Dansk
Beredskabskommunikation
FORBINDELSE MED SIKKERHED

Center for Cybersikkerhed

Glostrup 18. maj 2016

Sendt pr mail til jura@cfcs.dk
Kopi til: stibus@cfcs.dk

Vedr. Dansk Beredskabskommunikation A/S' bemærkninger til Høring om udkast til bekendtgørelser om net- og informationssikkerhed.

Dansk Beredskabskommunikation A/S (DBK) har den 29. april 2016 modtaget ovennævnte udkast til fire bekendtgørelser i høring fra Center for Cybersikkerhed (CFCS). Bekendtgørelserne har hjemmel i Lov nr.1567 af 15. december 2015 om net- og informationssikkerhed (NIS-loven) der træder i kraft 1. juli 2016.

DBK har den 29. juni 2007 indgået kontrakt med Økonomistyrelsen "om samordning af nød- og beredskabskommunikation m.v." (SINE-kontrakten) som regulerer en lang række af de forhold der nu søges reguleret i NIS-loven med nærværende udkast til bekendtgørelser.

Generelt.

Med reference til ovennævnte lov nr. 1567 af 15. december 2015, § 2 stk. 3 og stk. 5 anser DBK sig ikke omfattet af loven, og således heller ikke af bekendtgørelserne:

Fra lov nr.1567, § 2 (definitioner):

I denne lov forstås ved:

stk. 3): Offentligt tilgængelige net og tjenester: Net og tjenester, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere.

Stk. 4): Udbyder: Den, der med et kommercielt formål stiller produkter, net eller tjenester til rådighed for andre.

Stk. 5): Erhvervsmæssig udbyder: En udbyder, der med et kommercielt formål udbyder produkter, net eller tjenester som sin hovedydelse eller som en ikke accessorisk del af virksomheden.

Idet DBK alene leverer kommunikation via et lukket netværk, hvor slutbrugerkredsen er stærkt afgrænset og bestemt af vores kunde, Center for Beredskabskommunikation under Rigspolitiet (CFB) (SINE - kontraktpartner), er DBKs net ikke offentligt tilgængeligt (stk. 3).

Dansk Beredskabskommunikation A/S
CVR nr.: 26210895
Sydvestvej 21, 2600 Glostrup
Telefon: 70 116 112, Fax: 43 488 148

En begrænset del af nettet, som udbydes til private brugere, som individuelt godkendes af CFB, og som således forbliver at betragte som et ikke offentligt tilgængeligt net, er i alle sammenhænge at betragte som accessorisk i forhold til DBKs hoved virksomhed: leverance af lukkede net til beredskabsformål (stk. 5).

Det er således DBKs opfattelse, at definitionerne i udkastene til bekendtgørelserne, specielt

kapitel 1, § 9, Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester:

stk. b) Udbydere, der gennem aftaler med statslige myndigheder og institutioner betjener mere end 500 slutbrugere. Ved opgørelsen medregnes de statslige myndigheder og institutioners egne slutbrugere.

er underlagt definitionerne i lovteksten og at de således ikke er gældende for DBKs drift af SINE nettet.

DBK vil venligst udbede sig CFCS kommentar til DBKs ovennævnte fortolkning.

Kommentarer.

Skulle CFCS definere DBKs ejerskab og drift af SINE nettet anderledes, således at CFCS opfatter DBKs drift af SINE Nettet som værende omfattet af NIS-loven, og dermed også af udkastene til bekendtgørelserne, har DBK nedenstående bemærkninger til bekendtgørelserne:

Generelt:

Det er for DBK uklart hvilken rolle, DBKs kunde, CFB, har i forhold til loven og bekendtgørelserne. CFB er ifølge Bekendtgørelse nr. 262 af 22. april 2008 § 2, stk. 2 ansvarlig for Økonomistyrelsens aftale med leverandørerne af SINE nettet (DBK). Aftalen med staten om bygning og drift at SINE, SINE kontrakten omfatter en lang række bestemmelser som behandler de områder som alle fire udkast til bekendtgørelser omhandler.

DBK beder venligst CFCS forklare forholdet mellem bestemmelserne i SINE kontrakten og CFBs administration heraf i forhold til nærværende udkast til Bekendtgørelser.

Specifikke kommentarer

Vi har nedenfor anført bemærkninger til specifikke paragraffer i bekendtgørelserne:

Vedr: Udkast til Bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.

Det funktionelle indhold af dette udkast er sikret gennem konkrete bestemmelser i SINE kontakten, hvor administrationen heraf administreres af CFB.

Følgende paragraffer er i konflikt med DBKs forpligtelser i henhold til SINE kontrakten:

§ 8. Foranstaltninger til sikret adgang administreres af CFB. Såfremt CFCS skulle give påbud herunder, skal disse afklares med CFB og ikke med DBK.

§ 10. stk. 3. Afgørelser om bestilte kredsløb er beredskabsmæssigt relevante afgøres af CFB.

§ 11. Procedurer for behandling af bestilling af faste kredsløb til beredskabsmæssige formål er fastlagt via SINE kontrakten og administreres af CFB.

§ 14. Prioritering af kredsløb er ikke relevant, idet alle kredsløb i SINE nettet er prioriterede. Prioritering i beredskabssituationer administreres af CFB.

§ 18. SINE Nettet er etableret med TDC som underleverandør. Alle SINE forbindelser i TDCs netværk er etableret som prioriterede forbindelser.

Vedr: Udkast til Bekendtgørelse om informationssikkerhed og beredskab i net og tjenester.

§13. Etablering af logning, på det beskrevne niveau, vil være en væsentlig økonomisk omkostning for DBK. Idet SINE nettet er etableret, drives og administreres i et sikret miljø (alle medarbejdere er HEM klassificerede, alle systemer opereres i adgangssikrede områder) er logningen ikke en del af SINE kontraktens krav til driften af nettet.

§ 21. DBK benytter TDC som underleverandør til SINE nettet. Underleverancen er etableret som en kontrakt med TDC etableret på back-to-back vilkår med SINE kontrakten. DBK har en prioriteret position hos TDC, som sikrer vores rettigheder i forhold til SINE kontrakten. Det er uklart i hvilket omfang TDC som underleverandør vil være styret af CFB via DBK hhv. af CFCS.

§ 25. Informationssikkerhedsforanstaltninger er reguleret via SINE kontrakten. Foranstaltningerne overvåges af CFB. Etablering og administration af foranstaltninger under denne paragraf vil medføre væsentlige økonomiske omkostninger for DBK, ligesom der kan opstå konfliktende krav fra henholdsvis CFB og CFCS.

§ 26. Se §25 ovenfor.

§30. Krisestyring sker i henhold til SINE kontrakten og overvåges af CFB. Det er usikkert hvordan påbud fra CFCS skal håndteres i forhold til CFB. Beredskabssituationer håndteres i samarbejde med CFB – hvordan ses det ske i samarbejde med CFCS?

§ 31. Hvad vil CFCS' rolle være i forholdt til CFBs rolle?

§ 32. Hvad vil CFCS' rolle være i forholdt til CFBs rolle?

Vedr: Udkast til Bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed.

§ 3 - 6 Det er DBKs opfattelse, at CFCS eventuelle påbud i henhold til disse paragraffer alene vil tjene til forsinkelse af nødvendige aftaler og at sådanne forhold er bedst reguleret ved specifikke forhåndskrav til aftaler og aftalepartnere.

