigvis en direkte relation til slutbrugeren og kan ikke altid fastslå det præcise antal brugere, der tilgår tjenesten på et givent tidspunkt. I stedet for at overvåge individuelle brugere kan det være mere hensigtsmæssigt fx at spore fejlprocenter og fastsætte tærsklen ved API-endpoints, når der er tale om en cloud-tjeneste.

Tærsklen for, hvornår en hændelse er væsentlig, bør altså tage højde for, at det for mange virksomheder vil være uhensigtsmæssigt at skulle beregne antallet af slutbrugere. Dertil er tidsperspektivet også relevant. Hvor lang tid en tjeneste er utilgængelig, inden det har betydelige samfundsmæssige konsekvenser, vil variere på tværs af sektorer og virksomheder. Lovudkastet skelner derudover ikke mellem

hændelsestyper (tilgængelighed vs. integritet/kompromittering). Der bør tages højde for, at mange tjenester kan være utilgængelige af årsager, der ikke er relateret til cybersikkerhed, såsom vedligeholdelse eller opdateringer. Dette kan føre til overrapportering om hændelser, der ikke har noget med cybertrusler at gøre.

Grundlæggende skal tærsklen være meningsfuld og målbar og ikke for bred med meget skønsprægede og kvalitative kriterier. Tærsklen for væsentlige hændelser bør fokusere på den faktiske påvirkning, som direkte følger af en specifik hændelse, og ikke de hypotetiske konsekvenser. Det er fx tæt på umuligt for et Incident Response Team inden for de første 24 timer efter et angreb at vurdere, om hændelsen "*er i stand til at forårsage alvorlige økonomiske tab for den berørte enhed*." Et sådant krav vil desuden aflede ressourcer fra at håndtere reelle trusler og større hændelser for både berørte enheder og myndighederne. Kriterier, der relaterer sig til økonomisk tab og immaterielle skader, såsom omdømme, bør betragtes som et lavt prioriteret kriterium eller helt undlades.

§13 Om proces og detaljer for underretningspligter om væsentlige hændelser
Lovudkastet pålægger, at en enhed skal indsende en tidlig advarsel senest 24 timer efter, at enheden "har fået kendskab" til en væsentlig hændelse, men det defineres ikke, hvad "fået kendskab" betyder. Når virksomheden har opdaget en hændelse, vil den igangsætte en undersøgelse for at bekræfte hændelsens validitet. Først derefter kan hændelsen analyseres yderligere for at afgøre, om den opfylder kriterierne for en væsentlig hændelse, hvilket udløser flertrinstilgangen til underretninger. 24-timersreglen bør præciseres, så uret først starter, når virksomheden med en rimelig grad af sikkerhed ved, at tærsklen for en væsentlig hændelse er mødt. Underretningspligten bør altså først blive aktiveret, når der er tilstrækkelige beviser, der indikerer, at en væsentlig hændelse har fundet sted. Rapportering på et spekulativt niveau er hverken operationelt eller gavnligt for CSIRT'en eller kunder. Trin-for-trin vejledning vil gøre det nemmere for virksomheder at underrette myndighederne med den rette informationer efter en væsentlig hændelse.

§14 Frivillige underretninger om hændelser, nærvedshændelser og cybertrusler
Det er en forudsætning, at virksomheder, der vælger frivilligt at dele oplysninger om et angreb, kan gøre det uden risiko for, at omverdenen via aktindsigt får adgang til følsomme og forretningskritiske oplysninger, der kan skade virksomhedens omdømme. Det følger af § 14, stk. 3, at underretninger efter stk.1 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven. Når en virksomhed bliver hacket, vil der dog ofte også være sket et brud på persondatasikkerheden, og muligheden for at søge aktindsigt hos Datatilsynet kan derfor foregå sideløbende. Det er uklart for DI, hvordan denne situation vil blive håndteret fremadrettet.

Kapitel 4 Underretning og oplysning om væsentlige hændelser

§ 15 Underretning til modtagere om væsentlige hændelser og væsentlige cybertrussler

DI anerkender vigtigheden af kommunikation om væsentlige hændelser for at sikre, at berørte modtagere af tjenester har mulighed for at træffe eventuelle nødvendige foranstaltninger. Det er uklart, om "modtagerne" henviser til slutkunderne, business-to-business-relationer, individuelle maskiner, faciliteter, mv. Denne uklarhed komplicerer overholdelsen, da enheder vil have svært ved at afgøre, hvem de skal underrette om en hændelse, hvilket potentielt kan føre til over- eller underkommunikation. Bemærkningerne definerer ikke "modtagere" yderligere, men skriver, at underretning af modtagere "*alene skulle ske i relevant omfang"*, hvilket indebærer, *"at enhederne vil kunne undlade at foretage underretning af modtagerne ud fra en konkret vurdering af, at underretningen ikke vil være i modtagernes interesse*." DI opfordrer til en risikobaseret tilgang til at informere offentligheden om den væsentlige hændelse, der lægger vægt på at balancere den faktiske risiko/nødvendigheden af, at offentligheden bliver informeret og den potentielle indvirkning på den berørte virksomheds drift. Virksomhederne bør inddrages i en dialogen om en præcisering af "modtager", da det er vigtigt med klare retningslinjer og vejledning omkring, hvordan "modtager" og "i relevant omfang" skal forstås.

De sektorvise bekendtgørelser bør indeholde en uddybning af "*påvirke leveringen af deres tjenester negativt*" da det er uklart og kan fortolkes bredt – fx hvis en cloud-tjeneste er utilgængelig i 5 minutter, skal dette så underrettes til relevante modtagere? Desuden tager udkastet ikke højde for, at mange tjenester kan være utilgængelige af årsager, der ikke relaterer sig til cybersikkerhedshændelser. Til sidst er det uklart, om meddelelsen offentliggøres på et offentligt tilgængeligt websted (uden krav om konto eller login), eller skal den være tilgængelig direkte i platform for berørte brugere (med krævet konto eller login). Vi opfordrer myndighederne til at udvikle disse overvejelser i overensstemmelse med andre relevante lovgivningsmæssige rammer og ENISA relaterede standarder og retningslinjer.

§ 16 Orientering af offentligheden om den væsentlige hændelse
Af stk.1 fremgår det, at det vil være den sektoransvarlige myndighed, der efter høring af virksomheden kan informere offentligheden, mens der i stk. 2 står, at det kan kræves, at virksomheden informerer offentligheden. Det er uklart, om der i situationer, hvor offentligheden bør informeres, er et delt ansvar mellem myndighed og virksomhed i forhold til at informere offentligheden. Som udgangspunkt bør være virksomheden, der efter påbud informerer offentligheden om en væsentlig hændelse, hvis det ud fra en risikobaseret tilgang vurderes nødvendigt på grund af hændelsens karakter. Det bør være en forudsætning, at orientering af offentligheden er nødvendigt for at forebygge en væsentlig hændelse eller for at håndtere en igangværende hændelse. Kravene og ansvaret for offentlig orientering bør tydeliggøres og ensartes på tværs af relevant lovgivning.

Kapitel 5 CSIRT'ens opgaver

I §17 beskrives CSIRT'en opgaver, heriblandt bistand i forbindelse med hændelseshåndtering og med proaktive sårbarhedsscanninger af enhedens informationssystemer. DI opfordre til at kravene, der danner rammerne for CSIRT'ens virke udspecificeres yderligere og på samme niveau som er tilfældet i direktivet. Der er behov for videndeling, vejledning samt hurtigere afklassificering af data fra

CFCS/CSIRT'en, hvilket kan understøtte civile virksomheders evne til at håndtere hændelser og sårbarheder. Der mangler ligeledes en definition af CSIRT i §3 i den danske lovtekst.

I bemærkningerne står, at bistand skal forstås bredt og vil omfatte "*rådgivning om afhjælpende foranstaltninger, herunder eventuelt råd og vejledning i forhold til specifikation af ydelser eller produkter, som enheden kan købe hos private leverandører, samt efter omstændighederne mere konkret teknisk bistand.*" DI opfordre til dialog omkring det nærmere indhold af bistanden, så vi sikrer styrket kommunikation og forventningsafstemning mellem CFCS og virksomhederne. Vi tilskynder at CFCS stiller sin viden og kompetence til rådighed til gavn for civile virksomheder og infrastruktur, og at der skabes en mere åben kultur for den del af CFCS, der arbejder med de virksomhedsrettede opgaver. Derfor finder DI det positivt er der med §19 lægges op til, at CSIRT'en faciliterer en frivillig udveksling af oplysninger mellem enheder i såkaldte cybersikkerhedsfællesskaber. Dette bør ske i tæt samarbejde med erhvervs- og brancheorganisationerne, der allerede i dag driver netværk.

Af §18 fremgår det, at CSIRT'en sikrer, at fysiske og juridiske personer i anonymiseret form kan rapportere om sårbarheder. Denne mulighed for underretning kan misbruges og i værste fald blive anvendt som chikane, hvilket kan trække sikkerhedsmæssige ressourcer væk fra det arbejde og de opgaver, som virksomhederne reelt burde have fokus på.

Kapitel 6 Tilsyn og håndhævelse

Indledningsvis vil DI betone værdien af et dialogbaseret tilsyn, hvor virksomhederne og tilsynsmyndigheden i fælles dialog sikrer et højt cybersikkerhedsniveau.

§20 Kompetente myndigheder
Lovudkastet lægger vægt på, 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. Dette er særligt relevant for tilsyn med virksomheder, der indgår i flere omfattede sektorer, og hvor der derved kan være flere myndigheder, der skal føre tilsyn med de samme virksomheder. Det er vigtigt, at vi undgår en situation, hvor virksomheder, der er omfattet af flere sektorer, skal efterleve vidt forskellige krav, hvis tilsynsregimerne håndhæves forskelligt, hvilket vil aflede tid og ressourcer i virksomhederne fra arbejdet med at styrke cybersikkerheden. Det er derfor positivt at der i lovudkastet lægges op til, at der kan gennemføres fælles tilsynsbesøg og samarbejde om tilsynsressourcer, eksempelvis i form af et fælles sekretariat. DI opfordrer til, at man i stor udstrækning forfølger denne tankegang, og at de kompetente myndigheder forpligter sig til at koordinere tilsynsopgaven – både det løbende, proaktive tilsyn og det reaktive tilsyn. Dertil er det også vigtigt, at myndighederne læner sig ind i arbejdet i EU-Kommissionens Samarbejdsgruppe med henblik på at sikre at tilsynsregimerne ensartes på tværs af EU.

§ 21 stk. 1, punkt 4, om tilsynsforanstaltninger for væsentlige enheder

DI tager afstand fra forslaget om, at tilsynsmyndigheden skal kunne foretage sikkerhedsscanninger og penetrationstest af virksomhedens net- og informationssystemer. Dette er en meget vidtgående kontrolforanstaltning, der ikke ses at være i overensstemmelse med ordlyden i NIS2-direktivet, art. 32, stk. 2, litra d, der alene omtaler tilsynsmyndigheden beføjelse "*beføjelse til at pålægge disse enheder: (..) d) sikkerhedsscanninger baseret på objektive, ikkediskriminerende, fair og gennemsigtige risikovurderingskriterier, hvor det er nødvendigt i samarbejde med den berørte enhed*." Vurderingen af, hvorvidt sikkerhedsscanninger er en nødvendig del af den pågældendes sikkerhedsforanstaltninger må bero på virksomhedens egen risiko- og sårbarhedsvurdering. Hvis virksomheden selv foretager sikkerhedsscanninger, vil det fx kunne foreslås, at resultatet af testen kan præsenteres for tilsynsmyndigheden i forbindelse med et aktuelt tilsyn. Resultater og konklusioner af sikkerhedsscanninger bør være undtaget muligheden for aktindsigt.

§ 22. Direktivets art. 32, stk. 6, 1. pkt. er uhensigtsmæssigt formuleret som om retten til at repræsentere en virksomhed eksternt (det kunne i praksis være fx iht. tegningsregel eller prokura) nødvendigvis betyder, at de samme personer kan bestemme alle virksomhedens interne beslutninger (fx ift. cybersecurity tiltag). Implementeringen af art. 32 – ligesom med art. 20 – bør ikke ændre på gældende culpanorm for ledelsesansvaret i danske selskaber**.** Se bemærkningerne til §7.

Afgrænsning af § 22, punkt 6

Punkt 6 giver tilsynsmyndigheden muligheden for at "*påbyde enheden i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-5 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde*". Denne bestemmelse fremstår meget bred, og bør afgrænses, så den stemmer bedre overens med tilsvarende bestemmelse i NIS2-direktivet, art. 32, stk. 4, litra h, hvor udtrykket "*aspekter af overtrædelsen af dette direktiv*" anvendes, hvilket antyder en forholdsvis afgrænset oplysningspligt og/eller offentliggørelse.

§ 23. I forslaget er der både beføjelsen til midlertidig suspension af certificeringer eller godkendelse, og beføjelsen til midlertidig frakendelse af ledelsesretten, tillagt den kompetente myndighed i første instans. Der er tale om alvorlige og vidtrækkende indgreb i virksomhedens drift og ledelse– og i sidste ende brugernes drift. DI er derfor enig i bemærkningerne til bestemmelsen, hvor det fremgår at bestemmelsen *kun* bør anvendes som en sidste udvej, dvs. først efter at de øvrige, relevante håndhævelsesbestemmelser er udtømt, og at anvendelsen af bestemmelsen desuden skal være proportional med overtrædelsens alvor og under hensyntagen til omstændighederne i det enkelte tilfælde, herunder i lyset af om overtrædelsen var forsætlig eller uagtsom, og ethvert tiltag der er iværksat for at forebygge eller afbøde skaden. DI lægger endvidere vægt på, at virksomhederne har rimelige muligheder for at rette op og undgå indgreb.

DI har dog flere indvendinger imod det foreslåede udkast og gør opmærksom på, at udkastet på flere punkter ikke udgør en direktivnær minimumsimplementering, som det ellers er oplyst, skulle være intentionen. I direktivet har medlemslandene mulighed for at give den kompetente myndighed denne

beføjelse for så vidt angår suspension af virksomhedens certificeringer eller godkendelse, men medlemslandene kan også vælge at give denne beføjelse til domstolene "*i overensstemmelse med national ret*".

Direktivet indeholder derimod ikke samme beføjelse for den kompetente myndighed til midlertidigt at suspendere ledelsesretten for ovennævnte personkreds som første instans. Direktivet bestemmer i stedet, at den kompetente myndighed alene skal have beføjelse til "*at anmode de relevante organer eller domstole om i overensstemmelse med national ret midlertidigt at forbyde enhver fysisk person [..]*"

DI er derfor uforstående over for, at det i lovbemærkningerne konkluderes, at de eksisterende muligheder for rettighedsfrakendelse i straffeloven, som forudsætter en dom, ikke er tilstrækkelige til at sikre korrekt og tilstrækkelig gennemførelse af den relevante direktivbestemmelse. DI finder det retssikkerhedsmæssigt bekymrende, at udgangspunktet vendes om, således at det er virksomheden/ledelsesmedlemmet, der skal anlægge en retssag, og finder i øvrigt denne ret til sagsanlæg illusorisk, da skaden så allerede er sket. DI bemærker supplerende, at overtrædelse af § 22 allerede er bødebelagt.

DI noterer sig udkastets bemærkninger om, at begrebet "virkningsløse" er foreslået erstattet af "utilstrækkelige", fordi en anvendelse af den danske direktivversions begreb "virkningsløse" ville føre til et snævrere anvendelsesområde, end hvad der må formodes at være tiltænkt, når man sammenligner med f.eks. den engelske direktivversion, der anvender begrebet "ineffective". DI mener, at anvendelse af begrebet "utilstrækkelige" kan føre til, at anvendelsesområdet i stedet udvides.

DI bemærker, at begrebet "den juridiske repræsentant hos virksomheden" er et ukendt begreb i dansk selskabsret. Udkastets bemærkninger kunne indikere, at der med dette begreb menes:

"*I det omfang en virksomhed eller organisation ikke har en administrerende direktør, vil bestemmelsen omfatte den øverste leder af den pågældende væsentlige enhed, f.eks. en generalsekretær, direktør, koncernchef eller managing partner*."

Det bør dog præciseres, om lovbemærkningerne på dette punkt referer til lovtekstens "*den juridiske repræsentant hos virksomheden*".

§ 24 om tilsynsforanstaltninger for vigtige enheder

Jf. § 24 forventes myndighederne at have en reaktiv tilgang til tilsyn over for vigtige enheder. Kriterierne for, hvornår dette tilsyn aktiveres, bør defineres tydeligere. Myndighederne kan kræve at få udleveret oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført samt dokumentation for gennemførelsen af cybersikkerhedspolitikker. I den forbindelse bemærker DI, at flere medlemslande tillader, at overensstemmelse med NIS1-cybersikkerhedskravene kan baseres på ISO/IEC 27001-certificering eller brugen af nationale informationssikkerhedsstandarder, der er kompatible med ISO/IEC 27001, fx BSI IT-Grundschutz i Tyskland, E-ITS i Estland og CyberFundamentals Framework i Belgien. I Danmark kan

myndighederne ligeledes henvise til danske rammeværker som D-mærket som en måde, hvorpå vigtige enheder kan dokumentere overholdelse af direktivets krav.

Danske virksomheder har brug for en let tilgængelig og konkret måde at arbejde med kravene i NIS 2-direktivet på og samtidigt tydeligt vise, at de lever op til disse krav. Derfor opfordrer DI myndighederne til at vurdere D-mærket og andre lignende rammeværk som mulige værktøjer til efterlevelse og dokumentation af NIS 2-kravene, hvilket kan reducere virksomhedernes implementeringsomkostninger og sikre effektiv efterlevelse af NIS 2-direktivet for direkte omfattede virksomheder og deres underleverandører. D-mærket er en mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse, som Dansk Industri, Dansk Erhverv, Forbrugerrådet Tænk, SMVdanmark og Industriens Fond står bag. D-mærkets krav og kriterier er udformet efter NIS2-direktivets minimumskrav og baseret på internationale standarder. DI henviser derudover til D-mærkets høringssvar.

§25 Håndhævelsesforanstaltninger for vigtige enheder. Det er afgørende, at håndhævelsesforanstaltningerne for vigtige enheder er proportionale i forhold til overtrædelsens grovhed og omfang. Se bemærkningerne til §21, § 22 og § 23.

Kapitel 7 Gensidig bistand

DI finder det vigtigt, at det i forbindelse med gensidig bistand ikke kan kræves, at danske virksomheder udleverer fortrolig information om virksomhedens it-sikkerhedsforanstaltninger til en anden medlemsstats tilsynsmyndighed. En indsigt i virksomhedens foranstaltninger og eventuelle konklusioner fra tilsyns- og håndhævelsesforanstaltninger bør således alene kunne opnås ved samtidig medvirken af den danske tilsynsmyndighed og efter aftale med denne, mod fremvisning af behørig legitimation og dokumentation for gyldig sikkerhedsgodkendelse samt efter høring af den pågældende virksomhed. Når virksomheder deler sensitive oplysninger med de kompetente myndigheder, er det afgørende, at disse oplysninger behandles med højeste grad af fortrolighed og sikkerhed.

Kapitel 8 Videregivelse af oplysninger, digital kommunikation, gennemførelsesakter og operativ uafhængighed

§ 28 om videregivelse af oplysninger til andre medlemsstaters myndigheder og institutioner
Der er behov for at indføre særskilt hjemmel til at kunne videregive oplysninger af fortrolig karakter til andre medlemsstaters myndigheder og institutioner i EU. Udvekslingen af oplysninger skal bevare de pågældende oplysningers fortrolighed og beskytte de berørte enheders sikkerhed og kommercielle interesser. Det anbefales;

- at vedkommende myndighed, informerer den danske virksomheder, forud for at informationen videregives, hvis der er tale om oplysninger, som kan henføres direkte til en eller flere virksomheder.

- at vedkommende myndighed og den berørte virksomheder i fællesskab, eller efter høring af den berørte virksomhed, foretager en risikovurdering af kritikaliteten og fortroligheden af de informationer, som påtænkes videregivet mhp. at træffe nødvendige foranstaltninger forud for at informationen videregives.

DI opfordre til at Forsvarsministeriet tager stilling til hvordan begrebet "fortrolig" skal tolkes og holdningen hertil bør fremgå tydeligt af loven og bemærkningerne.

Det fremgår i bemærkningerne til § 31, at den pågældende minister kan fastsætte regler om at anvende løsninger såsom Virk.dk til at foretage underretninger om hændelser, og krav om at information og henvendelser "*ikke anses for behørigt modtaget af myndighederne, hvis de indsendes på anden vis end den foreskrevne digitale måde"* (s. 314). Det bør sikres, at der til enhver tid er alternative kommunikationsveje, så hverken myndigheder eller virksomheder er afhængige af kun én digital løsning. Det bør desuden til enhver tid være muligt at kunne opnå personlig kontakt med myndigheden via telefon. Igen finder DI det nødvendigt at nævne, at der er behov for, at bekendtgørelserne sendes i høring med en rimelig høringsfrist, så virksomhederne har mulighed for at give bemærkninger til eventuelle sikkerhedsmæssige forhold og hensyn, der måtte være i forbindelse med en konkretisering af § 30 og § 31.

Kapitel 9 Straf

Udstedelse af bøder samt udmåling af beløbsstørrelse skal som hovedregel altid foregå i det almindelige straffeprocessuelle system, hvor der er de fornødne retsikkerhedsgarantier for de sigtede juridiske og fysiske personer. Bødeniveauet for overtrædelser af NIS2 er højt, og det rejser en bekymring for, at bødesanktionerne ikke kommer til at stå mål med de pågældende overtrædelser. Vi opfordrer derfor til, at det i lovbemærkningerne tages højde for, at der skal være det nødvendige råderum for domstolene til at udmåle bødestraffen på grundlag af den enkelte sags konkrete omstændigheder, og derved ikke "fastlåses" til at gøre brug af forudsatte beløbsgrænser.

Kapitel 10 Ikrafttrædelse

§ 33 Ikrafttrædelse

Henset til, at en nærmere kategorisering og konkretisering af kravene samt vejledning i forhold til hvilke virksomheder, der er omfattet, udestår, står det klart, at lovens ikrafttrædelsesdato den 1. marts for mange virksomheder vil være udfordrende. Med et så omfattende lovforslag, der stiller en lang række organisatoriske og tekniske krav, samt håndhævelsesforanstaltningerne taget i betragtning, bør der være en rimelig implementeringsperiode efter ikrafttrædelsestidspunktet, så virksomhederne får mulighed for at implementere de nye omfattende krav, inden tilsynet begynder. Der henvises til de indledende bemærkninger, hvor DI påpeger, at virksomhederne skal have 12 måneder eller som minimum seks måneder til at efterleve kravene. Ikrafttrædelsesdatoen bør vel at mærke først ligge minimum seks 6-12 måneder efter, at indholdet i de sektorvise bekendtgørelser er kendt og vedtaget.

Der vil være stor forskel på virksomheders evne og mulighed for at efterleve kravene, hvor særligt de mindre virksomheder samt virksomheder, der ikke tidligere har været omfattet af NIS1, kan være særligt udfordrede. En lang række virksomheder vil være nødt til at trække på eksterne fagspecifikke konsulenter for at komme i mål, og dette fordrer, at der er den nødvendige fagbistand til rådighed, inden reglerne træder i kraft.

DI vil desuden understrege, at bekendtgørelserne bør træde i kraft på samme tidspunkt for ikke at skabe unødig forvirring, bureaukrati og en skævvridning af cybersikkerhedsniveauet på tværs af sektorerne. Der bør ligeledes tages højde for en rimelig indfasningsperiode efter ikrafttrædelsestidspunktet, hvor tilsynet i høj grad er rådgivende og ikke sanktionerende. En overgangsperiode vil give de relevante enheder bedre tid til at forstå kravene, udvikle implementeringsstrategier og sikre overholdelse uden risiko for sanktioner. Til sammenligning har myndighederne haft ca. 22 måneder fra offentliggørelsen af NIS2 i The Official Journal of the European Union den 27. december 2022 til fristen for at vedtage bestemmelserne den 17. oktober 2024.

Økonomiske konsekvenser for erhvervslivet

Forsvarsministeriet forventer, at de erhvervsøkonomiske konsekvenser vil være cirka 2,6-3 mia. kr. Det er svært at sige noget kvalificeret om de økonomiske konsekvenser, da vi ikke kender de konkrete krav, og da der er store forskelle i modenheden på tværs af sektorer og virksomheder. Dertil er der også mange virksomheder, der vil blive indirekte ramt af kravene jf. lovudkastets krav til leverandørkædesikkerhed, hvilket vil medføre yderligere store økonomiske konsekvenser, der er svære at overskue. Implementeringsopgaven er omfattende, og der er behov for åbenhed og vejledning i implementeringsfasen. DI deltager gerne i denne proces og opfordrer til, at CFCS og andre myndigheder parallelt med Folketingets beslutningsproces inviterer til dialog med centrale aktører på feltet.

Forholdet til Databeskyttelsesloven

Ad spørgsmålet om hjemmel til behandling, herunder videregivelse af personoplysninger
DI er glade for, at lovforarbejderne tager stilling til spørgsmålet om hjemmel til videregivelse i de nævnte situationer. Denne stillingtagen er vigtig for at skabe klarhed og hjælpe virksomhederne med at opfylde deres forpligtelser efter databeskyttelseslovgivningen. Lovforarbejderne er tydelige i deres vurdering af, hvilken hjemmel virksomhederne skal bruge ved videregivelse af personoplysninger til CSIRT'en og det centrale kontaktpunkt efter § 17.

Omvendt er det ikke klart for DI hvilken hjemmel virksomhederne skal benytte ved behandling af personoplysninger med henblik på at overholde lovens §§ 9, 10, 11, 12, 13, 21-23, 24 og 25. Lovforarbejderne nævner på s. 186 både databeskyttelsesforordningens artikel 6, stk. 1, litra c, e og f som behandlingshjemmel, men er ikke specifik om, hvilken hjemmel der knytter sig til hver behandling. DI opfordrer til at det præciseres i hvilke sammenhænge de forskellige behandlingshjemler er aktuelle, blandt andet fordi hjemmelsgrundlaget har betydning for, hvordan virksomhederne skal overholde

kravet om fortegnelse i databeskyttelsesforordningens artikel 30 og de registreredes rettigheder i databeskyttelsesforordningens kapitel III.

Ad spørgsmålet om overholdelse af de registreredes rettigheder
Nærværende høringssvar er afgrænset til visse af de registreredes rettigheder som DI i praksis har oplevet de fleste spørgsmål i relation til. Skulle Forsvarsministeriet i deres videre arbejde identificere andre relevante problemstillinger i relation til de nævnte artikler eller andre af de registreredes rettigheder, håber DI at ministeriet også vil medtage disse i forarbejderne.

Oplysningspligten
Modsat spørgsmålet om hjemmel til videregivelse, tager lovforarbejderne ikke stilling til spørgsmålet om virksomhedernes overholdelse af de registreredes rettigheder. Det gælder særligt oplysningsforpligtelsen efter databeskyttelsesforordningens artikel 13 og 14, indsigtsretten, jf. artikel 15 og retten til sletning, jf. artikel 17. For at sikre den bedste klarhed for virksomhederne, vil DI opfordre til at lovforarbejderne indeholder en vurdering af, om virksomhederne forventes at skulle opfylde deres oplysningspligt efter artikel 13 eller 14. Eksempler på spørgsmål relateret til oplysningspligten kunne være;
Med vedtagelse af loven og løbende ved opfyldelse af virksomhedernes forskellige forpligtelser, blive *viderebehandlet* personoplysninger til *andre formål* end personoplysningerne blev indsamlet til. Dermed opstår spørgsmålet om virksomhederne skal oplyse om dette nye formål og *hvornår* oplysningsforpligtelsen i så fald indtræder, eller om oplysningspligten i visse tilfælde bør undtages efter databeskyttelseslovens § 22.

I det omfang lovgivningen pålægger dataansvarlige virksomheder at videregive oplysninger, der er indsamlet fra tredjepart, ville det hjælpe virksomhederne at man i lovforarbejderne vurderer om – og eventuelt i hvilket omfang – de berørte virksomheder kan undtage oplysningspligten med henvisning til databeskyttelsesforordningens artikel 14, stk. 5, litra c og – hvis relevant – litra d.

Indsigtsretten
Forarbejderne kan ligeledes tage stilling til, om indsigtsretten skal efterleves ved underretninger, eller om indsigtsretten kan undtages, enten fordi underretninger ikke er omfattet af indsigtsretten i databeskyttelsesforordningens artikel 15, eller fordi indsigtsretten er undtaget efter databeskyttelseslovens § 22. Det ville eksempelvis være relevant at vurdere, om der er indsigt i underretninger efter lovforslagets § 14, stk. 1, da sådanne underretninger er undtaget aktindsigt og partsaktindsigt, jf. § 14, stk. 3. Efter databeskyttelseslovens § 22, stk. 3 kan indsigt i dag allerede undtages i en række situationer, hvor retten til aktindsigt ikke gælder, jf. §§ 19-29 og 35 i lov om offentlighed i forvaltningen. DI forstår umiddelbart reglerne sådan, at undtagelsesbestemmelsen i databeskyttelseslovens § 22, stk. 3 ikke kan benyttes i sådanne tilfælde, men det vil være fordelagtigt at det blev præciseret. Det vil ligeledes være relevant at vurdere, om der er forskel på undtagelserne fra retten til indsigt afhængig af om den underrettende part er offentlig myndighed eller privat enhed.

Retten til at blive glemt

Som nævnt i ovenstående afsnit om *'hjemmel til behandling, herunder videregivelse af personoplysninger*' har behandlingsgrundlaget i databeskyttelsesforordningens artikel 6 betydning for, I hvilke tilfælde en dataansvarlig virksomhed skal efterleve de registreredes rettigheder. De indholdsmæssige krav til behandling af persondata for så vidt angår lovens § 9-11 er så præcise, at hjemmel til behandling bør være art. 6, stk. 1, litra c (retlig forpligtelse). Derfor bør retten til sletning kunne undtages i mange tilfælde, jf. art. 17, stk. 3, litra b. De tilfælde, hvor der er ret til sletning bør dermed omfatte situationer, hvor oplysningerne iht. egne politikker og procedurer ikke er ajourførte eller nøjagtige.

Sammenspillet med øvrig EU-lovgivning

Klima-, Energi- og Forsyningsministeriet varetager implementeringen af NIS2 i energisektoren, Erhvervsministeriet i finanssektoren og Forsvarsministeriet i telesektoren. Dette vil forventeligt ske ved fremsættelse af særskilte lovforslag på disse områder. Som det ser ud nu, vil NIS2 træde i kraft for energisektoren den 1. januar 2025, mens Forsvarsministeriet lægger op til ikrafttrædelse den 1. marts 2025. Hvad angår teleområdet, er det uklart, om NIS2-kravene vil blive integreret i gældende love om cybersikkerhed, eller om der fremsættes en separat hovedlov. DI opfordrer til, at lovforslag, der implementerer NIS2, behandles samtidig i Folketinget, hvilket vil understøtte muligheden for at skabe koordination og ensartethed på tværs af sektorer. Der er behov for, at der etableres en god sammenhæng mellem Forsvarsministeriets og Klima-, Energi- og Forsyningsministeriets fremsatte lovforslag samt forpligtelserne om underretning af hændelser og sårbarheder. Den nationale lovgivning, som gennemfører EU's NIS2- og CER-direktiver, spiller sammen med anden lovgivning, herunder fx selskabsret, GDPR og national persondatalovgivning, TV-overvågningslovgivning, ISPS-lovgivning (havnesikring), forvaltningsloven og offentlighedsloven. Samspillet mellem de forskellige lovgivninger bør overvejes, bl.a. i relation til aktindsigt.

Vi står naturligvis til rådighed for yderligere drøftelser.

Med venlig hilsen

Helene Jakobe Bom
Konsulent
(+45) 5218 5993
hebo@di.dk

Dansk Internet Forum

Forsvarsministeriet

Sendt til: fmn@fmn.dk og jhb@fmn.dk

21/08/2024

Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-lovforslag)

Forsvarsministeriet har den 5. juli 2024 sendt udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-lovforslag) i høring.

Dansk Internetforum (DIFO) skal indledningsvist takke for muligheden for at komme med bemærkninger til Forsvarsministeriets udkast til ny NIS 2-lov.

DIFO som administrator af .dk-domænenavne

DIFO administrerer gennem sit driftsselskab, Punktum dk, cirka 1,3 millioner .dk-domænenavne. Et domænenavn er primært en teknisk "vejviser" på internettet, der gør det muligt for internetbrugere at sende og modtage e-mails samt tilgå en bestemt dansk hjemmeside. Punktum dk sikrer denne funktionalitet inden for rammerne af lovgivningen på domæneområdet.

Et .dk-domænenavn kan registreres af fysiske og juridiske personer bosiddende i og uden for Danmark. For at registrere et .dk-domænenavn skal registranten gå gennem en domænenavnsregistreringstjeneste (også kaldet en forhandler). I forbindelse med registreringen indgår registranten en aftale med Punktum dk om brugsretten til .dk-domænenavnet. Aftalen fornyes typisk én gang om året.

Punktum dk er efter § 18 i Lov om internetdomæner forpligtet til at sikre korrekt navn, adresse og telefonnummer på registranter. Oplysningerne skal gøres offentligt tilgængelige, medmindre oplysningerne i medfør af anden lovgivning er undtaget fra offentlighed, fx pga. navne- og adressebeskyttelse i medfør af CPR-loven. Som følge heraf udfører Punktum dk data- og ID-kontrol ved brug af MitID på alle registranter bosat i Danmark. Registranter bosat i udlandet udtages til manuel data- og ID-kontrol på baggrund af en vurdering af risikoen for, at registrantens kontaktoplysninger og identitet ikke er retvisende.

Som administrator af topdomænet .dk, betragtes Punktum dk som en "væsentlig enhed" i henhold til NIS 2-loven.

Generelle bemærkninger til udkast til lovforslaget

DIFO støtter grundlæggende NIS 2-lovens ambition om at øge og ensarte cybersikkerheden og beskyttelsen mod cybertrusler på tværs af EU. Et højt cybersikkerhedsniveau er afgørende for at opretholde et sikkert, stabilt og modstandsdygtigt internet, hvor både borgere og virksomheder har tillid til, at deres data og onlineaktiviteter er beskyttet.

DIFO finder det positivt, at Forsvarsministeriet lægger op til en minimumsimplementering af NIS 2-direktivet, der også omfatter, at bekendtgørelser udstedt i medfør af loven skal udfærdiges som minimumsimplementering. Der er dog flere steder i lovforslaget, hvor bestemmelserne efter DIFO's opfattelse er uklare og bemærkningerne ikke giver det fornødne bidrag til at fortolke bestemmelserne. Det skaber, særligt i forbindelse med lovens § 11 om retvisende domænenavnsregistreringsdata, usikkerhed om enheders råderum, forpligtelsernes omfang og hjemmelsgrundlag.

Nedenfor gennemgås konkrete steder, hvor DIFO mener, at der er behov for yderligere klarhed.

Bemærkninger til de konkrete bestemmelser

Bemærkninger til § 6 – Risiko for overimplementering af sikkerhedskrav

Det fremgår af § 6, stk. 1, at væsentlige og vigtige enheder skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger. Det fremgår endvidere af bemærkningerne, at de foranstaltninger, der fastsættes, skal stå i forhold til risiciene.

§ 6, stk. 1, oplister en række sikkerhedsforanstaltninger, som væsentlige og vigtige enheder som minimum skal iagttage. Sikkerhedsforanstaltningerne er for visse enheder nærmere fastlagt i Kommissionens implementeringsretsakt, som har været i høring. Implementeringsretsakten fastlægger minutiøst, hvilke foranstaltninger en enhed skal foretage uden at tilføje den risikobaserede tilgang.

Hvis udkastet til implementeringsretsakten bliver gældende i Danmark, vil der derfor efter DIFO's opfattelse ske en overimplementering af direktivet, og dermed ikke en minimumsimplementering. Hertil kommer, at overimplementeringen ikke nødvendigvis medfører et højere cybersikkerhedsniveau, da en risikobaseret tilgang netop medfører, at en enhed vil fastsætte relevante foranstaltninger tilpasset det aktuelle trusselsbillede og mulige konsekvens.

Forsvarsministeriet bedes bekræfte, at foranstaltninger fastsat i medfør af § 6 skal ske ud fra en risikobaseret tilgang, således som det fremgår af bemærkningerne til bestemmelsen og dermed ikke som det fremstår i den kommende implementeringsretsakt.

Bemærkninger til § 7 - Ledelsesorgan

I § 7 omtales enhedens ledelsesorgan. Det er uklart, hvem "ledelsesorganet" i denne bestemmelse er. Er det bestyrelsen, den administrererede direktør eller hele ledergruppen i en virksomhed?

Bemærkninger til § 11 – To regelsæt

Det fremgår af § 11, stk. 1, at Punktum dk og forhandlere skal indsamle, verificere og offentliggøre registreringsdata. Bestemmelsen kommer til at fungere parallelt med domæneloven, der som nævnt pålægger Punktum dk en tilsvarende forpligtelse til at indsamle og offentliggøre korrekte registranters kontaktoplysninger. Forsvarsministeriet er ifølge bemærkningerne på side 243 opmærksom på, at der vil være to parallelle regelsæt.

En opretholdelse af domænelovens parallelle bestemmelser virker i praksis som en overimplementering af direktivets bestemmelser. Hertil kommer, at opretholdelse af domænelovens § 18 gør det væsentligt sværere at verificere domænenavnsregistreringsdata for .dk-domænenavne i forhold til andre domænenavnsendelser, idet adressekravet ikke gør sig gældende hos de fleste andre topdomæneadministratorer. Det bliver særligt vanskeligt for forhandlere, der typisk tilbyder registrering af flere domænenavnsendelser end kun .dk. Her bidrager domænelovens § 18 til, at forhandlere ikke kan tilbyde en registrant at gennemgå én verifikation, som kan benyttes til samtidig registrering af domænenavne i flere EU-lande.

Den kommende EU-Wallet vil give registranter mulighed for at verificere deres data på en nem, sikker og pålidelig måde i EU – men ikke i Danmark, hvis den digitale tegnebog ikke indeholder postadresse. Registranter uden for Danmark vil derfor fremover stadig skulle verificere sig gennem en manuel kontrol, som er mere ressourcekrævende for registranterne og nemmere at omgå for ondsindede aktører. Kravet om postadresse kan således medføre lavere cybersikkerhed og ulige konkurrencevilkår.

For at sikre lige konkurrencevilkår og proportionale verifikationsprocedurer i overensstemmelse med lovens ønske om minimumsimplementering tillige med størst mulig udbredelse af best practice verifikation (eID) opfordrer DIFO til, at Forsvarsministeriet sammen med Digitaliseringsstyrelsen overvejer at ophæve domænelovens parallelbestemmelse om verifikation af registreringsdata.

Bemærkninger til § 11, stk. 1 – Omfattede enheder

Det fremgår af bestemmelsen, at den gælder for topdomæneadministratorer og enheder, der leverer domænenavnsregistreringstjenester (forhandlere). Det fremgår af lovudkastets § 3, at topdomænenavnsadministratorer, der kun anvender topdomænenavne til eget brug ikke er omfattet af bestemmelsen. En lignende undtagelse synes i medfør af lovforslaget ikke at gøre sig gældende for forhandlere, som kun registrerer domænenavne til sig selv eller en afgrænset kreds af registranter.

DIFO er derfor i tvivl om, hvorvidt bestemmelsen omfatter alle forhandlere, som har indgået aftale med Punktum dk om forhandling af .dk-domænenavne, herunder Statens It og universiteter, som kun registrerer domænenavne til eget brug eller til en afgrænset kreds af registranter, fx styrelser.

