Tak for henvendelsen.

Advokatrådet har besluttet ikke at afgive høringssvar.

Med venlig hilsen

ADVOKATSAMFUNDET
RETSSIKKERHED · UAFHÆNGIGHED · INTEGRITET

Henriette Fagerberg Erichsen
Sekretær

Kære Natasha Maj Christoffersen,

Mange tak for tilsendte materiale vedr. høringssvar 2020/004886.
Efter gennemlæsning af tilsendte materiale, har Borch Teknik A/S ikke yderligere kommenaterer eller bemærkninger.

Venlig hilsen / Best regards

Klaus Aare Bang
CEO
Borch Teknik A/S
kab@borchteknik.dk
+45 25 23 38 97

DATATILSYNET

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt til: fmn@fmn.dk
Cc: nmc@fmn.dk **og** nls@fmn.dk

25. august 2020

J.nr. 2020-11-0439
Dok.nr. 248593
Sagsbehandler
Sara Thorning Hansen

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Udkast til forslag til lov om ændring af lov om net og informationssikkerhed (Implementering af direktivet om oprettelse af europæisk kodeks for elektronisk kommunikation for så vidt angår sikkerhed i net og tjenester)

Ved brev af 30. juli 2020 har Forsvarsministeriet anmodet om Datatilsynets eventuelle bemærkninger til ovennævnte udkast.

Udkastet giver umiddelbart ikke Datatilsynet anledning til bemærkninger, idet det dog forudsættes, at enhver eventuel behandling af personoplysninger foranlediget af udkastet sker under iagttagelse af reglerne i databeskyttelsesforordningen og databeskyttelsesloven.

Med venlig hilsen

Sara Hansen

Til:
Forsvarsministeriet
fmn@fmn.dk med kopi til
nmc@fmn.dk,nls@fmn.dk,
nbb@fmn.dk , eba@fmn.dk

Den 27. august 2020
MOKR

Referencer: 2020/004886 og 2020/005122

Høringssvar vedr. informationssikkerhed i teleloven

1. Generelle bemærkninger

DI takker for muligheden for at afgive høringssvar til høringerne om:

- Mobilvarselssystemet
- Øvrige ændringer i teleloven for så vidt informationssikkerhed.

Dette høringssvar besvarer begge høringer.

Det skal nævnes generelt, at DI støtter en direktiv-nær implementering, hvor man forsøger at komme tættest muligt på kravene i de andre EU-lande. Udstyr, rutiner, kompetencer og processer bliver i høj grad standardiserede på europæisk/internationalt plan både for leverandører og operatører og derfor giver det ikke mening, at man skal møde 27 forskellige tolkninger i medlemslandene. DI noterer sig og støtter, at dette princip er indskrevet i de almindelige bemærkninger. Der er dog tvivl om, hvorvidt dette også praktiseres i de enkelte formuleringer.

Således er der flere bestemmelser med meget brede hjemler til senere at fastlægge krav i bekendtgørelser. Hvis ikke myndighederne er parat til i loven at formulere kravene præcist allerede nu, ønsker branchen som minimum en afgrænsning af hjemlerne, så alle kan se hvilke grænser, der gælder for de kommende bekendtgørelser.

Videre bør der indføres som princip, at man lægger sig op af standarder og definitioner, der er etablereret på internationalt niveau. Det fremgår af direktivets art 40, at procedurer og standarder skal lægge sig op af internationale standarder.

Endelig kan DI konstatere, at der hersker en betydelig uklarhed på markedet om, hvilke sikkerhedsretningslinjer teleselskaberne skal forholde sig til i forbindelse med investeringer i nye net. DI skal derfor understrege behovet for, at der fra regeringens side sikres klarhed om reglerne og ikke mindst udmeldingerne på området.

2. Konkrete bemærkninger

§3 stk.1

Jf. ovenfor bør der være en henvisning til, at minimumskrav i videst mulige omfang skal basere sig på internationale standarder. Herved vil implementeringen også være mere direktivnær. Samtidig bør den brede hjemmel afgrænses, så det fremgår, at der vil blive taget højde for at indgrebet skal være mindst muligt indgribende.

§ 3, stk. 3

CFCS giver i dette stykke sig selv et meget bredt mandat til at stille krav om, at udbydere skal træffe konkrete foranstaltninger. Det er i sig selv et stort indgreb i virksomhedernes ret til selv at imødegå trusler, og dertil kan krav fra CFCS være omkostningstunge og indgribende. Jf. overfor er dette et oplagt eksempel på, hvor man i hjemmelsbestemmelsen til en kommende bekendtgørelse enten bliver meget mere klar på, hvad man vil stille af materielle krav, og hvor vidtgående disse kan være, eller at man alternativt afgrænser mandatet. Det kan være i form af, at CFCS skal tage vidtgående hensyn til proportionalitetsprincippet og således stille krav om mindst mulige indgribende foranstaltninger for at imødegå en konkret trussel eller lignende.

Mobilvarslingssystemet

DI vurderer, at et nyt mobilvarslingssystem kan bidrage med ekstra sikkerhed og en bedre håndtering af kriser og ulykker og således er et fornuftigt initiativ. Samtidig foreslås det i lovforslaget, at staten afholder omkostningerne ved systemet. Det støtter DI, alt den stund, at teleudbyderne ikke har nogen kommerciel nytte af varslingssystemet – det tjener alene et samfundsformål.

Når det kommercielt licenserede mobilnet anvendes i katastrofesituationer og til beredskabskommunikation, bør netværksoperatøren ikke kunne gøres ansvarlig for følgerne af eventuelt svigtende kritisk kommunikation, idet tabene i en krisesituation kan være uforholdsmæssigt store.

DI stiller sig naturligvis til rådighed for at uddybe ovenstående.

Med venlig hilsen

Morten Kristiansen, Chefkonsulent, DI

Forsvarsministeriet
Holmens Kanal 9
1060 Copenhagen C
Denmark

Sendt til: fmn@fmn.dk og kopi til nmc@fmn.dk og nls@fmn.dk
Reference nummer: 2020/004886

27. august 2020

HØRINGSSVAR PÅ OFFENTLIG HØRING VEDRØRENDE UDKAST TIL FORSLAG TIL LOV OM ÆNDRING AF LOV OM NET OG INFORMATIONSSIKKERHED (IMPLEMENTERING AF DIREKTIVET OM OPRETTELSE AF EN EUROPÆISK KODEKS FOR ELEKTRONISK KOMMUNIKATION FOR SÅ VIDT ANGÅR SIKKERHED I NET OG TJENESTER)

Den 30. juli 2020 opfordrede det danske Forsvarsministerium (”**Ministeriet**”) til at indsende høringssvar til offentlig høring om lov nr. 1567 af 2015 om ændring af lov om net og informationssikkerhed (”**Lovudkastet**”), hvilket består i en delvis implementering af Direktivet om oprettelse af en Europæisk Kodeks for Elektronisk Kommunikation navnlig hvad angår sikkerhed i net og tjenester (”EECC” eller ”Direktivet”)

Huawei fremsætter hermed sine bemærkninger til Lovudkastet.

Implementering af lovgivning ved bekendtgørelse

Ministeriet anfører, at implementeringen er af ”teknisk karakter” i form af direkte implementering af konkrete bestemmelser i EECC. Der er dog også flere steder mandat til CFCS til at uddybe reguleringen yderligere. Huawei anser det på den baggrund for relevant at fremhæve, at væsentlige lovgivningsmæssige indgreb ikke bør implementeres ved sekundær lovgivning i form af bekendtgørelser. Dette er tilfældet, da bekendtgørelser ikke er underlagt den samme parlamentariske proces om behandling af lovforslag i Folketinget med tilhørende offentlig høring som er tilfældet for en lov. Lovgivning via bekendtgørelser udgør derudover en udfordring for den generelle regulatoriske transparens og gennemskuelighed, da det simpelthen er svært at overskue reguleringen i en samling af sideordnede og delvist overlappende bekendtgørelser, der er forankret i generelle mandater i den overordnede lovgivning.