§ 7. Det er uklart hvad der menes med "brud på informationssikkerheden". Er det brud på driften, er det brud på fortroligheden i kommunikationen?

§ 8. Det er uklart hvordan hele denne paragraf skal tolkes, og således hvordan et eventuelt brud på informationssikkerheden (som defineret i § 7) skal måles.

§ 11. Et påbud herunder vil tvinge DBK til at bryde med fortroligheds bestemmelserne i SINE kontrakten.

Vedr: Udkast til Bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet

Ingen kommentarer til dette udkast.

Vi er selvfølgelig til rådighed for en yderligere afklaring af vores kommentarer ovenfor og ser frem til at modtage jeres høringsnotat fra denne høring.

Venlig hilsen

Dansk Beredskabskommunikation A/S

Kalvs Berthelsen, Administrerende Direktør

DANSK ERHVERV
BØRSEN
DK-1217 KØBENHAVN K
WWW.DANSKERHVERV.DK

T. +45 3374 6000
-
-
INFO@DANSKERHVERV.DK

Center for Cybersikkerhed
Att.: Thomas Lund-Sørensen
Sendt til: jura@cfcs.dk og stibus@cfcs.dk

18. maj 2016

Høring over bekendtgørelser om net- og informationssikkerhed

Dansk Erhverv har 29. april 2016 modtaget udkast til fire bekendtgørelser om net- og informationssikkerhed, som Center for Cybersikkerhed sender i høring.

Generelle bemærkninger

Digitale teknologier skyller i disse år i over samfundet og forandrer præmisserne for at drive forretning. Med den digitale udvikling spiller geografiske afstande ikke længere samme rolle for samhandel, og der opstår nye digitale forretningsmodeller med globale potentialer. Det er en udvikling, som ligger Dansk Erhvervs medlemmer meget på sinde, og som Dansk Erhverv sætter højt på dagsordenen, senest med vores årsdag og kampagne om digital omstilling, "disruption.dk".

Teleinfrastrukturen er fundamentet for den digitale økonomi. Alle virksomheder har brug for en robust og tidssvarende digital teleinfrastruktur, uanset virksomhedens størrelse, branchetilknytning eller geografiske placering.

Dansk Erhverv anerkender således behovet for, at it-infrastrukturen følger med også på det sikkerhedsmæssige område, hvilket er baggrunden for NIS-loven og bekendtgørelserne, som aktuelt er i høring. It-sikkerhed har aldrig har været mere aktuel, idet samfundet til stadighed bliver mere afhængigt af en robust it-infrastruktur. Således bakkede Dansk Erhverv op om målene om at styrke og professionalisere it-sikkerheden i Danmark, da Center for Cybersikkerhed (CFCS) fik et lovgrundlag i 2014.

De aktuelle forslag til bekendtgørelser synes dog at tilsidesætte, at der også er behov for gode og stabile rammevilkår for at drive udviklingen. Aktører der udvikler, opbygger, driver og udbyder infrastrukturen har brug for regulatorisk forudsigelighed og EU-harmoniserede regler, og Danmark må ikke gå national enegang. Det ville sætte investeringer og innovation over styr.

Det er derfor bekymrende, hvis det sker med disse bekendtgørelser. Dansk Erhverv noterer sig med stor alvor, at Teleindustrien vurderer, at Danmark med de fire bekendtgørelser går videre

DANSK ERHVERV

-/JSA
jsa@danskerhverv.dk

Vores ref.: SAG-2014-02802
580277

end andre europæiske lande, Danmark normalt sammenligner sig med, og at interessentinddragelsen har været mangelfuld.

Dansk Erhverv mener, at den danske praksis for net- og informationssikkerhed skal harmoniseres på fælleseuropæisk niveau. Ikke mindst med tanke på internettets globale natur.

Specifikke bemærkninger

Administrative konsekvenser for erhvervslivet

Center for Cybersikkerhed oplyser i høringsbrevet, at Erhvervsstyrelsen har vurderet, at omkostningerne for forslagene beløber sig til 4 mio. kr., samt 10 mio. kr. i årlige efterlevelsesomkostninger. Henset til processen om sessionslogning tidligere på året – der som bekendt blev udskudt fordi udgifterne ved nærmere eftersyn viste sig ganske betydelige – er Dansk Erhverv ikke betrygget ved, at der her foreligger et tilstrækkelig robust grundlag for de reelle omkostninger. Også her henviser vi til Teleindustriens anbringende om utilstrækkelig interessentinddragelse.

Sektor og brancheneutralitet

Dansk Erhverv er ikke tryg ved, om definitionerne i udkast til bekendtgørelser er tilpas præcise, og om bekendtgørelserne som helhed er sektor- og brancheneutrale. Vi må ikke ende i en situation, hvor én type spillere på markedet pålægges større byrder, mens en anden type i praksis navigerer uden disse byrder - hvis de i praksis løser samme behov, men definitorisk falder i forskellige kategorier.

Underretning af Center for Cybersikkerhed om aftaleforhandlinger (§3 - §5, side 2)

Det er ganske usædvanligt at pålægge virksomheder at skulle underrette en myndighed, når der indledes forhandlinger med en anden virksomhed. Det er også ganske vidtgående, at Center for Cybersikkerhed får beføjelse til at påbyde kommercielle spillere at indsende udkast til aftaler, hvor Center for Cybersikkerhed kan stille en forhandling i bero i op mod 10 dage. Her bliver definitionen af "kritiske netværkskomponenter, systemer og værktøjer" ganske afgørende, og Dansk Erhverv opfordrer til en indskrænkende fortolkning, som samtidig er transparent for aktørerne på markedet.

Dansk Erhverv henviser i øvrigt til høringssvar fra Teleindustrien, IT-Branchen m.fl., som Dansk Erhverv bakker fuldt op om.

Med venlig hilsen

Janus Sandsgaard
Fagchef for it og digitalisering

DATATILSYNET

Center for Cybersikkerhed Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Sendt til: jura@cfcs.dk og stibus@cfcs.dk

18. maj 2016

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. 2016-122-1077, 2016-122-1078, 2016-122-1079 og 2016-122-1080
Sagsbehandler
Anders Petersen
Direkte 3319 3221

Vedrørende høring over udkast til fire bekendtgørelser om net- og informationssikkerhed

Center for Cybersikkerhed har den 29. april 2016 anmodet om Datatilsynets bemærkninger til centerets udkast til følgende bekendtgørelser:

- Bekendtgørelse om informationssikkerhed og beredskab i net og tjenester.
- Bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed.
- Bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.
- Bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet.

1. Det følger af persondatalovens[1] § 1, stk. 1, at loven gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Ved personoplysninger forstås, jf. persondatalovens § 3, nr. 1, enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede).

Ved behandling forstås, jf. persondatalovens § 3, nr. 2, enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for.

Efter en gennemgang af de tilsendte udkast til bekendtgørelser kan Datatilsynet ikke umiddelbart identificere, at bekendtgørelserne hjemler behandlinger omfattet af persondataloven.

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer

2. Datatilsynet skal dog understrege, at hvis der sker behandling af personoplysninger, skal behandlingen ske under behørig iagttagelse af persondatalovens og sikkerhedsbekendtgørelsens[2] regler.

