**DANSK ERHVERV**
Børsen
DK-1217 København K

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

Forsvarsministeriet
fmn@fmn.dk
Cc: tbl@kmn.dk og sbu@fmn.dk

4. februar 2019

# Høring over lov om Center for Cybersikkerhed, sagsnr. 2018/006599

## Generelle bemærkninger

Dansk Erhverv glæder sig over regeringens fornyede og skærpede fokus på informations- og cybersikkerhed, herunder Erhvervspartnerskab for it-sikkerhed, lanceringen af SikkerDigital.dk, Sikkerhedstjekket, samt strategi for cyber- og informationssikkerhed og de sektorspecifikke strategier, hvor Dansk Erhverv deltog i arbejde med teleinfrastruktur.

Dansk Erhverv anerkender behovet for løbende at vurdere om Center for Cybersikkerhed (CFCS) har de nødvendige redskaber og beføjelser. Det aktuelle lovudkast lægger op til at give Forsvarsministeriet en række ganske udvidede beføjelser, som Dansk Erhverv stiller sig kritisk over for.

Dansk Erhverv mener, at lovforslaget går for langt, idet der ikke i lovforslaget i tilstrækkeligt omfang redegøres for, hvordan de foreslåede tiltag er proportionale i forhold til deres indgriben i virksomhedernes private forhold. Desuden har lovforslaget et for ensidigt tilgang til virkemidler.

Dansk Erhverv kan derfor ikke støtte forslaget i sin nuværende form.

## Specifikke bemærkninger

### Påbud om tilslutning til CFCSs netsikkerhedstjeneste

Lovforslagets §3 giver CFCS mulighed for at pålægge virksomheder at lade sig tilslutte CFCSs sikkerhedstjeneste, herunder at CFCS vil kunne installere aktivt udstyr og software på virksomhedens infrastruktur, som CFCS kontrollerer, samt pålægge virksomheden at indrette sin eksisterende infrastruktur efter det. En sådan bestemmelse vil kunne ramme danske virksomheder negativt, fx hvad angår eksport, samt internationale samarbejde og teknologiudvikling. Lovforslaget siger ikke, hvilke typer (”samfundsvigtige”) virksomheder som CFCF kan kræve tilslutning til, hvilket Dansk Erhverv anser for nødvendigt at præcisere.

Dansk Erhverv kan ikke støtte, at der gives så vide beføjelser i udvælgelsen af, hvilke former for virksomheder, der kan forlanges tilsluttet den forslåede ordning. Desuden savnes en uddybning af, hvilke former for udstyr og software, der skal anvendes. Det er vigtigt for Dansk Erhverv, at

beslutningen om deltagelse overlades til den enkelte virksomheder, og ligeledes er det er virksomhederne, der beslutter, hvilket udstyr og software der er relevant at anvende.

**Ubegrænset adgang til data i virksomheder**
Lovforslagets §4 giver CFCS meget vidtgående beføjelser til "uden retskendelse [at] behandle trafikdata, pakkedata og stationære data". "Stationære data" defineres som "Data, som opbevares på servere, cloudtjenester, pc'ere, lagerenheder, netværksenheder, mobile enheder og tilsvarende".

Som Dansk Erhverv læser forslaget, indebærer det i praksis, at CFCS får uindskrænket adgang til alle data i de tilsluttede virksomheder, herunder persondata, forretningshemmeligheder, kundedata, private dokumenter m.v. på alt fra virksomhedens servere til den enkelte ansattes telefon eller laptop.

Der er uklart på hvilke præmisser CFCS kan anvende disse tekniske muligheder. Det skaber usikkerhed hos virksomhederne. Det handler ikke kun om, hvad CFCS kan og må foretage sig på en virksomheds it-infrastruktur. Det handler også om, hvad virksomheden kan fortælle sine kunder og samarbejdspartnere, herunder også hvordan CFCS samarbejder med tilsvarende tjenester i andre lande.

Dansk Erhverv mener ikke, at det er proportionelt, at CFCS får en sådan i praksis ubegrænset adgang til alle virksomhedens data. Dansk Erhverv kan derfor ikke støtte denne nye hjemmel.

