Advokatrådet

ADVOKAT SAMFUNDET

Forsvarsministeriet
Holmens Kanal 42

1060 København K

fmn@fmn.dk + jch@fmn.dk

KRONPRINSESSEGADE 2
1306 KØBENHAVN K
TLF. 33 96 97 98

DATO: 30. april 2015
SAGSNR.: 2015 - 1166
ID NR : 345117

Høring - over udkast til forslag til lov om net- og informationssikkerhed

Ved e-mail af 21. april 2015 har Forsvarsministeriet anmodet om Advokatrådets bemærkninger til ovennævnte udkast.

Indledningsvist bemærker Advokatrådet, at høringsmaterialet – som juridisk og teknisk ikke er ukompliceret – er fremsendt med en frist på 13 dage, heraf 8 hverdage. En sådan frist udelukker i realiteten en nærmere stillingtagen til de forslag, der er indeholdt i høringsmaterialet, hvorfor det må påregnes, at en række myndigheder og organisationer reelt ikke har mulighed for at udfylde den rolle som høringspart, som forudsættes i en almindelig demokratisk proces.

Advokatrådet har i øvrigt følgende bemærkninger:

Lovforslagets § 9, stk. 6 og 7, indebærer, at Center for Cybersikkerhed efter et varsel på mindst syv arbejdsdage uden retskendelse har adgang til forretningslokaler hos udbydere, og udbydernes samarbejdspartnere, leverandører eller underleverandører med henblik på at påse overholdelsen af loven mv.

Advokatrådet finder, at bestemmelser som den foreliggende, der udgør en undtagelse til grundlovens udgangspunkt om boligens ukrænkelighed, alene bør anvendes, hvor det ikke er muligt med et mindre indgribende middel at tilgodese kontrolhensynene. Tilsynsbesøg uden retskendelse bør således have undtagelsens karakter.

Advokatrådet har noteret, at tilsynsbesøg ikke sker uvarslet. Endvidere har Advokatrådet noteret, at tilsynsbesøg alene vil blive anvendt, såfremt et tilsvarende resultat ikke kan opnås ved anvendelsen af andre og mindre indgribende tilsynsmuligheder.

Det er imidlertid Advokatrådets erfaring, at de mest vidtgående tilsynsbeføjelser ofte ender med at blive udgangspunktet i stedet for undtagelsen[1], hvorfor man bør være yderst tilbageholdende med at indføre ordninger som den foreslåede.

Med venlig hilsen

Torben Jensen

[1] Se Advokatrådets bemærkninger i høringssvar af 21. september 2012 til lovforslag om ændring af lov om behandling af personoplysninger, lov om udgivelsen af en Lovtidende og Ministerialtidende, lov om hittegods og lov om skyldners ret til at frigøre sig ved deponering (Effektiv Administration mv.).

DANSK ENERGI

Forsvarsministeriet
Holmens Kanal 42
1060 København K
Sendt pr mail til fmn@fmn.dk & jch@fmn.dk

Dok. ansvarlig: MOB
Sekretær:
Sagsnr: s2015-339
Doknr: d2015-5479-10.0
04. maj 2015

Høring over udkast til forslag til lov om net- og informationssikkerhed

Forsvarsministeriet har den 21. april 2015 sendt udkast til forslag til lov om net- og informationssikkerhed i høring.

Dansk Energi, som blandt andet forestår interessevaretagelse for de bredbåndsudbydere, som er etableret af en række danske energiselskaber, takker for muligheden for at komme med bemærkninger til det fremsendte lovforslag.

Dansk Energi har følgende generelle og konkrete bemærkninger:

Generelle bemærkninger
Lovforslaget er et led i udmøntningen af regeringsgrundlaget "Et Danmark, der står sammen" og den nationale strategi for cyber- og informationssikkerhed. Lovforslaget, som er nationalt i sit sigte, retter sig mod kommunikationsnet og –systemer, som logisk er indbyrdes forbundne på tværs af landegrænser. Net- og informationssikkerhedshed har således en international dimension, hvilket bl.a. afspejles i det direktivforslag om Net og Informationssikkerhed (NIS-direktivet), som afventer endelig vedtagelse. NIS-direktivet vil pålægge både medlemsstater og en bred række af markedsoperatører at gennemføre en række organisatoriske og sikkerhedsmæssige foranstaltninger, og vil efter vedtagelse skulle gennemføres i national lovgivning.

Dansk Energi vurderer på den baggrund, at der er behov for at få afklaret om – og i givet fald hvordan – de i NIS-direktivet indeholdte krav og foranstaltninger afviger fra de krav og foranstaltninger, som følger af nærværende lovforslag således, at det sikres, at der fremover kan skabes en effektiv europæisk samordning, og at der ikke forekommer ukoordinerede reguleringsindgreb på dette område.

I den forbindelse noterer Dansk Energi sig, at nærværende lovforslag kun vil have retsvirkning i forhold til udbydere, som har virksomhedsadresse i Danmark, uagtet at udbydere uden for Danmark vil have indflydelse på de sikkerhedstrusler, som retter sig mod dansk netinfrastruktur. Dette taler for, at der søges skabt grundlag for en koordineret fælleseuropæisk reguleringsindsats.

Høringsfristen for nærværende lovforslag er 4. maj. EU-Kommissionen har annonceret, at kommissionen den 6. maj vil komme med sin meddelelse om en strategi for et europæisk Digital Single Market (DSM). Det kan ikke udelukkes, at EU-Kommissionen vil præsentere sin holdning til elementer, som bør indgå i en kommende EU-regulering i forhold til net- og informationssikkerhed, databeskyttelse og *privacy, og* som kan have relevans i forhold til nærværende lovforslag. Dansk Energi undrer sig derfor over, at høringen gennemføres forud for EU-Kommissionens offentliggørelse af sin meddelelse om DSM.

Lovforslaget har karakter af bemyndigelseslovgivning, hvorved der gives vidstrakte beføjelser til Center for Cybersikkerhed (herefter blot benævnt CFCS). I bemærkningerne til lovforslaget lægges der ikke skjul på, at gennemførelsen af lovforslaget vil være forbundet med administrative og økonomiske konsekvenser for udbydere af offentlige net og tjenester.

Hvis alle udbydere pålægges samme krav og foranstaltninger, vil det blive langt mere byrdefuldt at efterleve for en mindre udbyder end en større udbyder. Det kræver således forholdsmæssigt større ressourcer for en mindre udbyder med eksempelvis få ansatte at skulle underlægges et omfattende tilsyn og kontrolbesøg fra CFCS samt efterleve pålagte foranstaltninger, deltage i øvelser og få sikkerhedsgodkendt medarbejdere m.v., end for en større udbyder. Dansk Energi savner derfor en vurdering i lovforslaget af, hvordan dette væsentlige forhold vedrørende forholdsmæssighed tænkes håndteret.

Dansk Energi vil samtidig opfordre til, at CFCS´ regeludstedelse og tilsyn efter lovforslaget funderes i risiko- og konsekvensanalyser, som holdes op imod det aktuelle trusselsbillede. Ikke alle udbydere må således forventes i samme grad at være eksponeret overfor it-sikkerhedsmæssige trusler og hændelser, ligesom konsekvenserne af at en bestemt udbyder kompromitteres kan være langt mere alvorlige, end hvis en anden udbyder kompromitteres. Dette tilsiger efter Dansk Energis opfattelse, at der bør indgå overvejelser om proportionalitet i både CFCS´regeludstedelse og i centerets konkrete tilsyn, i den udstrækning dette er muligt.

Lovforslaget indebærer, at den eksisterende regulering af informationssikkerhed og beredskab på teleområdet samles i en ny lov under Forsvarsministeriet. Det skaber, ifølge bemærkningerne til lovforslaget (punkt 1, "Indledning"), en mere sammenhængende og overskuelig regulering på området, hvilket Dansk Energi bifalder.

Dansk Energi foreslår, at der tages initiativ til at samle ikke kun lov, men også de til en hver tid gældende bekendtgørelser og eventuelle andre regelforskrifter, som udstedes i medfør af bestemmelser om informationssikkerhed og beredskab, således at udbyderne også vil finde reguleringen både sammenhængende og overskuelig.

Det fremgår af bemærkningerne til lovforslaget (under punkt 1 "indledning"), at med lovforslaget "(.:) sker der en skærpelse af kravene til teleudbydernes informationssikkerhed, således at kravene i højere grad tager højde for samfundets afhængighed af telenettet og afspejler det aktuelle trusselsbillede".

Trusselsbilledet må logisk forventes at variere over tid. Dansk Energi er på den baggrund bekymret for, om de krav, der til en hver tid er gældende, rent faktisk vil afspejle det til en

hver tid aktuelle trusselsbillede. Dansk Energi savner derfor en mekanisme i lovforslaget, som sikrer, at krav, som er pålagt udfra et konkret trusselsbillede, der med tiden viser sig at være uaktuelt, irrelevant, baseret på forkert kildeinformation eller lignende, bortfalder.

Konkrete bemærkninger
Dansk Energi vurderer, at formålsbestemmelsen (§1) er kortfattet og enkel men samtidig så vidtgående, at det kan være svært at ane rækkevidden i lovens anvendelsesområde. Dansk Energi foreslår, at formålsbestemmelsen præciseret med angivelse af det formål, som er angivet i bemærkningerne til § 1.

I forhold til lovforslagets bestemmelse i § 3 vurderer Dansk Energi, at rammerne for CFCS´s regeludstedelse er upræcise, hvilket vil skabe usikkerhed hos udbyderne om hvilke typer krav, de kan forventes at skulle imødegå. Bestemmelsens anvendelsesområde bør derfor søges afgrænset nærmere i bemærkningerne til bestemmelsen.

