FORSVARSMINISTERIET
MINISTRY OF DEFENCE

Januar 2018

KOMMENTERET HØRINGSOVERSIGT
vedrørende
forslag til lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.

Et udkast til lovforslaget har i perioden fra 27. oktober 2017 til 24. november 2017 været sendt i høring hos:

Advokatrådet, Amnesty International, Danish Internet eXchange point (DIX), Dansk Erhverv, Dansk Industri (DI), Danske Advokater, Danske Regioner, Datatilsynet, Den Danske Dommerforening, DI ITEK, Domstolsstyrelsen, Institut for Menneskerettigheder, Internet eXchange point of the Oresund Region (IXOR), IT Branchen, IT-Politisk Forening, KL, Netnod IX Copenhagen, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Rådet for Digital Sikkerhed, Stockholm Internet eXchange AB (STHIX), Teleindustrien (TI), The Neutral Internet Exchange (NL-ix) og Tilsynet med Efterretningstjenesterne.

Forsvarsministeriet har modtaget høringssvar fra Datatilsynet, Institut for Menneskerettigheder, IT-Politisk Forening, Netnod, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening og Tilsynet med Efterretningstjenesterne. Forsvarsministeriet har endvidere modtaget en udtalelse fra Dansk Energi.

Nedenfor gennemgås og kommenteres de væsentligste bemærkninger fra de hørte parter til de enkelte emner i lovforslaget. Forsvarsministeriets kommentarer til høringssvarene er anførte med kursiv.

Det bemærkes, at enkelte høringsparter har henvist til de høringssvar, som de pågældende organisationer tidligere har afgivet i forbindelse med høringen over forslag til lov om Center for Cybersikkerhed (lovforslag nr. L 192, Folketinget 2013-14, fremsat den 2. maj 2014). Forsvarsministeriet henviser i den forbindelse til den kommenterede høringsoversigt vedrørende dette lovforslag.

1. Den overordnede model for implementering af NIS-direktivet på tværs af sektorer

Dansk Energi efterlyser en mere holistisk tilgang til cybertruslen fra myndighedernes side for at skabe mest muligt beredskab og sikkerhed for pengene. Dansk Energi anfører, at cybertruslen bør ses som en tværsektoriel udfordring, hvorfor der er behov for tværsektoriel koordinering og videndeling.

IT-Politisk Forening anfører, at placeringen af tilsynsmyndighederne inden for hvert ministeriums område ses at være inden for NIS-direktivets rammer, men at det generelt kan blive vanskeligt at udnytte synergieffekter mellem forskellige tilsynsområder, når tilsynsressourcerne bliver spredt mellem fire-fem (eller flere) myndigheder.

NIS-direktivet har et bredt anvendelsesområde, og direktivet berører så forskellige sektorer som finanssektoren, sundhedssektoren og energisektoren. En forudsætning for en målrettet og erhvervsvenlig implementering af direktivet, hvor danske erhvervsvirksomheder ikke pålægges unødvendige byrder, er, at de nye lovgivningskrav nøje tilpasses de enkelte sektorer. På grund af den store forskel mellem de sektorer, der er omfattet af direktivet, er det ikke muligt at fastlægge et fælles niveau for informationssikkerhed for alle de omfattede sektorer.

Derfor indebærer lovforslaget, at det såkaldte sektoransvar videreføres ved implementeringen af NIS-direktivet, således at de enkelte ressortmyndigheder inden for eget område fortsat har ansvaret for at fastsætte og håndhæve de nødvendige regler om informationssikkerhed.

Det bemærkes i den forbindelse, at der på flere ministerområder allerede er fastsat national regulering på informationssikkerhedsområdet. Også derfor er det hensigtsmæssigt, at implementeringen af NIS-direktivet varetages af ressortmyndighederne, der kan sikre, at den eksisterende lovgivning tilpasses, hvor det er nødvendigt, således at overlappende forpligtelser undgås, og således at erhvervsvirksomhederne ikke pålægges unødvendige byrder.