Datatilsynet kan navnlig pege på følgende regler i persondataloven:

- Grundbetingelserne i persondatalovens § 5 om god databehandlingsskik, saglighed, proportionalitet, datakvalitet og sletning
- Behandlingsbetingelserne i persondatalovens § 6 om almindelige personoplysninger, §§ 7 og 8 om følsomme personoplysninger samt § 11 om personnumre
- Reglerne om de registreredes personers rettigheder i kapitel 8-10, herunder
    - Den dataansvarliges oplysningspligt ved modtagelse/indsamling af oplysninger, jf. persondatalovens §§ 28 og 29
    - Den registreredes ret til indsigt og øvrige rettigheder
- Reglerne om datasikkerhed i §§ 41 og 42 – kravet om fornødne sikkerhedsforanstaltninger, skriftlig databehandleraftale og kontrol med databehandleren
- Reglerne om anmeldelse til og tilladelse/udtalelse fra Datatilsynet i kapitel 12 og 13 samt reglerne om tilladelse fra Datatilsynet i bl.a. § 10, stk. 3, og § 27, stk. 4

Hvis der i bekendtgørelser fastsættes regler om behandling af personoplysninger, skal der være hjemmel til dette i bemyndigelsesloven.

Eventuelle bestemmelser om behandling af personoplysninger i bekendtgørelserne må ikke fravige persondataloven. Fravigelse af persondataloven kan således kun ske ved lov, og det skal i den forbindelse fremgå af lovforslaget, at der tilsigtes en fravigelse af persondataloven.

Hvis der er særregler om behandling af personoplysninger i den lov, som bekendtgørelsen vedrører, skal disse regler også iagttages.

I sidste ende må Datatilsynet forbeholde sig sin stillingtagen til eventuelle behandlinger af personoplysninger som følge af bekendtgørelsernes bestemmelser i tilfælde af en eventuel klage eller lignende.

Med venlig hilsen

Anders Petersen

---

[2] Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001, om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

INSTITUT FOR
MENNESKE
RETTIGHEDER

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
DIREKTE 3269 8866
LGH@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 16/01472-3

Center for Cybersikkerhed
Kastellet 30
2100 København Ø
Danmark

Att. jura@cfcs.dk og stibus@cfcs.dk

18. MAJ 2016

HØRING OVER UDKAST TIL FIRE BEKENDTGØRELSER OM NET- OG INFORMATIONSSIKKERHED

Center for Cybersikkerhed har ved e-mail af 29. april 2016 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til udkast til

- Bekendtgørelse om informationssikkerhed og beredskab i net og tjenester
- Bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed
- Bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.
- Bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet

De fire bekendtgørelser udstedes med hjemmel i lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed (NIS-loven), der træder i kraft 1. juli 2016.

Instituttet afgav 7. maj 2015 høringssvar til det udkast til lovforslag, der gik forud for lov nr. 1567/2015. Instituttet fremsatte i høringssvaret en bekymring for, at lovforslaget overlod Center for Cybersikkerhed meget vide rammer i forhold til at kunne regulere området for net- og informationssikkerhed ved bekendtgørelse og herunder fastsætte regler om påbud til udbydere af offentligt tilgængelige net og tjenester.

Instituttet minder igen om sine anbefalinger af 7. maj 2015 og noterer sig i forlængelse heraf, at hjemmelen nu udmøntes i blandt andet en meget vidtgående adgang for Center for Cybersikkerhed til at give påbud til udbydere. Det gælder for eksempel bestemmelserne i kapitel 4 i udkastet til bekendtgørelse om informationssikkerhed og beredskab i net og tjenester (påbud om konkrete informationssikkerhedsforanstaltninger).

Det gælder også bestemmelserne i § 2 i udkastet til bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed (påbud om afgivelse af oplysninger til Center for Cybersikkerhed om udbyderens net og tjenester, herunder hardware, firmware og softwares fabrikat, konfiguration, typebetegnelse, serienummer, antal og lignende)

I lyset af at loven, herunder de mange og brede bemyndigelser til Center for Cybersikkerhed, blev vedtaget af Folketinget har instituttet dog ingen konkrete bemærkninger til de enkelte bekendtgørelser.

Med venlig hilsen

Lise Garkier Hendriksen
SPECIALKONSULENT

Vestre Landsret
Præsidenten

Forsvarets Efterretningstjeneste
Center for Cybersikkerhed
Kastellet 30
2100 København Ø

J.nr. 40A-VL-24-16
Den 09/05-2016

Center for Cybersikkerhed har ved brev af 2. maj 2016 sendt udkast til fire bekendtgørelser om net- og informationssikkerhed i høring.

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

Dette svar sendes efter anmodning til jura@cfcs.dk med kopi til stibus@cfcs.dk.

Med venlig hilsen

Bjarne Christensen

Østre Landsret
Præsidenten

Den - 3 MAJ 2016
J.nr. 40A-ØL-25-16
Init: cr

Center for Cybersikkerhed FE
Chef for Center for Cybersikkerhed Thomas Lund-Sørensen
Kastellet 30
2100 København Ø

Sendt pr. mail til jura@cfcs.dk og stibus.cfcs.dk

Center for Cybersikkerhed har ved brev af 29. april 2016 anmodet om eventuelle bemærkninger til høring over udkast til fire bekendtgørelser: Bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed, bekendtgørelse om informationssikkerhed og beredskab i net og tjenester, bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer m.v. og bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet.

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

Med venlig hilsen

Bent Carlsen

Ellen Buck Porsbo

Juridisk Sektion

Fra: Kjeld Røgilds-Heinsøe <krh@rigsrevisionen.dk>
Sendt: 18. maj 2016 12:22
Til: Juridisk Sektion; Stine Busch Østergren
Cc: Michael Kubel; Henrik Lange; Kjeld Røgilds-Heinsøe
Emne: Rigsrevisionens kontor for it-revision har gennemgået de 4 høringsudkast til bekendtgørelser om net- og informationssikkerhed, jf. CfCS' høringsbrev 29. april 2016.
Vedhæftede filer: Høringsbrev.pdf

Til Center for Cybersikkerhed

Kære Thomas Lund-Sørensen

Rigsrevisionens kontor for it-revision har gennemgået de 4 høringsudkast til bekendtgørelser om net- og informationssikkerhed (NIS-loven), jf. CfCS' høringsbrev 29. april 2016.

Vi vurderer, at de 4 høringsudkast ikke påvirker vores mulighed for at udføre it-revision på området.

Med venlig hilsen

Kjeld Røgilds-Heinsøe
Fuldmægtig, CISA

RIGSREVISIONEN

Landgreven 4
DK-1301 København K

Tlf. +45 33 92 84 00
Dir. +45 33 92 86 51

krh@rigsrevisionen.dk
www.rigsrevisionen.dk

Rådet for
Digital Sikkerhed

Center for Cybersikkerhed

Jura@cfcs.dk

Cc: stibus@cfcs.dk

18. maj 2016

Bemærkninger til udkast til bekendtgørelser vedrørende net- og informationssikkerhed

Rådet for Digital Sikkerhed afgiver hermed sine bemærkninger til bekendtgørelserne vedrørende lov om net- og informationssikkerhed. Lovens formål er at styrke informationssikkerheden i telesektoren og afspejler ifølge høringsbrevet det aktuelle trusselsbillede, hvor cyberangreb og avanceret industrispionage er stærkt stigende.

Vi vil som start gerne bemærke, at den meget korte høringsperiode på kun 20 dage er problematisk og giver meget kort tid til at vurdere og respondere på indholdet i de fire bekendtgørelser. Bekendtgørelserne kan have meget stor betydning for sikkerheden og økonomien i telebranchen, som er yderst væsentlig for Danmarks sikkerhed, og derfor finder vi det beklageligt, at der ikke er afsat tid til en grundigere høringsfase.

