ERHVERVSMINISTERIET

NOTAT

6. februar 2018
Sagsnr. 18/00208
/ERST

Høringsnotat vedr. forslag til lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester

1. Indledning

Forslag til lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester og ændring af lov om finansiel virksomhed og lov om kapitalmarkeder har været i høring fra den 17. oktober 2017 til den 17. november 2017.

Lovforslaget gennemfører direktiv 2016/1148/EU om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (herefter NIS-direktivet) på Erhvervsministeriets område.

NIS-direktivet dækker en række samfundsvigtige sektorer, herunder transport-, energi-, sundheds- og finanssektoren samt visse digitale tjenester. Direktivet gennemføres sektorvis i overensstemmelse med sektoransvarsprincippet på beredskabsområdet. Nærværende lovforslag gennemfører direktivet på Erhvervsministeriets områder, hvor direktivet skal gennemføres på det finansielle område samt for udbydere af domænenavnssystemer (som fx .org, .dk og .net) og for visse digitale tjenester (onlinemarkedsplads, onlinesøgemaskine og cloud computing-tjeneste).

Lovforslaget indeholder krav om, at aktører af væsentlige tjenester skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene i forhold til sikkerheden i de net- og informationstjenester, de udbyder. Formålet er samlet set at styrke net- og informationssikkerheden overfor it-sikkerhedshændelser.

Lovforslaget indeholder herudover krav om rapportering af it-sikkerhedshændelser både for så vidt angår domænenavnssystemer og visse digitale tjenester samt for den finansielle sektor. Endelig er der bestemmelser vedr. myndighedssamarbejde og tilsyn. De nærmere regler vedrører tekniske og organisatoriske sikkerhedskrav samt procedurer for indberetning af it-sikkerhedshændelser, der vil blive fastsat i bekendtgørelser.

Der er modtaget i alt 22 høringssvar, hvoraf 9 myndigheder, organisationer m.v. har haft bemærkninger til lovforslaget.

De væsentligste bemærkninger fra de hørte parter gennemgås og kommenteres nedenfor.

Høringssvarene har alene givet anledning til mindre justeringer. Der er endvidere foretaget konsekvensrettelser for at sikre ensartethed i forhold til tværgående forhold i de forskellige ressortministeriers lovforslag, der implementerer NIS-direktivet inden for deres respektive områder. Endelig er der foretaget ændringer på baggrund af den lovtekniske gennemgang.

2. Generelle bemærkninger

DI/DI DIGITAL finder det positivt, at der er lagt vægt på, at implementeringen af NIS-direktivet i dansk ret sker uden unødige byrder for virksomhederne.

DI/DI DIGITAL bemærker endvidere, at den del af lovforslaget, som vedrører udbydere af domænenavnssystemer og visse digitale tjenester er meget generelt, og at der lægges op til, at væsentlige dele af implementeringen af NIS-direktivet efterfølgende bliver fastsat i bekendtgørelser, hvilket gør konsekvenserne af lovforslaget svære at gennemskue.

DIFO anfører, at den del af lovforslaget, som vedrører udbydere af domænenavnssystemer og visse digitale tjenester er udformet som en rammelov, og at den nærmere udmøntning vil ske i en bekendtgørelse, herunder hvem som på domæneområdet vil blive omfattet af lovgivningens krav til sikkerhedsforanstaltninger. I lyset heraf anmoder DIFO om, at relevante aktører, herunder DIFO, bliver inddraget rettidigt i forberedelsesfasen til bekendtgørelsen, således at alle involverede parter får reel mulighed for at indrette sig efter de nye regler.

ALCO Company mener, at det er hensigtsmæssigt, at NIS-direktivet implementeres sektorvis. ALCO finder, at sikkerheden i de tjenester, som den del af lovforslaget, som vedrører udbydere af domænenavnssystemer og visse digitale tjenester vedrører, kan betragtes som en kæde, hvor kæden ikke er stærkere end det svageste led. Det er derfor selskabets opfattelse, at det er en fejl, at små virksomheder og mikrovirksomheder er undtaget fra lovforslagets krav om sikkerhedsforanstaltninger.

Kommentar

Med hensyn til bemærkningerne fra DI/DI DIGITAL og DIFO om, at lovforslaget er meget generelt, kan det oplyses, at der er valgt en tekstnær implementering af NIS-direktivet i lovforslaget. De nærmere krav fastsættes i bekendtgørelsesform. Dette muliggør, at der kan tages højde for eventuelle kommende retningslinjer, som fastsættes i EU-regi. Det gælder fx i forhold til sektorspecifikke kriterier for fastlæggelse af omfanget af en hændelses konsekvenser og anvendelsen af sikkerhedsstan-

darder. Derved undgås, at der sker overimplementering af direktivets krav i dansk lovgivning.

Hvad angår DIFO's ønske om, at interessenterne inddrages i forbindelse med udarbejdelsen af bekendtgørelsen, kan det oplyses, at interessenterne vil blive inddraget i forbindelse med fastsættelse af de nærmere regler.

For så vidt angår ALCO's bemærkninger om det uhensigtsmæssige i at undtage fra lovforslaget små virksomheder og mikrovirksomheder, som udbyder digitale tjenester, kan det oplyses, at dette følger af NIS-direktivet.