Det bedes præciseret, at bestemmelsen ikke finder anvendelse på alle domænenavns-registreringstjenester (forhandlere), hvis dette er tilfældet.

Bemærkninger til § 11, stk. 3 - Verifikationsprocesser

Verifikation af kontaktmåder

Det fremgår af bemærkningerne på side 244 til bestemmelsen, at Punktum dk og forhandlere, *"bør navnlig verificere mindst én kontaktmåde for registranten"*. Dvs. enten e-mail eller telefonnummer, som er de to kontaktmåder, loven lægger op til.

DIFO kan tilslutte sig, at verifikationen ikke nødvendigvis skal omfatte både telefonnummer og e-mailadresse. Dette er også i overensstemmelse med internationale organisationers retningslinjer som bemærkningerne henviser til. Således fremgår det af ICANN's[1] retningslinjer, at man kan vælge mellem at validerer e-mail eller telefonnummer.

Verifikationsprocesser

Det fremgår af bemærkningerne på side 244, at verifikationsproceduren eksempelvis kan bestå i en forudgående kontrol, der foretages på tidspunktet for registrering, og efterfølgende kontrol, der foretages efter registreringen.

DIFO opfatter dette således, at der gives metodefrihed ift. tilrettelæggelsen af verifikationsprocessen.

Det kunne med fordel fremstå klarere i bemærkningerne, at metodefriheden ikke kun omfatter tidspunktet for kontrollen, men også antallet af kontroller, udtagning til kontrol, frekvens mv.

Data- og ID-kontroller er relative omkostningsfulde og ressourcetunge. Det er derfor vigtigt, at ressourcerne udnyttes bedst muligt, og at de værktøjer og metoder, der allerede i dag anvendes af Punktum dk til at sikre retvisende oplysninger, kan bibeholdes.

Det er i den forbindelse vigtigt, at der ikke fastsættes specifikke krav om, at der skal ske verifikation med specifikke tidsintervaller, fx ved fornyelse af aftalen. Et sådan krav vil være meget omkostningsfuldt og ressourcetungt for Punktum dk, forhandlere og registranter.

Det skyldes, at domænenavne som udgangspunkt registreres for 1 år ad gangen. Det vurderes derfor, at der vil skulle laves op til 1 million ekstra verifikationer om året, hvis verifikationen skal følge fornyelsen af et domænenavn rent. Hertil kommer, at Punktum dk har knap 300.000 domænenavne, hvor fuldmægtigen er en anden end registranten.

Ovenstående vil også øge risikoen for, at registranter mister deres domænenavne, selv om oplysningerne er korrekte, fordi registranten overser eller glemmer at gennemføre verifikationen,

[1] ICANN er den multistakeholderorganisation, som administrerer internettets "IP-adresser og domænenavne" globalt.

særligt hvis de har valgt automatiske betalingsmetoder. Det vil også blive besværliggjort at have et .dk-domænenavn i forhold til andre domænenavne, som måske ikke sætter samme krav til verifikation.

Endvidere vil kriminelle kunne samle domænenavnet op, når det slettes og misbruge det, ved at oprette hjemmesider eller e-mailadresser, som kan forveksles med den tidligere registrants navn eller brand og bruges til fx phishing eller anden økonomisk kriminalitet. Dette er en kendt form for kriminalitet.

Punktum dk modtager automatiske navne- og adresseopdateringer fra CVR/CPR på ca. 90 % af sine registranter. Hverken danske eller udenlandske registranter vil fremover kunne ændre e-mailadresse uden, at den valideres først. Det synes derfor overflødigt, at registranten samtidig selv skal huske at gøre noget aktivt hvert år for ikke at miste brugsretten til sit domænenavn med risici det indebærer, jf. ovenfor.

Særligt for registranter bosat uden for Danmark kræver det et vist arbejde for registranten at indsamle dokumentation til en data- og ID-kontrol. Gentagne kontroller af samme data vil derfor medføre en vis byrde for disse registranter og det synes ikke korrekt, som det fremgår af lovforslaget, at lovforslaget ikke skulle have konsekvenser for borgerne.

For at sikre lige konkurrencevilkår og proportionale verifikationsprocedurer, er det vigtigt, at der i forbindelse med implementering af NIS 2-loven, herunder ved fastsættelse af eventuelle bekendtgørelser, ikke indføres krav, der går længere end NIS2-direktivet og i strid med lovens ønske om at foretage en minimumsimplementering og som kan risikere at skabe dårligere cybersikkerhed og øgede administrative byrder for borgerne.

Bemærkninger til § 11, stk. 4 – Offentliggørelse af oplysninger

Det fremgår af bestemmelsen, at Punktum dk og forhandlere skal gøre domænenavns-registreringsdata, der ikke er personoplysninger, offentligt tilgængelige.

I overensstemmelse med NIS 2-direktivets præambel 112, forstår DIFO bestemmelsen således, at e-mailadresser på fysiske personer (privatpersoner), herunder enkeltmands-virksomheder[2], aldrig må offentliggøres.

Der findes imidlertid ingen kendte tekniske løsninger til at afgøre, om en e-mailadresse indeholder personoplysninger eller ikke indeholder personoplysninger. Selv ved en manuel gennemgang vil det ikke være muligt at afgøre om en e-mailadresse til en virksomhed tilhører en bestemt ansat eller betyder fx "kundeservice", "kontakt" mv. på et af verdens mange tusind sprog.

Ifølge ordlyden af bestemmelsen vil offentliggørelse af e-mailadressen heller ikke kunne baseres på et samtykke, idet Punktum dk ikke vil overholde loven i de situationer, hvor e-mailadressen ikke indeholder personoplysninger, men registranten har valgt offentliggørelse fra.

[2] Ifølge Datatilsynet gælder databeskyttelsesforordningen bl.a., når offentlige myndigheder, private virksomheder, foreninger o.l. behandler oplysninger om fysiske personer. Begrebet "fysisk person" omfatter ifølge Datatilsynet også enkeltmandsvirksomheder, da det i praksis ikke er muligt at skelne mellem oplysninger om ejeren som individ og oplysninger om virksomheden.

Punktum dk og forhandlere står derfor i en situation, hvor det i praksis er umuligt at efterleve NIS 2-loven og databeskyttelsesreglerne samtidig.

Da offentliggørelse ikke kan baseres på et samtykke, bør det fremgå klart af loven, at det vil være i overensstemmelse med databeskyttelsesreglerne at offentliggøre e-mailadresser på juridiske personer, såfremt der inden offentliggørelsen gøres tydeligt opmærksom på, at e-mailadressen vil blive offentliggjort, hvorfor den ikke må indeholde personoplysninger. Samtidig gives der mulighed for, at e-mailadressen til enhver tid kan ændres, såfremt den måtte indeholde personoplysninger.

For ikke at stille Punktum dk og forhandlere i en situation, hvor det i praksis vil være umuligt at leve op til lovgivningen med risiko for bøder eller andre sanktioner, bedes ovenstående præciseret.

Bemærkninger til § 11, stk. 5 – Udlevering af oplysninger

Det fremgår af lovforslagets § 11, stk. 5, at topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester på baggrund af en konkret vurdering af nødvendigheden skal give adgang til specifikke domænenavnsregistreringsdata til legitime adgangssøgende senest inden for 72 timer.

Hvis det skal være reelt muligt at leve op til bestemmelsen, er det nødvendigt, at bestemmelsen præciseres og tydeliggøres på flere punkter. Uden klare retningslinjer må det forventes, at der vil blive fastlagt en meget forsigtig og restriktiv praksis for udlevering af oplysninger.

<u>Hvem må oplysninger udleveres til</u>
Det fremgår af bemærkningerne på side 245-246, "*...der ved legitime adgangssøgende forstås enhver fysisk eller juridisk person, der fremsætter en anmodning i henhold til EU-retten eller national ret. Dette omfatter de kompetente myndigheder, CSIRT'en og myndigheder, som i henhold til EU-retten eller dansk ret arbejder med at forebygge, efterforske eller retsforfølge strafbare handlinger.*"

DIFO forstår ovenstående således, at legitime adgangssøgende i loven er afgrænset til at omfatte kompetente myndigheder, herunder myndigheder der arbejder med at forebygge, efterforske eller retsforfølge strafbare handlinger, samt CSIRT'en i henhold til dansk ret eller EU-retten. Dvs., at privatpersoner og virksomheder ikke er at anse som legitime adgangssøgende.

I modsat fald vil forpligtelsen blive ganske omfattende og byrdefuld. Det forstærkes hvis legitime adgangssøgende også måtte omfatte juridiske og fysiske personer, herunder myndigheder, uden for Danmark, jf. bemærkningerne på side 246, hvor der både henvises til "EU-retten eller national ret" og lige efter til "EU-retten eller dansk ret".

DIFO skal derfor anmode om, at det bekræftes, at legitime adgangssøgende kun omfatter anmodninger fra danske myndigheder og CSIRT.

Hvis legitime adgangsøgende også omfatter juridiske og fysiske personer uden for Danmark, bedes det oplyses, hvordan Punktum dk og forhandlere skal kunne vurdere, om en ansøger, der udgiver sig for at være en myndighed reelt er, hvad den udgiver sig for at være. Samme gør sig i endnu højere grad gældende for privatpersoner og virksomheder i udlandet, som Punktum dk ikke kender sikre metoder til at afgøre om er "svindlere" eller reelle i den forstand, at de har den påståede saglige grund til at få udleveret de ønskede oplysninger.

Endelig skal DIFO anmode om, at det præciseres i lovforslaget, som skal sikre et højt cybersikkerhedsniveau, at legitime adgangssøgende skal arbejde med at forebygge, efterforske eller retsforfølge strafbare handlinger inden for cybersikkerhed som defineret i lovens § 3. Derved udelukkes en eventuel tvivl om, at myndigheder der beskæftiger sig med fx forebyggelse af strafbare handlinger inden for andre områder skulle kunne få udleveret oplysninger i medfør af bestemmelsen.

Hvornår må udlevering af oplysninger finde sted

Det fremgår af bestemmelsen og bemærkningerne på side 245, at Punktum dk og forhandlere skal vurdere, om en anmodning om udlevering af oplysninger er lovlig og nødvendig for at oplysninger kan udleveres.

I hvilket omfang nødvendighed og lovlighed skal efterprøves af enheden, bedes præciseret. Det vil således i praksis ikke være muligt for en enhed at vurdere, hvorvidt en legitim adgangssøgende har brug for de ønskede oplysninger og har den fornødne påståede hjemmel til at få oplysninger udleveret. En sådan vurdering vil kræve omfattende oplysninger fra den adgangssøgende, herunder oplysninger som den adgangssøgende ikke nødvendigvis vil være interesseret i at udlevere, fx ved efterforskning strafbare forhold, samt kendskab til forskellige lovgivninger.

Det bedes derfor præciseres, at enheden kan lægge den legitime adgangssøgendes begrundelse om nødvendighed og hjemmel til grund, uden at skulle foretage en selvstændig prøvelse heraf.

Såfremt legitime adgangsøgende også omfatter ansøgere uden for Danmark, vil det af retssikkerhedsmæssige grunde være hensigtsmæssigt, at grundlaget for vurderingen i stedet fortages af en dansk retlig eller administrativ myndighed eller af ENISA (på EU-plan). Det vil også sikre en ensartet praksis for udlevering af oplysninger mellem enheder i Danmark og alternativt på tværs af EU.

Bemærkninger til § 11, stk. 6 – Samarbejde

Det fremgår af bestemmelsen, at topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester skal samarbejde om overholdelsen af de forpligtelser, der er fastsat i stk. 1-5, med henblik på at undgå dobbeltindsamling af domænenavnsregistreringsdata.

Bestemmelsen er efter DIFO's opfattelse formuleret lidt kringlet. Punktum dk forstår dog bestemmelsen og bemærkningerne hertil således, at det vil være i overensstemmelse med lovens forpligtelser og formål, at Punktum dk og forhandlere samarbejder i bred forstand med henblik

på at undgå dobbeltarbejde i forbindelse med opfyldelse af alle forpligtelserne i stk. 1-5 og ikke kun indsamling i stk. 1.

Det betyder konkret, at bestemmelsen giver det retlige grundlag der er nødvendig i persondataretten til at udveksle oplysninger om registranters kontaktoplysninger, verifikation og offentliggørelse heraf, jf. stk. 1-4, og at det retlige grundlag i præampelbetragtning 109 i NIS 2-direktivet er videreført.

Forsvarsministeriet bedes bekræfte, at bestemmelsen giver det nødvendige retlige grundlag til at udveksle de nødvendige personoplysninger i medfør af fx persondataforordningens § artikel 6, stk. 1, litra c (retlig forpligtelse) eller litra f (legitim interesse).

Bemærkninger til § 17 – Ikke-indgribende scanninger

Det fremgår af bemærkningerne til bestemmelsen, at Forsvarsministeriet kan foretage ikke-indgribende scanninger af væsentlige og vigtige enheders net og systemer uden udtrykkelig lovhjemmel i bestemmelsen.

DIFO kan tilslutte sig hensynet bag, at CSIRT'en kan foretage ikke-indgribende scanninger uden anmodning herom.

Det er dog uklart, hvad gælder i situationen, hvor en scanning, CSIRT'en forventede eller vurderede ikke var indgribende, viser sig at have indgribende konsekvenser for enheden.

Henset til, at enheden ikke har accepteret scanningen eller har mulighed for at modsætte sig den, bør det klart fremgå, at CSIRT'en har det fulde ansvar, herunder det økonomiske ansvar, og at bevisbyrden er omvendt således, at det påhviler CSIRT'en at bevise, at et tab/konsekvens for enheden ikke skyldes deres scanning.

Med venlig hilsen

Jakob Bring Truelsen
Administrerende direktør, DIFO og Punktum dk

DANSK STANDARD

Dato: 2024-08-21
Ref.: 2024/004461

Dansk Standards høringssvar ift. udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Sagsnummer 2024/004461

Dansk Standard takker for muligheden for at afgive høringssvar vedr. udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

Dansk Standards høringssvar er formuleret på baggrund af drøftelser med Dansk Standards udvalg for cyber- og informationssikkerhed, der består af mere end 55 danske eksperter inden for cybersikkerhed, som også er involveret i det europæiske og internationale standardiseringsarbejde inden for området.

Standarder og standardisering

Forsvarsministeriet har i sit udkast lagt vægt på, at der foretages en direktivnær minimumsimplementering af NIS2-direktivet. Vi mener ikke, at det er direktivnært at udelade henholdsvis artikel 25 om standardisering eller henvisningen til internationale og europæiske standarder, som står nævnt i artikel 21, da det er en vigtig del af direktivets indhold. Standarder kan bidrage til at sikre en ensrettet tilgang på tværs af medlemslandene, og de kan styrke det generelle cybersikkerhedsniveau på tværs af medlemsstaterne via en fælles tilgang.

I direktivets artikel 21 om foranstaltninger står der, at *"…foranstaltningerne, under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder (…) skal tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene".* I udkastet til den danske lovtekst er europæiske og internationale standarder ikke nævnt, hvilket ikke er hensigtsmæssigt, da ambitionen med NIS2 er at have en fælles tilgang til håndteringen af cybersikkerhed på tværs af medlemslandene.

I direktivets artikel 21 stk. 5 nævnes det yderligere, at Kommissionen senest den 17. oktober 2024 *"…vedtager gennemførelsesretsakter, der fastsætter de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i stk. 2 (…)".* Der står også *"Ved udarbejdelsen af de gennemførelsesretsakter, der er omhandlet i nærværende stykkes første og andet afsnit, følger Kommissionen i videst muligt omfang europæiske og internationale standarder samt relevante tekniske specifikationer".* På den baggrund vil det også være en udfordring, at vi i Danmark ikke tilskynder til at anvende europæiske og

internationale standarder og tekniske specifikationer, hvis disse bliver en del af gennemførelsesretsakterne.

Som det fremgår af direktivets artikel 25, *"… tilskynder medlemsstaterne til at benytte europæiske og internationale standarder og tekniske specifikationer, der er er relevante for sikkerheden i net- og informationssystemer for at sikre en samordnet gennemførelse af artikel 21 stk. 1 og 2*". På den baggrund er det uhensigtsmæssigt, at direktivets artikel 25 om standardisering ikke er gengivet i den danske lovtekst. Som det fremgår af direktivets præambel 5, så er formålet at fjerne *"…store forskelle mellem medlemsstaterne, navnlig ved at fastsætte minimumsregler for hvordan en koordineret reguleringsramme fungerer…"* Derfor giver det ikke mening, at vi i Danmark udelader referencen til standarder, når det er et krav fra direktivet, som de andre medlemslande bibeholder i deres implementering. Ved ikke at henvise til internationale og europæiske standarder vil danske virksomheder ikke blive opfordret til at anvende de samme redskaber som andre europæiske virksomheder, hvilket potentielt kan stille dem ringere i en konkurrencemæssig situation.

I lovudkastets §21 nævnes tilsyn og audits, men det er ikke nærmere defineret, hvad disse audits og tilsyn skal hægtes op på. Ved at referere til standarder i lovteksten som et muligt redskab, vil det være mere håndgribeligt for organisationer og virksomheder at leve op til de krav om cybersikkerhed, som de stilles overfor samt at dokumentere det.

Direktivets artikel 14 nævner, at der som led i *"…at støtte og lette strategisk samarbejde og udvekslingen af oplysninger mellem medlemsstaterne samt for at styrke tillid og fortrolighed nedsættes der en samarbejdsgruppe."* En af samarbejdsgruppens opgaver er at udveksle bedste praksis og oplysninger vedrørende gennemførelsen af direktivet, herunder om bl.a. standarder og tekniske specifikationer. På den baggrund vil det være hensigtsmæssigt, at vi i den danske implementering også anbefaler danske virksomheder og organisationer til at anvende europæiske og internationale standarder og tekniske specifikationer.

De europæiske standardiseringsorganisationer CEN og CENELEC samarbejder med de internationale standardiseringsorganisationer ISO og IEC om at nå til enighed om fælles standarder, der kan anvendes over hele verden, inden for de emner, der ligger tættest på Europas grundlæggende værdier og interesser.

Brugen af standarder er med til at styrke EU's globale konkurrenceevne, da standarder fungerer som et fælles sprog. Mange danske virksomheder opererer globalt, og de har derfor glæde af, at identiske standarder kan anvendes internationalt og i Europa, således at de ikke skal tilpasse produktionslinjer og dokumentation til hvert enkelt marked. Det er med til at understøtte international handel, garantere forbrugersikkerhed og mindske handelsbarrierer for virksomheder. Virksomheder kan dermed vise, at de lever op til de krav og principper, der er i den/de pågældende standard(er) både over for forbrugere og andre virksomheder. I og med at standarderne er internationale, gør dette sig gældende på tværs af landegrænser, hvilket sikrer en mere gnidningsfri, international handel.

Internationale standarder i ISO/IEC 27000-serien anvendes bredt blandt danske virksomheder, og statslige myndigheder er også underlagt at følge ISO/IEC 27001. Derfor er det uhensigtsmæssigt, at det danske lovudkast ikke refererer artiklerne om standardisering, da det netop er et redskab for virksomhederne til at leve op til de foranstaltninger, der refereres til i artikel 21.

Generelle bemærkninger

Dansk Standard mener, at det er vigtigt at tydeliggøre, hvad der menes med ledelsesorgan i lovtekstens §7, så danske organisationer og virksomheder ikke er i tvivl om deres forpligtelser og ansvarsområder. Der er behov for at vide, på hvilket niveau ansvaret er placeret, og hvor langt ned i organisationen ansvaret går. Herunder om der er beskyttelse af de medarbejdere under direktørniveau, der skal implementere foranstaltningerne.

I lovtekstens §9 ift. registrerings- og underretningsforpligtelser er det nævnt i stk. 2, at *" Oplysningerne efter stk. 1 skal indgives senest den 17. januar 2025."* Eftersom den danske lov først træder i kraft den 31. marts 2025, er det en udfordring, at der henvises til en dato før dette.

I lovtekstens §14 nævnes nærvedshændelser. En definition af nærvedshændelser er dog ikke med i lovtekstens §3 med definitioner til trods for, at der findes en definition af nærvedshændelser i direktivets definitioner i artikel 6.

I lovtekstens §17 beskrives CSIRT'ens opgaver. Vi opfordrer til, at kravene for CSIRT'en udspecificeres yderligere på samme vis som i direktivet. Der mangler ligeledes en definition af CSIRT i §3 i den danske lovtekst.

I lovtekstens §23 ift. håndhævelsesforanstaltninger står der, at den kompetente myndighed kan træffe afgørelse om *"…at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos enheden at udøve ledelsesfunktioner i den pågældende enhed".* Der står således ikke noget om bestyrelsens ansvar. Spørgsmålet er, om der kan være en fejl i den danske oversættelse af direktivet, eftersom bestyrelsen ikke er nævnt.

Afsluttende bemærkninger

Dansk Standard synes, det er vigtigt for cybersikkerheden i hele Europa, at der fastsættes fælles regler for net- og informationssikkerhed. Ensretningen er essentiel for at styrke den fælleseuropæiske cybersikkerhed. Derfor er der også behov for, at vi i Danmark læner os op ad europæiske definitioner, der er på linje med, hvad de andre europæiske lande gør. Bekymringen går på, om vi i den danske lovtekst samt bekendtgørelser vil operere med danske definitioner og fortolkninger, der ikke er på linje med de andre europæiske lande,

hvilket på sigt kan gøre det mere vanskeligt for danske virksomheder og organisationer at samarbejde og konkurrere på europæisk plan.

Dansk Standard ønsker samtidig at komme med en opfordring til, at man fra dansk side er opmærksom på, hvordan NIS2 er koblet til den kommende Cyber Resilience Act, AI Act, Cyber Security Act og lov om kritiske enheders modstandsdygtighed. Det er lovgivninger, der rammer bredt blandt danske virksomheder og organisationer, og der er derfor behov for at samtænke lovgivningerne og dermed vise, at vi i Danmark forholder os til de aftalte rammer i EU. Et konkret eksempel er koblingen mellem NIS2 og CRA ift. indrapportering af hændelser, hvor NIS2 omhandler systemrapportering, og CRA'en har fokus på produktrapportering. For at afhjælpe byrden hos organisationer og virksomheder vil det være hensigtsmæssigt, at indrapporteringerne mere eller mindre er opbygget på samme måde.

Dansk Standard foreslår, at den danske lovtekst refererer direktivteksten helt tekstnært ift. artikel 21 og artikel 25 vedrørende standarder, og på den baggrund også anbefaler danske virksomheder og organisationer at anvende europæiske og internationale standarder og tekniske specifikationer, der er relevante for sikkerheden i net- og informationssystemer. Direktivets artikel 25 og 21, der nævner standarder og standardisering, kan med fordel indarbejdes i lovforslagets § 6 pkt. stk. 3.

Dansk Standard synes, det er vigtigt, at standarder og standardisering nævnes direkte i lovteksten og ikke udelukkende refereres i de kommende bekendtgørelser, da det vil være lovteksten, som virksomheder og organisationer primært orienterer sig imod. Også set i lyset af, at det er op til hver af de kompetente myndigheder/ressortministre at bestemme, hvilke krav og anbefalinger de stiller i bekendtgørelserne, hvilket igen kan skabe en uensartet tilgang på tværs af områderne i Danmark, hvilket er uhensigtsmæssigt for virksomhederne.

Med lovforslaget gives de relevante ressortministre bemyndigelse til at fastsætte nærmere regler i bekendtgørelsesform. Vi opfordrer til en inkluderende proces i udformningen af disse bekendtgørelser, og vi ser frem til at kunne bidrage konstruktivt. Vores mål er at sikre, at de centrale krav og regler i bekendtgørelserne både lever op til og tager højde for gældende europæiske og internationale standarder.

Vi står naturligvis til rådighed for eventuelle uddybninger eller spørgsmål.

Med venlig hilsen

Berit Aadal, chefkonsulent, Dansk Standard (baa@ds.dk / 26 22 46 96)

Til Forsvarsministeriet

21. august 2024

Høringssvar til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Danske Havne takker for muligheden for at afgive bemærkninger til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

NIS 2-direktivet har til formål at skabe et højere og mere ensartet cybersikkerhedsniveau på tværs af medlemsstaterne i EU. Direktivet stiller bl.a. cybersikkerhedskrav til virksomheder, myndigheder og organisationer (enheder) inden for en lang række samfundskritiske sektorer, som bl.a. omfatter energi, transport, bankvirksomhed, sundhed, drikke- og spildevand, digital infrastruktur og den offentlige forvaltning. Det er et lovforslag, der er vigtig for Danmarks – herunder danske erhvervshavnes – sikkerhed.

Danske Havne forholder sig enig i lovforslagets formål, og ser frem til muligheden for at afgive bemærkninger til bekendtgørelserne, når de sektor bestemte bekendtgørelse kommer i høring.

Danske Havne lægger vægt på at der ikke kommer uforholdsmæssige store økonomiske og/eller administrative implementeringsomkostninger for havnene.

Med venlig hilsen,

Danske Havne, Iben Birk

Forsvarsministeriet

fmn@fmn.dk

22-08-2024
EMN-2024-00900
1717832
mortw@regioner.dk

Danske Regioners høringssvar til lovforslag om foranstaltninger til sikring af højt cybersikkerhedsniveau

Forsvarsministeriet har d. 5. juli 2024 anmodet Danske Regioner om bemærkninger til lovforslag om foranstaltninger til sikring af højt cybersikkerhedsniveau. Den aktuelle høring omhandler den generelle lovgivning, som skal uddybes gennem sektorspecifikke bekendtgørelser.

Danske Regioner har indhentet bidrag fra regionerne vedrørende denne generelle lovgivning, og på baggrund heraf udarbejdet et samlet høringssvar på vegne af regionerne med overordnede bemærkninger til lovforslaget. Det samlede høringssvar er godkendt af Danske Regioners bestyrelse d. 22. august 2024.

Bedre rammer for regionernes arbejde med cybersikkerhed

Danske Regioner finder det overordnet positivt, at der med lovforslaget præciseres fælles rammer for de tekniske, operationelle og organisatoriske tiltag, der skal implementeres for at sikre vores centrale og samfundskritiske funktioner, herunder sundheds- og transportsektoren.

Den danske sundhedssektor er yderst digitaliseret og er en central samfundskritisk sektor, og cyberangreb mod sektoren kan få afgørende betydning for hospitalsdriften og dermed patientsikkerheden samt borgernes tillid til sundhedsvæsenet. Danske Regioner har derfor i de seneste Økonomiforhandlinger forsøgt at sikre at sundhedsvæsnets parter i fællesskab prioriterer sikring af sundhedssektoren mod cybertrusler, så der opnås et tilfredsstillende sikkerhedsniveau.

Danske Regioner mener at rammerne og retningen i lovforslaget grundlæggende set er et skridt i den rigtige retning for en fælles sikring og forpligtelse af vores centrale samfundsfunktioner.

Danske Regioner bakker derfor grundlæggende op om lovforslaget.

Bemærkninger til rammer for implementeringen

Selvom Danske Regioner overordnet finder lovforslaget positivt, har Danske Regioner en række bemærkninger til rammerne for implementeringen, der kan sikre at det fælles formål vedr. øgede foranstaltninger til sikring af et højt cybersikkerhedsniveau understøttes bedst muligt.

Sektorspecifikke bekendtgørelser

Danske Regioner anerkender at sektorspecifikke bekendtgørelser er nødvendige for at adressere de unikke udfordringer og behov inden for hver af de sektorer, der underlægges NIS2. Den nuværende lovtekst, på grund af den manglende specificitet, gør det dog vanskeligt for regionerne at forberede sig tilstrækkeligt på de kommende krav, som hver sektor vil blive underlagt. Denne usikkerhed kan føre til udfordringer i planlægningen og allokeringen af nødvendige ressourcer.

Danske Regioner opfordrer derfor til, at der så hurtigt som muligt udarbejdes sektorspecifikke bekendtgørelser, så regionerne kan få den nødvendige klarhed og forberedelsestid. Disse bekendtgørelser samt eventuel rammebekendtgørelse forventer Danske Regioner selvfølgelig i rettidig høring.

Minimum implementering

Danske Regioner ønsker at understrege vigtigheden af at fastholde lovforslagets og regeringens principper, der sikrer minimumsimplementering på tværs af alle sektorer, herunder sundhedsvæsenet. Dette indebærer, at kravene skal være realistiske og gennemførlige uden at skabe unødvendige byrder for de involverede aktører. Det er vigtigt, at minimumsimplementeringens principper følges hele vejen igennem lovgivningsprocessen for at sikre, at ressourcerne bruges effektivt, og at de krav, der stilles, er proportionale i forhold til den faktiske risiko og trussel.

Risikobaseret tilgang

Danske Regioner vil fremhæve behovet for at fastholde en risikobaseret tilgang til cybersikkerhed gennem hele implementeringen af NIS2. Det er afgørende, at indsatsen fokuserer på at håndtere de største risici først og tilpasses efter de konkrete trusler som hver sektor står over for. Dette sikrer, at ressourcerne anvendes mest effektivt, og at de mest kritiske samfundsfunktioner beskyttes bedst muligt. En risikostyret tilgang vil også give regionerne mulighed for at tilpasse deres sikkerhedsstrategier til deres specifikke behov og udfordringer.

Økonomiske rammer for implementering

Danske Regioner er grundlæggende enig i, at det nuværende lovforslag ikke kan fastlægge de økonomiske konsekvenser ved implementering af NIS2 med sikkerhed. Ifølge EU's egne beregninger, som også fremgår af lovforslaget, vil en NIS1-compliant organisation opleve en stigning på 12-15 % i it-sikkerhedsbudgettet, hvilket der i lovforslaget bliver estimeret til at koste regionerne mellem 60 og 100 mio. kr. årligt. Danske Regioner mener, at dette beløb er undervurderet, og set i lyset af, at kommende bekendtgørelser kan indeholde yderligere præciseringer, der vil øge omkostningerne yderligere, vil Danske Regioner forholde sig endeligt til økonomien når de specifikke bekendtgørelser foreligger.

Danske Regioner vil her særlig påpege Operational Technology -området, bl.a. CT-scannere, laboratoriesystemer og medicinfremstilling, og IOT-området, bl.a. glukosemålere, insulinpumper og andre typer af sensorer med netværksadgang. Det er uklart, hvorvidt, og i hvilket omfang, OT- og IOT-områder inkluderes i lovgivningen og begge er områder, der vil medføre betydelige ekstra omkostninger for regionerne. Vi opfordrer derfor til en præcisering på dette område i den sektorspecifikke bekendtgørelse, så det står klart, hvilke krav der vil gælde.

Danske Regioner vil pointere, at det er afgørende, at der sikres tilstrækkelige midler til at håndtere disse øgede omkostninger, både anlægs- og varige driftsmidler, så implementeringen af NIS2 ikke får negative implementeringskonsekvenser for de primære og samfundskritiske funktioner i sundhedsvæsenet.

Danske Regioner vil derfor, når de sektorspecifikke bekendtgørelser foreligger, løfte kompensation via DUT-forhandlingerne.

Implementeringsperiode

Givet de betydelige ændringer som NIS2-direktivet vil medføre, anbefaler Danske Regioner, at der gives tilstrækkelig tid og fleksibilitet i implementeringsperioden efter ikrafttrædelsesdatoen d. 1. marts 2025. Dette vil sikre, at regionerne kan foretage de nødvendige investeringer og organisatoriske ændringer uden at kompromittere den daglige drift, især inden for kritiske områder som sundhedsvæsenet. En realistisk og gradvis implementering vil også give mulighed for at justere og tilpasse indsatserne baseret på løbende erfaringer.

Tilsyn og Regulatorisk Sammenhæng

Danske Regioner anerkender behovet for at udmøntningen sker i sektorspecifikke bekendtgørelser, der sikrer de enkelte sektorers behov. Danske Regioner er dog bekymrede over, at forskellige sektorer vil være underlagt forskellige tilsynsmyndigheder med potentielt forskellige tilgange og krav. For regionerne, der opererer på tværs af sektorer, kan dette medføre en

fragmenteret og uensartet regulering, hvilket kan føre til administrative meromkostninger, uensartet implementering og deraf begrænset effekt af lovforslaget.

Danske Regioner anbefaler en koordineret tilgang mellem forsvarsministeriet og de pågældende ressortministerier, der skal sikre sammenhæng og ensartede krav på tværs af sektorer.

Administrative byrder

Implementeringen af NIS2-direktivet vil kræve betydelige ressourcer til at opbygge og vedligeholde de nødvendige strukturer og processer år efter år. Danske Regioner er bekymret over, at de administrative byrder vil være betydelige, og der opfordres til, at der tages hensyn til dette i den endelige implementering af direktivet.

Ressource- og kompetencemangel:

Danske Regioner er bekymrede for, at det vil blive vanskeligt at rekruttere tilstrækkeligt med kvalificeret arbejdskraft, da både den offentlige og private sektor vil skulle opfylde de samme krav i henhold til NIS2. Dette kan skabe en flaskehals i forhold til at få ansat de nødvendige it-specialister.

Koordinering med eksisterende nationale strategier

Danske Regioner anbefaler, at implementeringen af NIS2-direktivet koordineres tæt med eksisterende nationale strategier for cybersikkerhed og digitalisering, herunder den nationale strategi for cyber- og informationssikkerhed. Det er vigtigt, at de nye krav fra NIS2 harmoniseres med de initiativer og strukturer, der allerede er på plads, for at undgå overlap og dobbeltarbejde. Dette vil også bidrage til en mere effektiv udnyttelse af ressourcer og sikre en sammenhængende tilgang til cybersikkerhed på tværs af sektorer.

Kollektiv trafik

Inden for kollektiv transport deler vi de overordnede forbehold og bekymringer vedr. økonomi, implementering mv. og har enkelte særskilte opmærksomheds-punkter.

Med NIS2 vil flere transportaktører blive omfattet. Det fremgår af lovforslaget, at bl.a. jernbanevirksomheder og "vejmyndigheder… der er ansvarlige for trafikledelse, med undtagelse af offentlige enheder, for hvilke trafikledelse eller drift af intelligente transportsystemer er en ikkevæsentlig del af deres generelle aktivitet" samt "operatører af intelligente transportsystemer" er omfattet.

På baggrund af ovenstående er det uafklaret om, hvor store dele af de regionale trafikselskabers virksomhed, der skal leve op til NIS2 og kravene til

foranstaltninger til styring af cybersikkerhedsrisici. Det formodes, at en kommende sektorbekendtgørelse på transportområdet vil tydeliggøre om ud over de regionale baner også de regionale trafikselskabers buskørsel er omfattet, om den koordinerede kørsel i flextrafikken gør, at de her vil blive opfattet som operatører af intelligente transportsystemer samt om aktiviteterne i regi af Rejsekort og Rejseplan er omfattede. Der opfordres til, at den kommende sektorbekendtgørelse forholder sig til konsekvenserne af, at organiseringen af bl.a. de regionale baner adskiller sig – hvor kørslen nogle steder er udbudt til private aktører, så varetager andre lokalbaneselskaber selv driften.

I afsnit 4.1. 'Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige' fremgår, at "Der vurderes desuden at være negative implementeringskonsekvenser", hvilket i lovforslaget ikke er søgt kvantificeret. Det bemærkes, at implementeringskonsekvenserne alt andet lige må være højere for transportaktører, der ikke tidligere har været omfattet af kravene i NIS, end tilfældet er for andre aktører, der pt. lever op til kravene i NIS.

Også her er formodningen, at den kommende sektorbekendtgørelse på transportområdet vil være opklarende i forhold til de forventede økonomiske konsekvenser ved implementering og efterfølgende løbende opfyldelse.

Afslutningsvis vil Danske Regioner gerne udtrykke vores vilje til at samarbejde med relevante myndigheder for at sikre en effektiv og sammenhængende implementering af NIS2-direktivet.

På vegne af Danske Regioners bestyrelse

Anders Kühnau
Formand, Danske Regioner

Mads Duedahl
Næstformand, Danske Regioner

DANSKE REVISORER FSR

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Att.: Jakob Halkjær Brams
Pr. e-mail: fmn@fmn.dk; cc: jhb@fmn.dk

22. august 2024

FSR – danske revisorer
Slotsholmsgade 1, 4. sal
DK - 1216 København K

Telefon +45 7225 5703
fsr@fsr.dk
www.fsr.dk

CVR. 55 09 72 16
Danske Bank
Reg. 9541
Konto nr. 2500102295

Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau – sagsnummer 2024/004461

Tak for muligheden for at kommentere denne høring. Vi har følgende bemærkninger:

- § 12, stk. 2, definerer, hvilke typer hændelser der kan anses for væsentlige. Vi foreslår, at pkt. 1 "økonomisk tab for den berørte enhed" suppleres med "eller samfundet".

- § 21 indeholder en række metoder i relation til tilsyn med de væsentlige enheder. Vi gør opmærksom på muligheden for at sikre løbende overvågning via revisionserklæringer udarbejdet af godkendt uafhængig revisor. Til inspiration henvises til template "Uafhængig revisors ISAE 3000-erklæring med begrænset sikkerhed om foranstaltninger til styring af risici i relation til net- og informationssystemer og rapporteringsforpligtelser i henhold til aftale med [Kunde]" udarbejdet af FSR – danske revisorer: https://www.fsr.dk/fsr-danske-revisorer-lancerer-en-ny-nis2-net-og-informationssystemer-erklaeringstemplate-i-relation-til-leverandoerer-eller-tjenesteudbydere

- S.206: Der bliver beskrevet forskellige scenarier om, hvorvidt en enhed vil være omfattet af dansk jurisdiktion eller en anden medlemsstat i Unionen alt afhængig af, hvor tjenester bliver udbudt, eller hvor beslutninger bliver taget. Vi foreslår, at der gives nogle retningslinjer for, hvordan dette rent praktisk skal registreres over for myndighederne.

- S. 249: Det bliver beskrevet, at væsentlige hændelser dækker over: "1) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller 2) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade".

  Europa-Kommissionen har for nylig publiceret udkast til foranstaltninger til styring af cybersikkerhedsrisici på tværs af EU gennem udkastet til gennemførelsesforordning af 27/06/2024. Vi anbefaler, at dette bruges som inspiration til at definere mere kvantitative mål i forhold til, hvad en væsentlig hændelse dækker over.

- S. 280: Artikel 31 indeholder en række scenarier for, hvordan de kompetente myndigheder foretager inspektion hos NIS2-omfattede virksomheder. Vi

foreslår, at beskrivelsen uddyber, hvorvidt inspektionen planlægges med andre myndigheder i Unionen i tilfælde af, at virksomheden driver forretning uden for landets grænser.

- Generelt: Krav til OT (Operational teknologi) – sikkerhed fremgår ikke klart af lovteksten. Vi anbefaler, at der i lighed med informationssikkerhed også fokuseres på OT.

Vi står naturligvis gerne til rådighed, hvis vores bemærkninger giver anledning til spørgsmål eller uddybning.

På vegne af FSR – danske revisorers Cybersikkerhedsudvalg

Med venlig hilsen

Kasper Frølich Kristensen
Fagchef for revision og regnskab, statsaut. revisor

DANSKE
UNIVERSITETER
UNIVERSITIES DENMARK

21. AUGUST 2024

Høringssvar til udkast til Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Danske Universiteter har modtaget Forsvarsministeriets udkast til forslag til Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau i høring med svarfrist den 22. August 2024.

Det fremgår af bemærkningerne til § 1 side 202, at for så vidt angår uddannelsesinstitutioner forventes det primært at være aktuelt at sætte reglerne i kraft for universiteter omfattet af universitetsloven, jf. lovbekendtgørelse nr. 778 af 7. august 2019, hvorfor de otte universiteter forventer at blive omfattet at loven.
Danske Universiteter har på vegne af de otte danske universiteter følgende bemærkninger til lovudkastet:

Danske Universiteter høringssvar er koordineret med DEIC/DKCert.