Lovforslagets bestemmelse i § 4(2) om oplysnings- og underretningspligt i forhold til indgåelse af leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf, vurderer Dansk Energi som særdeles indgribende i kommerciel aftaleforhandling og -indgåelse på dette område. Dansk Energi savner derfor, at der i lovforslaget redegøres for de kritierier og forudsætninger, som ligger til grund for antagelsen om, at CFCS skulle have bedre kompetencer end aftaleparterne og disses rådgivere til at vurdere de eventuelle trusler og sårbarheder i forhold til informationssikkerheden, som en konkret leveranceaftale om hardware, firmware eller software måtte give anledning til. Dansk Energi vurderer endvidere, at de standstill-perioder, som der efter bestemmelsen kan fastsættes regler om, og som samlet kan løbe op i 20 arbejdsdage, burde kunne afkortes eller helt undgås, hvis indsatsen fokuserer på en dialog om sikkerhed inden aftaleforhandling indledes.

Dansk Energi er herudover generelt bekymret for, at bestemmelsen i § 4(2) kan give anledning til en udvikling, hvor statslig intervention på dette og andre aftaleområder kan ske under henvisning til det til en hver tid gældende trusselsbillede, der tegner sig for landets økonomi og sikkerhed.

Dansk Energi står til rådighed, såfremt der er behov for en uddybning af ovenstående bemærkninger.

Med venlig hilsen

Dansk Energi
Morten Baadsgaard Trolle

DANSKE
REGIONER

fmn@fmn.dk
kopi til jch@fmn.dk.

04-05-2015
Sag nr. 15/959
Dokumentnr. 23854/15
Katrine Stokholm
Tel. 3529 8490
E-mail: kst@regioner.dk

Høringssvar vedrørende forslag til lov om net- og informationssikkerhed

Forsvarsministeriet har sendt forslag til lov om net- og informationssikkerhed i høring den 21. april 2015.

Danske Regioner hilser velkommen, at indsatsen for informationssikkerhed styrkes, herunder informationssikkerheden i net- og tjenester. I forhold til lovforslaget fremstår det dog ikke klart hvilke minimumskrav, der vil blive stillet til udbydere af offentligt tilgængelige net. Det er derfor vanskeligt at vurdere konsekvenserne af lovforslaget.

Det er Danske Regioners opfattelse, at interne net for regionernes medarbejdere og sundhedsdatanettet ikke er omfattet af lovforslaget, da der er tale om net, der ikke er offentligt tilgængelige.

Derimod findes der blandt andet på hospitalerne offentligt tilgængelige net for patienter og pårørende. Disse net forventes i forhold til Erhvervsstyrelsens nuværende praksis om offentlige net at blive omfattet af lovforslaget. Dette er dog ikke indgået i den vurdering af de økonomiske konsekvenser for regionerne, der er foretaget i forbindelse med lovforslaget om net- og informationssikkerhed. Den foreliggende konsekvensberegning af lovforslaget er således utilstrækkelig.

Danske Regioner finder derfor, at der er behov for at gennemføre en økonomisk konsekvensberegning af lovforslaget, jævnfør det udvidede totalbalanceprincip (DUT), der tager højde for de offentligt tilgængelige net i regionerne.

Dampfærgevej 22
Postboks 2593
2100 København Ø

T 35 29 81 00
F 35 29 83 00
E regioner@regioner.dk

Med venlig hilsen

Tommy Kjelsgaard

DATATILSYNET

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt til: fmn@fmn.dk
med kopi til jch@fmn.dk

4. maj 2015

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. 2015-112-0440
Sagsbehandler
Martin Nybye-Petersen
Direkte 3319 3216

Vedrørende høring over udkast til forslag til lov om net- og informationssikkerhed

Ved e-mail af 21. april 2015 har Forsvarsministeriet sendt ovennævnte udkast til Datatilsynet med henblik på at modtage tilsynets eventuelle bemærkninger hertil.

Datatilsynet skal i den forbindelse udtale:

Datatilsynet forudsætter generelt, at eventuelle behandlinger af personoplysninger som vil ske som følge af lovforslagets bestemmelser, vil ske indenfor rammerne af persondataloven.

1. Det følger af forslagets § 10, stk. 1, at:

> *§ 10. Center for Cybersikkerhed kan i ikke-anonymiseret form offentliggøre:*
> *1) Afgørelser truffet i medfør af § 3, stk. 2 og 3, og § 5, stk. 4, samt afgørelser truffet i medfør af regler, der er udstedt i medfør af §§ 3-5 og § 6, stk. 6.*
> *2) Resultater af tilsyn efter § 9.*
> *3) Resuméer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af denne lov eller regler, der er udstedt i medfør af denne lov.*
> *4) Resuméer af domme i retssager, hvor Center for Cybersikkerhed er part.*

Datatilsynet kan i den forbindelse henlede Forsvarsministeriets opmærksomhed på Justitsministeriets betænkning nr. 1516 vedrørende offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser m.v.

2. Datatilsynet skal endvidere henlede opmærksomheden på persondatalovens § 57. Det fremgår heraf, at der ved udarbejdelse af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger, skal indhentes udtalelse fra Datatilsynet.

Det fremsendte udkast giver ikke Datatilsynet anledning til yderligere bemærkninger.

Med venlig hilsen

Martin Nybye-Petersen

4. maj 2015

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt pr. mail: fmn@fmn.dk og jch@fmn.dk

Høring over udkast til forslag til lov om net- og informationssikkerhed

Teleindustrien, IT-Branchen og DI ITEK (herefter høringsparterne) har den 22. april 2015 modtaget udkast til forslag til lov om net- og informationssikkerhed (dateret den 21. april 2014) i høring.

Høringsparterne kan konstatere, at en del af de kritikpunkter, som det første lovudkast fra november 2014 gav anledning til, er imødekommet og forbedret i det reviderede lovudkast. Ikke desto mindre er det fortsat høringsparternes opfattelse, at lovudkastet medfører en høj grad af uforudsigelighed om hvilke forpligtelser udbyderne kan blive pålagt, uklarhed om hvilke retssikkerhedsmæssige garantier udbyderne har, samt risiko for, at danske udbydere skal afholde væsentlige omkostninger og pålægges store administrative byrder.

Lovudkastet kommer før der er lavet fælles europæiske regler på området, og der er derfor risiko for, at loven går videre end de kommende europæiske regler. Det kan betyde, at danske udbydere kan blive pålagt strengere krav end øvrige udbydere i EU til skade for investeringerne i dansk teleinfrastruktur samt skabelsen af et fælles europæisk marked for elektroniske kommunikationstjenester. Høringsparternes mener derfor, at lovgivningen på området bør afvente arbejdet i EU frem for at lave danske særregler.

Lovforslaget forekommer at være baseret på en formodning om, at udbyderne har en kommerciel interesse i at gå på kompromis med sikkerheden. Dette er ikke tilfældet – vi deler Forsvarsministeriets interesse i at optimere sikkerheden i selskabernes netværk.

I det følgende er høringsparternes bemærkninger til lovforslaget uddybet.

Forholdet til EU
Kommissionen har ved KOM (2013) 48 af 7. februar 2013 fremsat forslag til et direktiv om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele EU.

På baggrund af dugfriske meldinger fra det lettiske formandskab forstår vi, at direktivforslaget står foran trepartsforhandlinger mellem Kommissionen, Rådet og Parlamentet.

I Grund- og nærhedsnotatet til Folketingets Europaudvalg om det nævnte direktiv fremhæves det gentagne gange, at regeringen støtter en harmoniseret tilgang til net- og informationssikkerhed i EU:

"Det er regeringens foreløbige generelle holdning, at der er behov for regler på EU-niveau, der sikrer et ensartet og højt niveau af net- og informationssikkerhed på tværs af medlemsstaterne. Dette skal ikke mindst ses i lyset af internettets og private netværks grænseoverskridende karakter og betydning for det indre marked. Således er det væsentligt at sikre lige vilkår for markedsoperatører, som underlægges forpligtelserne. En samordning mellem medlemsstaterne vil kunne sikre, at risici og hændelser håndteres effektivt i den tværnationale sammenhæng på en effektiv og tilfredsstillende måde.

Samtidig er det regeringens foreløbige generelle holdning, at det er vigtigt, at direktivet fastlægger et minimum, for så vidt angår de væsentligste sikkerhedsaspekter. Det bemærkes dog, at det også er regeringens foreløbige generelle holdning, at der skal arbejdes henimod en hensigtsmæssig grænsedragning til spørgsmål af national sikkerhedsmæssig karakter. Der skal endvidere arbejdes for en nærmere tilrettelæggelse og udførelse af opgaverne, herunder eksempelvis fleksibilitet for så vidt angår vilkår, formater og procedurer for anmeldelse af sikkerhedshændelser og i angivelsen af opgaver som en CERT bør varetage.

Det er regeringens foreløbige generelle holdning, at der i højere grad skal sikres et øget samarbejde og øget informationsudvikling vedrørende standarder, og det er i den forbindelse oplagt at skele til allerede eksisterende standarder på området"

Med udsendelse af lovudkastet må høringsparterne konstatere, at regeringen tilsyneladende og uden nærmere begrundelse har ændret holdning hertil, endda på et tidspunkt, hvor direktivforslaget ser ud til at bevæge sig fremad i forhandlingsforløbet. Høringsparterne opfordrer til, at der holdes fast i den hidtidige linje, således at området ikke gøres til genstand for dansk enegang men afventer en harmoniseret europæisk tilgang.