3. Bemærkninger til konkrete emner
Kommenteringen af høringssvarene vil ske med udgangspunkt i følgende overordnede opdeling:

3.1 Sikkerhedspolitikker

3.2 Afgrænsning af DNS-udbydere

3.3 Behandling af personoplysninger

3.4 Underretning af hændelser/koordinering af indberetninger

3.5 Videregivelse af oplysninger til CSIRT

3.6 Orientering af offentligheden

3.1 Sikkerhedspolitikker
DIFO bemærker, at den overordnede linje i angivelsen af krav i den del af lovforslaget, som vedrører udbydere af domænenavnssystemer og visse digitale tjenester fraviges i forhold til § 12, stk. 3, hvorefter Erhvervsstyrelsen kan kræve dokumentation af operatørerne for gennemførelse af sikkerhedspolitikker og i afsnit 3.1.1.3. i lovforslagets almindelige bemærkninger, hvori det forudsættes, at der udarbejdes sikkerhedsstrategier. DIFO anbefaler derfor, at lovforslaget beskriver, hvad der forstås ved sikkerhedspolitikker og sikkerhedsstrategier.

Kommentar:
Lovforslagets § 12, stk. 3 er en implementering af NIS-direktivets artikel 15, stk. 2. På baggrund af DIFO's bemærkning er der i lovforslagets bemærkninger foretaget en uddybning af, hvad der menes med sikkerhedspolitikker. Endvidere ændres sikkerhedsstrategier i afsnittene 3.1.1.3 og 3.1.2.2 til sikkerhedspolitikker, idet der rettelig skal stå sikkerhedspolitikker de pågældende steder.

3.2 Afgrænsning af DNS-udbydere
IT-Politisk Forening anfører med henvisning til NIS-direktivets artikel 1, stk. 3 og betragtning nr. 7, at udbydere af internetadgangstjenester ikke er

omfattet af NIS-direktivet, da der i forvejen er EU-regulering af net- og informationssikkerheden på området.

IT-Politisk Forening finder endvidere, at definitionen af DNS-tjenester i NIS-direktivet sammenholdt med undtagelsen af visse virksomheder i artikel 1, stk. 3 medvirker til, at det er uklart, hvilke tjenester, der er omfattet af forslaget.

Kommentar:
DNS-tjenesten oversætter et domænenavn til en IP-adresse (en talkode) og fungerer som internettets telefonbog.

Erhvervsministeriet har forelagt spørgsmålet om forståelsen af NIS-direktivets artikel 1, stk. 3 og betragtning nr. 7 for EU-Kommissionen.

Spørgsmålet er, om en internetudbyder, som er omfattet af sikkerhedskravene i telerammedirektivet for så vidt angår internettjenesten, bliver omfattet af NIS-direktivets sikkerhedskrav for et eventuelt udbud af en DNS-tjeneste, eller om DNS-tjenesten er omfattet af telerammedirektivets krav til sikkerhed.

Det er EU-Kommissionens opfattelse, at en udbyder af en internetadgangstjeneste med hensyn til et eventuelt udbud af en DNS-tjeneste er omfattet for DNS-tjenestens vedkommende af NIS-direktivets bestemmelser. Kommissionen har efterfølgende præciseret dette i bilaget til Kommissionens meddelelse (COM(2017) 476 final) om "Fuld udnyttelse af NIS – mod en effektiv gennemførelse af direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen".

Dette indebærer, at alle væsentlige udbydere af DNS-tjenester er omfattet af NIS-direktivets bestemmelser om sikkerhedskrav, underretningskrav mv. med hensyn til udbuddet af DNS-tjenesten. Alle væsentlige udbydere af DNS-tjenester vil således være underlagt samme krav.

Kommissionens forståelse af NIS-direktivets bestemmelser på ovennævnte område er lagt til grund i lovforslaget.

Med hensyn til den uklarhed, som IT-Politisk Forening finder, der er om hvilke DNS-tjenester, som er omfattet af lovforslaget, er således adresseret med Kommissionens fortolkning, idet alle væsentlige udbydere af DNS-tjenester er omfattet af lovforslagets bestemmelser.

Det kan supplerende oplyses, at lovforslagets kriterier til identifikation af væsentlige udbydere vil blive nærmere fastlagt i en kommende bekendtgørelse. Det er hensigten i bekendtgørelsen at få fastlagt grænseværdier,

fx i form af brugen af en væsentlig tjeneste, der afgrænser, hvornår en operatør anses for at drive en væsentlig tjeneste. Dette vil blive præciseret i lovforslagets bemærkninger. Det er således hensigten at kun de operatører med mange brugere og stor trafikvolumen bliver omfattet af krav til sikkerhedsforanstaltninger mv.

3.3 Behandling af personoplysninger

Datatilsynet påpeger, at det i forhold til muligheden for at orientere offentligheden om hændelser er uklart i hvilket omfang, der også vil kunne indgå personoplysninger. Det skal således sikres, at sådanne oplysninger ikke offentliggøres i strid med lovgivningen om persondatabeskyttelse. I den forbindelse bemærker Datatilsynet, at hvis der behandles personoplysninger i de net- og informationssystemer, som er omfattet af lovudkastet, skal den gældende lovgivning om behandling af personoplysninger iagttages.