Overordnede bemærkninger
Universitetssektoren i Danmark favner meget bredt indenfor mange forskellige forskningsdiscipliner og er kendetegnet ved tværgående samarbejder såvel internt som nationalt og internationalt. Samarbejdspartnere spænder over uddannelsesinstitutioner, herunder øvrige universiteter, til fonde, selskaber, foreninger og interesseorganisationer. Universitetssektoren er meget bevidste om det øgede trusselsniveau, der er på sektoren og anser arbejdet med cyber- og informationssikkerhed som en grundlæggende forudsætning for at universiteterne kan understøtte forskning og uddannelse. Et arbejde som universiteterne vurderer, bør hvile på en risikobaseret tilgang.

Danske Universiteter er generelt bekymrede for, om NIS2-direktivets brede generiske definitioner af omfattet infrastruktur (f.eks. Datacentertjeneste og Digital tjeneste), kan medføre en overimplementering af sikkerhed på universiteterne eller en tilbageholdenhed med deling af infrastruktur på tværs af universiteter såvel nationalt som internationalt, som negativt vil påvirke universiteternes evne til at løfte lovfastsatte opgaver, herunder forskning. Danske universiteter anbefaler derfor, at der fastsættes en mere snæver definition af genstandsfeltet således, at det alene er den af universiteterne drevne samfundsvigtige forskningsinfrastruktur og forskning, som er omfattet af NIS2 på universiteterne. Universiteternes øvrige dele bør falde uden for genstandsfeltet.

Det er givet, at de områder på universiteterne, som er en del af en kritisk national forsyningskæde, skal have et sikkerhedsniveau, der efterlever NIS2. Men datacentre på universiteterne, som leverer tjenester til forskningsprojekter uden for den

pågældende organisation, er ikke nødvendigvis nationalt kritiske. Det er væsentligt for Universiteterne, at der med afsæt i en risikovurdering skelnes tydeligt mellem universiteternes mange forskellige anvendelser af tjenester og infrastruktur, så det ikke er al delt forskningsinfrastruktur, der bliver underlagt NIS2.

Der lægges i loven op til at vedkommende minister bemyndiges til ved bekendtgørelse at bestemme, at loven helt eller delvist finder anvendelse. Her har universiteterne et ønske om at blive inddraget i arbejdet med en bekendtgørelse for universitetssektoren.

Koordineret implementering

Der er i EU-medlemslandene foretaget forskelligt valg i forhold til om universitetssektoren er omfattet af NIS2 direktivet. Her hører Danmark til de lande, som har valgt at lade Universitetssektoren blive omfattet af NIS2. Der er en bekymring fra Danske Universiteter om, at en forskelligartet implementering af NIS2 på tværs af EU vil vanskeliggøre samarbejdet mellem de danske universiteter og den store del af de europæiske universiteter, som ikke er omfattet af NIS2.

Danske Universiteter er bekymrede for, at man i forbindelse med underlægningen som konsekvens betinger sig, at også samarbejdspartnere i udlandet, fx EU-lande, vil være nødt til at leve op til NIS2-kravene. I så fald vil de danske universiteter i betydelig grad afskæres fra mulige samarbejder, og i særdeleshed fra EU-forskningsmidler, hvor der er krav om samarbejder på tværs af landegrænser. Det er således vigtigt, at underlægningen af de danske universiteter kun har rækkevidde til de danske universiteters aktiviteter.

For at sikre, at de danske universiteter kan have en balanceret tilgang til NIS2 direktivet, der ikke skader dansk forskning, er det essentielt, at det tydeligt fremgår af lovteksten, at implementeringen af sikkerhedsforanstaltninger skal ske proportionalt med risikoen for kritiske forsyningskæder og under hensyntagen til universiteternes aktuelle teknologiske stade jf. Specifikke bemærkninger punkt 6.

Indrapportering af sikkerhedshændelser

Det fremgår af loves bemærkninger, at der sektorvist efter behov kan fastsættes nærmere regler om, hvornår en hændelse anses for at være væsentlig, og derfor skal indrapporteres.

Danmark er i top tre af lande i Europa, der indberetter flest (GDPR) datasikkerhedsbrud målt pr. indbygger. Hvis de danske virksomheder og myndigheder udviser lige så høj compliance på indberetning af cybersikkerhedshændelser, vil der være tale om en væsentlig arbejdsbyrde, som mange andre europæiske universite-

ter ikke har. Det er derfor vigtigt, at sektoren inddrages i fastlæggelse af disse kriterier og at indrapportering af sikkerhedshændelser tager udgangspunkt i en risikobaseret tilgang så indrapporteringen ikke gælder hele universitetets virke men kun de områder som er kritisk for forsyningskæder.

Det bør også nøje overvejes, hvilke oplysninger der i forbindelse med indrapportering af sikkerhedshændelser bør være tilgængelig i agtindsigter efter offentlighedsloven, så der kommer den rette balance i forhold til gennemsigtighed kontra risikoen for, at man løber aktørernes ærinde i forhold til deres ønske om at skabe utryghed og frygt for dårligt omdømme.

Forskningssamarbejder

Universitetssektoren i Danmark arbejder pt. på at samarbejde om national infrastruktur til forskning. Dette foregår bl.a. i regi af Danish e-infrastructure Consortium (DeiC) og har til formål at sikre en mere effektiv udnyttelse af omkostningstunge dataprocesserings- og datalagringsressourcer (High Performance Computing, Big Data Storage etc.). Der er en fare for, at en for unuanceret implementering af NIS2 direktivet i forskningssektoren vil sætte dette arbejde i stå, da compliancekravene fra NIS2 til denne type infrastruktur er for høje til, at universiteterne generelt vil kunne leve op til dem indenfor et rimeligt tidsrum. Afhængig af typen af fælles forskningsinfrastruktur er der også en risiko for, at sikkerhedsinvesteringerne ikke bliver foretaget, der hvor truslerne er mest presserende. Det bør sikres, at de risici, som NIS2 direktivet skal beskytte Danmark og dansk forskning imod, står mål med de omkostninger, som universiteterne bliver pålagt, så NIS2 ikke bliver en hindring for den forskning, universiteterne skal levere til gavn for udviklingen af det danske samfund.

Yderligere fremgår det af lovens bemærkninger, at det er Forsvarsministeriets opfattelse, at hele enheden (CVR nr.) bliver omfattet, hvis der er dele af virksomheden/institutionen, der er omfattet – i relation til universiteterne fx HPC-anlæg og forskning, der kan kommercialiseres. Hvis det bliver tilfældet, vil det være meget relevant at få drøftet, hvordan det skærpede ledelsesansvar med mulighed for personlige sanktioner og bøder kan balanceres, så der stadig kan skabes gode rammer for at bedrive universiteternes kerneforretning: videnssamarbejde, undervisning og forskning.

Sikkerhed for forskning

I "udkast til Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau" lægges der op til at Center for Cybersikkerhed, som hører under FE, bliver en central koordinerende enhed i rollen som CSIRT. Danske Universiteter vil i forbindelse med dette gerne bede om, at det tydeliggøres, hvilke nye kompetencer Center For Cybersikkerhed får qua sin rolle som CSIRT, samt at det tydeliggøres, at Center

for Cybersikkerhed ikke får adgang til de omfattede enheders forretningsdata, herunder også forskningsdata, da dette vil kunne påvirke universiteternes evnes til at opretholde den nødvendige tillid til både datasubjekter og kommercielle samarbejdspartnere jf. Generelle bemærkninger punkt 5.

Generelle bemærkninger

Danske Universiteter har følgende overordnede bemærkninger til lovudkastet.

1. Det præciseres ikke i lovudkastet, men Danske Universiteter henstiller til, at bekendtgørelserne – ligesom NIS2-hovedloven – træder i kraft pr. 1. marts 2025, og at bekendtgørelserne suppleres af konkrete vejledninger til virksomheder og offentlige institutioner fra de relevante kompetente myndigheder, hurtigst muligt og helst inden ikrafttrædelsesdatoen.
2. Når der i 3.2.3 fastsættes at enheder, der indgår i flere sektorer, skal efterleve de krav, der gælder for de forskellige sektorer, så kan dette medføre udfordringer for dele af den offentlige sektor, da disse både er omfattet som offentlige myndigheder, men også fx som datacenter (Statens IT), som universiteter eller som sundhedsmyndigheder, og derfor skal efterleve mange forskellige krav. Derfor opfordres Forsvarsministeriet til at sikre en høj grad af koordinering mellem resortmyndighederne i forhold til både operationalisering af krav samt udarbejdelse af tilsynskoncepter.
3. I 3.5.2 fastsættes det, at det vil være Digitaliserings- og Ligestillingsministeren, som bemyndiges til at fastsætte regler om, at offentlige myndigheder kan pålægges administrative bøder. Det bør fremgå af lovteksten frem for at blive overladt til den konkrete kompetente myndighed for den offentlige sektor, da dette kan skabe usikkerhed om, hvorvidt dette forhold så kan ændre sig hurtigt.
4. I afsnit 2.2.2 forudsættes det, at der vil være en tæt koordination mellem de kompetente myndigheder i forbindelse med tilrettelæggelsen af tilsynsarbejdet, således at der i videst muligt omfang anlægges en fælles tilgang, samt at dette særligt vil være relevant for tilsynet med enheder, der måtte indgå i flere forskellige sektorer, og hvor der potentielt er flere kompetente myndigheder, som skal føre tilsyn med samme enhed. Danske Universiteter finder det positivt, at lovudkastet lægger op til en fælles tilgang til tilsyn og en tæt koordinering mellem de forskellige sektoransvarlige myndigheder, men vil gerne opfordre til, at der nedsættes et organ til at sikre denne koordination, da det ikke bør overlades til de enkelte myndigheder at sikre koordinering med andre myndigheder i forbindelse med tilsyn af enheder, som indgår i flere forskellige sektorer. CFCS kunne med fordel have en tværgående rolle eller udarbejde vejledninger på området.
5. Center for Cybersikkerhed (CFCS) skal ifølge NIS2-lovudkastet varetage rollen som CSIRT. Af §§ 17-19 følger CSIRT'ens opgaver. Danske Universiteter opfordrer til, at CFCS' ansvarsområde og opgaver som CSIRT præciseres yderligere, end tilfældet er i det nuværende NIS2-lovudkast (inkl. bemærkningerne til § 17), herunder ikke mindst hvad angår snitfladerne til og samarbejdet med de private cybersikkerhedsaktører. Dette især set i lyset

af CFCS' hidtidige rolle, som har været mere vendt mod efterretningstjenesten og ikke mod organisationer, som fungerer i det åbne og med transparens. Yderligere medfører den nye rolle et markant øget anvendelsesområde sammenlignet med NIS1, og der bliver tale om en markant større overordnet opgave for en CSIRT, som sandsynligvis ikke kan løftes uden involvering af private aktører.

Specifikke bemærkninger

1. I 3.3.3 fastslås det at vedkommende ressortminister inden for sit område fastsætter nærmere regler om, hvornår en hændelse anses for at være væsentlig. Hvorfor inkluderes indikatorerne fra direktivets præambelbetragtning 101 ikke som udgangspunktet, når der skal fastsættes nærmere regler?
2. Der bør indarbejdes en definition på uddannede fagfolk i forhold til udførelsen af tilsyn, således at dette er ens på tværs af de forskellige sektorer.
3. Det fremgår af lovforslaget, at indberetninger af hændelser under § 14, er undtaget aktindsigt, mens indberetninger som følge af § 12 ikke er undtaget aktindsigten. Det bør overvejes, om der skal indskrives en begrænsning af aktindsigten på netop indberettede hændelser under § 12.
4. Lovforslagets § 7, stk. 2 adskiller sig betydeligt for formuleringen af krav til uddannelse af ledelse i forhold til direktivets artikel 20, stk. 2. Dette kan potentielt skabe udfordringer for virksomheder med samarbejdspartnere i andre EU lande, hvis implementeringen er for forskellig, og der derfor opstår usikkerhed om compliance med reglerne. Derfor opfordres Forsvarsministeriet til at justere teksten i § 7, stk. 2, således at den afspejler teksten i artikel 20, stk. 2.
    a. § 7, stk. 2. Medlemmerne af en væsentlig eller vigtig enheds ledelsesorgan skal deltage i relevante kurser om styring af cybersikkerhedsrisici og overveje at tilbyde tilsvarende kurser til sine ansatte.
    b. Artikel 20, stk. 2: ledelsesorganer er forpligtet til at følge kurser, og skal tilskynde væsentlige og vigtige enheder til løbende at tilbyde tilsvarende kurser til deres ansatte, således at de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, der leveres af enheden.
5. Der er uoverensstemmelse mellem artikel 32, stk. 4j og § 22 punkt 5, idet direktivet fastsætter, at den kompetente myndighed kan udpege en overvågningsansvarlig, men af § 22 fremgår det, at myndigheden kan påbyde enheden at udpege en person med ansvar for at føre tilsyn med enhedens overholdelse af §§ 6, 12-13 og 15-16. Uoverensstemmelsen består derfor konkret i om det er den kompetente myndighed eller enheden selv der udpeger en overvågningsansvarlig.
6. I § 6 er kun medtaget en del af direktivets artikel 21, stk. 1. Der mangler afsnittet om, at implementeringen af sikkerhedsforanstaltninger skal ske "Under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne skal de i første afsnit omhandlede foranstaltninger tilveje-

bringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning." Idet risikovurdering ud fra samfundets interesse er et grundlæggende princip i NIS2 Direktivet, bør dette være en del af lovteksten. Afsnittet er fortsat med i betragtningerne til § 6 nederst på side 229, men kan med fordel indarbejdes i selve lovteksten for at sikre en ensartet forståelse af reglerne.

Med venlig hilsen

Thomas Buchvald Vind
Direktør på Syddansk Universitet
Formand for Universitetsdirektørudvalget

AARHUS UNIVERSITET

Danske Universiteter

Høringssvar til udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Jura og Sekretariat

Steen Dahl Pedersen
Juridisk chef og souschef

Dato: 14. august 2024

Mobiltlf.: +45 2910 1661
E-mail: sdpedersen@au.dk
Web:
au.dk/sdpedersen@au.dk

Journal nr.: 2024-0731630
Afs. CVR-nr.: 31119103
Reference: SDP

Aarhus Universitet (AU) har fra Danske Universiteter modtaget ovennævnte udkast til forslag til lov til bemærkninger.

Det er vores vurdering, at sektoren via Danske Universiteter bør afgive et samlet høringssvar, hvilket også er det, der er lagt op til fra Forsvarsministeriet, som er afsender af høringsbrevet.

AU har noteret sig, at udkastet til lovforslag er en minimumsimplementering af NIS2-direktivet. Der er ikke i lovforslaget lagt op til andet og mere end bestemt i direktivet.

I forbindelse med udkastet til lovforslag vil AU indledningsvist bemærke, at der op til direktivets vedtagelse var usikkerhed om, hvorvidt universiteterne skulle være omfattet af direktivet. Den usikkerhed forsvandt, idet forskningsvirksomheder er omfattet efter direktivets bilag 2.

Af udkast til lovforslag § 3, punkt 11 fremgår, at en forskningsorganisation er en enhed, hvis primære mål er at udføre anvendt forskning eller udvikling med henblik på at udnytte resultaterne af denne forskning til kommercielle formål. Indbefatter ikke uddannelsesinstitutioner.

AU har samtidigt noteret sig, at Forsvarsministeriet i bemærkningerne på side 152 skriver, at det er ministeriets opfattelse, at hele enheden vil være at anse for omfattet af direktivets anvendelsesområde, også selv om enheden har flere forretningsområder eller er opdelt i flere administrative enheder, og det f.eks. alene er ét af disse forretningsområder, som er omfattet af de sektorer, der er omhandlet i direktivets bilag.

AU opfatter ikke sig selv som en enhed, hvis primære mål er at udføre anvendt forskning eller udvikling med henblik på at udnytte resultaterne af denne forskning til kommercielle formål. AU mener heller ikke at have fakulteter eller institutter, som er omfattet. Der kan være enkelte forskningsgrupper, som falder ind under definitionen.

Det vil, set fra AU's synspunkt være uhensigtsmæssigt, hvis hele AU bliver omfattet af anvendelsesområdet, fordi en forsvindende lille del af virksomheden falder ind under anvendelsesområdet. Der bør derfor indføres et minimumskrav for, hvor lille en del af virksomheden, som skal falde ind under definitionen før hele virksomheden (samme cvr.nr.) er omfattet.

Herudover har AU for DeIc hosting af en supercomputer (HPC) GenomeDK. Betyder det at AU (hele virksomheden under AU's cvr.nr.) falder ind under NIS2 som operatør af digital infrastruktur jf. bilag 1 punkt 8?

På AU drives jf. bekendtgørelse nr. 1764 af 2018 et retsmedicinsk institut under AU's sundhedsvidenskabelige fakultet Health. Instituttets virksomhed i forbindelse med myndighedsbetjening er fastlagt ved bekendtgørelsens § 2 stk. 1 i relation til retsvæsnet og i stk. 3 i relation til sundhedsloven. AU kan være i tvivl om Institut for Retsmedicin er omfattet af offentlig forvaltning jf. bilag 1 punkt 10. Også om hele AU så, som en følge af forsvarsministeriets opfattelse bliver omfattet.

AU finder på baggrund af det ovenstående, at det er det væsentligt at få defineret, om universitetssektoren enten samlet eller delvist er omfattet af NIS2 som forskningsorganisationer eller i andre egenskaber. Det er også vigtigt at få afklaret, om ministeriets opfattelse af, hvad der skal til for at hele virksomheden (under samme cvr) er omfattet er endelig.

AU ønsker, at der fastsættes en mere snæver definition af genstandsfeltet for Nis2, således, at det alene er den af universiteterne drevne samfundsvigtige forskning infrastruktur og forskning, som er omfattet af NIS2 på universiteterne. Universiteternes øvrige dele bør falde uden for genstandsfeltet. Altså, at det ikke er hele universitetet som falder under NIS2, hvis det blot er en beskeden del som bør være omfattet.

Derudover vil AU pege på, at hvis AU eller andre universiteter helt eller delvist er omfattet som væsentlig virksomhed, kan der være tvivl om, hvem der er adressat for de sanktioner, som er omfattet af § 23 stk. 1, og herunder særligt 2. pkt. hvor det kan forbydes enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos enheden at udøve ledelsesfunktioner i den pågældende enhed. Universitetssektoren er ikke organiseret som de virksomheder der ellers er omfattet af udkastet til lovforslag.

Det synes ikke rimeligt, at der kan være tvivl om, hvem der kan rammes af den alvorlige sanktion, som et forbud mod at udøve ledelsesfunktioner udgør.

AARHUS UNIVERSITET

Venlig hilsen

Steen Dahl Pedersen
Juridisk chef

Kopi til:

[Navn]

Forsvarsministeriet
E-mail: fmn@fmn.dk
cc. nmc@fmn.dk, nls@fmn.dk
J./sags nr. 2020/004886

Dato: 19. august 2024

Høringssvar: Udkast til lov om ændring af lov om net- og informationssikkerhed

Generelle bemærkninger

Danske Vandværker er tilfredse med, at NIS 2-direktivet nu implementeres i Danmark. Vi havde gerne set, at hele implementeringen med de tilhørende bekendtgørelser var sket helt synkront med implementeringen af CER-direktivet. Dette ville være en fordel i forhold til optimering af vores medlemmers ressourceforbrug, samt give en bedre forståelse af, om de er en kritisk enhed.

Forslag til implementering - "trappemodel"

Ved implementeringen mener vi, at der skal være proportionalitet imellem risiko og effekt på den ene side, og vandforsyningernes størrelse og administrative ressourcer på den anden. Vi er opmærksomme på, at der er behov for et bredt beredskab, men vi finder at grænsen for at være omfattet af NIS 2, som er foreslået i Niras´-konsulentrapport (udpumpet vandmængde årligt på 200.000 m3) er for lav i forhold til den nødvendige proportionalitet. Vandforsyninger med en så lav udpumpet vandmængde har hverken en organisation, eller administrative ressourcer, til at kunne leve fuldt op til compliance kravene i NIS 2.

Vi vil derfor foreslå en alternativ model, som sikrer, at der stadig stilles krav til et bredt beredskab og en bred modstandsdygtighed, også hos de mindre vandforsyninger. Dette kan ske ved at skyde et ekstra niveau ind og etablere en "trappemodel", for eksempel som denne(der lægger sig op af den model Energistyrelsen arbejder med):

Niveau	Type af vandværk	Øvrige krav	NIS2 og CER direktiverne
2	> 10.000 forbrugssteder		Omfattes af NIS2 og CER direktiver
1	750 – 9.999 forbrugssteder	Krav om net og informationssikkerheds-; Risikoanalyse Kortlægning af net- og informationssystemer Beredskabsplan Hændelsesrapportering Awarenesstræning	Omfattes ikke*
0	< 749 forbrugssteder	Krav om beredskabsplan der også omhandler net og informationssystemer.	Omfattes ikke*

*Forsyner et selskab anden kritisk infrastruktur, er man, uanset øvrige kriterier, omfattet af NIS2 og CER.Den beskrevne "trappemodel" vil efter vores opfattelse øge fokus bredt på cyber- og informationssikkerhed og beredskab betragteligt. Danske Vandværker har allerede arbejdet aktivt med at få cyber- og informationssikkerhed medtaget i vandforsyningernes beredskabsplaner. Den beskrevne "trappemodel" er således udtryk for, at vi mener, alle vandforsyninger skal have øget fokus på cyber- og informationssikkerhed. Dette skal ske på en måde, hvor der er en tilstrækkelig organisation, og tilstrækkelige ressourcer til, at det er realistisk at få en effektiv implementering.

Ensartethed og højt fagligt niveau af tilsyn

For Danske Vandværker er det afgørende at sikre både ensartethed og koordinering i implementeringen, og et højt fagligt niveau i det fremtidige tilsyn. Der bør derfor kun være ét samlet tilsyn for sektoren.

Danske Vandværker I Solrød Center 20 C I 2680 Solrød Strand
Tlf.: 56 14 42 42 I info@danskevv.dk I www.danskevv.dk I CVR: 9513 9655

Opgaverne bør fordeles ud fra en nærmere analyse af, hvor det er mest hensigtsmæssigt at placere dem, men vi har ikke specifikke krav/ønsker til dette, så længe kravene om ensartethed, koordinering og faglighed i tilsyn opfyldes. Vi kan dog henvise til det arbejde der allerede er udført i samarbejde med Miljøstyrelsen med hensyn til ansvarsfordeling mv. (vedhæftet bilag 1).

Behovet for ensartethed, koordinering og samlet tilsyn understreges af, at der i mange tilfælde er tale om multiforsyninger, der dækker flere forskellige forsyningsgrene.

Det er væsentligt, at et kommende tilsyn er dialogbaseret og værdiskabende. For vandforsyningerne er der tale om en ny opgave, som der kun er begrænset erfaring med. Derfor vil der være behov for, at tilsynet også kan rådgive forsyningerne, og ikke fokuserer for meget på kun at finde fejl og mangler i implementeringen.

Gebyrer, sikkerhedsgodkendelse og sikkerhedstjenester – omkostninger bør minimeres
Det er for os væsentligt, at de tilsyn som udføres, skal være proportionale i både omfang og hyppighed i forhold til vandforsyningernes størrelse (risiko og effekt). Der bør ikke pålægges forsyningerne urimeligt store gebyrer, især ikke for mindre forsyninger med en begrænset økonomisk formåen.

Heller ikke sikkerhedsgodkendelser bør medføre urimelige administrative og økonomiske belastninger. Sikkerhedsgodkendelser bør kunne ske på en nem og praktisk måde.

Vandforsyningernes tilkøb og brug af sikkerhedstjenester anses for at være formålstjenesteligt og det støtter vi op om. Det må dog være op til den enkelte vandforsyning selv at afgrænse deres behov, samt at vælge den sikkerhedstjeneste, der samlet set bedst imødekommer vandforsyningens behov både administrativt og økonomisk.

For eksempel giver et medlemskab hos SektorCERT mening for nogle af de store vandforsyninger, hvor det ikke vil være proportionalt for en mindre forbrugerejet vandforsyning.

Datasikkerhed
I forbindelse med indrapportering og tilsyn er det for os væsentligt, at der sikres den nødvendige sikkerhed, så sikkerheden ikke kan kompromitteres.

Specifikke bemærkninger
Suspensioner
På nogle vandforsyninger er der kun 1 (eller ingen) ansatte. En suspension vil således betyde, at der ikke vil være nogen til at løse opgaven. Dette understreger behovet for en højere grænse for fuld implementering, og en "trappemodel".

Venlig hilsen

Susan Münster

Direktør
Danske Vandværker

DanskeRederier FærgeRederierne

Forsvarsministeriet
Holmens Kanal 9
1060 København K

(Sendt elektronisk til fmn@fmn.dk og i kopi til jhb@fmn.dk)

Høringssvar vedr. forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau – Sagsnummer 2024/004461

22. august 2024

Sagsnummer:
EMN-2022-00585

Danske Rederier kvitterer hermed for modtagelsen af høringsbrev af 5. juli 2024 om udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, sagsnummer 2024/004461. Da medlemskredsen af Færgerederierne også har en interesse i lovforslaget fremsendes i fællesskab mellem Danske Rederier og Færgerederierne nedenstående kommentarer til lovforslaget.

Indledningsvis finder Danske Rederier og Færgerederierne det positivt, at der med NIS 2-direktivet (Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148)) søges skabt et højere og mere ensartet cybersikkerhedsniveau på tværs af EU-medlemsstaterne, samt at der med hovedloven skabes en fælles lovgivningsramme for at sikre en vis ensartethed og koordinering på tværs af de forskellige sektorer, som efterfølgende skal udmøntes i sektorspecifikke bekendtgørelse, der kan tage hensyn til sektorernes forskelligheder. Lovgivning om foranstaltninger til sikring af et højt cybersikkerhedsniveau kan have stor betydning i disse tider med ændrede trusselsbilleder. Vi havde dog gerne set, at denne høring havde været udsendt samtidig med høring om udkast til lovforslag om styrket beredskab i energisektoren inden for Klima-, Energi- og Forsyningsministeriets område.

Vi finder det også positivt, at der ved Center for Cybersikkerhed sikres en tværgående rolle til at facilitere tæt samarbejde mellem de forskellige sektoransvarlige myndigheder. Ligeledes er det positivt, at der lægges

op til, at der med lovforslaget sker en minimums- og tekstnær implementering af direktivet, samt at tilhørende bekendtgørelser også holder sig inden for rammerne af en minimumsimplementering af direktivet.

Endelig noterer vi os med tilfredshed, at jf. § 1, stk. 3 kan ressortministeren beslutte at der gælder lex specialis, såfremt anden i Danmark gældende EU-lovgivning har mindst samme virkning.

I det følgende anføres en række specifikke bemærkninger kategoriseret under emner.

Anvendelsesområdet

Det anføres på bemærkningernes side 152, at "det er Forsvarsministeriets opfattelse at hele enheden anses omfattet af direktivets anvendelsesområde, også selv om enheden har flere forretningsområder eller er opdelt i flere administrative enheder, og det eksempelvis alene er ét af disse forretningsområder, som er omfattet af de sektorer, der er omhandlet i direktivets bilag."

Ovenstående giver anledning til behov for en nærmere afklaring af, hvilken betydning denne tilgang vil have for, at en enhed bliver udpeget som omfattet af reguleringen i relation til kriterierne for mellemstore og store virksomheder (antal beskæftigede og finansielle tærskler)? Kan der gås ud fra, at det udelukkende er det forretningsområde, som er omfattet af direktivets bilag, hvor antal beskæftigede og finansielle tærskler skal tages i betragtning?

Ad. § 5

Det anføres i § 5, stk. 1: "Enheder, der ikke opfylder kriterierne for at være væsentlige enheder i medfør af § 4, stk. 1-3, anses for at være vigtige enheder."

Denne formulering kan godt misforstås, da man skal huske den indledende afgræsning som fremgår af § 1, stk. 1 som henviser til direktivets artikel 2, hvor der i stk. 1 sker en afgrænsning, således at direktivet som

udgangspunkt kun gælder for mellemstore og store virksomheder. Det kan måske med fordel skrives lidt tydeligere, at der gælder nogle krav til antal beskæftigede og finansielle tærskler før en enhed er omfattet, evt. ved også at inkludere en henvisning til § 1, stk. 1. Det vil tydeliggøre. at små enheder som udgangspunkt ikke er omfattet af lovgivningen. Det er dog noteret, at forholdet beskrives i bemærkningerne til § 1 nederst side 194.

Forsyningskædesikkerhed

Som del af bemærkningerne til § 6, stk. 1, fremgår det på side 229, at en af de foranstaltninger, som væsentlige og vigtige enheder skal træffe for at styre risiciene for sikkerheden i net- og informationssystemer, er at tage højde for "forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere."

I den forbindelse noteres det desuden, at der på side 232 står, "ved at bekendtgørelserne udstedes af de relevante ressortministre inden for deres områder, vil reglerne kunne målrettes de enkelte sektorer. Reglerne vil dermed i relevant omfang kunne tilpasses de enkelte sektorers specifikke forhold, ligesom der i overensstemmelse med direktivets forudsætninger ud fra en risikobaseret tilgang vil kunne fastsættes differentierede regler…", og på side 233 står der "Center for Cybersikkerhed vil endvidere have til opgave at påse, at der ikke fastsættes regler, som er indbyrdes modstridende på tværs af sektorerne". Det er betragtninger vi finder meget positive og relevante.

Efter Danske Rederier og Færgerederiernes opfattelse rejser § 6, stk. 1, nummer 4 dog spørgsmålet om, hvilke krav der kan stilles til en underleverandør, både fra myndighedernes og den væsentlige / vigtige enheds side? Umiddelbart ser vi en risiko for en potentiel udbredelse af lovforslagets rammer, da det bør bemærkes, at en leverandør kan komme fra en anden sektor, hvor der måske stilles andre lovmæssige krav end for den omfattede væsentlige / vigtige enhed. Yderligere er det værd at være opmærksom på, at der kan være kommercielle forhold, som kan begrænse hvad en væsentlig / vigtig enhed med rimelighed kan kræve at

kontrollere hos sin leverandør. Der bør, af hensyn til leverandører som indgår i forsyningskæden, være klarhed over omfanget af krav, der inden for rimelighedens grænser kan stilles dem. Desuden bør det præciseres, hvilke regler og krav der gælder for underleverandører, som kommer fra en anden sektor, uden at lovgivningen kommer i strid med sektoransvarsprincippet.

Ad. § 7

Danske Rederier og Færgerederierne noterer os, at der for væsentlige og vigtige enheder er et ledelsesmæssigt ansvar for overholdelse af § 6, stk. 1-3, og at der i den forbindelse stilles uddannelsesmæssige krav til ledelsesorganet. Umiddelbart fremgår det ikke nærmere defineret, hvad der forstås ved ledelsesorganet, om det udelukkende er enhedens direktion, eller om det også omfatter en evt. bestyrelse?

Tilsyn

Danske Rederier og Færgerederierne støtter forslaget om, at det er de kompetente myndigheder inden for deres respektive områder, som fører tilsyn med væsentlige og vigtige enheders efterlevelse af loven og de regler, der udstedes i medfør af loven. Men det giver anledning til følgende spørgsmål:

Hvilken betydning har det i forhold til en enhed, som måske ikke er udpeget som væsentlig eller vigtig, men indgår som underleverandør til en sådan, og vil der så igen være forskel på, om det er en væsentlig eller vigtig enhed?

Vil en underleverandør også kunne pålægges krav og tilsyn, hvis denne kommer fra en anden sektor, og i så fald af hvem?

Hvis der stilles krav til en underleverandør, vil denne så have samme mulighed som væsentlige og vigtige enheder til at trække på ressourcerne fra CSIRT'en?

Ikrafttrædelse

I § 33 anføres den 1. marts 2025 som ikrafttrædelsesdatoen. Danske Rederier og Færgerederierne noterer os, at det i bemærkningernes side 183 anføres at "Europa-Kommissionens konsekvensvurdering fra december 2020 angiver, at en gennemsnitlig virksomhed skal bruge 22-25% af sine nuværende omkostninger til it-sikkerhed på at omstille sig til kravene i NIS 2-direktivet. Tallet er 12-15% for virksomheder, der allerede er omfattet af NIS 1-direktivet. Europa-Kommissionens konsekvensvurdering indeholder ikke en kvantificering af de løbende omkostninger." Samtidig med at Forsvarsministeriets indledende estimat viser, at omkring 2.000 danske virksomheder kan blive omfattet, i forhold til de ca. 150 danske virksomheder, som i dag er omfattet af NIS 1-direktivet og derved efterlever en del af de krav, der følger af NIS 2-direktivet. Desuden noteres det, at begge tal er omfattet af en vis usikkerhed. I tillæg til dette, er det anført, at lovforslaget vil blive fulgt op af nærmere regler fastsat på bekendtgørelsesniveau.

Derfor er det Danske Rederier og Færgerederiernes opfattelse, at der af budget-, planlægnings- og investeringsmæssige hensyn, ikke mindst for de virksomheder, der ikke tidligere har været omfattet af NIS 1-direktivet, bør være en rimelig og realistisk implementeringsfase. Umiddelbart fremgår der ikke noget om overvejelser i den retning i bemærkningerne til lovforslaget.

Danske Rederier og Færgerederierne ser frem til den videre dialog med relevante sektoransvarlige myndigheder om udformningen af nærmere regler og lovgivning i forlængelse af implementeringen af NIS 2-direktivet ved dette lovforslag.

Med venlig hilsen

Morten Glamsø
Sikringschef
mgl@danishshipping.dk

Forsvarsministeriet
Sagsnummer 2024/004461

fmn@fmn.dk
jhb@fmn.dk

DATO: 22. august 2024
PROJEKTNR.: 3012
pm/hka

Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Dansk Vand- og Spildevandsforening, DANVA, takker for muligheden for at afgive høringssvar vedr. udkast til Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

DANVAs medlemmer er drikkevands- og spildevandsselskaber, som står for drift af kritisk infrastruktur i vandsektoren. En meget stor del af DANVAs medlemmer vil blive omfattet af loven – og Lov om kritiske enheders modstandsdygtighed.

CFCS har løbende hævet trusselsvurderingen for Danmark. Det samme har SektorCERT, som er CERT indenfor kritisk infrastruktur. SektorCERT har et sensornetværk med sensorer placeret i over 300 forsyningsselskaber indenfor drikkevand, spildevand og energi. Sensornetværket er med til at forhindre cyberangreb og giver et indblik i et – desværre – stigende antal cyberangrebsforsøg og -trusler.

En række danske drikkevands- og spildevandsforsyninger er blevet ramt af cyberangreb – som har haft store konsekvenser. Disse hændelser og trusselssituationen har kaldt på ekstra opmærksomhed, cybersikkerheds- og beredskabsaktiviteter hos DANVAs medlemmer indenfor de senere år.

DANVA hilser derfor loven velkommen og vil arbejde for at implementeringen kan være med til at sikre en fortsat høj forsyningssikkerhed og levering af tjenesteydelser - under hensyntagen til cybertruslerne.

Lov om kritiske enheders modstandsdygtighed og Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau hænger tæt sammen. Derfor vil dette høringssvar i nogen grad gengive kommentarer fra DANVAs høringssvar vedr. Lov om kritiske enheders modstandsdygtighed. Hertil kommer, at en række vandselskaber også bliver omfattet af energisektorens regulering, idet flere af selskaberne er multiforsyningsselskaber med energivirksomhed. DANVA plæderer for en reel sammentænkning på nationalt niveau af Lov om styrket beredskab i energisektoren, Lov om kritiske enheders modstandsdygtighed og Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

Herunder har DANVA nogle generelle bemærkninger og derefter nogle bemærkninger til de enkelte paragraffer.

Generelle bemærkninger

Vi har bemærket, at loven er en **meget** overordnet rammelov, hvor sektorernes myndigheder får stor indflydelse på den praktiske udmøntning i sektorerne.

De sektorspecifikke bekendtgørelser, administrative bestemmelser mv. og praktisk udmøntning vil kunne afstedkomme, at forsyningssektorerne får forskellige, måske meget forskellige, implementeringer af de to love, hvis der ikke er en effektiv koordinering.

Loven er en rammelov – og det er vigtigt, at udmøntningen i sektorspecifikke bekendtgørelser, vejledninger mv. giver lovgivningsmæssige passende krav for de omfattede selskaber, som fremmer cybersikkerheden, og at indsatsen giver høj værdi i forhold til de økonomiske og administrative omkostninger, loven vil afstedkomme for selskaberne. Det er vigtigt at sikre, at implementeringen bliver smidig, passende, og at omfattede enheder, såvel som sektormyndighederne, får gode rammer og vilkår. Dialog i processen er afgørende.

DANVA er bekymret over, at lovudkastet ikke samtænker forsyningsarterne drikkevand og spildevand med øvrige forsyningsarter som regelsættes i "Forslag til Lov om styrket beredskab i energisektoren", der netop har været i høring i perioden fra 12. juni til 10. juli 2024. Drikkevand og spildevand har en lang række fællesnævnere og indbyrdes afhængigheder med de øvrige forsyningsarter, som ikke håndteres i de to udkast til lovforslag fra henholdsvis Energistyrelsen og Forsvarsministeriet.

Vi vurderer ikke, at en almindelig, overordnet koordinering på nationalt niveau er tilstrækkelig. DANVA efterlyser en reel samtænkning på nationalt niveau. En samlet lovgivningspakke indeholdende Lov om styrket beredskab i energisektoren, Lov om kritiske enheders modstandsdygtighed og Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau vil kunne fremme dette.

Opsummering af hovedbudskaber

- Forsyningsarternes gensidige afhængighed og eksistensen af multiforsyninger kalder på samtænkning – og ikke blot en overordnet koordinering på nationalt niveau.

- Der skal være én myndighed, som er ansvarlig for at samtænke alle forsyningsarter, uanset om vi taler om national strategi, udpegning af kritiske enheder, baggrundskontrol, tilsyn m.m. Alternativt skal der være én myndighed, som har ansvaret for at sikre en omfattende koordinering.

- Det er uhensigtsmæssigt, at vand- og spildevandsforsyninger ikke har samme sektormyndighed som de øvrige forsyningsarter. DANVA har således bekymring for, om der vil være midler til at opkvalificere Miljøstyrelsen, så styrelsen har den nødvendige kompetence til at udfylde opgaven som myndighed der dels er sammenlignelig med kompetencen i Energistyrelsen, dels afspejler behovet på vand- og spildevandsområdet.

- DANVA støtter, at der er fokus på at undgå dobbeltarbejde, herunder at det skal være muligt at anvende bl.a. risikovurderinger udført med afsæt i såvel andre EU-retsakter som national lovgivning. Det bør dog også i lovbemærkningerne angives, at det også omfatter arbejde grundet frivilligt standardiseringsarbejde, der ofte indeholder beredskabsrelaterede elementer.

- Det anbefales, at der i lovbemærkninger understreges, at medlemslandene har en forpligtigelse til at støtte de kritiske enheder, væsentlige og vigtige enheder med at styrke deres cybersikkerhed og modstandsdygtighed.

- Det er bydende nødvendigt, at der i lovbemærkninger er angivet, at sektormyndighed, andre relevante myndigheder samt økonomiske regulatorer er forpligtiget til aktivt at understøtte virkeliggørelsen af beredskabs- og cybersikkerhedsaktiviteterne. Deri skal også være en accept af, at enheder, af forskellige omstændigheder, gør mere end absolut minimum.

