FORSVARSMINISTERIET

BILAGSOVERSIGT

BILAG 1	Kommissorium for analyse af CFCS' forankring ved FE
BILAG 2	Detaljeret overblik: erhvervs- og brancheorganisationernes erfaringer med CFCS
BILAG 3	Høringssvar fra Dansk Erhverv
BILAG 4	Høringssvar fra Dansk Industri
BILAG 5	Høringssvar fra IT-Branchen
BILAG 6	Høringssvar fra Rådet for Digital Sikkerhed
BILAG 7	Høringssvar fra de private medlemmer af Cybersikkerhedsrådet
BILAG 8	Høringssvar fra Industriens Fond
BILAG 9	Høringssvar fra Teleindustrien
BILAG 10	Høringssvar fra SMVdanmark
BILAG 11	Høringssvar fra NRGi og Finans Danmark (i egenskab af deres tidligere medlemskab af Virksomhedsforum for Digital Sikkerhed)

FORSVARSMINISTERIET

BILAG 1

FORSVARSMINISTERIET

Kommissorium

Virksomhedsindsatsen på cybersikkerhedsområdet

Formål
Regeringen og forsvarsforligspartierne ønskede med *Aftale om et Styrket Cyberforsvar* (24. juni 2021) at styrke Danmarks robusthed over for cyberangreb. Med aftalen blev det besluttet at igangsætte en analyse af Center for Cybersikkerheds (CFCS) forankring under Forsvarets Efterretningstjeneste (FE), herunder fordele og ulemper ved at lægge en del af virksomhedsindsatsen i en selvstændig enhed under Forsvarsministeriet:

> *"For at kunne evaluere og styrke CFCS' virke med særligt fokus på at øge den samlede indsats over for den private sektor, igangsættes en analyse af CFCS' forankring under FE, herunder fordele og ulemper ved at lægge en del af virksomhedsindsatsen i en civil enhed på Forsvarsministeriets område. Analysen skal foreligge inden sommeren 2022, idet en delrapport om rådgivning og uddannelse skal foreligge i efteråret 2021."*[1]

Baggrund
For at styrke Danmarks beskyttelse mod cyberangreb blev CFCS oprettet den 18. december 2012 som en del af FE. Baggrunden for placeringen af CFCS ved FE var et ønske om at opnå synergieffekter i form af eksempelvis udnyttelse af FE's viden inden for it-sikkerhedsområdet, viden om det internationale trusselsbillede på cyberområdet samt særlig adgang til efterretninger om cybertrusler fra udlandet.

Udviklingen inden for cybersikkerhed går stærkt, og truslen har udviklet sig løbende. Det har affødt et stadigt stigende behov for robuste løsninger, og CFCS har på den baggrund gennem en årrække udvidet både sin kapacitet og sin opgaveportefølje.

CFCS arbejder bredspektret med at opdage, analysere og varsle om truslen og vedligeholde et nationalt situationsbillede. CFCS rådgiver myndigheder og virksomheder om de organisatoriske og tekniske foranstaltninger, der skal til for at skabe robusthed. Og når uheldet er ude, kan CFCS bistå myndigheder og virksomheder.

CFCS arbejder desuden tæt sammen med de samfundsvigtige sektorer og erhvervslivet gennem fælles videndelingsnetværk, Cybersikkerhedsrådet, Strategisk Samarbejdsforum for Cybersikkerhed og bidrager til arbejdet i Virksomhedsforum for Digital Sikkerhed. Som led i denne indsats varsler CFCS om cyberangreb, aktuelle trusler og sårbarheder med konkrete tekniske anbefalinger for både myndigheder og virksomheder. Hertil udgiver CFCS vejledninger, trusselsvurderinger og undersøgelsesrapporter - eksempelvis om passwords, phishing, ransomware, logning og hjemmearbejde under COVID-19.

I forlængelse af etableringen af CFCS og den voksende portefølje har en række aktører udtrykt bekymring over, om CFCS' organisering er tilstrækkelig befordrende for videndeling og åbenhed, herunder ift. CFCS placering under FE. Dertil kommer spørgsmål om CFCS' rolle på

[1] Aftale om et styrket cyberforsvar. 24. juni 2021. https://fmn.dk/da/nyheder/2021/enighed-om-et-styrket-dansk-cyberforsvar/

teleområdet, hvor CFCS fungerer som både IT-sikkerhedsmyndighed, kompetencecenter og tilsynsmyndighed.

På den baggrund er der politisk ønske om at evaluere og styrke CFCS' virke med særligt fokus på at øge den samlede indsats over for den private sektor, herunder så det sikres, at der sker bedst mulig videndeling, og at rådgivning og vejledning kommer til nytte hos flest mulige virksomheder, herunder også SMV'er.