Rådet for Digital Sikkerheds vision er at skabe et trygt og frit digitalt samfund for alle, i balance mellem adgang til og effektiv brug af moderne it-teknologi og behovet for beskyttelse mod it-relaterede trusler. Set i dette lys, finder Rådet for Digital Sikkerhed det glædeligt at CFCS vil hjælpe med den sikkerhedsmæssige udvikling i telebranchen, men finder dog at omfanget af de i bekendtgørelserne beskrevne forpligtelser er for vidtgående og i nogen grad hindrende for udviklingen af sikkerhed i branchen.

Vi mener som udgangspunkt at CFCS's rolle i forbindelse med sikkerhed i privat erhverv bør være vejledende, ikke styrende. Telebranchen bør ikke fratages råderet over udvikling af sikkerheden i egne digitale platforme og lægge opskriften på "rigtig sikkerhed" i hænderne på offentlige myndigheder. Derudover mener vi ikke at det er gavnligt for sikkerheden at påføre hverken private eller offentlige aktører et dokumentationsregime, der ikke er umiddelbart skønnes proportionalt med ønsket om øget informationssikkerhed.

I nuværende form, mener vi at forslaget kan stække Danmarks mulighed for at følge med den teknologiske udvikling, idet de berørte virksomheder vil have færre ressourcer til forskning og udvikling, og idet aftaleindgåelse på markedet besværliggøres. Dette vurderes umiddelbart rent faktisk, at kunne sænke sikkerhedsniveauet hos udbyderne da indgrebet også vil påvirke implementeringen af nye sikkerhedsteknologier, der således også skal godkendes og kontrolleres af myndighederne.

Rådet stiller yderligere spørgsmålstegn ved den stærkt udvidede indberetningspligt af sikkerhedsmæssige dybt forretningsfortrolige områder, til offentlige myndigheder. Der nævnes f.eks. "hardware, firmware og softwares fabrikat, konfiguration, typebetegnelse, serienummer, antal og tilsvarende, oplysninger om netarkitektur og -design, eventuelle leverandører, herunder driftsleverandører, samt den geografiske placering af udbydernes og relevante leverandørers hardware og drifts- og supportcentre."

Underretningspligter

Bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed §3 og §5 tilsiger, at netudbydere skriftligt skal underrette CFCS forud for, at der indledes forhandlinger om aftaler,

der vedrører kritiske netkomponenter, samt at aftaler først kan indgås, når udbyderen på forhånd har sendt aftaleteksten til CFCS og modtaget en tilbagemelding.

Da der forventeligt vil være tale om et meget stort antal aftaler, der årligt skal vurderes af CFCS, vil dette kræve en centralisering af forhandlingsprocedurerne i den enkelte virksomhed, samt en væsentlig forsinkelse af alle forhandlinger, idet der skal afventes tilbagemeldinger fra CFCS.

Det er efter vores vurdering ikke åbenlyst, at denne foranstaltning medfører en forbedring af informationssikkerheden, tværtimod kan det forsinke en eventuel forbedring af sikkerheden. Vi forudser også, at dette vil medføre et ikke ubetydeligt ressourcepres på CFCS, hvorfor lang sagsbehandlingstid må forventes.

Rådet for Digital Sikkerhed foreslår, at der indføres et væsentlighedskriterium i §3 og §5, således at udbydere alene pålægges at underrette CFCS på forhånd og afvente tilbagemelding for aftaler, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf.

Vurdering af 'væsentlig samfundsmæssig betydning'

I bekendtgørelse om informationssikkerhed og beredskab i net og tjenester §25 og §26 fremgår, at CFCS "såfremt det er af væsentlig samfundsmæssig betydning, efter en konkret vurdering" kan påbyde netudbydere at foretage en række foranstaltninger.

Vi vil dertil bemærke, at definitionen af 'væsentlig samfundsmæssig betydning' bør konkretiseres nærmere i bekendtgørelsen. Alternativt bør der af retssikkerhedsmæssigt hensyn indføres et krav om, at CFCS i sådanne tilfælde kan begrunde og dokumentere den væsentlige samfundsmæssige betydning af foranstaltningen.

Med venlig hilsen

Bestyrelsen
Rådet for Digital Sikkerhed

Center for Cybersikkerhed

jura@cfcs.dk
stibus@cfcs.dk

18. maj 2016

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

Teleindustrien, IT-Branchen og DI Digital (herefter branchen) har den 29. april 2016 modtaget udkast til forslag til bekendtgørelser om net- og informationssikkerhed i høring.

Branchen udtalte i forbindelse med høringen over lov om net- og informationssikkerhed (NIS-loven), at de foreslåede regler 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. Branchen har derfor haft en klar forventning om, at udmøntningen af lovens rammebestemmelser i bekendtgørelsesform ville sikre, at disse bekymringer blev iagttaget. Branchen kan imidlertid konstatere, at dette på ingen måde er tilfældet.

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

Bekendtgørelserne indeholder vide skønsbeføjelser og muligheder for Center for Cybersikkerhed (CFCS) til at træffe meget vidtgående påbud uden nærmere afgrænsning af kriterierne for skønsudøvelsen. Bekendtgørelserne ses at mangle grundlæggende proportionalitetsbetragtninger og kriterier for udøvelse af CFCS' skøn.

Udmøntningen i de foreliggende bekendtgørelser går videre end de gældende EU-regler og indføres før, der er lavet fælles europæiske regler på området. Det betyder, at danske udbydere bliver 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.

Branchen er uforstående overfor, at der er behov for, at der i Danmark indføres sikkerhedsbestemmelser, der går videre end de gældende regler i EU og i øvrigt går langt videre end andre europæiske lande som Danmark normalt sammenligner sig med. Bekendtgørelserne er således både i strid med

Regeringens byrdestop for erhvervslivet og Regeringens 5 principper for implementering af EU-retsakter.

Branchen mener derfor, at detail lovgivningen på området bør afvente arbejdet i EU frem for at lave danske særregler.

I det følgende er branchens bemærkninger til bekendtgørelserne struktureret som følger:

1. Barrierer og økonomiske konsekvenser
2. Afgrænsning af hvilke dele af udbydernes virksomhed der er omfattet
3. Ikrafttræden
4. Underretningspligt og stand still ved aftaleforhandlinger
5. Påbud
6. Specifikke bemærkninger til bekendtgørelserne

1. Barriere for udbuddet af innovative teknologier og økonomiske konsekvenser

Branchen undrer sig over, at de leverandører (udstyr, netværk, it, drift mv.), der opererer på det danske marked, og som vil være helt afgørende i relation til udbydernes efterlevelse af bekendtgørelsernes forpligtelser ikke er blevet hørt eller inddraget direkte (hver især) i forbindelse med udarbejdelsen af bekendtgørelserne på samme vis som teleudbyderene.

Branchen erfarer, at visse af sådanne leverandører har givet udtryk for, at en sådan regulering, der jo er en dansk særregulering, kan udgøre en væsentlig barriere for udbuddet af nye innovative tjenester, teknologier og systemer på det danske marked, da kravene er signifikant anderledes, end hvad der gælder i Europa i øvrigt. Med andre ord er der en væsentlig risiko for, at Danmark isoleres på det europæiske marked til skade for innovationskraften på telemarkedet og i sidste ende forbrugernes adgang til nye tjenester og teknologier.