Center for Cybersikkerhed vil desuden som nationalt centralt kontaktpunkt og CSIRT varetage en række tværgående funktioner, herunder monitorering af hændelser på nationalt plan samt formidling af information om risici og hændelser til sektormyndighederne og andre relevante interessenter. Dermed vil der ske en koordination og erfaringsudveksling på tværs af sektorerne.

2. Forholdet til den nationale strategi for cyber- og informationssikkerhed

Dansk Energi finder det bemærkelsesværdigt, at dele af lovforslagets initiativer (nationalt centralt kontaktpunkt og CSIRT) kommer før offentliggørelsen af den nationale strategi for cyber- og informationssikkerhed.

NIS-direktivet skal være gennemført af medlemsstaterne senest den 10. maj 2018. Den nationale regulering, der bl.a. skal implementere direktivets sikkerhedskrav og underretningspligter, skal derfor være trådt i kraft inden denne dato.

Udover sikkerhedskrav og underretningspligter fastsætter NIS-direktivet, at hver medlemsstat skal vedtage en national strategi for sikkerheden i net- og informationssystemer, der fastlægger, hvilke strategiske mål og konkrete politiktiltag, der skal gennemføres for at nå og bibeholde et højt sikkerhedsniveau i net- og informationssystemer.

Regeringen er i færd med at udarbejde en ny national cyber- og informationssikkerhedsstrategi. Strategien forventes færdiggjort i første kvartal af 2018 og forventes bl.a. at have fokus på de enkelte sektorer, herunder energisektoren, der forudsættes at kunne indgå i et nært dagligt, operationelt samarbejde med bl.a. Center for Cybersikkerhed, herunder også i forhold til centerets funktioner efter NIS-direktivet. Strategien vil således have fokus på at videreføre og styrke de initiativer, der allerede er gennemført på cyber- og informationssikkerhedsområdet, bl.a. i forbindelse med implementeringen af NIS-direktivet, og vil i den forbindelse have særlig fokus på en helhedsorienteret tilgang.

3. Placering af funktionen som nationalt centralt kontaktpunkt hos Center for Cybersikkerhed

Dansk Energi finder, at der i Danmark er behov for en national, koordinerende enhed for oplysninger og informationsudveksling vedrørende cybertruslen. Dansk Energi anfører, at Center for Cybersikkerhed kan være dette koordinerende kontaktpunkt, men opfordrer regeringen til at undersøge og afdække andre muligheder. Dansk Energi anfører i den forbindelse, at konstruktionen med Center for Cybersikkerhed har vist sig at være uhensigtsmæssig, bl.a. fordi centeret har haft svært ved at komme ind på livet af de samfundskritiske sektorer qua sektoransvaret og fordi der har været en generel udfordring for centeret med at rekruttere og fastholde stærkt specialiserede medarbejdere. Dansk Energi vurderer endvidere, at Center for Cybersikkerheds forankring under Forsvarets Efterretningstjeneste udgør en barriere for et mere frugtbart samarbejde med sektorerne og virksomhederne. Dansk Energi anfører, at der er behov for en endnu tættere dialog med de samfundsvigtige aktører for at sikre, at placeringen af et nationalt centralt kontaktpunkt skaber mest værdi for såvel myndigheder som virksomheder.

Retspolitisk Forening anfører, at i betragtning af, at Center for Cybersikkerhed er henlagt til Forsvarets Efterretningstjeneste, forekommer det som en logisk konsekvens, at også dette område placeres her, men at der med lovforslaget sker en yderligere kompetencetilførsel til Forsvarets Efterretningstjeneste, og at der dermed, for så vidt angår Forsvarsministeriets område, sker en styrkelse af denne efterretningstjenestes virksomhed på områder af ikke forsvarsmæssig karakter.

NIS-direktivet forpligter medlemsstaterne til at udpege et nationalt centralt kontaktpunkt. Det nationale centrale kontaktpunkt skal udgøre et forbindelsesled, som faciliterer det grænseoverskridende samarbejde med andre medlemsstater, CSIRT-netværket og Samarbejdsgruppen. Samarbejdsgruppen er et forum etableret i EU-regi, der fokuserer på det strategiske samarbejde om sikkerhed i net- og informationssystemer mellem medlemsstater. Herudover skal det centrale kontaktpunkt én gang om året forelægge en sammenfattende rapport for Samarbejdsgruppen vedrørende underretninger om hændelser i henhold til NIS-direktivet.