Opgaven
Der skal på den baggrund udarbejdes en analyse af CFCS, herunder med fokus på samarbejdet med private virksomheder for derigennem at understøtte, at der findes holdbare løsninger, som gør virksomhederne bedst mulig i stand til at løfte ansvaret for deres egen cybersikkerhed. Følgende forhold belyses i analysen:

1) Første del af analysen kortlægger CFCS' ansvar og opgaver og snitflader til øvrige relevante myndigheder (Erhvervsstyrelsen, Sikkerhedsstyrelsen, PET, Rigspolitiet, Digitaliseringsstyrelsen) i forhold til cybersikkerheden i Danmark fokuseret på den virksomhedsrettede indsats i hele den private sektor – herunder samfundsvigtige virksomheder.
    a. Som led i ovenstående, analyseres de særlige opgaver og beføjelser, som CFCS er tillagt i forhold til telesektoren. Her vil det specifikt blive belyst, hvilke fordele og ulemper, herunder i forhold til gældende sektorlovgivning og til de nuværende særlige lovgivningsmæssige undtagelser for CFCS, der vil være ved flytning af denne virksomheds- og sektorrettede opgave til en civil enhed på Forsvarsministeriets område.
2) Anden del af analysen evaluerer CFCS' opgavevaretagelse i forhold til den private sektor. Evalueringen skal afdække, hvad der fungerer godt i opgaveløsningen, og hvad der med fordel kan gøres anderledes i relation til CFCS' lovbundne og øvrige opgaver. Analysen skal pege på mulige tiltag, som vil kunne bidrage til at styrke den samlede indsats over for virksomheder, herunder SMV'er på cybersikkerhedsområdet.
3) Sidste del af analysen redegør for fordele og ulemper ved CFCS' forankring under FE mht. samarbejdet med den private sektor, herunder fordele og ulemper ved at placere en del af CFCS' virksomhedsindsats uden for FE. Herunder vurderes hensigtsmæssigheden af forskellige typer af civile enheder på Forsvarsministeriets område.

Analysen vil bygge på bidrag, og eventuelt opfølgende kvalitative interviews, fra relevante myndigheder, brancheorganisationer, forskere og eksperter samt sammenlignelige landes arbejde med cybertruslen. Forsvarsministeriet faciliterer analysen.

Der nedsættes en tværministeriel følgegruppe bestående af relevante myndigheder. Der vil ligeledes blive indsamlet relevante udenlandske erfaringer i forhold til forskellige modeller for national forankring af cybersikkerhedsområdet.

Et udkast til analysen vil blive gjort til genstand for høring blandt de primære interessenter, herunder brancheorganisationer, Cybersikkerhedsrådet og Virksomhedsforum for Digital Sikkerhed.

Analysen skal foreligge inden sommerferien 2022.

FORSVARSMINISTERIET

BILAG 2

FORSVARSMINISTERIET

DETALJERET OVERBLIK – ERHVERS- OG BRANCHEORGANISATIONERNES ERFARING MED CFCS

Anden del af analysen har til formål at evaluere CFCS' opgavevaretagelse i forhold til den private sektor og pege på mulige tiltag, som vil kunne bidrage til at styrke indsatsen over for virksomheder. Forsvarsministeriet har på den baggrund hørt en række erhvervs- og brancheorganisationer om deres erfaring med og perspektiver på CFCS' arbejde i relation til den private sektor.

Dertil har CFCS bidraget med erfaringer med- og perspektiver på deres virksomhedsrettede samarbejde og opgaver med udgangspunkt i samme spørgsmål.

Forsvarsministeriet har modtaget høringssvar fra Dansk Erhverv, Dansk Industri, IT-Branchen, Rådet for Digital Sikkerhed, de private medlemmer af Cybersikkerhedsrådet, Industriens Fond, Teleindustrien og SMVdanmark. NRGi og Finans Danmark har desuden afgivet høringssvar i egenskab af deres tidligere medlemskab af Virksomhedsforum for Digital Sikkerhed.

I dette bilag har Forsvarsministeriet samlet og sammenskrevet erfaringerne fra høringssvarene for at give et overblik over perspektiver, behov og foreslåede tiltag. På punkter, hvor erhvervs- og brancheorganisationerne udtrykker ensartede perspektiver er disse skrevet sammen, mens selvstændige pointer så vidt muligt er bibeholdt med deres oprindelige ordlyd. I flere høringssvar nævnes områder, der ikke relaterer sig til CFCS' ansvarsområde. Disse passager er som udgangspunkt ikke medtaget. Nærværende fremlæggelse af tilkendegivelser fra høringssvarene har været sendt til de respektive høringsparter med henblik på at sikre korrekt repræsentation af deres synspunkter. De enkelte høringssvar kan ses af bilag 6 til 14.

Det følgende afsnit er tematisk struktureret. Den første del af afsnittet fokuserer på erhvervs- og brancheorganisationernes erfaringer med CFCS, herunder CFCS' generelle virke, CFCS' vejledning og trusselvurderinger, indsamling af data, videndeling og informationsflow samt uklarhed om ansvar og roller. Anden del af afsnittet omhandler løsninger og tiltag i relation til den private sektor, herunder behov og ønsker, holdninger og forslag i relation til en mulig organisatorisk opsplitning. Til sidst fremsættes interessenternes perspektiver og behov for så vidt angår CFCS' relation til telesektoren.

