

3. juni 2016

## **KOMMENTERET HØRINGSOVERSIGT vedrørende udkast til bekendtgørelser om net- og informationssikkerhed**

Udkast til fire bekendtgørelser om net- og informationssikkerhed har i perioden 29. april 2016 til 18. maj 2016 været i høring hos:

Advokatrådet, Amnesty International, Danmarks Radio, Dansk Beredskabskommunikation A/S, Dansk Energi, Dansk Erhverv, Dansk Industri (DI), DANSK IT, Danske Advokater, Danske Regioner, Datatilsynet, Den Danske Dommerforening, DI Digital, Domstolsstyrelsen, Forenede Danske Antenneanlæg, Global Connect A/S, Hi3G Denmark ApS, HORESTA, Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, KL, Nianet A/S, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Retssikkerhedsfonden, Rigsrevisionen, Rådet for Digital Sikkerhed, SE/Stofa A/S, TDC A/S, Teleindustrien (TI), Telenor A/S, TeliaSonera Danmark A/S, Teracom A/S, TT-Netværket P/S, TV 2 | Danmark A/S og Waoo! A/S.

Heraf har Center for Cybersikkerhed modtaget høringssvar fra:

Dansk Beredskabskommunikation A/S, Dansk Erhverv, Datatilsynet, DI Digital, Institut for Menneskerettigheder, IT-Branchen, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Rigsrevisionen, Rådet for Digital Sikkerhed, Teleindustrien (TI) og TV 2 | Danmark A/S.

De væsentligste bemærkninger fra de hørte parter til de enkelte emner i bekendtgørelsesudkastene gennemgås og kommenteres nedenfor. Center for Cybersikkerheds bemærkninger til høringssvarene er anført med kursiv.

### **Høringssvarene**

Det følgende er overordnet baseret på strukturen i det fælles høringssvar fra Teleindustrien (TI), IT-Branchen og DI Digital (herefter Branchen), men centrale problemstillinger fra øvrige høringssvar er også behandlet.

## 1. Inddragelse af interessenter

Dansk Erhverv (og delvist Branchen) har anført, at der ikke har været tilstrækkelig inddragelse af interessenterne i processen med udarbejdelse af bekendtgørelserne. Endvidere har Rådet for Digital Sikkerhed anført, at en høringsperiode på kun 20 dage er problematisk.

*Center for Cybersikkerhed har lagt vægt på en tæt inddragelse af branchen under udarbejdelsen af bekendtgørelserne. Dette er sket i tre faser. I første fase har der været ført en intensiv dialog med de vigtigste aktører i branchen om afgrænsning af centrale definitioner i bekendtgørelserne. På den baggrund har Center for Cybersikkerhed færdiggjort de første udkast til bekendtgørelser. I anden fase har branchen modtaget udkastene til bekendtgørelserne i præhøring med en høringsfrist på små to uger. På baggrund af branchens tilbagemeldinger har Center for Cybersikkerhed tilpasset bekendtgørelserne, således at en meget stor del af branchens udtrykte bekymringer har kunnet imødekommes. Endelig har der i en tredje fase været gennemført den offentlige høring med en høringsfrist på små tre uger. Interessenterne har dermed været inddraget i væsentligt større omfang, end der normalt er praksis for ved udarbejdelse af regulering.*

Branchen har bemærket, at leverandører af udstyr, netværk, it, drift mv. ikke har været inddraget under det forberedende arbejde med bekendtgørelserne.

*Det har i forbindelse med udarbejdelsen af reguleringen på net- og informationssikkerhedsområdet været overvejet, om kravene i forbindelse med informationssikkerhed helt eller delvist burde rettes mod leverandørerne frem for mod teleudbyderne. Vurderingen er, at en sådan konstruktion vil være stærkt uhensigtsmæssig. Teleudbyderne vurderes således at være nærmest til at fremme informationssikkerheden i deres egne net, idet alene de har forudsætningerne for at foretage en samlet vurdering af informationssikkerheden. En konstruktion, hvor kravene rettes mod en lang række forskellige leverandører, vil skabe en meget fragmenteret tilgang til informationssikkerhed, hvor det potentielt er hundredevis af leverandører hos den enkelte teleudbyder, der hver for sig skal sikre elementer af informationssikkerheden.*