Center for Cybersikkerhed, der er en del af Forsvarets Efterretningstjeneste, er i forvejen national it-sikkerhedsmyndighed og står for en forebyggende rådgivnings- og oplysningsvirksomhed om cybersikkerhed i forhold til både den offentlige og private sektor samt en reaktiv indsats ved cyberangreb. Center for Cybersikkerhed varetager en række myndighedsopgaver i den forbindelse, og centeret er således allerede den centrale nationale myndighed vedrørende cybersikkerhed. På den baggrund vil varetagelsen af funktionen som nationalt centralt kontaktpunkt ligge i naturlig forlængelse af centerets øvrige opgaver.

4. Placering af funktionen som CSIRT hos Center for Cybersikkerhed

Dansk Energi bakker ikke op om, at funktionen som CSIRT placeres hos Center for Cybersikkerhed, Dansk Energi finder, at denne funktion bør være forankret tættest muligt på de virksomheder, som CSIRT-enheden skal understøtte og medvirke til at beskytte mod cybertruslen. At forankre en (eller flere) operationelle CSIRT-enhed(-er) under Center for Cybersikkerhed som en del af Forsvarets Efterretningstjeneste, harmonerer ifølge Dansk Energi ikke med virksomhedernes og operatører af samfundsvigtig og forsyningskritisk infrastrukturs behov for tidlig varsling og størst mulig åbenhed om cybertruslen for at kunne beskytte kritisk infrastruktur bedst muligt. Dansk Energi er ikke betrygget i, at Center for Cybersikkerhed i tilstrækkelig grad kan, må og vil dele information om det aktuelle trusselbillede i rette tid til, at virksomhederne kan modstå og/eller dæmme op for truslen. Dansk

Energi anfører i den forbindelse, at Center for Cybersikkerheds forankring i Forsvarets Efterretningstjeneste opleves som en barriere for nødvendig videndeling.

Institut for Menneskerettigheder bemærker generelt vedrørende udpegningen af Center for Cybersikkerhed som CSIRT, at dette vil have som konsekvens, at stadig flere oplysninger fra en række samfundssektorer således vil kunne blive udvekslet med Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste.

IT-Politisk Forening finder det meget betænkeligt, at Center for Cybersikkerhed, som er en del af Forsvarets Efterretningstjeneste, får en så betydelig rolle i forhold til cybersikkerheden i den offentlige og private sektor i Danmark. IT-Politisk Forening finder af principielle årsager, at såvel den danske CSIRT som det danske centrale kontaktpunkt bør være civile myndigheder.

NIS-direktivet forpligter medlemsstaterne til at udpege en eller flere nationale CSIRT'er. En CSIRT skal fungere som national beredskabsenhed til håndtering af it-sikkerhedshændelser og vil bl.a. have til opgave at foretage monitorering af hændelser på nationalt plan samt udsende tidlige varslinger, advarsler og meddelelser samt formidle information til relevante interessenter om risici og hændelser. CSIRT'en vil endvidere skulle reagere på hændelser og udarbejde dynamiske risiko- og hændelsesanalyser samt situationsrapporter. Endelig vil CSIRT'en skulle deltage i CSIRT-netværket og etablere samarbejde med den private sektor.

At Center for Cybersikkerhed skal varetage funktionen som national CSIRT efter NIS-direktivet indebærer imidlertid ikke, at centeret nødvendigvis skal håndtere konkrete hændelser på sektorniveau. Centeret kan dog behandle anmodninger om bistand til at håndtere en cybersikkerhedshændelse fra en operatør eller en tilsynsmyndighed i en anden sektor, ligesom centeret kan tilbyde sin bistand i forhold til at foretage foranstaltninger i den forbindelse.

Center for Cybersikkerhed besidder allerede i dag mange af de kompetencer, der er nødvendige for at kunne varsle sektorerne samt reagere på hændelser, og centeret vil tillige kunne operere døgnet rundt. CSIRT-funktionen efter NIS-direktivet har således en nær sammenhæng med Center for Cybersikkerheds eksisterende opgaver.