Dette skal særligt ses i lyset af, at de fleste teleudbydere i Danmark indgår i koncernfællesskab med både tværeuropæiske og internationale udbydere, der kan vælge at placere aktiviteter eller dele heraf i andre lande, der ikke har samme krav, som i Danmark.

Skøn, afgørelser og klageadgang

Flere steder i lovforslaget tillægges CFCS vidtgående rettigheder til udøvelse af sit skøn, m.v. herunder bl.a. til at få adgang til faciliteter uden kendelse og pålægge udbyderne væsentlige økonomiske byrder. Lovforslaget ses imidlertid at mangle grundlæggende proportionalitetsbetragtninger og kriterier for udøvelse af myndighedens skøn.

Der ses i den forbindelse heller ikke i lovforslaget taget eksplicit stilling til klageadgangen for de mange afgørelser, påbud m.v., som CFCS måtte blive tillagt, skulle lovforslaget blive vedtaget.

På trods af den umiddelbare undtagelse af CFCS fra visse dele af forvaltningsloven i Lov om Center for Cybersikkerhed, må vi forudsætte, at CFCS's vide beføjelser – måske med undtagelse af i akutte nødstilfælde - skal udmøntes i form af forvaltningsretlige afgørelser, der bl.a. skal begrundes og kunne påklages, da hensigten vel næppe er at fritage teleudbyderne fra den-

ne sådan grundlæggende retssikkerhed i tilfælde, hvor der er tale om almindeligt tilsyn, planlægning m.v.

Henset til den uklarhed omkring begreber, afgrænsninger, skønsbeføjelser og øvrige bemyndigelser, som CFCS tillægges i medfør af lovforslaget, samt de væsentlige økonomiske konsekvenser og byrder for branchen, som baseres på disse uklarheder og skøn, skal vi opfordre til, at de forvaltningsretlige aspekter af CFCS's beslutninger samt klageadgangen eksplicit fremhæves i loven, således at CFCS – måske med undtagelse af handlinger i akutte nødstilfælde – omfattes af forvaltningsloven i sin helhed.

Med det nuværende lovudkast bliver det CFCS, der på den ene side skal udmønte den kommende detailregulering i bekendtgørelser og siden påse, at reglerne bliver overholdt. Efter høringsparternes opfattelse bliver CFCS således reelt både den lovgivende og udøvende magt i forhold til teleudbyderne. Høringsparterne skal derfor opfordre til, at kompetencen til at udstede de konkrete bekendtgørelser på området lægges hos Forsvarsministeren mens tilsynsopgaven lægges i CFCS. Dermed opnås der kunne opnås en vis grad om legalitetskontrol med de kriterier, der skal være til stede for at CFCS kan træffe forvaltningsretlige afgørelser over for udbyderne.

I den forbindelse skal høringsparterne fremhæve, at høringsparterne ikke anser det for tilstrækkeligt, at Forsvarsministeriet udgør klageinstans for afgørelser m.v. truffet af CFCS i medfør af lovforslaget, men skal foreslå, at der oprettes et klagenævn, der kan sikre den fornødne uvildighed og ekspertise på dette yderst teknisk komplicerede område.

Henset til de nævnte usikkerheder, herunder manglende definitioner og klarhed, brede formuleringer og vide skønsmarginer ses lovforslagets vurdering af de økonomiske byrder for erhvervslivet i øvrigt at være nedtonet til et urealistisk niveau.

Manglende definitioner/klarhed
Der mangler definitioner og klarhed om væsentlige elementer i loven. For det første er lovens formål at fremme net- og *informationssikkerheden* i samfundet, jf. § 1. Begrebet informationssikkerhed benyttes også hyppigt i lovens bestemmelser uden dog at være defineret. Begrebet er videreført fra andre love og er således ikke et nyt begreb, men ikke desto mindre bør det defineres i denne lov, da det er det essentielle begreb, som loven er baseret på.

Ligeledes er det foreslået i § 4, stk. 1, nr. 3, at Center for Cybersikkerhed (CFCS) skal underrettes ved *brud på informationssikkerheden*. Der mangler en definition af, hvad "brud på informationssikkerheden" er. Det er uklart om, begrebet svarer en sikkerhedshændelse som defineret i Lov om Center for Cybersikkerhed § 2, stk. 1. Tilsvarende er det uklart hvordan denne underretningspligt hænger sammen med den underretningspligt, der er over for Erhvervsstyrelsen i forhold til brud på persondatasikkerheden, jf. Kommissionens forordning nr. 611/2013.

For brede hjemmelsbestemmelser og lovgivning i bemærkningerne
På flere områder er de tillagte hjemmelsbestemmelser for CFCS for bredt formuleret. Eksempelvis fastslås det i § 3, stk. 3, at CFCS – såfremt det er af væsentlig samfundsmæssig betydning – kan påbyde udbydere at træffe konkrete foranstaltninger med henblik på at sikre informationssikkerheden.

Det er ikke nærmere angivet, hvilke kriterier, der skal opfyldes for at det kan udløse "konkrete foranstaltninger" over for udbyderne. På samme vis fore-

slås i § 5, stk. 4, at CFCS i beredskabssituationer og i andre ekstraordinære situationer kan påbyde udbyderne uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger i tilfælde af en hændelse eller trussel, der i betydeligt omfang påvirker eller vurderes at ville kunne påvirke udbuddet af net eller tjenester negativt.

Lovudkastet indeholder endvidere vidtgående lovgivning, som alene fremgår af lovens bemærkninger, det gælder bl.a. lovudkastets § 4, stk. 1, nr. 1, om afgivelse af oplysninger om udbyderens net og § 3, stk. 3, om indstationering af medarbejdere hos underleverandører, jf. kommentarerne nedenfor. Det er retssikkerhedsmæssigt betænkeligt, at der fremgår så bebyrdende forpligtelser, som ikke direkte er fremhævet i lovteksten.

Ovenstående forhold bevirker, at CFCS får en ubegrænset hjemmel til at pålægge udbyderne vidtgående forpligtelser. Forslagets uklarhed og brede formulering har som konsekvens, at udbyderne end ikke kan undersøge på forhånd, om deres systemer er indrettet til at foretage de foranstaltninger, som vil kunne påbydes, og hvor omkostningstungt det i givet fald vil kunne blive at opfylde de pågældende påbud. Hertil kommer desuden lovens § 14, stk. 1, nr. 1, der foreslår bødestraf for den, som undlader at efterkomme CFCS' påbud i medfør af to ovenstående bestemmelser, hhv. § 3, stk. 3 samt § 5, stk. 4.

Indstationering af medarbejdere hos underleverandører
Som eksempel på de vidtgående beføjelser der gives til CFCS fremgår det af bemærkningerne til § 3, stk. 3, (side 29) at der kan stilles krav til udbyderen om, at denne ved outsourcing fast skal indstationere egne medarbejdere i en underleverandørs organisation med henblik på at kunne udføre sikkerhedskontrol. Høringsparterne har vanskeligt ved at se, at udbyderne kan kræve at egne medarbejdere fast skal indgå i en underleverandørs organisation og at en sådan ordning kan gennemføres i praksis overfor globale leverandører af udstyr og driftsydelser.

Informationspligt
Efter lovudkastets § 4, stk. 1, nr. 1, og § 9, stk. 2, kan udbyderne pålægges en vidtgående informationsforpligtelse om udbyderens net. I lovbemærkningerne til § 4, stk. 1, nr. 1, (side 30) er det yderligere præciseret, at forpligtelsen bl.a. kan bestå i, at frembringe oplysninger om udstyrsleverandørens hardware og software. Der kan således være tale om, at udbyderne bliver forpligtet til at fremskaffe eksempelvis kildekode eller andre forretningshemmeligheder, hvilket kan vise sig at være umuligt, idet udstyrsleverandøren ikke vil udlevere sådanne oplysninger.

Hvis udbyderne tvinges til at indarbejde krav om udlevering af sådanne oplysninger i selskabernes aftaler med udstyrsleverandørerne er der betydelig risiko for, at udstyrsleverandører ikke vil levere det mest moderne og teknologisk bedste udstyr til det danske marked.

Udbyderne kan således stå i en situation, hvor man enten bliver mødt med et bødepålæg for ikke at fremskaffe oplysninger der er umulige at fremskaffe eller må risikere at nødvendigt udstyr ikke kan blive leveret.

Stand still periode
Den i § 4, stk. 1, nr. 2, foreslåede ordning er vidtgående og meget bebyrdende i praksis for udbyderne. Desuden er det vanskeligt at afgøre, hvad et "endeligt udkast" er, og hvis aftalen først skal fremsendes, når parterne er klar til at sætte deres underskrift på aftalen, er det en væsentlig kommerciel ulempe for os, at vi skal stoppe underskrivelsesprocessen og i stedet indsen-

de aftaleudkastet til CFCS. Efter en stand still periode på op til 10 dage er det ikke givet, at parterne længere ønsker at underskrive det udkast, som CFCS har gennemgået. Hertil kommer, at den eventuelle rådgivning, som CFCS måtte komme med som resultat af deres gennemgang, i givet fald vil komme meget sent – ja, faktisk efter afsluttet forhandlingsproces, idet det jo netop er endeligt aftaleudkast, der fremsendes. Hvis CFCS' kommentarer efterfølgende skal implementeres, skal den ellers afsluttede forhandlingsproces startes op igen.