ERHVERVS- OG BRANCHEORGANISATIONERNES ERFARINGER MED CFCS

Erhvervs- og brancheorganisationerne er blevet bedt om at forholde sig til oplevelserne med CFCS' virksomhedsrettede indsats for så vidt angår det, der fungerer godt i samarbejdet samt de udfordringer, der måtte opleves.

CFCS' generelle virke

Af høringssvarene fremgår det, at en stor del af organisationerne anerkender CFCS' arbejde med at styrke den danske cybersikkerhed, og at virksomheder med samfundsvigtige funktioner mødes af en høj faglighed i CFCS.

Dansk Erhverv (DE), **IT-branchen (ITB)**, **Rådet for Digital Sikkerhed (RfDS)**, **Dansk Industri (DI)** og de private medlemmer af **Cybersikkerhedsrådet** oplever en høj faglighed og stærke kompetencer på cyberområdet i CFCS. Der er enighed om, at CFCS spiller en vigtig rolle i beskyttelsen af Danmark og danske interesser mod cybertruslen og i at styrke den danske cybersikkerhed.

RfDS og **DI** konstaterer, at CFCS spiller en vigtig rolle i den offentlige debat og kvitterer for CFCS' villighed til at stille op til konferencer, i netværk og lignende for at udbrede viden om cybertruslen. **Industriens Fond (IF)** oplever en god villighed fra CFCS' side til at række ud og deltage i projekter og tiltag, der ligger på kanten af kerne-opgaveporteføljen for CFCS. **DE** konstaterer, at deres medlemmer anerkender, at CFCS til tider udfylder en opsøgende rolle og proaktivt varsler virksomheder om fx Solar Winds-angrebet. **DI** nævner, at der blandt **DI**'s medlemmer i samfundskritiske sektorer også er flere positive oplevelser af hjælpen fra CFCS i forbindelse med enkeltstående angreb på virksomheden.

Teleindustrien (TI) og **ITB** bemærker, at CFCS står til rådighed for branchernes selskaber og er tilgængelig for dialog, hvilket er med til at styrke samarbejdet. Hertil roser **ITB** CFCS for sine udadvendte, virksomhedsrettede aktiviteter.

CFCS' vejledning og trusselsvurderinger

Blandt høringssvarene fremgår der forskellige perspektiver på anvendeligheden af CFCS' vejledning samt trusselsvurderinger for de private virksomheder. Samtidig understreges det, at CFCS' opgaver ikke må være konkurrenceforvridende.

ITB, **RfDS**, **Finans Danmark (FD)** og de private medlemmer af **Cybersikkerhedsrådet** anerkender generelt CFCS for deres arbejde med vejledninger, rapporter og trusselsvurderinger, som er et vigtigt bidrag i forhold til at højne opmærksomheden omkring cyber- og informationssikkerhed i de private virksomheder. Samtidig bemærker de private medlemmer af **Cybersikkerhedsrådet**, at meget af denne information dog forudsætter, at der i virksomheder er dedikerede ressourcer til at forstå og tolke meldingerne for CFCS, hvilket ikke er tilfældet i alle dele af SMV-segmentet.

TI bemærker, at processen omkring clearing og nedklassifikation af informationer i FE af og til er en barriere og forsinkende faktor for deling af informationer til virksomhederne i forbindelse med eksempelvis trusselvurderinger eller informationer om specifikke hændelser af særlig relevans. **DE** og **RfDS** finder, at indholdet af CFCS' vejledninger og trusselsvurderinger ikke umiddelbart retfærdiggør CFCS' placering i FE, da indholdet bygger på kendt viden

og dermed lige så godt kunne udfærdiges af en civil styrelse eller lignende. **DE** finder overordnet ikke CFCS' trusselsvurderinger fyldestgørende, og **DE**'s medlemmer finder det fortsat nødvendigt at bruge mange ressourcer på at indkøbe mere tidssvarende og detaljerede trusselsvurderinger på det private marked.

DI fremhæver, at det i forbindelse med ændringen af CFCS-loven i 2019 blev besluttet, at CFCS skulle tildeles midler til udarbejdelse af forebyggende it-sikkerhedsydelser, som fx penetrationstest. **DI** understreger, at dette også tilbydes på det private marked, og **DI** finder det derfor konkurrenceforvridende. **DI** mener, at det i vurderingen af CFCS' samarbejde med den private sektor er en vigtig faktor, at de fremadrettede opgaver ikke er opgaver, der allerede løftes af andre.

Indsamling af data, videndeling og informationsflow

CFCS' viden og dataindsamling er et gentagende tema blandt størstedelen af høringssvarene. Der lader til at være en forskellig afvejning blandt organisationerne mellem fordelen ved CFCS' adgang til efterretninger og efterspørgslen på en højere grad af videndeling med de private virksomheder.