Huawei følger nøje implementeringen af EECC i hele EU og kan konstatere, at størstedelen af medlemsstaterne da også har valgt at implementere Direktivet direkte ved lov.

Huawei anser introduktion af ny lovgivning som en mulighed for at øge kvaliteten og forudsigeligheden i lovgivningen og er positivt indstillet over den nye lovgivning. På denne baggrund opfordrer Huawei til, at Ministeriet afstår fra at indføre materielle regulatoriske krav i bekendtgørelser fremfor regulering ved lov og i øvrigt gennemfører implementeringen af EECC så tekstnært som muligt.

Artikel 40 (1) i EECC foreskriver, at en medlemsstat skal træffe: *”[..]passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for på passende vis at styre risiciene for sikkerheden i net og tjenester.”* Artikel 40 (5) i EECC uddyber henvisningen til tekniske og organisatoriske foranstaltninger ved at specificere, at udgangspunktet for

sådanne foranstaltninger *"[..]i videst muligt omfang baseres på europæiske og internationale standarder"*

Det er Huaweis mål at 5G netværket i Danmark og EU udstyres med den nyeste sikkerheds- og cyber modstandsdygtighed. Huawei er samtidig overbevist om, at eventuelle risici adresseres bedst muligt ved at fastsætte kriterier som er målbare og verificerbare.

Huawei opfordrer derfor Ministeriet til at tage europæiske og internationale standarder for sikkerhed i 5G i betragtning i sin udformning af lovgivningen. På den baggrund bør Ministeriet sikre, at lovgivningen indeholder specifikke henvisninger til standarder, såsom NESAS (Network Equipment Security Assurance Scheme) og (Security Assurance Specifications), navnlig på grund af deres uafhængige revisioner og evalueringer. Anvendelse af de generelle sikkerhedsstandarder sikrer stabile rammer for en ensartet og skræddersyet tilgang til sikkerhedsrevisioner. Samtidig afkræver strenge sikkerhedsstandarder et højt niveau af engagement fra operatører og leverandører.

ENISAs Technical Guideline on Security Measures under the EECC[1] anfører følgende anbefaling: *"Competent authorities should take into account that some (especially the large) providers may operate in several EU countries, and that it would be cumbersome for these providers to adopt different standards in different countries. In this respect it could be useful to allow providers to use international standards which are widely used across the EU and in this way reduce compliance costs for these providers."*

Den generelle anvendelighed af NESAS ses ved, at flere globale leverandører nu er certificeret af uafhængige sikkerhedsrevisorer under NESAS. Huawei ser dette som et tydeligt udtryk for, at markedet generelt opfatter NESAS som en integreret del af fremtidens sikkerhedspolitik for leverandørhåndtering.

I den forbindelse vil Huawei henlede Ministeriets opmærksomhed på, at trusselsbilledet er i konstant forandring, og at en etablering af eller henvisning til "god skik" eller "internationale standarder eller krav", vil hjælpe leverandører med at overholde kravet om at kunne identificere "betydelige trusler". Udkastet til de seneste ENISA Technical Guideline on Security Measures under the EECC opfordrer ligeledes til brugen af en god skik-standard i identificeringen af trusler: *"[..] Competent authorities should take into account that best practices in network and information security are rapidly changing, because information technology changes rapidly and because the capability of attackers changes rapidly."*[2]

Konkrete bemærkninger

Retssikkerhed og forudsigelighed i lovgivningen

Lovudkastet indfører en ny bestemmelse i § 3, stk. 3 der lyder som følger:

> *Stk. 3. Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester at træffe konkrete foranstaltninger, der er nødvendige for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, når en betydelig trussel er identificeret.* ***Centeret fastsætter nærmere regler herom****"[vores fremhævelse]*

Forarbejderne beskriver, at den nye § 3, stk. 3 tilføjes for at implementere EECC artikel 41 (1). Med henblik på at fremme retssikkerhed og forudsigelighed i lovgivningen opfordrer Huawei Ministeriet til yderligere at afgrænse og kvalificere CFCS's mandat.

[1] Version 2.2, 08 juli 2020, s. 31 linje 670-674

[2] Version 2.2, 08 juli 2020, s. 31 linje 681-683

For at opnå dette, anbefaler Huawei, at det defineres klart i Lovudkastet og dets forarbejder hvad en "betydelig trussel" indebærer, og, at der gives en mere detaljeret redegørelse for, hvilke "konkrete foranstaltninger" lovgiver forestiller sig.

Der bør som minimum fastsættes en tærskel for, hvornår en trussel kan kvalificeres som "betydelig", inden den resulterer i et påbud fra CFCS.

I den forbindelse mener Huawei, at det er relevant at understrege hovedformålene i EECC om; at fremme forudsigeligheden i tilsynet med teleoperatører samt at fremme konkurrence og tilskynde investeringer[3]. I EECC anføres det til dette formål, at: *"Der bør tilskyndes til både reelle investeringer og konkurrence, som går hånd i hånd, således at økonomisk vækst, innovation og forbrugernes valgmuligheder øges.[4]"* samt, at de nationale myndigheder – for at forfølge disse mål bør *"[..]fremme forudsigelighed i reguleringen ved at sikre en ensartet tilsynspraksis[..][5]"*

Huawei opfordrer til, at lovgivningen rammer den rette balance mellem rimelige 5G udrulningspriser og sund konkurrence på markedet og samtidig fremmer investeringer samt langsigtet innovation for at opnå målene i EECC. Den danske implementering bør inddrage hensynene bag EECC, artikel 41 (5). Huawei foreslår derfor, at følgende tilføjes til den nye § 3, stk. 3:

> *Stk. 3. Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester at træffe konkrete foranstaltninger, der er nødvendige for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, når en betydelig trussel er identificeret. [**I relevant omfang skal der træffes foranstaltninger, herunder kryptering, for at forhindre og begrænse sikkerhedshændelsers påvirkning af slutbrugere samt andre elektroniske kommunikationsnetværk -og tjenester, herunder nummer uafhængige interpersonelle kommunikationstjenester. De specifikke foranstaltninger bør i videst muligt omfang være baseret på europæiske og internationale standarder] Centeret fastsætter nærmere regler og anbefalinger herom baseret på god skik**"[vores fremhævelse]*

Tidsperspektiv for udstedelsen af bekendtgørelser

Huawei bemærker, at medlemsstaterne har indtil den 21. december 2020 til at implementere EECC, jf. Direktivets artikel 104 (1).

I den forbindelse ønsker Huawei at understrege, at retssikkerhed og transparens i lovgivningen er afgørende, ikke alene for Huawei, men for branchen som helhed. I den henseende udgør den forholdsvis åbne henvisning til CFCS videre regulering en usikkerhed, der ikke stemmer overens med de overordnede hensyn.

Huawei opfordrer derfor endvidere Ministeriet til at sikre, at relaterede bekendtgørelser udstedes hurtigst muligt og senest den 21. december 2020.

Overordnet vil Huawei opfordre Ministeriet til at, afklare hvordan sådanne nærmere regler vil blive fastlagt; i) ved udstedelsen af en ny bekendtgørelse som føjer til de eksisterende

3 Jf.. Artikel 3 (2) EECC
4 Jf. Artikel 3 (4) (a) EECC
5 Jf. Article 3 (4) (a) EECC

bekendtgørelser (Bekendtgørelse nr. 567 eller Bekendtgørelse nr. 1256), ii) ved at introducere nye bekendtgørelser til fuld erstatning af de nævnte eksisterende bekendtgørelser, eller iii) ved administrativ afgørelse.

Huawei har tillid til, at nye bekendtgørelser vil være genstand for offentlig høring og vil sætte pris på muligheden for at give sit besyv med ved et høringssvar i den anledning.