Ordningen er særlig uproportional, når der henses til de reaktionsmuligheder, som CFCS har. Som det er angivet i forslagets bemærkninger, så vil der *"...ikke være tale om, at Center for Cybersikkerhed skal godkende aftaler, der er omfattet af nr. 2, ligesom centeret heller ikke kan nedlægge forbud mod indgåelse af en aftale efter standstill-periodens udløb"*. Således kan CFCS ikke forbyde en aftales indgåelse, og derfor er det særligt uforholdsmæssigt, at en aftale, der ellers er klar til underskrivelse, skal afvente CFCS' gennemgang i en periode på op til 10 dage. Dertil kommer, at der består en betydelig kommerciel risiko i, at en færdigforhandlet aftale "åbnes op" på ny så sent i forhandlingsforløbet.

Høringsparterne mener i stedet, at en drøftelse med CFCS af et givent aftaleforhold løbende igennem aftaleprocessen med nye potentielle samarbejdspartnere bør være mest hensigtsmæssig. Det er i alle tilfælde udbyderens ansvar at have sikkerheden på plads, når der indgås en ny aftale med en samarbejdspartner – og derfor bør man kunne hvile på princippet om (og tilliden til), at udbyderne selv konsulterer CFCS inden endelig aftale indgås. Hvis CFCS herefter ikke mener, at aftalen medfører et tilstrækkeligt sikkerhedsniveau, kan de benytte de øvrige muligheder, som loven giver dem, til at gribe ind og få rettet op på dette.

Teleudbyderne vil med en sådan model bære risikoen for ikke at spørge CFCS på forhånd, men har samtidig den kommercielle frihed til at tilrettelægge forhandlingsforløbet med potentielle leverandører. Det kan overvejes i stedet at indsætte en mulighed for forhåndsbesked, som kendes fra eksempelvis forbruger- og konkurrencelovgivningen, hvorefter en udbyder kan anmode CFCS om at vurdere om et konkret aftaleforhold udgør en risiko for informationssikkerheden og dermed opnå sikkerhed for, at aftalen ikke efterfølgende bliver genstand for øgede og nye krav fra CFCS.

Prioriteringsordninger
CFCS får i § 5, stk 3, hjemmel til generelt at påbyde prioritetsordninger, hvor prioritering i dag er baseret på frivillige aftaler. Høringsparterne finder at den nuværende ordning med frivillige aftaler har vist sig at være konstruktiv og afbalanceret – dette på trods af at beredskabsmyndighederne har været meget længe om at tage de etablerede ordninger i anvendelse. Høringsparterne skal derfor opfordre til, at det præciseres i lovbemærkningerne, at CFCS vil være tilbageholdende med at udstede påbud på området og at indgåelse af frivillige aftaler med branchen fortsat er den foretrukne løsningsmodel.

Kravet om sikkerhedsgodkendelser
Der er uklart om den foreslåede § 6 indebærer at teleoperatørerne skal have sikkerhedsgodkendt flere medarbejdere end tilfældet er i dag. Teleoperatørerne har dog erfaret efter dialog med CFCS, at CFCS gerne ser at langt flere er sikkerhedsgodkendte. Telebranchen har allerede i dag flere tusinde medarbejdere der er sikkerhedsgodkendte og såfremt en øget andel skal sikkerhedsgodkendes, vil det være en væsentlig byrde for operatørerne.

Høringsparterne noterer sig derfor med tilfredshed, at det er præciseret i lovbemærkningerne, at der ikke kan kræves sikkerhedsgodkendelse blot fordi en medarbejder har adgang til udbyderens kritiske infrastruktur, og at kravet om sikkerhedsgodkendelse skal ske ud fra en konkret vurdering.

Kravet om uafhængig sikkerhedsrevision
Kravet om *uafhængig sikkerhedsrevision* i § 9, stk. 5 kan blive bekosteligt for teleudbyderne. Det er således høringsparternes vurdering at en sådan revision let kan koste ½ mio. kr. pr. teleudbyder pr. gang. Af denne årsag bør en sådan sikkerhedsrevision kun kunne foranstaltes ved en mistanke om manglende sikkerhed eller misligholdelse af visse forhold.

Det fremgår af lovbemærkningerne (side 42), at der alene vil blive stillet krav om uafhængig sikkerhedsrevision, hvor der er indikationer på, at en udbyder ikke overholder centrale regler vedrørende informationssikkerhed i net og tjenester. Denne formulering bør fremgå direkte i bestemmelsen, således at det står helt klart, at CFCS kun har hjemmel til at kræve revision i sådanne tilfælde.

Tilsyn i form af inspektioner
Med den foreslåede § 9, stk. 6 og 7, får CFCS hjemmel til uden retskendelse at få adgang til udbyderen eller dennes samarbejdspartnere. En sådan adgang er en væsentligt indgribende foranstaltning, og bør derfor anvendes med forsigtighed.

Formuleringen af § 9, stk. 6 er uklar. Adgangen til forretningslokaler kan ifølge bestemmelsens ordlyd benyttes, *"hvis det er nødvendigt af hensyn til informationssikkerheden"*. Samtidig er det angivet i bestemmelsens bemærkninger (s. 21 og igen s. 43), at der er tale om et rutinemæssigt tilsyn, *"...der kun forudsættes anvendt, såfremt et tilsvarende resultat ikke kan opnås ved anvendelse af andre og mindre indgribende tilsynsmuligheder..."*. Denne formulering bør fremgå direkte i bestemmelsen, således at det står helt klart, at CFCS kun har hjemmel til at inspicere, såfremt de øvrige muligheder for at få oplyst et konkret forhold (krav om fremlæggelse af alle oplysninger og materiale, jf. stk. 2 samt krav om skriftlige udtalelser, jf. stk. 4) ikke er tilstrækkelig.

Adgang til 3. parters faciliteter
Lovforslaget pålægger endvidere flere steder forpligtelser på 3. parter (andre end udbyderne), herunder i lovforslagets § 9, stk. 7, hvorefter CFCS uden retskendelse og mod behørig legitimation kan få adgang til forretningslokaler hos udbyderes samarbejdspartnere, leverandører eller underleverandører.

Høringsparterne skal fremhæve, at de danske udbydere ikke kan indestå for en sådan adgang, der måtte blive pålagt sådanne 3. parter, da den rette adressat for et sådant indgreb vil være 3. parten.

Høringsparterne skal videre bemærke, at CFCS kun har jurisdiktion i Danmark. Derfor kan § 9, stk. 7, ramme skævt, idet kun leverandører og samarbejdspartnere i Danmark vil være omfattet. Dette kan for det første betyde, at bestemmelsen bliver en fordel for de udenlandske leverandører og samarbejdspartnere frem for de danske af slagsen. For det andet kan bestemmelsen være til hinder for at vi kan dele tjenester/udstyr med andre koncernforbundne enheder i udlandet, idet en adgang til vores udstyr/tjenester i et sådan delt scenarie vil kunne give adgang til andre udenlandske udbyderes tjenester.

Offentliggørelse af afgørelser mv.
Lovforslagets § 10 ønsker indført en adgang til offentliggørelse af afgørelser, resultater af tilsyn, mv., og i bemærkningerne til bestemmelsen er det angivet, at bestemmelsen har til formål at give udbyderne øget incitament til overholdelse af kravene til informationssikkerhed og beredskab. Høringsparterne mener ikke, at denne "gabestok-metode" er proportional.

Som nævnt tidligere sætter de danske udbydere sikkerhed i selskabernes net meget højt, og hvis CFCS skulle finde en fejl eller forhold, som de ønsker forbedret, er det ikke ensbetydende med, at udbyderne har "sløset" med sikkerheden og dermed bør hænges ud i offentligheden.

Det skal i den forbindelse tages med i betragtning, at sikkerhedstrusler er i konstant forandring og sikkerhedsforanstaltninger der er gældende i dag ikke nødvendigvis er relevante eller tilstrækkelige på et senere tidspunkt. Det vil derfor ofte være forbundet med en betydelig grad af skøn og usikkerhed om en given sikkerhedsforanstaltning har været tilstrækkelig.

En optimal sikring af net- og informationssikkerheden fordrer derfor, at udbyderne og CFCS kan udveksle informationer om sikkerhedshændelser uden at udbyderne risikere, at blive stillet offentligt til skue. Selv hvis udbydernes identitet holdes hemmeligt i forbindelse med en offentliggørelse, vil det alene pga. det begrænsede antal udbydere i Danmark ikke være svært for offentligheden at finde frem til de selskaber der måtte være berørt.

Forslaget om offentliggørelse undergraver derfor den tillid og det samarbejde, som vi ønsker med CFCS.

Med venlig hilsen

Mette Lundberg
Direktør, politik og kommunikation
IT-Branchen

Christian Hannibal
Chefkonsulent
DI ITEK

Jakob Willer
Direktør
Teleindustrien

Domstolsstyrelsen

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Store Kongensgade 1-3
1264 København K
Tlf. +45 70 10 33 22
post@domstolsstyrelsen.dk
CVR-nr. 21659509
EAN-nr. 5798000161184

Sendes alene pr. e-mail til fmn@fmn.dk og jch@fmn.dk

J.nr.: 2015-4102-0026-3
Sagsbehandler: Katrine Valbjørn Trebbien
Mail: kat@domstolsstyrelsen.dk
4. maj 2015

Høring over udkast til forslag til lov om net- og informationssikkerhed

Forsvarsministeriet har ved e-mail af 21. april 2015 anmodet om eventuelle bemærkninger til udkast til forslag til lov om net- og informationssikkerhed.

Domstolsstyrelsen kan i den anledning oplyse, at styrelsen ikke har bemærkninger til udkastet.

Med venlig hilsen

Katrine Valbjørn Trebbien

Forsvarsministeriet
Holmens Kanal 42
1060 København K
Fremsendt pr email til: fmn@fmn.dk og jch@fnm.dk

4. maj 2015

Vedr: Høring over udkast til forslag til lov om net- og informationssikkerhed.

