DANSK ERHVERV
Børsen
1217 København K

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

Forsvarsministeriet
Att.: Lea Møberg Kristensen
Holmens Kanal 9
1060 København K

Den 17. februar 2022

Høring: Den private sektors samarbejde med CFCS

Hermed afgives Dansk Erhvervs høringssvar vedr. samarbejdet mellem den private sektor og Center for Cybersikkerhed (CFCS).

Generelle bemærkninger
Dansk Erhverv ser nogle overordnede problemstillinger ift. samarbejdet mellem CFCS og private virksomheder. Dette skyldes ikke manglende vilje til samarbejde på den ene eller anden side. Den organisatoriske placering af centeret har – på trods af de mulige fordele, placeringen medfører – flere negative konsekvenser for samarbejdet med den private sektor, hvilket både gælder virksomheder i den kritiske infrastruktur og erhvervslivet bredere set. Derfor mener Dansk Erhverv, at en opsplitning af CFCS vil styrke samarbejdet.

CFCS råder over dygtige og engagerede medarbejdere, stor viden og ressourcer – derfor mener vi, at et stærkere samarbejde mellem CFCS og dansk erhvervsliv bør prioriteres højt, og at de mulige negative konsekvenser af en organisatorisk opsplitning vil blive opvejet af de positive effekter af et bedre samarbejde.

Specifikke bemærkninger
De specifikke bemærkninger er organiseret efter de opstillede spørgsmål i høringsmailen.

<u>Hvad fungerer godt i samarbejdet med CFCS mht. den virksomhedsrettede indsats?</u>
Dansk Erhvervs medlemmer beretter om dygtige og engagerede medarbejdere i CFCS, og som organisation har samarbejdet mellem CFCS og Dansk Erhverv også været præget af et gensidigt ønske om at arbejde for at sikre Danmark og danske virksomheder bedre mod cybertrusler.

Fra Dansk Erhvervs medlemmer har der også været en positiv anerkendelse af, at CFCS til tider har udfyldt en opsøgende rolle og proaktivt varslet virksomheder om fx Solar Winds-angrebet. Flere af de vejledninger og nogle af trusselsvurderingerne, CFCS' udarbejder, er af udmærket kvalitet, men indholdet giver ikke umiddelbart anledning til at retfærdiggøre CFCS' placering i FE, da disse bygger på kendt viden og dermed lige så godt kunne udfærdiges af en civil styrelse el. lign., ligesom aktualiteten af trusselsvurdering kritiseret (jf. nedenfor).

Fra medlemmer i den kritiske infrastruktur har der desuden været ros til CFCS' medarbejdere ifm. gennemførte PEN-test.

Hvilke udfordringer opleves i relation til CFCS mht. den virksomhedsrettede indsats?
Når der til trods for ovenstående positive elementer, som fremhæves blandt Dansk Erhvervs medlemmer, fortsat opleves udfordringer i CFCS' samarbejde med den private sektor, bunder mange af de frustrationer, vores medlemmer giver udtryk for, i en organisationskultur, som er stærkt præget af at være placeret som en del af Forsvarets Efterretningstjeneste (FE).

Derudover er der en uklarhed om, hvad centerets rolle ift. erhvervslivet er – det opfattes af vores medlemmer som meget vagt defineret, hvilket gør det vanskeligt at få klarhed for, hvad centerets bundne leverancer til virksomhederne er – særligt for den del af erhvervslivet, som ikke er en del af landets kritiske infrastruktur.

Der er ligeledes en udfordring ift. de i medierne omtalte sager vedr. spionage mod tætte allierede, samarbejde med NSA m.v., hvilket uheldigvis skaber mistro mod efterretningsvæsnet i nogle dele af erhvervslivet. Fra topledelses- og bestyrelsesniveau kommer i nogle tilfælde meldinger om, at man naturligvis skal samarbejde med myndighederne, men at man ikke ønsker at blive associeret med FE/CFCS. Dette kan især gøre sig gældende hos virksomheder, der har kunder og/eller samarbejdspartnere i de lande, hvor efterretningssamarbejdet har været genstand for kritik.

