**IT-Branchens svar på høring over Bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste**

IT-Branchen har modtaget Forsvarsministeriets høring af den vedrørende bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste. IT-Branchen har følgende bemærkninger til bekendtgørelsen.

IT-Branchen vurderer fortsat, at det er højest problematisk, at Center for Cybersikkerhed (CFCS) med de seneste ændringer af lov om Center for Cybersikkerhed, kan påbyde private virksomheder at blive tilsluttet netsikkerhedstjenesten. Vi mener således, at udmøntningen af loven risikerer at skade den danske digitale førerposition, ligesom krav om tilslutning kan have betydelige skadevirkninger for danske virksomheder.

Vi har en lang tradition i Danmark for tillid og åbenhed, og Danmark er internationalt kendt for at have et statsapparat med en høj grad af transparens. Danmark har en international styrkeposition, fordi der er tillid til dansk digitalisering, og fordi digitaliseringen er sket i tæt samspil mellem det offentlige og erhvervslivet.

For mange virksomheder kan det kan imidlertid være kritisk at blive tvunget til tilslutning, uden at kunne redegøre overfor kunder og ejerkreds, hvad data bliver brugt til og hvor de havner.   
  
Tvangstilslutning til overvågningstjenesten risikerer derfor både at ramme danske virksomheders eksport samt internationale investeringer i forskning og produktudvikling i Danmark.

Henset til de potentielle skadevirkninger bør bemyndigelsen til CFCS derfor afgrænses så snævert som muligt og så klart som overhovedet muligt.

Det er således afgørende for IT-Branchen, at bekendtgørelsen om tilslutning til CFCS netsikkerhedstjeneste sikrer, at CFCS kun har mulighed for at påbyde tilslutning for de allermest samfundskritiske virksomheder, samt at påbud kun anvendes hvis CFCS ikke på anden, mindre indgribende vis kan indsamle de relevante oplysninger. Endelig er det afgørende, at påbudte virksomheder ikke pålægges for omfattende krav, som vil være dyre eller problematiske at overholde.

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

Af bekendtgørelsen fremgår det, at CFCS i sin vurdering af, om en virksomhed kan påbydes tilslutning til netsikkerhedstjenesten skal lægge vægt på, om en sikkerhedshændelse vil kunne medføre konsekvenser for *nationale sikkerhedsinteresser*.

IT-Branchen er særligt bekymret for den meget brede definition i §2 stk. 3 af hvad nationale sikkerhedsinteresser omfatter. IT-Branchen vurderer særligt at punkt 5 ”interesser knyttet til befolkningens grundlæggende sikkerhed og velfærd” er formuleret så bredt, at stort set alle større virksomheder vil kunne falde ind under kategorien.

Det overlades hermed til CFCS selv og tilsynsmyndigheden i den relevante sektor 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 fjerner §2 stk. 3, punkt 5, og at beskrivelsen af hvilke virksomheder der kan påbydes tilslutning udbygges, således at der sker en afgrænsning.

1. **Proportionalitet**

IT-Branchen hæfter sig særligt ved, at det i §2 stk. 4 fremgår, at påbud kun kan meddeles, såfremt mindre indgribende midler ikke er tilstrækkelige.

IT-Branchen vurderer, at det til en hver tid vil være muligt at opnå formålet med påbuddet med mindre indgribende midler, fx gennem tilbud om tilslutning med virksomhedernes eget valg af teknologi og udstyr, hvor virksomheden selv ejer og kontrollerer udstyret. Udveksling af data vil med et sådan setup kunne ske på den tilsluttede virksomheds præmisser, krypteret og i et standardiseret format.

IT-Branchen foreslår, at CFCS pålægges altid at tilbyde denne mindre indgribende løsning inden der udsteds påbud om placering af CFCS’s eget udstyr hos virksomheden.

1. **Store krav til påbudte virksomheder**

Endvidere frygter IT-Branchen, at der med bekendtgørelsen om tilslutning til CFCS netsikkerhedstjeneste stilles mange dyre og omfattende krav til de tilsluttede virksomheder.

I §3 stk. 1 fremgår det at virksomheder der er påbudt tilslutning, loyalt skal medvirke til netsikkerhedstjenestens opsætning og drift af en eller flere alarmenheder, og i stk. 3 punkt 1-3 pålægges virksomheder at blandt andet at stille den nødvendige fysiske, tekniske og netværksmæssige understøttelse til rådighed samt at etablere passende sikkerhedsforanstaltninger for adgang til netsikkerhedstjenestens alarmenheder.

Dette er meget upræcist formulerede krav, der lukker op for en bred fortolkning. Hvad er fx ”passende sikkerhedsforanstaltninger”. Disse krav kan nemt løbe op i en stor regning for de påbudte virksomheder. IT-Branchen foreslår, at påbudte virksomheder kompenseres for disse udgifter.

1. **Problematiske krav ift driftsleverandører**

Enkelte krav i bekendtgørelsen kan være særligt problematiske at efterleve for en virksomhed.

Af §3 stk. 6 fremgår det, at en virksomhed der er meddelt et påbud, skal sikre, at eventuelle driftsleverandører i nødvendigt omfang medvirker til opsætning og drift af alarmenhederne.

Det må forventes at mange af de virksomheder der kan risikere et påbud om tilslutning til netsikkerhedstjenesten vil have en lang række driftsleverandører, herunder flere cloud-leverandører bl.a. med servere placeret i udlandet. Hvordan forestiller Forsvarsministeriet sig, at dette krav skal kunne håndteres, fx i en situation hvor en dansk virksomhed får driftet en løsning i EU eller i et tredje land? Og hvordan skal en virksomhed håndtere det, hvis driftsleverandøren ikke ønsker at medvirke til opsætning og drift af alarmenhederne?

IT-Branchen vurderer, at dette krav i realiteten vil være umuligt at overholde for en virksomhed, der får driftet et eller flere systemer i skyen. Dette krav, kan derfor reelt ende med at umuliggøre anvendelse af cloud-løsninger for en meget lang række danske virksomheder.

1. **Øvrige bemærkninger**

I § 4 stk. 2 fastslås det, at CFCS er dataansvarlig for det indsamlede data. Det fremgår dog ikke om det kan sluttes heraf, om den oprindelige dataansvarlige, er friholdt fra GDPRs krav om at informere datasubjekterne når data overlades/overføres til en anden dataansvarlig. Dette bør fremgå af bekendtgørelsen.

Der er ingen beskrivelse af eventuelle krav om hemmeligholdelse. Det bør gøres klart, om det står det parterne frit at kommunikere offentlig om at de har givet/fået påbud og om der er et timelimit på evt. hemmeligholdelse.

**Vi stiller gerne op**

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