Hi3G er enig i, at informationssikkerhed er den vigtigste faktor i at drive en televirksomhed i Danmark. Hi3G ved også, fra tilkendegivelser fra danske myndigheder, at den danske teleinfrastruktur er én af de mest robuste i Europa og på verdensplan.

Televirksomhederne har i dag et tæt samarbejde med CFCS omkring nuværende regulering og Hi3G så gerne, at dette gode samarbejde forsatte med nuværende lovgivning, frem for dette meget indgribende og brede lovforslag.

Det er Hi3G's vurdering, at lovforslaget er for indgribende overfor teleselskaberne i Danmark. Der eksistere allerede en lovgivning på beredskab og informationssikkerhed, der er noget mere skærpende end hvad minimumsreguleringen fra EU foreskriver, hvorfor vi er af den opfattelse, at lovforslaget er yderst byrdefuldt og ikke proportionalt for teleselskaberne i Danmark i forhold til, hvilke krav, der stilles i andre EU lande. Desuden bør Danmark afvente det arbejde, der pt. pågår i EU, således vi i Danmark følger samme krav som i andre EU lande. Særligt bør det haves for øje, at teleoperatørerne i Danmark er meget små set i forhold til større televirksomheder i EU og på verdensplan, samt at leverandørerne oftest er meget store. Derfor vil lovforslaget betyde, at de krav, der stilles overfor leverandørerne, kan blive ekstra økonomisk byrdefulde for de danske televirksomheder, da disse krav stilles af meget små televirksomheder og kan være forskellige fra de krav, der vil blive stillet på EU niveau.

Desuden vurderer vi generelt, at lovteksten er alt bred i sine formuleringer, hvilket vil gøre det vanskeligt og økonomisk byrdefuldt for televirksomhederne at drive forretning i Danmark.

Lovforslaget indeholder ikke en ankemulighed for operatørerne svarende til nuværende regulering, hvor der kan klages til Forsvarsministeren. Jeg beder venligst Forsvarsministeriet om at oplyse hvorfor og på hvilken baggrund ankemuligheden foreslås udtaget?

Hermed specifikke bemærkninger til de enkelte bestemmelser:

- §3 Her bør formålet med fastsættelse af reglerne ligeledes fremgå, da lovbestemmelsen ellers er for bred.

- § 4 stk. 2: Her udestår en nærmere beskrivelse af hvad "væsentlige dele af udbyderens net eller tjenester eller driften heraf " er. Dette bør klart defineres, da det i bredeste fortolkning kan omfatte hele nettet og tjenesterne bag. Bestemmelsen er alt for vidtgående. Hi3G er meget bekymrede for effekten af denne bestemmelse, særligt om dette kan få en negativ betydning på de kommercielle forhold mellem teleselskabet og leverandørerne jf. også de generelle bemærkninger ovenfor.

- 4 stk. 3: er meget uklar, hvad betyder det konkret når noget har "væsentlige følger for driften af net eller tjenester". Vi har allerede i dag fastlagt bestemmelserne for underretningspligterne og har brug meget tid herpå – både i samarbejde med CFCS og tidligere IT – og Telestyrelsen, samt implementeret disse retningslinjer i alle selskaber. Forestiller man sig at nye processer, definitioner og retningslinjer skal implementeres og hvad er det nye der skal opnås herved? Dette bør fremgå af lovbestemmelsen mere tydeligt.

- §4 stk. 4: det bør også være mulighed for at det kun er det berørte slutbruger der skal underrettes og ikke kun offentligheden som helhed.

- § 5 er en meget bred bestemmelse. Forventer man yderligere krav end der allerede er i dag ?

- § 5 stk. 3: Mobilprioritering foreslås lovbestemt, herunder også, at det er CFCS, der kan fastsætte reglerne herom. Hi3G har igennem en årrække deltaget aktivt arbejdet omkring mobilprioritering og har løbende vedligeholdt og implementeret økonomisk meget byrdefylde løsninger på mobilprioritering. Ordning er ikke på samme tilfredsstillende vis blevet implementeret af myndighederne. Derfor finder vi det yderst bekymrende om myndighederne uden videre fremadrettet kan forlange yderligere investeringer til nye løsninger, hvor vi endnu ikke efter 7 års arbejde har set effekten af de investeringer i millionklassen som teleselskaberne har brugt i den nuværende løsning.

- § 5 stk. 4. Det bør beskrives nærmere hvad " angivne sikkerhedsforanstaltninger" kan være og særligt at når dette kan påtvinges ved en forventning om en eventuel påvirkning. Desuden bør operatøren være en del af denne beslutning.

- § 9 stk. 6 og stk 7. CFCS skal ikke have mulighed for adgang til Selskabernes lokaler uden retskendelse. Dette er et grundlæggende krav i retsplejeloven og bør ikke tilsidesættes ved denne lov. Desuden vil der være oplysninger, der ikke må

udleveres som følge af retsplejelovens bestemmelser. Jeg beder venligst FM oplyse, hvorledes der nærmere i disse tilfælde vil blive administreret?

- § 10 bør der som minimum indsættes et krav om, at Operatøren skal godkende det, der påtænkes offentliggjort af CFCS, herunder at der kan gøres undtagelse fra offentliggørelse i det tilfælde der er tale om forretningshemmeligheder.

Med venlig hilsen

Anne Louise Vogensen
Hi3G Denmark ApS

Fra: Bjørn Borre [bjb@itb.dk]
Sendt: 4. maj 2015 14:04
Til: FMN-JCH Thomsen, Jens-Christian Hedegaard; FMN-MYN-FORSVARSMINISTERIET
Emne: SV: Høring over udkast til forslag til lov om net- og informationssikkerhed

Kategorier: Birte

(FKIT besked: Denne mail kommer fra Internettet.)

IT-Branchen takker for at være en del af høringen om udkast til forslag om net- og informationssikkerhed.

Vi henviser til vores med TeleIndustrien fælles afgivne høringssvar.

Noter endvidere IT-Branchens opbakning til kommentarer i høringssvaret fra Rådet for Digital Sikkerhed om hensynstagen til databeskyttelse, menneskerettigheder og grundlovsrettigheder. Herunder anbefalingerne om, at det medtages i formålsbestemmelsen at krav der stilles til udbydere i medfør af loven sker i overensstemmelse med databeskyttelsesregler.

Kommentarerne kalder samlet på dels en udskydelse af behandlingen af lovforslaget, dels en justering i forhold til kommende EU-regler og kommentar i de nævnte høringssvar.

Mvh

Bjørn Borre
Chefkonsulent

IT-Branchen
Børsen – 1217 København K
Direkte: +45 7225 5503
Mobil: +45 2752 2524
E-mail: bjb@itb.dk
Web: itb.dk

"Danmarks største brancheorganisation og forretningsnetværk for it-virksomheder"

"Sæt kryds 17/9! ITB Lederdøgn 2015 – Tredive års jubilæumsudgave"

Fra: FMN-FMN Forsvarsministeriet [mailto:fmn@fmn.dk]
Sendt: 21. april 2015 19:32
Til: samfund@advokatsamfundet.dk; amnesty@amnesty.dk; info@dbkas.dk; info@danskenergi.dk; danskerhverv@danskerhverv.dk; di@di.dk; dit@dit.dk; mail@danskeadvokater.dk; regioner@regioner.dk; dt@datatilsynet.dk; MikaelSjoberg@OestreLandsret.dk; itek@di.dk; post@domstolsstyrelsen.dk; fda@fda.dk;

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt pr email til: fmn@fmn.dk
med kopi til: jch@fmn.dk

IT-Politisk Forening
c/o Niels Elgaard Larsen
Århusgade 35, 1.
2100 København Ø

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

Dato : 4. maj 2015

Høringsssvar vedr. forslag til lov om net- og informationssikkerhed

I forbindelse med nedlæggelsen af IT- og Telestyrelsen valgte regeringen at dele ansvaret for teleområdet mellem Erhvervsstyrelsen og Forsvarsministeriet, således at Forsvarsministeriet administrerer bestemmelserne om informationssikkerhed og beredskab. Forsvarsministeriet har placeret dets ansvarsområder hos Center for Cybersikkerhed, der er en del af Forsvarets Efterretningstjeneste (FE).

Lovudkastet flytter lovbestemmelserne under Forsvarsministeriets område fra teleloven (lov om elektroniske kommunikationsnet og -tjenester) til en ny lov om net- og informationssikkerhed. Samtidig kommer der på visse områder en udvidelse af beføjelserne til Center for Cybersikkerhed i forhold til i dag samt en række nye oplysningspligter for teleselskaberne.

Generelle bemærkninger

Informationssikkerheden i telesektoren er vigtig for hele samfundet: Televirksomheder kan have særlig interesse for hackere, fordi et angreb kan give adgang til telekundernes kommunikation, herunder oplysninger om borgeres private forhold og virksomheders forretningshemmeligheder. Denne trussel må forventes at komme fra såvel kriminelle organisationer som statslige aktører. Via Snowden afsløringerne har vi erfaret, at GCHQ har hacket det belgiske teleselskab Belgacom, så truslen mod Danmark og danske interesser kan reelt komme fra alle statslige aktører. Det er ikke blot Kina og Nordkorea, som vi bør frygte i denne forbindelse.

Inden for det sidste halve år har der, i medierne, været historier om mulig kompromittering af informations-sikkerheden i mobiltelefoni via SS7-svagheder og falske basestationer (IMSI catchers). I følge en Version2 artikel den 19. december 2014, "Hvem undersøger mobilspionage i Danmark?" var det tilsyneladende ikke klart, om ansvaret for falske basestationer ligger hos Center for Cybersikkerhed eller Erhvervsstyrelsen.