ITB, **DI, FD** og **DE** bemærker, at CFCS' nuværende placering giver CFCS en unik, direkte adgang til viden om trusselsbilledet på cyberområdet, herunder særlig adgang til efterretninger om cybertrusler fra udlandet. Samtidig påpeger **ITB**, **DI**, **DE**, **TI** og **RfDS**, at CFCS' placering ved FE udfordrer et gensidigt, operativt samarbejde mellem CFCS og de private virksomheder, fordi CFCS' efterretningsbaserede oplysninger er klassificerede. Virksomhederne oplever, at de skal udlevere så meget information som muligt til CFCS, mens CFCS er tilbageholdende med deling af information og viden den anden vej. **RfDS** pointerer, at det ikke er hensigtsmæssigt, at CFCS på den ene side er meget kompetent og har adgang til gode datakilder grundet placeringen ved FE, hvis sådanne oplysninger på den anden side ikke kan stilles til rådighed for erhvervslivet i bred forstand.

DI bemærker, at den tætte relation til forsvaret har fået virksomheder til at fravælge CFCS – eksempelvis tilslutning til netsikkerhedstjenesten. **DE**, **ITB, DI** og **RfDS** påpeger en tilbageholdenheden fra virksomheder i forhold til at tilslutte sig CFCS' sensornetværk grundet manglende gennemsigtighed om brugen af data og for lidt oplevet udbytte af at være tilsluttet.

DE og **RfDS** finder, at organisationskulturen i CFCS er stærkt præget af placeringen ved FE, hvilket vurderes at skabe udfordringer i samarbejdet med den private sektor. De private medlemmer af **Cybersikkerhedsrådet** ser ikke placeringen af CFCS' virksomhedsrettede indsats som årsagen til udfordringer med eksempelvis deling af information. I stedet opfattes udfordringerne relateret CFCS' tilgang til samarbejdet med private virksomheder.

DE bemærker, at de aktuelle sager vedr. spionage mod tætte allierede, samarbejde med NSA m.v. i medierne uheldigvis skaber mistro mod efterretningsvæsenet i nogle dele af erhvervslivet. Hertil bemærker **DE**, at de på den baggrund møder forbeholdenhed fra topledelses- og bestyrelsesniveau overfor at blive associeret med FE/CFCS.

DE påpeger, at CFCS' mulighed for at give virksomheder påbud i forhold til deres it-drift kan give udfordringer. **DE** eksemplificerer det med påbud om patching, da patching på uhensigtsmæssige tidspunkter i sig selv kan medføre sikkerhedsbrister og/eller driftsnedbrud.

Her pointerer **DE**, at CFCS ikke har kompetencer til at udbedre eventuelle skader og/eller kan holdes økonomisk ansvarlige for skader, der sker som følge at et påbud.

Uklarhed om ansvar og roller

Høringssvarene bærer præg af, at der er uklarhed om ansvarsfordelingen blandt myndighederne på hele cyberområdet. For mange virksomheder står det ikke klart, hvad de kan forvente af hjælp og støtte fra CFCS. Samtidig forholder flere af høringssvarene sig til opgaver uden for CFCS' ansvarsområde, såsom cyberkriminalitet og efterforskning, hvilket indikerer, at der ikke er tilstrækkelig indsigt i myndighedernes forskellige opgaveporteføljer.

DE, DI og **IF** angiver, at der er uklarhed om CFCS' rolle i forhold til erhvervslivet – særligt virksomheder uden for den kritiske infrastruktur, herunder opgavefordelingen mellem CFCS og Erhvervsstyrelsen. **RfDS** understreger, at flere aktører har haft en urealistisk forventning om, at CFCS kan "redde" virksomheder, der har været udsat for et cyberangreb, og at det derfor er nødvendigt, at CFCS' rolle over for private virksomheder præciseres. **DI** angiver, at rollefordelingen på tværs af de mange myndigheder, der i Danmark er inde over cyberdomænet – fx mellem politiet, Digitaliseringsstyrelsen, Erhvervsstyrelsen og CFCS – opleves som uklar.

DI mener, at rollefordelingen og myndighedssamarbejdet grundlæggende skal give borgerne og virksomhederne mest mulig cybersikkerhed for pengene. **DI** stiller spørgsmålstegn ved, om det sker bedst ved at holde fast i sektoransvarsprincippet, og hvad **DI** oplever som ressortkampe, uklar rollefordeling, manglende prioritering og koordination etc., eller om arbejdet med cybersikkerhed i den offentlige sektor skal centraliseres som fx Finland eller Israel har gjort.