- Implementeringen af direktivet er et pionerarbejde, som fordrer en evaluering af reguleringen inden for rimelig kort tid; 2-3 år.

Uddybning

National strategi på tværs af sektorer (forsyningsarter)

DANVA opfordrer til, at lovbemærkningerne omtaler, at der i den nationale strategi og risikovurdering skal ske en omtale af de forskellige forsyningsarters gensidige afhængighed.

Placering af energisektoren og forsyningerne for vand og spildevand i to forskellige hovedlove finder vi, som nævnt, uheldigt:

1. Sektoren for drikkevand og spildevandssektoren er særdeles afhængig af leverancer fra energisektoren, hvorfor koordinering er afgørende.
2. Flere af DANVAs medlemmer er multiforsyninger. For disse er det afgørende, at der sker en prioritering af koordineringen mellem de relevante sektorer/ministerier, hvilket en national strategi vil kunne bidrage til.
3. Det forventes, at spildevandsektoren i den nære fremtid får en afgørende betydning for PtX, som også vil kunne bidrage med energiforsyning.

Desuden er der tekniske muligheder, som peger i retning af øget samspil mellem fjernvarme- og spildevandsforsyning samt drikkevandsforsyning og kølingsformål.

Sektoransvar

De danske forsyningsarter har ikke samme sektormyndighed, når emnet er cybersikkerhed og beredskab. Dette afspejler efter vores vurdering ikke virkelighedens behov. Der er multiforsyninger, som organiserer flere forskellige forsyningsarter, hvor hver forsyningsart vil være omfattet af dels NIS2, dels CER-direktivet.

Koncerner med flere forskellige forsyningsarter bliver reelt omfattet af forskellige reguleringer, der desuden er udformet af flere ministerier, og som tilmed forventes at have forskellig tilgang til implementeringen (overimplementering contra minimumsimplementering).

Det er afgørende, at der, i tilblivelsen af lovgivningen, sker en prioritering af koordineringen mellem de relevante ministerier, og at der dermed sikres en sammenlignelighed i bl.a. termer, krav, tilsyn og håndhævelse. Det bør være et klart mål, at multiforsyningerne ikke oplever uhensigtsmæssig administration eller ekstra omkostninger grundet det fragmenterede sektoransvar.

At de faktiske rammevilkår for forsyningsarterne er sammenlignelige, kommer bl.a. til udtryk i, at der er et tæt samarbejde i regi af SektorCERT, der er en foreningsaktivitet, der er afgørende for skabelsen af den nødvendige it-sikkerhed for kritisk infrastruktur i Danmark. Det vil, som ovenstående eksempler illustrerer, være hensigtsmæssigt at samordne forsyningsarterne under samme sektormyndighed. Alternativt bør regelsættene for forsyningsarterne samtænkes.

Da hver sektor ifølge sektoransvaret er ansvarlig for egen modstandsdygtighed, bør der ved kritiske hændelser sikres agilitet via entydig kommandovej fra den pågældende minister til sektorens kritiske enheder og vice versa. Eksempelvis vil nogle erfaringer fra andre sektorer være væsentlig at få distribueret til andre sektorer hurtigt, hvilket ligeledes stiller krav til agilitet i Beredskabsstyrelsens (og Energistyrelsens) koordinering.

Desuden bør det sikres, at kriterierne for iværksættelse af cybersikkerheds- og beredskabsforanstaltninger i relation til kommende beredskabsniveauer er klare, entydige og kommunikeret til enhederne.

Støtte til Miljøministeriet - Sektorbekendtgørelsen for drikkevand og spildevand

DANVA forventer, at Forsvarsministeriet som den tværgående koordinerende myndighed støtter op om Miljøministeriet, så forpligtigelserne tilknyttet sektoransvaret og den fragmenterede organisering kan løftes. Siden udskillelsen af de kommunale vand- og spildevandsselskaber i 2010 har DANVA kunnet notere, at ministeriet kun i begrænset omfang har taget aktion med henblik på at planlægge opretholdelse og videreførelse af samfundets funktioner i tilfælde af større ulykker og katastrofer, hvilket kræves jf. beredskabslovens § 24.

DANVA opfordrer til, at der i lovbemærkningerne angives eksplicit, at Danmark som medlemsland er forpligtiget til at sikre tilstrækkelige midler til, at de kompetente myndigheder kan løfte deres opgaver – herunder lovgivningsarbejdet.

DANVA foreslår, at der i lovbemærkningerne utvetydigt angives, at de respektive kompetente myndigheder snarest muligt påbegynder en dialog om kriterier og de potentielle kritiske enheder.

Udpegning af kritiske enheder, væsentlige og vigtige enheder

Der er tale om en stor og meget kompleks opgave, som har betydning for om samfundskritiske sektorer kan opretholde levering af tjenesteydelser i krisesituationer.
Kritiske enheder bør udpeges af en central myndighed for at sikre ensartethed i udpegningen. Som lovudkastet ligger nu, vil det være Miljøministeriet/Miljøstyrelsen som varetager udpegningen indenfor forsyningsarterne drikkevand og spildevand.
Der lægges i udkastet stor vægt på, at der er tale om en minimumsimplementering af NIS2-direktivet. Det er vigtigt, at dette fokus ikke står i vejen for, at loven bliver operationel og smidig. Forstået således, at der ikke skal udføres dobbeltarbejde i form af produktion og vedligeholdelse af dokumentation, rapportering af de samme informationer til flere myndigheder eller andre aktiviteter, hvor der allerede eksisterer velfungerende processer/rutiner for de pågældende aktiviteter. Konkrete eksempler på dette er risikoanalyser, dokumentation og audits som gennemføres i forbindelse med drift af eksisterende certificerede ledelsessystemer.

Støtte til de udpegede kritiske enheder, væsentlige og vigtige enheder

I DANVA har vi noteret os, at lovbemærkningerne meget kort omtaler medlemslandenes forpligtigelser til at støtte de kritiske enheder med at styrke deres modstandsdygtighed. Se CER-direktivets artikel 10 samt artikel 4 stk. 2 litra e. Vi vil opfordre til, at det også nævnes eksplicit i lovbemærkninger, at medlemsstaterne kan stille finansielle ressourcer til rådighed for kritiske enheder, hvor det er nødvendigt og begrundet i mål af samfundsmæssig interesse.

DANVA forventer, at der ydes støtte til de udpegede kritiske enheder, hvilket skyldes drikke- og spildevandsforsyningens centrale placering i samfundet. Vores forventninger understøttes af udmeldingen af støtteeksempler i artiklen, herunder omtale af finansieringsmulighederne.

Såvel drikkevands- som spildevandsforsyning er baseret på et hvile-i-sig-selv-princip. Dertil kommer at de juridiske enheder er små sammenholdt med enheder i mange andre sektorer med henvisning til listen i EU-forordning 2023/2450 over væsentlige tjenester.

Tilsyn

DANVA efterlyser, at der i lovbemærkningerne angives, at den opfølgende lovgivning skal fremme et dialogbaseret fysisk beredskab, cybersikkerhedsberedskab og tilsyn. Det vil være et vigtigt signal, som vil fremme et hurtigere løft af cybersikkerheds- og beredskabskompetencen hos både myndigheder og selskaberne.

DANVA foreslår, at én central myndighed varetager tilsynet. Herved sikres ensartethed i kvantitet og kvalitet af tilsynet. Der skal i den forbindelse tænkes på tværs af forsyningsarter for ikke at pålægge multiforsyninger unødig administrativ byrde.

Økonomiske konsekvenser

Det skal sikres, at drikkevands- og spildevandsforsyningernes opgaver ifølge dette regelsæt kan håndteres efter de økonomiske regler, givet i vandsektorloven, vandforsyningsloven og betalingsloven. Derudover er det vigtigt for drikkevands- og spildevandsforsyningerne, at omkostningerne afholdt til at opfylde lovens bestemmelser bliver betragtet som en ikke-påvirkelig omkostning, hvilket betyder, at omkostningerne bliver fritaget for effektiviseringskrav. Selskabernes omkostninger til SektorCERT-samarbejdet i den kritiske infrastruktur skal i den sammenhæng ses som en omkostning til at opfylde loven. SektorCert bidrager til NIS2-compliance, øget cybersikkerhed og derudover er SektorCERT en integreret del af Strategi for cyber- og informationssikkerhed i vandsektoren, som er en delstrategi under Den nationale strategi for cyber- og informationssikkerhed. Alternativt vil forsyningernes mulighed for fremadrettet at finansiere de nødvendige tiltag efter lovens bestemmelser være markant svækket.

Som led i udarbejdelsen af sektorbekendtgørelsen efterlyser DANVA, at der foretages en grundig analyse af de økonomiske omkostninger, der følger af implementeringen af NIS2 og CER-direktivet.

Omdrejningspunktet må være, at der skal være proportionalitet mellem omkostningsniveau og merværdi for den konkrete enhed og dens rolle i samfundet. Desuden bør reguleringen, bredt set og i praksis, understøtte, at der er vandforsyninger og/eller spildevandsforsyninger, som vælger at følge de mere vidtgående cybersikkerheds- og beredskabsrelaterede regler kendt fra energisektoren. Dette bør fremgå af såvel lovbemærkninger og den kommende sektorbekendtgørelse.

Lokal cybersikkerheds- og beredskabskoordinering øger sikkerheden og samfundets robusthed

DANVA vil opfordre til at benytte implementeringen af de to beredskabsdirektiver til at fremme lokal cybersikkerheds- og beredskabskoordinering, hvor omdrejningspunktet er den lokale kompetente beredskabsmyndighed/kommunalbestyrelsen, herunder den lokale beredskabsstab (LBS) eller politiet og repræsentanter for de udpegede kritiske enheder, væsentlige og vigtige enheder.

Evaluering

Implementering af NIS2- og CER-direktivet er et pionerarbejde, som fordrer, at der er en politisk vilje til at sikre evaluering af reguleringen inden for rimelig kort tid; 2-3 år. Der kan utvivlsomt ske en optimering af organisering m.m., og dette vil være synligt og mærkbart i praktikken forholdsvist hurtigt. Nogle optimeringstiltag vil kunne ske via ændring af bekendtgørelser, men der vil også være emner, som er lovbaserede og derfor kræver Folketingets involvering.

Bemærkninger til lovens paragrafer

§ 4 og § 6

Lov om kritiske enheders modstandsdygtighed (CERD-loven) afstedkommer en række krav til selskaberne. Der er en klar kobling mellem de to love – fx bliver enheder, der er identificeret som kritiske enheder i henhold til lov om kritiske enheders modstandsdygtighed anset som væsentlige enheder. Denne kobling (Hvor en kritisk enhed i CERD-loven ses som en væsentlig enhed i NIS2-loven) giver umiddelbart god mening. I den sammenhæng er det vigtigt at sikre, at udmøntninger af beredskabslovene bliver koordineret – så udmøntningen på 'beredskabsområdet', samlet set, gøres operationel, brugbar, ikke-bureaukratisk, og at enhederne får klarhed over hvilke krav, der stilles til dem – uanset om enheden er en multiforsyningsvirksomhed.

Sektoransvarsprincippet betyder, at hvert ministerområde har ansvaret for egen sektor, fx. ift. beredskab og cybersikkerhed. Erfaringerne fra implementeringen af NIS1-direktivet fra 2018 viser, at der kunne have været en bedre koordinering mellem ressortministerierne. Fx fungerer tilsynet forskelligt på tværs af de omfattede sektorer, og mængden af ressourcer, myndighederne har til opgaverne, varierer meget. Når NIS2 skal implementeres i dansk lovgivning, opfordrer vi til, at der sker koordination mellem ressortområderne, så tiltag er sammenlignelige, afspejler sammenhængen mellem sektorerne og kan rapporteres på en fælles form.

§ 6

I § 6 gengives NIS2-diretivets (artikel 21) overordnede krav i punktform. For hvert nævnt overordnede krav bør der være operationelle, veldefinerede underliggende, ensartede fælles krav for forsyningssektorerne.

Hvis det ikke defineres klart, gældende for alle forsyningssektorer (hvoraf en del har flere forsyningsarter) vil det kunne afstedkomme misforståelser, når myndighederne på et tidspunkt begynder at gennemføre tilsyn. Som eksempel kan nævnes, at der bør være ensartethed på tværs af sektorerne mht. adressering af forsyningskædesikkerhed.

Sektorspecifikke bekendtgørelser, vejledninger, guidelines, skabeloner mv. kan der i nogen grad samarbejdes om. DANVA er klar over, at nogle sektorer er meget forskellige og i nogen grad har særlige forhold og behov, men en række forhold/vilkår og behov er bredt gældende for enhederne, som er omfattet af loven. Det bør fremgå tydeligligt, at der skal samarbejdes og videndeles mellem sektorerne.

§ 7

I henhold til paragraffen skal foranstaltninger, som en væsentlig eller vigtig enhed træffer på baggrund af forpligtelserne i § 6, være godkendt af enhedens ledelsesorgan, og ledelsesorganet skal føre tilsyn med foranstaltningernes gennemførelse og sikre, at foranstaltningerne virker.

Begrebet 'enhedens ledelsesorgan' er ikke klart defineret, og det er uklart hvilken rolle fx bestyrelserne har i forbindelse med godkendelsen af foranstaltningerne og tilsynet.

Det fremgår også af paragraffen, at medlemmerne af en væsentlig eller vigtig enheds ledelsesorgan skal deltage i relevante kurser om styring af cybersikkerhedsrisici. Det er her igen uklart, hvad der menes. Menes der fx, at alle bestyrelsesmedlemmer og ledere skal have gennemført en uddannelse (med et særligt indhold), og at medlemmerne løbende skal uddannes? Uddannelseskravet bør beskrives nærmere.

§ 12

Der er ikke i § 12, som det er i § 14 stk. 3 vedr. frivillige underretninger, beskrevet, at underretningerne er fritaget for aktindsigt. Det konkrete indhold i en underretning vil oftest være at betragte som fortroligt for enheden, idet det indeholder informationer om sårbarheder i enheden. Ved at beskytte den konkrete underretning mod aktindsigt, vil enheden sandsynligvis være mere tilbøjelig til at dele informationer, som ikke nødvendigvis er påkrævet men som kan have stor værdi for CSIRT'en (CFCS).
Det er i forvejen en mulighed for kompetente myndigheder, bl.a. i § 16 & § 22 stk. 6, at vurdere om en konkret hændelse skal deles videre eller offentliggøres.

Beskrivelsen af hvornår en hændelse anses for væsentlig bør i højere grad referere til, om hændelsen forårsager, eller er i stand til at forårsage, alvorlige driftsforstyrrelser i relation til den tjeneste, enheden leverer som er kritisk for samfundet. I den nuværende formulering kan det forstås som, at enhver alvorlig hændelse for enheden skal afføde en underretning – også selvom hændelsen ikke har eller kunne have en påvirkning af den tjeneste der er kritisk for samfundet.

- Det fremgår af Bemærkninger til lovforslagets enkelte bestemmelser til § 13, at underretning til den kompetente myndighed eller CSIRT skal ske ved hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Det kan overvejes ligeledes at præcisere dette i lovteksten.

Det bør præciseres, hvornår en hændelse, der ikke fik nogen konsekvenser, men var i stand til at forårsage alvorlige konsekvenser, skal anmeldes, da organisationer løbende rammes af mange hændelser, som har potentiale til at være alvorlige, men som de afværger.

§ 13 stk. 3

Essensen i kravet om tidlig underretning fra enheden til CSIRT (§13 stk. 1) understøtter værdien af tidlig vidensdeling i en krisesituation. Men hvor tidsgrænsen for enheden i §13 stk.1 er defineret som et absolut krav ("under alle omstændigheder inden for 24 timer…"), er der for CSIRT'en ikke defineret et krav om, hvor hurtigt en tilbagemelding skal ske, men der er en mere blød formulering: "hvor det er muligt, inden for 24 timer". Dette er uhensigtsmæssigt, da enheden i den givne situation skal bruge kostbar energi og fokus på at forholde sig til, hvornår der kan ventes en tilbagemelding og evt. på at rykke for svar. Loven bør fastsætte samme krav - altså et krav om, at tilbagemelding skal ske ("under alle omstændigheder inden for 24 timer…").

§ 15 stk. 1

De vigtige og væsentlige enheder leverer flere forskellige tjenester, hvor kun nogle af dem kan betragtes som værende kritiske. Det bør derfor præciseres i sætningen "… påvirke leveringen af deres tjenester negativt", at der her alene er tale om "kritiske tjenester".

§ 17 stk. 1

Der benyttes her termen "it-sikkerhed", mens der generelt andre steder, herunder i definitionen, omtales "Cybersikkerhed". Hvis det forståelsesmæssigt tænkes at være det samme, bør samme term bruges. Hvis der er tale om forskellige forståelser, bør "it-sikkerhed" defineres i §3

§ 31

Beskrivelsen her er meget bred og målet er uklart, i forhold til hvilke områder det dækker. Paragraffen har potentiale til at kunne række langt videre end forhold der er relevante ift. cybersikkerhed.

Det fremgår af "Bemærkninger til lovforslagets enkelte bestemmelser", at paragraffen er tiltænkt at have betydning i forhold til, hvordan kommunikation mellem enheden og CSIRT (ex. Virk.dk) skal ske. Dette kan med fordel præciseres i §31

Kommentar til "Almindelige bemærkninger"

3.1.2 Forsvarsministeriets overvejelser (s.152)
I en virksomhed med moder-/ datterselskaber, har moderselskabet og hver underenhed eget CVR-nr. Dette kan give et unødigt komplekst scenarie i forbindelse med en hændelse, da flere vandselskaber har oprettet en holding-struktur med flere CVR-nr. alene for at efterleve krav til regnskabsstruktur og økonomisk adskillelse. I praksis er mange selskaber driftsmæssigt struktureret som én digital enhed, og en cyber-hændelse vil have samtidig og ensartet effekt på tværs af flere datterselskaber (f.eks. vand og spildevand). Det it-beredskab der er aktiveret for at imødegå hændelsen vil i mange tilfælde operere på moderselskabsniveau. Det er derfor ikke hensigtsmæssigt, hverken for CSIRT eller enheden, at hændelsen skal håndteres parallelt som flere identiske sager for flere individuelle CVR-nr. Dette vil mere hensigtsmæssigt kunne håndteres, hvis en hændelse kan håndteres under moderselskabets CVR-nr., hvor det så blot anføres, hvilke øvrige CVR-nr. der er omfattet af hændelsen.

Vi ser frem til at bidrage positivt til det lovgivningsmæssige og øvrige arbejde, som implementeringen af loven afstedkommer.

DANVA imødeser en yderligere dialog om implementering af loven og står gerne til rådighed med yderligere dokumentation og viden, der kan belyse høringssvaret yderligere.

Eventuelle spørgsmål eller kommentarer bedes rettet til Peter Mortensen på telefon 8793 3502 eller på mail pm@danva.dk.

Med venlig hilsen

Carl-Emil Larsen
DANVA

Kopi til: Miljøministeriet, Miljøstyrelsen, Energistyrelsen, Green Power Denmark, Dansk Fjernvarme og Danske Vandværker

Sekretariatet for
Dataetisk Råd

dataetiskraad@dketik.dk
Dato: 17. juli 2024

Forsvarsministeriet
Holmens kanal 9
1060 København K

Forsvarsministeriet skal anmode om at modtage eventuelle bemærkninger senest den 22. august 2024 kl. 12. Bemærkninger bedes sendt på e-mail til fmn@fmn.dk med kopi til jhb@fmn.dk samt med henvisning til sagsnummer 2024/004461.

Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

Dataetisk Råd takker for den fremsendte høring. Rådet har i dette tilfælde valgt ikke at udarbejde et egentligt høringssvar.

Der kan være flere årsager til, at Dataetisk Råd ikke vælger at udarbejde høringssvar, herunder at rådet har valgt at prioritere andre opgaver, at det ikke efter rådets opfattelse er muligt på forsvarlig vis at analysere og behandle høringen i den enkeltheder og detaljer inden for høringsfristen, eller at høringen ikke ses at indebære dataetiske spørgsmål, som faldet inden for rådets kommissorium.

Det bemærkes dog, at, rådet generelt anbefaler, at ministerier redegør for de dataetiske konsekvenser af lovforslag. Dataetiske konsekvensanalyser sætter fokus på værdier og principper som blandt andet velfærd og demokrati, værdighed, selvbestemmelse, lighed, gennemsigtighed, sikkerhed og privatliv. Dataetiske konsekvensanalyser vil således hjælpe med at bringe fordele, ulemper og utilsigtede konsekvenser ved lovforslag frem i lyset og dermed bidrage til, at Folketingets beslutninger tages på et mere kvalificeret grundlag. Dette gælder naturligvis i særlig grad lovforslag, som angår persondata.

Dataetisk Råd kan i den forbindelse henvise til rådets værktøj 'Dataetik – Sådan gør du', der operationaliserer identificeringen og stillingtagen til dataetiske dilemmaer.

Dataetisk Råd står til rådighed for uddybning og yderligere rådgivning.

På vegne af Dataetisk Råd og med venlig hilsen

Johan Busse

Formand

DATATILSYNET

Forsvarsministeriet, Departementet
Holmens Kanal 9
1060 København K

Sendt til: fmn@fmn.dk
Kopi sendt til: jm@jm.dk

20. august 2024

J.nr. 2024-11-0155
Dok.nr. 614238
Sagsbehandler
Signe Vestergård
Spring

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

1. Indledende bemærkninger

Ved brev af 5. juli 2024 har Forsvarsministeriet anmodet om Datatilsynets eventuelle bemærkninger til ovennævnte udkast til lovforslag.

Datatilsynet skal i den anledning udtale følgende:

2. Anvendelsesområde

2.1. Det følger af udkastets § 4, stk. 3, nr. 2 at statslige myndigheder uanset deres størrelse anses for at være væsentlige enheder.

Datatilsynet er ligesom en række øvrige statslige myndigheder, herunder Domstolsstyrelsen, Rigsrevisionen og Folketingets Ombudsmand, en uafhængig myndighed. Det følger af databeskyttelsesforordningens artikel 51, stk. 1, og artikel 52, stk. 1, samt databeskyttelseslovens § 27, stk. 1, 2. pkt.

Datatilsynet bemærker, at flere af udkastets bestemmelser umiddelbart virker indgribende i sit indhold i forhold, at Datatilsynet som tilsynsmyndighed skal udføre sine opgaver og udøve sine beføjelser i henhold til databeskyttelsesforordningen og databeskyttelsesloven i fuld uafhængighed, jf. databeskyttelsesforordningens artikel 51, stk. 1, og artikel 52, stk. 1, samt databeskyttelseslovens § 27, stk. 1, 2. pkt.

På den baggrund skal Datatilsynet opfordre til, at det undersøges, hvordan direktivet implementeres i de øvrige medlemslande i forhold til uafhængige statslige myndigheder, herunder andre tilsynsmyndigheder på databeskyttelsesområdet. I den forbindelse bemærker Datatilsynet, at en uensartet implementering på tværs af medlemslandene kan medføre en disharmoni i forhold til myndighedernes udførelse af deres opgaver.

I tilfælde af at Datatilsynet f.eks. pålægges at anvende specifikke produkter, løsninger og processer mv. efter regler fastsat efter udkastets § 8 til udførelsen af sine opgaver som tilsynsmyndighed for databeskyttelsesreglerne, kan dette efter tilsynets opfattelse potentielt medføre, at tilsynet ikke kan udøve sine funktioner i fuld uafhængighed som tiltænkt efter databeskyttelsesforordningen. Dette bør efter Datatilsynets opfattelse tages i betragtning ved fastsættelse af regler om anvendelse af specifikke IKT-produkter, -tjenester og -processer efter

udkastets § 8. Datatilsynet forudsætter i den forbindelse at blive hørt i forbindelse med udarbejdelse af bekendtgørelser i medfør af denne bestemmelse i lovforslaget.

I forhold til udkastets § 8 skal Datatilsynet endvidere bemærke, at det må være en forudsætning for at pålægge enheder at anvende specifikke produkter, løsninger og processer mv. til aktiviteter, hvor der behandles personoplysninger, at behandlingen kan ske lovligt i henhold til databeskyttelsesreglerne, herunder reglerne om overførsel af personoplysninger til tredjelande. Dette bør efter Datatilsynets opfattelse præciseres i bemærkningerne til bestemmelsen.

2.2. Det følger af udkastets § 1, stk. 7, at vedkommende minister inden for sit område kan fastsætte regler om, at loven helt eller delvist også finder anvendelse på henholdsvis offentlige forvaltningsenheder på lokalt plan og uddannelsesinstitutioner.

Det fremgår bl.a. af udkastets bemærkninger til bestemmelsen, at det på nuværende tidspunkt ikke er intentionen at fastsætte regler om, at kommunerne omfattes af loven.

Datatilsynet bemærker i den forbindelse, at der igennem tiden har været mange eksempler på, at kommuner ikke har gennemført passende sikkerhedsforanstaltninger i forhold til deres behandling af personoplysninger. Dette kunne efter tilsynets opfattelse tale for, at kommunerne omfattes af loven, så de bliver underlagt de samme krav til styring af cybersikkerhedsrisici, som f.eks. statslige myndigheder, der ifølge udkastets § 4, stk. 3, nr. 2, alle anses for at være væsentlige enheder.

3. Generelle bemærkninger om samarbejde og vejledning

Datatilsynet har konstateret, at en del af de begreber og krav, der fremgår af udkastet og NIS 2-direktivet[1] minder om de begreber og krav, der følger af databeskyttelsesforordningen og databeskyttelsesloven. Det gælder i særlig grad udkastets kapitel 2, som indeholder krav til væsentlige og vigtige enheder i forhold til at træffe passende foranstaltninger til styring af cybersikkerhedsrisici, hvor databeskyttelsesforordningens artikel 32 således også indeholder forpligtelser for dataansvarlige og databehandlere til at gennemføre passende sikkerhedsforanstaltninger i forhold til de risici, som behandlingen af personoplysninger medfører for fysiske personers rettigheder og frihedsrettigheder. Et andet eksempel er udkastets § 12 om en underretningspligt i tilfælde af væsentlige hændelser, hvor databeskyttelsesforordningens artikel 33 indeholder en anmeldelsespligt i tilfælde af brud på persondatasikkerheden.

Derudover formoder Datatilsynet, at en del af de myndigheder, virksomheder og organisationer, som omfattes af udkastets anvendelsesområde, også behandler personoplysninger – enten som databehandler eller dataansvarlig – og skal dermed tillige overholde databeskyttelsesforordningen og databeskyttelsesloven.

Det er derfor efter Datatilsynets opfattelse nødvendigt med et tæt og koordineret samarbejde mellem Datatilsynet og Center for Cybersikkerhed, samt de øvrige myndigheder, der udpeges som kompetente myndigheder, i forhold til bl.a. håndtering af underretninger om væsentlige hændelser, som også udgør brud persondatasikkerheden, og eventuelt også i forhold til vejledning om kravene til implementering af sikkerhedsforanstaltninger.

1 Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet)

Endvidere foreslås det i udkastets § 6, stk. 3, og § 12, stk. 3, at de pågældende ministre inden for deres respektive områder bemyndiges til at fastsætte nærmere regler om henholdsvis krav til foranstaltninger efter udkastets § 6, stk. 1, og om hvornår en hændelse anses for at være væsentlig.
Datatilsynet bemærker i den forbindelse, at det særligt i forhold til disse områder – men også helt generelt – er nødvendigt med praktisk og anvendelig vejledning fra Center for Cybersikkerhed til de myndigheder, virksomheder og organisationer, der omfattes af loven.

4. Indberetning af hændelser

Det følger af udkastets § 12, stk. 1, at det er væsentlige og vigtige enheder, der skal underrette de relevante kompetente myndigheder og CSIRT'en om enhver væsentlig hændelse. Derudover følger det af udkastets § 4, stk. 3, nr. 2, at statslige myndigheder uanset deres størrelse anses for at være væsentlige enheder.

Datatilsynet skal i den forbindelse bemærke, at Statens IT leverer it-drift og services til en efterhånden omfattende kreds af statslige myndigheder. En hændelse – f.eks. et hackerangreb – hos Statens IT kan således medføre, at et betydeligt antal statslige myndigheder skal foretage underretning om samme forhold i medfør af udkastets § 12, stk. 1. Det bør derfor efter Datatilsynets opfattelse præciseres i lovforslaget, hvilken rolle Statens IT har i forbindelse med underretning om væsentlige hændelser. Dette er særligt henset til de korte frister for varslinger og hændelsesunderretninger, der foreslås fastsat i udkastets § 13.

5. Videregivelse af personoplysninger til CSIRT'en

Det følger af udkastets § 17, stk. 1, nr. 1 og 3, at CSIRT'en efter anmodning fra en væsentlig eller vigtig enhed kan yde bistand vedrørende realtids- eller nærrealtidsmonitorering af enhedens net- og informationssystemer og foretage en proaktiv scanning af enhedens net- og informationssystemer, der anvendes til levering af enhedens tjenester, for at opdage sårbarheder med en potentielt væsentlig indvirkning.

Det fremgår af afsnit 8.1. i udkastets almindelige bemærkninger, at hvis disse it-systemer indeholder personoplysninger, herunder følsomme personoplysninger og personoplysninger vedrørende straffedomme og lovovertrædelser, vil det ikke helt kunne udelukkes, at Center for Cybersikkerhed vil få adgang til disse oplysninger. Det fremgår endvidere, at det i så fald vil betragtes som en videregivelse mellem to selvstændige dataansvarlige, og at videregivelsen sker inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

Datatilsynet bemærker i den forbindelse, at hvis en virksomhed eller myndighed behandler personoplysninger på vegne af en dataansvarlig, er den pågældende virksomhed eller myndighed databehandler i forhold til behandlingen af personoplysninger. Databehandlerens behandling skal være reguleret af en databehandleraftale, som skal opfylde en række specifikke krav, der følger af databeskyttelsesforordningens artikel 28, stk. 3, litra a-h. Det skal efter artikel 28, stk. 3, litra a fastsættes, at databehandleren kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. I så fald skal databehandleren som udgangspunkt underrette den dataansvarlige om dette retlige krav inden behandlingen.

Hvis en væsentlig eller vigtig enhed er databehandler for en eller flere dataansvarlige, skal det således som udgangspunkt reguleres i databehandleraftalen, under hvilke omstændigheder databehandleren kan give CSIRT'en adgang til eventuelle personoplysninger i et it-system, samt hvorvidt databehandleren skal underrette den dataansvarlige i tilfælde af, at databehandleren ønsker at anmode CSIRT'en om bistand i overensstemmelse med de ovenfor nævnte

bestemmelser i udkastet. I den forbindelse bemærkes det, at disse forhold f.eks. skal præciseres i statslige myndigheders databehandleraftaler med Statens IT som databehandler.

Datatilsynet foreslår på den baggrund, at det tilføjes i bemærkningerne til ovennævnte bestemmelse i udkastet, at myndigheder, virksomheder og organisationer, der er dataansvarlige for behandling af personoplysninger bør afklare, om (nogle af) deres databehandlere er omfattet af lovens anvendelsesområde som væsentlige og vigtige enheder. I den forbindelse kan det tilføjes, at de dataansvarlige skal sikre, at det i deres databehandleraftaler fastsættes, under hvilke omstændigheder deres databehandlere kan give CSIRT'en adgang til personoplysninger, som behandles på vegne af den dataansvarlige, samt hvorvidt databehandleren skal underrette den dataansvarlige i tilfælde af, at databehandleren ønsker at anmode CSIRT'en om bistand i overensstemmelse med de ovenfor nævnte bestemmelser i udkastet.

6. Aktindsigt

Det følger af udkastets § 14, stk. 1, at offentlige og private enheder kan underrette CSIRT'en om hændelser, nærvedhændelser og cybertrusler. Disse underretninger er undtaget fra aktindsigt efter offentlighedsloven og forvaltningsloven. Det følger af udkastets § 14, stk. 3.

Det fremgår af udkastets bemærkninger til § 14, at anvendelsesområdet er begrænset til at omfatte de frivillige underretninger, der modtages i medfør af § 14, stk. 1, og at de obligatoriske underretninger i medfør af § 12, således ikke vil være omfattet af § 14, stk. 3.

Derudover fremgår følgende bl.a. af bemærkningerne til § 14:

> "[…]
>
> Særligt for virksomheder kan oplysninger om, at der f.eks. er gennemført et vellykket hackerangreb, hvor virksomheden har mistet data, i høj grad skade virksomhedens omdømme, og det kan i praksis afholde mange virksomheder fra frivilligt at underrette CSIRT'en om et sådant hackerangreb. Derfor foreslås det med bestemmelsen, at underretningerne i deres helhed undtages fra aktindsigt, herunder partsaktindsigt efter forvaltningsloven. Undtagelsen kan omfatte underretningssagen som helhed.
>
> […]"

Datatilsynet bemærker i den forbindelse, at tilsynet i perioder modtager et stort antal aktindsigtsbegæringer i de anmeldelser af brud på persondatasikkerheden, som Datatilsynet har modtaget i henhold til § 33 i databeskyttelsesforordningen. En del af disse aktindsigtsanmodninger vedrører anmeldelser af brud på persondatasikkerheden, som skyldes hackerangreb. Nogle af disse anmeldelser er også stilet til Center for Cybersikkerhed i medfør af § 8, stk. 1, i lov om sikkerhed i net og tjenester.

Datatilsynet har ikke hjemmel til at undtage anmeldelsessager i deres helhed fra aktindsigt, som Center for Cybersikkerhed har i medfør af § 8, stk. 2, i lov om sikkerhed i net og tjenester i forhold til underretninger, som er omfattet af lovens § 8, stk. 1. Der er imidlertid ved tilsynets behandling af aktindsigtsbegæringer grundlag for i en del af sagerne at undtage oplysninger i anmeldelserne og eventuelle øvrige dokumenter på sagerne i henhold til henholdsvis § 30, nr. 2, 33, stk. 1, og § 33, nr. 5 i offentlighedsloven.

Datatilsynet er naturligvis særdeles opmærksom på hensyn til cyber- og informationssikkerhed ved vurderingen aktindsigtsbegæringer i en eller flere anmeldelser af brud på persondatasikkerheden og har etableret en fast procedure for høring af Center for Cybersikkerhed, som iværksættes, når det konkret vurderes relevant. Datatilsynet foretager således høring af Cen-

ter for Cybersikkerhed, når den anmeldelse, der anmodes om aktindsigt i, også er stilet til Center for Cybersikkerhed i henhold til § 8, stk. 1, i lov om sikkerhed i net og tjenester. Derudover foretager Datatilsynet også høring af Center for Cybersikkerhed ved behandling af sager om aktindsigt og dataudtræk i en del andre af tilsynets sager, der indeholder oplysninger om sårbarheder i forhold til IT-sikkerheden.

Datatilsynet bemærker på den baggrund, at tilsynet også fremadrettet efter en eventuel ikrafttrædelse af udkastet til lovforlag forventer at inddrage Center for Cybersikkerhed i sager om aktindsigt i sager om anmeldelse af brud på persondatasikkerheden og andre sager, der indeholder oplysninger om sårbarheder i forhold til IT-sikkerheden.

Derudover opfordrer Datatilsynet til, at det overvejes om ikke også Datatilsynets sager om anmeldelse af brud på persondatasikkerheden generelt skal undtages fra aktindsigt i sin helhed, da de samme hensyn, der fremgår af bemærkningerne til udkastets § 14, stk. 3, efter Datatilsynets opfattelse også gør sig gældende i forhold til disse sager.

7. Bødestraf

I udkastets § 32, stk. 3, foreslås, at hvis der er pålagt en bøde for overtrædelse af databeskyttelsesforordningen[2] eller databeskyttelsesloven[3], kan der ikke pålægges en bøde for overtrædelse af denne lov eller regler udstedt i medfør af loven, hvis overtrædelsen skyldes den samme adfærd som den, der var genstand for bøden i medfør af databeskyttelsesforordningen og databeskyttelsesloven.

Det følgende fremgår bl.a. af afsnit 3.5.2.4. i de almindelige bemærkninger til lovforslaget:

> "[…]
>
> Henset til, at et brud på cybersikkerheden også efter omstændighederne kan udgøre et brud på persondatasikkerheden, er bestemmelsen i NIS 2-direktivets artikel 35, stk. 2, udtryk for det almindelige forbud mod dobbelt strafforfølgning. Det anføres således i præambelbetragtning nr. 131, at pålæggelse af sanktioner for overtrædelse af de nationale regler, der gennemfører NIS 2-direktivet, ikke bør føre til et brud på princippet om ne bis in idem som fortolket af Den Europæiske Unions Domstol.
>
> […]"

Datatilsynet bemærker i den forbindelse, at selvom en adfærd, der udgør en overtrædelse af den foreslåede lov, ikke har ført til et brud på persondatasikkerheden, som defineret i databeskyttelsesforordningens artikel 4, nr. 12, kan der være tale om en adfærd, der udgør en overtrædelse af databeskyttelsesforordningens artikel 32, stk. 1.

Af databeskyttelsesforordningens artikel 32, stk. 1, fremgår, at den dataansvarlige skal træffe passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er ved den dataansvarliges behandlinger af personoplysninger. Der påhviler den dataansvarlige en pligt til at identificere de risici, den dataansvarliges behandling udgør for de registrerede og til at sikre, at der indføres passende sikkerhedsforanstaltninger, der beskytter de registrerede mod disse risici.

2 Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

3 Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

Ved vurderingen af, hvilket sikkerhedsniveau der er passende, skal der navnlig tages hensyn til de risici, som behandlingen udgør, navnlig ved brud på persondatasikkerheden. Det følger af databeskyttelsesforordningens artikel 32, stk. 2.

Dataansvarliges og databehandleres overtrædelse af deres forpligtelser i henhold til bl.a. databeskyttelsesforordningens artikel 32 kan straffes med bøde. Det følger af databeskyttelseslovens § 41, stk. 1, nr. 1, jf. stk. 3, jf. stk. 6, jf. databeskyttelsesforordningens artikel 83, stk. 2, og stk. 4, litra a, jf. stk. 9. Datatilsynet kan således foretage politianmeldelse af dataansvarlige og databehandlere for overtrædelse af databeskyttelsesforordningens artikel 32, stk. 1, hvis tilsynet har vurderet, at den pågældende myndighed eller virksomhed ikke har gennemført passende sikkerhedsforanstaltninger, uanset om der er sket et brud på persondatasikkerheden.

På den baggrund foreslår Datatilsynet, at afsnittet omformuleres. Dette kan f.eks. ske på følgende måde:

"Henset til, at utilstrækkelige foranstaltninger til styring af cybersikkerhedsrisici også efter omstændighederne kan udgøre utilstrækkelige foranstaltninger i forhold til kravene i databeskyttelsesforordningens artikel 32, stk. 1, og som kan medføre brud på persondatasikkerheden, er bestemmelsen i NIS 2-direktivets artikel 35, stk. 2, udtryk for det almindelige forbud mod dobbelt strafforfølgning. Det anføres således i præambelbetragtning nr. 131, at pålæggelse af sanktioner for overtrædelse af de nationale regler, der gennemfører NIS 2-direktivet, ikke bør føre til et brud på princippet om ne bis in idem som fortolket af Den Europæiske Unions Domstol."

8. Underretning af Datatilsynet

Det fremgår af artikel 35, stk. 1, i NIS 2-direktivet, at hvor de kompetente myndigheder i forbindelse med tilsyn eller håndhævelse bliver opmærksomme på, at en væsentlig eller vigtig enheds overtrædelse af forpligtelserne i dette direktivs artikel 21 og 23 kan medføre et brud på persondatasikkerheden som defineret i artikel 4, nr. 12, i databeskyttelsesforordningen, som skal anmeldes i henhold til databeskyttelsesforordningens artikel 33, underretter de uden unødigt ophold tilsynsmyndighederne efter databeskyttelsesforordningen.

