INSTITUT FOR
MENNESKE
RETTIGHEDER

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
MOBIL 9132 5775
LGH@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 17/02284-2

Forsvarsministeriet
Holmens Kanal 42
1060 København K
Danmark

fmn@fmn.dk, kopi til mfk@fmn.dk

23. NOVEMBER 2017

HØRING OVER UDKAST TIL FORSLAG TIL LOV OM SIKKERHED I NET- OG INFORMATIONSSYSTEMER FOR OPERATØRER AF VÆSENTLIGE INTERNETUDVEKSLINGSPUNKTER M.V.

Forsvarsministeriet har ved e-mail af 27. oktober 2017 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til udkast til forslag til lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.

Udkastet til lovforslag er et af flere forslag, der gennemfører det såkaldte NIS-direktiv (direktiv 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen). Udkastet gennemfører således direktivet på Forsvarsministeriets område samtidig med at andre udkast til lovforslag er udarbejdet på andre ministerområder.

Instituttet har en bemærkning vedrørende udpegningen af Center for Cybersikkerhed som såkaldt national "CSIRT" (Computer Security Incident Response Team), som led i direktivets gennemførelse.

I 2014, da lovforslaget til lov om Center for Cybersikkerhed (lov nr. 713 af 25. juni 2014) var i høring, bemærkede instituttet det problematiske i, at en række IT-sikkerhedsopgaver, som hidtil havde ligget i civilt regi, blev forankret i Forsvarsministeriets Efterretningstjeneste. Forsvarets Efterretningstjeneste er som udgangspunkt undtaget fra offentlighedslovens og persondatalovens anvendelsesområde og fra centrale dele af forvaltningsloven (undtaget i forhold til aktindsigt, partshøring, begrundelse).

Center for Cybersikkerhed forventes ifølge udkastet til lovforslag at blive udpeget som CSIRT. CSIRT'en skal blandt andet monitorere og håndtere IT-sikkerhedshændelser på nationalt plan, iværksætte tidlig varsling om risici og hændelser og deltage i et CSIRT-netværk i EU.

Som led i gennemførelsen af direktivet i andre sektorer, for eksempel vedr. den finansielle sektor, skal forskellige myndigheder kunne videregive oplysninger til Center for Cybersikkerhed under forudsætning af, at oplysningerne er nødvendige for Center for Cybersikkerhed til opfyldelse af centerets lovbestemte opgaver i sin egenskab af at være CSIRT.

I takt med at NIS-direktivet bliver gennemført i lovgivning vedrørende en række samfundssektorer vil stadig flere oplysninger således kunne blive udvekslet med Center for Cybersikkerhed i Forsvarets Efterretningstjeneste.

NIS-direktivets artikel 2, stk. 1, kræver, at behandling af personoplysninger i henhold til direktivet sker i overensstemmelse med EU's databeskyttelsesdirektiv. Fra 25. maj 2018 vil det i stedet være EU's databeskyttelsesforordning, der finder anvendelse. Ifølge den nuværende persondatalov, såvel som det forslag til ny databeskyttelseslov som justitsministeren har fremsat (L 68), er Forsvarets Efterretningstjeneste undtaget fra den gældende persondatalov og fremsatte databeskyttelseslov.

En dansk national CSIRT, etableret som en del af Center for Cybersikkerhed under Forsvarets Efterretningstjeneste, er således generelt undtaget for den EU-retlige ramme for databeskyttelse, som NIS-direktivets artikel 2 henviser til.

- Instituttet anbefaler, at regeringen genovervejer og præciserer, hvorledes beskyttelsen af personoplysninger i den danske gennemførelse af NIS-direktivet kan leve op til kravet i direktivets artikel 2 (samt artikel 8 i Charter om Grundlæggende Rettigheder).

Instituttet ønsker i den forbindelse endnu en gang at fremhæve det principielt problematiske i, at centrale, civile samfundsstrukturer i Danmark skal varetages af Forsvarets Efterretningstjeneste med de begrænsninger, det giver i forhold til indsigt og databeskyttelseskrav. Instituttet kan i den forbindelse henvise til sit høringssvar af 4. marts 2014 til lovforslaget til lov om Center for Cybersikkerhed.