IT-Politisk Forening skal på den baggrund opfordre til, at ansvarsfordelingen mellem Erhvervsstyrelsen og Center for Cybersikkerhed beskrives mere præcist i lovforslagets bemærkninger.

Center for Cybersikkerheds adgang til teleselskabernes infrastruktur

IT-Politisk Forening noterer med tilfredshed, at det af § 9, stk. 6 og 7 nu fremgår, at Center for Cybersikkerhed, i forbindelse med adgang til udbyderens forretningslokaler for at udføre tilsynsopgaver, ikke kan tilgå kommunikation til, fra eller mellem udbyderens kunder.

IT-Politisk Forening går ud fra, at det omfatter såvel indholdet af kommunikationen som metadata/trafikdata vedrørende denne (telefonnumre, IP-adresser, email-adresser, etc), og i så fald skal vi opfordre til, at dette bliver præciseret i lovforslagets bemærkninger.

Detailregulering vs rette incitamenter for teleselskaberne

Danske teleselskaberne er private virksomheder, og de bør som udgangspunkt frit kunne vælge såvel teknisk udstyr som leverandører ud fra normale forretningsmæssige hensyn. På grund af teleselskabernes helt centrale betydning for cybersikkerheden og fortroligheden af kundernes kommunikation, er det både rimeligt og nødvendigt at stille særlige krav til teleselskaberne, for eksempel særlige undersøgelsespligter.

Det er også vigtigt, at lovgivningen giver teleselskaberne de rette incitamenter til at sikre teleinfrastrukturen så godt

som muligt. De muligheder for offentliggørelse, som § 10 i lovforslaget giver, kan bidrage til at skabe de rette incitamenter. Men i sidste ende bør det være teleselskaberne som træffer de endelige afgørelser om f.eks. valg af udstyr eller indretning af deres infrastruktur. Med den nuværende tele-infrastruktur, får vi aldrig 100% sikkerhed mod hackerangreb eller kompromittering af kundernes kommunikation, og grundlæggende mener IT-Politisk Forening, at teleselskaberne har bedre forudsætninger for at træffe de rigtige valg end embedsmænd fra Center for Cybersikkerhed.

På den baggrund er vi skeptiske over for beføjelserne til Center for Cybersikkerhed i § 3, stk. 3, hvor der i visse situationer af væsentlig samfundsmæssig betydning kan udstedes direkte påbud til teleselskaberne. Det fremgår ikke helt klart af lovforslagets bemærkninger, om det alene er påbud om at foretage visse undersøgelser ved mistanke om sårbarheder i teleselskabernes infrastruktur, eller om det også kan være påbud om at undlade at anvende bestemte tekniske løsninger (udstyr) i infrastrukturen?

IT-Politisk Forening ser ikke noget problem i, at Center for Cybersikkerhed kan pålægge teleselskaberne at undersøge deres infrastruktur for sårbarheder, men hvis beføjelserne også omfatter muligheden for at nedlægge forbud mod at anvende bestemte typer udstyr mod teleselskabets vilje, vil vi være skeptiske over for om det er hensigtsmæssigt. Vi kan ikke ud af lovforslagets bemærkninger læse, om Center for Cybersikkerhed får denne beføjelse, men hvis det er tilfældet, bør det være en beføjelse som kun anvendes i helt ekstraordinære tilfælde.

Informationsdeling mellem Center for Cybersikkerhed og Forsvarets Efterretningstjeneste

Center for Cybersikkerhed er en institution under Forsvarets Efterretningstjeneste, og det kan give anledning til nogle potentielle konflikter. Center for Cybersikkerhed skal bidrage til at beskytte den danske teleinfrastruktur, en rent defensiv operation, mens FE i teorien kan have offensive operationer, som involverer indtrængen hos teleselskaber i andre lande. IT-Politisk Forening har naturligvis ingen konkret viden om at FE gør eller

planlægger dette, men da FEs aktiviteter i udlandet ikke er reguleret af dansk lov, kan det ikke udelukkes.

Af blandt andet moralske årsager vil IT-Politisk Forening finde det forkert, hvis viden om konkrete sårbarheder, som Center for Cybersikkerhed erhverver sig fra danske teleselskaber, bruges til offensive operationer hos FE, eller hvis FE deler denne viden med offensive enheder hos samarbejdspartnere som GCHQ og NSA. Ud over det rent moralske aspekt, kan der desuden være en risiko for, at udenlandske teleselskaber ikke vil dele viden om sårbarheder med danske teleselskaber, hvis de udenlandske teleselskaber frygter, at viden om disse sårbarheder via Center for Cybersikkerhed kan havne hos for eksempel GCHQ eller NSA og blive misbrugt der. En sådan tilbageholdenhed med at dele viden om sårbarheder vil være til skade for informationssikkerheden i den danske teleinfrastruktur.

Efter IT-Politisk Forenings opfattelse bør der være vandtætte skotter mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste for så vidt angår viden om konkrete sårbarheder i teleinfrastrukturen, som Center for Cybersikkerhed erfarer i forbindelse med dets tilsynsopgaver overfor danske televirksomheder.

Forsvarsministeriet
Holmens Kanal 42
1060 København K
Sendt pr mail til fmn@fmn.dk & jch@fmn.dk

Glostrup d. 4. maj 2015

Kontakt: Per Skovgaard Rosen
Direkte: 26 11 22 33
E-mail: psr@nianet.dk

Høring over udkast til forslag til lov om net- og informationssikkerhed

Forsvarsministeriet har den 21. april 2015 sendt udkast til forslag til lov om net- og informationssikkerhed i høring.

Nianet A/S takker for muligheden for at komme med bemærkninger til det fremsendte lovforslag.

På baggrund af kort høringsfrist, har Nianet i denne sag koordineret synspunkter med og valgt at tilslutte sig Dansk Energi's høringssvar af 4. maj 2015.

Venlig hilsen

Per Skovgaard Rosen
CTO, Nianet A/S

Nianet A/S
Ejby Industrivej 1
DK-2600 Glostrup
Tlf.: +45 70 20 87 30
Fax: +45 70 20 87 32

Web: www.nianet.dk
E-mail: info@nianet.dk

CVR nr.: 27172776

Vestre Landsret
Præsidenten

Forsvarsministeriet
Holmens Kanal 42
1060 København K

J.nr. 40A-VL-25-15
Den 29/04-2015

Forsvarsministeriet har ved brev af 21. april 2015 (sagsnr. 2014/004373) anmodet om en udtalelse om et udkast til forslag til lov om net- og informationssikkerhed.

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

Dette svar sendes efter anmodning til fmn@fmn.dk med kopi til jch@fmn.dk.

Med venlig hilsen

Bjarne Christensen

Østre Landsret
Præsidenten

Den 23 APR. 2015
J.nr. 40A-OL-27-15
Init: cr

Forsvarsministeriet
Holmens Kanal 42
1060 København K

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

Forsvarsministeriet har ved brev af 21. april 2015 (Sagsnr. 2014/004373) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om net- og informationssikkerhed.

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

Med venlig hilsen

Bent Carlsen

Ellen Busck Porsbo

Fra: Per Steinbach [pst@rigsrevisionen.dk]
Sendt: 29. april 2015 12:29
Til: FMN-MYN-FORSVARSMINISTERIET
Emne: Høringssvar fra Rigsrevisionen vedr. udkast til forslag til lov om net- og informationssikkerhed (j.nr. 2015-4500-58)

Kategorier: Tina

(FKIT besked: Denne mail kommer fra Internettet.)

Til Forsvarsministeriet

Rigsrevisionens 16. kontor (it-revision) fremsender hermed høringssvaret vedrørende Forsvarsministeriet udkast til forslag til lov om net- og informationssikkerhed.

Høringssvaret:
Rigsrevisionens gennemgang af lovforslaget har vist, at det ikke indeholder bestemmelser med betydning for regnskabsaflæggelse og revision.
Gennemgang har derfor ikke givet anledning til bemærkninger vedrørende revisionsmæssige forhold.

Med venlig hilsen
Per Steinbach
Rigsrevisionen

Fra: FMN-FMN Forsvarsministeriet [mailto:fmn@fmn.dk]
Sendt: 21. april 2015 19:32
Til: samfund@advokatsamfundet.dk; amnesty@amnesty.dk; info@dbkas.dk; info@danskenergi.dk; info@danskerhverv.dk; di@di.dk; dit@dit.dk; mail@danskeadvokater.dk; regioner@regioner.dk; dt@datatilsynet.dk; MikaelSjoberg@OestreLandsret.dk; itek@di.dk; post@domstolsstyrelsen.dk; fda@fda.dk; info@globalconnect.dk; ann-louise.hansen@3.dk; michelle.baunknudsen@3.dk; horesta@horesta.dk; info@humanrights.dk; itb@itb.dk; bestyrelse@it-pol.dk; kl@kl.dk; info@nianet.dk; post@vestrelandsret.dk; post@oestrelandsret.dk; sekretaer.retspolitik@gmail.com; post@retssikkerheds-fonden.dk; Rigsrevisionen; info@digitalsikkerhed.dk; tm@stofa.dk; tdc@tdc.dk; jw@teleindu.dk; NKP@telenor.dk; MEVI@telenor.dk; men@telenor.dk; thomas.michael.pedersen@teliasonera.com; jesper.fejerskov@telia.dk; peter.andersen@teracom.dk; info@tt-network.dk; Info-sec@waoo.dk
Emne: Høring over udkast til forslag til lov om net- og informationssikkerhed

"Hermed sender Forsvarsministeriet udkast til forslag til lov om net- og informationssikkerhed i høring. Der henvises til vedhæftede."