Det følgende fremgår bl.a. af afsnit 3.5.2.4. i de almindelige bemærkninger til udkastet:

> "[…]
>
> De kompetente myndigheder vil derfor alene skulle foretage underretning af Datatilsynet på baggrund af NIS 2-direktivets artikel 35, stk. 1, om mulige brud på persondatasikkerheden, hvis det ikke er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Der må overlades de kompetente myndigheder et bredt skøn ved foretagelsen af denne vurdering.
>
> […]"

Datatilsynet har forstået, at artikel 35, stk. 1, i NIS 2-direktivet indebærer, at de kompetente myndigheder i Danmark skal underrette Datatilsynet i tilfælde, hvor de i forbindelse med tilsyn eller håndhævelse bliver opmærksomme på, at en væsentlig eller vigtig enheds overtrædelse af artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser) kan medføre et brud på persondatasikkerheden. Datatilsynet har således forstået, at de kompetente myndigheder ikke skal have konstateret mulige brud på persondatasikkerheden men blot en overtrædelse af ovennævnte bestemmelser – f.eks. manglende im-

plementering af passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger – der kan medføre brud på persondatasikkerheden.

På den baggrund foreslår Datatilsynet, at afsnittet omformuleres. Dette kan f.eks. ske på følgende måde:

"De kompetente myndigheder vil derfor skulle foretage underretning af Datatilsynet på baggrund af NIS 2-direktivets artikel 35, stk. 1, om forhold der kan medføre et brud på persondatasikkerheden, medmindre det er usandsynligt, at et eventuelt brud på persondatasikkerheden vil indebære en risiko for fysiske personers rettigheder eller frihedsrettigheder. Der må overlades de kompetente myndigheder et bredt skøn ved foretagelsen af denne vurdering."

Derudover foreslår Datatilsynet, at der i afsnit 3.5.2.4. i de almindelige bemærkninger til udkastet tilføjes et afsnit om, at hændelser, som de væsentlige og vigtige enheder skal underrette den relevante kompetente myndighed og CSIRT'en om i overensstemmelse med udkastets §§ 12 og 13, efter omstændighederne kan udgøre brud på persondatasikkerheden. I afsnittet foreslår Datatilsynet, at det tilføjes, at de dataansvarlige for behandlingen af de pågældende personoplysninger, der er omfattet af et brud på persondatasikkerheden, er forpligtede til at anmelde bruddet til Datatilsynet i overensstemmelse med databeskyttelsesforordningens artikel 33, medmindre det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder og frihedsrettigheder. En sådan anmeldelse skal foretages uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet på persondatasikkerheden.

Brud på persondatasikkerheden kan anmeldes til Datatilsynet via Virk.dk, hvor der i dag også kan ske indberetning af sikkerhedshændelser, der vedrører væsentlige dele af Danmarks infrastruktur f.eks. forsyning og digital infrastruktur, finans og telekommunikation.

Datatilsynet forudsætter, at underretninger af væsentlige hændelser, der også udgør brud på persondatasikkerheden vil skulle sendes til de relevante kompetente myndigheder og CSIRT'en (Center for Cybersikkerhed) via Virk.dk, hvor underretningen/anmeldelsen også kan sendes til Datatilsynet.

Datatilsynet foreslår endvidere, at det tilføjes i ovennævnte afsnit i de almindelige bemærkninger, at i tilfælde af at en hændelse udgør et brud på persondatasikkerheden, skal den dataansvarlige overveje, om det pågældende brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder. I så fald skal den dataansvarlige underrette de registrerede om bruddet på persondatasikkerheden, jf. databeskyttelsesforordningens artikel 34, stk. 1.

9. Påbud om offentliggørelse af afgørelser mv. i ikke-anonymiseret form

Det følger af udkastets § 22, nr. 6 og § 25, nr. 4, at den kompetente myndighed kan påbyde væsentlige og vigtige enheder i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter henholdsvis § 22, nr. 1-5 og § 25, nr. 4 i lovforslaget samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

Det følgende fremgår bl.a. af bemærkningerne til henholdsvis lovforslagets § 22, nr. 6 og § 25, nr. 4:

"[…]

> I overensstemmelse med principperne i betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. forudsættes det, at den kompetente myndighed ved beslutningen om, hvilke oplysninger en enhed pålægges at offentliggøre, i fornødent omfang bl.a. iagttager de hensyn til fortrolighed, der fremgår af forvaltningslovens § 27 om offentligt ansattes tavshedspligt, herunder bl.a. hensynene til enkeltpersoners private forhold, forretningshemmeligheder samt forebyggelse, efterforskning og forfølgning af lovovertrædelser.
>
> […]"

Derudover fremgår det bl.a. i afsnit 8 i de almindelige bemærkninger til lovforslaget, at der kan blive behandlet personoplysninger i forbindelse med anvendelsen af tilsyns- og håndhævelsesforanstaltninger i medfør af de foreslåede bestemmelser i §§ 21-23 og §§ 24 og 25. Det fremgår i den forbindelse, at de oplysninger, der måtte blive behandlet i denne forbindelse, vil udgøre oplysninger om enhedens medarbejdere, og at disse oplysninger primært vil udgøre kontaktoplysninger på enhedens kontaktpersoner, ligesom der eksempelvis kan være tale om oplysninger om hvilke medarbejdere, der har adgang til enhedens net- og informationssystemer.

Datatilsynet lægger til grund, at det ikke kan udelukkes, at nogle væsentlige og vigtige enheder kan være enkeltmandsejede virksomheder. I den forbindelse bemærker tilsynet, at oplysninger om enkeltmandsejede virksomheder udgør personoplysninger. Et påbud om offentliggørelse af afgørelser om håndhævelsesforanstaltninger samt resumeer af domme eller bødevedtagelser i ikke-anonymiseret form vil således medføre, at den pågældende virksomhed skal offentliggøre personoplysninger.

Oplysninger om en overtrædelse af lovgivning udgør oplysninger om strafbare forhold, også selvom det ikke har udløst eller kan udløse et egentligt strafansvar, men eventuelt andre sanktioner, som f.eks. rettighedsfrakendelse.[4] Det følger af databeskyttelseslovens § 8, stk. 3, at private må behandle, herunder videregive, oplysninger om strafbare forhold, hvis den registrerede har givet sit udtrykkelige samtykke hertil, eller hvis det er nødvendigt til varetagelse af en berettiget interesse og denne interesse klart overstiger hensynet til den registrerede.

Forsvarsministeriets ses ikke i lovforslagets bemærkninger at have forholdt sig til, om kompetente myndigheder kan påbyde enkeltmandsejede virksomheder at offentliggøre afgørelser om håndhævelsesforanstaltninger samt resumeer af domme eller bødevedtagelser i ikke-anonymiseret form i overensstemmelse med databeskyttelsesforordningen og databeskyttelsesloven.

10. Videregivelse af oplysninger til andre medlemsstaters myndigheder og til institutioner i Den Europæiske Union

Det følger af udkastets § 28, at de relevante myndigheder kan videregive oplysninger til andre medlemsstaters myndigheder og til institutioner i Den Europæiske Union for at varetage de opgaver, som følger af denne lov eller NIS 2-direktivet.

Det fremgår af udkastets bemærkninger til bestemmelsen, at det er Forsvarsministeriets opfattelse, at der er behov for at indføre særskilt hjemmel til at kunne videregive oplysninger af fortrolig karakter til andre medlemsstaters myndigheder og til institutioner i Den Europæiske Union.

4 Det fremgår af bemærkningerne til § 8 i Forslag til Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) Fremsat den 25. oktober 2017

Det fremgår ikke af bemærkningerne til den foreslåede bestemmelse, om der efter bestemmelsen kan videregives personoplysninger, herunder oplysninger om eventuelle enkeltmandsejede virksomheder.

Forholdet til de databeskyttelsesretlige regler ses at være behandlet i afsnit 8 i de almindelige bemærkninger til lovforslaget. I afsnittet er en række af lovforslagets bestemmelser omtalt i forhold til, at lovforslaget indebærer en række forpligtelser for omfattede enheder samt myndighedsopgaver for de relevante myndigheder, der i et vist omfang vil indebære behandling af personoplysninger. Udkastets § 28 ses ikke at være omtalt i dette afsnit.

Datatilsynet forudsætter imidlertid, at den eventuelle behandling af personoplysninger, som anvendelsen af den foreslåede bestemmelse vil medføre, sker under iagttagelse af databeskyttelseslovgivningen.

11. Afsluttende bemærkninger

Datatilsynet forudsætter at blive hørt i forbindelse med udarbejdelse af bekendtgørelser og lignende generelle retsforskrifter i medfør af lovforslaget, hvis disse vil have betydning for beskyttelsen af privatlivet i forbindelse med behandling af personoplysninger, jf. databeskyttelseslovens § 28.

Kopi af dette brev er sendt til Justitsministeriets Lovafdeling orientering.

Med venlig hilsen

Signe Vestergård

De Samvirkende Købmænd
Islands Brygge 26, DK-2300 København S
T +45 39 62 16 16 | dsk@dsk.dk

CVR nr. 15232013 | Danske Bank 4180-4110212313

Forsvarsministeriet
Holmens Kanal 9
1060 København K
Sagsnummer 2024/004555

København, den 22. august 2024

Høringssvar vedr. forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

De Samvirkende Købmænd (DSK) takker for muligheden for at afgive bemærkninger til ovennævnte lovforslag.

DSK forholder sig alene til lovforslagets betydning for fødevarevirksomheder og henviser i den forbindelse til høringssvaret fra Dansk Erhverv.

Med venlig hilsen

ANNETTE NORUP THOMSEN
Erhvervsjuridisk chef

D-mærkets høringssvar på udkast til forslag om lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Vedr. sagsnummer: 2024/004461

21. august 2024

Til:
Forsvarsministeriet
Holmens Kanal 9
1060 København K
fmn@fmn.dk

Kopi:
Jakob Halkjær Brams: jhb@fmn.dk

Vedr. sagsnummer: 2024/004461

Høringssvar på udkast til forslag om lov om foranstaltninger til sikring af et højt cyber-sikkerhedsniveau

D-mærket vil gerne takke for muligheden for at afgive høringssvar til det fremsatte lovforslag om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

Vi anerkender vigtigheden af at styrke cybersikkerheden i Danmark og EU i lyset af den stigende digitalisering og den høje cybertrussel og støtter målet om at øge modstandsdygtigheden i kritisk infrastruktur samtidig med, at der skabes grundlag for at højne den digitale tryghed for bl.a. borgere og samfundet på tværs af EU.

Mærkningsordninger er noget, som vi er kendt for i Danmark, og som både giver forbrugerbeskyttelse- og -tillid samt øger konkurrenceevnen for virksomheder. D-mærket er Danmarks mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse.

Overordnet kommentar

NIS 2-direktivet vil stille krav til udvalgte virksomheders cybersikkerhed. Direktivet omfatter virksomheder, der defineres som kritisk infrastruktur og indirekte deres underleverandører. Dette indebærer, at mange danske virksomheder vil skulle investere betydelige ressourcer i at opfylde de nye krav. Især små og mellemstore virksomheder (SMV'er) og underleverandører til NIS 2-omfattede virksomheder vurderer D-mærket skal have hjælp i processen henimod at leve op til og kunne dokumentere de nye krav.

D-mærket
H. C. Andersens Boulevard 18 I 1553 I København V
Telefon: +45 33 77 33 77 I kontakt@d-maerket.dk I www.d-maerket.dk

D-mærkets bemærkninger

Vedr. implementering af NIS 2-direktivet og anvendelse af relevante rammeværk

Danske virksomheder har brug for en lettilgængelig og konkret måde at arbejde med kravene i NIS 2-direktivet på og samtidig tydeligt vise, at de lever op til disse krav.

D-mærket bemærker, at flere medlemslande i forbindelse med NIS 1-cybersikkerhedskravene har tilladt, at overensstemmelse kan baseres på ISO/IEC 27001-certificering eller brugen af nationale informationssikkerhedsstandarder, der er kompatible med ISO/IEC 27001, fx BSI IT-Grundschutz i Tyskland, E-ITS i Estland og Cyberfundamentals framework i Belgien.

NIS 2-direktivet tilskynder til, at virksomheder og organisationer bruger europæiske eller internationalt accepterede sikkerhedsstandarder eller EU-landenes egne nationale standarder for at sikre, at direktivet efterleves[1]. Derfor er det relevant for myndighederne at vurdere og tage stilling til, hvorvidt D-mærket og andre rammeværk kan anvendes af virksomhederne i deres implementering af NIS 2-direktivet.

Det bemærkes, at der er god overensstemmelse mellem D-mærkets kriterier og krav og NIS 2-direktivets krav til hhv. styring og forankring i ledelsen samt krav til risikostyring og sikkerhedsforanstaltninger som angivet i NIS 2-direktivets artikel 20 og 21 og lovudkastets §§ 6 – 7. Denne overensstemmelse fremgår af D-mærkets overordnede mapping til NIS 2-direktivet[2].

Vedr. minimimumsimplemtering af NIS 2-direktivet

D-mærket støtter en direktivnær gennemførsel med minimumsimplementering, der skal sikre ensartethed og koordination på tværs af sektorer, hvilket er afgørende for at undgå modsatrettede krav for tværsektorielle aktører.

Vedr. operationalisering af krav

For at sikre en så effektiv implementering af NIS 2-direktivet som muligt, er det vigtigt, at myndighederne bidrager til at understøtte overgangen fra lovgivning over konkrete krav og vejledning til tilsyn. I overgangen fra lovgivning til konkrete krav bifalder D-mærket, at udmøntningen sker i bekendtgørelsesform, og disse vil kunne tage højde for særlige sektorvise forhold. D-mærket vil anbefale, at sektorbekendtgørelserne offentliggøres i god tid og minimum 6 måneder, inden loven træder i kraft.

For at lette virksomhedernes implementering af de konkrete bekendtgørelser anbefaler D-mærket, at myndighederne foretager en mapping af de centrale krav i kommende bekendtgørelser til anerkendte internationale rammeværker som ISO/IEC 2700X, NIST CSF og CIS18 og europæiske eller danske rammeværker såsom D-mærket. Dette vil hjælpe virksomhederne med at identificere nødvendige tiltag og sikre en mere effektiv efterlevelse af NIS 2-direktivet. En sådan mapping vil gøre det enklere for de virksomheder, der allerede

[1] NIS 2-direktivet, artikel 25
[2] D-maerkets-mapping-til-NIS2.pdf

D-mærket
H. C. Andersens Boulevard 18 I 1553 I København V
Telefon: +45 33 77 33 77 I kontakt@d-maerket.dk I www.d-maerket.dk

arbejder efter rammeværker og best practice at se, hvor der er 'gaps' ift. NIS 2-efterlevelse, medvirke til at reducere virksomhedernes ressourcer til fortolkning af krav og retningslinjer og give virksomheder incitament til at arbejde efter standarder og rammeværker – herunder D-mærket.

Vedr. hjælp til styring af underleverandører

I forbindelse med effektiv implementering af NIS 2-direktivet er der også behov for, at der tages hånd om de virksomheder, der bliver indirekte omfattet af NIS 2-direktivet i kraft af at være underleverandører til NIS 2-omfattede virksomheder. Her er det vigtigt, at de NIS 2-omfattede virksomheder får hjælp til at anlægge en proportional og risikobaseret tilgang til styring af deres underleverandører, så underleverandørerne ikke pålægges krav, der ligger ud over, hvad der er nødvendigt i forhold til at tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risici.

Vedr. ensartet tilsynstilgang fra myndighederne

Det er vigtigt, at virksomheder ikke møder forskellige tilgange til tilsyn, når de interagerer med de kompetente myndigheder. Derfor bifalder D-mærket, at der påtænkes en tæt koordination mellem de kompetente myndigheder i forbindelse med tilrettelæggelsen af tilsynsarbejdet. En ensartet tilgang fra tilsynsmyndighederne vil reducere virksomhedernes administrations- og implementeringsomkostninger, hvilket D-mærket ser som en vigtig forudsætning for en vellykket implementering af direktivet i Danmark.

Vedr. tilsyn for vigtige enheder

NIS 2-direktivet skelner mellem væsentlige og vigtige enheder. Da myndighederne kun vil foretage proaktivt tilsyn for væsentlige enheder (jf. § 21), kan D-mærket også være et værktøj til at understøtte efterlevelse hos vigtige enheder (jf. § 24).

Vedr. koordinering med myndighederne ift. udmøntning af krav og tilhørende tilsyn

Hvis virksomheder skal anvende D-mærket og andre rammeværk som værktøj til efterlevelse af NIS 2-direktivet, er det vigtigt, at virksomhederne oplever, at det pågældende rammeværks kriterier og tilhørende tilsyn flugter med myndighedernes tilgang for at lette virksomhedernes administrations- og implementeringsomkostninger.

For at det kan ske, er det derfor vigtigt, at der sker en koordination mellem de kompetente myndigheder og Center for Cybersikkerhed (i kraft af CfCS' rolle som centralt kontaktpunkt) på den ene side og fx D-mærket på den anden, så det sikres, at et anvendt rammeværk flugter med de kommende bekendtgørelser og tilhørende tilsynskoncept(er), så danske virksomheder kan blive betrygget i, at bl.a. Center for Cybersikkerhed "siger god for" fx D-mærket i relation til NIS 2. Dette indsatsområde er også beskrevet som en del af arbejdsporet om D-mærket i Cybersikkerhedspagten.

D-mærket
H. C. Andersens Boulevard 18 I 1553 I København V
Telefon: +45 33 77 33 77 I kontakt@d-maerket.dk I www.d-maerket.dk

Vedr. international interessevaretagelse samt opdatering af den nationale cybersikkerhedsstrategi

Mange virksomheder arbejder internationalt og har underleverandører, der ikke er danske. For dem er det vigtigt, at de værktøjer, de anvender som udgangspunkt for efterlevelse, såsom D-mærket, ikke blot er et dansk initiativ, men på sigt også bliver et europæisk eller internationalt initiativ.

Det kan vi i Danmark sammen være med til at sikre. Dels ved at de kompetente myndigheder i Danmark tager D-mærket og andre relevante initiativer med i dialogen med andre medlemsstaters kompetente myndigheder – og hvor relevant – Europa-Kommissionen og Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), men også at D-mærket og andre relevante initiativer tænkes ind i forbindelse med opdatering af den nationale cybersikkerhedsstrategi, der bl.a. har til hensigt at udmønte NIS 2-direktivets artikel 7.

Konklusion

D-mærket støtter behovet for lovgivning på cybersikkerhedsområdet på tværs af EU. Det bliver en krævende opgave for mange danske virksomheder at leve op til NIS 2-lovkravene, og danske virksomheder har brug for en lettilgængelig og konkret måde at arbejde med kravene i NIS 2-direktivet på og samtidig tydeligt vise, at de lever op til disse krav.

D-mærket støtter den danske tilgang med fokus på minimumsimplementering og ensartethed i bekendtgørelser, der implementerer kravene, samt myndighedernes tilgang til tilsyn.

D-mærket opfordrer myndighederne til at vurdere D-mærket og andre lignende rammeværk som mulige værktøjer til efterlevelse og dokumentation af NIS 2-kravene for at reducere virksomhedernes implementeringsomkostninger og sikre effektiv efterlevelse af NIS 2-direktivet for de direkte omfattede virksomheder og deres respektive underleverandører.

D-mærket opfordrer de kompetente myndigheder til at arbejde for, at de valgte implementeringstilgange kan anvendes på tværs af EU.

Vi ser frem til fortsat dialog med myndighederne for at sikre en effektiv implementering af NIS2-direktivet. Vi står til rådighed for yderligere samarbejde og drøftelser om dette vigtige emne.

Venlig hilsen,

Mikael Jensen
Direktør
D-mærket

D-mærket
H. C. Andersens Boulevard 18 I 1553 I København V
Telefon: +45 33 77 33 77 I kontakt@d-maerket.dk I www.d-maerket.dk

Forsvarsministeriet

26. august 2024

Sendt pr. mail til: jhb@fmn.dk

Dok.nr.: 24/18419-9
Sagsbehandler:
Emilie Kjersner
Mail: EMK@domstolsstyrelsen.dk

Domstolsstyrelsens høringssvar

Forsvarsministeriet har ved mail af 5. juli 2024 anmodet Domstolsstyrelsen om eventuelle bemærkninger til udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsnivea.

Domstolsstyrelsen har i den anledning følgende bemærkninger:

Af NIS2-direktivets artikel 2, stk. 7, fremgår, at direktivet ikke finder anvendelse på offentlige forvaltningsenheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.

Domstolene ikke er en "offentligt forvaltningsenhed" og dermed allerede af denne grund ikke omfattet af direktivet. Domstolsstyrelsen foreslår, at dette præciseres i forarbejderne til loven, ved at der tilføjes en bemærkning om, at domstolene ikke er omfattet af direktivet.

For så vidt angår lovforslagets anvendelsesområde i forhold til Domstolsstyrelsen, Procesbevillingsnævnet og Ungdomskriminalitetsnævnet foreslår Domstolsstyrelsen, at det fremgår direkte i lovudkastet § 1, stk. 2, eller i forarbejderne hertil, at Domstolsstyrelsen, Procesbevillingsnævnet og Ungdomskriminalitetsnævnet ligeledes er undtaget anvendelsesområdet med henvisning til NIS2-direktivets 2, nr. 8.

På det foreliggende har Domstolsstyrelsen ikke grundlag for at vurdere omfanget af merudgifter for domstolene for så vidt angår udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, idet der for nuværende ikke foreligger en vurdering fra Rigsadvokaten af det forventede antal sager ved domstolene, som lovforslaget vil medføre.

Domstolsstyrelsens vurderer, at lovforslaget vil medføre et øget antal sager ved domstolene, herunder for så vidt angår § 23, stk. 3, jf. § 23, stk. 1, samt det anførte i de almindelige bemærkninger til lovforslaget. Domstolsstyrelsens vurdering af de økonomiske konsekvenser for domstolene må dog afvente Rigsadvokatens skøn over det forventede antal ekstra sager ved domstolene, der er under udarbejdelse.

I lovforslagets afsnit 4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige fremgår det ikke direkte, at der vil være merudgifter ved domstolene. Såfremt det på baggrund af oplysninger fra Rigsadvokaten om det forventede sagsantal viser sig, at lovforslaget har økonomiske konsekvenser på Justitsministeriets, herunder Rigsadvokaten og domstolene, bør det overvejes, at dette tydeliggøres i lovforslaget.

Med venlig hilsen

Laila Lindemark

fmn@fmn.dk
jhb@fmn.dk
trm@trm.dk
cyber@trafikstyrelsen.dk

Sagsnummer 2024/004461

Københavns Lufthavne A/S
Box 74
Lufthavnsboulevarden 6
2770 Kastrup
www.cph.dk

Tlf.: +45 32 31 32 31
Fax: +45 32 31 31 00
E-mail: cph@cph.dk
CVR: 14 70 72 04

København, 22. august 2024

Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

Med henvisning til høringsbrev ønsker DSB og Københavns Lufthavne A/S at afgive et fælles høringssvar til udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau. Sagsnummer 2024/004461.

Bemærkninger er sendt til fmn@fmn.dk med kopi til jhb@fmn.dk, trm@trm.dk og cyber@trafikstyrelsen.dk.

Vi har med interesse læst lovforslaget og har følgende bemærkninger:

Kapitel 6, §21, stk. 1, punkt 2): Vi har gode erfaringer med ISO27001 certificering og audit fra et kvalificeret godkendt organ. Præampelbetragtning 79 i NIS 2-direktivet nævner krav i 27000-serien som mulige foranstaltninger for virksomheder til at kunne opfylde kravene i NIS 2-direktivet. Vi ser fortsat gerne, at vi kan opfylde kravene ved at have en ISO27001 certificering.

Hvis vi fremadrettet også skal have tilsyn foretaget af - eller på foranledning af - Trafikstyrelsen, vil vi foreslå, at Trafikstyrelsen fortsætter med at holde fast i krav om en ISO27001 certificering. At have en certificering er værdiskabende for os som virksomheder og Trafikstyrelsen kan drage nytte af dette i deres planlægning af tilsyn. Så virksomheder med en ISO27001 certificering ikke får en audit eller tilsvarende fra Trafikstyrelsen.

Vi ser frem til den fortsatte dialog i forbindelse med udformning af såvel ressortlovgivning som bekendtgørelse mv.

På vegne af DSB og Københavns Lufthavne.

Med venlig hilsen

Mette Andreasen
Senior IT Compliance Manager

From: Dan Banja <es@es-daa.dk>
Sent: 22-08-2024 08:34:32 (UTC +02)
To: FMN-MYN-Forsvarsministeriet <fmn@1net.fmn.dk>
Cc: FMN-JHB Brams, Jakob Halkjær <JHB@1net.fmn.dk>; Dan Banja <es@es-daa.dk>
Subject: Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau sagsnr. 2024/004461: ES 224-24.
Categories: Amanda

(FMI-CD besked: Denne mail kommer fra Internettet.)

ES 224-24

Erhvervsflyvningens Sammenslutning (ES) takker for muligheden for at deltage i høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

Det noteres, at et nyt EU direktiv 2022/2555 af 14. december 2022 erstatter det tidligere NIS2 direktiv 2018/1972.

Forsvarsministeriet foreslår, at detailudmøntning af NIS2 direktivet uddelegeres til de enkelte ressortministre, hvilket vurderes som en hensigtsmæssig ordning, som ES kan støtte.

NIS2 direktivet omfatter også luftfarten under transport.

Luftfartens SMV med under 50 ansatte og med mindre årlig omsætning end 10 mio. Euro er ikke omfattet af NIS2.

Kommercielle luftfartsselskaber (defineret i forordning EF 300/2008), lufthavnsdriftsorganer (2009/12/EF og EU 1315/2013) og trafikledelse (EF 549/2004) er allerede omfattet af EASA Part-IS.

I lovforslagets punkt. 29 (Udkastets side 29) anføres:

(29) For at undgå huller mellem eller overlapning af cybersikkerhedsforpligtelser, der pålægges enheder i luftfartssektoren, bør nationale myndigheder i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 (11) og (EU) 2018/1139 (12), og de kompetente myndigheder i henhold til dette direktiv samarbejde om gennemførelsen af foranstaltninger til styring af cybersikkerhedsrisici og tilsynet med overholdelsen af disse foranstaltninger på nationalt plan. En enheds overholdelse af sikkerhedskravene i forordning (EF) nr. 300/2008 og (EU) 2018/1139 og i de relevante delegerede retsakter og gennemførelses-retsakter, der er vedtaget i henhold til nævnte forordninger, vil af de kompetente myndigheder i henhold til dette direktiv kunne anses for at udgøre opfyldelse af de tilsvarende krav, der er fastsat i dette direktiv.

Det er ES opfattelse, at dette punkt 29 i NIS2 direktivet muliggør, at myndighederne for luftfarten kan acceptere Part-IS som værende dækkende for NIS2 for at undgå dobbeltlovgivning.

Ved udkastets foreslåede implementering af punkt 29, vil dansk luftfart således undgå dobbeltlovgivning og dermed et ekstra ressourcekrævende arbejde med implementering af NIS2.

ES anmoder om, at dette forhold klarificeres i den kommende lov og i bemærkninger til loven.

Med venlig hilsen / Best Regards
Dan Banja
Oberstløjtnant / Lt. Colonel
Generalsekretær / Secretary-General
Vice-President ECOGAS & Member of GA.CSTG, AG.004 & CA.CSTG
Blålersvej 51
DK-2990 Nivå
Mobil: +45 2480 2256
www.es-daa.dk

FDA FORENEDE DANSKE ANTENNEANLÆG
Danish Cable Television Association
www.fda.dk

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt via mail til fmn@fmn.dk og til jhb@fmn.dk

Højby den 23. august 2024.

Sagsnummer 2024/004461 - Høringssvar – Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS-2).

Kære Jakob Halkjær Brams,

FDA, Forenede Danske Antenneanlæg har ikke fået tilsendt forslaget, men er blevet opmærksom på det og håber, at dette svar kan nå at komme i betragtning i den videre proces, uanset at vi er knapt et døgn for sent på den i forhold til den angivne høringsfrist.

FDA vil udtrykke et enkelt ønske i forhold til forslaget, nemlig at det bliver helt ubetinget klart, i hvilket omfang det brugerejede antenneanlæg skal leve op til de kommende regler og hvad det er for krav, de i givet fald skal leve op til.

Vi har forsøgt at sætte os ind i, hvilket omfang de kommende regler vil være gældende for netop de brugerejede antenneanlæg og dernæst hvad disse regler så konkret vil kræve. Det har helt ærligt været voldsomt svært.

Vi håber således – og opfordrer så stærkt som vi kan til – at reglerne bliver klare.

Samtidig vil vi appellere til, at det indgår i overvejelserne at der findes et betydeligt antal mindre brugerejede antenneanlæg i regi af egentlige antenneforeninger, grundejerforeninger, almene boligafdelinger m.v. Disse anlæg ejes og drives af de tilsluttede brugere i fællesskab i rigtig mange tilfælde af en valgt frivillig og ulønnet bestyrelse i deres fritid og uden ansat personale. Disse anlæg vil have endog meget svært ved at skulle løfte en betydelig administrativ opgave, ligesom de ikke er økonomisk rustet til i noget omfang af betydning at kunne købe sig til at få det løst af andre.

Vi appellerer således så stærkt som vi kan til, at det overvejes om reglerne skal omfatte også de (mindre) brugerejede antenneanlæg.

Med venlig hilsen
FDA, Forenede Danske Antenneanlæg

[afsendt elektronisk uden signatur]
Søren Birksø Sørensen
Sekretariatschef

From: Ragnar Heldt Nielsen <rhn@gts-net.dk>
Sent: 20-08-2024 19:58:34 (UTC +02)
To: FMN-MYN-Forsvarsministeriet <fmn@1net.fmn.dk>
Cc: FMN-JHB Brams, Jakob Halkjær <JHB@1net.fmn.dk>
Subject: SV: Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau
Categories: Amanda

(FMI-CD besked: Denne mail kommer fra Internettet.)

Til Forsvarsministeriet,

I forhold til lovforslag om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2) bemærker GTS-foreningen på vegne af de danske GTS-institutter, at der er et generelt behov for nærmere retningslinjer og vejledning om de krav, der stilles til virksomheder som konsekvens af lovimplementeringen.

Det gælder eksempelvis:
1) Konkretisering af foranstaltningerne oplistet i lovforslagets § 6;
2) Definition af ledelse i lovforslagets § 3 med henblik på at sikre (a) nødvendig træning mv. til en korrekt afgrænset ledelsesgruppe, og (b) korrekt afgrænsning af ansvarssubjekt.

Med venlig hilsen
Ragnar Heldt Nielsen
Direktør

GTS - Godkendt Teknologisk Service
Gregersensvej 1 - 2630 Taastrup
Dir/mob +45 4516 2620
Office +45 4516 2626
rhn@gts-net.dk
Twitter: @ragnarhn
Linkedin profile
www.gts-net.dk

Fra: Forsvarsministeriet <fmn@fmn.dk>
Sendt: fredag, juli 5, 2024 14:20
Til: FMN <FMN@FMN.dk>
Emne: Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Se venligst vedhæftede dokumenter.

FORSVARSMINISTERIET
Holmens Kanal 9, DK-1060 København K
Telefon + 45 72 81 00 00
Fax + 45 72 81 03 00

E-mail: fmn@fmn.dk
www.fmn.dk

22. AUGUST 2024
GREEN POWER DENMARK
LANGEBROGADE 3H
1411 KØBENHAVN K

Forsvarsministeriet
Holmens Kanal 9
1060 København K

DOK. ANSVARLIG: ASB
SEKRETÆR: SLS
SAGSNR.: S2024-669
DOKNR: D2024-2906521-08-2024

Til: fmn@fmn.dk

Cc: jhb@fmn.dk og alg@fmn.dk

Høringssvar til udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (sagsnummer 2024/004461) og forslag til lov om kritiske enheders modstandsdygtighed (sagsnummer 2023/009004)

Green Power Denmark takker for muligheden for at afgive bemærkninger i forbindelse med høring af forslag til hhv. lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau og forslag til lov om kritiske enheders modstandsdygtighed (herefter lovforslagene).

Green Power Denmark anerkender vigtigheden af, at implementering af NIS2- og CER-direktiverne kan være med til at styrke Danmarks sikkerhed og robusthed mod flere og mange forskelligartede trusler.

Energisektoren er af stor samfundskritisk betydning, som går på tværs af forskellige sektorer i Danmark. En række af de sektorer og enheder, der bliver omfattet af de to hovedlove, er meget afhængige af vedvarende energiforsyning og høj leveringssikkerhed. Der er med andre ord tale om en høj grad af gensidig afhængighed mellem forskellige samfundskritiske sektorer. Derudover står Danmark overfor en række komplekse og forskelligartede trusler, som går på tværs af sektorielle grænser. Det er således afgørende, at der sikres en ensartet og konsistent tilgang til den retlige regulering af Danmarks nationale sikkerhed.

Derfor ønsker Green Power Denmark at afgive nogle generelle og mere overordnede bemærkninger til lovforslagene, selvom om energisektoren er reguleret sektorvist under Klima-, Energi- og Forsyningsministeriet, som varetager implementeringen af NIS2- og CER-direktiverne for energisektoren.

Green Power Denmark anbefaler, at myndighederne, herunder klima-, energi- og forsyningsministeren og forsvarsministeren m.fl. benytter opgaven med implementering af NIS2- og CER-direktiverne til i fællesskab og i dialog med repræsentanter fra de samfundskritiske sektorer, herunder repræsentanter fra energisektoren, at afdække sektorernes gensidige afhængigheder.

Green Power Denmark har i høringssvar af 10. juni 2024 afgivet bemærkninger til lovforslag om styrket beredskab i energisektoren, som er sendt i høring af Klima-, Energi- og Forsyningsministeriet. Vores høringssvar er vedlagt som kopi.

Generelle bemærkninger

Green Power Denmark vil særligt fremhæve to overordnede temaer vedrørende implementeringen af NIS2-direktivet og CER-direktivet: 1) Fælles sikkerhed og samordnet beredskab og 2) ensartet og konsistent lovgivning.

Ad 1: Fælles sikkerhed og samordnet beredskab

Green Power Denmark finder det vigtigt, at virksomhederne får mulighed for at kunne samordne deres beredskab. Muligheden for samordnet beredskab ser vi som en anledning til at styrke virksomheders, koncerners og dermed sektorernes beredskabs- og sikkerhedsarbejde, idet mindre organisationer derved vil kunne udnytte synergier på tværs og dermed skabe grundlag for i fællesskab at opbygge (og fastholde) dedikeret beredskabs- og sikkerhedsmæssig kompetence. Energisektoren har historisk god erfaring med at samordne beredskab på tværs af forskellige virksomheds- og forsyningstyper.

Green Power Denmark anmoder derfor om, at ny lovgivning, herunder implementering af NIS2- og CER-direktiverne, ikke ændrer på, men snarere støtter op om, at virksomheder kan indgå i samordnet beredskab. Vi anbefaler samtidigt, at myndighederne balancerer hensynet til, at bekendtgørelser løbende tilpasses som følge af ændrede trusler, teknologisk udvikling o.l., med hensynet til at undgå detailregulering.

Green Power Denmarks anbefaling om samordnet beredskab skal ses i lyset af, at sikkerhed og beredskab ikke bør være konkurrenceparameter. Hvis myndighederne vurderer at reglerne om funktionel adskillelse, herunder også anden konkurrencelovgivning, anses som en hindring for samordnet beredskab, anbefaler vi, at der indledes en tættere dialog med branchen og relevante myndigheder herom.

Green Power Denmark mener tilsvarende, at det bør være en klar myndighedsopgave at udarbejde sektorspecifikke trusselsvurderinger, som er tilstrækkeligt operationaliserbare til, at de omfattede virksomheder kan omsætte dem til konkrete risikoanalyser og -vurderinger i forhold til digitale og fysiske trusler.

Ad 2: Ensartet og konsistent lovgivning

Green Power Denmark appellerer til, at implementering af NIS2- og CER-direktiverne sker ensartet og konsistent på tværs af sektorer. Det er navnlig vores bekymring, at virksomheder, som indgår i flere forskellige sektorer, kan blive mødt med modsatrettede krav og vilkår. En ensrettet implementering kan bl.a. sikres ved:

- Samtidig fremsættelse af lovforslag: Green Power Denmark appellerer til, at fremsættelsen af samtlige hovedlove, der implementerer NIS2-direktivet og CER-direktivet i dansk ret, herunder sektorspecifik implementering, fremsættes for Folketinget som én samlet pakke. Derved sikres, at reglerne på områderne koordineres i nødvendigt omfang, og at der ikke skabes forskellige regler, definitioner og fortolkninger i de forskellige hovedlove. Derudover sikres også en synkron ikrafttræden for alle lovforslag.

- Fælles ikrafttræden for alle hovedlove: Der lægges i lovforslagene op til, at de træder i kraft den 1. marts 2025, hvorimod forslag til lov om styrket beredskab i energisektoren skal træde i kraft den 1. januar 2025. Ikrafttrædelsesdato for lov om cybersikkerhed i telesektoren er fortsat ukendt, da lovforslaget endnu ikke er sendt i høring. Green Power Denmark anbefaler, at alle hovedlove får synkron ikrafttræden qua sektorernes gensidige afhængigheder og risikoen for hybride og tværsektorielle trusler.

- Definitorisk klarhed på tværs af sektorlovgivning: Green Power Denmark finder det afgørende, at der skabes en fælles forståelse for de anvendte begreber og udtryk i lovforslagene, inklusiv sektorspecifik implementering, så der ikke opstår uklarheder i retsanvendelsen, der kan svække forudsigeligheden og de enkelte aktørers retssikkerhed. Green Power Denmark kan f.eks. konstatere, at der eksisterer flere uklarheder og begrebsforskelle mellem lovforslagene og udkast til lov om styrket beredskab for energisektoren. Green Power Denmark opfordrer til, at Forsvarsministeriet i samarbejde med relevante ressortministerier sikrer en definitorisk og terminologisk harmonisering af begreber, herunder at der kontrolleres for overlappende begreber.

- Nye bekendtgørelser: Green Power Denmark imødekommer, at sektorvise bekendtgørelser udstedes efter forhandling med forsvarsministeren for at sikre en ensartethed. Vi vil, som i tilfældet med hovedlovene, appellere til, at de forskellige sektorvise bekendtgørelser sendes i høring samtidigt, så det er muligt for de berørte sektorer at danne sig et samlet indtryk af deres indbyrdes sammenhænge og evt. forskelle qua sektorernes gensidige afhængigheder og risikoen for hybride og tværsektorielle trusler. Vi imødeser ligeledes, at de sektorvise bekendtgørelser træder i kraft på samme tid.

Bemærkninger til udkast til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Green Power Denmark har følgende bemærkninger til udkast til foranstaltninger til sikring af et højt cybersikkerhedsniveau:

- Detailregulering af IKT-produkter, -tjenester og -processer: Der lægges i lovforslaget op til, at en ressortminister efter forhandling med forsvarsministeren fastsætter regler for at sikre beskyttelsen af net- og informationssystemer og regler om anvendelse af særlige IKT-produkter, -tjenester og -processer. Green Power Denmark er bekymret for, at tekniske detailkrav risikerer at begrænse teknologisk udvikling og virksomhedernes brug af ny teknologi eller vil kræve omfattende og omkostningstunge tilpasninger af eksisterende anlæg og systemer.

