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