4. maj 2015

Forsvarsministeriet
Holmens Kanal 42
1060 København K
Att. Thomas Kvistholm Thrane
fmn@fmn.dk
jch@fmn.dk

Høringssvar vedr. udkast til lov om net- og informationssikkerhed

Rådet for Digital Sikkerhed (RfDS) takker for høringsanmodningen fra Forsvarsministeriet i anledning af udkast til lov om net- og informationssikkerhed.

RfDS finder det som udgangspunkt positivt, at der med lovforslaget tages skridt til at øge informationssikkerhedsniveauet og skabe en robust informations- og kommunikationsteknologisk infrastruktur (ikt-infrastruktur) i Danmark.

Selvom lovforslaget i hovedsagen angår teleområdet, finder RfDS, at formålet for indsatsen og de midler, der bringes i anvendelse til opfyldelse af formålet, bør tilpasses de mål og principper, der i EU er defineret i Strategien for cybersikkerhed og det tilhørende direktivudkast. Kommissionens udkast blev den 13. marts 2014 vedtaget af EU-Parlamentet[1] og afventer endelig godkendelse i EU's ministerråd.

RfDS ønsker her særligt at fremhæve EU indsatsens overordnede formål om "et åbent, sikkert og beskyttet cyberspace", hvor forebyggelse og reaktioner på cyberforstyrrelser og -angreb sker på en måde, der sikrer det bedste resultat, skaber vækst i den digitale økonomi og samtidig fremmer europæiske værdier som frihed og demokrati. Parlamentet har i forbindelse med sin behandling af direktivudkastet i flere ændringsforslag understreget vigtigheden af at sikre effektiv beskyttelse af borgernes privatliv og data. [2]

De følgende bemærkninger til lovforslaget skal læses i lyset af EU-indsatsen og de principper, den bygger på, samt den retsudvikling i forhold til forståelsen af beskyttelse af grundrettigheder i en digital tidsalder, som den kommende EU forordning om databeskyttelse er udtryk for og som EU-domstolen har skabt med sin afgørelse om ugyldigheden af EU's logningsdirektiv i april 2014.[3]

---

1 Se strategi og direktivudkast er http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[2] Se direktivudkast med Parlamentets ændringsforslag her:
http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0244

[3] Se pressemeddelelse her:
http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf
og dommen her:
http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DA&cid=522546

Baggrunden for RfDS' bemærkninger udgøres tillige af virksomheders behov for beskyttelse og sikkerhed, herunder af integritet, autenticitet og fortrolighed, der kan være af afgørende forretningsmæssig værdi og i nogle tilfælde en forudsætning for at kunne bidrage til den økonomiske digitale vækst.

Lovens formål – lovforslagets § 1
Med lovforslaget bliver Center for Cybersikkerhed (CFCS) bemyndiget til at stille en række krav til teleudbydere og andre udbydere at net- kommunikationstjenester, der alle vil have direkte eller indirekte indvirkning på håndteringen af personoplysninger, herunder også personfølsomme oplysninger. Dette gælder i forhold til lovforslagets hjemmel til CFCS om at stille minimumskrav til informationssikkerhed, risikostyring, leverandørkrav, pålæg af foranstaltninger, oplysnings- og underretningspligt samt beredskabskrav hos udbyderne.

RfDS anbefaler derfor, at lovforslaget udvides med en bestemmelse i § 1, der fastslår, at krav, der stilles til udbydere i medfør af lovforslaget, opfylder persondatalovens krav til beskyttelse af personoplysninger og sikkerhedsbekendtgørelsens krav til sikkerhed, og at CFCS skal påse dette, således at virksomheder ikke udsættes for modstridende lovkrav.

En sådan bestemmelse nødvendiggøres af, at CFCS med Lov om Center for Cybersikkerhed er undtaget fra persondataloven, og alene efter lovens bemærkninger forventes at følge persondatalovens principper.

Et udtrykkeligt krav i § 1 om efterlevelse af persondataloven vil sikre beskyttelse af borgernes grundrettigheder på niveau med det kommende EU NIS direktiv og vil tillige etablere parathed til opfyldelse af den kommende EU forordning om databeskyttelse.

Definitioner – lovforslagets § 2
Lovforslagets bestemmelser indeholder en række begreber, der ikke er nærmere defineret i lovteksten eller i bemærkningerne. For at skabe transparens og forudsigelighed for de virksomheder, der vil blive berørt af loven, anbefaler RfDS, at disse begreber defineres i lovteksten og evt. forklares yderligere i bemærkningerne. Begreberne omfatter:

Informationssikkerhed
Begrebet bør defineres i overensstemmelse med det kommende EU NIS direktiv, som stiller krav til såvel resiliens som sikkerhed på et passende niveau. Informationssikkerhed er herefter:

> *"et nets eller et informationssystems evne til, på et givet tillidsniveau, at modstå uheld, ulovlige handlinger og handlinger i ond hensigt, der er til skade for disponibiliteten, autenticiteten, integriteten og fortroligheden i forbindelse med arkiverede og overførte data og de dermed forbundne tjenester, der tilbydes eller er tilgængelige via dette net eller system. Sikkerhed omfatter passende tekniske anordninger, løsninger og driftsprocedurer, der sikrer overholdelse af sikkerhedskravene i dette direktiv"*

Risiko
Begrebet risiko bør defineres i overensstemmelse med det kommende EU NIS direktiv, der fastslår, at risiko er:

> *"enhver rimeligt identificerbar omstændighed eller begivenhed, der har en potentiel negativ indvirkning på sikkerheden"*

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

Lovudkastets anvendelse af begreberne *drift* og *driftsopgaver* bør ligeledes af hensynet til lovhjemlens kvalitet beskrives i lovtekstens § 2. Forklaringer er i lovudkastet medtaget i bemærkningerne til § 3 og 4. Det samme gælder begreberne *beredskabssituationer* og *ekstraordinære situationer,* som alene er forklaret i lovudkastets bemærkninger til § 5

Krav til informationssikkerhedsniveauet – lovforslagets § 3
Med lovforslagets § 3 gives CFCS bemyndigelse til at fastsætte minimumsregler for informationssikkerhed for udbydere af offentligt tilgængelige net og tjenester (stk. 1), inddrage områder og trusler i deres risikostyringsprocesser (stk. 2) og påbyde dem at træffe konkrete foranstaltninger for at sikre informationssikkerheden (stk. 3).

RfDS bemærker hertil, at selv om opgavevaretagelsen af net- og informationssikkerhed med lovforslaget fremadrettet varetages af CFCS under Forsvarets Efterretningstjeneste, er CFCS ikke fritaget fra at overholde den Europæiske Menneskerettighedskonventions bestemmelser om respekt for privatlivets fred, herunder beskyttelse af personoplysninger, som er afspejlet i EU Traktatens Charter om grundrettigheder, artikel 7 og 8.

Da de krav, som CFCS med lovgrundlaget vil kunne stille til udbyderne, har direkte og/eller indirekte indvirkning på håndteringen af borgernes personoplysninger, skal de påse, at udbyderne i deres opfyldelse af kravene ikke handler i strid med grundrettighederne.

Risikoen herfor kan afbødes ved, at hjemmelsgrundlaget udformes i en kvalitet, der sikrer transparens og forudsigelighed for de aktører, det berører, og ved at de foranstaltninger, udbyderne påbydes at gennemføre, er nødvendige og proportionale i forhold til formålet. På grund af udbydernes datamængde, herunder dens omfang og det forhold, at data omfatter hele befolkningens tele- og datatrafik, må det formodes, at der gælder et skærpet nødvendighedskrav.

I praksis betyder det, at CFCS kun vil kunne stille krav til udbyderne om deres net- og datahåndtering, herunder som led i forebyggelse, detektering, analyse, begrænsning af samt reaktion på sikkerhedshændelser, der opfylder grundrettighedernes krav til databeskyttelse.

Oplysnings- og underretningspligt – lovforslagets § 4
Med lovforslagets § 4 udstyres CFCS med bemyndigelse til at fastsætte regler for udbydernes pligt til at oplyse om væsentlige dele af deres net og tjenester eller driften af disse, samt underretning om leverandøraftaler. Bestemmelsen giver også CFCS mulighed for at fastsætte regler om underretning om brud på informationssikkerheden til CFCS og til offentligheden.

RfDS bemærker hertil, at det for nogle udbydere vil kunne være vanskeligt at opfylde en oplysnings- og underretningsforpligtelse, der drejer sig om deres drift, herunder drift, der er outsourcet til leverandører. Oplysninger om tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale services, driften heraf, herunder driftensns tilrettelæggelse, styring samt risikohåndtering, udgør en del af udbydernes kerneforretning, og det vil derfor kunne være tæt forbundet med indvirkning på udbyders konkurrencemæssige stilling på markedet, hvis sådanne oplysninger skal videregives til CFCS.

Problematikken understreges af, at CFCS med sin placering i FE, som udgangspunkt ikke vil kunne orientere udbyderne om, hvad deres oplysninger bliver anvendt til, herunder hvem de videregives til som led i samarbejde med andre efterretningstjenester i medfør af FE-loven og CFCS-loven.

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

RfDS anbefaler, at hensigtsmæssigheden i at placere opgaven med at modtage oplysning og underretning hos CFCS om udbydernes drift af og brud på informationssikkerheden, undergives ny vurdering og politisk debat.