BEHOV, LØSNINGER OG TILTAG

Erhvervs- og brancheorganisationerne er i deres høringssvar blevet bedt om at svare på, hvad der kan imødegå de udfordringer, der peges på i relation til CFCS' samarbejde med den private sektor og hvilke tiltag, der vil kunne styrke CFCS' virksomhedsrettede indsats. Her bliver det nævnt, at en højere grad af gennemsigtighed, operativ videndeling, afklassificering af oplysninger og en større SMV-indsats vil kunne øge og styrke samarbejdet med den private sektor.

Tillid og gennemsigtighed

RfDS, **ITB, DI** og **TI** understreger, at gensidig tillid mellem den private sektor og CFCS er afgørende. **RfDS** bemærker hertil, at der er behov for et mere formaliseret samarbejde med de konkrete virksomheder og en national myndighed, således at der kan laves mere konkret erfaringsudveksling, opbygges tillid på forhånd og sikres en passende gennemsigtighed om selve samarbejdsrelationen.

ITB påpeger, at der er behov for større åbenhed omkring, hvad CFCS ønsker at bruge indsamlet data fra virksomhederne til, hvis der skal skabes en tillidsfuld og værdiskabende relation mellem parterne. I lighed hertil bemærker **DI**, at virksomhederne efterspørger større klarhed og gennemsigtighed om de kriterier CFCS, som eksempelvis telemyndighed, kan fremsætte.

Konkret og operativ videndeling

Flere interessenter fremhæver et behov for mere konkret og operativ videndeling fra CFCS. De private medlemmer af **Cybersikkerhedsrådet** vurderer eksempelvis, at der er behov for en styrkelse af CFCS' operative samarbejde med de private virksomheder og behov for, at CFCS går væsentligt længere med informationsdeling end hidtil. **NRGi** bemærker, at der er behov for, at CFCS oftere varsler og deler viden.

ITB mener, at der er behov for at gentænke både indhold og formidlingsformat for viden og vejledninger på cybersikkerhedsområdet samt hvem, der er den rette afsender, hvis der skal nås bredt ud til erhvervslivet. I den sammenhæng påpeger **ITB**, at det ikke vil være tilstrækkeligt med tilgængelig viden på en hjemmeside.

I relation til samarbejdet mellem CFCS og it-sikkerhedsbranchen ser **DI** et behov for et mere formaliseret samarbejde om fx systematisk deling af information, end den ad-hoc praksis, **DI** oplever i dag.

Konkrete forslag

- **DE** og **RfDS** foreslår, at CFCS udgiver mere operationelle trusselsvurderinger, hvilket med fordel kan udføres i samarbejde med it-sikkerhedsvirksomheder, aftagere og relevante erhvervsorganisationer.

- **DE** mener, at et stærkere internationalt samarbejde med fx Europol kan være med til at løfte kvaliteten af CFCS' trusselsvurdering. **DE** fremhæver OSINT-dashboardet som en god ressource til trusselsinformation, og foreslår at der samarbejdes om at lave regionale eller nationale versioner af OSINT, som kan være tilgængelige for virksomheder.

<u>Klassificering af oplysninger</u>

DI bemærker, at leverandørerne ikke oplever, at det i dag er muligt at drage nytte af den værdi, der ligger i, at CFCS er placeret ved FE. **RfDS**, **DI**, **ITB**, **DE** og de private medlemmer af **Cybersikkerhedsrådet** påpeger behovet for at de-klassificere oplysninger for at imødekomme en større informationsdeling og videndeling med virksomhederne, så virksomhederne i højere grad kan modtage aktuel og relevant/vedkommende viden, der kan bruges operationelt i virksomhedernes egne, konkrete trusselsvurderinger og sikkerhedsforanstaltninger.

Konkrete forslag

- **IF** foreslår, at CFCS' viden om hændelser og trusler formidles i en mere tilgængelig form – fx via andre aktører – til virksomhederne.

- **DE** foreslår, at man ser mod praksis i UK, hvor man arbejder med hurtig de-klassificering af størstedelen af efterretninger, så de kan deles med virksomheder.

- De private medlemmer af **Cybersikkerhedsrådet** foreslår, at CFCS i samarbejde med private sikkerheds- og rådgivningsvirksomheder finder en model for deling af klassificeret information, som eksempelvis kan tage udgangspunkt i den norske kvalitetsordning for leverandører som håndterer IKT-hændelser.

    - I tillæg foreslås det, at virksomheder kunne få medarbejdere godkendt til at modtage klassificerede informationer.

- **DE** bemærker, at de nuværende undtagelser fra offentlighedsloven og forvaltningsloven bør fjernes, så den civile del er underlagt de almindelige forvaltningsretlige regler. Ifølge **DE** indeholder offentlighedsloven og forvaltningsloven tilstrækkelige muligheder for, at myndighederne kan undtage efterretningsoplysninger fra aktindsigt og partshøringer.

- **DE** foreslår, at en lovændring i forhold til CFCS-loven – fx en oplysningspligt – kan overvejes, så det i højere grad er muligt at dele viden.