Der henvises til sagsnr.: 2017/006372.

Med venlig hilsen

Lise Garkier Hendriksen
CHEFKONSULENT

DANSK ENERGI

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt pr mail til fmn@fmn.dk og til mfk@fmn.dk

Vedr. sagsnr.: 2017/006372

Dok. ansvarlig: PHA
Sekretær:
Sagsnr: s2017-888
Doknr: d2017-18926-2.0
24. november 2017

Høringssvar på lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.

Som brancheorganisation for el- og energibranchen takker Dansk Energi for muligheden for at afgive høringssvar på lovforslag om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v. (herefter benævnt lovforslaget).

Vores høringssvar repræsenterer i denne omgang landets elnetselskaber, centrale og decentrale elproducenter samt elhandlere og produktionsbalanceansvarlige virksomheder i den danske elsektor – altså aktører i én af landets samfundskritiske sektorer.

I vores høringssvar vil vi derfor primært fokusere på de forhold, hvor vi ser, at lovforslaget vil få eller kunne få indflydelse på beredskabet og sikkerheden i elsektoren.

Vi har valgt at opdele vores høringssvar inden for tre overskrifter:

- Sektoransvar i en verden med grænseoverskridende og tværsektorielle cybertrusler
- Center for Cybersikkerhed som nationalt centralt kontaktpunkt
- Center for Cybersikkerhed som national beredskabsenhed (CSIRT)

Generelt opfordrer vi fra Dansk Energis side til, at virksomhederne i de samfundskritiske sektorer tages endnu mere med på råd i forhold til at udtænke, hvilken national ramme inden for hvilken at virksomheder og myndigheder i fællesskab skal søge at bekæmpe, dæmme op for og håndtere cybertruslen. Dette bør ske ud fra det faktum, at virksomhederne udgør Danmarks "for-poster" i det danske "forsvarsværk" mod cybertruslen. Det bør dog også ske for at understøtte ambitionen om mere erhvervsrettet regulering, som samtidig understøtter en åben og tillidsbaseret videndeling om cybertruslen – noget, som Dansk Energi anser, som de centrale grundsten for nationens cyber- og informationssikkerhedsarbejde i fremtiden.

Dansk Energi og foreningens Beredskabs- og IT-sikkerhedsudvalg er til hver en tid åben for yderligere dialog om, hvordan myndighedernes fremtidige initiativer bedst og mest erhvervsvenligt kan implementeres og understøtte beredskabs- og IT-sikkerhedsarbejdet i den danske elsektor for i sidste ende at skabe reel sikkerhed til glæde for hele det danske samfund.

Sektoransvar i en verden med grænseoverskridende og tværsektorielle cybertrusler

I lovforslagets bemærkninger lægges der op til, at det nuværende sektoransvar skal fastholdes.

Dansk Energi ser imidlertid cybertruslen som en tværsektoriel udfordring. Af samme grund ser vi behov for tværsektoriel koordinering og videndeling.

Dansk Energi efterlyste derfor i efteråret 2016 på et ekstraordinært dialogmøde i Center for Cybersikkerheds Strategiske Samarbejdsforum (afholdt 6. september 2016) en tværsektoriel analyse af fordele og ulemper ved sektoransvarsprincippet i forhold til, at virksomheder og samfundsvigtige sektorer kan agere effektivt og dermed blive modstandsdygtig overfor en meget dynamisk cybertrussel.

I efteråret 2017 har Dansk Energi – som del af myndighedernes arbejde med den nye nationale strategi for cyber- og informationssikkerhed – givet bidrag til et sektor-indspil til Energistyrelsen på en halvdags workshop.

Vi ser frem til at se, hvilke tanker der er gjort og hvilke initiativer, som der lægges op til, når den nye nationale strategi for cyber- og informationssikkerhed offentliggøres.

Af samme grund finder vi det bemærkelsesværdigt, at dele af lovforslagets initiativer (nationalt kontaktpunkt og beredskabsenhed) kommer før offentliggørelsen af den nationale strategi for cyber- og informationssikkerhed.