Det bemærkes, at netværksleverandører hidtil har anvendt det danske marked til at afprøve nye teknologier, hvilket danske teleselskaber har kunnet drage fordel af dels i form af at ny teknologi kan udrulles hurtigere til de danske forbrugere og dels i form af, at det har været muligt at forhandle fordelagtige indkøbsaftaler.

Branchen støtter synspunktet og beklager, at området ikke underlægges en harmoniseret fælleseuropæisk tilgang.

Erhvervsøkonomiske konsekvenser
Branchen (ved TI) påpegede i forbindelse med pre-høringen over udkast til bekendtgørelser behovet for en nærmere erhvervsøkonomisk analyse.

Branchen henviste i den forbindelse til, at Forsvarsministeren ved udvalgsbehandlingen i forbindelse med vedtagelsen af hjemmelsloven (lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed) udtalte følgende:

"De bekendtgørelser, der skal udmønte bemyndigelserne i lovforslaget, vil endvidere blive udarbejdet under inddragelse af telebranchen og Erhvervsstyrelsen. Der vil ved udarbejdelsen være fokus på at sikre en hensigtsmæssig balance mellem på den ene side de økonomiske og administrative byrder, som reguleringen kan medføre, og på den anden side hensynet til informationssikkerheden.

Bekendtgørelserne vil også blive sendt i offentlig høring. I den forbindelse vil Center for Cybersikkerhed i overensstemmelse med Erhvervsstyrelsens vejledning om erhvervsøkonomiske konsekvensvurderinger gøre brug af og offentliggøre Erhvervsstyrelsens særlige skabelon for vurdering af erhvervsøkonomiske konsekvenser i bekendtgørelser."

CFCS har i følgebrevet i forbindelse med høringen oplyst, at Erhvervsstyrelsen har været inddraget i belysning af de erhvervsøkonomiske konsekvenser og har i den forbindelse vurderet at de samlede administrative omkostninger for erhvervslivet udgør 4 mio. kr. årligt og 10 mio. kr. årligt i efterlevelsesomkostninger.

De oplyste tal kan branchen svært forestille sig udgør en reelt billede af de omkostninger erhvervslivet vil blive pålagt. Branchens aktører har i øvrigt ikke været inddraget en sådan analyse, og branchen stiller sig derfor undrende overfor, hvordan Erhvervsstyrelsen kan komme frem til ovenstående tal uden at inddrage branchen.

Dertil kommer, at de meget brede skønsbeføjelser for CFCS kan medføre, at selskaberne undervurderer omkostningerne og konsekvenserne af de påbud selskaberne kan blive mødt med.

Eksempelvis vil et påbud om at skulle hjemtage opgaver der er outsourcet eller påbud om at indstationere egne medarbejdere hos underleverandører, jf. bemærkningerne nedenfor, kunne løbe op i adskillige millioner for et enkelt selskab

Den erhvervsøkonomiske analyse tager heller ikke højde for, at de danske særregler kan afholde internationale netværksleverandører fra at anvende det danske marked, jf. bemærkningerne ovenfor, hvilket alt andet lige vil medføre øgede investeringsomkostninger for teleudbyderne for at tiltrække netværksleverandører.

2. Afgrænsning af hvilke dele af udbydernes virksomhed der er omfattet

Der mangler gennemgående i alle udkast til bekendtgørelser en afgræsning af hvilke dele af udbydernes net og systemer, der er omfattet af de forpligtelserne som udbyderne skal overholde.

CFCS har med definitionen af *"Kritiske netkomponenter, systemer og værktøjer"* forsøgt at afgrænse området, men definitionen er skrevet så bredt, at alle dele af udbydernes net, systemer og tjenester i praksis vil være omfattet.

Branchen finder, at definitionen er unødvendig bedt formuleret og kommer til at omfatte langt flere elementer end nødvendigt. Branchen har eksempelvis vanskeligt ved at se, at business supportsystemer, der ikke håndtere afvikling af trafikdata udgør en sikkerhedsrisiko i forhold til integritet, tilgængelighed og fortrolighed i net og tjenester.

Ved at lade systemer der ikke håndterer afvikling af trafikdata i elektroniske kommunikationsnet være omfattet af definitionen, vil udbyderne blive pålagt byrder, der stiller udbyderne i en ulige konkurrencesituation med udenlandske "over the top" tjenesteudbydere (OTT-tjenester). Eksempelvis er traditionelle tjenester så som taletelefoni, lineært TV, sms/MMS under voldsom konkurrenceudsættelse fra udbydere som Google, Facebook og Microsoft, der ikke er omfattet af udbyderbegrebet i Lov om Net og informationssikkerhed.

Sådanne udbydere vil ikke blive mødt med tilsvarende sikkerhedskrav til administrative systemer herunder business support systemer.

Det skal videre bemærkes, at administrative systemer der behandler andre typer af kundedata end trafikdata, er omfattet af de persondataretlige regler, og der er således allerede i dag to myndigheder i form af Datatilsynet og Erhvervsstyrelsen, der påser, at udbyderne overholder reglerne om behandling af persondata i selskabernes management og supportsystemer.

Det er derfor vigtigt, at forpligtelser i relation til net- og informationssikkerhed alene berører kritiske netkomponenter, systemer og værktøjer, der direkte anvendes til netværksdriften af elektronisk kommunikationsnet eller tjenester.

Branchen foreslår definitionen i bekendtgørelserne affattes som følger:

"Kritiske netkomponenter, systemer og værktøjer: Operations support systemer, network management systemer og business support systemer, der benyttes til at aflæse, ændre indhold af eller dirigere ***trafikdata*** *i elektronisk kommunikationsnet- eller tjenester, samt hardware, firmware og software, der afvikler eller behandler trafikdata i core-net i mobilnet, fastnet og internet, eller i centrale routere og servere i backbonenettene eller i kontrolenheder, der anvendes til styring i mobilnettenes radionet."*

3. Ikrafttræden og implementering

Branchen har noteret sig, at bekendtgørelserne forventes – som NIS-loven – at træde i kraft den 1. juli 2016, idet bekendtgørelsen om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet dog først forventes at træde i kraft den 1. januar 2017, således at der tages højde for ekspeditionstiden for sikkerhedsgodkendelser.

Branchen har også noteret sig, at CFCS i høringsbrevet bemærker, at CFCS i resten af 2016 vil have fokus på en dialog med de teleudbydere, der er omfattet af bekendtgørelserne, om den praktiske implementering af de nye krav, der følger af bekendtgørelserne. Centeret forventer således først i 2017 at iværksætte et egentligt tilsynskoncept til sikring af, at bekendtgørelsernes krav efterleves.

Branchen bemærker, at en væsentlig del af forpligtelserne i udkastene, herunder eksempelvis kapitel 2 og 3 i udkast til bekendtgørelse om informationssikkerhed og beredskab i net og tjenester, samt i bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet i sin helhed, er nye ift. den gældende retstilstand på området, og træder i kraft umiddelbart ved bekendtgørelsens ikrafttræden.

Branchen skal bemærke, at omfanget af disse nye forpligtelser er signifikant, og at implementeringen heraf vil kræve tid, planlægning og ressourcer af et ikke uvæsentligt omfang. Visse forpligtelser fordrer endda potentielt inddragelse af leverandører og myndigheder f.eks. i forbindelse med sikkerhedsgodkendelse.

Branchen bemærker, at overholdelse af de nye forpligtelser i bekendtgørelserne kræver en rimelig og realistisk implementeringstid.

