Forsvarsministeriet
Holmens Kanal 9
1060 København KØ

Rådet for Digital Sikkerheds høring over Udkast til Forslag til Lov om leverandørsikkerhed i den kritiske teleinfrastruktur

Forsvarsministeriet har sendt udkast til forslag til Lov om leverandørsikkerhed i den kritiske teleinfrastruktur i høring.

Rådet for Digital Sikkerhed finder det positivt, at cybersikkerhed gøres til en parameter i forbindelse med indkøb af komponenter til den kritiske infrastruktur. Det er dog væsentligt, at evt. indgreb overfor væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester sker proportionalt og med retssikkerhed/klagemuligheder.

Rådet for Digital Sikkerhed takker for muligheden for at afgive høringssvar til Lov om leverandørsikkerhed i den kritiske teleinfrastruktur. Det bemærkes dog, at der er tale om en forkortet høringsperiode hen over en juleferie, det er ikke optimalt, specielt ikke når der er tale om indskrænkninger i den almindelige retssikkerhed

Det er vigtigt, at udbydere af *elektroniske kommunikationsnet og -tjenester* infrastruktur har forudsigelige rammer, og at der en markedsbaseret udvikling for at sikre fortsatte investeringer i en robust og sikker dansk teleinfrastruktur uden for indgribende regulering fra myndighedsside. Forslag til lov om leverandørsikkerhed indeholder dog en række indgribende beføjelser, der begrænser aftalefriheden for udbyderne. Aftaler der er indgået på lovlig vis kan blive ændret og udbyderen kan tvinges til at omlægge sin infrastruktur.

Hvis der med lovforslaget helt kan udelukkes givne leverandører, vil det have betydning for udbydernes mulighed for at vælge leverandører og det vil dermed mindske udbydernes muligheder for at vælge leverandør og dermed kan det i sidste ende have negative konsekvenser for konkurrencen.

Rådets holdning:

- *Proportionalitet*: Der er behov for proportionalitets overvejelser når myndighederne på denne måde griber ind i og endda forhindrer markedet i at fungere. Indgrebsmuligheden bør anvendes helt undtagelsesvis og efter en nøje afvejning af truslen mod statens sikkerhed på den ene side og de operationelle sikkerhedsaspekter samt markedsmæssige konsekvenser på den anden side
- *Retssikkerhed:* Der skal være retssikkerhedsmæssige garantier for leverandørerne.

    - Der skal være mulighed for at leverandører kan klage over afgørelser, og klageretten bør ikke kunne tilsidesættes politisk ligesom der skal være mulighed for partshøring og begrundelse for afgørelserne.
    - Afgørelser om forbud bør kun udstedes, hvis påbud efter lov om net- og informationssikkerhed har vist sig ikke at være tilstrækkelige. Der bør indføres regler om effektiv prøvelse af afgørelser og tilsyn med Center for Cybersikkerhed.
    - Endvidere skal forbudsbeslutninger foretages af Forsvarsministeren efter indstilling fra CFCS og høring af andre relevante myndigheder.
- *Erstatning:* Leverandørerne skal have ret til fuld erstatning ved forbud, der får betydning for anvendelse af lovligt leveret udstyr uanset, om det kan anses for at udgøre ekspropriation. Derudover kan det kun være for 'allerede indgåede aftaler' og fordi man har besluttet at gennemføre loven med tilbagevirkende kraft
- *Regulatorisk forudsigelighed:* Gennemtvinges en forceret omlægning, kan det påvirke den sikkerhedsmæssige stabilitet i infrastrukturen og medføre store omkostninger for udbyderne. Dette kan have alvorlige økonomiske konsekvenser og også påvirke incitament for leverandørerne til at udvikle innovative løsninger. Det er væsentligt at disse omkostninger holdes nede også af hensyn til brugerne af disse tjenester, da disse i sidste ende risikeres at bliver væltet over på bruger af tjenesterne.
- Det bør altid vurderes, om *leverandørsikkerhed kan opnås på en mindre indgribende måde.*
- *EU harmonisering:* det giver ikke mening med den danske forsimpling af kritisk eller ikke kritisk infrastruktur, når EU arbejder med flere nuancer.

Om loven:

Det fremgår af lovforslaget, at CfCS kan forbyde udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at anvende givne leverandører:

- § 2. Center for Cybersikkerhed kan i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at indgå en aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, såfremt aftalen vurderes at udgøre en trussel mod statens sikkerhed.
- Ligesom CfCS jf § 3 kan forbyde teleudbydere, at opretholde en indgået aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf,
- Forsvarsministeren kan bestemme, at der af sikkerhedsmæssige grunde ikke udleveres kopi til den særlige advokat (der varetager interesser for parten/teleudbyderen) – jf §8 stk. 3.

På bestyrelsens vegne

Henning Mortensen
Formand, Rådet for Digital Sikkerhed