  Vi er tilsvarende bekymrede for, at der kan stilles krav om brug af særlige IKT-produkter, -tjenester og –processer, uden at det synes nærmere beskrevet, hvad som potentielt ligger heri. Herunder også sikkerhed og

dokumentation for, at der reelt er leverandører, som kan og vil tilbyde disse særlige produkter, tjenester og processer, samt prisen herfor. Dette rejser også spørgsmålet om omkostningsdækning ved krav om indkøb og brug af særlige IKT-produkter, herunder forceret udskiftning af nuværende komponenter, anlæg og systemer.

- Strengere nationale krav: Green Power Denmark er ligeledes bekymret for, at der indføres nationale krav om geografisk placering af systemer, medarbejdere og leverandører, herunder brug af cloud, som ikke er afstemt på EU-niveau. Nationale krav risikerer at pålægge virksomhederne endog meget store ekstraordinære omkostninger som konsekvens af myndighedspålagte ændringer af allerede indgåede kontrakter og serviceaftaler samt eksisterende filialer og driftsorganisationer uden for Danmarks grænser.

- Differentieret reguleringstryk: Det fremgår af bemærkningerne til lovforslaget side 155, at en enhed, som har aktiviteter i flere sektorer, i sin helhed vil skulle anses for en væsentlig enhed, hvis enheden i én af sektorerne lever op til kriterierne for at være en væsentlig enhed. Det rejser et principielt og generelt spørgsmål om, hvilke kriterier og procedurer der forventes at blive fastsat i det tilfælde, at den kompetente myndighed finder det nødvendigt at rykke en virksomhed fra ét niveau til et andet, herunder også i hvilket omfang dette kan ske, fordi virksomheden leverer en (væsentlig) tjeneste til en identificeret enhed i en anden kritisk sektor – og omvendt.

- Sikker kommunikation: Green Power Denmark er bekymret for, om kravet i lovforslagets § 6, stk. 10, til sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer - både til sektorintern kommunikation og til kommunikation med andre sektorer og til myndigheder, reelt kan forventes at være tilgængeligt og muligt i en omfattende krise på grund af sektorernes gensidige afhængigheder.

- CSIRT: Vi noterer os, at der i lovforslagets § 17, nr. 3, lægges op til, at virksomheder indenfor de samfundskritiske sektorer har mulighed for at anmode den nationale CSIRT (i praksis Center for Cybersikkerhed) om "… at foretage en proaktiv scanning af enhedens net- og informationssystemer, der anvendes til levering af enhedens tjenester, for at opdage sårbarheder med en potentielt væsentlig indvirkning." Vi støtter, at virksomheder i energisektoren også får adgang til denne mulighed for anmodning om proaktiv scanning. Proaktive scanninger bør dog alene ske efter gensidig aftale og dialog med den pågældende virksomhed.

- Undtagelse fra aktindsigt og fortrolighed: Det bør sikres, at resultater og konklusioner af sikkerhedsscanninger og eventuelle penetrationstest er undtaget for muligheden for aktindsigt, idet der er tale om sensitive oplysninger, som kan anvendes til skade for en virksomhed.

  Det fremgår desuden af lovforslagets § 16, at myndighederne kan informere offentligheden om væsentlige hændelser. Vi anbefaler i denne

sammenhæng, at landets sikkerhedsmyndigheder, herunder Politiets Efterretningstjeneste (PET) og Forsvarets Efterretningstjeneste (FE), inddrages i drøftelserne og i en risikovurdering af, hvilke data og informationer der skal beskyttes og behandles som fortrolige, og hvilke data og informationer der kan offentliggøres.

- Håndhævelsesforanstaltninger: Det fremgår af lovforslagets § 23, at tilsynsmyndigheden har mulighed for at fastsætte en frist, inden for hvilken en enhed skal foretage nødvendige tiltag for at afhjælpe manglerne eller opfylde den kompetente myndigheds krav. Bestemmelsen kan anvendes, hvor de relevante foranstaltninger anses for at være *"utilstrækkelige"*. Green Power Denmark har noteret, at Forsvarsministeriet derved bevidst har valgt at afvige fra den danske oversættelse af NIS2-direktivet, der anvender kriteriet "virkningsløse". Det bør genovervejes, hvorvidt det mere subjektive begreb "*utilstrækkelige*" i paragraffen bør erstattes med det mere objektive begreb "ineffektive", idet der er en nuanceforskel, der medfører, at lovforslagets brug af "utilstrækkelige" forekommer at være en skærpelse. Der henvises i øvrigt til, at den svenske oversættelse af direktivet anvender ordet "*ineffektiva*", dvs. uden virkning, ligesom den tyske oversættelse ligeledes har valgt en direktivkonform implementering ved brug af ordet "*unvirksam*". Alternativt bør kriteriet "*utilstrækkelige*" uddybes og afgrænses i lovbemærkninger for at sikre en klar retsanvendelse samt retssikkerhed for de berørte aktører.

- Suspension af certificering- eller godkendelsesordninger: Det fremgår af bemærkningerne til lovforslaget, at Forsvarsministeriet ser et behov for at foretage et nærmere analysearbejde for at klarlægge, om der er ordninger, som bør være omfattet af den af direktivet foreskrevne mulighed for at suspendere certificering- eller godkendelsesordninger. Green Power Danmark opfordrer til, at Forsvarsministeriet deler yderligere oplysninger om, hvorvidt arbejdet er igangsat, og om muligheden for at foretage suspensioner vil omfatte alle samfundskritiske sektorer.

- "Security by design": "Security by design" er et velkendt teknisk koncept, der sikrer, at cybersikkerhed er en integreret del af soft- og hardwareudvikling. Green Power Denmark mener, at "security by design" tilsvarende bør indtænkes som et grundlæggende princip, der skal tages højde for, når der reguleres på cybersikkerhedsområdet. For eksempel finder vi det bekymrende, at lovforslaget lægger op til, at visse enheder skal oplyse IP-intervaller. En systematisk indsamling af IP-intervaller for de samfundskritiske sektorer i Danmark og på tværs af EU er i vores optik en meget bekymrende tendens. Selv om IP-intervaller er relativt offentligt tilgængelig information, kan en kompromittering af denne systematisk indsamlede information potentielt få vidtrækkende konsekvenser og misbruges i de forkerte hænder. En systematisk indsamling bør derfor kun ske på baggrund af en risikovurdering holdt op imod, hvilket formål og hvilken sikkerhedsmæssig gevinst en indsamling vil have for den enkelte sektor og for Danmarks sikkerhed.

- Ledelsesbegrebet: Det er vigtigt, at begrebet ledelsesorgan, der bl.a. anvendes i tilknytning til §§ 6-7 defineres og afgrænses, så det er klart, hvilke ledelsesroller og funktioner begrebet dækker over, herunder om bestyrelsen er omfattet. Ledelsesbegrebet skal desuden være entydigt, også i koncernsammenhænge.

- Midlertidig rettighedsfrakendelse: Det er en ganske vidtgående beføjelse, som den kompetente myndighed ifølge lovforslaget tildeles. På dette punkt synes lovforslaget at gå klart videre end NIS2-direktivets artikel 32, stk. 5, litra b. Et indgreb af denne karakter forudsætter en særskilt prøvelse med de nødvendige retssikkerhedsmæssige garantier. En sådan rettighedsfrakendelse bør af samme grund ske via domstol eller domstolslignende organ.

Bemærkninger til udkast til lov om kritiske enheders modstandsdygtighed

Green Power Denmark har følgende bemærkninger til udkast til lov om kritiske enheders modstandsdygtighed:

- Baggrundskontrol og sikkerhedskontrol: Der lægges i lovforslaget op til, at kritiske enheder skal sikre passende medarbejdersikkerhedsstyring, herunder baggrundskontrol, jf. de foreslåede § 6, stk. 5 og §9. Green Power Denmark efterlyser generelt mere klarhed over, hvilke virksomheder som forventes at skulle foretage baggrundskontrol og søge sikkerhedsgodkendelse af medarbejdere, og til hvilket sikkerhedsniveau disse nøglemedarbejdere vil skulle godkendes til. Vi savner også mere klarhed over, hvordan der mellem myndigheder og virksomheder i de enkelte sektorer, men også på tværs af sektorer, aftales en procedure for, hvordan en virksomhed kan verificere, at én person er sikkerhedsgodkendt, samt en procedure for, at virksomheder med sikkerhedsgodkendte medarbejdere og/eller leverandører informeres, hvis myndighederne trækker en sikkerhedsgodkendelse af en medarbejder tilbage. Dette skal igen ses ud fra sektorernes gensidige afhængigheder og risikoen for hybride og tværsektorielle trusler.

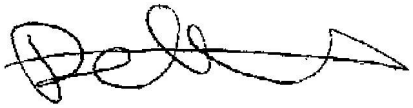
- Kritiske enheder af særlig europæisk betydning: Green Power Denmark anbefaler, at virksomheder i energisektoren, der er identificeret som kritisk virksomhed efter den foreslåede § 4, stk. 1, har pligt til at oplyse den kompetente myndighed om, at virksomheden leverer de samme eller lignende tjenester til eller i seks eller flere medlemsstater. Dette krav fremgår på nuværende tidspunkt ikke af lovforslag om styrket beredskab i energisektoren, jf. denne lovs foreslåede § 5, stk. 2.

Green Power Denmark står naturligvis til rådighed for evt. spørgsmål til vores bemærkninger til lovforslagene. I er velkomne til at kontakte chefkonsulent Asbjørn Thranov, asb@greenpowerdenmark.dk eller undertegnede, Peter Kjær Hansen, pha@greenpowerdenmark.dk.

Afslutningsvis appellerer og opfordrer vi til en fortsat tæt dialog i forbindelse med den kommende proces med udarbejdelse af de beredskabs- og sikkerhedsbekendtgørelser, som følger med implementering af de forskellige hovedlove.

Med venlig hilsen

Green Power Denmark



Peter Kjær Hansen
Afdelingschef, Netanalyser & Asset Management

IDA
Kalvebod Brygge 31-33
DK-1780 København V
Tlf. +45 33 18 48 48

ida.dk

Forsvarsministeriet
fmn@fmn.dk
jhb@fmn.dk

Høringssvar til forslag til Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

21. august 2024

Hermed IDAs svar på forslag til Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau. Mange tak for muligheden for at kommentere på lovforslaget, der har til formål at implementere NIS2-direktivet.

IDA er overordnet meget positive overfor direktivet, der har til formål at sikre et højere og ensartet niveau af cybersikkerhed blandt virksomheder og offentlige institutioner i Europa. Dette er nødvendigt og nye og ekstra tiltag er afgørende for, at Europa kan fungere effektivt digitalt.

Lovforslaget vil, som følge af kravene i direktivet, være en udfordring for virksomheder og myndigheder, både økonomisk og i forhold til at sikre de rette kompetencer til at følge kravene i lovgivningen. Når IDA støtter lovforslaget på trods af udfordringen, er det fordi, at Danmark er et digitalt land og det er vores overbevisning, at de konsekvenser, tab og omkostninger, økonomiske som menneskelige, der kan føre af den stigende risiko for cyberkriminalitet, overbelastningsangreb og hackerangreb m.v. vil risikere at blive endnu større. Derudover vil implementeringen af NIS2 være med til at hæve opmærksomhedsniveauet, kompetenceniveauet og de tekniske løsninger i det danske samfund generelt og dermed også være med til at styrke forebyggelsen af it-kriminalitet m.v.

Men det bør tænkes ind, at loven skal være så let som mulig at efterleve, ligesom den skal implementeres effektivt. IDA anbefaler derfor:

At retningslinjerne og bekendtgørelser bliver så klare og lette at forstå som muligt, så der ikke overimplementeres eller at virksomheder og institutioner ender med at opgive digitaliseringsinitiativer, som ellers kunne være gavnlige.

At der hurtigst muligt udarbejdes konkrete vejledninger i forlængelse af bekendtgørelserne fra de enkelte ressortministerier. Vejledninger kan evt. henvise til ISO 27002 eller D-mærket.

At det sikres, at de relevante myndigheder, der skal vejlede og føre tilsyn med implementeringen af loven, har de nødvendige ressourcer.

Det fremgår af høringsmaterialets almindelige bemærkninger, kap. 5, s. 183 i materialet, at der ikke på nuværende tidspunkt er et fuldt overblik over, hvor mange danske virksomheder, der vil blive omfattet af forslaget, men at det indledende forventes at være omkring 2000. Det vurderes også, at ca. 150 af disse virksomheder allerede er omfattet af NIS 1-direktivet. En nærmere vurdering af, hvem de resterende virksomheder er, vil iflg. teksten blive defineret bl.a. af de kommende sektorspecifikke bekendtgørelser.

Det er vigtigt for IDA at påpege, at Danmark som bekendt allerede er bagud i forhold til at skulle være klar når NIS2 træder i kraft. Det må derfor understreges, at der er behov for hurtigst muligt at få meldt ud til de enkelte virksomheder, hvem der er omfattet. Der findes allerede en række kurser og vejledninger fra bl.a. IDA og D-mærket, men vi oplever også en vis tøven og usikkerhed fra virksomheder, der er i tvivl om de er omfattet og hvor meget de skal investere i at blive klar. I den bedste af alle verdener burde alle virksomheder og offentlige organisationer leve op til NIS2, men realiteten er, at det kræver investeringer i tid, efteruddannelse og i nogle tilfælde konsulentbistand. Det er derfor ikke hensigtsmæssigt, at de pågældende virksomheder og offentlige organisationer ikke får klar besked meget hurtigt.

Endelig undrer det, at kommunerne som udgangspunkt holdes udenfor loven og kun vil blive omfattet i det omfang, de udfører opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, jf. §4, f.eks. indenfor sundhedstjenesteydelser (s.203, bemærkninger til §1).

Kommunerne udgør en vital del af samfundets digitale infrastruktur på f.eks. sundhed, affald, vandforsyning m.v. og ligger inde med enorme mængder følsomme persondata. Det virker mere fornuftigt at kommunerne som udgangspunkt er omfattet, men at fast definerede områder indenfor kommunernes virke evt. bliver undtaget.

IDA finder det dog positivt, at der forventes at blive fastsat tværgående regler for kommuner og regioner i det omfang kommunerne måtte

være omfattet (s. 219, bemærkninger til §4). IDA er på baggrund af erfaringerne fra implementeringen af GDPR af den overbevisning, at kommunerne vil have brug for klare fælles retningslinjer.

Derudover har IDA disse specifikke kommentarer:

Jf. §1, stk. 6: IDA finder det positivt, at offentlige og private enheder, der ikke er omfattet af lovens område, frivilligt kan underrette CSIRT og deltage i den frivillige udveksling af oplysninger efter §19. Jo bedre overblik, der kan udarbejdes over trusler og hændelser, jo mere effektiv kan der forebygges og hjælpes.

Jf. §§4 og 5: IDA enig i definitionen mellem væsentlige og vigtige enheder.

Jf. §7: IDA er enig i, at medlemmer af ledelsesorganer i både vigtige og væsentlige enheder skal deltage i relevante kurser i styring af cybersikkerhedsrisici og overveje at tilbyde tilsvarende kurser til sine ansatte.

Jf. §10: IDA finder det positivt, at enheder, der leverer tjenester i flere sektorer, kun vil skulle foretage én samlet registrering via en fælles digitale indgang. Dette er en god hjælp til at gøre efterlevelsen af NIS2 lettest mulig.

Jf. § 12 stk. 2: IDA er enig i definitionen af, at en hændelse anses for væsentlig når:
1) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller
2) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.
IDA finder det positivt, at væsentlige og vigtige enheder kan melde hændelser ind som én samlet underretning via en fælles digital indgang. Dette er med til at gøre efterlevelsen af NIS2 lettest muligt.

Jf. § 13: IDA noterer sig tidsfristerne for underretninger af væsentlige hændelser, jf. § 12, som beskrevet stk. 1 – 4 og i afsnit 102 i NIS2-direktivet. Det er afgørende, at systemet for underretninger fungerer optimalt og er så ligetil og hurtigt at bruge. IDA anbefaler, at der evalueres efter en periode på 1 eller 2 år, så mulighederne for underretning evt. kan rettes til og optimeres.

Jf. § 14: IDA finder det positivt, at offentlige og private enheder kan underrette CSIRT'en om hændelser, nærvedhændelser og cybertrusler.

Det er vigtigt for en fremtidig indsats for at sikre det højest mulige niveau af cybersikkerhed, at der findes et samlet overblik over hændelser og trusler, der er så komplet som muligt.

Jf. §§ 17-19: IDA er enig i CSIRT'ens opgaveformulering. IDA understreger, at det er vigtigt, at CSIRT'en har de nødvendige ressourcer til at yde bistand og hjælpe væsentlige og vigtige enheder ved hændelser. IDA anbefaler, at der evalueres på CSIRT'ens opgaveløsning efter 2-3 år for at optimere og evt. tilrette ressourcetilførslen.

Jf. § 23-25: IDA er enig i de nævnte muligheder for at afhjælpe mangel på opfyldelse af myndighedernes krav i hhv væsentlige og vigtige enheder.

Med venlig hilsen

Grit Munk
Digitaliseringspolitisk chef
IDA

Høringssvar fra Industriens Fond til lovforslag om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2)

Industriens Fond takker for muligheden for at afgive bemærkninger til lovforslaget.

Først og fremmest bakker vi op om nødvendigheden af at styrke cybersikkerheden i Danmark, hvilket der er stort behov for. Der er rigtig mange gode tiltag i lovforslaget, herunder de opstillede foranstaltninger, som – hvis implementeret ordentligt – vil kunne løfte cybersikkerheden i det danske samfund betydeligt.

Det er i den sammenhæng afgørende, at krav og kriterier bliver klare og gennemskuelige at navigere efter som virksomhed. Der lægges i lovforslaget op til, at "Væsentlige og vigtige enheder skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene...". Dette er på mange måder en fornuftig tilgang grundet virksomhedernes forskelligheder, men det kan imidlertid være meget vanskeligt for virksomhederne at vurdere, hvornår noget er 'passende' og 'forholdsmæssigt' og dermed tilstrækkeligt.

Der er derfor behov for hurtigst muligt at stille handlingsorienteret hjælp og vejledning til rådighed for virksomhederne. I den forbindelse vil vi opfordre til, at man fra de relevante ministeriers side benytter sig af etablerede værktøjer. Industriens Fond har over de seneste år udviklet en række tilbud, som kan være relevante i implementeringen af NIS2. Det gælder fx Bestyrelsesforeningens Center for Cyberkompetencers initiativer rettet mod at styrke cyberkompetencer blandt virksomhedernes topledelse og bestyrelsesmedlemmer: https://industriensfond.dk/projekt/styrkelse-af-strategiske-cyberkompetencer/ og https://bcfc.dk/.

Derudover er der D-mærket (https://www.d-maerket.dk/), som er skabt af DI, DE, SMVdanmark og Forbrugerrådet TÆNK og er en mærkningsordning, der har fokus på it-sikkerhed, datasikkerhed og dataetik. Samtidig er mærkets kriteriesæt bygget op, så det er tilpasset virksomhederne, hvilket taler ind i lovforslagets tilgang med passende og forholdsmæssige foranstaltninger. D-mærket er ved at udvikle et specifikt NIS2-modul, og et samarbejde mellem D-mærket og de ansvarlige myndigheder vurderes oplagt. De D-mærkede virksomheder kommer fra alle sektorer, men særligt de NIS2-underlagte sektorer har vist interesse for mærket den seneste tid.

I og med, at lovforslaget ikke lægger op til, at der fra offentligt hold udpeges, hvilke virksomheder der er omfattet, foreslås det, at der i et offentligt-privat samarbejde udvikles en form for værktøj, der hjælper virksomhederne med denne afklaring.

Industriens Fond gennemførte i 2023 en kortlægning af, hvor mange virksomheder der så ud til at blive omfattet af NIS2, hvor langt de var i implementeringen, og hvad de havde behov for at hjælp og vejledning, se https://industriensfond.dk/vores-fokusomrader/cybersikkerhed/nis2/. I alt 16 brancheorganisationer og myndigheder deltog i arbejdet. Fonden stiller sig gerne til rådighed for dialog ift., hvordan NIS2-

direktivet gennem den rette hjælp til virksomhederne kan blive en reel løftestang for cybersikkerheden i Danmark.

Forsvarsministeriet

Att.: Jakob Halkjær Brams
Holmens Kanal 9
1060 København K

Sendt pr. mail til fmn@fmn.dk med kopi til jhb@fmn.dk

Jeres ref.: Vores ref.: Kundenr.: Dato: 06-08-2024
Sagsnummer 2024/004461.

Høring – FMN – Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

ITD takker for muligheden for at afgive et svar på høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, som er planlagt til at træde i kraft den 1. marts 2025. ITD har følgende generelle bemærkninger til høringen.

ITD støtter generelt op om sikring af et højt niveau af cybersikkerhed og om et ensartet cybersikkerhedsniveau på tværs af medlemsstaterne. Net- og informationssystemer spiller en afgørende rolle i samfundet, og både virksomheder, myndigheder og borgere er i høj grad afhængige af digitale systemer i hverdagen. Digitalisering leder dog til en høj grad af sårbarhed, hvor nedbrud, systemsvigt, menneskelige fejl, svindel, tyveri, afpresning, spionage og sabotage kan få alvorlige konsekvenser for virksomheder og samfundet generelt.

ITD finder det positivt, at der i Danmark er valgt en minimumsimplementering af NIS2-direktivets krav. Selv med denne tilgang estimeres det, at de omkring 2.000 virksomheder, som kan blive omfattet af direktivet, vil skulle bruge 22-25 % af deres nuværende omkostninger til it-sikkerhed på at omstille sig til kravene i NIS2-direktivet.

Som udgangspunkt synes kun få medlemmer af ITD at være omfattet af NIS2's bilag II (transportvirksomheder, som er beskæftiget med post- og kurertjenester, affaldshåndtering, distribution af kemikalier eller distribution af fødevarer) og dermed at blive direkte omfattet af reglerne i lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau. Men vi forventer, at lovgivningen på sigt vil medføre lignende krav til disse vigtige enheders underleverandører.

ITD bemærker dog, at der synes at være en vis usikkerhed om, præcist hvilke virksomheder der bliver omfattet af reglerne. Det gælder også ved de forskellige myndigheder. Der bør skabes mere klarhed over, hvilke virksomheder der bliver omfattet indenfor de forskellige sektorer, og det er vigtigt, at myndighederne også kan hjælpe virksomhederne med at afklare, hvorvidt de er omfattet.

Af høringen fremgår, at der vil være flere ressortministerier i Danmark, og at deres ministre på visse områder bemyndiges til at fastsætte regler i bekendtgørelser. ITD ser visse fordele ved opsplitning på ressortministerier, men vi er også bekymrede for, om myndighedernes kompetencer inden for cybersikkerhed udvandes.

Vi finder det derfor særdeles vigtigt, at der sikres tilstrækkeligt med ressourcer centralt i Center for Cybersikkerhed. Center for Cybersikkerhed bør ikke bare bistå med i videst muligt omfang at skabe et fælles cybersikkerhedsniveau på tværs af de omfattede sektorer, men i særdeleshed bistå med kompetencer, ressourcer og vejledning, for herved at understøtte udvikling og vedligehold af et højt cybersikkerhedsniveau hos danske virksomheder og myndigheder.

ITD opfordrer til, at det overvejes, om myndighederne, som angivet i CER-direktivets artikel 10, via lovgivning bør forpligtes at støtte enheder med at styrke deres cybersikkerhedsniveau ved f.eks. at udvikle vejledninger og metoder, støtte til tilrettelæggelse af øvelser for at afprøve deres modstandsdygtighed, og rådgivning og uddannelse af personale i enheder i f.eks. andre kritiske sektorer.

ITD har følgende bemærkninger til indholdet i de enkelte paragraffer:

Uddannelse
Ad § 7, stk. 2.: ITD støtter kravet om, at medlemmerne af en væsentlig eller vigtig enheds ledelsesorgan skal deltage i relevante kurser om styring af cybersikkerhedsrisici og overveje at tilbyde tilsvarende kurser til deres ansatte.

ITD opfordrer til, at sådanne kurser blandt andet tilbydes som online kurser, så de er lettilgængelige, hvad tid og sted angår. Vi opfordrer til, at Center for Cybersikkerhed løbende publicerer anbefalinger til relevante temaer, som virksomhedslederen og virksomhedens ansatte bør komme på kursus i.

Som en sidebemærkning undrer vi os i øvrigt over ordet ”overveje”. Måske skulle der i § 7, stk. 2 stå ”bør”.

Underretningspligter og frivillig underretning
Væsentlige og vigtige enheder skal uden unødigt ophold underrette den relevante kompetente myndighed og CSIRT om enhver væsentlig hændelse. En underretning skal indeholde oplysninger, der gør det muligt at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

Det fremgår af høringsmaterialet, at Center for Cybersikkerhed kommer til at varetage opgaven som cyberkrisestyringsmyndighed, CSIRT og centralt kontaktpunkt. Center for Cybersikkerhed har allerede i dag til opgave at koordinere operative opgaver i tilfælde af cyberangreb mod og på tværs af samfundskritiske sektorer.

En hændelse anses for at være væsentlig, hvis:

1) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller
2) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.

ITD opfordrer til, at der etableres effektive og funktionsdygtige metoder til underretning af CSIRT, og at der samtidig kan trækkes på ekspertisen hos Center for Cybersikkerhed. Proceduren for underretning i lovens § 13 synes omstændelig, og særligt punkt 4 (endelig rapport) synes at være bagudskuende.

ITD frygter, at rapporten blot bliver en administrativ byrde for virksomheden, især hvis ikke den anvendes i forbindelse med hjælp her og nu samt til forebyggende indsats i forhold til virksomheder, der risikerer at opleve lignende hændelser.

Målet er netop at forebygge hændelser, og ikke at pålægge yderligere administrativt arbejde. For at kunne opnå dette mål, må det også afspejle sig i reglerne. Risikoen er ellers, at omfattede enheder tvinges til administrativt arbejde alene for reglernes skyld, og ikke med henblik på at undgå hændelser. Dette vil være kontraproduktivt.

CSIRT's opgaver
ITD er tilfreds med, at Center for Cybersikkerhed varetager funktionen som CSIRT og håndterer it-sikkerhedshændelser. For virksomheder vil det som oftest være af stor betydning at få kompetent rådgivning, hjælp og monitorering af enhedens net- og informationssystemer ud fra en risikobaseret tilgang.

ITD finder det positivt, at CSIRT efter anmodning fra en væsentlig eller vigtig enhed forventes at foretage en proaktiv scanning af enhedens net- og informationssystemer, der anvendes til levering af enhedens tjenester, for at opdage sårbarheder med en potentielt væsentlig indvirkning.

ITD finder det positivt, at CSIRT sikrer, at fysiske og juridiske personer i anonymiseret form kan rapportere om sårbarheder.

Tilsyn og håndhævelse
Det vil påhvile de relevante ressortministerier at oprette eller udpege kompetente myndigheder med ansvar for cybersikkerhed og ansvar for at føre tilsyn med de enkelte sektorer.

ITD er bekymret for, om disse ressourcer anvendes mest effektivt, og om der er de nødvendige kompetencer hos myndigheder til at føre tilsyn med vigtige enheder. Med det sparsomme antal af it-uddannede personer i Danmark, så appellerer vi til, at disse anvendes særdeles hensigtsmæssigt.

ITD opfordrer til, at disse ressourcer især anvendes til forebyggelse ved at vejlede og rådgive virksomheder frem for at sanktionere virksomhederne, bl.a. ved midlertidigt at suspendere topledere i enhederne eller udstede bøder.

Efter NIS2-direktivets artikel 34, stk. 5, skal vigtige enheders overtrædelser af direktivets artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser) straffes med et maksimum på mindst 7.000.000 euro eller på mindst 1,4 % af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den vigtige enhed tilhører, alt efter hvad der er højest.

I forhold til sanktioneringen skal ITD bemærke, at fokus først og fremmest bør være på at vejlede virksomhederne til at sikre en bedre cybersikkerhed, og ikke på at kunne udstede store bøder. I de tilfælde, der sanktioneres, bør der ses på de konkrete omstændigheder og under hensyntagen til, om

virksomheden har forsøgt at overholde reglerne samt sikre sig bedst muligt. Der bør tages hensyn til, at der er tale om et kompliceret regelsæt. Fokus ved sanktioneringen bør derfor primært være på virksomheder, som bevidst ignorerer at sikre sig.

Med venlig hilsen

ITD

Camilla Wiig
Chefkonsulent

IT-BRANCHENS HØRINGSSVAR TIL UDKAST TIL LOV OM FORANSTALTNINGER TIL SIKRING AF ET HØJT CYBERSIKKERHEDSNIVEAU

UDARBEJDET I REGI AF IT-BRANCHENS
POLICY BOARD FOR CYBERSIKKERHED

IT·BRANCHEN

IT-Branchen har modtaget Forsvarsministeriets udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveauet (herefter NIS2-lovudkastet) i høring. Af nærværende høringssvar fremgår vores bemærkninger til NIS2-lovudkastet.

Generelle bemærkninger

IT-Branchen vil gerne kvittere for muligheden for at kommentere på det foreliggende danske NIS2-lovudkast, som tydeligt hviler på et omstændeligt lovarbejde, og som i udgangspunktet lægger op til et fornuftigt NIS2-implementeringsniveau i Danmark, selvom de nærmere NIS2-sektorkrav stadig udestår.

Dog vil det være afgørende for en hurtig og effektiv implementering af NIS2-kravene, at NIS2-loven hurtigst muligt følges op af sektorbekendtgørelser og konkret hjælp og vejledning til virksomhederne. Virksomhederne bør i den forbindelse også kunne rette henvendelse til en sektoransvarlig myndighed og modtage et klart og bindende svar på, om de er omfattede af NIS2.

Hvad angår kommunerne, mener IT-Branchen, at de utvetydigt bør omfattes af NIS2, og at dette eksplicit bør fremgå af NIS2-loven.

Endelig savner IT-Branchen nogle klare hegnspæle i NIS2-lovudkastet for CFCS' ansvarsområde og opgaver som CSIRT og en præcisering af snitfladerne til og samarbejdet med de private cybersikkerhedsaktører. CFCS står overfor en markant større, overordnet CSIRT-opgave end tidligere, som der kan sættes spørgsmålstegn ved, om centret har de nødvendige ressourcer til at løfte, og som alt andet lige ikke kan løftes uden omfattende involvering af private aktører.

Vores bemærkninger uddybes i det følgende.

Specifikke bemærkninger

Minimumsimplementering og sektorbekendtgørelser

Der lægges med NIS2-lovudkastet op til en minimumsimplementering af NIS2-direktivet, og lovudkastets krav om foranstaltninger til styring af cybersikkerhedsrisici gengiver, jf. §6, NIS2-direktivets artikel 21 uden uddybelser. IT-Branchen ser frem til, at de konkrete krav til virksomhedernes cybersikkerhed præciseres i sektorbekendtgørelserne udarbejdet af de relevante ressortmyndigheder i samarbejde med FMN/CFCS.

IT-Branchens input:

- ➔ Det præciseres ikke i NIS2-lovudkastet, men IT-Branchen henstiller til, at bekendtgørelserne – ligesom NIS2-hovedloven – træder i kraft pr. 1. marts 2025, og at bekendtgørelserne *inden* ikrafttrædelsesdatoen og hurtigst muligt suppleres af konkrete vejledninger til virksomhederne fra de relevante sektoransvarlige myndigheder, så virksomhederne får de bedst mulige betingelser for rettidigt at efterleve NIS2-lovkravene.
- ➔ Henset til betydningen og kompleksiteten af indholdet i de kommende sektorbekendtgørelser henstiller IT-Branchen til, at den vejledende høringsfrist på fire uger som minimum overholdes og også gerne forlænges, hvilket ikke altid er praksis.
- ➔ Såfremt sektorbekendtgørelserne og de præciserende vejledninger ikke tilgængeliggøres inden NIS2-lovens ikrafttræden, bør de sektoransvarlige myndigheder indledningsvis anlægge et dialogbaseret og vejledende tilsyn og ikke gøre brug af deres sanktionsbeføjelser, før de NIS2-omfattede enheder har haft passende mulighed for at sætte sig ind i samt implementere de nærmere sektorlovkrav. Til det formål vil vejledninger og konkrete eksempler på bedste praksis – og ikke blot bekendtgørelser – være nødvendige for at understøtte de omfattede enheder i regelefterlevelsen. Til inspiration ift. konkretiseringsniveau har vi i IT-Branchens eget NIS2-vejledningsunivers listet en række konkrete, tekniske minimumsforanstaltninger, der varierer afhængigt af vurderet risikoprofil.
- ➔ Som et af de vigtigste, første fokusområder skal der tilvejebringes vejledning, der kan hjælpe omfattede enheder med en kritikalitetsvurdering – dvs. hjælp og vejledning til at vurdere, hvilken del af en enheds forretning, der ud fra en risikovurdering kan have betydning for anmeldelse af sikkerhedshændelser. Herved opnås en væsentlig forståelse til at sikre en unødig overimplementering af NIS2 i danske virksomheder.

- ➔ Herudover efterlyser IT-Branchen – i NIS2-lovudkastet og generelt – en detaljeret oversigt over de forskellige sektoransvarlige myndigheder, som de danske virksomheder kan modtage vejledning fra og rette henvendelse til med tvivlsspørgsmål.

Ikrafttrædelsesdato 1. marts 2025

Jf. §33 i NIS2-lovudkastet træder loven i kraft den 1. marts 2025, lidt over fire måneder efter NIS2-direktivets implementeringsfrist.

IT-Branchens input:

- ➔ IT-Branchen finder det uhensigtsmæssigt, at vi i Danmark ikke overholder NIS2-direktivets implementeringsfrist, og at vedtagelsen af den danske NIS2-lov endnu engang udskydes. Det sender et uheldigt signal – også til de cyberkriminelle – om, at cybersikkerheden ikke tages alvorligt i Danmark, og at vi nedprioriterer området.
- ➔ IT-Branchen forudser i henhold til art. 26 stk. 2, at danske virksomheder, der – foruden Danmark – opererer i eller leverer tjenesteydelser til NIS2-omfattede virksomheder i andre EU-lande, hvor den nationale implementeringslovgivning ikke bliver forsinket i samme omfang som i Danmark, kan risikere at være omfattet af jurisdiktionen i andre lande end Danmark i perioden frem til den 1. marts 2025. Det er således uklart, hvilket lands lov der gør sig gældende, og hvad der sker med jurisdiktionsbestemmelsen for omfattede enheder under de i §2 stk. 3-identificerede områder, så længe vi ikke har en vedtaget NIS2-lov i Danmark.
- ➔ For at undgå udfordringer og uklarheder som de ovenfor beskrevne – også på sigt – er det ifølge IT-Branchen vigtigt, at Danmark bidrager aktivt til en konsekvent harmonisering af NIS2-reglerne på tværs af EU-medlemslandene.
- ➔ For at sikre ensretning og effektiv implementering på tværs af sektorer på nationalt plan, vil det tilsvarende være vigtigt, at de særskilte cybersikkerhedsreguleringer i fx energi- og telesektorerne – der skal tilpasses NIS2-kravene – i videst muligt omfang fremsættes, behandles og træder i kraft på samme tid og parallelt med NIS2-loven og de relaterede sektorbekendtgørelser.

Omfattede enheder og registreringspligt

Det fremgår af §9, at det påfalder "*DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder der leverer domænenavnsregistreringstjenester og udbydere af cloudcomputing-tjenester, datacentertjenester, indholdsleveringsnetværk, administrerede tjenester, administrerede sikkerhedstjenester, onlinemarkedspladser, onlinesøgemaskiner og platforme for sociale netværkstjenester*" selv at registrere sig hos den relevante, kompetente myndighed. Af §9 stk. 2 følger det, at registreringen skal ske senest den 17. januar 2025.

IT-Branchens input:

- ➔ Det er IT-Branchens overbevisning, at det på det eksisterende tekstgrundlag i NIS2-lovudkastet vil blive vanskeligt for mange danske enheder/virksomheder at vurdere, om de er omfattet af NIS2 og proaktivt bør lade sig registrere hos den relevante, kompetente myndighed. Særligt de mange ny-omfattede enheder, der følger af et markant udvidet anvendelsesområde sammenlignet med NIS1, vil blive udfordret.
- ➔ For at undgå ovenstående uklarhed/uvished – og en medfølgende tilbageholdenhed i virksomhederne ift. at gå i gang med at styrke cybersikkerhedsniveauet – foreslår IT-Branchen følgende tiltag:
    - Hurtig tilvejebringelse af konkret vejledningsmateriale og hjælp til enheder/virksomheder med at vurdere, om de er omfattet af NIS2
    - Hurtig identificering og offentliggørelse af de sektoransvarlige myndigheder, hvorfra virksomheder kan modtage vejledning og rette henvendelse med tvivlsspørgsmål (jf. tidl. input i nærværende høringssvar)
    - Etablering af en instans/funktion i hver enkel "relevant kompetent myndighed", hvor virksomheder løbende kan henvende sig og modtage klart og bindende svar på, om de er omfattet af NIS2. Som inspiration kunne man etablere en ordning, som anvendes inden for skatteområdet, hvor der kan indhentes bindende svar fra myndighederne.
- ➔ IT-Branchen finder det desuden problematisk og juridisk uholdbart, at registreringen til relevante kompetente myndighed ifølge lovudkastet skal ske senest den 17. *januar* 2025 – det vil sige 1,5 måned *inden,* der er en vedtaget NIS2-lov at falde tilbage på. Kan der være tale om, at datoen fejlagtigt er videreført fra NIS2-direktivet, og at man ikke har indregnet den danske lovforsinkelse? Af §10 stk. 2 følger det, at domæneregistreringstjenester skal registrere sig senest den 17. *april* 2025.

Kommunerne

Det fremgår af §1 stk. 7, at vedkommende minister inden for sit område kan fastsætte regler om, at loven helt eller delvist også finder anvendelse på henholdsvis offentlige forvaltningsenheder på lokalt plan og uddannelsesinstitutioner. Det fremgår videre af bemærkningerne til §1, at det på nuværende tidspunkt ikke er intentionen at fastsætte regler om, at kommunerne omfattes af loven.

IT-Branchens input:

- ➔ IT-Branchen er indforstået med, at NIS2-direktivet giver medlemslandene mulighed for selv at vurdere og bestemme, om direktivet skal finde anvendelse på offentlige forvaltningsenheder på lokalt plan, såfremt disse ikke leverer tjenester i kritiske sektorer, som omfatter dem via direktivets anvendelsesområde. IT-Branchen mener imidlertid, at kommunerne utvetydigt bør omfattes af NIS2, og at dette eksplicit bør fremgå af den danske NIS2-lov. For at imødegå cybertruslen og værne om vores samfundssikkerhed, er der behov for, at de offentlige myndigheder lever op til en række skærpede og mere ensartede cybersikkerhedskrav på tværs af stat, regioner og kommuner. Hertil vil NIS2-loven være en kærkommen løftestang til at hæve cybersikkerhedsniveauet i kommunerne. Cybersikkerheden i kommunerne er vital for at bevare borgernes tillid til systemerne og for at sikre opbakning til de effektive, digitale løsninger, der er nødvendige for kritiske, kommunale velfærdsydelser og den gode borgerservice. I yderste konsekvens kan det store antal cyberangreb mod kommunerne, som KL har identificeret (hver fjerde kommune rammes dagligt af over 200 forsøg på angreb), risikere at kompromittere eller skade de samfundsvigtige funktioner, som kommunerne har ansvaret for.
- ➔ I forlængelse af ovenstående finder IT-Branchen det nødvendigt, at NIS2-loven præciserer, hvordan og hvor meget kommunerne er omfattet, så der ikke kan opstå uklarheder eller fortolkningstvivl (fx ift. det at være sundhedstjenesteyder), og så ingen kommune kan undslå sig at være omfattet af NIS2. Der skal videre skabes klarhed omkring, hvad det har af betydning ift. ansvarspådragelsen, når kritiske tjenester og velfærdsydelser udliciteres i kommunerne mv. IT-Branchen noterer sig også, at KL selv har ytret ønske om, at kommunerne omfattes af NIS2.
- ➔ Af §4 stk. 2 fremgår det, at kommuner og regioner omfattes af loven i det omfang, de måtte udføre opgaver som udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester. IT-Branchen henstiller til,

at det præciseres og eventuelt eksemplificeres, hvilke typer af sådanne kommunikationsnet og -tjenester i kommunalt og regionalt regi, der her henvises til.