Datatilsynet bemærker endvidere, at det forudsættes, at den til enhver tid gældende lovgivning om behandling af personoplysninger iagttages, hvis der videregives fortrolige personoplysninger til Center for Cybersikkerhed.

Kommentar

Det kan bekræftes, at personoplysninger ikke offentliggøres i strid med lovgivningen om persondatabeskyttelse, ligesom den gældende lovgivning om behandling af personoplysninger iagttages ved behandling af personoplysninger i de net- og informationssystemer, som er omfattet af lovudkastet.

Af bemærkninger til lovforslaget til ny lov om domænenavnssystemer fremgår bl.a, at "i tilfælde hvor der er tale om behandling af personhenførbare oplysninger, vil lovgivningen for databeskyttelse, jf. Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger finde tilsvarende anvendelse. Reglerne i databeskyttelsesforordningen vil finde anvendelse, når disse træder i kraft den 25. maj 2018."

For så vidt angår de foreslåede ændringer til lov om finansiel virksomhed og lov om kapitalmarkeder skal det bemærkes, at det fremgår af lovforslagets bemærkninger til den foreslåede § 354 h i lov om finansiel virksomhed og til den foreslåede § 236 a i lov om kapitalmarkeder, at Finanstilsynet får mulighed for at kunne offentliggøre oplysninger om konkrete hændelser, såfremt offentlighedens kendskab hertil er nødvendigt for at forebygge eller håndtere en igangværende hændelse. Finanstilsynet vurderer i den sammenhæng hvorvidt offentliggørelse skal ske ved at offentliggøre navnet på den berørte virksomhed, eller om det samme resultat kan nås med en anonymiseret offentliggørelse, som alene om-

fatter den konkrete hændelse. En offentliggørelse vil dog altid forudsætte, at den berørte virksomhed er blevet hørt herom.

Det skal i øvrigt bemærkes, at ved behandling af personoplysninger herunder offentliggørelse og videregivelse af personoplysninger vil den til enhver tid gældende lovgivning om persondata finde anvendelse, hvorfor behandling af persondata altid vil ske under iagttagelse af gældende lovgivning. Dette vil blive præciseret i lovforslagets bemærkninger til lov om finansiel virksomhed samt til lov om kapitalmarkeder.

3.4 Underretning af hændelser/koordinering af indberetninger

DI/DI DIGITAL mener, at det bør fremgå mere klart, hvilken type hændelser, der vil kunne være omfattet af rapporteringspligten.

Finans Danmark bemærker ligeledes i sit høringssvar, at bemærkningerne til bekendtgørelseshjemlerne i forhold til lov om finansiel virksomhed er meget generelle. Det anføres endvidere, at det bør fremgå mere klart, hvilke typer af hændelser, man forestiller sig, vil være omfattet af rapporteringspligten.

IT-Politisk Forening har anført betænkeligheder ved, at der efter lovforslaget alene skal ske direkte underretning til den kompetente myndighed (Erhvervsstyrelsen eller Finanstilsynet), som herefter vil kunne videregive oplysninger til CSIRT'en.

DI/DI DIGITAL anfører ligeledes, at myndighederne i udarbejdelsen af procedurerne for virksomhedernes indberetning skal tage højde for de øvrige underretningsforpligtelser, som virksomhederne har i henhold til anden regulering, således at dobbeltrapportering undgås.

Landbrugsstyrelsen anfører, at det bør tages til efterretning, at kravene i lovudkastets §§ 6 og 7 om hhv. underretning af Erhvervsstyrelsen om væsentlige hændelser og viderebringelse af oplysninger til Center for Cybersikkerhed er tilstrækkeligt koordineret.

Finans Danmark foreslår endeligt, at myndighederne ved udvikling af rapporteringssystemer tager højde for andre rapporteringsforpligtelser, som virksomhederne er underlagt i henhold til anden regulering, så dobbeltrapportering undgås.

Kommentar

Lovforslagets kriterier for rapportering af hændelser til myndighederne følger tekstnært NIS-direktivets bestemmelser. De nærmere regler vil blive fastlagt i bekendtgørelser på baggrund af eventuelle retningslinjer, der måtte blive udarbejdet i EU-regi. Det er hensigten i bekendtgørelser-

ne at få fastlagt grænseværdier for, hvornår en hændelse anses for væsentlig. Dette vil blive præciseret i bemærkningerne til lovforslaget.

For så vidt angår Finans Danmarks bemærkning om, at det bør fremgå mere klart af bemærkningerne til bekendtgørelseshjemlerne i lov om finansiel virksomhed, hvilke typer af hændelser, man forestiller sig, vil være omfattet af rapporteringspligten, skal det bemærkes, at det fremgår af lovforslaget vedrørende ændringerne i lov om finansiel virksomhed, at rapporteringspligten omfatter en hændelse, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som virksomheden leverer. En hændelse skal forstås som værende enhver begivenhed, der har en negativ indvirkning på sikkerheden i virksomhedens net- og informationssystemer, hvilket vil blive præciseret i bemærkningerne til lov om finansiel virksomhed og lov om kapitalmarkeder.