Branchen anser det for absolut nødvendigt, at CFCS tilføjer overgangsbestemmelser i bekendtgørelserne, hvorefter udbyderne gives den fornødne tid til implementering af de nye bestemmelser, herunder afdækning af æn-

dringsbehov, planlægning af implementering, implementering, udvikling, inddragelse af leverandører m.v. i fornødent omfang mv.

Implementeringstiderne vil være forskellige afhængigt af kravenes omfang, udbydernes nuværende set-up, brug af underleverandører, netværk, systemer mv., hvorfor branchen skal foreslå, at bekendtgørelserne tilføjes overgangsbestemmelser, der udtrykker den hensigt, som CFCS har udtrykt i høringsbrevet, nemlig at der gives rimelig og realistisk tid til implementering af bekendtgørelsernes forpligtelser på basis af en konkret dialog mellem CFCS og de omfattede udbydere.

Branchen støtter derfor CFCS's løfte om en konkret dialog med udbyderne om implementeringen af bekendtgørelsernes forpligtelser, og et udskudt tilsyn, men skal anmode om, at det formaliseres i bekendtgørelserne.

Branchen kan foreslå følgende ordlyd indsat i ikrafttrædelsesbestemmelserne i bekendtgørelsesudkastene:

*"**§ 38.** Bekendtgørelsen træder i kraft den 1. juli 2016.*
Stk. 2. Udbydernes implementering af bekendtgørelsens forpligtelser tilrettelægges konkret i dialog med Center for Cybersikkerhed, og et egentligt tilsynskoncept implementeres tidligst i 2017 under hensyntagen til en rimelig og realistisk implementering af bekendtgørelsens forpligtelser."

4. Underretning og stand still ved aftaleforhandlinger

Set i forhold til det oprindelige udkast til bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed, som branchen (ved TI) fik i pre-høring, stiller branchen sig positivt til den lempelse som er foretaget i § 5.

Branchen vil stadig understrege, at udgangspunktet om indrapportering og stand-still periode på 10 dage, stadig er meget vidtgående og indgribende, og vil påvirke danske teleselskabers forhandlingsposition.

Det skal også understreges, at forhandling af forskellige aftaler foregår i forskellige dele af virksomheden, og at der ikke nødvendigvis findes noget generelt administrativt overblik over disse processer. En praktisk gennemførelse af denne bestemmelse vil kræve særlige dedikerede ressourcer på området, som igen vil påføre branchen omkostninger.

I og med at afgræsningen af "kritiske netkomponenter, systemer og tjenester" ikke er afgrænset, jf. bemærkningerne ovenfor, er stort set alle komponenter og systemer i udbyderes virksomhed, omfattet, således, at udbyderne skal underrette CFCS om alle aftaleforhandlinger uden hensyn til, om de enkelte forhandlinger vedrører væsentlige dele af udbyderens net og uanset om systemerne konkret har betydning for udbyderens informationssikkerhed.

Branchen skal gentage, at det fremgår af hjemlen til denne bestemmelse (NIS-lovens § 4, stk. 1, nr. 2), at Erhvervsmæssige udbydere af offentligt tilgængelige net og tjenesters alene skal underrette CFCS ved påtænkt indgåelse af aftaler om leverancer, der vedrører <u>væsentlige</u> dele af udbyderens net eller tjenester eller driften heraf.

Branchen understreger, at det manglende væsentlighedskriterium i praksis vil føre til, at forhandlinger om stort set alle systemer og netkomponenter hos de erhvervsmæssige udbydere vil være omfattet af underretningspligten,

og at stort set alle tilhørende aftaler vil skulle forelægges for CFCS, herunder et væsentligt antal aftaler, der ikke kan anses for relevante i lovens forstand. Der til kommer, at eksempelvis en genforhandling af en eksisterende aftale vedrørende pris og varighed vil skulle forelægges CFCS og afvente stand still selvom der ikke er ændret i aftalens ydelsesbeskrivelse og dermed de forhold som eventuelt kunne udgøre et relevant forhold for CFCS at forholde sig til.

Branchen anslår, at §§ 3 og 5 i deres nuværende form vil fordre underretning til CFCS af flere hundrede aftaler årligt fra de væsentlige erhvervsmæssige udbydere i Danmark.

Det er efter vores vurdering ikke åbenlyst, at denne foranstaltning medfører en forbedring af informationssikkerheden, der står mål med den byrde, der pålægges erhvervslivet. Vi forudser også, at dette vil medføre et ikke ubetydeligt ressourcepres på CFCS, hvorfor lang sagsbehandlingstid må forventes.

Branchen foreslår derfor, at begrebet "kritiske netkomponenter, systemer og værktøjer" afgrænses yderligere, således at kun væsentlige dele af udbydernes net og tjenester omfattes af bestemmelsen.

5. Påbud

CFCS tillægges i kapitel 4 i udkast til bekendtgørelse om informationssikkerhed og beredskab i net- og tjenester et bredt katalog af mulige påbud, der kan pålægges udbyderne.

Det fremgår, at CFCS "såfremt det er af væsentlig samfundsmæssig betydning, efter en konkret vurdering" kan påbyde netudbydere at foretage en række foranstaltninger. Vi vil dertil bemærke, at definitionen af 'væsentlig samfundsmæssig betydning' bør konkretiseres nærmere i bekendtgørelsen. Samtidig bør der indføres et krav om, at CFCS i sådanne tilfælde skal begrunde og dokumentere den væsentlige samfundsmæssige betydning af foranstaltningen.

Ud fra et retssikkerhedsmæssigt synspunkt er det afgørende, at der fastlægges kriterier for hvornår CFCS kan tage de enkelte påbudsbestemmelser i anvendelse.

Dette gælder særligt for bestemmelserne i § 26 om bl.a. uafhængig sikkerhedsvurdering (nr. 1), forbud mod supportforbindelser (nr. 2), indstationering af medarbejdere (§ 26 nr. 4) og mulighed for hjemtagning af opgaver (nr. 5).

Branchens bemærkninger til §§ 25 og 26 er kommenteret mere uddybende nedenfor.

6. Specifikke bemærkninger til de enkelte bekendtgørelser

6.1. Bekendtgørelse om informationssikkerhed og beredskab i net og tjenester

Informationssikkerhedsforanstaltninger (§12)
I § 12 bør det uddybes, hvad der menes med logisk og fysisk adgangskontrol.

Auditering (23)
Det er uklart, hvad de konkrete krav til intern auditering, som fremgår af § 23, er.

Påbud (§§25 og 26)
Der er klart behov for at konkretisere/afgrænse, i hvilke tilfælde CFCS kan foretage de nævnte foranstaltninger. Det fremgår ikke tydelig, hvad der ligger i "væsentlig samfundsmæssig betydning", og hvad den konkrete vurdering beror på.

I §26, nr. 1 fremgår, at en netudbyder kan pålægges at gennemføre en "uafhængig sikkerhedsvurdering i forbindelse med leverancer af netkomponenter, systemer og værktøjer fra *en specifik leverandør*, såfremt den pågældende leverandør eller den pågældende leverance ud fra en *generel sikkerhedsmæssig betragtning* eller det *aktuelle trusselsbillede* vurderes at udgøre en særlig sikkerhedsrisiko" (vores fremhævning). Samme referencer til trusselsbilledet og den generelle sikkerhedsmæssige betragtning indgår i §26 nr. 2, som forbyder direkte elektroniske supportforbindelser mellem en leverandør og udbyder.