Derudover opfordrer Huawei til, at der gives klar mulighed for at påklage CFCS's afgørelser under de nye regler til en højere instans, samt at der generelt sikres transparens i CFCS' afgørelser.

***

Huawei står til rådighed for Ministeriets for spørgsmål eller kommentarer.

Med venlig hilsen,

JiangLichao
Adm. Direktør
Huawei Technologies Denmark Aps

INSTITUT FOR
MENNESKE
RETTIGHEDER

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

Forsvarsministeriet
Holmens Kanal 42
1060 København K
Danmark

fmn@fmn.dk
kopi til nmc@fmn.dk og nls@fmn.dk

DOK. NR. 20/01891-2

11. AUGUST 2020

HØRINGSSVAR VEDR. IMPLEMENTERING AF DIREKTIVET OM OPRETTELSE AF EN EUROPÆISK KODEKS FOR ELEKTRONISK KOMMUNIKATION FOR SÅ VIDT ANGÅR SIKKERHED I NET OG TJENESTER

Forsvarsministeriet har ved e-mail af 30. juli 2020 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til et udkast til forslag til lov om ændring af lov om net- og informationssikkerhed (Implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation for så vidt angår sikkerhed i net og tjenester)

Instituttet har ingen bemærkninger.

Der henvises til Forsvarsministeriets sagsnummer 2020/004886.

Med venlig hilsen

Lise Garkier Hendriksen
CHEFKONSULENT

Københavns Byret

Præsidenten
Domhuset, Nytorv 25
1450 København K.
Tlf. 99 68 70 15
CVR 21 65 95 09
administration.kbh@domstol.dk
J.nr. 9099.2020.37

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Den 3. august 2020

Ved en mail af 30. juli 2020 har Forsvarsministeriet anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om ændring af lov om net- og informationssikkerhed (Implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation for så vidt angår sikkerhed i net og tjenester).

Jeg skal i den anledning på vegne af byretspræsidenternes oplyse, at byretterne ikke ønsker at udtale sig om udkastet.

Der henvises til Deres j.nr. 2020-004886.

Med venlig hilsen

Søren Axelsen

Vestre Landsret
Præsidenten

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt pr. mail til fmn@fmn.dk og nmc@fmn.dk og nls@fmn.dk

J.nr. 40A-VL-50-20
Den 03/08-2020

Forsvarsministeriet har ved brev af 30. juli 2020 (sagsnr. 2020/004886) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om ændring af lov om net- og informationssikkerhed (Implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation for så vidt angår sikkerhed i net og tjenester).

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

Med venlig hilsen

Helle Bertung

Østre Landsret
Præsidenten

Den 07-08-20
J.nr. 40A-ØL-51-20
Init: sdy

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt pr. mail til fmn@fmn.dk, nmc@fmn.dk og nls@fmn.dk

Forsvarsministeriet har ved brev af 30. juli 2020 (Sagsnr. 2020/004886) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om ændring af lov om net- og informationssikkerhed (Implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation for så vidt angår sikkerhed i net og tjenester).

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

Med venlig hilsen

Bent Carlsen

Ellen Basse Porsbo

Regionshuset
Viborg

Regionssekretariatet
Skottenborg 26
Postboks 21
DK-8800 Viborg
Tel. +45 7841 0000
kontakt@rm.dk
www.rm.dk

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Høringssvar fra Region Sjælland, Region Syddanmark og Region Nordjylland vedr. udkast til forslag til lov om ændring af lov om net- og informationssikkerhed

Dato 27-08-2020
Sagsbehandler Malene Nyman
malene.nyman@stab.rm.dk
Tel. Sagsnr. 1-16-4-1-20

Region Sjælland
Region Sjælland bakker helt generelt op om nationale initiativer, der bidrager til at styrke samfundets – og dermed regionernes – muligheder for at imødegå cyberangreb mod kommunikationsnet- og tjenester og ønsker naturligvis at bidrage til denne udvikling og samarbejdet herom.

Region Sjælland er dog stærkt bekymret for, om lovforslaget er for indgribende og giver Center for Cybersikkerhed (CFCS) hjemmel til beføjelser og mandater, der i sidste ende kan føre til indgriben i regionernes selvstændige myndighedsudøvelse samt registrerede og borgernes rettigheder. Det er Region Sjællands opfattelse, at CFCS med lovforslaget vil få mulighed for, ved identifikation af en betydelig trussel, at prioritere handlinger i regionernes it-infrastruktur uden involvering af regionale prioriteringer, kompetencer og indsigt.
Set i et regionalt perspektiv er det problematisk, hvis udformningen af lovforslaget giver hjemmel til, at cybersikkerhed centralt fra kan prioriteres over patientsikkerheden, da regionens telemedicinske løsninger vil være omfattet af loven. Derudover er Region Sjælland bekymret for, at det ikke af lovforslaget er klart, hvilke konsekvenser et påbud om "at træffe konkrete foranstaltninger, der er nødvendige for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme", jf. lovens § 3, stk. vil medføre, fx i relation til tilgængelighed, ydeevne og økonomiske omkostninger forbundet herved.

Region Sjælland finder det bekymrende, at der i loven lægges op til, at et påbud skal ske uden retskendelse. Region Sjælland savner derudover en nærmere afklaring af hjemlen for påbuddet, herunder en præcisering af "en betydelig trussel". Videre er der behov for at

præcisere, hvorledes et påbud tænkes ophævet, når trusselsbilledet ændrer sig.

Region Syddanmark
Målgruppe
Den, der med et kommercielt formål stiller produkter, elektroniske kommunikationsnet eller -tjenester til rådighed for andre. Begrebet omfatter ikke udbydere af NUIK-tjenester.

NUIK
Der ændres en række formuleringer, bl.a. for at implementere EU-forordningen vedrørende sikkerhed i net og tjenester.

Der er i alle tilfælde, hvor der er henvisning til udbydere tilføjet en ny type udbydere (NUIK), og de defineres således:
Udbyder af NUIK-tjeneste: Udbyder af en nummeruafhængig interpersonel kommunikationstjeneste i form af en tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer, hvem modtageren eller modtagerne skal være. Omfattet er ikke tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste. Tjenesten etablerer ikke forbindelse til offentligt tildelte nummerressourcer, dvs. et eller flere numre i nationale eller internationale nummerplaner, eller muliggør ikke kommunikation med et eller flere numre i nationale eller internationale nummerplaner.

Det må være nye services, der udbydes af en ny type udbydere, og denne type udbydere har ikke ansvar for eller kan påvirke stabiliteten eller opbygningen af de eksisterende udbyderes tjenester.

Det kunne være virksomheder, der sælger ydelser, der understøtter Tetra (SINE), IoT, LoRaWan eller tillægsydelser, som skal bruge allerede eksisterende netværk, der udbydes af andre udbydere.
Det er os ikke helt klart, hvilke udbydere der er tænkt på, ej heller typen af kommunikationsform og type, der er tænkt på. Det er ej heller nævnt, i hvilke situationer NUIK benyttes. Der er stor forskel på kravene til NUIK udbyderne, hvis det er SINE kommunikation eller i stedet ikke kritiskkommunikation ydelse, der udbydes.

Autenticitet
Der introduceres endvidere autenticitet som en parameter for netværksydelser:
Loven anvender således i dag begrebet informationssikkerhed, hvilket forstås som sikring af tilgængelighed, fortrolighed og integritet i net og tjenester. Med definitionen af sikkerhed i net og tjenester udvides

sikkerhedsområdet til – ud over tilgængelighed, fortrolighed og integritet – også at omfatte autenticitet. Der henvises herom til bemærkningerne til lovforslagets § 1, nr. 4.