Fra Dansk Energis side savner vi med andre ord en mere holistisk tilgang til cybertruslen fra myndighedernes side for at skabe mest muligt beredskab og sikkerhed for pengene. Vi opfordrer derfor til stadigt mere og tættere dialog mellem virksomheder og myndigheder om udfordringer og muligheder og deraf følgende fremtidige løsninger og initiativer.

<u>Center for Cybersikkerhed som nationalt centralt kontaktpunkt</u>

Dansk Energi er enig i, at vi i Danmark og herunder landets samfundsvigtige sektorer behøver en national, koordinerende enhed for oplysninger og informationsudveksling om cybertrusler.

Center for Cybersikkerhed kan være dette koordinerende kontaktpunkt. Vi ser dog også andre muligheder. Vi opfordrer derfor til, at disse muligheder undersøges og afdækkes i allernærmeste fremtid. Cybertruslen mod Danmark vil kun øges og blive forstærket de kommende år. Derfor er det vigtigt, at vi som nation hurtigst muligt får fundet frem til de "rigtige" initiativer, som vil kunne skabe mest værdi og sikkerhed for landet – herunder virksomhederne i de samfundsvigtige sektorer.

På mange leder og kanter har tilblivelsen af Center for Cybersikkerhed været en "hård fødsel". Intentionen har på mange punkter været god og rigtig. Konstruktionen har dog – i Dansk Energis optik – vist sig at være uhensigtsmæssig.

Center for Cybersikkerhed har fx haft svært ved at komme ind på livet af de samfundskritiske sektorer qua sektoransvaret og samarbejdet (eller mangel på samme) med de sektoransvarlige myndigheder.

På tilsvarende vis har flere virksomheder i Dansk Energis medlemskreds oplevet at dialogen med Center for Cybersikkerhed snarere har været en "monolog", hvor Center for Cybersikkerhed har ønsket en masse information fra virksomhederne, men reelt kun leveret meget lidt ny viden retur – og ofte først noget tid efter at web-medier og kommercielle sikkerhedsfirmaer har tilvejebragt informationen til virksomhederne. Virksomhederne i Dansk Energis medlemskreds – altså elselskaberne – har således kun oplevet relativ begrænset merværdi fra Center for Cybersikkerhed.

Endelige opleves der en generel udfordring for Center for Cybersikkerhed med at rekruttere og fastholde stærkt specialiserede medarbejder, hvor lønniveauet i det offentlige har svært med at konkurrere med tilsvarende i den private sektor.

Fra Dansk Energis side vurderer vi, at Center for Cybersikkerheds forankring under Forsvarets Efterretningstjeneste yderligere udgør en barriere for et mere frugtbart samarbejde med sektorerne og virksomhederne.

Derfor mener Dansk Energi, 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.

Center for Cybersikkerhed som national beredskabsenhed (CSIRT)

Dansk Energi kan ikke bakke op om, at Center for Cybersikkerhed skal være Danmarks nationale beredskabsenhed (herefter nævnt "CSIRT-enhed").

I Dansk Energis optik er CSIRT-enheder operationelle enheder, som 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 i Dansk Energis optik 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.

Til dato har Dansk Energi ikke oplevet en nævneværdig åbenhed fra Center for Cybersikkerheds side til, at vi er betrygget i, at Center for Cybersikkerhed (som en enhed under Forsvarets Efterretningstjeneste) i tilstrækkelig grad kan, må og vil dele information om det aktuelle trusselsbillede i rette tid til, at virksomhederne kan modstå og/eller dæmme op for truslen. Centrets forankring i Forsvarets Efterretningstjeneste opleves også her som en barriere for nødvendig videndeling.

Dansk Energi kan derfor ikke støtte op om, at Center for Cybersikkerhed udpeges som national CSIRT-enhed.

Etablering af CSIRT-enheder bør i stedet være en opgave, som de enkelte sektorer og virksomhederne selv skal løfte. Fx har den nordiske finanssektor etableret et CERT-samarbejde

i form af *Nordic Financial CERT*. På tilsvarende vis ses et sektorsamarbejde i Norge for den norske el- og energisektor i form af *KraftCERT*. Disse sektor-CSIRT-enheder har allerede i dag tæt og løbende dialog med nationale og internationale myndigheder.

