Fra:	Henriette Fagerberg Erichsen
Til:	Sikkerhedsstyrelsen Hovedpostkasse (SIK)
Emne:	Sv: Høring over udkast til forslag til lov om certificering af cybersikkerhed (Sagsnr.: 2020 - 3)
Dato:	19. oktober 2020 11:50:13
Vedhæftede filer:	image001.png image003.png image005.png InlineImage 1.png

Tak for henvendelsen.

Advokatrådet har besluttet ikke at afgive høringssvar.

Med venlig hilsen

ADVOKATSAMFUNDET
RETSSIKKERHED · UAFHÆNGIGHED · INTEGRITET

Henriette Fagerberg Erichsen
Sekretær

Advokatsamfundet, Kronprinsessegade 28, 1306 København K
D +45 33 96 97 28
hfe@advokatsamfundet.dk - www.advokatsamfundet.dk

Til: Sikkerhedsstyrelsen Hovedpostkasse (SIK (sik@sik.dk)
Fra: Anders Holt (anho@sik.dk)
Titel: Høring over udkast til forslag til lov om certificering af cybersikkerhed
Sendt: 19-10-2020 10:50

Hermed fremsendes høring over udkast til forslag til lov om certificering af cybersikkerhed.

Sikkerhedsstyrelsen anmoder om, at eventuelle bemærkninger sendes til sik@sik.dk senest den 16. november 2020.

Venlig hilsen

Anders Holt
Fuldmægtig
SIKKERHEDSSTYRELSEN

Direkte: 33732036
Mobil: 25431636
E-mail: anho@sik.dk

Sikkerhedsstyrelsen
Esbjerg Brygge 30
6700 Esbjerg
Tlf.: +45 33 73 20 00
www.sik.dk

DANSK ERHVERV
Børsen
1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. + 45 3374 6000

Sikkerhedsstyrelsen
Att.: Anders Holt
Nørregade 63
6700 Esbjerg

Den 16. november 2020

Høringssvar vedr. udkast til lov om certificering af cybersikkerhed
Hermed sender Dansk Erhverv og Teleindustrien et fælles høringssvar om udkast til lov om certificering af cybersikkerhed.

Generelle bemærkninger
Dansk Erhverv bakker op om lovforslagets hensigt om at øge sikkerheden i IKT-produkter, -processer og -tjenester.

Cybersikkerhed defineres i den nationale cyber- og informationssikkerhedsstrategi som:

> ”Cybersikkerhed omfatter beskyttelse imod de sikkerhedsbrud, der opstår som følge af angreb mod data eller systemer via en forbindelse til et eksternt net eller system. Arbejdet med cybersikkerhed fokuserer således på sårbarheder ved sammenkoblingen mellem systemer, herunder forbindelser til internettet.”

Der er altså tale om en mere snæver definition, som handler specifikt om systemsammenkobling, hvor nærværende lovforslag kan opfattes som et, der i højere grad handler om informationssikkerhed. Dansk Erhverv opfordrer regeringen til at være konsistent i anvendelsen af begreber, så unødig forvirring undgås.

Placeringen af ansvaret hos Sikkerhedsstyrelsen betyder, at styrelsen vil få behov for kompetencer og viden indenfor cybersikkerhed bl.a. for at kunne vurdere indholdet og behandle klagesager. Derfor må der afsættes ressourcer til at sikre styrelsen disse.

Dansk Erhverv mener, at det er positivt, at certificeringsordningen er frivillig. Såfremt der findes nogle kategorier af produkter, tjenester eller processer, hvor certificering vil være obligatorisk (fx indenfor de samfundskritiske sektorer), bør dette fremgå tydeligt.

Loven gælder for produkter, tjenester og processer, hvilket betyder at det fx i telesektoren vil være muligt at certificere tjenester såsom bredbåndsforbindelser. Dette er en nødvendig udvikling og kan være positivt for sikkerhedsniveauet af udbudte tjenester, men kan dog give en konkurrencefordel til de større selskaber indenfor et givent område.