Disse formuleringer indebærer en mulighed for særregler for specifikke leverandører på et meget generelt grundlag, hvilket fra et retssikkerhedsperspektiv er problematisk. Vi mener derfor, at det bør præciseres i bekendtgørelsen, hvilke sikkerhedsmæssige betragtninger eller hvilke elementer i et trusselsbillede, der kan danne grundlag for anvendelse af en så vidtgående paragraf. Uafhængig sikkerhedsvurdering af potentielt samtlige komponenter, systemer og værktøjer – samt forbud mod direkte supportlinjer - vil medføre en betydelig ekstraudgift for mange leverandører og netudbydere og kan i praksis medføre, at der er produkter og ydelser, der ikke indføres på det danske marked.

Sikkerhedsgodkendelse (§ 26, stk. 1, nr. 3)
Et krav om sikkerhedsgodkendelse vil kunne have den konsekvens, at udenlandske medarbejdere vil være afskåret fra at udføre deres arbejde. Ansættelsesretligt kan man ikke uden videre opsige nogen, fordi de ikke kan opnå en sikkerhedsgodkendelse, hvilket i yderste konsekvens vil kunne medføre, at vi som arbejdsgivere er forpligtet til at have medarbejdere ansat, der ikke kan gennemføre deres arbejdsopgaver. I tillæg vil det også have betydning for innovation, kompetenceudvikling og mulighed for indhentelse af udenlandsk specialkompetence.

Indstationering af medarbejdere hos underleverandører (§ 26, stk. 1, nr. 4)
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. TI 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.

Hjemtagning af outsourcede opgaver (§ 26, stk. 1, nr. 5)
Det fremgår af § 26, stk. 1, nr. 5, i bekendtgørelse om informationssikkerhed og -beredskab i net og tjenester, at CFCS kan påbyde væsentlige erhvervsmæssige udbydere at sikre, at der i tilfælde af misligholdelse af en kontrakt om outsourcing kan ske hjemtagning af opgaver, der er outsourcede til en udenlandsk leverandør. Der kan herunder stilles krav om, at udbyderen skal fastlægge procedurer for hjemtagning af outsourcede områder.

Det bemærkes i den forbindelse, at det er uklart, hvad der skal forstås ved en udenlandsk leverandør, og dette bør i givet fald defineres nærmere.

Hjemtagning er en meget tidskrævende og kompleks opgave, og fastlæggelse af procedurer for dette vil praktisk være nærmest umulig. Sådan som vi ser det, bør det vigtigste være, at mulighed for hjemtagning er en del af aftalen, og også særlig knyttet op på mislighold.

Det er uklart om CFCS som en del af et sådan påbud tiltænkes at kunne påbyde, at en udbyder konkret skal hjemtage en given opgave eller om udbyderen blot at sikre, at en sådan mulighed fremgår af den aftale udbyderen har indgået med 3. part.

Branchen skal bemærke, at der ikke er hjemmel i loven for CFCS til at kunne påbyde hjemtagning af specifikke opgaver, jf. lovbemærkningerne til lovens § 3, stk. 3.

Branchen skal opfordre til, at det præciseres, at CFCS ikke kan udstede påbud om at hjemtage opgaver. Såfremt CFCS alligevel tillægges en sådan kompetence, bør det fremgå, at et sådan påbud kun kan udstedes, når alle andre muligheder er udtømte og kun kan ske, når der foreligger en særlig dokumenteret høj sikkerhedsrisiko.

Sikring af konfiguration (§ 26, stk. 1, nr. 8)
CFCS opfordres til at oplyse, hvad de nærmere angivne konkrete trusler og sårbarheder er, og hvilke nærmere fastsatte internationale standarder eller anbefalinger det er tale om.

Krisestyringsplan (§ 30, stk. 2)
Branchen stiller sig også undrende over rationalet bag bestemmelsen i § 30, stk. 2, da et teleselskab jo altid vil være interesseret i at genetablere net og tjenester. Vi efterspørger derfor mere information omkring både tanken bag ved bestemmelsen, og hvad der tænkes at skulle være proceduren.

6.2. Bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed

Afgivelse af oplysninger om væsentlige dele af udbydernes net og tjenester (§2)
Mange udbydere vil sandsynligvis ikke have tilgang til de oplysninger som § 2, stk. 2 lægger op til, at udbyderne skal fremskaffe,

Udbydernes netværk er som regel bygget op over lang tid, og de oplistede oplysninger er ikke noget det nødvendigvis er mulig at fremskaffe på det detaljeringsniveau, som er foreslået.

Det skal understreges, at såfremt information efter § 2, stk. 4, skal sendes elektronisk, skal denne være krypteret.

Underretning om aftaleforhandlinger (§5)
Se bemærkningerne ovenfor under punkt 4.

Underretningspligt ved brud på informationssikkerheden (§8)
CFCS har lagt op til at underretningspligten bliver væsentlig udvidet i forhold til den gældende regulering.

Branchen har noteret sig, at CFCS ikke i væsentlig grad har forholdt sig til branchens (ved TI) bemærkninger til grænseværdierne for indberetning ved brud på informationssikkerheden. Branchen er ikke enig i, at den foreslåede afgrænsning i § 8 er nødvendig for at tilnærme sig ENISA's tekniske guidelines. Det fremgår i øvrigt, at overgangen til de nævnte grænseværdier sker ud fra ønsket om at forpligtelserne er overskuelige. Det er branchens opfattelse at de nuværende regler er overskuelige, og i givet fald CFCS ikke er enig heri, skal branchen oplyse, at udbyderne hellere vil bevare det nuværende regime henset til, at det er mindre byrdefyldt for selskaberne.

Branchen finder ikke, at en sådan udvidelse synes begrundet i noget sagligt. Det følger heller ikke af loven eller dens lovbemærkninger, at underretningspligten skal udvides.

Branchen er opmærksom på, at underretningspligten er en implementering af EU's Rammedirektiv artikel 13a, stk. 3, men den allerede gældende ordning lever fuldt ud op til de europæiske anbefalinger på området.

I forhold til gældende krav om indberetning af brud på informationssikkerhed har CFCS udgivet en vejledning, der tager udgangspunkt i ENISA's anbefaling. Branchen anbefaler, at det er denne model, der videreføres da den både tager hensyn til de enkelte teleselskabers størrelse samt geografiske forhold.

Det er branchens vurdering, at konsekvensen af den nuværende formulering i bekendtgørelsen vil være, at antallet af straks-rapporteringer mindst vil blive fordoblet.

Såfremt CFCS alligevel vil fastholde, at der skal indføres nye græseværdier for underretning, skal branchen opfordre til at begrebet "brud på informationssikkerheden" nærmere defineres.

Det formodes i øvrigt, at grænseværdierne i § 8 stk. 2 og 4 er behæftet med en fejl i udregningen af brugertimer. CFCS skriver i e-mail af 4. april 2016 følgende:

"Formålet med bestemmelsen er at videreføre implementeringen af direktivkravene og dermed fastsætte grænseværdier, der ligger tæt op ad de grænseværdier, der følger af ENISA's tekniske guidelines. Samtidig er det vigtigt for os, at forpligtigelsen er overskuelig. Det bemærkes i den forbindelse, at grænseværdierne er beregnet med henblik på, at der skal ske underretning ved brud, der berører mere end 1 % af brugerne af en given tjeneste i mere end otte timer."