Det bør i den forbindelse sikres, at sektorielle og operationelle CSIRT-enheder og myndigheder (både lovgivende og tilsynsførende) har en armslængde imellem sig. Dette er tilfældet i Norge. Operationelle CSIRT-enheder skal være og skal anses som en del af de enkelte virksomheders og sektorers operationelle beredskab mod cybertruslen og dermed en del af virksomhedernes beredskabsarbejde og beredskabsforanstaltninger.

Konkret for el-sektorens side skal nævnes, at den systemansvarlige virksomhed, Energinet, i dag varetager både en koordinerende rolle og en tilsynsrolle i elsektoren med virksomhedernes beredskabsarbejde. En forankring af en evt. fremtidig CSIRT-enhed, som tænkes at skulle dække og servicere den danske el-sektor, bør derfor etableres af sektorens virksomheder, men uafhængigt af Energinet for at sikre førnævnte armlængdeprincip mellem tilsynsmyndighedsrollen og sektorens operationelle og koordinerende beredskabsopgaver.

Dansk Energi bakker naturligvis op om, at virksomhederne og sektorerne skal være underlagt løbende underretningspligt til det nationale centrale kontaktpunkt således, at der ved beredskabssituationer, sikkerhedshændelser el.lign. der har væsentlig forstyrrende virkning på levering af virksomhedernes tjenester stadig kan tilvejebringes et nationalt overblik og sikres tværsektoriel koordinering og samtidig evt. suppleres med internationale informationer.

Endvidere skal en løbende underretningspligt, som også vil tilfredsstille Forsvarets Efterretningstjenestes behov naturligvis tilsikres.

Hvorledes underretningspligten og informationsudvekslingen mellem virksomheder, CSIRT-enheder, sektormyndigheder og nationalt kontaktpunkt skal effektueres og foretages i praksis bør naturligt overvejes og afstemmes mellem alle aktørerne i en konstruktiv dialog.

En sektor- og virksomhedsforankret tilgang til CSIRT-enheder harmonerer efter Dansk Energis opfattelse fint med kravene i NIS-direktivets Artikel 9.

Afslutningsvis anmoder Dansk Energi at blive sat på høringslisten til fremtidige høringer, som omhandler Center for Cybersikkerheds virke og cybertruslen mod landets samfundskritiske sektorer. Fremtidigt høringsmateriale bedes sendt til de@danskenergi.dk.

Med venlig hilsen
Dansk Energi

Peter Kjær Hansen

Vestre Landsret
Præsidenten

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt pr. mail til fmn@fmn.dk og mfk@fmn.dk

J.nr. 40A-VL-96-17
Den 31 10-2017

Forsvarsministeriet har ved brev af 27. oktober 2017 (sagsnr. 2017 006372) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Helle Bertung

Østre Landsret
Præsidenten

Den 30-10-17
J.nr.40A-ØL-97-17
Init: sdy

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Forsvarsministeriet har ved brev af 27. oktober 2017 (Sagsnr. 2017/006372) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Bent Carlsen

Ellen Busck Porsbo

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Dato 22. november 2017
Sagsbeh Andreas J. Teckemeier
Sagsnr 2017-152-36
Dok 12229

Høring over udkast til lovforslag om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.

Ved e-mail af 31. oktober 2017 har Forsvarsministeriet anmodet Tilsynet med Efterretningstjenesterne om en udtalelse vedrørende ovennævnte lovforslag.

I den anledning kan tilsynet oplyse, at udkastet ikke giver anledning til bemærkninger.

Med venlig hilsen
Tilsynet med Efterretningstjenesterne

v/Emil Bock Greve
Sekretariatschef

Borgergade 28, 1.
DK-1300 København K
t 25 50 10 34
www.tet.dk

DATATILSYNET

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt til: fmn@fmn.dk og
mfk@fmn.dk
Cc: jm@jm.dk

2. november 2017

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2017-112-0791
Dok.nr. 449527
Sagsbehandler
Viktor Ingemann
Herskind
Direkte 3319 3242

Vedrørende høring over udkast til forslag til lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v. – ministeriets sagsnr. 2017-006372

Ved brev af 27. oktober 2017 har Forsvarsministeriet anmodet om Datatilsynets eventuelle bemærkninger til ovennævnte udkast til lovforslag.