Videndeling og trusselsvurderinger
Placeringen af centeret under FE vurderes at have en negativ indvirkning på CFCS-medarbejdernes mulighed for at dele viden med private virksomheder. Oplysninger, der kommer ind til CFCS, hemmeligstemples i et omfang, der bl.a. betyder, at virksomhederne ikke kan få adgang til de informationer, de selv har meldt ind til centeret.

Det bemærkes, at flere medlemmer giver udtryk for, at CFCS' trusselsvurderinger ikke er fyldestgørende, og at virksomhederne fortsat finder det nødvendigt at bruge mange ressourcer på at indkøbe mere tidssvarende og detaljerede trusselsvurderinger på det private marked. CFCS' trusselsvurderinger opfattes af nogle som utidssvarende – fx er centerets vurdering af truslen fra statsstøttede destruktive cyberangreb fortsat lav, selvom flere stemmer har gjort opmærksom på, at det aktuelle konfliktniveau i Europa faktisk har medført en stigende trussel. Den seneste trusselvurdering på dette område er i øvrigt fra sommeren 2021.

Sensornetværk
CFCS' sensornetværk mødes generelt med skepsis blandt medlemmer af Dansk Erhverv. Vores medlemmer oplever det som en "black box", og spørger retorisk, om der er nogen andre former for samarbejdspartnere, man som erhvervsdrivende ville tillade at installere den slags probe uden at vide, hvilke oplysninger, der indhentes, hvad de bruges til osv., ligesom der ikke opleves nogen gevinst for virksomhederne ved at blive koblet op på sensornetværket.

Vores medlemmer oplever, at CFCS har meget stort fokus på at tilskynde virksomheder til at koble sig på sensornetværket. I erhvervslivet er der en aversion mod at takke ja til så indgribende tilbud fra en myndighed, som 1) af efterretningsmæssige hensyn ikke deler nok viden med erhvervslivet,

og 2) for telesektoren også er tilsynsmyndighed, som kan sanktionere virksomheder, efter de har fået massivt indblik i de pågældende virksomheder.

Hertil er der den bekymring ved et bredt sensornetværk, som både skal placeres på yder- og indersiden af virksomhedernes net, at det risikerer at skabe et potentielt *single point of failure* i hele Danmarks kritiske infrastruktur. CFCS vil skulle placere ukendt udstyr i it-infrastrukturen, som introducerer mulige sårbarheder for, at virksomheder kan angribes og overvåges, hvis systemet kompromitteres – sektioneringen i den danske infrastruktur kompromitteres på den måde.

Telesektoren
Der er en bred opfattelse blandt virksomheder i telesektoren af, at sammenblanding af tilsynsmyndighed og efterretningsvæsen er uhensigtsmæssig. Teleområdet lægger ressortmæssigt i Klima-Energi- og Forsyningsministeriet (Energistyrelsen) og Erhvervsministeriet (Erhvervsstyrelsen). Dertil kommer tilsynsrollen, der ligger i Forsvarsministeriet (FMN), hvilket giver en unødvendig fragmentering af forvaltningen.

Vores medlemmer er kritiske overfor, at tilsynet med telesektoren er lagt i en forvaltningsmyndighed under Forsvarets Efterretningstjeneste og ikke som al anden erhvervsrettet lovgivning i den civile del af forvaltningen. Dette medfører, at reguleringen af telesektoren på dette område ikke ses i sammenhæng med den øvrige regulering, og at selskaberne ikke har den nødvendige sikkerhed for inddragelse af andre samfundshensyn end militære strategiske sikkerhedshensyn.

Derudover nævnes CFCS' mulighed for at give virksomheder påbud ift. deres it-drift. Det gælder fx ift. patching. Patching på uhensigtsmæssige tidspunkter kan i sig selv medføre sikkerhedsbrister og/eller driftsnedbrud, men centeret har ikke kompetencer til at udbedre eventuelle skader og/eller kan ikke holdes økonomisk ansvarlige for skader, der sker som følge at et påbud.