Det bemærkes i øvrigt, at Center for Cybersikkerhed har oplyst, at centeret og Dansk Energi har haft en god og positiv dialog som opfølgning på Dansk Energis høringssvar. I den forbindelse er der enighed om, at der skal ske en styrkelse af samarbejdet gennem en mere regelmæssig og ledelsesrettet kommunikation mellem Center for Cybersikkerhed, Dansk Energi og Dansk Energis medlemsvirksomheder. Der er endvidere enighed om, at det også vil styrke det daglige samarbejde, at energisektoren fremover indstationerer en sektorekspert i Center for Cybersikkerheds særlige trusselsvurderingsenhed, hvor der i forvejen er indstationeret eksperter fra telesektoren, sundhedssektoren og finanssektoren. Indstationeringen af sektoreksperter har bl.a. til formål at sikre, at kendskab til de særlige sektorspecifikke forhold og aktører kobles med Center for Cybersikkerheds viden, således at information deles rettidigt og med et operationelt sigte. Etablering af sektor-CERT'er i en eller flere sektorer, f.eks. en Energi-CERT, vil desuden kunne styrke samarbejdet omkring cybersikkerhed, da en sektorspecifik CERT vil være en naturlig samarbejdspartner for den nationale CSIRT og dermed for Center for Cybersikkerhed.

5. Placering af funktionen som tilsynsmyndighed for operatører af væsentlige internetudvekslingspunkter

IT-Politisk Forening anfører, at det kan overvejes at henlægge opgaven som tilsynsmyndighed for internetudvekslingspunkter under Energistyrelsen eller Erhvervsstyrelsen i stedet for under Center for Cybersikkerhed.

NIS-direktivet forpligter bl.a. medlemsstaterne til at udpege en eller flere nationale kompetente myndigheder. De nationale kompetente myndigheder fører tilsyn med anvendelsen af direktivet, og de betegnes derfor som tilsynsmyndigheder. I Danmark udpeger de relevante ressortmyndigheder de tilsynsmyndigheder, der skal føre tilsyn med de enkelte sektorer.

På Forsvarsministeriets område implementerer lovforslaget bl.a. de dele af NIS-direktivet, der vedrører sikkerhedskrav og underretningspligter på informationssikkerhedsområdet for internetudvekslingspunkter. Center for Cybersikkerheds rolle som tilsynsmyndighed for internetudvekslingspunkter har nær tilknytning til centerets eksisterende rolle som tilsynsmyndighed for informationssikkerhed i telesektoren. Placeringen af tilsynskompetencen vedrørende internetudvekslingspunkter hos Center for Cybersikkerhed ligger derfor i naturlig forlængelse af centerets nuværende opgaver, hvilket vil medvirke til at sikre en effektiv udnyttelse af ressourcerne.

6. Forholdet til persondataretten

IT-Politisk Forening og Institut for Menneskerettigheder anfører, at den danske implementering af NIS-direktivet ikke ses at leve op til direktivets artikel 2, hvorefter behandling af personoplysninger skal udføres i overensstemmelse med databeskyttelsesdirektivet. IT-Politisk Forening anfører i den forbindelse, at dette vil kunne medføre, at Center for Cybersikkerhed på grund af manglende retsgarantier om databeskyttelse ikke vil kunne modtage personoplysninger fra andre EU-lande og således ikke vil kunne opfylde sine forpligtelser efter direktivet. IT-Politisk Forening anbefaler, at regeringen genovervejer Forsvarets Efterretningstjenestes undtagelse fra databeskyttelsesforordningen, og at Center for Cybersikkerhed som minimum omfattes af reglerne i forbindelse med varetagelse af funktionerne efter NIS-direktivet.

Center for Cybersikkerhed vil som led i centerets nye funktioner som tilsynsmyndighed, nationalt centralt kontaktpunkt og CSIRT skulle behandle visse personoplysninger, dog primært i form af f.eks. IP-adresser, ligesom der i visse tilfælde bl.a. vil kunne ske videregivelse heraf.