Udkastet giver umiddelbart ikke Datatilsynet anledning til bemærkninger. Datatilsynet skal for god ordens skyld gøre opmærksom på, at databeskyttelsesforordningen[1] – som skal erstatte persondataloven – får virkning fra den 25. maj 2018.

Kopi af dette brev sendes til Justitsministeriets Lovafdeling til orientering.

Med venlig hilsen

Viktor I. Herskind

[1] 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.

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt per email til **fmn@fmn.dk**
med kopi til **mfk@fmn.dk**

IT-Politisk Forening
c/o Jesper Lund
Carl Bernhards Vej 15, 2.tv
1817 Frederiksberg C

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 24. november 2017

Høringssvar vedr. udkast til forslag til lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v. (sagsnr. 2017/006372)

Lovforslaget gennemfører NIS-direktivet på Forsvarsministeriets område. Efter lovforslaget skal Center for Cybersikkerhed være kompetent myndighed for internetudvekslingspunkter (IXP'er), som i NIS-direktivet (bilag II) hører under sektoren digital infrastruktur. Derudover skal Center for Cybersikkerhed udføre de tværgående opgaver efter NIS-direktivet (opgaver på tværs af sektorer på nationalt plan og på tværs af landegrænser på EU-plan) som CSIRT og nationalt centralt kontaktpunkt.

Lovforslaget følger strukturen og terminologien i NIS-direktivet. IT-Politisk Forening har i dette høringssvar bemærkninger til regeringens overordnede strategi for at gennemføre NIS-direktivet, placeringen af tilsynsansvaret for IXP'er og behandlingen af personoplysninger i forbindelse med underretning af hændelser.

Regeringens overordnede strategi for at gennemføre NIS-direktivet

Regeringen har valgt at gennemføre NIS-direktivet med sektorspecifikke love, hvor en eksisterende institution under det pågældende ministerium får tilsynsopgaven som

kompetent myndighed. NIS-direktivets artikel 8, stk. 1 overlader det til medlemsstaterne at fastsætte, om der skal være en eller flere kompetente myndigheder. En kompetent myndighed for hvert ministeriums område er som sådan inden for rammerne af artikel 8, stk. 1. Hvis der kommer 4-5 (eller flere) kompetente myndigheder i Danmark (jf. sektoropdelingen i bilag II i NIS-direktivet), kan tilsynsressourcerne blive spredt mere end godt er, og synergieffekter mellem forskellige tilsynsområder kan blive vanskelige at udnytte.

Et væsentligt element i NIS-direktivet er at medlemsstaterne skal vedtage en samlet national strategi for sikkerheden i net- og informationssystemer, og der skal være en effektiv informationsudveksling på tværs af sektorer på nationalt plan samt mellem EU-landene på internationalt plan. De tværgående opgaver vil blive varetaget af den danske CSIRT-enhed og det centrale kontaktpunkt, jf. NIS-direktivet. Efter lovforslaget placeres disse opgaver hos Center for Cybersikkerhed.

Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, som generelt opererer under andre rammebetingelser end civile myndigheder, for eksempel med betydelige undtagelser fra offentlighedsloven, forvaltningsloven og persondataloven. IT-Politisk Foreninger finder det meget betænkeligt, at Center for Cybersikkerhed via gennemførelsen af NIS-direktivet får en så betydelig rolle i forhold til cybersikkerheden i den offentlige og private sektor i Danmark. Af principielle årsager mener vi, at de(n) danske CSIRT(er) og det centrale kontaktpunkt bør være civile myndigheder.

Det gælder ikke mindst i de situationer, hvor det kan blive nødvendigt at behandle personoplysninger i forbindelse med underretning af den kompetente myndighed om hændelser. Dette punkt uddybes nedenfor.

Placeringen af tilsynsansvaret for IXP'er

Efter lovforslaget hører internetudvekslingspunktet (IXP'er) under Forsvarsministeriets ressortområde. Nogle IXP'er vil være drevet som en del af en teleudbyder, hvor Center for Cybersikkerhed efter den gældende lovgivning (lov nr 1567 af 15/12/2015 om net- og informationssikkerhed) har

tilsynsansvaret for sikkerheden. Disse IXP'er hos teleudbydere vil dog være undtaget fra NIS-direktivet, jf. artikel 1, stk. 3, og dermed fra nærværende lovforslag.

