**IT-Branchens svar på høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed**

IT-Branchen hilser Regeringens store fokus på cybersikkerhed velkommen. Cybersikkerhed er en afgørende forudsætning for vores gennemdigitaliserede samfund, og derfor er det glædeligt, at regeringen, med den nationale strategi for cyber og informationssikkerhed og de mange sektorstrategier, har forstået at løfte indsatsen på området markant.

Center for Cybersikkerhed (CfCS) spiller en central rolle i regeringens indsats på cybersikkerhedsområdet, og får med det nuværende lovforslag en endnu mere central rolle. CfCS har de seneste år i høj grad vist sin berettigelse, og har været med til at øge awareness og hjælpe danske myndigheder og virksomheder med at forebygge, imødegå og beskytte sig mod cyberangreb.

IT-Branchen har dog en række bekymringer omkring den rolle, som CfCS vil få som følge af Regeringens lovforslag.

1. **Påbud om tilslutning til sensornetværket er problematisk**

Det er højest problematisk, at lovforslaget lægger op til, at CfCS kan påbyde private virksomheder at blive tilsluttet Netsikkerhedstjenesten.

For mange virksomheder kan det kan være kritisk at blive tvunget til tilslutning, uden at kunne redegøre overfor kunder og ejerkreds, hvad data bliver brugt til og hvor de havner.

Vi har en lang tradition i Danmark for tillid og åbenhed, og Danmark har en international styrkeposition, fordi der er tillid til dansk digitalisering, og fordi Danmark internationalt er kendt for, at have et åbent statsapparat.  
  
Tvangstilslutning til overvågningstjenesten risikerer derfor både at ramme danske virksomheders eksport samt internationale investeringer i forskning og produktudvikling i Danmark.

1. **Der mangler klarhed om hvem der kan blive påbudt tilslutning**

Det er meget bekymrende at der ingen steder i lovforslaget er nærmere defineret, hvilke typer af virksomheder der kan påbydes at blive tilsluttet Netsikkerhedstjenesten. Begrebet ”samfundsvigtige virksomheder” er et meget uklart og kan tolkes meget bredt.

Det overlades hermed til centeret selv og Forsvarsministeren egenhændigt at beslutte, hvilke virksomheder der skal påbydes at blive tilsluttet. Det vil skabe en stor usikkerhed hos mange virksomheder. IT-Branchen anbefaler derfor at man fastholder at anvende begrebet samfundskritisk infrastruktur (jf. NIS-direktivet), samt definerer hvad begrebet dækker i Danmark og lader det være scope for loven.

1. **Mangel på effektivt demokratisk tilsyn**

Med udvidelsen af CfCS’s beføjelser er der en stigende nødvendighed for at sikre at centrets beføjelser ikke misbruges.

Lovforslaget lægger op til at skabe en myndighed, som får øgede beføjelser over for civilsamfundet uden at være underlagt domstolsprøvelse eller offentlig kontrol – bortset fra Folketingets kontroludvalg. Ud over mulighed for at påbyde tilslutning til sensornetværket får centeret blandt andet også mulighed for jf. kapitel 4 at tilgå data hos private virksomheder uden retskendelse.

I en tid hvor den frie vestlige verden generelt går mod større åbenhed og kontrol med efterretningsvæsenet, går Danmark den stik modsatte vej med dette lovforslag.

IT-Branchen vil på det kraftigste opfordre til at CfCS, underlægges almindelig parlamentarisk kontrol, ligesom deres afgørelser bør kunne prøves ved civile domstole.

1. **Gør tilslutning frivillig**

IT-Branchen anbefaler derfor på det kraftigste, at tilslutning til Netsikkerhedstjenesten gøres frivillig. Den enkelte virksomhed eller myndighed bør selv træffe beslutning om hvilke sikkerhedsforanstaltninger de anvender. Hvis CfCS alligevel finder det afgørende at påbyde tilslutning til Netsikkerhedstjenesten bør tilslutning i disse tilfælde kunne ske gennem virksomhedernes eget valg af teknologi og udstyr. Udveksling af data vil med et sådan setup kunne ske på den tilsluttede virksomheds præmisser, krypteret og i et standardiseret format.

1. **Centerets aktiviteter vil konkurrere på ulige vilkår med kommercielle it-sikkerhedsleverandører**

Flere elementer i lovforslaget vil gøre CfCS i stand til at tilbyde og påbyde ydelser gratis, som i dag tilbydes af kommercielle aktører. Det er yderst problematisk for det danske marked for it-sikkerheds produkter og services.

I bemærkningerne til lovforslaget fremhæves flere steder, at CfCS kan noget private leverandører ikke kan, da centerets løsning er efterretningsbaseret. Vi er ikke i tvivl om, at CfCS har adgang til efterretningsviden, som it-leverandørerne ikke har, og at det kan give centret nogle muligheder, som branchen ikke har. Men det kan kun være relevant for en lille delmængde af de aktiviteter centeret har. Mange af centerets informationer kommer fra de kommercielle aktører og langt de fleste aktiviteter vil kunne løses mindst ligeså godt af private aktører.

Med det nuværende lovforslag som udvider centerets aktiviteter markant, vil en stadigt større del af centerets aktiviteter være i direkte og ulige konkurrence med private aktører. Som eksempler på foreslåede aktiviteter, der vil konkurrere med private leverandører, kan nævnes muligheden for at tilbyde et aktivt cyberforsvar (3.2), installation af sikkerhedssoftware på lokale netværk og enheder (3.3) og forebyggende sikkerhedstekniske undersøgelser (3.4).

Hvis CfCS ligger inde med efterretningsmæssig information der kan forbedre den sikkerhedssoftware, der allerede findes på markedet anbefaler IT-Branchen i øvrigt, at centeret stiller disse til rådighed for de relevante private aktører så de kan indlejres i deres sikkerhedssoftware.

1. **Brug markedet aktivt som medspiller**

I stedet for at tilbyde aktiviteter i konkurrence med markedet, vil IT-Branchen anbefale at CfCS i langt højere grad gør brug af de kommercielle aktører.

Den ekspertise som hele erhvervslivet besidder inden for IT sikkerhed kan bringes langt bedre i spil, ved at CfCS alene forestår det efterretningsbaserede analysearbejde, mens fx den konkrete dataindsamling og det aktive cyberforsvar kan overlades til den tilsluttede organisation selv eller private aktører efter udbud. En model der kunne overvejes er fx stille minimumskrav til sikkerheden i virksomheder der varetager kritisk infrastruktur, eller ved at indgå en rammeaftale med flere leverandører, således at alle kan tilsluttede organisationer kan vælge mellem en række godkendte løsninger.

Herved kan CfCS bruge deres kompetencer og ressourcer mere effektivt, ligesom ressourcerne i den danske it-sikkerhedsbranche ligeledes kan bringes bedre i spil. Samlet set vil indsatsen kunne nå ud til langt flere.

**Vi stiller gerne op**

IT-Branchen ser frem til den fortsatte dialog, og vi står naturligvis til rådighed for en uddybning af ovenstående.