Virksomhedsindsats og indsatsen overfor SMV'er

ITB og de private medlemmer af **Cybersikkerhedsrådet** bemærker, at der er behov for at styrke det civile arbejde med cybersikkerhed og i højere grad hjælpe de danske virksomheder med at løfte opgaven i forhold til cyberbeskyttelse ved at styrke samarbejdet mellem offentlige og private sikkerhedskompetencer. **DI** bemærker, at den virksomhedsrettede indsats i CFCS, som ikke er målrettet samfundskritiske sektorer eller virksomheder med samfundsvigtige funktioner, bør være en tydeligt prioriteret opgave.

SMVdanmark, **FD** og de private medlemmer af **Cybersikkerhedsrådet** påpeger, at SMV'erne mangler konkrete værktøjer og forståelige guidelines til, hvordan de styrker deres cybersikkerhed og minimerer risikoen for cyberangreb. Der er således behov for en mere håndholdt indsats overfor SMV'er for at forstå og tolke informationen fra CFCS.

DI bemærker, at virksomhederne efterspørger en indsats fra CFCS til håndtering af supply-chain trusler og hjælp til danske cybersikkerhedsvirksomheder med eksportpotentiale, så CFCS er med til at gøre cybersikkerhed til en dansk styrkeposition for branchen. **DI** ser ligeledes, at der er behov for, at CFCS spiller en tydeligere rolle i vurderingen af nye teknologiers betydning for udvikling af cybertruslen.

RfDS og **DI** bemærker, at CFCS' kompetencer fortrinsvis stilles til rådighed for virksomheder i samfundskritiske sektorer, hvorfor særligt SMV-segmentet ikke kan drage nytte af CFCS' mere konkrete hjælp. Herudover konstaterer NRGi, at de savner, at CFCS er mere synlige over for virksomheder af alle størrelser.

Konkrete forslag

- **ITB** foreslår at styrke og udbygge etablerede fora som Cybersikkerhedsrådet og Virksomhedsforum for Digital Sikkerhed som informations- og formidlingskanaler og dermed gøre videndeling mere nærværende for det brede danske erhvervsliv.

- De private medlemmer af **Cybersikkerhedsrådet, DI** og **RfDS** forslår oprettelsen af en SMV-CERT til at rådgive og give konkrete varslinger til virksomhederne med henblik på at øge robustheden hos SMV'er. De private medlemmer af **Cybersikkerhedsrådet** ser gerne, at en sådan varslingstjeneste oprettes i samarbejde med Erhvervsstyrelsen.
    - **IF** oplyser, at de i samarbejde med offentlige og private aktører arbejder med udviklingen af en varslingstjeneste, og at det vil være af stor værdi, hvis CFCS bidrog til arbejdet.

- **RfDS** og **ITB** foreslår, at der etableres en organisation bestående af repræsentanter fra både myndigheder og virksomheder, der varetager opgaven med at indsamle og dele cybertrusler og komme med råd og konkrete operationelle anbefalinger, som både de offentlige og private virksomheder – ikke kun i samfundskritiske/-vigtige sektorer – kan tilgå og agere proaktivt på.
  - **ITB** foreslår, at organisationen skal fungere som koordinerende organ på tværs af eksisterende aktører og fora på cybersikkerhedsområdet, men samtidig skal have en aktiv og udøvende rolle i forhold til at indsamle, koordinere og validere viden og yde vejledning om beredskab og forebyggende sikkerhedsforanstaltninger samt rådgivning og hjælp til håndtering af sikkerhedshændelser i samspil med private cybersikkerhedseksperter.

- **RfDS** foreslår, at der oparbejdes netværk til videndeling og tillidsopbygning efter inspiration fra NC3 Skyt [kaldes nu NC3 Erhverv], således at der opbygges et landsdækkende netværk baseret på både lokalområder og på tværs af sektorer og teknologier.

- **DI** foreslår, at man kunne prioritere at gøre det til en dansk styrkeposition at udvikle kryptering til en verden med kvanteteknologi, når Danmark i forvejen har et stærk forskningsmiljø inden for kryptering.

- **TI** foreslår, at CFCS' virksomhedsrettede indsats kan styrkes ved, at CFCS får mere konkret kendskab til de mekanismer og måder at agere på, der kendetegner større private virksomheder, herunder kommercielle aspekter og overvejelser samt hierarkiske beslutningsgange.

- **RfDS** og de private medlemmer af **Cybersikkerhedsrådet** mener, at der er behov for at data indsamles på tværs af myndigheder, såsom Rigspolitiet og Datatilsynet, hvorefter disse data bearbejdes og stilles til rådighed for private virksomhed til fx at skabe et situationsbillede.

<u>Mulighed for en organisatorisk opsplitning</u>

En række af erhvervs- og brancheorganisationerne påpeger i deres høringssvar, at CFCS' forankring ved FE hæmmer samarbejdet med den private sektor, og at en organisatorisk opsplitning eller reorganisering af CFCS vil kunne styrke den virksomhedsrettede indsats. Samtidig er det vigtigt for organisationerne, at CFCS' efterretningsbaserede oplysninger kan stilles til rådighed for en potentielt ny enhed uden for FE. Herudover nævnes det også, at der er behov for en større analyse af cybersikkerhedsområdet end indeværende analyse.