*Derudover bemærkes det, at høringen har været gennemført som en offentlig høring på statens offentligt tilgængelige platform, Høringsportalen, hvor interesserede leverandører fuldt ud har haft mulighed for at komme med bemærkninger til bekendtgørelserne. De involverede brancheorganisationer og teleudbydere har desuden selv haft mulighed for at inddrage relevante leverandører i høringsprocessen.*

## 2. Branchens egen interesse i sikkerhed

Branchen har anført, at teleudbyderne ikke har en kommerciel interesse i at gå på kompromis med sikkerheden, samt at de deler Forsvarsministeriets interesse i at optimere sikkerheden i teleudbydernes net.

*Center for Cybersikkerhed har med tilfredshed noteret sig denne tilkendegivelse fra branchen. Det er centerets opfattelse, at de regler, der er fastsat i bekendtgørelserne, i altovervejende grad svarer til de tiltag, som en sikkerhedsbevidst teleudbyder også ud fra en kommerciel interesse ville tage med henblik på at opretholde et tilfredsstillende sikkerhedsniveau på længere sigt (og dermed også en høj grad af driftsstabilitet).*

### **3. Forholdet til EU-reguleringen**

Branchen har anført, at bekendtgørelserne går videre end de gældende EU-regler, og at regulering på området burde afvente arbejdet i EU. Bekendtgørelserne er endvidere efter Branchens opfattelse i strid med regeringens fem principper for implementering af EU-retsakter. Dansk Erhverv har desuden anført, at den danske praksis for net- og informationssikkerhed skal harmoniseres på fælleseuropæisk niveau.

*For så vidt angår implementeringen af de bagvedliggende EU-direktiver er det Center for Cybersikkerheds opfattelse, at der er tale om en minimumsimplicitering. Derudover er der ud fra et rent nationalt sikkerhedshensyn indført supplerende regler om informationssikkerhed. Det bemærkes i den forbindelse, at spørgsmålet om implementeringen af de bagvedliggende EU-direktiver har været forelagt sekretariatet for EU-implementeringsudvalget i overensstemmelse med Erhvervs- og Vækstministeriets guide til ministerier vedrørende arbejdet i regeringens EU-implementeringsudvalg og Implementeringsrådet. Sekretariatet noterede i den forbindelse, at bekendtgørelserne ikke skulle forelægges for regeringens EU-implementeringsudvalg, idet det var vurderingen, at implementeringen var sket i overensstemmelse med regeringens principper herfor. Endelig skal Center for Cybersikkerhed bemærke, at der ikke i EU på nuværende tidspunkt ses at være planer om en substantiel revision af de relevante bestemmelser i de bagvedliggende direktiver.*

### **4. Mulige skadevirkninger for innovationen**

Branchen har anført, at skærpede sikkerhedskrav i Danmark vil kunne skade innovationen på telemarkedet, da disse sikkerhedskrav vil udgøre en barriere for udenlandske leverandørers introduktion af nye og innovative tjenester, teknologier og systemer på det danske marked.

*Center for Cybersikkerhed skal bemærke, at det ikke nødvendigvis vil være en ulempe, såfremt udenlandske leverandører, der ser de relativt beskedne sikkerhedskrav i bekendtgørelserne som en barriere, fravælger det danske marked. Dette skal ses i sammenhæng med, at Danmark som et højt digitaliseret samfund er særligt afhængigt af et sikkert og velfungerende telenet. En situation, hvor der i Danmark etableres et marked med sikkerhed som et konkurrenceparameter, må således anses for at være en fordel i sig selv. Et sådant marked vurderes også at kunne styrke de danske*

*teleudbyderes position internationalt i takt med, at markedsudviklingen i stigende grad fører til en fokusering på digitale løsninger med et højt sikkerhedsniveau.*

## **5. Erhvervsøkonomiske konsekvenser**

Branchen har anført, at de ikke mener, at vurderingen af de erhvervsøkonomiske konsekvenser af bekendtgørelserne giver et reelt billede af de omkostninger, erhvervslivet vil blive pålagt. Bekendtgørelserne er endvidere efter branchens opfattelse i strid med regeringens byrdestop. Branchen har i den forbindelse også anført, at vurderingen af de erhvervsøkonomiske konsekvenser burde være sket på baggrund af en inddragelse af branchen. Dansk Erhverv har desuden anført, at de ikke er betryggede ved, at der foreligger et tilstrækkeligt robust grundlag for de reelle omkostninger.