Risikovurdering

§6 i NIS2-lovudkastet angiver, at væsentlige og vigtige enheder skal træffe en række "passende" og "forholdsmæssige" tekniske, operationelle og organisatoriske minimums-foranstaltninger til styring af cybersikkerhedsrisici.

IT-Branchens input:

- ➔ IT-Branchen vil gerne påpege vigtigheden af, at proportionaliteten af de angivne minimumsforanstaltninger tager udgangspunkt i en samlet risikovurdering, der også indebærer de *samfundsmæssige* og *økonomiske* indvirkninger af en hændelse. Derfor foreslås det, at andet led/afsnit i Artikel 21 stk. 1 i NIS2-direktivet tilføjes i starten af §6 i den danske NIS2-lov, ligesom første led/afsnit i Artikel 21 stk. 1 i NIS2-direktivet allerede er gengivet i starten af §6. Det manglende led lyder: *"Under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne skal de i første afsnit omhandlede foranstaltninger tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning."* Leddet er gengivet i betragtningerne til §6 nederst på side 229, men der må ikke lovgives i betragtningerne, hvorfor det bør være en del af selve lovteksten.

Underretningspligter og frivillig indberetning

§12,13, 14, 15, 16.

IT-Branchens input:

- ➔ IT-Branchen undrer sig over, at det kun er frivillige indberetninger af hændelser under §14, som er undtaget aktindsigt. De almindelige indberetninger som følge af §12 er ikke undtaget aktindsigten. Dette bør genovervejes, eller også bør man som minimum begrænse aktindsigten i de almindelige indberetninger under §12, da der allerede under databeskyttelsesreglerne har været hændelser, hvor der af Datatilsynet er givet

aktindsigt i sager, hvor dette har skadet efterforskningen og skabt problemer for de omfattede organisationer.

- ➔ Af §16 fremgår det, at myndighederne kan vælge at offentliggøre væsentlige hændelser, hvis det er nødvendigt for at forebygge og håndtere andre hændelser, eller hvis det er i offentlighedens interesse. Dette skal ifølge NIS2-udkastet fornuftigvis ske efter høring af den pågældende enhed, men IT-Branchen efterlyser, at det nærmere præciseres, hvornår/hvor hurtigt en hændelse kan offentliggøres – fx om der vil være tilstrækkelig tid til, at den pågældende enhed kan have håndteret hændelsen – eller hvor lang høringen af den pågældende enhed kan/vil være.
- ➔ IT-Branchen efterlyser en utvetydig melding om, hvem underrettelsespligten påfalder i tilfælde, hvor leverandører er involveret, og hvorvidt tidsrammen gælder fra det tidspunkt, den NIS2-omfattede enhed bliver opmærksom på hændelsen, eller fra det tidspunkt enhedens leverandør bliver det. Her savner vi sondring mellem eksempelvis "data processor" og "data controller" som kendt fra GDPR.
- ➔ For at lette de administrative omkostninger for erhvervslivet og fremme den generelle indberetning, vil det være vigtigt, at der faciliteres én indberetning/indgang/formular – også for væsentlige og vigtige enheder, der er beskæftiget i mere end én af de NIS2-omfattede sektorer (à la Virk.dk i dag).

CFCS som CSIRT

Center for Cybersikkerhed (CFCS) skal ifølge NIS2-lovudkastet varetage rollen som CSIRT. Af §17-19 følger CSIRT'ens opgaver.

- ➔ IT-Branchen henstiller til, at CFCS' ansvarsområde og opgaver som CSIRT præciseres yderligere i NIS2-loven, herunder ikke mindst hvad angår snitfladerne til og samarbejdet med de private cybersikkerhedsaktører. Med et markant øget anvendelsesområde sammenlignet med NIS1 – og et estimeret antal omfattede enheder i Danmark, der stiger fra 130 til 2.000 – vil der blive tale om en markant større, overordnet opgave for en CSIRT end tidligere, som der kan sættes spørgsmålstegn ved, om CFCS har de nødvendige ressourcer til at løfte, og som alt andet lige ikke kan løftes uden omfattende involvering af private aktører. Der er ydermere behov for nogle klare hegnspæle for en offentlig CSIRT's aktiviteter i NIS2-loven, så der ikke opstår unfair konkurrence og skævvridning af det private marked. Endelig vil det være væsentligt for de NIS2-omfattede enheder at få klarhed over, hvad der forventes løftet af en offentlig CSIRT, og hvornår og hvordan der henvises til hjælp fra private aktører.

Tilsyn og håndhævelse

IT-Branchen finder det positivt, at lovudkastet lægger op til en fælles tilgang til tilsyn og en tæt koordinering mellem de forskellige sektoransvarlige myndigheder – særligt for at tilgodese enheder, der indgår i forskellige sektorer - med mulighed for fælles tilsynsbesøg og deling af tilsynsressourcer/-sekretariater på tværs af ressortmyndigheder.

IT-Branchens input:

- ➔ Der henvises i NIS2-lovudkastet til et forestående analysearbejde – og det foreslås, at vedkommende ressortminister bemyndiges til at fastsætte nærmere regler i bekendtgørelsesform – men IT-Branchen efterlyser en præcisering af, hvilke certificeringer og godkendelser der kan blive genstand for suspension ved manglende NIS2-regelefterlevelse. Samtidig er det i NIS2-lovudkastet ikke beskrevet, om/hvordan en midlertidig suspension vil have opsættende virkning, hvis suspensionen påklages til en rekursmyndighed, eller der anlægges en sag ved domstole.

Øvrige, tekstnære bemærkninger

- ➔ Definitionen på side 231 af, hvilke net- og informationssystemer, der er omfattet ud fra en betragtning af, hvordan de kan påvirke enhedens levering af de tjenester eller aktiviteter, som er baggrunden for at enheden er omfattet af direktivet, bør fremhæves og gøres til en del af de fleste vejledninger, da den manglende forståelse af dette skaber forvirring mange steder.
- ➔ På side 255 nævnes muligheden for at DCIS'erne kan komme med tilbagemeldinger på indberetning af hændelser. Hvis dette skal være en mulighed, bør det så ikke fremgå mere tydeligt af lovteksten, at DCIS'erne kan spille en myndighedsrolle i forhold til implementeringen af direktivet i dansk lovgivning?
- ➔ På side 280 står der, at væsentlige enheder vil blive underlagt "*løbende tilsyn*". Dette bør uddybes eller konkretiseres, således at det er tydeligt om dette fx betyder at alle væsentlige enheder skal underlægges mindst et tilsyn om året.
- ➔ Af artikel 32 stk. 4 litra g fremgår det at den kompetente myndighed kan udpege en overvågningsansvarlig, men på side 282 (og § 22 punkt 5) fremgår det, at den kompetente myndighed kan opbyde enheden at udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med enhedens overholdelse af §§ 6, 12, 13, 15

og 16, samt regler udstedt i medfør heraf. Det virker som om, der ikke helt er sammenhæng mellem direktivets tekst og lovens tekst på dette punkt.

På vegne af IT-Branchen og IT-Branchens Policy Board for Cybersikkerhed,

Med venlig hilsen

Troels Johansen
Chefkonsulent
IT-Branchen
Mobil: 9384 9383
Mail: tjoh@itb.dk

Torsdag den 22. august 2024

Til Forsvarsministeriet

Emne: Høringssvar vedr. Udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Ref.: Sagsnr.: 2024/004461

Forsvarsministeriet, der er ressortsansvarlig for at omsætte EU's NIS2 direktiv til dansk lov, har den 5. juli sendt lovforslaget i høring med frist den 22. august 2024, kl. 12.

Loven forventes først at skulle træde i kraft den 1. marts 2025, længe efter EU's fastsatte deadline. Så det kan undre, at høringen skal hastes igennem. Forsvarsministeriet har selv taget sig mere end god tid til udarbejdelse af lovudkastet.

Lovforslaget er på 325 sider. På CFCS's hjemmeside, er formålet med NIS2-direktivet anført til yderligere at styrke og ensarte cybersikkerheden og modstandsdygtigheden overfor cybertrusler på tværs af EU for virksomheder inden for en lang række sektorer og for offentlige myndigheder, som anses for at være kritiske for økonomien og samfundet.

Med NIS2 indføres således en række nye krav til at omfatte virksomheder og myndigheder. NIS2 stiller bl.a. krav om gennemførelse af cybersikkerhedsforanstaltninger, hændelsesrapportering samt giver styrkede tilsyns- og håndhævelsesbeføjelser.

Lovudkastet har været længe undervejs og i flere omgange blevet udsat på grund af sagens kompleksitet og sværhedsgrad, som Troels Lund Poulsen formulerede det ved den sidste af flere udsættelser.

Forsvarsministeriet har haft mere end god tid til at formulere lovudkastet, idet det formelle EU NIS2 direktiv allerede i december 2022 forelå i fuld færdig form hos alle medlemslandene og selvsagt også Forsvarsministeriet.

Også flere år forinden 2022 var Forsvarsministeriet involveret i de første udkast til NIS2 direktivet, men har først nu – ca. 4 år senere fremkommet med lovforslaget. Sagsbehandlingstiden må derfor anses for kritisabelt, den alvorlige sikkerhedspolitiske situation taget i betragtning, med mange daglige hybride angreb, herunder cyberangreb og angreb på kritisk infrastruktur.

I øvrigt vil hverken energi-, finans- og telesektorerne blive omfattet af NIS2-hovedloven. Implementeringen af NIS2-direktivet vil ske særskilt for hver af disse sektorer. Og Energisektoren har allerede sendt sin eget lovudkast i høring, uafhængigt af FM-lovudkastet.

Så ønsket om en hovedlov der kunne samle Danmark til en samlet kamp mod de cyberkriminelle, herunder stjæle befolkningens penge og destabilisere vores samfundet, ses ikke tilgodeset med den forventede lov Forsvarsministeriet ønsker vedtaget.

Forsvarsministeriet er sat til at koordinere og styre implementeringen af NIS2-direktivet. Men i praksis overlades det til andre ministerier og styrelser at udarbejde sektorvise bekendtgørelser, der er alt det praktiske og besværlige, og som kommer til at koste mange penge. Penge der skal findes i egne budgetter på bekostning af andre vitale områder, der må nedprioriteres. De mange penge bevilget til området beholder Forsvarsministeriet, FE og CFCS selv.

Mange konsulenthuse og advokatfirmaer er allerede kontaktet af virksomheder, myndigheder og andre, der har brug for hjælp. For de skal lige om lidt efterleve og i al hast implementere de krav direktivet og loven fastsætter. Lovudkastet afslører, et usammenhængende og fragmenteret produkt, der skaber mere usikkerhed end klarhed.

Der udestår en række ubesvarede spørgsmål og uklarheder. F.eks., hvorledes er en sektorvis fragmentering (energi, tele, finans) af implementeringen af NIS-2 i dansk lovgivning forenelig med en samlet og sammenhængende implementering, centreret i en overordnet lov omfattende i det mindste Danmark, men principielt for hele rigsfællesskabet?

Foreligger der forud for fragmenteringen i foreløbigt to lovforslag (CER og NIS2) vedrørende implementeringen af EU-direktiverne en aftale mellem energistyrelsen og forsvarsministeriet om den herved etablerede praksis?

Har der forud for den sektorvise fragmentering af implementeringen af EU-direktiverne været konsultationer mellem forsvarsministeriet og regeringens sikkerhedsudvalg, subsidiært statsministeriet?

Der kan og bør i det hele taget stilles spørgsmålstegn ved hensigtsmæssigheden, i at FE og CFCS er sat til at være ansvarlige myndigheder for arbejdet med det nationale kompetencecenter for cybersikkerhed, der rådgiver myndigheder og virksomheder for at styrke cybersikkerhed.

Det skal i den forbindelse bemærkes, at det var FE og CFCS, der i 2012 formåede at tildele sig opgaver de to institutioner selv syntes de burde løse uden en egentlig forudgående demokratisk dialog eller involvering af Folketinget. Allerede fra starten gik det således galt.

Det er ikke nok at rådgive og komme med vejledninger, som det sker nu. Det har de mange næsten dagligt forkomne og alvorlige cyberangreb vist. Det er ikke blevet bedre i de 13 år, hvor CFCS har eksisteret. Nærmest tværtimod. Så det anses ikke for nogen god idé at sætte dem til at være den overordnede instans, der skal kunne hjælpe andre. CFCS formår ikke engang at sikre egne interne instanser mod angreb og trusler, hvilket er dokumenteret i en række tilfælde.

I stedet for råd og formaninger burde FE og CFCS sørge for, at de mange alvorlige cyberangreb slet ikke fik fodfæste, og satte alle ressourcer og ekspertise ind på i tide at opdage, inddæmme og neutralisere angrebene før de gør skade. Det sker bare ikke.

Råd og henvisninger er i orden, men det er de ovennævnte opgaver, der er brug for at blive løst samt centerets oplysning, videndeling og information om det lykkes og hvordan. Alt det andet (råd og henvisninger) er en gratis omgang, der endog fremgår bedre og i rigelige mængder, i åbne kilder.

Det er på høje tid og ikke et øjeblik for tidligt, at der tages hånd om Danmarks mangelfulde indsats for cybersikkerhed og beskyttelse af samfundsvigtig og kritisk infrastruktur, og at der findes løsninger på udfordringerne hurtigst muligt - hellere i dag end i morgen.

Situationens alvor og problemerne skyldes primært et politisk svigt i forhold til samfundet, hele befolkningen og den enkelte borger. De løsninger der de sidste 10-15 år er benyttet har spillet fallit og kan ikke længere bruges. .

Cybertruslerne og de mange dagligt forekommende angreb bliver der kun flere af til trods for et hav af bestemmelser og love, der spyttes ud i en lind strøm fra EU, Folketinget og Forsvarsministeriets side. Lige meget har det hjulpet. Efterlevelse af reglerne koster kassen i den helt store stil, men pengene er stort set spildt og hældes ned i et stort sort hul uden at gøre gavn. Loven ses ikke at ville kunne afhjælpe problemet. Nærmest tværtimod.

F.eks **steg antallet af ransomwareangreb med 74 procent** sidste år på globalt plan. Det viser tal fra Cyber Threat Intelligence Integration Center (CTIIC). I Danmark føres der ikke statistik eller tal over de mange angreb, men alle kan i medierne dagligt læse om brud på sikkerheden, eksempler på cyberangreb af alvorlig karakter og firmaer der må gå neden om og hjem. Offentlige myndigheder, institutioner, kommuner, regioner og mange andre går det også stærkt ud over.

Indsatsen og kampen mod de formastelige og banditterne i cyberspace er fragmenteret og ustruktureret, selvom politikerne og myndighederne kontinuerligt forsøger sig med mere lovgivning, strengere regler og bekendtgørelser, der har vist sig nytteløse.

Tiden er kommet og ”long overdue”, til at oprette en civil myndighed, der ligesom i Sverige, Norge og Finland, bedre kan varetage samfundets og befolkningens interesser samt ve og vel, når det kommer til at beskytte og afhjælpe angreb på samfundsvigtig kritisk infrastruktur og alvorlige cyberangreb, der går ud over civilbefolkningen.

Det kan og må ikke overlades til en militær organisation, der de sidste 20 år beviseligt har svigtet befolkningen, og gør det igen med dette lovudkast. Lad militæret få ro til at opbygge det nedslidte forsvar og overlad opgaven med samfundssikkerhed og beredskab, herunder cybersikkerhed, til en civil instans/myndighed.

Det kan gøres billigt, hurtigt og effektivt ved at samle allerede eksisterende og spredte styrelser og myndigheder m.fl. under en hat. Der kunne spares mange ressourcer og midler, der kunne gøre større gavn andet sted, i stedet for som nu, at forsætte den hidtidige praksis med at overlade opgaven og ansvaret til Forsvarsministeriet, FE og CFCS. De magter det ikke.

Det foreliggende lovudkast ses således ikke at kunne forbedre samfundets krav på bedre cybersikkerhed og beskyttelse af samfundsvigtig kritisk infrastruktur.

J. M.Foley, Seniorrådgiver It- og Cybersikkerhed, Dalgas Boulevard 85, st.tv. Frederiksberg

Forsvarsministeriet
Att.: fmn@fmn.dk
(Cc: jhb@fmn.dk)
Sagsnummer: 2024/004461

Dato: 22. august 2024

Sags ID: SAG-2022-00167
Dok. ID: 3485542

E-mail: MJT@kl.dk
Direkte: 3370 3214

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Opfordring til at inddrage kommunerne helt i en mere ambitiøs gennemførelse af NIS2 på cybersikkerhed - Høringssvar KL

KL kvitterer hermed for muligheden for at kommentere på forslaget til Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, der anviser den nationale implementering af NIS2-direktivet.

Det er vigtigt, at samfundet fungerer dér, hvor det møder borgerne. Derfor finder KL, at kommunerne bør omfattes af NIS2. Det er samfundskritisk, at de borgervendte opgaver, som kommunerne varetager, får samme beskyttelse som øvrige samfundskritiske funktioner ift. cybertrusler. Kommunerne leverer hver dag service og velfærdsydelser til borgere og virksomheder. Alle opgaver er digitalt understøttede, og digitalt sammenkoblede, dermed er kommunal service sårbar overfor cybertrusler og -kriminalitet.

Kritiske opgaver er fx monitorering af KOL-patienter i eget hjem, livsnødvendige skærmbesøg fra kommunale sygeplejersker, hjemmepleje og støtte til ældre i eget hjem, support af borgernes brug af "MitID", afvikling af valg osv. Kommunerne er en digitalt understøttet arbejdsplads for over 400.000 medarbejdere.

KL finder ikke, at en sektoropdelt tilgang til national cyberbeskyttelse duer. Kommunerne er bl.a. sat i verden for at løse opgaver på tværs af sektorskel til gavn for borgeren. Det tager regeringens oplæg til NIS2 implementering ikke højde for. Derfor finder KL ikke, at oplægget til beskyttelse af Danmark mod cybertrusler rammer plet. Det duer ikke at efterlade de borgernære services uden den nødvendige fælles beskyttelse. Det er ikke hensigten med loven, men vil blive konsekvensen. Nedenfor uddybes dette.

Sørg for at borgernære opgaver beskyttes
NIS2-direktivet er udformet, så hvert EU-medlemsland skal tilrettelægge gennemførelsen efter egne forhold for at få høj og ensartet cybersikkerhed. KL mener, at det er utilstrækkeligt at henvise til, at man vælger en minimumsimplementering. Det skal vurderes, hvilket niveau af cybersikkerhed der er nødvendigt, og hvordan det så skal sikres indenfor direktivet.

Det undrer KL, at de borgernære samfundsopgaver i kommunerne ikke som udgangspunkt omfattes. Regeringen har valgt, at kommuner ikke er omfattet som myndigheder, men at fagministerierne kan omfatte

Dato: 22. august 2024

Sags ID: SAG-2022-00167
Dok. ID: 3485542

E-mail: MJT@kl.dk
Direkte: 3370 3214

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

kommunerne på enkelte opgaver i sektor-bekendtgørelser. Sektortilgangen er uhensigtsmæssigt af flere årsager:

- Der er øget risiko for, at krav bliver modstridende
- Forskelligartede krav vil lede til mere omfattende implementering end oplægget til en minimumsimplementering og vil dermed give unødvendigt forøgede omkostninger og bureaukrati.
- Det er uhensigtsmæssigt at skille den kommunale digitale infrastruktur i flere dele og opbygge parallelle systemer. Det er fordyrende og en barriere ift. de opgaver kommunerne varetager. Det vil svække sammenhængen i opgaveløsningen og flytte fokus fra at højne cybersikkerhed til snævert fokus på investering i at opsplitte it og opgaveområder for at honorere sektorkrav, der peger i flere retninger.

KL finder, at det af hensyn til samfundssikkerheden er nødvendigt, at kommunerne i helhed omfattes af NIS2. Det stiller øgede krav til kommunerne, men det er nødvendigt, for at imødekomme de trusler vi står overfor.

Sektortilgang er en udfordring for sikkerheden
Udover at kommunerne bør omfattes samlet af NIS2, finder KL, at der er brug for, at der udarbejdes én samlet og tydelig vejledning til krav til kommunerne. Vejledningen skal sikre, at sektorkrav ikke er en udfordring for sikkerheden, ved at specificere, hvilke foranstaltninger der skal træffes i kommunerne, hvilke ledelsesmæssige forpligtigelser og ansvar det medfører, samt hvordan og af hvilken myndighed der førers tilsyn med kommunerne.

KL indgår gerne i dialog om udarbejdelse af bekendtgørelser og vejledninger til kommunerne.

Sørg for et samlet tilsyn
I lovforslaget lægges der op til, at tilsynsopgaven varetages af sektorministerier. Dvs. de kommunale myndigheder risikerer at møde forskellige og potentielt modstridende krav fra forskellige tilsynsmyndigheder. Dette er uhensigtsmæssigt og vil give ekstra administration i kommunerne. I lovbemærkninger åbnes der for tæt koordination mellem ministerierne om tilrettelæggelsen af tilsynsarbejdet, så der kan anlægges en fælles tilgang. Dette er positivt, men KL finder, at der er brug for én tilsynsmyndighed for kommunerne, så der er ét samlet og koordineret tilsyn med kommunerne.

Det skal desuden stå helt klart, hvor kommunernes egen opgave og ansvar ender, og tilsynets krav tager over. Erfaringerne med uklarhed er mange fra implementeringen af f.eks. GDPR. Det bør ikke gentages.

Lovgivningen udsendes tæt på ikrafttrædelsesdatoen. Bekendtgørelser og vejledninger er endnu ukendte, derfor opfordrer KL til, at der gives god tid til indfasning og tydeliggørelse af krav, inden tilsynet går i gang med tilsynsarbejde.

Ifølge lovforslaget skal kommunerne kunne ifalde bøder. KL henstiller, at tilsynene pålægges i første omgang at udstede påbud. Såfremt påbud ikke efterleves, kan bøder overvejes.

Dato: 22. august 2024

Sags ID: SAG-2022-00167
Dok. ID: 3485542

E-mail: MJT@kl.dk
Direkte: 3370 3214

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

CSIRT og øvrige opmærksomhedspunkter
Lovforslaget indeholder beskrivelse en CSIRT'ens rolle. Direktivet indeholder klare beskrivelser af, at Danmark skal etablere en CSIRT, der kan vejlede og stille konkret hjælp til rådighed bl.a. ved angreb. KL opfordrer til, at den national CSIRT pålægges disse opgaver, så kommunerne og andre myndigheder får adgang til vigtig information og kan bidrage med egen viden og dermed bidrage til den samlede cybersikkerhed i Danmark. Endelig er det ikke klart hvilke kommunale opgaver, der er sikret finansiering til, og det kræver en afklaring ift., om det er kommunerne, der skal iværksætte de nødvendige foranstaltninger hver for sig eller i fællesskab.

KL stiller sig til rådighed ift. drøftelser og opklarende spørgsmål i den kommende proces og efterfølgende udarbejdelse af bekendtgørelser mv. Lydhørhed overfor kommunalt input vil gøre Danmark mere robust ift. at modstå cyberangreb imod borgernære opgaver og borgernes tillid og tryghed.

./. I vedlagte bilag er konkrete spørgsmål til lovteksten og enkelte af ovenstående argumenter uddybes.

Med venlig hilsen

Pia Færch
Kontorchef, KL

NOTAT

Bilag – til KLs høringssvar til hovedlov om NIS2

Dato: 22. august 2024

Sags ID: SAG-2022-00167
Dok. ID: 3485618

E-mail: MJT@kl.dk
Direkte: 3370 3214

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

I dette bilag stilles konkrete spørgsmål til lovteksten og gives uddybning af enkelte af KLs overvejelser og opfordringer ift. den forslåede implementering af NIS2.

Alternativ til sektortilgang
Det undrer, at der så stor forskel på det, der anbefales i lovteksten og det der angives i bemærkningerne til loven. Lovteksten angiver, at det er kommunale opgaver, der vil blive omfattet, men ikke hele kommunen. Men i lovbemærkningerne fremgår det på forskellig vis, at hvis dele af en enhed (her en kommune) omfattes af direktivet, så bliver den samlede enhed omfattet. Det fremgår f.eks. i høringsmaterialet på side 155: ” *Forsvarsministeriets opfattelse, at en enhed, som har aktiviteter i flere sektorer, i sin helhed vil skulle anses for en væsentlig enhed, såfremt enheden i én af sektorerne lever op til kriterierne for at være en væsentlig enhed*.”.

Det fremgår også af lovbemærkningerne, at kommuner der overstiger tærsklen for mellemstore-virksomheder skal opfattes som væsentlige enheder jf. side 220: ”*I tilfælde hvor en kommune eller region måtte overskride tærsklerne for at være en mellemstor virksomhed, vil enheden være at betragte som en væsentlig enhed i medfør af den foreslåede bestemmelse i § 4, stk. 1*.”

KL indgår gerne i dialog om, hvordan kommunerne omfattes, og hvordan det kan afgrænses, men undres over at kommunerne ikke er omfattet som organisationer.

En ambitiøs og understøttende rolle til national CSIRT
I lovforslaget lægges der op til, at Center for Cybersikkerhed (CFCS) bliver national CSIRT. I direktivet er der opstillet høje krav til en national CSIRT. Ift. disse ser det ud til, at der udestår en klar og ambitiøs definition af de opgaver som CSIRTen skal løfte over for omfattede enheder. Det er pt. uklart, om CSIRT vil kunne udføre rådgivning, vejledning, reaktionsbistand i tilstrækkelig grad som beskrevet i direktivet artikel 11, i forbindelse med hændelser, samt kunne facilitere cybersikkerhedsfællesskaber for alle enheder. Det er KLs forståelse, at det er netop dette, der er intentionen med CSIRT’en.

KL og kommunerne indgår gerne i dialog om, hvordan snittet mellem CSIRT og kommunal sektor lægges så, kommunerne kan stå samlet og koordineret og dermed indgå i effektivt samarbejde med CSIRT om de vigtigste prioriteter. KL mener, at kommunernes adgang til information om aktuelle trusler, sårbarheder og angreb er afgørende for, at kommunerne aktivt kan bidrage til den samlede cybersikkerhed i Danmark. Dette ligger efter KLs opfattelse som en del af CSIRT beskrivelsen i direktivet.

Dato: 22. august 2024

Sags ID: SAG-2022-00167
Dok. ID: 3485618

E-mail: MJT@kl.dk
Direkte: 3370 3214

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Økonomi
Et styrket cyberforsvar forudsætter investeringer i at opnå og opretholde et højt og ensartet niveau for cybersikkerhed. KL noterer sig, at der i bemærkningerne til Hovedloven er forventning om udgifter i kommunerne på 95-280 mio. kr. Niveauet vil i den foreslåede sektor-tilgang afhænge af indholdet i efterfølgende sektorbekendtgørelser. KL kvitterer for, at det anerkendes, at kommunerne pålægges udgifter. Det fremgår dog ikke af lovforslaget, hvad midlerne forventes anvendt til. Det er derfor ikke muligt at vurdere, om de i tilstrækkelig grad dækker omkostningerne til de opgaver kommunerne forventes pålagt. Udgifterne ved at implementere NIS2 i den kommunale sektor vil fordele sig på de enkelte kommuner. KL finder, at midler til kommunal cybersikkerhed desuden skal kunne puljes til fx etablering af fælleskommunalt cyberværn.

Strafansvar for offentlige myndigheder
KL finder ikke, at ministeren skal have hjemmel til at fastsætte regler om bøder til kommuner i videre omfang end straffelovens § 27, stk. 2, giver mulighed for. Det er KL's opfattelse, at den meget grundige behandling af spørgsmålet om bødeansvar til offentlige myndigheder, som er blevet foretaget af straffelovrådet (betænkning fra 1995 (nr. 1289)), ikke på ny skal tilsidesættes med så sparsom argumentation som i nærværende lovudkast. Grundlæggende bør offentlige myndigheder ikke pålægges bøder og i hvert fald ikke uden forudgående advarsel.

Kommunernes rolle ift. telesektoren
Der kan være behov for at genoverveje, hvordan kommunerne betragtes ift. telesektoren. Kommunerne er ikke-kommercielle aktører og dermed ikke i traditionel forstand en "udbyder". Kommunerne kan som led i deres opgaver overfor borgerne stille services og ydelser til rådighed, uden at kommunen agerer kommercielt: Jf. lovforslaget side 6, § 4. stk. 2. "*I det omfang kommuner eller regioner måtte udføre opgaver som udbydere af offentlige elektroniske kommunikationsnet eller udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, og er af en størrelse, der svarer til tærsklerne for mellemstore virksomheder, anses de for at være væsentlige enheder*."
Det vil være uheldigt, hvis f.eks. offentlig WiFi på biblioteker og i borgerservice vil være en teleydelse, der er omfattet af NIS2, hvor kommunen sidestilles med en teleudbyder. Det vil medføre unødigt bureaukrati at tilbyde denne service fremadrettet, og kan lede til at kommunerne stopper at tilbyde dette. Det kan gå ud over de allersvageste borgere i Danmark, der har behov for at finde netadgang via kommunernes tilbud. Det er uklart om dette har været hensigten og hvad begrundelsen er.

Gråzoner på bl.a. forsynings- og trafikområdet
I høringssvaret opfordrer KL til at gå væk fra sektor-tilgangen. Nedenfor gives eksempel på uhensigtsmæssigheder inden for en del af kommunens opgaver mhp. at udfolde problemstillingen. Tilsvarende vil sektor-opdeling ift. sundhed, omsorg, genoptræning og ældre mv. blive kunstig ift. kommunernes opgaver og it-understøttelse.
Kommunerne har inden for teknik & miljøområdet en række opgaver med relation til sektorer, der står anført i direktivet som værende væsentlige områder, bl.a. vand, affald, veje/transport og forsyning. Kommunerne har

historisk været tættere inde på disse opgaver, der nu i vidt omfang er selskabsgjort og varetages af forskellige selskabstyper med større eller mindre relation til kommunerne, hver for sig eller som sammenslutninger. En række af disse opgavers tilknytning til "hjemkommune(r)" vil variere på tværs af kommunerne pga. kommunale forskelle i infrastruktur og geografi (bl.a. ift. transportområdet).

KL finder, at der er kompleksitet, der kan blive håndteret forskelligt af de enkelte sektorministerier. I det omfang reguleringen udlægges fuldstændigt til sektorministerierne vil det brede perspektiv og prioritering ift. fælles og national samfundskritikalitet kunne stå i skyggen af et fagligt betinget fokus på at holde hele sektoren kørende eller at have mindre fokus på, hvordan infrastruktur eller forsyning kan have afgørende betydning ift. andre sektorer (fx tilgængelighed af rent vand i sundheds- og plejesektor). Dermed er der risiko for, at nationale beslutninger på tværs bliver mindre effektive eller slet og ret ikke kan gennemføres. De nuværende uklarheder i modellen for gennemførelse af NIS er uhensigtsmæssigt for så store og vigtige dele af det danske samfund.

Dato: 22. august 2024

Sags ID: SAG-2022-00167
Dok. ID: 3485618

E-mail: MJT@kl.dk
Direkte: 3370 3214

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

KOMBIT A/S
Halfdansgade 8
2300 København S

Tlf. +45 33 34 94 00
kombit@kombit.dk
www.kombit.dk

CVR-nr.: 19435075
EAN-nr. 5790001969370

Forsvarsministeriet

22. august 2024

Høringssvar til udkast til
Forslag til Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

KOMBIT indkøber og forvalter en række af de største og mest udbredte it-løsninger for landets 98 kommuner. Det gælder bl.a. for it-løsninger, der sikrer borgerne nogle af de mest centrale velfærdsydelser indenfor den kommunale forvaltning på social-, sundheds- og beskæftigelsesområdet. KOMBIT står også for den nye valg-løsning. En væsentlig del af de it-løsninger, kommunerne anvender, er samfundskritiske og kan dermed også være oplagte mål for ondsindede aktører, der måtte ønske at skade Danmark og danskerne. Cybersikkerhed i den kommunale digitale forvaltning er derfor et kerneområde i KOMBITs strategi.

KOMBIT hilser Forsvarsministeriets udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-lovforslag) velkommen. Reguleringen har potentialet for at skabe et stærkt fundament for den digitalisering, der understøtter samfundskritiske tjenester i Danmark. Det er imidlertid en forudsætning, at det bagvedliggende NIS2-direktiv implementeres med danske forhold for øje. Dette omfatter nødvendigvis også den kommunale struktur, hvor langt størstedelen af borgernes møde med det offentlige foregår, herunder ikke mindst digitalt og tværsektorielt.

1. Implementering efter danske forhold

På den baggrund finder KOMBIT ikke, at cybersikkerheden i kommunerne er tilstrækkeligt varetaget i NIS2-lovforslaget. Det afspejler ikke strukturen, hvor hver enkelt kommune er bemyndiget til som én juridisk enhed at løse opgaver på tværs af sektorer. Desuden tager lovforslaget ikke tilstrækkeligt klart og præcist højde for, at den kommunale digitalisering er bygget op omkring netværk og infrastruktur, der er sammenhængende og effektiv på tværs af sektorer.

Det bagvedliggende NIS2-direktiv giver en udtrykkelig mulighed for at lade kommuner som helhed være omfattet af NIS2-lovforslaget og dermed understøtte en sammenhængende, ensartet og effektiv sikring af cybersikkerheden for kommunerne. Det er fravalgt.

NIS2-lovforslaget har reelt store indirekte konsekvenser i kommunerne, og det vil koste kommunerne langt mere end estimeret i lovforslaget. Dog udelades at lade kommunerne som helhed være omfattet. Der nævnes i lovforslaget et usikkert estimat for udgifter i kommunerne på 95 – 280 mio. kr. årligt foruden såkaldte ”negative implementeringskonsekvenser”.

2. Den sektorspecifikke tilgang til sikring af informationssikkerhed

Forsvarsministeriet har i lovforslaget fremhævet, at det på nuværende tidspunkt ikke er intentionen at fastsætte regler om, at kommunerne som helhed omfattes af loven. Kommunerne vil dog kunne være direkte omfattet, når de udøver aktiviteter indenfor de sektorer, som udtrykkeligt nævnes i NIS2-lovforslaget. De eksisterende organisatoriske og tekniske forhold, der knytter sig til kommunernes virke, indebærer imidlertid, at kommunerne i praksis vil blive ramt af kravene i lovforslaget i langt større omfang:

Organisatoriske udfordringer
Kommunerne udøver både aktiviteter, der er omfattet af de i NIS2-lovforslaget nævnte sektorer, og aktiviteter der ikke er omfattet. I de ikke omfattede aktiviteter vil der ikke desto mindre alligevel skulle gennemføres risikobaserede foranstaltninger til sikring af informationssikkerheden for de it-løsninger, der benyttes. Kommunen står dermed tilbage med en risiko for uhensigtsmæssig differentiering i implementering af sikkerhedskrav, som skaber en kompleksitet, der i sig selv er en risiko for cybersikkerheden. En risiko, der kan nedbringes ved at implementere det strengeste regelsæt; altså det der gælder for væsentlige enheder i NIS2-lovforslaget.

Tekniske udfordringer
Ud fra et teknisk perspektiv er det heller ikke muligt at operere med en sektorspecifik sondring. Det skyldes som nævnt, at kommunernes digitalisering i vid udstrækning er helhedsorienteret. Dvs. at en stor del af infrastrukturen fungerer på tværs af kommunens forvaltningsområder. Dette er såvel økonomisk som sikkerhedsmæssigt en fornuftig model. Det er med andre ord ikke muligt at udskille den del af netværk og anden infrastruktur, der stilles sektorspecifikke krav til i medfør af NIS2-lovforslaget. Derfor vil kommunerne også her skulle implementere det strengeste regelsæt; altså det der gælder for væsentlige enheder i NIS2-lovforslaget.

Konsekvensen af lovforslaget for kommunerne bliver dermed utilsigtet overimplementering, uanset hvor meget det fremhæves af Forsvarsministeriet, at der er tale om minimumsharmonisering.

På den baggrund vil det blive op til den enkelte kommune at sikre en sammenhængende, ensartet og effektiv sikring af cybersikkerheden, der bygger bro over en unødig kompleksitet, som NIS2-lovforslaget pt. lægger op til. I praksis vil lovforslaget føre til, at en kommune skal kunne efterleve forskellige statslige sektormyndigheders bekendtgørelser for de dele af kommunens virke, der er omfattet af NIS2-lovgivningen. Derudover bliver det nødvendigt at implementere tilsvarende sikkerhedskrav for de dele af kommunens virke, der falder udenfor NIS2-lovgivningen. Dette kan undgås ved at lade kommunerne som helhed være omfattet af lovforslaget.

KOMBIT

3. Kommunernes leverandører er omfattet af NIS2-lovforslaget

Der må desuden forventes en udgiftstung konsekvens for kommunerne som følge af, at KOMBIT og KOMBITs største leverandører ser ud til at blive omfattet af NIS2-lovforslaget som væsentlige enheder af typen "udbyder af administrerede tjenester". Denne type enhed hører til Forvaltning af IKT-tjenester (business-to-business), som er en af de nye sektorer, der fremgår af NIS2-direktivet.

Udbyder af administrerede tjenester er defineret som: "En enhed, der leverer tjenester i forbindelse med installation, administration, drift eller vedligeholdelse af IKT-produkter, -net, -infrastruktur, -applikationer eller andre net- og informationssystemer via assistance eller aktiv administration, der udføres enten i kundernes lokaler eller på afstand."

Uanset et allerede højt niveau af cybersikkerhed vil der været store udgifter forbundet med, at nye regulatoriske sikkerhedskrav rammer kommunernes leverandørkæde, der forvaltes af KOMBIT. Disse udgifter vil i sagens natur også ende hos kommunerne, som gennem KL ejer KOMBIT.

KOMBIT skal på den baggrund foreslå Forsvarsministeriet

- at drøfte med KL og KOMBIT, hvordan NIS2-lovforslaget vil kunne beriges, så det kan understøtte en sammenhængende, ensartet og effektiv cybersikkerhed i de danske kommuner,

- at præcisere i lovforslaget, så det også beskriver de afledte konsekvenser med dertilhørende realistiske estimat af udgifter, som NIS2-lovforsalget vil indebære for kommunerne, hvis den nuværende sektorspecifikke tilgang bibeholdes, og

- under alle omstændigheder medtager i NIS2-lovforslaget, at der skal ske en evaluering af, om den vedtagne lov virker hensigtsmæssigt til sikring af et højt niveau af cybersikkerheden i det danske samfund, herunder i kommunerne senest tre år fra lovens ikrafttræden.

Med venlig hilsen

Kristian Vengsgaard

Administrerende direktør
Dir. tlf. +45 50 77 71 24
Mail KRV@kombit.dk

Kommunale Velfærdschefer

Til **22. august 2024**

Forsvarsministeriets departement

Holmens Kanal 9

1060 København K

Sendt til: fmn@fmn.dk og jhb@fmn.dk i kopi.

Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Kommunale Velfærdschefer takker for muligheden for at afgive høringssvar til ovenstående og fremsender hermed høringssvar på foreningens vegne.

Kommunale Velfærdschefer anerkender vigtigheden af at styrke cybersikkerheden og beskytte kritisk digital infrastruktur. Vi ønsker at fremhæve nogle overvejelser og potentielle konsekvenser, som lovforslaget kan have for kommunerne.