Udbydernes ansvar har tidligere været at sikre at der skal være forsvarsmekanismer, der skal kunne forhindre tab af tilgængelighed, integritet og fortrolighed for den kommunikation der "flyder" i nettene. Der er tale om en ny definition af "sikkerhed i net og tjenester", der skal implementere artikel 2 i EU's telekodeks. Det kunne være en udvidelse af begrebet, der er tilsagt af EU's implementering af NSIS standarden.
Der kunne være god mening i, at teleudbydere skal understøtte standarden og stille infrastruktur til rådighed, der generelt på nettet kan verificere brugeres autenticitet. Det vil dog være en meget stor ændring i forhold til, hvordan Internettet fungerer i dag, idet der vil være store krav til håndtering af privatlivets fred of fortrolighed – herunder fortrolighed i henhold til brevhemmeligheden.

Beredskab
Der står i forslaget, at mobilnettet skal kunne bruges til beredskabsmeldinger. Det kan det ikke i dag, både pga. at tjenesten ikke er til rådighed, men også at der ikke er tilstrækkelig resiliens og klassifikation for mobilnettet til at kunne understøtte situationer, hvor beredskabsmeldinger er nødvendige. Ønsket om, at denne ydelse skal kunne varetages af mobilnettet, er en følge af, at det gamle system med sirener ikke dækker hele landet, og det er sikkert heller ikke tidssvarende, og der er ikke planer om at udbygge det eksisterende system.

Udbygning af redundans og resiliens samt udvikling af en digital varslingstjeneste, hvor mobilnettet udgør kernen, udgør en ikke ubetydelig udgift, idet mobilnettet ikke er designet til at kunne understøtte beredskabssituationer. De eneste radiomaster, der er klassificerede til dette, er Cibicoms master der benyttes til at udsende tv og radio signaler samt bl.a. 450MHz digital netværk via firmaet Net1.

Herom skrives der i forslaget:
Den foreslåede bestemmelse i § 5 a har til formål at sikre, at mobiloperatørerne træffer alle nødvendige foranstaltninger for at undgå, at udstyr og systemer, der anvendes i forbindelse med transmission af offentlige advarsler, afbrydes. Mobiloperatørerne vil i forlængelse af eksisterende forpligtelser til at sikre en robust teleinfrastruktur i medfør af lovens § 3, stk. 1, og § 5, stk. 1, skulle planlægge og sørge for opretholdelsen af uafbrudt transmission af offentlige advarsler, herunder i relation til udstyr og systemer, der anvendes til transmission af offentlige advarsler, bl.a. tage stilling til

fremskaffelse af det nødvendige reserveudstyr, og sikring af redundans og nødstrømsforsyning.

Der er derfor tale om en kvalitetsmæssig opgradering, der understøtter den eksisterende praksis, hvor mobilnettet i dag bruges til alle former for kommunikation, både af borgere og af redningspersonel i bl.a. ambulancer. Det er kun få regioner, der ikke bruger data services fra det generelle mobilnet. I tilfælde af bortfald af de generelle kablede telefonitjenester, er Region Syddanmarks kontrolcentral (AMK) afhængig af en backup procedure, der er benytter mobilnettet fra flere udbydere.

At varsling skal funderes på en højteknologisk løsning, gør os som land sårbare idet, der ved et sammenfald af sikkerhedshændelser, kan være risiko for at teknikken går ned, og at varsling via mobilnettet ikke får den ønskede udbredelse. Det vil give rigtig god mening at foretage et teknologisk tilbagespring, der gør at vi i disse situationer ikke bliver afhængig af smartphones og app-teknologi, som ikke har en stabilitet og kvalitet der tilsiger det kan bruges når det virkelig gælder.

CFCS
Kan i beredskabssituationer påbyde udbydere at foretage nærmere angivne sikkerhedsforanstaltninger:
… kan Center for Cybersikkerhed i beredskabssituationer og i andre ekstraordinære situationer påbyde erhvervsmæssige udbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger i tilfælde af en hændelse eller en trussel, der i betydeligt omfang påvirker eller kan påvirke udbuddet af net eller tjenester negativt.
samt:
Det fremgår af den gældende § 3, stk. 1, at Center for Cybersikkerhed fastsætter regler om minimumskrav til informationssikkerhed for udbydere af offentligt tilgængelige net og tjenester. Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til informationssikkerhed i net og tjenester og opretholdelse af et passende informationssikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankre-de processer.

Bestemmelsen implementerer i dag rammedirektivets artikel 13 a, stk. 1 og 2.

Det følger af den foreslåede nyaffattelse af § 3, stk. 1, at Center for Cybersikkerhed fastsætter regler om minimumskrav til sikkerhed i net og tjenester for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester.

Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til sikkerhed i net og tjenester og opretholdelse af et passende sikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Region Nordjylland

Fra Region Nordjyllands side hilser vi enhver passende tilpasning af lovgivningen velkommen. Imidlertid finder vi, at det udsendte udkast skaber mere forvirring om omfattelsesniveauet end gavnligt er. Der er efter vores opfattelse tale om omfattende udvidelse af beføjelser for Center for Cybersikkerhed (CFCS) i en sådan grad, at det er svært som aktør at vide hvad man bliver omfattet af, både i umiddelbar, men også fjernere fremtid.

Definitioner:
§ 2, definition 3:
Definitionen i udkastet er meget bred, og det er Region Nordjyllands opfattelse, at denne kan omfatte alle borgerrettede løsninger, som regionen/regionerne måtte udvikle og/eller stille til rådighed for borgerne.

§ 2, definition 6:
Region Nordjylland finder det uklart hvornår en løsning falder ind under definition. Især formuleringen "…, som normalt ydes mod betaling… " giver anledning til usikkerhed ift. Hvilke borgerrettede løsninger, der måtte være omfattet.

§ 3, stk. 1:
Den skrevne formulering giver ingen informationer om hvilke minimumskrav til sikkerhed, der vil blive fastlagt af CFCS. Der er reelt tale om carte blanche til CFCS om hvilke krav, der vil blive stillet, og formuleringen "Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger…" giver ikke regionerne nogen klarhed over hvordan eventuelle krav fra CFCS vil blive fastlagt eller effektueret.

§3, stk. 3:
Det er meget uklart hvad kriterierne for "en betydelig trussel" er. Er dette en vurdering fra CFCS alene, eller enighed blandt ledende aktører inden for sikkerhedsbranchen? Hvordan er aktører sikret ift. at fjerne de af CFCS definerede konkrete foranstaltninger, når en "betydelig trussel" ikke længere er til stede?

§4, nr. 5:

Det vil i praksis være yderst vanskeligt at informere alle brugere på eksempelvis gæstenetværk på hospitaler om en potentiel sikkerhedshændelse. Der må gives plads til individuelle vurderinger af impactet for de relevante netværk. Det må derudover anses for værende på grænsen af gældende lovgivning at logge så mange detaljer om enheder på eksempelvis gæstenetværk, at en bruger kan entydigt identificeres.

Kommentarer til bemærkninger til lovforslaget:
Bemærkning 3.2.3 (side 11):
Det er særdeles vanskeligt for regionerne at gennemskue i hvor høj grad vi omfattes af dette forslag til lovændringen. Det er desuden ikke muligt at vurdere omfanget af krav, der kan blive stillet, hvad enten regionerne fremadrettet er omfattet af § 2, definition 3 eller §2, definition 6.

Bemærkning 3.3.3 (Side 12):
Det er vanskeligt at udarbejde et regulært høringssvar, idet uklarheden omkring hvordan loven praktisk skal udmøntes er så stor, at det er svært at vurdere, hvad der udfærdiges et høringssvar på.

Bemærkning 3.4.3 (Side 14):
Information til brugere om mulige beskyttelsesforanstaltninger kræver at det er muligt at identificere brugerne. Indsamling af data for at muliggøre dette, eksempelvis brugere der har været forbundet til et gæstenetværk på et sygehus, vil være af et sådant omfang, at det med stor sandsynlighed vil være i strid med eksisterende lovgivning omkring logning. Kravet må derfor anses som værende urimeligt.