ITB bemærker, at den virksomhedsrettede indsats på cyberområdet – herunder ikke mindst videndelingen med virksomhederne – i dag er utilstrækkelig. **ITB** ser ikke, at CFCS' nuværende organisering og kultur kan levere på den øgede åbenhed og videndeling med det brede danske erhvervsliv og SMV'erne. **TI** vurderer, at en stærkere civil forankring af CFCS potentielt vil kunne skabe et mere effektivt informationsflow mellem en civil del af CFCS og erhvervslivet. **DE** vurderer, at de mulige negative konsekvenser af en organisatorisk opsplitning vil blive opvejet af de positive effekter af en mere åben og civil relation og herved et bedre samarbejde med den private sektor.

RfDS mener, at alle de opgaver, som kan varetages uden for FE, bør varetages i civilsamfundet i et bredt samarbejde med andre aktører. Det betyder, at vejledende, rådgivende, netværksopbyggende og kriminalitetsbekæmpende indsatser rettet mod det private erhvervsliv med fordel kan foretages uden for FE. **RfDS** bemærker hertil, at de data, FE kan stille til rådighed, så kan tilflyde den foreslåede organisation.

ITB vurderer, at en entydig opsplitning af CFCS i en militær enhed ved FE og en civil enhed uden for FE ikke nødvendigvis er vejen frem, da CFCS har stærke kompetencer og en adgang til viden om trusselsbilledet gennem efterretninger. **ITB** understreger, at såfremt CFCS' virksomhedsrettede indsats placeres uden for FE, ser **ITB** det som centralt, at der kan trækkes på den viden og de kompetencer, der allerede er opbygget med CFCS, og at der i videst muligt omfang kan drages nytte af de efterretninger på cyberområdet, der tilgår FE. **ITB** og **TI** er opmærksomme på, at det kan vise sig svært eller umuligt for en civil enhed uden for FE at blive delagtiggjort i – og hermed kunne drage nytte af – de pågældende efterretninger, som indhentes via samarbejde med andre efterretningstjenester

FD vurderer, at organisationen overordnet er rigtig.

Konkrete forslag

- **DE** ser en reorganisering af CFCS som det mest effektive tiltag i forhold til at styrke CFCS' virksomhedsrettede indsats.

- **TI** mener, at det bør konsekvensanalyseres, i hvilket omfang, der risikeres kompetencetab og rekrutteringsudfordringer ved udskilning af en civil myndighed fra FE, som primært vil varetage enten tilsyns- eller rådgivningsopgaver.

- **DI** mener, at indeværende analyse bør tage udgangspunkt i den samlede myndighedsindsats over for virksomhederne, og i den forbindelse opfordrer **DI** til, at der tænkes på tværs af ressortområder, hvis virksomhedsindsatsen skal forankres i en ny organisation, så virksomhederne skal forholde sig til færre myndigheder. Hermed vil der blive draget bedre nytte af meget efterspurgte cybersikkerhedskompetencer, og så der sikres bedre koordination og ressourceforbrug. Hertil påpeger **DI**, at det er en væsentlig faktor i disse overvejelser, at kontakten til efterretningstjenesterne medtænkes, og at den etablerede synergi ikke mistes. **DI** bemærker, at man eksempelvis kan skele til den måde, Israel har organiseret sig på.

TELESEKTOREN

Som det fremgår i første del af analysen, har CFCS sektoransvar for visse dele af telesektoren, hvilket indbefatter tilsyn med telesektoren og koordination af håndteringen af særlige trusler, der kan påvirke informationssikkerheden i telesektoren. I nedenstående en række af erhvervs- og brancheorganisationernes perspektiver og løsningsforslag i relation til CFCS' telerettede opgaver.

DE bemærker, at der er en bred opfattelse blandt virksomheder i telesektoren af, at sammenblanding af tilsynsmyndighed og efterretningsvæsen er uhensigtsmæssig, og **DE**'s medlemmer er kritiske overfor at tilsynet, som al anden erhvervsrettet lovgivning, ikke ligger i den civile del af forvaltningen. **DE** bemærker, at reguleringen af telesektoren på dette område ikke ses i sammenhæng med den øvrige regulering, og at selskaberne ikke har den nød-

vendige sikkerhed for inddragelse af andre samfundshensyn end militære strategiske sikkerhedshensyn. Hertil bemærker **DE**, at de oplever en tilbageholdenhed i forhold til at virksomheder i telesektoren tilslutter sig sensornetværket, da CFCS vil få data og indblik i de virksomheder, som de grundet rollen som tilsynsmyndighed også kan sanktionere.