Dette betyder at hvis der er ca. 6 til 7 millioner mobilabonnementer vil regnestykket se således ud:

(1% af 6.000.000) = 60.000 * 8 timer = 480.000 brugertimer

Branchen skal med henvisning til TI's høringsvar i pre-høringen opfordre til at grænseværdierne tilrettes. Hvis grænseværdierne ikke rettes, bør CFCS nærmere redegøre for og begrunde, hvorfor man fraviger den 1% grænse, som CFCS tidligere har oplyst at ville anvende.

Branchen finder det i øvrigt uklart, hvad der menes med "øvrige tjenester" i stk. 4, nr. 5, som ikke er omfattet af stk. 4, nr. 1-4, idet tjenesterne i nr. 1-4 omfatter de elektroniske kommunikationstjenester, der anvendes i elektroniske kommunikationsnet. CFCS bedes redegøre for dette.

6.3 Bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.

Prioriteret afgang til fastnet (§2)
Der behov for en afklaring af, hvorvidt offentligt tilgængelige taletelefonitjenester i fastnet også dækker IP-telefoni over fastnettet (VOIP).

Branchen er ikke bekendt med, at der er selskaber, der leverer VoIP, der har en funktionalitet i deres VoIP-platform, som giver særlig adgang til prioritet. Den type af prioritet, der er beskrevet i udkastet til bekendtgørelser, er knyttet til TDC's PSTN-platform, som TDC planlægger at nedlægge i løbet af ganske få år.

Teknologisk set er funktionen indført for at løse de specifikke problemer i PSTN-teknologien, som optræder ved ekstrem høj tilbudt trafik. Dvs. adgang til klartonen og kredsløbskapacitet, som er en reel knap ressource i PSTN. Situationen er anderledes i VoIP, hvor trafikken fremføres igennem IP-nettet. Her udgør taletrafikken – selv ved ekstrem trafikbelastning – kun en mindre del af den samlede IP-kapacitet. Ydermere fremføres VoIP med prioritet (Expedited Forwarding) frem for andre trafikarter, så i den forstand kan man sige, at problemet ikke er aktuelt i VoIP.

Der til kommer, at konkurrencesituationen på markedet for fastnettelefoni, har medført, at der i dag er en lang række af udbydere af IP-telefoni, der har implementeret med forskellige tekniske løsninger. Eventuel regulering af prioritering af IP-telefoni egner sig derfor bedst til regulering via brancheaftaler.

TI skal opfordre til, at kravet om prioritet for fastnettelefoni afgrænses til PSNT-tjenesten og eventuelle ordninger med prioritet for IP-telefoni overlades til brancheaftaler, hvis det efter en nærmere analyse viser sig nødvendig med en særlig ordning for IP-telefoni

Sikkerhedsbeskyttelse af kredsløbsoplysninger (§16)
I udkastet til bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i bredskabssituationer indeholder i § 16 en udvidet forpligtelse til at klassificere udbyderens registre, der indeholder oplysninger om faste kredsløb til beredskabsmæssige formål, i overensstemmelse med Justitsministeriets cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret).

Efter de gældende regler har udbyderne alene været forpligtet til holde fortroligt at en givent kredsløb blev anvendt til bredskabsformål. Det bemærkes, at kredsløb der anvendes til bredskabsforhold anlægges, drives og leveres ved brug af samme netværk og systemer som anvendes til udbydernes øvrige net og tjenester. Udbyderne hidtil kunne opfylde fortrolighedsforpligtelsen ved at sløre anvendelsesformålet for et givent kredsløb, og der har ikke været noget specifikt krav om, at driftsstøttesystemerne eller systemer der indeholder oplysninger om netværk og designinformation af de dele af netværket der anvendes til sikkerhedskredsløb, som helhed er klarificeret.

Det skal bemærkes, at design og netværksbeskrivelser af et hvert kredsløb i udbydernes net indgår som en integreret del af udbydernes netværkssystemer og der anvende sikke særlige systemer til produktion af sikkerhedskredsløb. Det vil derfor i praksis betyde, at udbydernes netværkssystemer som helhed risikere at skulle opfylde kravene til sikkerhedsgodkendelse.

Branchen opfordrer derfor til, at det præciseres, at det alene er de registre, der identificere en givent kredsløb som et kredsløb til brug for bredskabs-formål, der skal klassificeres.

Øvrige foranstaltninger (§17)
Som en generel kommentar til § 17 vil vi påpege, at et teleselskab normalt altid være interesseret i at genetablere net og tjenester, og at vi derfor ikke forstår rationalet bag denne bestemmelse.

Med venlig hilsen

Mette Lundberg
Direktør, politik og kommunikation
IT-Branchen

Peder Søgaard-Pedersen
Fagleder
DI Digital

Jakob Willer
Direktør
Teleindustrien

Juridisk Sektion

Fra:	Birgitte Uhrhammer <biuh@tv2.dk>
Sendt:	18. maj 2016 10:29
Til:	Juridisk Sektion; Stine Busch Østergren
Cc:	Tom Taul Bjerre; Steen Hyrlov; Magnus Rask Detlif; Sebastian Rosenkjær; Ole Søgaard Berthou; Morten Stagaard
Emne:	SAG-2016-00262 - Høring over 4 bekendtgørelser om net- og informationssikkerhed

Center for Cybersikkerhed har den 29. april 2016 sendt fire bekendtgørelser om net- og informationssikkerhed i høring.

TV 2 DANMARK A/S (herefter TV 2) har følgende bemærkninger til de fremsendte udkast:

Det er overordnet særdeles vanskeligt for TV 2 at konstatere, hvorvidt TV 2 er omfattet af bekendtgørelserne. Således falder TV 2 ikke umiddelbart ind under definitionen af "væsentlige erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester", som er angivet i tre af de fire bekendtgørelser, idet definitionen omtaler "Udbydere af net". TV 2 er ikke udbyder af net, idet TV 2 (og DR) i 2010 solgte sendenettet til Teracom AB.

Det vil være ønskeligt, om definitionerne i bekendtgørelserne tydeligere kunne præcisere de leverancer, som er omfattet, f.eks. om der i forbindelse med "net" er er tale om ejerskab af fysiske netværk som anvendes til transport af indhold for 3. part, og om der i forbindelse med "tjenester" kun er tale om tjenester med det formål at give en 3. part adgang til at anvende transportnettet.

For det tilfælde, at TV 2 måtte være omfattet bekendtgørelserne, skal fremføres følgende, yderligere bemærkninger:

Bekendtgørelserne implementerer i praksis væsentlige dele af ISO 27001/2, hvilket påfører de virksomheder og organisationer, der er omfattet af bekendtgørelserne en betydelig administrativ byrde. Typisk implementeres sådanne forpligtelser successivt over en længere periode. I dette tilfælde er fristen for implementering af bekendtgørelserne meget kort. Det vurderes således som yderst vanskeligt at leve op til forpligtelserne, hvis bekendtgørelserne skal træde i kraft 1. juli 2016.

Endvidere vil en forceret implementering vil være forbundet med meromkostninger og må påregnes at belaste de forpligtede virksomheder og organisationers generelle aktiviteter mærkbart i implementeringsperioden.

TV 2 foreslår derfor, at der indføres en implementeringsperiode af passende længde, som giver de omfattede virksomheder og organisationer mulighed for, at leve op til bestemmelserne.

Med venlig hilsen

MORTEN STAGAARD
Advokat (L)
TV 2 Jura

M +45 20243706, T +45 65211404
staq@tv2.dk

TV 2 DANMARK A/S
Rugaardsvej 25, DK-5100 Odense
Teglholm Allé 16, DK-2450 København SV
www.tv2.dk