Bemærkning 4 (Side 16):
I dette afsnit omtales kun telesektoren specifikt, hvorfor det må antages, at lovgivningen kun er gældende for denne, men den nævnte definition på NUIK-tjenester skaber uklarhed om hvorvidt offentlige instanser fremadrettet vil være omfattet også. Det er derfor Region Nordjyllands opfattelse, at en vurdering af at implementering kan ske under eksisterende bevillingsmæssige rammer ikke er korrekt, da ingen kender konsekvenserne ved implementering af lovforslaget.

Bemærkning 5.2 (Side 17):
Placeringen af dette punkt og den nævnte vurdering fra Klima-, Energi- og Forsyningsministeriet vedr. at der vil være 10-20 danske internetbaserede kommunikationstjenester, der vil kunne blive omfattet af definitionen indikerer, at regionerne som offentlig myndighed ikke vil være opfattet som udbyder af NUIK-tjenester. Imidlertid er definitionen på NUIK-tjenester så vag, at regionernes borgerrettede løsninger kan opfattes som værende omfattet. Det er

derfor Region Nordjyllands holdning, at det er nødvendigt at præcisere dette yderligere

Bemærkning 10 (Side 19):
Vurderingen vedrørende positive/negative konsekvenser forudsætter efter Region Nordjyllands opfattelse, at regionerne ikke er omfattet af lovgivningen. Såfremt regionerne er omfattet, eksempelvis gennem borgerrettede løsninger, er der risiko for at den nævnte vurdering ikke vil være korrekt, idet omfang og/eller konsekvenser af implementering af forslaget ikke er klarlagt.

Afsluttende kommentarer
Som region er Region Nordjylland bekendt med, at der påhviler regionen et særligt ansvar for at beskytte data, herunder personoplysninger. Det er dog ikke muligt ud fra den konkrete høring at vurdere i hvilket omfang regionerne er omfattet af lovgivningen, eller hvilke konsekvenser der vil være, såfremt regionerne er omfattet af lovgivningen.

Antagelsen om at løsningerne kan implementeres indenfor eksisterende bevillinger er en yderst risikabel antagelse, idet aktørerne ikke har, og ikke kan forvente at få, overblik over hvilke krav de kan blive mødt med fra udøvende myndighed.
Det er naturligt, at lovgivning ikke kan blive fuldt detaljeret omkring alle forhold vedr. implementering, men idet der ikke er nogle bekendtgørelser eller cirkulærer til at understøtte definitionerne i lovforslaget, ønskes teksten i lovforslaget præciseret, således at relevante aktører ikke kan være i tvivl om omfatningsgraden af lovforslaget.

Med venlig hilsen

Region Sjælland, Region Syddanmark og Region Nordjylland

Forsvarsministeriet har den 30. juli 2020 sendt udkast til forslag til lov om ændring af lov om net- og informationssikkerhed i høring.

Ministeriernes forpligtelse til at høre Rigsrevisionen er fastlagt af rigsrevisorloven, §§ 7 og 10 (Lovbekendtgørelse nr. 101 af 19/01/2012) og angår revisions- og/eller regnskabsforhold, der kan have betydning for Rigsrevisionens opgaver.

Vi har gennemgået lovforslaget og kan konstatere, at det ikke omhandler revisions- eller regnskabsforhold i staten eller andre offentlige virksomheder, der revideres af Rigsrevisionen.

Vi har derfor ikke behandlet henvendelsen yderligere.

Med venlig hilsen

Mette E. Matthiasen
Ledelsessekretariatet

FOLKETINGET
RIGSREVISIONEN

Landgreven 4
DK-1301 København K

Tlf. +45 33 92 84 00
Dir. +45 33 92 85 73
mem@rigsrevisionen.dk

www.rigsrevisionen.dk

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt pr. mail til fmn@fmn.dk,
nmc@fmn.dk, nls@fmn.dk,
nbb@fmn.dk, eba@fmn.dk

Sagsnummer 2020/004886 &
Sagsnummer 2020/005122

København, 26. august 2020

Høring over forslag til lov om ændring af lov om net- og informationssikkerhed (implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation for så vidt angår sikkerhed i net og tjenester) samt høring over udkast til forslag til lov om ændring af lov om elektroniske kommunikationsnet og -tjenester (etablering af mobilbaseret varslingssystem)

Generelle bemærkninger

Teleindustrien og IT-Branchen (herefter høringsparterne) har noteret sig Forsvarsministeriets offentlige høring over lovforslaget om ændring af lov om net- og informationssikkerhed (NIS-loven) samt høringen over udkast til forslag til lov om ændring af lov om elektroniske kommunikationsnet og -tjenester (Teleloven) fsva. etablering af mobilbaseret varslingssystem) og fremsender herunder sine bemærkninger.

Da begge lovforslag, som er sendt i høring, omfatter delelementer af etableringen af mobilbaseret varslingssystem, fremkommer høringsparterne med ét samlet høringssvar på begge disse høringer.

Lovforslagene implementerer dele af direktiv 2018/1972/EU om oprettelse af en europæisk kodeks for elektronisk kommunikation (herefter direktivet). Indledningsvist vil høringsparterne gerne kvittere positivt for den relativt tekstnære direktivimplementering.

Høringsparterne kvitterer positivt for, at udbydere af nummeruafhængige interpersonelle kommunikationstjenester til forskel fra tidligere nu bliver genstand for en række forpligtelser i relation til sikkerheden i sådanne tjenester. Samlet er der dog behov for en ensretning af definitioner med de tilsvarende definitioner i Teleloven.

Høringsparterne sætter pris på Forsvarsministeriets udkast til ændring af Teleloven fsva. etablering af mobilbaseret varslingssystem. Det gælder særligt beslutningen om, at et mobilt varslingssystem baseres på cell broadcast-teknologi, samt at Forsvarsministeriet dækker udgifterne til etableringen og driften af et sådant system.

Høringsparterne sætter desuden spørgsmålstegn ved den nye foreslåede forpligtelse om, at udbydere skal informere brugere om mulige beskyttelsesforanstaltninger i tilfælde af en særlig og betydelig trussel om sikkerhedshændelse. Høringsparterne har svært ved at gennemskue, hvorledes teleudbydere skal kunne informere en specifik (gruppe af) forbrugere, der fx anvender sikkerhedsmæssigt kompromitterbart brugerudstyr, og mener, at det bør præciseres, hvordan der tages beslutning om eventuel informering af brugere om potentielle trusler eller sikkerhedshændelser og mulige beskyttelsesforanstaltninger konkret udmøntes i praksis. Den konkrete udmøntning vil være afgørende for den faktiske mulighed for efterlevelse og for de reelle omkostninger af løsningen. Løsning bør være omkostningseffektiv og proportional i forhold til den ønskede effekt.

Høringsparterne fremsender herunder sine specifikke bemærkninger til lovforslagene, hvor talmarkeringen følger nummerering af foreslåede lovændringer i NIS-loven henholdsvis Teleloven.

Specifikke bemærkninger til ændring af NIS-loven

Nr. 1-3 om ændring af lovens titel

Høringsparterne har forståelse for den foreslåede ændring af lovens titel, da denne er som konsekvens af tilsvarende begrebsændring i teledirektivet. I lyset af ændring af lovens definitioner bør anvendelsen af begreberne "*net og tjenester*" imidlertid ikke anvendes i overskriften, da de rejser tvivl om lovens anvendelsesområde. Høringsparterne opfordrer til, at telelovens begreber "elektroniske kommunikationsnet og -tjenester" anvendes i stedet, jf. også nedenfor. Høringsparterne undres dog over ændringen til det meget generelle begreb "sikkerhed", da der ikke synes at være en konkret begrundelse herfor. Høringsparterne finder, at "informationssikkerhed" er et bredere begreb.