Som et eksempel herpå kunne tænkes at en bank bliver ramt af et hackerangreb, som betyder, at mange systemer, der normalt anvendes af både privatkunder i hele Danmark og internt i banken, ikke længere kan anvendes. Konsekvensen er, at de ramte brugere ikke vil kunne tilgå deres ellers berettigede bankfunktioner, hvilket i sidste ende vil kunne have økonomiske og samfundsmæssige konsekvenser.

Et andet eksempel kunne tænkes at være, at der under en større systemopdatering i en bank, sker en teknisk fejl, som betyder at der ikke kan gennemføres transaktioner på tværs af landegrænser i flere dage. Disse manglende transaktioner vil kunne have store konsekvenser både økonomisk og samfundsmæssigt, eftersom brugere ikke vil have mulighed for at styre transaktionerne.

Som nævnt ovenfor omfatter rapporteringspligten en hændelse, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som virksomheden leverer. En hændelses konsekvenser fastlægges navnlig ud fra antallet af brugere, der berøres af afbrydelsen af den væsentlige tjeneste, hændelsens varighed og den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen. For at Finanstilsynet og Center for Cybersikkerhed, som CSIRT og nationalt kontaktpunkt, kan vurdere en hændelses konsekvenser, skal underretningerne derfor indeholde oplysninger, der gør det muligt at fastslå hændelsens omfang og herunder eventuelle grænseoverskridende konsekvenser for hændelsen.

Det forventes derfor fastsat på bekendtgørelsesniveau i medfør af den foreslåede § 71, stk. 2, 2. pkt., at en underretning skal indeholde oplysninger om antallet af brugere, som berøres af afbrydelsen af den væsentlige tjeneste, oplysninger om hændelsens varighed, oplysninger om den geografiske udbredelse med hensyn til det område, der er berørt af hæn-

delsen, oplysninger om eventuelle grænseoverskridende konsekvenser af hændelsen m.v.

For så vidt angår bemærkningerne IT-Politisk Forening om, at underretning skal ske direkte til den kompetente myndighed (altså Erhvervsstyrelsen eller Finanstilsynet), hvorfor der kan opstå problemstillinger i forhold til videregivelsen af oplysninger til Center for Cybersikkerhed som CSIRT, skal det bemærkes, at lovforslaget vil blive justeret således, at indberetninger om hændelser skal ske til både den kompetente myndighed (Erhvervsstyrelsen eller Finanstilsynet) og til Center for Cybersikkerhed som CSIRT. Dermed vil Center for Cybersikkerhed hurtigst muligt modtage alle relevante oplysninger direkte fra operatøren.

Endelig skal det bemærkes, at Erhvervsministeriet er opmærksom på, at der som følge af en række direktiver og forordninger, såsom NIS-direktivet, Persondataforordningen og 2. betalingstjenestedirektiv (PSD2), vil være en række rapporteringsforpligtelser for de finansielle virksomheder. Disse mange rapporteringsforpligtelser kan medføre, at en hændelse vil være omfattet af flere regelsæt og at en finansiel virksomhed dermed vil skulle afrapportere flere gange til flere forskellige myndigheder. Det forventes i den sammenhæng, at der vil blive etableret en fælles indberetningsløsning, fx gennem en fælles portal på virk.dk, hvorigennem en operatør af væsentlige tjenester vil kunne indgive alle rapporteringer, hvormed dobbeltrapportering undgås. Dette vil blive præciseret i lovforslagets bemærkninger. En fællesoffentlig indrapporteringsløsning indebærer endvidere, at Center for Cybersikkerhed, som vil være national CSIRT, kan modtage indberetning af sikkerhedshændelser på samme tid som henholdvis Erhvervsstyrelsen og Finanstilsynet. En CSIRT er en national it-beredskabsenhed, der håndterer sikkerhedshændelser, og som har ansvar for at sikre samarbejdet om sikkerheden i net- og informationssystemer i EU. Indberetningsløsningen sætter således Center for Cybersikkerhed i stand til hurtigt at kunne håndtere og varsle om indberettede sikkerhedshændelser.

Det er i lovforslaget blevet præciseret, at Erhvervsstyrelsen kan videregive oplysninger til Center for Cybersikkerhed om hændelser med henblik på Center for Cybersikkerheds opfyldelse af deres opgaver som nationalt centralt kontaktpunkt og CSIRT.

3.5 Videregivelse af oplysninger til CSIRT

Finans Danmark henstiller i sit høringssvar til, at det præciseres i lovforslaget at videregivelse af oplysninger om eventuelle hændelser i medfør af de foreslåede ændringer til § 354, stk. 6, nr. 44, i lov om finansiel virksomhed alene kan ske under hensyntagen til opretholdelse af sektorens og den finansielle institutions sikkerhed og forretningshemmeligheder.

DI/DI DIGITAL mener, at det bør præciseres at videregivelse af oplysninger om konkrete hændelser til Center for Cybersikkerhed og orientering af offentligheden alene kan ske under hensyntagen til opretholdelse af erhvervslivets sikkerhed og forretningshemmeligheder. En sådan videregivelse eller orientering må således ikke kompromittere sikkerheden i erhvervslivet.