*De erhvervsøkonomiske konsekvenser er beregnet i overensstemmelse med Erhvervs- og Vækstministeriets vejledning på området og under inddragelse af Erhvervsstyrelsen. I overensstemmelse med den faste procedure på området er branchen ikke blevet inddraget. En sådan inddragelse skal således først ske, hvis omkostningerne overstiger de bagatelgrænser, der er fastsat af Erhvervs- og Vækstministeriet. Ved beregningen af omkostningerne har Center for Cybersikkerhed gjort brug af den betydelige viden om teleudbydernes sikkerhedsmæssige forhold, som centeret har opnået gennem de seneste års tilsynsvirksomhed.*

## **6. Definitioner**

Branchen har anført, at definitionen af kritiske netkomponenter, systemer og værktøjer indebærer, at alle dele af teleudbydernes net, systemer og tjenester i praksis vil være omfattet. Dansk Erhverv opfordrer derudover til en indskrænkende fortolkning af definitionen, som samtidig er transparent for aktørerne på markedet.

*Den anvendte definition har været nøje overvejet, og det er Center for Cybersikkerheds vurdering, at definitionen, hvor der sker en detaljeret opregning af de omfattede dele, sikrer, at bekendtgørelsernes centrale krav er rettet mod netop de netkomponenter, systemer og værktøjer, som er kritiske i forhold til informationssikkerheden for så vidt angår såvel tilgængelighed som integritet og fortrolighed.*

## **7. Implementeringsfrist**

Branchen har anført, at implementeringen af de nye forpligtelser vil kræve tid, planlægning og ressourcer, og at det kræver en rimelig og realistisk implementeringstid.

*Den forventede regulering i bekendtgørelserne er beskrevet meget detaljeret i forarbejderne til lov om net- og informationssikkerhed, som blev fremsat som lovforslag i oktober 2015 og vedtaget i december 2015. Rammerne for reguleringen har således været kendt af branchen i over et halvt år.*

*På baggrund af præhøringen har Center for Cybersikkerhed endvidere valgt at ændre ikrafttrædelsestidspunktet for den bekendtgørelse, der vedrører sikkerhedsgodkendelse, således at der tages højde for branchens bemærkninger vedrørende implementeringstiden. Endelig har centeret tilkendegivet overfor branchen, at centeret først i 2017 vil iværksætte et egentligt tilsynskoncept til sikring af, at bekendtgørelsernes krav efterleves, hvilket da også anerkendes af Branchen i deres høringssvar.*

## **8. Underretningspligt ved aftaleforhandlinger**

Branchen har i forhold til underretningsordningen ved aftaleforhandlinger anerkendt den lempelse, som er foretaget på baggrund af branchens tilbagemeldinger efter præhøringen. Branchen har dog anført, at et udgangspunkt om indrapportering og standstill-periode på 10 dage er meget vidtgående og indgribende.

*Det anførte om, at der som udgangspunkt er en standstill-periode på 10 dage, bygger på en misforståelse. Efter den nævnte lempelse er udgangspunktet, at der ikke indtræder en standstill-periode i forbindelse med aftaleindgåelse. Standstill-perioden vil således kun indtræde, såfremt Center for Cybersikkerhed i forhold til den enkelte aftaleproces udsteder påbud herom. Et sådant påbud vil alene blive udstedt, såfremt det vurderes nødvendigt ud fra aftalens nærmere indhold sammenholdt med det aktuelle trusselsbillede.*

Branchen har endvidere anført, at der hos de enkelte teleudbydere ikke nødvendigvis findes noget generelt overblik over de aftaleforhandlinger vedrørende bl.a. kritiske netkomponenter, systemer og værktøjer, som gennemføres i forskellige dele af virksomheden.