Lovforslaget nævner ikke muligheder for indsigt i de sager, Sikkerhedsstyrelsen og/eller andre aktører i certificeringsarbejdet, beskæftiger sig med. Det skal naturligvis være muligt at få indsigt i, hvilke produkter, tjenester og processer, som lever op til kravene om at modtage certificeringen, men der bør tages aktivt hensyn til at de interne mellemregninger i certificeringsprocessen, der kan indeholde fortrolige oplysninger, ikke kommer til offentlighedens kendskab.

Dansk Erhverv er positive overfor lovforslaget, som særligt vil kunne bidrage til at flere IoT-produkter får et sikkerhedsmæssigt løft.

Lovforslaget indeholder ikke oplysninger om, hvilke standarder der skal danne grundlag for certificeringen. Disse skal fastsættes af ENISA i samarbejde med interessenter og ECCG. Dette vil formentlig betyde, at der endnu kan gå lang tid, før certificeringerne kan finde anvendelse.

Specifikke bemærkninger
Afsnit 4, side 19: med lovforslaget afsættes 2,7 mio. kr. til myndighedsopgaven. Dette kan synes utilstrækkeligt, når der tages højde for, at styrelsen skal kunne behandle klager, foretage kontroller m.v., ligesom der skal medtages behovet for nye kompetencer (jf. ovenfor).

Med venlig hilsen,

Jakob Willer
Adm. direktør, Teleindustrien

Christian von Stamm Jonasson
Erhvervspolitisk konsulent, Dansk Erhverv

16. november 2020

Sikkerhedsstyrelsen
Att.: sik@sik.dk

Dansk Industri
Confederation of Danish Industry

Høring over forslag til lov om certificering af cybersikkerhed

DI takker for modtagelsen af ovennævnte høring. DI finder det positivt, at der med cybersikkerhedsforordningen etableres en ramme for europæisk cybersikkerhedscertificering, så virksomhederne fremadrettet undgår at skulle leve op til forskellige certificeringskrav til deres produkter i de forskellige EU medlemslande.

Det fremgår af bemærkningerne til lovforslaget, at certificeringen er frivillig, og har det formål, at virksomhederne kan markedsføre sine produkter som sikre. Formålet er således i høj grad sammenfaldende med målet for den kommende mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse, som DI etablerer i samarbejde med en række andre parter med støtte fra Industriens Fond.

Mærkningsordningen er et mærke til virksomheder. Mærket har bl.a. til formål at give dansk erhvervsliv et solidt løft for it-sikkerhed og ansvarlig dataanvendelse og give forretningsværdi for den enkelte virksomhed. Ordningen vil tilbyde konkret vejledning og hjælp til de virksomheder, der ønsker at øge deres sikkerhed.

Det vil derfor være oplagt at se på, om der er nogen synergieffekter i forhold til mærkningsordningens arbejde, herunder tilsynet med om virksomhederne lever op til mærkningsordningens otte krav, der skal efterleves, og Sikkerhedsstyrelsens arbejde som myndighed for certificering af cybersikkerhed. Der bør derfor etableres mulighed for dialog mellem de to typer tilsyn.

Det bemærkes, at selvom der er ligheder mellem de opgaver sikkerhedsstyrelsen varetager i dag, så er der også væsentlige forskelle mellem bemyndigelse af overensstemmelsesvurderingsorganer inden for de områder styrelsen varetager i dag og IoT-produkter, software mv. Det vil derfor være væsentligt at styrelsen trækker på den nødvendige faglige kompetencer hos fx Center for Cybersikkerhed og som foreslået ovenfor, mærkningsordningen for it-sikkerhed og ansvarlig dataanvendelse.

Specifikke bemærkninger

§ 13
Det fremgår, at Sikkerhedsstyrelsen til enhver tid mod behørig legitimation og uden retskendelse har ret til adgang til alle lokaler hos overensstemmelsesvurderingsorganer eller

H. C. Andersens Boulevard 18
1553 København V
Danmark

(+45) 3377 3377
di@di.dk
di.dk

CVR: 16 07 75 93

indehavere af en europæisk cybersikkerhedsattest med henblik på at føre kontrol. Det bør præciseres, at der skal være tale om lokaler der er *relevante* for den konkrete certificering. Såfremt et overensstemmelsesvurderingsorgan udfører andre forretningsaktiviteter på adressen, bør disse lokaler således ikke automatisk være omfattet.