Institut for Menneskerettigheder finder, at det er principielt problematisk, at der i takt med implementeringen af NIS-direktivet i dansk ret videregives oplysninger fra sektormyndighederne til den nationale CSIRT, der etableres som en del af Center for Cybersikkerhed under Forsvarets Efterretningstjeneste (FE), særligt i lyset af de begrænsninger dette medfører i forhold til indsigt og databeskyttelse, idet FE som udgangspunkt er undtaget fra offentlighedsloven, persondataloven og dele af forvaltningsloven. Institut for Menneskerettigheder anbefaler i den forbindelse, at regeringen genovervejer og præciserer, hvorledes beskyttelsen af personoplysninger i den danske gennemførelse af NIS-direktivet lever op til EU's databeskyttelsesregler og Charter om Grundlæggende Rettigheder.

IT-Politisk Forening, anfører, at man er betænkelig ved, at Erhvervsstyrelsen eller Finanstilsynet ved hændelsesrapportering kan modtage personoplysninger (fx en IP-adresse), og at sådanne oplysninger vil blive videregivet til Center for Cybersikkerhed som national CSIRT, idet FE er undtaget fra de EU-retlige regler om persondatabeskyttelse.

Kommentar
I dag er oplysninger, som Finanstilsynet modtager som led i sin tilsynsvirksomhed, underlagt en skærpet tavshedspligt efter bl.a. § 354, stk. 1, i lov om finansiel virksomhed, og Finanstilsynet må alene videregive fortrolige oplysninger til en række nærmere angivne personer, myndigheder m.v. og under nærmere angivne betingelser. Derudover er alle, der modtager fortrolige oplysninger fra Finanstilsynet, undergivet den samme skærpede tavshedspligt. Dette er direktivkrav.

Med lovforslaget foreslås det – på tilsvarende måde – at give Finanstilsynet mulighed for at videregive fortrolige oplysninger til Center for Cybersikkerhed under nærmere angivne betingelser. Det vil sige, at Finanstilsynet kun kan videregive oplysninger til Center for Cybersikkerhed, under forudsætning af, at oplysningerne er nødvendige for dem til opfyldelse af deres lovbestemte opgaver i deres egenskab af national CSIRT eller nationalt centralt kontaktpunkt. Også Center for Cybersikkerhed vil ved modtagelsen af oplysningerne være undergivet den skærpede tavshedspligt. Forslaget vil på den baggrund blive opretholdt.

Med hensyn til IT-Politisk Forenings og Institut for Menneskerettigheders bemærkninger, herunder spørgsmålet om, hvorvidt den danske implementering af NIS-direktivet er i overensstemmelse med direktivets artikel 2, hvorefter behandling af personoplysninger skal udføres i overensstemmelse med databeskyttelsesdirektivet, henvises til Forsvarsministeriets kommenterede høringsoversigt vedrørende forslag til lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.

Videregivelsen af oplysninger om hændelsesunderretninger til CSIRT'en og det nationale centrale kontaktpunkt, som varetages af Center for Cybersikkerhed, er forudsat i NIS-direktivet og er således nødvendig med henblik på en korrekt implementering af direktivet.

For så vidt angår DI/DI DIGITAL's bemærkning om, at videregivelse af oplysninger om konkrete hændelser til Center for Cybersikkerhed og orientering af offentligheden alene kan ske under hensyntagen til opretholdelse af erhvervslivets sikkerhed og forretningshemmeligheder, vil Center for Cybersikkerhed sikre, at erhvervslivets sikkerhed og forretningshemmeligheder ikke kompromitteres i forbindelse med de hændelsesunderretninger, som centeret modtager.

Af lovforslaget fremgår, at myndighederne efter høring af udbyderen kan offentliggøre konkrete hændelser eller kræve, at udbyderen gør dette, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse, eller hvis offentliggørelse i øvrigt er i offentlighedens interesse. Det er ikke hensigten med offentliggørelsen, at erhvervslivets sikkerhed og forretningshemmeligheder kompromitteres.

3.6 Orientering af offentligheden

Forsvarsministeriet foreslår, at det er Center for Cybersikkerhed i koordination med sektormyndigheden, som står for orientering af offentligheden om hændelser, der berører flere samfundsmæssige sektorer. Forsvarsministeriet finder endvidere, at det alene bør være sektormyndigheden, som kan pålægge udbydere af digitale tjenester at offentliggøre hændelser, jf. § 11, stk. 2.

Finans Danmark henstiller i sit høringssvar til, at det præciseres i lovforslaget, at offentliggørelse af eventuelle hændelser i medfør af den foreslåede ændring til § 354 h alene kan ske under hensyntagen til opretholdelse af sektorens og den finansielle institutions sikkerhed og forretningshemmeligheder.

Kommentar

På baggrund af Forsvarsministeriets bemærkninger vil det i bemærkningerne til den del af lovforslaget, som vedrører udbydere af domænenavnssystemer og visse digitale tjenester blive præciseret, at Center for Cybersikkerhed i koordination med sektormyndigheden kan orientere offentligheden om hændelser, der berører flere samfundsmæssige sektorer. Det vil fortsat være sektormyndigheden, der står for orientering af offentligheden om hændelser i net- og informationssystemer, som kun berører den pågældende sektor.