De øvrige operatører af IXP'er, som ikke samtidig er teleudbydere, er ikke i dag underlagt et tilsyn fra Forsvarsministeriet. Det naturlige ressortområde for disse virksomheder er snarere Erhvervsstyrelsen (Erhvervsministeriet) eller Energistyrelsen (Energi-, Forsynings- og Klimaministeriet).

Inden for sektoren digital infrastruktur skal medlemsstaterne efter NIS-direktivet også identificere væsentlige operatører af DNS-tjenester. Internetforbindelser leveres typisk sammen med en DNS-tjeneste af en internetudbyder, som er omfattet af lov om informationssikkerhed med Center for Cybersikkerhed som tilsynsmyndighed. På trods af dette overlap placeres DNS-tjenesteudbydere på Erhvervsstyrelsens ressortområde (altså de DNS-tjenesteudbydere som ikke allerede er omfattet af lov om net- og informationssikkerhed) ifølge det lovforslag om gennemførelse af NIS-direktivet, som Erhvervsministeriet har sendt i høring.

På den baggrund kunne det også overvejes at placere tilsynsansvaret for væsentlige internetudvekslingspunkter hos Erhvervsstyrelsen, som er en civil myndighed.

Hvis hovedparten af de danske internetudvekslingspunkter er undtaget fra NIS-direktivet, fordi de drives af en teleudbyder som er omfattet af lov om informationssikkerhed, kan det af hensyn til synergieffekter i tilsynsarbejdet være hensigtsmæssigt at placere det generelle tilsynsansvar for væsentlige internetudvekslingspunkter under Center for Cybersikkerhed. Ifølge de specielle bemærkninger til lovforslagets § 2 vil et internetudvekslingspunkt være omfattet af NIS-direktivet og dermed lovforslaget, hvis det drives i et datterselskab eller associeret selskab af en teleudbyder, eller hvis flere (tele)udbydere i fællesskab driver internetudvekslingspunktet. Ud fra den beskrivelse vil IT-Politisk Forening forvente, at de fleste danske internetudvekslingspunkter (IXP'er) ikke vil falde ind under lov om net- og informationssikkerhed, men i stedet vil være omfattet af de(t) lovforslag, som skal gennemføre NIS-direktivet. I så fald er eventuelle synergieffekter i

forhold til det eksisterende tilsyn med teleudbydere under Center for Cybersikkerhed begrænset.

IT-Politisk Forening vil på den baggrund opfordre regeringen til at overveje, om tilsynsansvaret for internetudvekslingspunkter skal placeres hos en civil tilsynsmyndighed, for eksempel Erhvervsstyrelsen.

Behandling af personoplysninger i forbindelse med underretning om hændelser

Lovforlagets § 4, jf. NIS-direktivets artikel 14, stk. 3, fastsætter en pligt til hurtigt at underrette Center for Cybersikkerhed (den kompetente myndighed) om hændelser, der har væsentlig betydning for kontinuiteten af de leverede tjenester.

I nogle tilfælde vil de nødvendige oplysninger i forbindelse med underretningen om en hændelse indeholde personoplysninger. Det kunne være IP-adresser, men også oplysninger fra et IT-systems databaser, som er forsøgt hacket (exfiltreret) og måske optræder i logfiler.

Lovforslaget har kun ganske få overvejelser om dette. Det nævnes i de almindelige bemærkninger pkt. 3.2.1, at videregivelse af oplysninger kan være omfattet af persondataloven, og efter lovforslagets § 6, stk. 4, nr. 4 må orientering til offentligheden om en hændelse ikke indeholde oplysninger om enkeltpersoners forhold, altså et krav om anonymisering af personoplysninger. Men derudover har lovforslaget ingen overvejelser om eksempelvis hjemmel i persondataloven til videregivelse af personoplysninger i forbindelse med en hændelse, og hvordan eventuelle videregivne personoplysninger skal behandles af Center for Cybersikkerhed.