*Center for Cybersikkerhed anser det for stærkt bekymrende, såfremt der hos disse teleudbydere, som driver centrale dele af den kritiske danske infrastruktur, indgås aftaler om anskaffelse af kritiske netkomponenter, systemer eller værktøjer, uden at sådanne anskaffelser – der kan have væsentlig betydning for informationssikkerheden – er kendt af f.eks. den pågældende teleudbyders centrale sikkerhedsorganisation. Det af branchen anførte må således anses for at være et selvstændigt argument for indførelse af underretningspligten.*

Branchen og Rådet for Digital Sikkerhed har foreslået, at underretningspligten begrænses til leverancer, der vedrører væsentlige dele af teleudbyderens net eller tjenester eller driften heraf.

*Med den lempelse, der skete på baggrund af branchens tilbagemeldinger efter præhøringen, omfatter underretningspligten alene aftaler vedrørende en forholdsvis lille delmængde af den samlede*

*mængde af netkomponenter, systemer og værktøjer. Der er således alene udvalgt de elementer, der må anses for at være kritiske og dermed særligt væsentlige i forhold til informationssikkerheden.*

## **9. Påbudsmulighederne**

I forhold til påbudsbestemmelserne i kapitel 4 i bekendtgørelsen om informationssikkerhed og beredskab i net og tjenester har Branchen og Rådet for Digital Sikkerhed anført, at kriteriet "væsentlig samfundsmæssig betydning" bør konkretiseres nærmere.

*Med anvendelsen af kriteriet "væsentlig samfundsmæssig betydning" understreges det, at påbudsmulighederne i bekendtgørelsens kapitel 4 alene vil kunne anvendes, når særlige forhold gør sig gældende. Det kunne f.eks. – som anført i forarbejderne til lov om net- og informationssikkerhed – være tilfældet, hvis der er tale om trusler mod funktioner, som er særligt vigtige for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed, herunder funktioner inden for sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet.*

*Det skal i øvrigt bemærkes, at udstedelse af et påbud er en forvaltningsretlig afgørelse. Center for Cybersikkerhed vil derfor i forbindelse med udstedelse af et påbud skulle efterleve de forvaltningsretlige principper om bl.a. proportionalitet, ligebehandling, begrundelse, partshøring, vejledning, repræsentation og klagevejledning. Det indebærer således også, at centeret vil være forpligtet til at behandle ensartede forhold lige, ligesom der altid vil skulle foretages en proportionalitetsafvejning, inden der udstedes et påbud.*

Branchen har anført, at et påbud om indstationering af medarbejdere hos udenlandske underleverandører vil kunne være vanskeligt at gennemføre, da teleudbyderne ikke nødvendigvis vil kunne kræve noget sådant af en global leverandør.

*Det skal understreges, at et påbud fra Center for Cybersikkerhed alene vil kunne omfatte mere detaljerede krav om indstationerede medarbejders adgang til leverandørens it-systemer, såfremt dette er i overensstemmelse med det pågældende lands nationale lovgivning. Endvidere vil Center for Cybersikkerhed i forbindelse med teleudbyderens aftaleforhandlinger kunne rådgive teleudbyderen om, hvorvidt et krav om indstationering vil kunne blive aktuelt i forbindelse med den pågældende aftale. Dermed vil den enkelte teleudbyder kunne stille krav om en sådan indstationeringsmulighed allerede i forbindelse med aftaleforhandlinger.*

Branchen har anført, at det er usikkert om Center for Cybersikkerhed vil kunne udstede et påbud om hjemtagning af opgaver, der er outsourcet til en udenlandsk leverandør.

*Som det udtrykkeligt fremgår af den pågældende bestemmelse, vil et påbud alene kunne omfatte krav om, at der på **teleudbyderens foranstaltning** i tilfælde af misligholdelse af en kontrakt om outsourcing kan ske hjemtagning af opgaver, der er outsourcete til en udenlandsk leverandør. Center for Cybersikkerhed vil således ikke kunne påbyde en teleudbyder at hjemtage en given opgave.*

## **10. Omfanget af oplysningspligten**

Branchen har anført, at mange teleudbydere vil have vanskeligt ved at fremskaffe de oplysninger om deres hardware, firmware og software mv., som Center for Cybersikkerhed kan påbyde teleudbyderne at stille til centerets rådighed. Det skyldes bl.a., at teleudbydernes netværk er bygget op over lang tid.