Det vil endvidere blive præciseret i lovbemærkningerne til den del af lovforslaget, som vedrører udbydere af domænenavnssystemer og visse digitale tjenester, at det alene er den relevante tilsynsmyndighed, som kan pålægge udbydere af digitale tjenester at orientere offentligheden om hændelser.

For så vidt angår Finans Danmarks bemærkninger om, at det bør præciseres i lovforslaget til lov om finansiel virksomhed, at offentliggørelse af eventuelle hændelser alene vil kunne ske under hensyntagen til opretholdelse af sektorens og den finansielle institutions sikkerhed og forretningshemmeligheder, vil dette blive præciseret i den foreslåede § 354 h i lov om finansiel virksomhed.

Det skal i den forbindelse bemærkes, at det fremgår af NIS-direktivets præambel, at offentliggørelse af oplysninger om hændelser bør ske i en sammenfattet form. Det fremgår videre, at oplysninger der betragtes som værende fortrolige i overensstemmelse med EU-regler og nationale regler om forretningshemmeligheder, altid bør sikres denne fortrolighed under udførelsen af aktiviteterne og opfyldelsen af målene i direktivet. Det indebærer, at Finanstilsynets offentliggørelse af oplysninger om en hændelse bør tage hensyn til eventuelle forretningshemmeligheder. Lovforslagets § 354 h vil derfor blive præciseret, så det tydeligt fremgår, at offentliggørelsen ikke må indeholde fortrolige oplysninger om kundeforhold eller oplysninger omfattet af § 30 i lov om offentlighed i forvaltningen eller fortrolige oplysninger, der hidrører fra finansielle tilsynsmyndigheder i andre lande inden for eller uden for Den Europæiske Union, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse.

4. Oversigt over hørte organisationer, myndigheder mv.

24-7 Net, 3Shape A/S, Abakomp Internet Service ApS, AciaNet, ACN, Activewebs A/S, Adapt Group A/S, Adform A/S, Advice Digital ApS, Advokatrådet, AF-Vejen, AirNet, Akademisk Arkitektforening, ALCO Company ApS, Altibox Danmark A/S, Andelskassen, Andelsnet ApS, Antenneforening Vejen, Antennelauget Flimmer, Arbejderbevægelsens-Erhvervsråd, Arbejdsmarkedets Erhvervssygdomssikring (AES), Arbejdsmarkedets Tillægspension (ATP), Arbejdsskadestyrelsen, Ascio

Technologies Inc. Danmark, Asiainfo Denmark ApS, Atea A/S, Athena IT-Group A/S, ATZtel, Aura Energi, Axcess A/S, Azehosting ApS, Balle-Bredsten Antenneforening, Banedanmark, Barablu, BC Hospitality Group A/S, Bjerringbro Kabelnet, Bluegarden A/S, Bo Data ApS, Bolignetforeningen, Bolignet-Aarhus, Boligselskabernes Landsforening, Bonavent Invest A/S, Bording Data A/S, Bornfiber, Boxer, Brancheforum Digitale Medier (Branchen ForbrugerElektronik), Bredalsparken, Bredbånd Nord, Bricksite ApS, Bruun Rasmussen Kunstauktioner A/S, Børsmæglerforeningen, Baagøe ApS, C & B Systemer A/S, Cbrain A/S, CBS, CCI Europe A/S, Team Effektiv Regulering (TER), Cicoor Host & Saas ApS, Cirque Bredbånd A/S, Cloudnordic ApS, Co3 A/S, Colt Technology Services A/S, Columbus A/S, Combine, Comflex Networks ApS, Comm2ig A/S, Compusoft A/S, Concept Data A/S, Configit A/S, Connect-me, Conscia A/S, Corporate Services A/S, Cortex Consult A/S, CSC Danmark A/S, CSC Scandihealth A/S, Danaweb A/S, Dancenter A/S, DanDial Networks A/S, Dandomain A/S, Danhost ApS, Danish Venture Capital and Private Equity Association, Danmarks Grundforskningsfond, Danmarks Nationalbank, Danmarks Rederiforening, Danmarks Skibskredit A/S, Dansk Aktionærforening, Dansk Arbejdsgiverforening, Dansk Beredskabskommunikation A/S, Dansk BiblioteksCenter A/S, Dansk Byggeri, Dansk Ejendomsmæglerforening, Dansk Energi, Dansk Erhverv, Dansk Forening for International Motorkøretøjsforsikring (DFIM), Dansk Industri, Dansk Investor Relations Forening – DIRF, Dansk IT, Dansk Kabel TV A/S, Dansk Kredit Råd, Dansk Media, Dansk Metal, Dansk Pantebrevsforening, Danske Advokater, Danske eWire A/S, Danske Forsikringsfunktionærers Landsforening, Danske Handicaporganisationer, Danske Maritime, Danske Medier, Danske Regioner, DanskNet A/S, Datagruppen Multimed A/S, Den Danske Aktuarforening, Den Danske Dommerforening, Den Danske Finansanalytikerforening, Den danske Fondsmæglerforening, Det Centrale Handicapråd, Dialoga Group, Dansk Internet Forum (DIFO), DI Digital, Digital Rights, Digizuite A/S, Dis/Play A/S, DK-Hostmaster A/S, DLG Tele, DLX A/S, Dyrup Sanderum Antenneforening, EbeltoftS.net, Economic International A/S, Edlund A/S, Eg A/S, Ejendomsforeningen, Elro Erhverv A/S, Ementor Danmark A/S, Energi Fyn, Energi og Olieforum, EnergiMidt, Entertainment Trading ApS (Coolshop), Eriksminde Medienet, Evercall ApS, EWII, Exaweb ApS, Facilicom A/S, Falcon.io ApS, FasCom A/S, Fastline, FDA, FDE, FDFA – Foreningen af Danske Forsikringsmæglere og Forsikrings Agenturer, FDIH – Foreningen for Distance- og Internethandel, Fest.dk A/S, Fiber2you, Fiberby, Fibia, Finans og Leasing, Finans Danmark, Finansforbundet, Finanshuset i Fredensborg A/S,
Finansiel Stabilitet, Finansrådet, Finanssektorens Arbejdsgiverforening, Fionia IT ApS, Firstcom A/S, Fonet A/S, Forbrugerombudsmanden, Forbrugerrådet, Forbrugsforeningen, Foreningen af Danske Internet Medier (FDIM), Foreningen af Forretningsførere for Udenlandske Forsikringsselskaber, Foreningen af Interne Revisorer, Foreningen Bankdata, For-