**Offentlige private samarbejder**
Dansk Erhverv mener ikke, at man kan slutte, at fordi få virksomheder i dag er tilsluttet CFCS netsikkerhedstjeneste, så er der få virksomheder der foretager monitorering af nettrafik, som er præmissen i lovforslagets bemærkninger (bemærkninger til lovforslaget, side 11-).

Det er ikke korrekt, når lovforslaget slutter, at der i dag ikke foregår monitorering af nettrafik for avancerede angreb. Flere virksomhederne investerer allerede i systemer, der eksempelvis kan detektere mistænkelige mønstre i nettrafik, som kan være tegn på sikkerhedshændelser.

Dansk Erhverv finder, at det er en for unuanceret tilgang, når lovforslaget fokuserer alene på CFCS egne systemer.

Dansk Erhverv opfordrer til at undersøge andre muligheder, fx tættere samspil mellem CFCS og den enkelte virksomhed om allerede etablerede systemer. Det er i det hele taget oplagt at satse på et samarbejde, rammer og evt. krav for de systemer virksomhederne benytter, frem for alene at fokusere på at installere CFCSs egne teknologier som CFCS kontrollerer.

**Persondataforordningen og lov om Center for Cybersikkerhed**
De virksomheder der omfattes at den forslåede ordning skal overfor de personer, de behandler personoplysninger om være i stand til at oplyse, at de indgår i CFCS overvågning. Oplysninger om personer registret hos de omfattede virksomheder vil efter Dansk Erhvervs vurdering skulle informeres i henhold til GDPR. Derfor opfordrer Dansk Erhverv Forsvarsministeriet til at bistå til

dette ved at udarbejde en standard informationstekst med ministeriet som afsender, som virksomheder kan anvende og lade indgå i deres eksisterende persondatapolitikker

Persondataforordningen stilles skærpede krav om sikkerhed i forhold til behandling af personoplysninger, hvilket betyder at mange virksomheder over de seneste år har investeret betydeligt i at opdaterer deres it-sikkerhed. Det er således helt oplagt at tænke i løsninger, der spiller sammen med allerede implementerede sikkerhedsforanstaltninger.

**Andre bemærkninger**
Processen med persondataforordningen har medført en ny og anderledes samtale om persondata i samfundet. Fra direktionslokalet til kakkelbordet, og det er grundlæggende sundt. Det aktuelle lovforslag står i kontrast til dette, og ville efterlade tilsluttede virksomheder med et forklaringsproblem over for ansatte, kunder og samarbejdspartnere. Det kan i sidste ende få negative konsekvenser for den enkelte virksomheder, og for Danmark som land for investeringer og teknologiudvikling.

Dansk Erhverv mener den offentlige sektor - som landets ubetinget største dataansvarlige og den dataansvarlige, der behandler flest personfølsomme og fortrolige personoplysninger - bør gå forrest og vise vejen for korrekt og etisk behandling af personoplysninger. Det gælder ikke mindst Center for Cybersikkerhed.

It-kriminalitet er et globalt fænomen, som vi så det med angrebene, der forrige år hærgede lande over hele verden, og som lagde tusindvis af it-systemer ned. Ingen enkeltaktør kan håndtere denne udfordring alene - hverken nogen enkelt virksomhed eller nogen stat. Udfordringen kræver derfor et samarbejde mellem offentlige og private spillere, og det kræver et internationalt samarbejde som i sidste ende globalt. Det var i det lys, at Dansk Erhverv bakkede op om en ”digital genevekonvention” (sommeren 2017), som oprindeligt foreslået af Brad Smith, president and chief legal officer, Microsoft.

Der er behov for en vifte at indsatser, og det er afgørende at der sker som ligebyrdigt samspil mellem offentlige og private spillere, og i et samarbejde hvor viden går begge veje. Der er andre måder at dele viden med CFCS end at give CFCS beføjelser til påbud og vidtrækkende dataadgang med CFCS som den kontrollerende part. Dansk Erhverv mener, at Rådet for Digital Sikkerhed kan spille en vigtig rolle som brobygger her, lige som Dansk Erhverv selvfølgelig selv står til rådighed med vores dialog med erhvervslivet.

Med venlig hilsen

Janus Sandsgaard
Fagchef for it og digitalisering