Nr. 4 om ensretning af definitioner med telelovens definitioner

Høringsparterne kvitterer for, at der med ændringen søges en ensretning af definitionerne med de tilsvarende definitioner i Teleloven. Der er dog i enkelte af definitionerne, hvor Forsvarsministeriet lægger op til visse nuanceforskelle i ordvalget. Høringsparterne opfodrer generelt til, at definitionerne affattes fuldstændigt ordret med tilsvarende definitioner i Teleloven, således at der ikke opstår fortolkningstvivl om definitionerne i de to love skal forstås forskelligt.

Høringsparterne skal i øvrigt opfordre til, at definitionerne "*elektroniske kommunikations net og -tjenester*" anvendes konsekvent gennem hele loven i stedet for "net- og tjenester". Eksempelvis fremgår "*net og -tjenester*" fortsat af ændringen til § 2 stk. 1, nr. 8.

Nr. 4 om ny definition af udbyder af nummeruafhængig interpersonel kommunikationstjeneste jf. § 2, nr. 6

Høringsparterne kvitterer umiddelbart positivt for den foreslåede definition i medfør af § 2, nr. 6, af udbyder af nummeruafhængig interpersonel kommunikationstjeneste (i lovforslaget udbydere af NUIK-tjenester). Høringsparterne mener, at denne definition bør være identisk med samme definition som foreslået i § 2, nr. 20 i Lov om Elektroniske kommunikations net og -tjenester (Teleloven), hvilket tillige fremgår som hensigten i lovbemærkningernes side 8 g 23, således at der til enhver tid sikres en ensartet forståelse af begreberne. Dette kan bør gøres ved henvisning til definitionen i Teleloven.

Høringsparterne gør desuden opmærksom på, at begrebet "en nummeruafhængig interpersonel kommunikationstjeneste" ikke forkortes i Teleloven. Således kunne der med fordel skabes mere ensartethed og juridisk klarhed ved at behandle samme begreb på samme måde. Høringsparterne anbefaler at skrive begrebet fuldt ud gennemgående i loven.

Endvidere mener høringsparterne, at udbydere af nummeruafhængige interpersonelle kommunikationstjenester, der opretter forbindelse til offentligt tildelte nummerressourcer, tillige bør være omfattet af definitionen. Sådanne tjenester er allerede omfattet af definitionen om en "*elektronisk kommunikationstjeneste*", jf. Teleloven, da der er tale om en tjeneste, der helt eller delvis består i elektronisk overføring af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter. Høringsparterne ønsker derfor dette entydigt afklaret i lovens bemærkninger.

Høringsparterne finder det desuden uklart, hvorledes flere af branchens value-added-tjenester vil blive omfattet af definitionen. Det være sig fremtidens interaktive TV-produkter, hvor kommunikation mellem TV-brugere eller kundeservice muliggøres som en støttefunktion. Der kunne også være tale om e-mail-tjenester tilknyttet slutbrugeres bredbåndsabonnement. Såfremt sådanne value-added tjenester menes omfattet, bør det fremgå tydeligt af lovens bemærkninger. Høringsparterne gør tillige opmærksom på, at det er væsentligt at sikre et 'level playing field' i forhold til andre udbydere af fx e-mail-konti, der – såfremt ovenstående bør være omfattet – tillige underlægges samme krav og forpligtelser.

Høringsparterne mener desuden, at det i lovens bemærkninger bør specificeres, hvad der menes med "*som der normalt ydes mod betaling*", som både fremgår direkte af bestemmelsen og af lovbemærkningerne på side 24. Det bør i lovens bemærkninger afklares, hvorvidt der alene er tale om en tjeneste, der normalt ydes mod monetær betaling, eller om betalingen også kan udgøre adgang til brugerens data. Ovenfornævnte tjenester, interaktive tv-pakker og e-mail-tjenester, er eksempelvis ikke tjenester, som kunden betaler monetært for, men er en value-added tjeneste i fx bredbåndsabonnementet.

Nr. 4 om ny definition af sikkerhed i net og tjenester jf. § 2, nr. 7

Høringsparterne noterer sig, at "autenticiteten" nu også er indbefattet i definitionen af "*sikkerhed i net og tjenester*" jf. § 2, nr. 7, som teledirektivets artikel 2, nr. 21, foreskriver, værende i tillæg til tilgængeligheden, integriteten og fortroligheden af elektroniske kommunikations net og -tjenester. Høringsparterne henfører til, at "autenticiteten" i lovbemærkningernes side 24 nærmere defineres som, *"at data og informationssystemer mv. er, hvad de foregiver at være. Begrebet anses således at handle om ægthed og originalitet"*.

Høringsparterne vurderer, at ændringen vil medføre, at teleoperatører i fremtiden fx skal rapportere til myndighederne, hvis data og informationssystemer mv. således ikke er, hvad de foregiver at være.

Et eksempel herpå kunne i praksis være, hvis en ondsindet aktør implementerede et delelement i en operatørs netværk, som operatøren ikke umiddelbart havde kendskab til. Derved ville en given kunde tilgå operatørens systemer, som ikke nødvendigvis er, hvad de foregiver at være, nemlig operatørens fuldt kontrollerede udstyr og systemer. Dette ville i så fald skulle rapporteres til myndighederne, når hændelsen bliver kendt af operatøren.

Hvis ovenstående eksempel er korrekt forstået, finder høringsparterne det rimeligt, at teleoperatørerne bliver genstand for en sådan forpligtelse.

Nr. 4 om ny definition af sikkerhedshændelse jf. § 2, nr. 8

Høringsparterne støtter den foreslåede definition af en sikkerhedshændelse og støtter desuden, at der ikke fokuseres på en potentiel, men en faktisk, indvirkning på sikkerheden. Høringsparterne gør dog opmærksom

på, at graden af den "faktiske negative påvirkning" ikke kendes umiddelbart ved sikkerhedshændelsens begyndelse.

Nr. 6-9 om minimumskrav til informationssikkerhed for udbydere jf. § 3

Høringsparterne støtter den foreslåede ændring af § 3, stk. 1 og 3, om inkludering af nummeruafhængige interpersonelle kommunikationstjenester med samme forbehold som anført ovenfor ved punkt 4. Det er her væsentligt at sikre en level playing field blandt elektroniske kommunikationstjenester, der i stigende grad konkurrerer med hinanden.

I den nye foreslåede § 3, stk. 3, anvendes begrebet "betydelig trussel" om en sikkerhedshændelse, der kan lede til påbud fra myndighederne om at træffe nødvendige foranstaltninger, hvis en sådan identificeres. Høringsparterne finder det hensigtsmæssigt, at begrebet specificeres i lovens bemærkningerne. Høringsparterne finder det ligeledes hensigtsmæssigt, at det specificeres, hvilke typer påbud man påtænker at anvende, samt hvilke konsekvenser disse påbud kan have for operatøren.

Som nævnt ovenfor kendes graden af den faktiske negative påvirkning af en sikkerhedshændelse, og dermed tillige den faktiske negative påvirkning af en betydelig trussel om en sikkerhedshændelse, først senere i forløbet. Derfor kan det være vanskeligt konkret af vurdere den faktiske påvirkning af en betydelig trussel. Høringsparterne finder i øvrigt, at Domstolene bør afsige kendelse om påbuddet, hvis disse foranstaltninger indebærer begrænsninger i de grundlæggende rettigheder.

Selvom vi forstår og anerkender hensynet med og baggrunden for den foreslåede bestemmelse, herunder dens ophav i artikel 41 i teledirektivet, er vi bekymrede over det upræcise omfang af bestemmelsens rækkevidde i forhold til den kompetence, der tillægges CFCS. Omfanget af de konkrete foranstaltninger, CFCS kan pålægge de enkelte udbydere at foretage, er kun i meget begrænset omfang specificeret i lovforslaget og kan med den foreslåede ordlyd af bemærkningerne potentielt tolkes meget bredt.