DI står naturligvis til rådighed for en uddybning af ovenstående bemærkninger.

Med venlig hilsen

Ida Kragh-Vodstrup
Chefkonsulent, DI

Fiolstræde 17 B, Postboks 2188, 1017 København K
taenk.dk · fbr@fbr.dk · +45 7741 7741
CVR: 6387 0528

Sikkerhedsstyrelsen
Sendt pr. e-mail til sik@sik.dk

18-11-2020
Dok. 204461/

Forbrugerrådet Tænks høringssvar om udkast til forslag til lov om certificering af cybersikkerhed

I det vi takker for Sikkerhedsstyrelsens e-mail af 19. oktober 2020, skal Forbrugerrådet Tænk hermed afgive sine bemærkninger.

IT-sikkerhed og databeskyttelse er et højt prioriteret område i Forbrugerrådet Tænk, og vi ser derfor frem til at følge udviklingsarbejdet med en kommende dansk cybersikkerhedscertificering, herunder arbejdet i Den Europæiske Unions Agentur for Cybersikkerhed ENISA samt Sikkerhedsstyrelsen konkrete certificering af – og tilsyn med blandt andet internetforbundne produkter (IoT).

Henset til digitaliseringens hastighed og forbrugernes stigende brug af IoT-produkter støtter Forbrugerrådet Tænk i høj grad forslaget, men er på linje med vores søsterorganisation BEUC i Bruxelles uforstående overfor, at så væsentligt et regelsæt, skal være frivilligt for producenter at følge.

Certificeringskravene vil øge sikkerheden for den enkelte forbruger, lette gennemsigtigheden for komplekse produkter, tjenester og processer og mindske risikoen for cyberangreb til samfundets ulempe, hvilket samlet set vil øge trygheden og fremme tilliden til digitaliseringen. Derfor mener vi, at kravene bør være bindende, men også fordi, det kun er rimeligt, at virksomheder, der er mere optagede af profit end it-sikkerhed ikke går fri af at skulle levere basal sikkerhed til forbrugerne.

Vi hæfter os dog ved, at virksomheder, i det øjeblik de tilslutter sig certificeringsordningen, forpligtes til at efterleve kravene i certificeringen, og at Sikkerhedsstyrelsen kan fratage certificerings-attester samt pålægge virksomheder at fjerne usikre produkter fra handlen. Vi synes dette er meget vigtigt, ligesom Sikkerhedsstyrelsens adgang til at påbyde at markedsføring indstilles eller afhjælpning af produkter foretages. Den klageadgang, som forbrugerne har til Sikkerhedsstyrelsen er ligeledes af stor betydning for området.

En frivillig ordning kræver stor velvillighed fra virksomhedernes side, ikke bare i Danmark men i hele EU, da forbrugerne indkøber og anvender digitale produkter og tjenester på tværs af grænser.

Det forpligter også myndighederne, særligt Sikkerhedsstyrelsen, til at sikre tilstrækkelig information om, hvad certificeringsordningen/evt. et mærke indebærer, sørge for adgang til at se, hvem der har tilsluttet sig ordningen samt oplyse om, hvilke konsekvenser det har at købe/tilgå ikke-mærkede produkter og tjenester, herunder produkter importeret fra lande udenfor EU.

I forhold til selve kriterierne, som nu skal udvikles og danne fundamentet i certificeringsordningen, hæfter vi os ved, at EU-Kommissionen i sikkerhedsforordningen

Fiolstræde 17 B, Postboks 2188, 1017 København K
taenk.dk · fbr@fbr.dk · +45 7741 7741
CVR: 6387 0528

fastslår, at de foruden krav om indbygget sikkerhed i hele produktets levetid, også er optaget af indbygget privatlivsbeskyttelse. Forbrugerrådet Tænk støtter netop, at certificeringskravene både stiller krav om sikkerhed og databeskyttelse by design og default.