Databeskyttelsesdirektivet er i dansk ret implementeret ved persondataloven, og det følger af persondatalovens § 2, stk. 10, at loven ikke gælder for behandlinger, der udføres for politiets og forsvarets efterretningstjenester. Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, og centerets virksomhed er dermed undtaget fra persondataloven, jf. også § 8 i lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed. Denne retstilstand ventes videreført, når persondataloven med virkning fra 25. maj 2018 erstattes af databeskyttelsesforordningen og databeskyttelsesloven.

Uanset at Center for Cybersikkerheds virksomhed er undtaget fra persondataloven, gælder størstedelen af de centrale principper i persondataloven for centeret, jf. kapitel 6 i lov om Center for Cybersikkerhed. Det gælder dog bl.a. ikke oplysningspligt over for den registrerede samt den registreredes indsigtsret og indsigelsesret.

Særligt for så vidt angår Center for Cybersikkerheds virksomhed som national it-sikkerhedsmyndighed og som myndighed for informationssikkerhed og beredskab på teleområdet blev det i forbindelse med forslaget til lov om Center for Cybersikkerhed overvejet, om der var behov for at indføre oplysningspligt over for den registrerede samt give den registrerede indsigts- og indsigelsesret, således som det er tilfældet efter persondataloven. Det fremgår i den forbindelse af lovforslaget (lovforslag nr. L 192, Folketinget 2013-14, fremsat den 2. maj 2014), at det karakteristiske for disse myndighedsopgaver er, at centerets myndighedsudøvelse som altovervejende hovedregel er rettet mod andre myndigheder og virksomheder. Det var derfor vurderingen, at der ikke var behov for at indføre en oplysningspligt i forhold til fysiske personer. Det blev dog også vurderet, at der var behov for at skabe en mulighed for at lade persondatalovens kapitel 8-10 (om oplysningspligt over for den registrerede, den registreredes indsigtsret og øvrige rettigheder, bl.a. indsigelsesret) finde anvendelse på de pågældende myndighedsområder.

Det følger således af § 8, stk. 2, i lov om Center for Cybersikkerhed, at forsvarsministeren kan bestemme, at kapitel 8-10 i persondataloven helt eller delvis skal finde anvendelse for Center for Cybersikkerhed vedrørende centerets virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet.

Center for Cybersikkerheds rolle som tilsynsmyndighed for operatører af væsentlige internetudvekslingspunkter har betydelige lighedspunkter med centerets tilsvarende rolle som tilsynsmyndighed for teleudbydere. Forsvarsministeriet finder det på den baggrund naturligt, at bemyndigelsen i § 8, stk. 2, også omfatter de myndighedsopgaver, som Center for Cybersikkerhed måtte få tillagt i forbindelse med implementeringen af NIS-direktivet. Der henvises i den forbindelse til det udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed, som i perioden fra 13. december 2017 til 15. januar 2018 har været i høring. Med det pågældende lovforslag vil bl.a. bemyndigelsen i § 8, stk. 2, blive tilpasset til den nye regulering på databeskyttelsesområdet.

7. Jurisdiktion

Netnod henviser til, at det er uhensigtsmæssigt, at en organisation kan blive forpligtet til at underrette om en hændelse til mere end én myndighed, herunder på tværs af medlemsstaterne. Netnod henviser til, at organisationen risikerer at skulle foretage underretning om den samme hændelse til myndighederne i henholdsvis Sverige og Danmark.

Det følger af NIS-direktivet, at hver medlemsstat skal fastsætte sikkerhedskrav og underretningspligter for operatører af væsentlige tjenester. En operatør, der har aktiviteter i en eller flere medlemsstater, vil på den baggrund være omfattet af de nationalt fastsatte sikkerhedskrav og underretningspligter i de pågældende medlemsstater. En operatør vil derfor eventuelt skulle foretage underretning om en hændelse til både Center for Cybersikkerhed og en eller flere andre medlemsstaters myndigheder m.v.

Det følger af NIS-direktivet, at medlemsstaterne i forbindelse med identifikation af operatører af væsentlige tjenester skal høre hinanden, hvis en operatør leverer en væsentlig tjeneste i flere medlemsstater. Derudover sker der overordnet koordination af medlemsstaternes implementering af NIS-direktivet i Samarbejdsgruppen i EU-regi.