<u>Hvordan kan eventuelle ovenstående udfordringer løses?</u>
En væsentlig kilde til ovenstående udfordring ligger i CFCS' organisatoriske placering som en del af FE – og for telesektoren giver dobbeltrollen som tilsynsmyndighed og efterretningstjeneste yderligere udfordringer. Hensigten med at placere CFCS under FE for at få adgang til FE's viden om det internationale trusselsbillede m.v. har muligvis været god, men det er Dansk Erhvervs opfattelse, at dette mål er opnået på bekostning af muligheden for at dele disse oplysninger med både virksomhederne i Danmarks kritiske infrastruktur og erhvervslivet generelt.

Ift. telesektoren er det overordnede løsningsforslag, vi har hørt fra mange medlemmer og som Dansk Erhverv har været fortaler for, at CFCS får en stærkere civil forankring. Dette kan fx ske ved en organisatorisk opsplitning, hvor bl.a. de opgaver, der knytter sig til CFCS' rolle som tilsynsmyndighed for telesektoren, adskilles fra efterretningstjenesten. Denne enhed kan med fordel placeres i Erhvervsstyrelsen, men kan også være en mulighed med en civil enhed i Forsvarsministeriet. Placering af enheden i Forsvarsministeriet kan muligvis gøre det lettere at samarbejde om udveksling af informationer fra FE-delen af CFCS, da begge enheder i så fald vil ligge i samme ministerium.

En organisatorisk opsplitning vil medføre, at der vil være en langt mere åben og civil relation og dermed et langt mere produktivt samarbejde. Det er vigtigt at pointere, at erhvervslivet gerne vil samarbejde med efterretningstjeneste og levere data, når det er i interesse for nationens sikkerhed.

Ønsket om en opsplitning eller en mere selvstændig civil myndighed, bunder i et ønske om, at rådgivning, koordination og interaktion generelt i forbindelse med trusler, angreb og efterforskning foregår i en civil ånd og dermed skaber værdi for virksomhederne.

Hvilke tiltag vil kunne styrke CFCS' virksomhedsrettede indsats?
Dansk Erhverv mener, at en reorganisering af CFCS vil være det mest effektive tiltag for at styrke CFCS' virksomhedsrettede indsats. Derudover kan det overvejes at

Lovændring ift. Lov om Center for Cybersikkerhed – fx en oplysningspligt – kan gøre det muligt at dele viden, hvilket lige nu er vanskeligt pga. de særlige regler, der gælder for efterretningstjenesten. Her kan der med fordel ses mod praksis i UK, hvor man arbejder med hurtig de-klassificering af størstedelen af efterretninger, så de kan deles med virksomheder.

Derudover kan det bemærkes, at de nuværende undtagelser fra offentlighedsloven og forvaltningsloven bør fjernes, så den civile del er underlagt de almindelige forvaltningsretlige regler. Såvel offentlighedsloven som forvaltningsloven indeholder tilstrækkelige muligheder for, at myndighederne kan undtage efterretningsoplysninger, der kan skade den danske stat, hvis de bliver genstand for aktindsigt og partshøring, og dermed er undtagelsen ikke nødvendig.

Dansk Erhverv har i samarbejde med Rådet for Digital Sikkerhed stillet forslag på anmodning fra FMN om, at CFCS kan styrke sin opgaveløsninger med at udgive mere operationelle trusselsvurdering. Dette arbejde kan med fordel udføres i samarbejde med it-sikkerhedsvirksomheder, aftagere og relevante erhvervsorganisationer.

Derudover kan et stærkere internationalt samarbejde m. fx Europol være med til at løfte kvaliteten af CFCS' trusselsvurdering. OSINT-dashboardet fremhæves som en god ressource til trusselsinformation, og et samarbejde kunne dreje sig om at lave regionale eller nationale versioner af OSINT og gøre det tilgængeligt for virksomheder.

Dansk Erhverv sætter pris på at være blevet hørt i denne vigtige sag og står til rådighed for uddybning af ovenstående.

Med venlig hilsen,

Christian von Stamm Jonasson
Chefkonsulent