eningen Danske Revisorer, FOREX, Forsikring & Pension, Forsikringens Datacenter A/S, Forsikringsmæglerforeningen, Frivilligrådet, Fsa-net.dk, FSR – danske revisorer, Funktionærernes og Tjenestemændenes Fællesråd (FTF), Faaborg Vest Antenneforening, FaaborgVestAF, G4S Security Services A/S, Galten Elværk, Garantiformuen, Garban-Intercapital Scandinavia, GE Erhverv A/S, GEV A/S, Gigabit, Gigahost ApS, Glenten, Global Crossing, GlobalConnect A/S, GlobalTel, Golden Planet ApS, Gram Bynet, GVD, Gørlev Antenneforening, Hansen Technologies Denmark A/S, HAS Hjørring Antenneselskab, HashøjNet, HEF, Hi3G Denmark ApS, Hiper, Horesta, Hosters A/S, Hosthouse Avalonia ApS, Hostnordic A/S, Højen Antennelaug, Høng Antennelaug, Håndværksrådet, Hårlev Antenneforening, I P Group A/S, I/S Bredbånd Nord, IBM Danmark, ICE.NET/Net1, Indsamlingsorganisationernes Brancheorganisation (ISOBRO), Info Key A/S, Info-Connect A/S, Infolink ApS, Installa'sjon, Internet Danmark Holding ApS, Internet4u/Computer Problemer, Intertrust (Denmark), Inventio.it A/S, Investeringsfondsbranchen, IP Group, ipnordic A/S, Ipvision A/S, ISACA Denmark Chapter, IT Forum Gruppen A/S, IT Overblik ApS, It Relation A/S, IT Universitetet, IT-Afdelingen A/S, IT-Branchen, Itide A/S, It-Kompagniet Jylland ApS, IT-Lauget Parknet, Itpilot ApS, IT-Politisk Forening, IT-R ApS, ITR Data A/S, J. H. Schultz Information A/S, Jansson Kommunikation A/S, Jaynet A/S, JCD A/S, Jels Antenneforening, Jerlev Antenneforening, JN Data A/S, Just Eat·dk ApS, Kabelplus, Kalundborg AF, Kjærgaard A/S, Kjærgaard-Nettet, Klarup Kabelnet, Klein-Data, KMD A/S, KommuneKredit, Kommunernes Landsforening, Konform A/S, Kortermann-Hosting ApS, Korup Antennelaug, Kronholm Kommunikation, Kuratorforeningen, Kviknet, Københavns Energi, Købmandstandens OplysningsBureau, Landbrug & Fødevarer, Landsforeningen af forsvarsadvokater, Landsforeningen for Bæredygtigt Landbrug, Landsorganisationen i Danmark (LO), Larsen Data ApS, Lauritz·com A/S, Lebera Mobile Danmark, LEGO GROUP, Lessor A/S, Lokale Pengeinstitutter, Lollands.net, Lycamobile, Lønmodtagernes Dyrtidsfond (LD), Markmonitor ApS, Maxtel.dk ApS, Mb Solutions A/S, Mediaconnect ApS, Mentor It A/S, Mira Internet ApS, Miracle A/S, Montes A/S, Morud Antenneforening, Mundio Mobile ApS, MWAzone, Mybanker, NAL MedieNet ApS, NASDAQ Copenhagen A/S, NEF Fiber A/S, Netcompany A/S, Net-group A/S, Netic A/S, Netip A/S, netordre·dk ApS, Netplan System Design.dk ApS, Nets Denmark A/S, Netsite A/S, Netteam A/S, NetTel ApS, Newangle Software ApS, Newwweb ApS, Next Level Internet A/S, NHC A/S, NHL Data ApS, Nianet A/S, NM Net ApS, Nn Hosting, NNIT A/S, Nordby Antenneforening/Fanø Net, Nordby AF, Nordea, Nordic Connect, Nordit A/S, Novasol A/S, Novicell ApS, NRGi, NTI Cadcenter A/S, Nyfors, Odder Antenneforening, One.com A/S, Orange Business Services Denmark A/S, Origo Systems ApS, Osted Nettet, Parcelhusejernes Landsforening, Parknet, PDC A/S, Pentacon A/S, Perspektiv Bredbånd, Phone-IT A/S, PIL - Professionelle Internet Løsninger ApS, Pi-Web I/S, Plenti, PLM Group