Årsagen er, at IoT-produkter desværre, foruden ringe sikkerhed, ofte er kendetegnet ved en vidtgående dataindsamling og automatisk deling af data til 3. parter. Dette er en udvikling, som vi gerne ser minimeret gennem tekniske krav til designet, så datahøst ikke blot er et emne, som forbrugerne kan finde information om i de alenlange, komplicerede vilkår, der medfølger IoT-produkter (typisk i den app, som downloades sammen med installationen af produktet).

Også dataetik er et emne, som for alvor er kommet på dagsorden i Danmark og som foruden privacy kunne have relevans for de kriterier, der skal udvikles i cybersikkerheds-certificeringen. I den forbindelse skal vi henvise til den danske mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse, som både erhvervs- og forbrugersiden står bag.

Vi håber i det hele taget, at der sker en koordinering mellem de to certificeringsordninger, både af hensyn til virksomhederne, som gerne skulle efterleve dem begge og forbrugerne, som skal navigere efter dem, så de forhåbentlig lettere kan træffe et oplyst valg.

Desuden skal nævnes Dataetisk Råd, som netop har offentliggjort et konkret værktøj målrettet myndighedernes databehandling og samkøring, og som også kan bruges som inspiration til kriterie-udviklingen. Endelig skal vi opfordre til at indhente input fra Cybersikkerhedsrådet, som pt. diskuterer behovet for øget sikkerhed i IoT og hvor der i øvrigt er konsensus om, at IoT-produkter både skal styrkes i forhold til sikkerhed og privatlivsbeskyttelse.

Forbrugerrådet Tænk skal afslutningsvis nævne, at vores seneste digitale kampagne, netop omhandlede sikkerhed i IoT-produkter. Vi deler gerne vores materiale, herunder de forbrugerkrav, som er udviklet på europæisk plan af BEUC, ANEC og Consumers International. Desuden bemærkes, at Datatilsynet konkret behandler en sag om ringe sikkerhed i størstedelen af de digitale ringeklokker, som vi testede i forbindelse med kampagnen.

I er naturligvis velkommen til at kontakte undertegnede for uddybning eller lignende.

Med venlig hilsen

Vicedirektør Mette Raun Fjordside Chefjurist Anette Høyrup

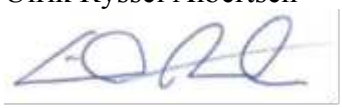
Fra:	Foreningen af Rådgivende Ingeniører
Til:	Sikkerhedsstyrelsen Hovedpostkasse (SIK)
Emne:	SV: Høring over udkast til forslag til lov om certificering af cybersikkerhed
Dato:	27. oktober 2020 10:41:43
Vedhæftede filer:	image002.png image001.png image003.png image005.png

FRI takker for muligheden for at afgive høringssvar på ovenstående høring.

Vi har ingen bemærkninger til den, da den ikke direkte påvirker rammebetingelserne for rådgivende ingeniørvirksomheder.

Med venlig hilsen

Ulrik Ryssel Albertsen



Erhvervspolitisk Chef
Foreningen af Rådgivende Ingeniører

Fra: Anders Holt <anho@sik.dk>
Sendt: 19. oktober 2020 10:51
Til: Sikkerhedsstyrelsen Hovedpostkasse (SIK) <sik@sik.dk>
Emne: Høring over udkast til forslag til lov om certificering af cybersikkerhed

Hermed fremsendes høring over udkast til forslag til lov om certificering af cybersikkerhed.

Sikkerhedsstyrelsen anmoder om, at eventuelle bemærkninger sendes til sik@sik.dk senest den 16. november 2020.

Venlig hilsen

Anders Holt
Fuldmægtig

SIKKERHEDSSTYRELSEN

Direkte: 33732036
Mobil: 25431636
E-mail: anho@sik.dk

Sikkerhedsstyrelsen
Esbjerg Brygge 30
6700 Esbjerg
Tlf.: +45 33 73 20 00
www.sik.dk