Efter IT-Politisk Forenings opfattelse bør der fastsættes lovregler (eventuelt i bekendtgørelsesform), som begrænser behandlingen af personoplysninger til det strengt nødvendige for at klarlægge omfanget af hændelsen og dens eventuelle grænseoverskridende konsekvenser. Der bør desuden være et eksplicit krav om at disse personoplysninger skal slettes eller anonymiseres hurtigst muligt. Det vil være i overensstemmelse med udtalelsen af 14. juni 2013 vedrørende udkast til NIS-

direktivet fra Den Europæiske Tilsynsførende for Databeskyttelse [1].

Udover at Center for Cybersikkerhed som tilsynsmyndighed kan modtage oplysninger om hændelser fra IXP'er, jf. lovforslagets § 4, kan Center for Cybersikkerhed som CSIRT også modtage oplysninger om hændelser fra andre kompetente myndigheder (tilsynsmyndigheder). Efter NIS-direktivets artikel 10, stk. 2 skal CSIRT'en have adgang til oplysninger om hændelser, der er underrettet af operatører af væsentlige tjenester eller udbydere af digitale tjenester, hvis hændelserne ikke direkte rapporteres til CSIRT'en.

Det indebærer en forpligtelse til at videregive oplysninger om hændelser, herunder eventuelle personoplysninger, fra andre tilsynsmyndigheder til Center for Cybersikkerhed. En specifik hjemmel hertil bør fremgå af lovforslagene om at gennemføre NIS-direktivet på de respektive ministeriers område.

Center for Cybersikkerhed bør også have en specifik lovhjemmel til at modtage oplysninger om hændelser fra andre kompetente myndigheder, især hvis de indeholder personoplysninger. IT-Politisk Forening antager, at en sådan hjemmel til at modtage oplysninger fra andre tilsynsmyndigheder er underforstået i lovforslagets § 7, selvom § 7 og bemærkningerne hertil formelt kun nævner videregivelse fra Center for Cybersikkerhed til andre myndigheder i Danmark eller EU.

NIS-direktivets artikel 2, stk. 1 kræver, at behandling af personoplysninger i henhold til direktivet sker i overensstemmelse med direktiv 95/46/EF, og fra 25. maj 2018 databeskyttelsesforordningen (EU) 2016/679. Ifølge den nuværende persondatalov, og det forslag til ny databeskyttelseslov som Justitsministeren har fremsat 25. oktober 2017 (L 68), er Forsvarets Efterretningstjeneste (FE) undtaget fra de EU-retlige regler om databeskyttelse. Undtagelsen er for FE som institution, og vil derfor også gælde, når FE udøver aktiviteter inden for EU-retten, eksempelvis cybersikkerhedsopgaver i forbindelse med NIS-direktivet.

Hvis den fuldstændige undtagelse fra databeskyttelses-forordningen opretholdes for Center for Cybersikkerhed

(under FE), vil det efter IT-Politisk Forenings opfattelse ikke være muligt for Danmark at gennemføre NIS-direktivet på en korrekt måde. Beskyttelsen af personoplysninger i den danske gennemførelse af direktivet vil ikke kunne leve op til kravet i NIS-direktivets artikel 2 (samt artikel 8 i Charter om Grundlæggende Rettigheder).

NIS-direktivet forudsætter også, at der kan udveksles personoplysninger mellem EU-lande i forbindelse med cybersikkerhedsopgaver. Center for Cybersikkerhed vil som det nationale centrale kontaktpunkt ikke kunne modtage personoplysninger fra andre EU-lande og behandle dem i overensstemmelse med NIS-direktivets krav. De manglende retsgarantier om databeskyttelse ved videregivelse af personoplysninger fra andre EU-lande til Danmark kan ultimativt medføre, at andre EU-lande ikke vil videregive relevante oplysninger om cybersikkerhedshændelser til Danmark. Det vil selvsagt være til stor skade for den danske cybersikkerhed, det internationale samarbejde og formålet med NIS-direktivet.

IT-Politisk Forening vil anbefale, at regeringen i forbindelse med gennemførelsen af NIS-direktivet genovervejer den fuldstændige undtagelse af Forsvarets Efterretningstjeneste fra databeskyttelsesforordningen. Som minimum bør Center for Cybersikkerheds behandling af personoplysninger i forbindelse med varetagelsen af opgaver under NIS-direktivet ikke være undtaget fra databeskyttelsesforordningen.