ApS, plusTEL ApS, PMR-brugergruppen, Polperro A/S, PostNord, Powerhosting ApS, Powernet ApS, Primanet, Proactive A/S, ProData Consult A/S, PROSA - Forbundet af it-professionelle, Proudwing ApS, Præstø Antennelaug, Puzzel A/S, Rambøll Danmark A/S, Redspot ApS, Region Hovedstaden, Regionale Bankers Forening, Revisornævnet, Ricoh Danmark A/S, Rosenholms Net, Rådet for større IT-sikkerhed, Sac-IT A/S, Sagitta ApS, Sammenslutning af Lokale Radio- og TVstationer, Samsø Bredbånd, Saxo Payments A/S, Schantz A/S, SE Fibernet A/S, SEAS-NVE, SEF Fiber, Semler Services A/S, Service Center Fyn/ Lars Falck Jershauge, Shopstart ApS, Silkeborg Data A/S, SimCorp A/S, Sitecore Corporation A/S, Skagen Antennelaug, Skagennet, Skibs- og Bådebyggeriets Arbejdsgiverforening, Skjern Bredbånd, Skodborg Antennelaug, Skovsby Internet, Softwork ApS, Sol og Strand Feriehusudlejning A/S, Solutio ApS, Sprint- Link Danmark ApS, Stilmark, Stofa A/S, Sundbynet, Syd Energi, Syddansk Universitet, Sydfyns Intranet A/S, Systematic A/S, Systemhosting A/S, Sæby Antenneforening, Sønderho Antenneforening, Talk IP, TDC A/S, Team Nethosting ApS, Telanco ApS, Teleankenævnet, Telecom X ApS, Teleklagenævnet, Telekommunikationsindustrien i Danmark, Telenor A/S, Telia Danmark, Tellio ApS, Tetra- Star A/S, ThomsenTrampedach, Thomson Reuters Nordic, Thyfon A/S, Thy-Mors Energi A/S, Tia Technology A/S, Timecomputer A/S, Tjeep, Toftlund Bynet, Transparency International Danmark, Travelmarket A/S, TREFOR Bredbånd A/S, Trifork A/S, Truecommerce Denmark ApS, Trådløsfiber .dk, TS Computer ApS, Tune Kabelnet, UNI-C, Unik System Design A/S, Uni-tel A/S, Universal Telecom, Unwire, Uptime-IT ApS, Verdo Tele A/S, Verizon Business A/S, Vest Net A/S, VestjyllandS.net, Vestnet ApS, Videbæk Antenneforening, Vindinge Antennelaug, Viptel ApS, Visma Consulting A/S, VK Data ApS, VP Securities A/S, Waoo! A/S, Webbureauet Infoserv ApS, Webhosting A/S, Webhot ApS, Western Union, Wified, WWI A/S, Yaygroup I/S, Yderholm Antenneforening, ZebNet, ZenSystem, Zibra Wireless, Zitcom A/S, Ønet, Ørum Net, Aalborg Universitet, Aalbæk Bugt Antenneforening, Årslev Net, Færøernes Hjemmestyre via Rigsombudsmanden på Færøerne, Grønlands Selvstyre via Rigsombudsmanden i Grønland, Beskæftigelsesministeriet, Børne- og Socialministeriet, Energi-, Forsynings- og Klimaministeriet, Erhvervsministeriet, Finansministeriet, Forsvarsministeriet, Justitsministeriet, Kirkeministeriet, Kulturministeriet, Miljø- og Fødevareministeriet, Skatteministeriet, Statsministeriet, Sundheds- og Ældreministeriet, Transport-, Bygnings- og Boligministeriet, Uddannelses- og Forskningsministeriet, Udenrigsministeriet, Udlændinge- og Integrationsministeriet, Undervisningsministeriet, Økonomi- og Indenrigsministeriet, Arbejdsskadestyrelsen, Beredskabsstyrelsen, Datatilsynet, Energistyrelsen, Forsvarets Efterretningstjeneste, Konkurrence- og Forbrugerstyrelsen, Moderniseringsstyrelsen, Patent- og Varemærkestyrelsen, Politiets Efterretningstjeneste, Rigspolitiet, Rigsrevisionen, Sikkerhedsstyrelsen, Statens It, Statsadvokaten for Særlig Økonomisk og International

Kriminalitet, Styrelsen for It og Læring, Søfartsstyrelsen, Nævnenes Hus, Udbetaling Danmark.

5. Følgende organisationer, myndigheder mv. har haft bemærkninger til lovforslaget:
ALCO Company, Datatilsynet, DI/DI DIGITAL, DIFO, Finans Danmark, Forsvarsministeriet, Institut for Menneskerettigheder, IT-Politisk Forening, Landbrugsstyrelsen.