Oplysningspligt og kontrolbesøg – lovforslagets § 9
Med lovforslagets § 9 bliver CFCS tillagt beføjelse til at foretage kontrolbesøg, ikke blot hos udbydere (stk.6), men også hos udbyderes samarbejdspartnere, leverandører og underleverandører (stk. 7.)

RfDS hæfter sig ved, at det eksplicit fremgår af lovforslaget, at CFCS i forbindelse med kontrolbesøget ikke kan tilgå kommunikation til, fra eller mellem udbydernes kunder.

Kontrolbesøg vil kunne gennemføres med henblik på at påse overholdelse af loven og regler udstedt i medfør af loven, hvis det er "nødvendigt af hensyn til informationssikkerheden". Kontrolbesøget kræver ikke retskendelse, men foretages efter et varsel på 7 dage.

RfDS bemærker, at virksomheders forretningslokaler er omfattet af privatlivsbeskyttelsen i den europæiske menneskerettighedskonventions artikel 8, EU Charterets artikel 7 og grundlovens § 72. Grundloven kræver en lovbestemt "særegen undtagelse" for at fravige kravet om retskendelse ved adgang til sådanne lokaler, mens de andre bestemmelser kræver nødvendighed og proportionalitet. Retspraksis fra Menneskerettighedsdomstolen viser eksempler på, at nødvendighedskravet er skærpet, når indgrebet foretages af efterretningstjenester.

I lyset heraf, er det RfDS' vurdering, at lovudkastets nødvendighedskrav bør kvalificeres i selve lovteksten, således at det klart fremgår, hvilke kriterier, der skal være opfyldt førend kontrolbesøg kan gennemføres.

Anbefalinger
Samlet set giver udkast til lovforslag om Net- og Informationssikkerhed RfDS anledning til at foreslå følgende justeringer:

- det medtages i lovens formålsbestemmelse, at krav, der stilles til udbyderne i medfør af loven, sker i overensstemmelse med persondataloven;
- lovforslagets liste over definitioner udvides med begreberne: informationssikkerhed, risiko, drift og driftsopgaver, beredskabssituationer og ekstraordinære situationer;
- hensigtsmæssigheden i at placere opgaven med at modtage oplysning og underretning om udbydernes drift af og brud på informationssikkerheden hos CFCS, undergives ny vurdering og politisk debat;
- oplistning i lovteksten af klare kriterier for, hvornår et kontrolbesøg kan varsles og gennemføres hos udbyderne;
- at det overvejes, at udskyde vedtagelse af et dansk lovgrundlag til endelig vedtagelse af NIS direktivet, således af formål og principper heri sikres i den danske indsats for en robust ikt-infrastruktur.

At skabe den bedst mulige informationssikkerhed handler for RfDS om, at de strukturer og institutioner, der udstyres med beføjelser til at definere krav om informationssikkerhed og føre kontrol med deres implementering, fremmer befolkningens tillid til digitaliseringen og respekterer

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

vores grundlæggende rettigheder til privatliv, persondatabeskyttelse, ytringsfrihed og tilgængelighed.

RfDS opfrodrer derfor til, at det i den politiske debat om lovforslaget gøres til et omdrejningspunkt, at sikkerhed og frihed vægtes lige højt, og skaber grundlaget for såvel vision som fundament for etableringen af en robust ikt-infrastruktur i Danmark.

Med venlig hilsen

Birgitte Kofod Olsen
Formand

Rasmus Theede
Næstformand

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

Forsvarsministeriet
Sendt per mail til: fmn@fmn.dk med kopi til jch@fmn.dk.

4. maj 2015

Høringssvar vedr. høring over udkast til forslag til lov om net- og informationssikkerhed

SE/Stofa vil gerne kvittere for muligheden for at kommentere på udkast til forslag til lov om net- og informationssikkerhed og skal blot henvise til høringssvarene fra Teleindustrien og fra Dansk Energi, som vi støtter.

I den forbindelse kan vi bekræfte, at forslaget giver anledning til øgede administrative byrder, der for os bl.a. indebærer ansættelse af ekstra personale for at kunne imødekomme den øgede informationsbyrde.

Med venlig hilsen

SE/Stofa - Jes B. Christensen

JUSTITIA

Skrevet af
Jacob Mchangama
d. 28. april 2015

Høringssvar til udkast til lov om net- og informationssikkerhed

1. Indledning

Forsvarsministeriet har d. 21. april udsendt udkast til lov om net- og informationssikkerhed, med frist for eventuelle bemærkninger d. 4. maj 2015.

Justitia vil på baggrund af det udsendte lovudkast sammenholdt med det lækkede lovudkast, som blev refereret i Information og dertil hørende bemærkninger til lovudkastet, vurdere de retssikkerhedsmæssige konsekvenser af de ændringer, der er indført i lovudkastet.

Herudover vil Justitia behandle de retssikkerhedsmæssige problemstillinger, der stadigvæk kan rejses i det nye lovudkast. Hertil anføres nogle generelle bemærkninger om udviklingen i retskendelseskravet i dansk lovgivning, og på den baggrund vil Justitia fremsætte nogle anbefalinger.

2. Forskellen mellem det lækkede lovudkast og det nye lovudkast

Det fremgår af Informations gennemgang af det lækkede lovudkast og dertilhørende bemærkninger, at Center for Cybersikkerhed (CFCS) *»til enhver tid« og uden retskendelse kan få adgang til teleselskaber, når det sker »med henblik på indsamling af oplysninger«. Desuden skal centeret »efter anmodning« have adgang til selskabernes teleinfrastruktur.* Justitia kritiserede i februar denne brede og upræcise hjemmel og foreslog, at *[d]et ville være klogt at skrive tydeligt ind i lovudkastet, at det ikke er meningen, at centeret må gøre sig bekendt med borgeres kommunikation.*

Det fremgår af det nye forslag, § 9, stk. 6, 2. pkt., at CFCS' adgang til udbyderes forretningslokaler, som hjemlet i § 9, stk. 6, 1. pkt. ikke giver CFCS adgang til at *tilgå kommunikations til, fra eller mellem udbyderens kunder.*

Justitia
Lautrupsgade 13, 6. sal
2100 København Ø
(+45) 2466 4220
(+45) 2466 4220
info@justitia-int.org

Justitia anser denne ændring i forhold til det lækkede udkast som en positivt tilføjelse, der medfører øget fokus på beskyttelse af borgernes retssikkerhed og ret til meddelelseshemmelighed, og som på tilfredsstillende vis fastslår, at CFCS' tilsynsvirksomhed ikke medfører beføjelser til indgreb i meddelelseshemmeligheden.

Det fremgår af det nye forslag, § 9, stk. 6, 1. pkt., at *hvis det er nødvendigt af hensyn til informationssikkerheden, har* CFCS *efter et varsel på mindst syv arbejdsdage uden retskendelse [...] adgang til udbyderes forretningslokaler, med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven.*

Denne del af lovforslaget er således en tilføjelse til rækken af undtagelser til grundlovens § 72, som foreskriver, at *[h]usundersøgelse [...]må, hvor ingen lov hjemler en særegen undtagelse, alene ske efter en retskendelse.*

Justitia henviser i denne forbindelse til seneste analyse, som viser en løbende stigning i antallet af hjemler, som giver myndighederne bemyndigelse til at foretage husundersøgelser uden forudgående retskendelse. Justitia stiller sig derfor kritisk over for denne fortsatte udvikling i antallet af undtagelsesbestemmelser til grundlovens § 72.

Det ovenfor anførte gør sig ligeledes gældende i henhold til Lov om net- og informationssikkerheds § 9, stk. 7, 1. og 2. pkt., som foreskriver samme beføjelser for CFCS i forhold til teleudbydernes samarbejdspartnere, leverandører og underleverandører. Det må endda anses for endnu mere betænkeligt, at også samarbejdspartnere, leverandører og underleverandører gøres til genstand for CFCS' uprøvede husundersøgelser.

3. Anbefalinger og konklusion

Justitia anser det som en positiv udvikling af lovforslaget, at der nu eksplicit opstilles forbud mod, at CFCS kan indhente oplysninger om udbydernes kunder (borgerne). Det nye lovforslag indeholder således retssikkerhedsmæssige forbedringer sammenlignet med det lækkede udkast.

Justitia
Lautrupsgade 13, 6. sal
2100 København Ø
(+45) 2466 4220
(+45) 2466 4220
info@justitia-int.org

Skrevet af
Jacob Mchangama
d. 28. april 2015

Justitia anser det fortsat for betænkeligt, at der til stadighed vedtages flere undtagelsesbestemmelser til grundlovens § 72. Som det fremgår af hjemlen i Lov om net- og informationssikkerheds § 9, stk. 6, 1. pkt. og Lov om net- og informationssikkerheds § 9, stk. 7, 1. pkt. er det et krav, at tilsynsvirksomheden kun må udføres af hensyn til informationssikkerheden og altså ikke som tilfældigt kontroltjek. Således anses det for betænkeligt, at der ikke stilles krav om retskendelse.

Justitia anser dog 7-dages notifikationskravet i Lov om net- og informationssikkerhed som en forbedring i forhold til hjemmelsbestemmelser, som ikke indeholder et lignende krav for myndighederne. Justitia anbefaler på den baggrund, at tilsvarende krav stilles på andre områder, hvor myndighederne har adgang til borgeres eller virksomheders bolig eller forretningslokaler uden forudgående retskendelse, og hvor man fra lovgivers side ikke ønsker at ophæve en sådan hjemmel.

Justitia
Lautrupsgade 13, 6. sal
2100 København Ø
(+45) 2466 4220
(+45) 2466 4220
info@justitia-int.org