Noter

[1] Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, 14. juni 2013 (resumé i EU-Tidende C 32 af 4.2.2014, s. 19) https://edps.europa.eu/sites/edp/files/publication/13-06-14_cyber_security_en.pdf

RETSPOLITISK FORENING
www.retspolitik.dk

HØRINGSSVAR

Høring over udkast til forslag til lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.

Svar til: fmn@fmn.dk og mfk@fmn.dk

Sagsnummer: 2017/006372

Retspolitisk Forening har ikke særskilte bemærkninger til dette lovforslag, der er en implementering af Europaparlamentet og Rådet har vedtaget direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet).

I betragtning af, at Center for Cybersikkerhed er henlagt til Forsvarets Efterretningstjeneste forekommer det som en logisk konsekvens, at også dette område placeres her.

Foreningen skal dog for god ordens skyld bemærke, 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. Foreningen har med høringssvar af 3. marts 2014 vedrørende høring over udkast til forslag til Lov om Center for Cybersikkerhed (sagsnummer: 2013/003214) udtalt sine principielle og konkrete betænkeligheder herved.

København, den 23. november 2017

Bjørn Elmquist
Formand

Leif Hermann
Bestyrelsesmedlem

netnod

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sagsnummer 2017/006372

Forslag til Lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.1

Netnod Internet Exchange i Sverige AB (Netnod) have been given the ability to come with comments on the proposal for implementation of the NIS-Directive in Denmark, Sagsnummer 2017/006372.

Netnod as a Swedish Organization that provide services in Sweden reports incidents according to the Swedish implementations of ***Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive),*** more specifically ***Lag (2003:389) om elektronisk kommunikation, Förordning (2003:396) om elektronisk kommunikation*** and ***PTSFS 2015:2 Post- och telestyrelsens föreskrifter om krav på driftsäkerhet***.

The IXP that Netnod operates in Malmö also gives the ability for organizations in Denmark to connect to Netnod equipment located in Denmark. Any incidents on such services are according to Netnod escalation and reporting processes reported to affected customers as well as according to instructions provided by The Swedish Post and Telecom Authority (PTS). Specifically ***PTSFS 2015:2 Post- och telestyrelsens föreskrifter om krav på driftsäkerhet***.

Regarding the proposed legislation, Netnod already in the comments provided for the proposed implementation in Sweden[1] point out it is important each organization do not have to report to multiple agencies (part from the affected customers) and this not only based on the services provided but also cross border situations like the services Netnod provides in Copenhagen.

[1] https://www.netnod.se/news/netnod-comments-on-the-nis-directive

Netnod
POST ADDRESS Box 30194
SE-104 25 Stockholm, Sweden

PHONE +46 8 562 860 00
FAX +46 8 442 09 67
info@netnod.se • www.netnod.se

netnod

In Sweden providers of IXP services are covered by the implementation of ***Directive 2002/21/EC*** and although the NIS-Directive (***Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union***) covers IXPs explicitly, the implementation of ***Directive 2002/21/EC*** has precedence. The following can be found in Article 1 of the NIS-Directive:

> 3. The security and notification requirements provided for in this Directive shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC, or to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.

Netnod wants to, based on this information, provide the following two comments:

1. The contact point for certain services depends on the implementation of Directive 2016/1148 in another member state. In the case of Sweden and IXPs, it might not be the CSIRT, but instead the regulator PTS as IXPs are covered by the implementation of relevant portions of Directive 2002/21/EC.

2. If an organization in one member state provide services in also other member states it is our view that the legislation applies that is implemented in the member state where the organization resides. In the case of Netnod that is Sweden, and oversight over Netnod operation is the The Swedish Post and Telecom Authority (PTS) and specifically in this case ***PTSFS 2015:2 Post- och telestyrelsens föreskrifter om krav på driftsäkerhet***.

For Netnod Internet Exchange i Sverige AB

Lars Michaël Jogbäck
CEO

Netnod
POST ADDRESS Box 30194
SE-104 25 Stockholm, Sweden

PHONE +46 8 562 860 00
FAX +46 8 442 09 67
info@netnod.se • www.netnod.se