Det fremgår således af bemærkningerne, at "*det vil afhænge af sikkerhedshændelsens karakter, hvilke foranstaltninger der er nødvendige for at afhjælpe denne", og at en udbyder kan blive pålagt at sikre, "at leverancer af hardware, firmware eller software, der kan udgøre en sårbarhed i den pågældende udbyders net eller tjeneste, skal undersøges for sårbarheder, samt at foretage logisk og fysisk adgangskontrol til nærmere angivne systemer eller udstyr og sikre sporbarhed heraf*."

Dermed tillægges CFCS en i praksis næsten ubegrænset mulighed for at kræve, at konkrete udbydere foretager potentielt særdeles indgribende og omkostningstunge foranstaltninger. Høringsparterne skal kraftigt opfordre til, at denne bestemmelse indsnævres, og at det i langt højere grad præciseres, hvor vidtrækkende kompetencer CFCS får med denne bestemmelse.

Høringsparterne har forståelse for og støtter, at den foreslåede § 3, stk. 4, om at traditionelle teleudbydere kan pålægges forpligtelser ved hensyn af væsentlig samfundsmæssig betydning, fortsætter som hidtil med de mindre, foreslåede sproglige præciseringer.

I lovens bemærkninger på side 10 fremgår et ønske, med henvisning til teledirektivet, om at fremme kryptering, som ikke umiddelbart er en del af det eksisterende lovgrundlag i dag, med mindre det anskues som en del af den interne risikostyringsproces i medfør af lovens § 3, stk. 1. Høringsparterne anerkender dog også, at denne bestemmelse stammer fra teledirektivets artikel 40, stk. 1.

For danske teleudbydere er kryptering i risikostyringen, fx af management styring af infrastrukturen, allerede fuldt implementeret, hvorfor høringsparterne ikke umiddelbart kan se, hvorledes yderligere fremhævelse af kryptering kan/bør ske i Danmark. Høringsparterne har dog ikke kendskab til, hvorledes kryptering anvendes

for udbydere af nummeruafhængige interpersonelle kommunikationstjenester. På den baggrund finder høringsparterne det rimeligt, at der stilles krav til kryptering både på teleoperatørniveau og blandt nye typer af tjenesteudbydere. Endelig anmoder høringsparterne om særlig forsigtighed og proportionalitet i overvejelserne herom, da vidtgående (system-)krav herom kan udgøre væsentlige ekstraomkostninger for udbyderne. Endelig ønsker høringsparterne at gøre opmærksom på, at fremtidens mobile teknologier, herunder 5G, har kryptering af data mellem mobilnetværkets radio access netværk og mobil core-systemet indbygget som standard.

I lovens bemærkninger på side 10, fremgår det desuden af udbydere af nummeruafhængige interpersonelle kommunikationstjenester kan have egen teknisk infrastruktur. Høringsparterne gør i den anledning opmærksom på, at denne type infrastruktur ikke alene omhandler "*forbindelser til internetudbydernes net, som kan blive omfattet sikkerhedskrav*" jf. lovbemærkningernes side 10, men også andre typer af infrastrukturejerskab og drift af fx store datacentre, som bør tages højde for i lovforslaget og dets bemærkninger.

Nr. 11-14 om oplysnings- og underretningspligter for udbydere jf. § 4

Høringsparterne finder det relevant, at udbydere på det danske marked pålægges at informere CfCS om sikkerhedshændelser og anerkender, at den foreslåede ændring i § 4, nr. 3, om såvel tilføjelsen af udbydere af nummeruafhængige interpersonelle kommunikationstjenester samt tilføjelsen af "*uden unødigt ophold*" er en implementering af teledirektivets artikel 40, stk. 2. TI finder dog, at tilføjelsen af "*uden unødigt ophold*" er en signifikant stramning af bestemmelsen i forhold til i dag, hvor fristen er 14 dage. TI skal opfordre til, at denne frist fastholdes i den konkrete udmøntning i bekendtgørelsen.

Høringsparterne finder tilføjelsen af ny nr. 4 i § 4 særligt bekymrende, om at udbydere generelt i alle tilfælde skal underrette offentligheden ved sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester.

Høringsparterne er bekymret over udsigten til i medfør af den foreslåede § 4, stk. 4, at skulle informere offentligheden som sådan om sikkerhedshændelser, der i øvrigt måtte være forsvarligt håndteret. Der vil være stor risiko for, at en generel udmelding til offentligheden om en afsluttet trussel kunne skabe unødig utryghed.

Samtidig bør det overvejes nøje, hvilke risici der løbes, ved at der kommer information om sikkerhedstrusler ud i offentligheden. Høringsparterne er bekymret for, at hvis der er offentlighed om en trussel (uanset om denne anses for at være afsluttet), kan anspore hackere til at gå målrettet mod en udbyder eller en sektor, der har været ramt.

Høringsparterne skal i stedet foreslå, at bestemmelsen ændres således, at udbyderne i stedet forpligtes til at informere konkrete berørte kunder om sikkerhedshændelsen og eventuelt om, hvilke forholdsregler de konkret berørte kunder kan tage i den forbindelse, eller alternativt blødgøres med tilføjelse af "*hvor det findes relevant*".

Høringsparterne sætter imidlertid spørgsmålstegn ved den nye foreslåede bestemmelse i § 4, stk. 5, om at udbydere skal informere brugere om mulige beskyttelsesforanstaltninger i tilfælde af en særlig og betydelig trussel om sikkerhedshændelse. Høringsparterne har således svært ved at gennemskue, hvorledes teleudbydere skal kunne informere en specifik (gruppe af) forbrugere, der fx anvender sikkerhedsmæssigt kompromitterbart brugerudstyr (CPE), fx en ukurant WiFi-router, når denne type information ikke er kendt af teleudbyderen. Høringsparterne anerkender dog også, at teleudbyderne har en interesse i at sikre et så sikkert netværk, som muligt, hvorfor intentionen med forslaget giver god mening.

Usikkerheden omkring udmøntningen af kravene i medfør af § 4, nr. 4, indebærer, at det for visse udbydere i branchen er usikkert, om der skal etableres nye funktioner i virksomheden til at håndtere sådanne nye krav. Det er således nærliggende, at det vil have yderligere omkostningsmæssige konsekvenser for sådanne udbydere at opfylde kravene.

Af bemærkningerne til lovforslaget fremgår det derudover, at "*Som i dag indebærer dette, at udbyderne efter påbud skal underrette offentligheden, eller at CFCS kan foretage underretning af offentligheden, hvis det godtgøres, at dette er i offentlighedens interesse*". Det kan have stor skadegørende effekt på en udbyder, hvis det påbydes en udbyder at melde ud til brugere og offentligheden om mulige trusler eller hvis der af CFCS meldes offentligt ud om mulige trusler. Dette gør sig særligt gældende, når selve hjemmelsgrundlaget for at udstede påbud vedrørende sikkerhedstrusler er uklart. Derfor bør det i loven og bemærkningerne fastlægges under hvilke omstændigheder denne ret til at meddele påbud og egen offentliggørelse kan udnyttes, herunder at udbyderen får mulighed for at blive partshørt, medmindre det af tidsmæssige grunde er umuligt.

Endelig bør det derfor præciseres, hvordan der tages beslutning om eventuel informering af brugere om potentielle trusler eller sikkerhedshændelser og mulige beskyttelsesforanstaltninger konkret udmøntes i praksis.