Lovforslaget vil få væsentlige konsekvenser for kommunernes bureaukratiske processer, borgerne og kommunens ressourcer, både i implementeringsfasen og i de daglige arbejdsgange.

Det er områder som risikostyring, foranstaltninger, ledelsesansvar, tilsyn, deltagelse i kurser for ledere, underretning om hændelser, rapporteringsforpligtelse og sanktioner, som kan betyde store forandringer i forhold til hvordan det er i dag.

Betydning for bureaukratiske processer:

Implementeringen af de foreslåede tiltag vil kræve betydelige ændringer i kommunernes eksisterende administrative processer. Dette inkluderer:

- **Øget dokumentationskrav**
    - Der vil være behov for omfattende dokumentation af sikkerhedsforanstaltninger, risikovurderinger og hændelsesrapporter. Dette kan medføre en øget administrativ byrde for vores medarbejdere, som skal sikre, at alle krav overholdes og dokumenteres korrekt.
- **Nye registrerings- og underretningspligter**
    - Kommunerne skal registrere sig hos relevante myndigheder og underrette om væsentlige hændelser. Dette kræver etablering af nye procedurer og systemer for at sikre overholdelse. Det kan også betyde, at kommunerne skal ansætte eller omplacere personale til at håndtere disse opgaver.
- **Koordinering med eksterne parter**

- Der vil være behov for tæt samarbejde med eksterne leverandører og partnere for at sikre, at alle dele af kommunernes net- og informationssystemer opfylder de nye sikkerhedskrav. Dette kan medføre yderligere administrative opgaver og koordinationsarbejde.

Betydning for borgeren:

- **Øget sikkerhed**
  - Borgerne vil nyde godt af øget sikkerhed og beskyttelse af deres personlige data og kommunikationstjenester. Dette kan øge tilliden til kommunernes digitale tjenester og forbedre borgernes oplevelse.
- **Potentielle forsinkelser**
  - Implementeringen af nye sikkerhedsforanstaltninger kan medføre midlertidige forsinkelser i leveringen af visse kommunale tjenester, mens systemer og processer tilpasses de nye krav. Dette kan påvirke borgernes adgang til vigtige tjenester i en overgangsperiode.
- **Øget gennemsigtighed**
  - De nye krav om underretning og rapportering kan føre til øget gennemsigtighed omkring sikkerhedshændelser, hvilket kan styrke borgernes tillid til kommunernes håndtering af cybersikkerhed.

Ressourcebehov i implementeringsfasen og generelt:

Implementeringen af lovforslaget vil kræve betydelige ressourcer, både i form af tid og økonomi.

- **Økonomiske omkostninger**
  - Investering i nye teknologier, sikkerhedssystemer og uddannelse af medarbejdere vil medføre betydelige omkostninger. Kommunerne forventer at blive kompenseret for disse.
- **Tid og arbejdskraft**
  - Implementeringen vil kræve dedikeret tid og arbejdskraft fra it-afdeling og andre relevante afdelinger. Dette kan påvirke kommunens evne til at levere andre vigtige tjenester i implementeringsfasen. Vi foreslår, at der etableres en overgangsperiode, hvor kommunerne får tid til at tilpasse sig de nye krav.
- **Løbende vedligeholdelse**
  - Efter implementeringen vil der være behov for løbende vedligeholdelse og opdatering af sikkerhedssystemer, hvilket vil kræve ressourcer og opmærksomhed. Dette kan også inkludere regelmæssige sikkerhedsrevisioner og opdateringer af vores cybersikkerhedspolitikker. Kommunerne forventer kompensation for disse udgifter.

Mvh

Jakob Bigum Lundberg

Formand, Kommunale Velfærdschefer

Københavns Byret

Forsvarsministeriet

Præsidenten
Domhuset, Nytorv 25
1450 København K.
Tlf. 99 68 70 15
CVR 21 65 95 09
adm.kbh@domstol.dk
J.nr. 24/18764

Den 23. august 2024

Ved mail af 5. juli 2024 har Forsvarsministeriet anmodet om eventuelle bemærkninger over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

Jeg skal i den anledning på byretspræsidenternes vegne oplyse, at byretterne ikke har bemærkninger til udkastet.

Der henvises til J.nr. 2024/004461.

Med venlig hilsen

Nikolaj Aarø-Hansen

Landbrug & Fødevarer F.m.b.A.

Axelborg, Axeltorv 3
DK 1609 København V

T +45 3339 4000
E info@lf.dk
W www.lf.dk

CVR DK 25 52 95 29

Til Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt via email til fmn@fmn.dk, cc: jhb@fmn.dk

Høringssvar vedr.: Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (sagsnummer 2024/004461)

Landbrug & Fødevarer takker for muligheden for at afgive høringssvar vedr. forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau i høring.

Indledningsvis kvitteres for den gennemgående tilgang med minimumsimplementering. Landbrug & Fødevarer bakker også op om ambitionen i sektortilgangen og ser frem til udfoldelsen af dette, hvilket Landbrug & Fødevarer ønsker at bidrage til.

I den sammenhæng foreslås, at der laves et samlet overblik over processerne for de relevante, kompetente myndigheder. Det fremgår af bemærkningerne, at der vil blive skabt et overblik over de kompetente myndigheder, der får respektive sektoransvar. Det vil i forlængelse heraf også være ønskværdigt med et overblik over deres processer – medmindre de forventes at køre helt parallelt.

Ift. sektordeling af ansvaret, så opfordrer Landbrug & Fødevarer til, at ambitionerne for koordinering ikke alene forekommer ved udformning af regler, men også vedr. tilsyn, se nærmere under kommentarer til § 21.

Herunder er kommentarer og spørgsmål til specifikke paragraffer og bemærkninger til samme.

§ 5
Af bemærkninger til § 4 (bemærkninger s. 223) fremgår en vejledningspligt overfor væsentlige enheder: *"Desuden forudsættes det, at de kompetente myndigheder i relevant omfang vejleder enheder inden for deres sektor om forståelsen af § 4, stk. 3, nr. 5"*.

Kunne lignende vejledningsforpligtelser indskrives i bemærkninger til § 5, eller er de vigtige enheder dækket af bemærkningerne til § 4?

§ 16
Landbrug & Fødevarer kan kun bakke op om, at der foretages en høring af enhed inden offentliggørelse af en hændelse. I forlængelse heraf må høres til hvad "anden offentlig interesse" indbefatter?

§ 20
Som nævnt indledningsvis kan Landbrug & Fødevarer se ræson i den sektorbaserede tilgang. Men hvem har ansvaret for at sikre koordinering, når en enhed kan falde under flere sektorer? Og hvor kan man klage ved konflikt? Er det CFCS? Eller de udpegede myndigheder?

§21
Vil den sektorbaserede tilgang i relation til tilsyn indebærer risiko for tilsyn fra flere kompetente myndigheder? Hvis det er tilfældet, opfordres til et skarpt fokus på koordinering også på dette område, så virksomhederne ikke udsættes for dobbelttilsyn.

Af bemærkningerne fremgår det, at der er risiko for fortolkningstvivl, idet ”off-site supervision” er oversat til ”eksternt tilsyn”. Herfra kvitteres for at opfange den sproglige nuance og der bakkes op om den foreslåede specifikation.

§ 23
I bemærkningerne specificeres eventuelle suspenderingers midlertidige karakter, hvor *”afgørelsen kun kan opretholdes, så længe enheden ikke har truffet de nødvendige tiltag for at afhjælpe de mangler eller efterleve de krav fra myndigheden, som gav anledning til, at foranstaltningerne blev anvendt*”. Med ”truffet de nødvendige tiltag” forstås så, at tiltagene skal være igangsat? Eller skal de være fuldt gennemførte og virksomme? Herfra skal lyde opfordring til første – dvs. igangsat.

Herfra opbakning til den sproglige afklaring der specificerer, at ledelsesansvaret pålægges alene den administrerende direktion (eller anden titel for øverste leder) og ikke alle eventuelle medlemmer af en direktion.

Vedrørende certificerings- og godkendelsesordninger, der vil kunne medføre suspendering, er alle ordninger i reelt i spil, eller skal det relatere sig til cybersikkerhed på den ene eller anden måde?

Med venlig hilsen

Kathrine Blæsbjerg Sørensen
Projektleder, chefkonsulent

Erhverv & Viden

M +45 4031 5718
E kbs@lf.dk

MEDICO INDUSTRIEN
MEDTECH DENMARK

Forsvarsministeriet
Att. Jakob Halkjær Brams
fmn@fmn.dk
jhb@fmn.dk

22. august 2024

Høringssvar vedr. udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau - sagsnummer 2024/004461

Medicoindustrien takker indledningsvist for modtagelsen af høringen over forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, der som vi forstår det er hovedloven i den danske implementering af NIS2-direktivet.

Medicoindustrien har forstået, at man fra danske side har besluttet sig for en minimumsimplementering og dermed ikke ønsker at pålægge de omfattede sektorer yderligere krav og forpligtelser, end dem der følger af direktivet. Denne tilgang er Medicoindustrien meget tilfreds med. Vi oplever at EU-lovgivninger vedtages med stigende hast og større kompleksitet koblet med en efterfølgende langsommelig gennemførsel, og derfor er der ikke behov for, at vi går enegang fra dansk side og underlægger industrien yderligere krav og forpligtelser, end hvad der følger af EU-lovgivningen. Medicobranchen er i forvejen en gennemreguleret branche, som er underlagt to sektorforordninger, MDR og IVDR, der blev vedtaget i 2017 men fortsat mangler væsentlig infrastruktur, og samtidigt er vi en global branche, der i vidt omfang er certificerede i henhold til standarder indenfor cybersecurity, f.eks. ISO 27001 og ANSI/AAMI SW96:2023, TIR 57 og TIR 97 etc.

Vi forstår samtidigt også, at man efter vedtagelsen af hovedloven tilsvarende vil pålægge de sektoransvarlige myndigheder at udstede bekendtgørelser, der regulerer de enkelte sektorer. Denne kommende sektorlovgivning ser vi frem til at følge tilblivelsen af, og om muligt bidrage til. For os giver det god mening at de sektoransvarlige myndigheders ekspertise i deres respektive område sættes i spil her.

I medlemskredsen herskede der i kølvandet på vedtagelsen af NIS2-direktivet i december 2022 en vis usikkerhed om, hvorvidt vores medlemmer – de virksomheder, der er tilstrækkeligt store til at være omfattet af NIS2 – vil være at betragte som væsentlige eller vigtige i relation til direktivet. I den forbindelse ser vi positivt på, at det af bemærkningerne til forslaget fremgår, at Forsvarsministeriets foreslår, at den relevante kompetente myndighed ud fra en konkret vurdering kan træffe afgørelse om, at en enhed, der som udgangspunkt anses for at være væsentlig i stedet skal anses for at være vigtig.

I stigende grad er medicinsk udstyr også digitalt, og i relation til NIS2 er det således Medicoindustriens bekymring, at Forsvarsministeriet i bemærkningerne til forslaget bekræfter, at man kan være omfattet af to forskellige sektorbekendtgørelser. Dette vil for vores medlemmer, der som nævnt ovenfor i forvejen er underlagt en stærk sektorregulering, øge kompleksiteten, f.eks. at skulle dobbelthændelsesapportere til to forskellige sektormyndigheder. Her vi vil opfordre til, at man de to sektormyndigheder imellem forholder sig til, hvilken myndighed der konkret skal rapporteres til.

Medicoindustrien
Bøge Allé 5
2970 Hørsholm
Denmark
+45 49 18 47 00
medico@medicoindustrien.dk
medicoindustrien.dk

Afslutningsvist skal Medicoindustrien opfordre til, at der i forbindelses med udstedelsen af sektorbekendtgørelserne tillige gives en fyldig vejledning til de omfattede virksomheder, både omkring definitioner, krav og forpligtelser for 'væsentlige' og 'vigtige' enheder, men også i forhold til hændelsesrapportering og sikkerhedskrav, herunder hvordan man nærmere definerer og kvantificerer en væsentlig hændelse.

Medicoindustrien står selvfølgelig til rådighed med henblik på en uddybning af vores synspunkter.

Med venlig hilsen

Lene Laursen

Vicedirektør

Medicoindustrien
Bøge Allé 5
2970 Hørsholm
Denmark

+45 49 18 47 00
medico@medicoindustrien.dk
medicoindustrien.dk

From: Hoeringer <Hoeringer@naviair.dk>
Sent: 09-08-2024 12:25:40 (UTC +02)
To: FMN-MYN-Forsvarsministeriet <fmn@1net.fmn.dk>
Cc: FMN-JHB Brams, Jakob Halkjær <JHB@1net.fmn.dk>; nkk@trm.dk <nkk@trm.dk>; trm@trm.dk <trm@trm.dk>; Sigurd Slot Jacobsen <ssj@naviair.dk>; Hoeringer <Hoeringer@naviair.dk>
Subject: Svar vedr. sagsnummer 2024/004461 - Høring fra Forsvarsministeriet over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau
Categories: Amanda

(FMI-CD besked: Denne mail kommer fra Internettet.)

Att. Forsvarsministeriet

Tak for høringsudkastet vedr. udkast til "Lov om foranstaltninger til sikring af et højt cyber-sikkerhedsniveau".

Naviair har ingen bemærkninger til lovudkastet.

Med venlig hilsen

Charlotte Mulle Birn
Specialkonsulent • Operational Strategy & Compliance, OD
T +45 3247 7910 • cmb@naviair.dk

Naviair • Naviair Allé 1 • DK 2770 Kastrup • Danmark
T +45 3247 8000 • www.naviair.dk

Fra: Jesper Bach Gustafson <jbg@trm.dk>
Sendt: 10. juli 2024 14:43
Til: Sigurd Slot Jacobsen <ssj@naviair.dk>
Cc: Michael Birch <mbh@trm.dk>; Nikolaj Klint Kistorp <NKK@trm.dk>
Emne: Høring fra Forsvarsministeriet over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Kære Sigurd Slot Jacobsen

Transportministeriet fremsender hermed udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, som er blevet sendt i høring af Forsvarsministeriet. Vi henviser til vedlagte høringsbrev fra Forsvarsministeriet samt vedlagte udkast til lovforslag.

I anmodes i denne forbindelse om at bidrage med eventuelle bemærkninger til vedlagte udkast til lovforslag senest den 13. august 2024.

Eventuelle bemærkninger bedes sendt på e-mail til fmn@fmn.dk med kopi til jhb@fmn.dk, NKK@trm.dk og trm@TRM.dk samt med henvisning til sagsnummer 2024/004461.

På forhånd tak og god sommer.

Mvh. Jesper

Venlig hilsen

Jesper Bach Gustafson
Fuldmægtig

Transportministeriet
Selskabs- og Koncernstyringsenheden
Frederiksholms Kanal 27 F
DK-1220 København K

Naalakkersuisut
Goverment of Greenland
Digitaliseringsstyrelsen

Digitalinngortitsinermut
Aqutsisoqarfik

31. juli 2024
Sagsnr.: 2024 - 14403

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt via: fmn@fmn.dk og cc jhb@fmn.dk

Høringssvar over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

Digitaliseringsstyrelsen i Grønland takker for muligheden for at kunne afgive et høringssvar til forslaget til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

Digitaliseringsstyrelsen har følgende bemærkninger til forslaget.

Til § 27
Giver kun kompetente myndigheder adgang til at samarbejde med andre kompetente myndigheder i andre EU-lande.

Grønlands Selvstyre har til hensigt at etablere en kompetent myndighed med de samme formål, som lovforslaget har for kompetente myndigheder i Danmark.

Grønlands Selvstyre ønsker, at lovforslaget også kommer til at indeholde en lovhjemmel til, at kompetente myndigheder i Danmark kan samarbejde med en kompetent myndighed i Grønland.

Grønlands Selvstyre har et stærkt behov for et sådant samarbejde. Flere kritiske IT-systemer for Grønland er danske IT-systemer:

- Folkeregisteret, der varetages af Indenrigsministeriet
- MitID og Nemlog-in, der varetages af Digitaliseringsstyrelsen I Danmark og Nets A/S
- CVR-registeret, der varetages af Erhvervsstyrelsen
- Elektronisk betaling, der varetages af Nets
- Dronning Ingrids Hospitals samarbejde med sundhedsorganisationer i Danmark
- Listen er ikke udtømmende

Digitalinngortitsinermut
Aqutsisoqarfik
Postboks 1078
3900 Nuuk
Tel: (+299) 346407
E-mail: erfr@nanoq.gl
www.naalakkersuisut.gl

Grønlands Selvstyre har derfor en stærk interesse i at kunne deltage i et samarbejde, hvor en grønlandsk kompetent myndighed kan blive involveret i en væsentlig hændelse, der måtte ske i kritiske it-systemer, der vil kunne have virkning i Grønland. En væsentlig hændelse i disse it-systemer vil have en væsentlig virkning for det grønlandske samfund.

En grønlandsk kompetent myndighed vil blive pålagt de opgaver, som forslaget tillægger CSIRT. Den kompetente myndighed får behov for i realtid at kunne reagere på de udfordringer en væsentlig hændelse i et af de nævnte it-systemer kan medføre for det grønlandske samfund.

Omvendt hvis en væsentlig hændelse måtte have sit udgangspunkt fra Grønland, at en relevant dansk kompetent myndighed kan blive informeret om den væsentlige hændelse.

For at kunne sikre et højt cybersikkerhedsniveau for it-systemer, der anvendes af både Grønland og Danmark, skal kompetente myndigheder i begge lande kunne samarbejde.

Ligeledes har Grønland brug for Danmarks bistand til at kunne sikre et højt cybersikkerhedsniveau i forbindelse med søkablerne til Grønland.

I den forbindelse har Grønland brug for formålet, som er angivet i § 27 samarbejde med andre EU-landes kompetente myndigheder, hvor de grønlandske søkabelforbindelser rammer en teleinfrastrukturaktør i et EU-land.

Til § 28
Ligeledes skal der gives adgang til, at kompetente myndigheder kan udveksle information med den grønlandske kompetente myndighed, herunder også personoplysninger.

Til § 38
Grønlands Selvstyre har til hensigt til at indføre lovgivning med samme formål, som dette forslag har. Anordningsmuligheden skal derfor ikke anvendes på grønlandske myndigheder og andre juridiske enheder som selvstyre har lovgivningskompetence over.

En cyberkrisestyringsmyndighed kan ikke varetage en sådan opgave fra Danmark. En væsentlig hændelse kunne ramme kommunikationslinjerne mellem Grønland og Danmark og dermed forårsage, at en cyberkrisestyringsmyndighed ikke kan fungere.

Dette udelukker ikke et behov for en anordning af denne lov vedrørende rigsmyndigheder i Grønland.

De statslige myndigheder, der efter denne lov vil blive anset for væsentlige eller vigtige enheder, der har rigsmyndigheder i Grønland bør også i Grønland anses at være enten væsentlige eller vigtige enheder i Grønland.

Disse rigsmyndigheder skal derfor pålægges de samme krav til sikring af et højt

Digitalinngortitsinermut Aqutsisoqarfik
Postboks 1078
3900 Nuuk
Tel: (+299) 346407
E-mail: erfr@nanoq.gl
www.naalakkersuisut.gl

cybersikkerhedsniveau som deres modermyndighed i Danmark.

Rigsmyndighederne i Grønland må ikke efterlades i et vakuum. Det vil udgøre en uacceptabel sikkerhedsrisiko for det grønlandske samfund.

Inussiarnersumik inuulluaqqusillunga
Med venlig hilsen

Erik Frydensberg-Holm
Chefkonsulent

Digitalinngortitsinermut
Aqutsisoqarfik
Postboks 1078
3900 Nuuk
Tel: (+299) 346407
E-mail: erfr@nanoq.gl
www.naalakkersuisut.gl

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

From: Lise Emilie Berendt <leb@samaqua.dk>
Sent: 20-08-2024 17:00:59 (UTC +02)
To: FMN-MYN-Forsvarsministeriet <fmn@1net.fmn.dk>
Cc: FMN-JHB Brams, Jakob Halkjær <JHB@1net.fmn.dk>
Subject: Høringssvar (sagsnummer 2024/004461)
Categories: Amanda

I forbindelse med høringen over forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, indgiver SamAqua følgende høringssvar:

Vedr. lovforslagets § 1
Loven finder anvendelse på enheder under de udpegede sektorer, som udgør mellemstore virksomheder, eller som overskrider tærsklerne for mellemstore virksomheder, samt enheder, som er identificeret som kritiske enheder efter direktiv 2022/2557.

For at være en mellemstor virksomhed skal enheden beskæftige mindst 50 personer og have en årlig omsætning eller en samlet årlig balance på over 10 mio. euro. Der henvises i lovbemærkningerne til henstilling 2003/361/EF for en beregning af antal ansatte og omsætning. Det ønskes dog afklaret, hvordan beregningen foretages for koncernforbundne selskaber, herunder om der foretages en forholdsmæssig fordeling (henstillingens artikel 6).

I forlængelse heraf gøres opmærksom på, at der er en særlig problemstilling for de mange vand- og spildevandsselskaber, som har en mindre energiproduktion: Hvis beregningen foretages på baggrund af koncernen uden en forholdsmæssig fordeling på de enkelte selskaber, vil flere af disse vand- og spildevandsselskaber ligeledes blive omfattet af reguleringen under energisektoren - dette på trods af, at energiproduktionen er under de tærskelværdier, som fremgår af lovforslaget for energisektoren. Vi er opmærksomme på henvisningen i lovudkastets bemærkninger til præambel 16, hvorefter der er mulighed for at undtage en enhed fra anvendelsesområdet, selvom enheden opfylder størrelseskravet. Problemstillingen vedrørende de nævnte vand- og spildevandselskaber er dog af en så betydelig og generel karakter, og det bør behandles i lovudkastet, så det sikres, at vand- og spildevandsselskaber med en mindre energiproduktion alene underlægges reguleringen under vand- og spildevandssektoren.

Vedr. lovforslagets § 7
Enhedernes ledelsesorgan pålægges en række forpligtelser og ansvar efter loven, og loven bør derfor indeholde en præcis definition af, hvad der forstås ved enhedens ledelsesorgan (hvem er omfattet).

I er velkomne til at kontakte mig, hvis I har spørgsmål til ovenstående.

Med venlig hilsen

Lise Emilie Berendt
Specialkonsulent

Direkte:
Mobil: +45 24 48 56 59
E-mail: leb@samaqua.dk
Web: www.samaqua.dk

SamAqua

TEKNIQ ARBEJDSGIVERNE

Forsvarsministeriet

Sendt til fmn@fmn.dk
med kopi til jhb@fmn.dk

Paul Bergsøes Vej 6
2600 Glostrup

Billedskærervej 17
5230 Odense M

Telefon 4343 6000
tekniq@tekniq.dk
www.tekniq.dk

Mobil:
Email: jas@tekniq.dk

Dato: 19. august 2024

TEKNIQ Arbejdsgivernes svar på høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (sagsnummer 2024/004461)

Forsvarsministeriet har med annoncering på Høringsportalen.dk den 5. juli 2024 igangsat høring over "udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau" (NIS2-direktivet), og beder om høringssvar senest 22. august 2024.

TEKNIQ Arbejdsgiverne er stærkt optaget af sikkerhedsområdet generelt, og loven berører vigtige forretningsområder for vores medlemsvirksomhederne, hvorfor vi svarer på høringen.

Generelle bemærkninger
TEKNIQ Arbejdsgiverne er helt enig i, at der er behov for en opstramning af it-sikkerheden i Danmark. Fra den enkelte virksomheds daglige praksis til myndighedernes håndtering af og vejledning i cybersikkerhed.

TEKNIQ Arbejdsgiverne hilser derfor intentionerne i NIS2-direktivet velkomne. For at intentionerne i NIS2 kan være med til at løfte sikkerheden i Danmark er det afgørende, at gøre indsatserne konkrete og forretningsnære. TEKNIQ glæder sig derfor over, at den danske lovproces nu går i gang og håber at forsinkelsen i lovprocessen ikke er udtryk for regeringens prioritering af området.

Lovudkastet viser, at der et stykke vej endnu. Der udestår bl.a. et antal vigtige sektorspecifikke bekendtgørelser, som definerer de nærmere betingelserne, som virksomhederne skal efterleve fra 1. marts 2025. Det gælder ikke mindste de nærmere tekniske krav (§ 6, stk. 3), som Forsvarsministeriet flager (bemærkningerne side 182-183).

TEKNIQ Arbejdsgiverne mener der er risiko for at der opstår "panik for lukketid" i implementeringsarbejder for virksomhederne - herunder om direkte omfattede virksomheder pga. tidspres, uklarheder og udsigten til nye restriktioner kommer til at stille upræcise eller unødigt høje krav til sine leverandører.

TEKNIQ Arbejdsgiverne ser derfor stort behov for målrettede vejledninger fra de ansvarlige myndigheder til de potentielt berørte virksomheder. Både til de virksomheder, der bliver direkte omfattet af loven, og de virksomheder, der omfattes indirekte som leverandører (forsyningskædesikkerhed).

TEKNIQ Arbejdsgiverne indgår gerne i en dialog om en sådan indsats.

Specifikke bemærkninger

Behov for tæt koordinering og klar kommunikation (§20, stk. 1)
De enkelte ministerområder udpeger forskellige kompetente myndigheder til at varetage tilsyn og håndhævelse af loven (§20, stk. 1), som afspejler NIS2-direktivets udvidelse af omfattede sektorområder.

TEKNIQ Arbejdsgiverne forstår intentionen om at direktivets krav målrettes og tilpasses de enkelte sektorers særlige forhold, men ser også nogle udfordringer i at sprede ansvaret på forskellige ministerområder. Det gælder f.eks. virksomhed i det tekniske erhvervsliv, der leverer til alle dele af samfundet, herunder til sundhedssektoren, drikkevandsforsyningen og til fødevarevirksomheder.

TEKNIQ Arbejdsgiverne noterer sig, at Forsvarsministeriet er opmærksomt på udfordringerne og man tilstræber ensartethed og tæt koordinering i tilsyn, håndhævelse og i de sektorspecifikke bekendtgørelser (bemærkningerne, side 145 og 146).

TEKNIQ Arbejdsgiverne ser et stort behov for at afklare og kommunikere, hvordan en virksomhed der agerer i forskellige sektorer, skal referere til hvilke myndigheder.

Center for Cybersikkerheds centrale rolle
Center for Cybersikkerhed (CFCS) spiller en helt central rolle i NIS2 - som facilitator af et tæt samarbejde mellem de ressortansvarlige myndigheder, og som "Computer Security Incident Response Teams" (CSIRT), som NIS 2-direktivet forpligter medlemsstaterne til at udpege, og hvis ansvarsområder er defineret Kapitel 5, §17-19.

Med tanke på CFCSs forankring i Forsvarsministeriet er det afgørende, at CFCS til stadighed arbejder med åbenhed og videndeling ift. civile virksomheder – fx at dele viden og advare om sårbarheder og igangværende angreb (punk 62, side 39).

Dette bl.a. med henvisning til bl.a. IT-Branchens som har efterlyst større åbenhed hos CFCS, "øget, hurtigere og en mere konkret videndeling i en let tilgængelig form", samt bedre samspil med den private sektor (pressemeddelelse fra IT-Branchen "En løsningsfattig analyse om Center for Cybersikkerhed" ifbm. analysen af CFCSs virksomhedsrettede cybersikkerhedsindsats, 31. marts 2023).

Paul Bergsøes Vej 6
2600 Glostrup

Billedskærervej 17
5230 Odense M

Telefon 4343 6000
tekniq@tekniq.dk
www.tekniq.dk

Mobil:
Email: jas@tekniq.dk

Paul Bergsøes Vej 6
2600 Glostrup

Billedskærervej 17
5230 Odense M

Telefon 4343 6000
tekniq@tekniq.dk
www.tekniq.dk

Mobil:
Email: jas@tekniq.dk

Uklarhed om hvilke virksomheder omfattes
Forsvarsministeriet konstaterer, at der nuværende tidspunkt ikke er fuldt overblik over, hvor mange danske virksomheder som vil blive omfattet af lovforslaget, men læner sig op ad et indledende estimat på 2.0000 virksomheder, og påpeger behov for en nærmere vurdering i forbindelse med det videre implementeringsarbejde, bl.a. med de sektorspecifikke bekendtgørelser (Almindelige bemærkninger side 183).

TEKNIQ Arbejdsgiverne opfordrer sine medlemsvirksomheder til at tage en dialog med potentielt omfattede virksomhedskunder, men det er tydeligt, at der hersker stor usikkerhed i markedet, hvilket begrænser indsatsen.

Det manglende overblik skaber frustrationer i markedet. Ikke mindst for virksomheder som leverer til (potentielt) omfattede virksomheder.

Selvregistrering
Danmark er forpligtet til senest april 2025 at dele en liste over omfattede virksomheder i EU-samarbejdet (ENISA). Det er op til virksomhederne selv at registrere sig, hvis man mener at man er omfattet af NIS2 (§10).

Også her mener TEKNIQ Arbejdsgiverne at der er behov for nærmere vejledning fra myndighederne. Fx kunne de myndighederne kontakte alle virksomheder inden for deres sektor mhbp. at afklare om og hvordan virksomhederne er omfattet. Det må være i alles interesse at listen bliver retvisende og ikke skyder hverken under eller over målet.

Tilsyn
NIS2-direktivet skelner mellem ”væsentlige” og ”vigtige enheder”, og Forsvarsministeriet lægger op til at denne skelnen afspejles i myndighedernes tilsyn, ”således at der løbende føres tilsyn med væsentlige enheders efterlevelse af lovgivningen, mens der ved tilsynet med vigtige enheder anlægges en rent reaktiv tilgang, således at der først ved tegn på, at den vigtige enhed ikke overholder lovgivningen, iværksættes et tilsyn” (side 170).

Det er ikke indlysende for TEKNIQ Arbejdsgiverne, hvordan det vil fungere i praksis. Fx med tanke på virksomheder der opererer inden for flere sektorer.

Sanktioner – suspension af certifikater
Forsvarsministeriet lægger op til at kunne ”suspendere eller anmode et certificerings- eller godkendelsesorgan eller en domstol om i overensstemmelse med national ret midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, der leveres, eller aktiviteter, der udføres af en væsentlig enhed”.

Sanktionen er tiltænkt væsentlige enheder i de tilfælde hvor "en række mindre indgribende midler har vist sig ikke at være tilstrækkelige", og der drages sammenligning med fødevarelovens §52, som giver mulighed for at nedlægge forbud mod drift af en fødevarevirksomhed op til 6 måneder.

Det er selvsagt omvæltende for en virksomhed at fx at få frataget sit ISO-certifikat, som kan være en væsentlig forudsætning for deres virke. TEKNIQ Arbejdsgiverne forventer derfor en præcis beskrivelse af hvordan en sådan sanktion kan anvendes for at sikre retssikkerheden og klare procedurerne op til en sådan evt. sanktion, som er i alles interesse at undgå.

Økonomiske konsekvenser for erhvervslivet

Forsvarsministeriet konstaterer, at gennemførelse af NIS2-direktivet ventes at få "væsentlige erhvervsøkonomiske konsekvenser" (side 183), som er vanskelige at estimere nærmere på nuværende tidspunkt.

Det skyldes ikke mindst at "lovforslagets mest centrale krav – herunder navnlig kravene til foranstaltninger til styring af cybersikkerhedsrisici i medfør af lovforslagets § 6, stk. 3 – konkretiseres yderligere i bekendtgørelser".

Forsvarsministeriet vurdering lige nu – på baggrund af tal fra bl.a. Europakommissionen og ENISA og med store forbehold – er at de erhvervsøkonomiske konsekvenser ligger i et spænd på 2,6 mia. kr. – 3 mia. kr.

TEKNIQ Arbejdsgiverne anerkender udfordringen med at estimere udgifterne på nuværende tidspunkt, men vurderer umiddelbart, at de samlede udgifter bliver del højere.

TEKNIQ Arbejdsgiverne opfordrer til en revideret vurdering af de erhvervsøkonomiske udgifter også omfatter ikke-direkte omfattede virksomheder, og altså ikke kun de antageligt omkring 2.000 direkte omfattede virksomheder.

TEKNIQ Arbejdsgiverne står naturligvis til rådighed for en uddybning af vores høringssvar.

Med venlig hilsen

Janus Sandsgaard

Paul Bergsøes Vej 6
2600 Glostrup

Billedskærervej 17
5230 Odense M

Telefon 4343 6000
tekniq@tekniq.dk
www.tekniq.dk

Mobil:
Email: jas@tekniq.dk

Til Forsvarsministeriet
Sendt pr. e-mail til:
fmn@fmn.dk og jhb@fmn.dk

Sagsnr.: 2024/004461.

22.08.2024

Høringssvar til høring over udkast til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

TI skal hermed afgive høringssvar til lovforslaget til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau. Høringssvaret indeholder to generelle bemærkninger og én konkret bemærkning.

Generelle bemærkninger:

Uklarhed omkring den samlede lovgivningspakke

Lovforslaget til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (herefter NIS2-hovedloven) er fremsat på samme tid som lovforslag om kritiske enheders modstandsdygtighed (herefter CER-loven). De to lovforslag er en del af en samlet pakke, der sammen med den sektorspecifikke lovgivning skal implementere CER-direktivet og NIS-2-direktivet i dansk lovgivning.

TI's medlemmer er imidlertid i et vist omfang undtaget fra både CER-loven og NIS2-hovedloven, da der for udbydere af elektroniske kommunikationsnet og -tjenester vil komme en sektorspecifik NIS2-lov (lov om cybersikkerhed i telesektoren) med flere supplerende bekendtgørelser, som vi endnu ikke har set forslagene til. Det er derfor ikke muligt for TI's medlemmer på nuværende tidspunkt at afklare, hvordan de sektorspecifikke love og bekendtgørelser kommer til at spille sammen med NIS2-hovedloven. TI finder det grundlæggende kritisabelt, at det ikke er muligt for TI's medlemmer at danne sig et samlet overblik over den kommende regulering, særligt henset til, at reglerne træder i kraft om kort tid.

Flere af TI's medlemmer opererer i forskellige sektorer og udbyder også andre tjenester end 'offentligt tilgængelige elektroniske kommunikationstjenester', eksempelvis DNS-tjenester, der omfattes af NIS2-hovedloven. For disse medlemmer er det i særdeleshed vigtigt at

kende det samlede billede således, at eventuelle uhensigtsmæssigheder eller uklarheder kan påpeges allerede i høringsprocessen.

Behov for koordination mellem de kompetente myndigheder

Reglernes kompleksitet og det faktum, at flere af TI's medlemmer opererer i forskellige sektorer, stiller store krav til selskaberne, og de ønsker derfor en høj grad af ensartethed på tværs af sektorerne. For at minimere eller helt at undgå, at TI's medlemmer kommer til at skulle forholde sig til for mange forskelligartede krav og forpligtelser, bør processerne for hændelsesunderretning, tilsynsaktiviteter mv. strømlines så meget som muligt. TI hilser det derfor velkomment, at både forslaget til NIS2-hovedlov og forslaget til CER-loven lægger meget vægt på, at der skal være et stærkt tværgående samarbejde og koordination myndighederne imellem. Det vil mindske de administrative byrder væsentligt, hvis de forskellige myndigheders håndtering af reglerne kan blive så ensartet som muligt.

TI forudsætter i den forbindelse, at der følger de nødvendige økonomiske ressourcer med til formålet således, at der også i praksis kan ske den fornødne koordinering mellem myndighederne.

Konkret bemærkning:

Uklarhed om rækkevidden af undtagelsen i den foreslåede § 1, stk. 2

Det fremgår af lovforslagets § 1, stk. 2, at "loven ikke finder anvendelse på enheder i det omfang, de er omfattet af lov om cybersikkerhed i telesektoren… Dog gælder lovens § 17 for de enheder".
Når TI læser lovbemærkningerne fremgår det også her klart, at NIS 2-hovedloven som udgangspunkt ikke skal finde anvendelse på enheder i telesektoren.

Der er således meget til støtte for at antage, at TI's medlemmer i deres udbud af offentligt tilgængelige elektroniske kommunikationsnet- og tjenester kan se helt bort fra NIS2-hovedloven (undtagen bestemmelserne vedr. CSIRT'en), men når indholdet af den sektorspecifikke lov endnu ikke kendes, skaber det en vis usikkerhed om fortolkningen af § 1, stk. 2.

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

Med venlig hilsen

Jakob Willer
Direktør

TRAFIKSELSKABERNE I DANMARK

Forsvarsministeriet
Holmens Kanal 9
1060 København K
Att.: Jakob Halkjær Brams
E-mail: fmn@fmn.dk
CC: jhb@fmn.dk

18. august 2024

Vedr.: Høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau – NIS2

Trafikselskaberne er ikke udpeget som høringspart over udkast til lov om sikring af et højt cybersikkerhedsniveau (NIS2), da det er Trafikstyrelsens umiddelbare vurdering, at trafikselskaberne formentlig ikke er omfattet af nogen af de to lovforslag. Lokalbanerne fremgår heller ikke af høringslisten. Trafikstyrelsen har dog oplyst, at den endelige tekst på dansk og yderligere analyser kan ændre vurderingen af, hvem der er omfattet af forordningen.

Flertallet af trafikselskaber er umiddelbart enige i, at trafikselskaberne ikke synes at være omfattet af NIS2. Det gælder dog ikke lokalbanerne, som alle trafikselskaber vurderer, er omfattet af forslaget. Trafikselskaberne i Danmark skal derfor indledningsvis bede om en afklaring af, om trafikselskaberne, og/eller de selskaber, de deltager i, vurderes at kunne blive omfattet af forslaget.

Trafikselskaberne skal i den sammenhæng tage et generelt forbehold for, at det vil betyde øgede omkostninger og ressourcetræk hos trafikselskaberne, og dermed behov for kompensation, såfremt de er omfattet af forslaget. Det samme gælder, hvis de selskaber, som trafikselskaberne deltager i, bliver omfattet af reglerne. Her kan bl.a. peges på FlexDanmark og Rejsekort & Rejseplan A/S.

Der tages ligeledes forbehold for, at i det omfang trafikselskabernes operatører omfattes af lovforslaget, med øgede omkostninger til følge, vil det udløse krav til trafikselskaberne om økonomisk kompensation. Et mere præcist estimat for disse omkostninger kan ikke gives på det foreliggende grundlag, men det fremgår af både lovforslag og EU-direktiv, at der er tale om omkostninger i en anselig størrelse.

Trafikselskaberne vil afvente eventuelle mere detaljerede bemærkninger til den varslede bekendtgørelse.

Specifikke bemærkninger
Vi skal venligst bede om at få afklaret/præciseret i bemærkningerne til NIS2-forslaget, at trafikselskaber ikke udgør "regionale forvaltningsmyndigheder" i direktivets forstand, jf. direktivets bilag 1, nr. 10, jf. definitionen i art. 6, nr. 35), da dette ikke er klart på baggrund af en læsning af direktivet/lovforslaget. For god ordens skyld henledes opmærksomheden på, at trafikselskaber henregnes til den offentlige forvaltning, jf. lov om trafikselskaber.

Med venlig hilsen

Lone Rasmussen
Sekretariatschef

+ 45 23 40 16 39
lor@moviatrafik.dk
Trafikselskaberne i Danmark

Vestre Landsret
Præsidenten

Forsvarsministeriet
Holmens Kanal 9
1060 København K

23. august 2024

J.nr.: 24/18269-2

Sendt pr. mail til fmn@fmn.dk og jhb@fmn.dk

Sagsbehandler: Lars B Olesen

Forsvarsministeriet har ved brev af 5. juli 2024 (sagsnr. 2024/004555) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Jens Røn