*Center for Cybersikkerhed vil anse det for bekymrende, såfremt der måtte være teleudbydere, som ikke allerede i dag er i besiddelse af de ganske basale oplysninger om væsentlige dele af deres net og tjenester eller varetagelsen af driften heraf, som er omfattet af den pågældende bestemmelse. Det af Branchen anførte må således anses for at være et selvstændigt argument for indførelse af den oplysningspligt, der følger af lov om net- og informationssikkerhed og udmøntes med bekendtgørelserne.*

## **11. Underretningspligten ved brud på informationssikkerheden**

Branchen har anført, at der med bekendtgørelserne sker en udvidelse af underretningspligten ved brud på informationssikkerheden, samt at antallet af såkaldte straks-rapporteringer mindst vil blive fordoblet.

*Underretningspligten følger af EU's rammedirektiv, og der er således tale om implementering af EU-regulering. Også ved implementeringen af underretningspligten er der alene sket en minimums-implementering. Implementeringen er tilpasset de detaljerede retningslinjer, der er udarbejdet af EU-organet ENISA.*

*Center for Cybersikkerhed skal i øvrigt bemærke, at der ikke i forbindelse med underretningspligten opereres med straks-rapportering. Tværtimod er der i forhold til gældende ret sket en lempelse, således at underretningen kan ske op til 14 dage efter et brud på informationssikkerheden.*

Branchen har anført, at udregningen af grænseværdierne, som danner grundlag for underretningspligten, formodes at være behæftet med fejl i forhold til de retningslinjer fra ENISA, som grænseværdierne for underretningspligten er baseret på.

*ENISA's retningslinjer tager udgangspunkt i de situationer, hvor den nationale myndighed – her Center for Cybersikkerhed – skal foretage indberetning til ENISA. Sådanne underretninger vil skulle*

*ske, hvor der er tale om hændelser, der har væsentlig betydning for den samlede telekommunikation i Danmark. Derfor tager ENISA's retningslinjer udgangspunkt i en hændelses påvirkning af det samlede antal telekunder i Danmark. En hændelse, der alene berører et mindre antal kunder hos den enkelte teleudbyder, vil imidlertid – såfremt den påvirker flere forskellige teleudbydere på samme tid – kunne have væsentlig betydning for den samlede telekommunikation i Danmark. I så fald vil Center for Cybersikkerhed være forpligtet til at foretage indberetning til ENISA. Derfor er det ved implementeringen af underretningspligten søgt at sikre, at Center for Cybersikkerhed underrettes om alle relevante hændelser, således at Danmark opfylder sine EU-retlige forpligtelser.*

## **12. Prioriteret adgang til fastnet**

Branchen har anført, at der er behov for en afklaring af, hvorvidt kravene til prioriteret adgang til fastnet også omfatter IP-telefoni over fastnettet (VoIP).

*VoIP, det vil sige internetbaseret telefoni, vil ikke være omfattet af kravene til prioriteret adgang til fastnet. Prioriteret adgang til fastnet omfatter således alene analog telefoni (PSTN).*

## **13. Sikkerhedsbeskyttelse af kredsløbsoplysninger**

Branchen har anført, at kravet om sikkerhedsbeskyttelse af kredsløbsoplysninger indebærer en udvidelse af forpligtelsen i forhold til gældende ret. Branchen finder således anledning til at påpege, at teleudbyderne med bestemmelsen vil risikere, at deres netværkssystemer som helhed vil skulle opfylde kravene til sikkerhedsgodkendelse.

*Center for Cybersikkerhed skal bemærke, at ordlyden af bestemmelsen blev ændret på baggrund af præhøringen. Ordlyden i den bekendtgørelse, der har været i høring, tager således allerede højde for det af Branchen anførte. Der er med bestemmelsen alene et krav om klassifikation af registre, der giver mulighed for at identificere kredsløb som værende faste kredsløb til beredskabsmæssige formål, men vel at mærke kun, hvis registeret i forvejen er omfattet af Justitsministeriets sikkerhedscirkulære, fordi der behandles klassificerede informationer.*