Høringsparterne finder, at den konkrete udmøntning af bestemmelsen i en bekendtgørelse vil være afgørende for den faktiske mulighed for efterlevelse og for de reelle omkostninger af løsningen. Høringsparterne mener, at den løsning, som tænkes implementeret i Danmark, bør være omkostningseffektiv og proportional i forhold til den ønskede effekt. Som eksempel kunne en samlet informationsportal om kompromitterbart brugerudstyr, som bliver bekendt for teleudbyderen, gøres tilgængeligt for offentligheden og udbyderens kunder på en samlet internetside. Der er mange eksempler på, at dette ikke i praksis er muligt, da udbyderne ikke har de nødvendige processer og data til at sikre effektiv, praksis udmøntning af en sådan løsning. Høringsparterne finder således, at det som minimum tydeliggøres i lovbemærkningerne, hvorledes myndighederne forventer, at udbydere kan designe et system, som kan håndtere dette, og samtidig beskrive de væsentlige omkostninger, der eventuelt vil være forbundet med et sådant system.

Andre bemærkninger

Høringsparterne har ingen indholdsmæssige bemærkninger til lovforslagets punkter 17-27.

Høringsparterne anser desuden, at de i lovbemærkningerne anførte økonomiske konsekvenser for erhvervslivet virker særdeles underestimerede særligt henset til lovforslagets mange usikkerheder. Lovforslaget lægger op til, både direkte og indirekte gennem efterfølgende udmøntning i bekendtgørelser, at flere nye systemer skal designes, indkøbes og implementeres hos udbyderne. Derudover bidrager usikkerheden om kravene til beskyttelsesforanstaltninger og kryptering tillige til øget usikkerhed om omkostningerne. Når det endnu ikke er fuldt ud belyst, hvilke foranstaltninger og lignende loven og efterfølgende bekendtgørelser vil medføre, er det ikke muligt for høringsparterne at vurdere omfanget af de økonomiske konsekvenser for de enkelte selskaber. Samtidig må det forventes, at når udbydere af nummeruafhængige interpersonelle kommunikationstjenester indbefattes en række nye krav, vil det medføre øgede omkostninger for erhvervslivet.

Specifikke bemærkninger til etablering af mobilbaseret varslingssystem jf. NIS-lovens § 5 a og Telelovens §§ 61 a og 81

Generelt

Høringsparterne støtter Forsvarsministeriets forslag til etablering af mobilbaseret varslingssystem jf. NIS-lovens § 5 a og Telelovens §§ 61 a og 81. I særdeleshed beslutningen om, at et mobilt varslingssystem baseres på cell broadcast-teknologi, samt at Forsvarsministeriet afholder omkostningerne ved etablering og drift af et sådant system.

Nr. 1 om etablering af mobilbaseret varslingssystem jf. Teleloven § 61 a

Høringsparterne ser positivt på implementeringen af teledirektivets artikel 108, 2. pkt., om et offentligt mobilbaseret varslingssystem, der kan udsende offentlige advarsler om overhængende eller truede nødsituationer og katastrofer. En forpligtelse til at indføre et sådant system er dog ikke uproblematisk, da mobilselskaberne ikke på nuværende tidspunkt råder over et sådant, og ikke selv har incitament til at indføre systemer, der ikke understøtter driften af selskabernes netværk og forretning. Høringsparterne deler Forsvarsministeriets vurdering af etableringsomkostninger på ca. 140 mio. kr. og årlige driftsomkostningerne på 10 mio. kr. For at undgå unødige tunge økonomiske byrder på erhvervslivet, sætter høringsparterne stor pris på, som det indgår i lovforslaget om ændring af Teleloven, at staten afholder udgifterne forbundet med etablering og drift af det mobilbaserede offentlige varslingssystem. Høringsparterne støtter tillige, at staten også vil afholde dokumenterede udgifter forbundet med krav i medfør af den foreslåede bestemmelse, som ikke allerede følger af de gældende §§ 3 og 5 i NIS-loven. I forlængelse heraf sætter høringsparterne pris på lovbemærkningerne til nr. 1 om, at mobiloperatørerne forud for større økonomiske dispositioner kan have en dialog med de relevante beredskabsmyndigheder med henblik på at afklare, om dispositioner har en karakter, hvor der kan ydes refusion.

Desuden støtter høringsparterne op om Forsvarsministeriets overvejelser og vurdering af, at et mobilbaseret varslingssystem bør baseres på cell broadcast-system. Høringsparterne er enige i, at den foreslåede løsning baseret på cell broadcast-teknologien er den bedste løsning til formålet, blandt andet på grund af de fordele, der nævnt i høringsmaterialet, herunder særligt det forhold, at alle nyere mobiltelefoner kan modtage sådanne beskeder, og at der ikke sker registrering af personoplysninger i forbindelse med brug af systemet.

Der kan synes at være en begrebsforvirring til, hvem pligtsubjektet i medfør af forpligtelsen i den foreslåede bestemmelse i Telelovens § 61 a, hvor begrebet "*Udbydere af elektroniske kommunikationstjenester i mobilnet og udbydere af mobilnet*" anvendes. Dette begreb er imidlertid ikke nærmere defineret i Teleloven. Høringsparterne anbefaler således, at det gøres klart for hvem denne forpligtelse konkret påhviler såvel i Telelovens § 61 a og NIS-lovens § 5a med korrekt anvendelse af klart definerede begreber jf. Telelovens § 2 og NIS-lovens § 2. Således anbefaler TI, at Telelovens § 61 a, stk. 1, affattes:

> "***§ 61 a.*** *Udbydere af* ***offentlige*** *elektroniske kommunikations****net og -****tjenester ~~i mobilnet og udbydere af mobilnet~~ skal på vegne af beredskabsaktører udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer til berørte slutbrugere. Udbyderne skal udsende offentlige advarsler til de slutbrugere, der i varslingsperioden opholder sig i nærmere angivne geografiske områder, straks efter modtagelse af anmodning herom."*

Samt at NIS-lovens § 5a affattes:

> ***"§ 5 a.*** *Center for Cybersikkerhed fastsætter regler om, at udbydere, som i medfør af telelovens* ***§ 61 a*** *skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne."*

Nr. 16 om uafbrudt transmission af offentlige advarsler jf. NIS-lovens § 5 a

Høringsparterne ser frem til at bidrage konstruktivt i forbindelse med den konkrete udmøntning af bestemmelsen i bekendtgørelsen, herunder hvorledes *"alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne"* konkret skal forstås, da dette synes noget uklart. Heriblandt hvad der menes med "uafbrudt", som ikke indgår i ændringen af Telelovens § 61 a. Høringsparterne anbefaler, at den konkrete løsning er fleksibel samt at krav hertil er proportionelle.

I forlængelse heraf vil høringsparterne sætte pris på en bekræftelse af, at opfyldelse af kravet om "uafbrudt transmission" er dækket af Forordning om foranstaltninger vedrørende adgang til det åbne internet artikel 3, stk. 3, 3. afsnit, hvori det fremgår, at udbyderen af internetadgangstjenester kan foretage mere vidtgående trafikstyringsforanstaltninger, hvis det er nødvendigt for at overholde lovgivning, for at opretholde integriteten og sikkerheden i nettet eller for at forebygge truende overbelastning af nettet og afbøde virkningerne af ekstraordinære eller midlertidige overbelastning af nettet.

Da systemet skal kunne tages i brug senest den 22. juni 2022, og da der vi være tale om et teknisk kompliceret setup med høje driftssikkerhedskrav, sætter høringsparterne pris på, at der med lovforslaget er lagt op til et tæt samarbejde mellem mobilselskaberne og Forsvarsministeriet om indførelsen af systemet, herunder udvikling, test, etablering og drift, samt ikke mindst en løbende dialog om de nødvendige økonomiske dispositioner med henblik på at sikre, at mobiloperatørerne kun disponerer således, at der kan ydes refusion af de afholdte udgifter.

Afsluttende bemærkninger

Høringsparterne står naturligvis til rådighed måtte Forsvarsministeriet, Klima-, Energi- og Forsyningsministeriet, Center for Cybersikkerhed, Energistyrelsen eller andre relevante myndigheder have opklarende spørgsmål til ovenstående.

Med venlig hilsen

Mette Lundberg, direktør, IT-Branchen

Jakob Willer, direktør, Teleindustrien