TI bemærker, at størstedelen af de udfordringer, som **TI** oplever i relation til den virksomhedsrettede indsats, har rod i, at CFCS varetager flere funktioner og roller som både IT-sikkerhedsmyndighed, kompetencecenter, rådgivningsfunktion, tilsynsmyndighed og ikke mindst som efterretningstjeneste. **FD** bemærker, at man grundet udfordringer i forhold til teleområdet bør overveje en anden organisering. **ITB** og **DE** bemærker, at foruden CFCS som sikkerhedsmyndighed for telesektoren er Energistyrelsen og Erhvervsstyrelsen også væsentlige myndigheder for telesektoren, hvilket **DE** vurderer giver en unødvendig fragmentering af forvaltningen.

TI fremhæver, at CFCS er gode til at stå til rådighed for virksomhederne. Det gælder eksempelvis ved deltagelse i **TI**'s Sikkerhedsgruppe og ikke mindst ved en aktiv deltagelse og støtte til TeleDCIS-branchesamarbejdet. **TI** vurderer desuden, at det operationelle samarbejde med CFCS generelt fungerer godt. Gennem løbende operationelle statusmøder med CFCS sikres en fælles faglig forståelse på området, hvilket muliggør et smidigt og konstruktivt samarbejde.

Konkrete forslag

- **TI, ITB** og **DE** foreslår, at en organisatorisk opsplitning af CFCS' opgave i relation til telesektoren kan være med til at skabe en mere civil forankring og imødekomme de modsatrettede interesser, der kan være ved at CFCS har flere funktioner, og roller som tilsynsmyndighed, rådgivningsfunktion og efterretningstjeneste. **DE** foreslår, at dette eksempelvis kan ske ved at adskille de opgaver, der knytter sig til CFCS' rolle som tilsynsmyndighed for telesektoren fra efterretningstjenesten.

- **TI, DE** og **ITB** foreslår, at det undersøges, hvorvidt der er fordele ved at placere dele af teleopgaverne i CFCS i en eksisterende struktur og sammen med øvrige relevante myndigheder i stedet for blot at vurdere en placering i en civil enhed under Forsvarsministeriet.
  - **DE** og **TI** foreslår, at man analyserer, om det er mere hensigtsmæssigt at placere et separat tilsyn i Erhvervsstyrelsen. **TI** foreslår at en separat rådgivningsfunktion kan placeres i eksempelvis Digitaliseringsstyrelsen, om end **TI** er opmærksom på, at der også kan være udfordringer hermed.
  - **DE** ser også, at det kan være en mulighed med en civil enhed i Forsvarsministeriet og bemærker, at denne placering muligvis kan 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.
  - **ITB** foreslår, at det skal vurderes, om en placering uden for FE kan bidrage til en mere præcis beskrivelse af objektive krav til udstyrsleverandører, hvilket vil gøre det enklere for både teleudbydere og leverandører at navigere i henhold til lovens krav.
  - **TI** foreslår, at man kan samle én fælles IT- og cybersikkerheds-tilsynsmyndighed. **TI** vurderer, at denne model har flere fordele, fx mindsket kompleksitet blandt for-

skellige offentlige tilsynsmyndigheder, samt sikring af nødvendig adskillelse mellem CFCS' rolle som både rådgivende myndighed og tilsynsmyndighed.

- Hvis nuværende organisering af CFCS fastholdes, opfordrer **TI** på det kraftigste til en række operationelle tiltag.
  - **TI** opfordrer CFCS til at være mere åben i forhold til deling af viden om kendte cyberangreb, kommende trusler (aktuelt trusselsbillede) og trusselsscenarier med de væsentlige teleudbydere.
  - **TI** ser, at denne mere værdifulde og fortrolige videndeling eventuelt kan foregå i en tillidsbaseret dialog mellem myndighederne og grupper af sikkerhedsgodkendte medarbejdere fra de væsentlige teleudbydere, herunder eventuelt i lukkede grupper eller ved både formelle og/eller uformelle fysiske møder.
  - **TI** oplever, at hastigheden for distribution af trusler og sårbarheder ofte foregår i et tempo, så teleudbyderne får informationerne via andre kanaler, før de meldes ud fra CFCS. Derfor opfordrer **TI** CFCS til i videst muligt omfang at sætte hastigheden for distribution af vigtige informationer til virksomhederne op.

Hovedpointer

- Erhvervs- og brancheorganisationerne oplever, at CFCS besidder en **høj faglighed** og **stærke kompetencer**, der er med til at **styrke Danmarks cybersikkerhed**.
- Høringssvarene fra erhvervs- og brancheorganisationerne afspejler, at der er **uklarhed** omkring CFCS' ansvar over for den private sektor og **snitfladerne** mellem de statslige myndigheder på cyberområdet.
- En større grad af **åbenhed**, **videndeling**, **afklassificering** og **SMV-indsats** vil kunne styrke CFCS' samarbejde med den private sektor.
- Erhvervs- og brancheorganisationerne afvejer på forskellig vis hensynet til en **større åbenhed** på den ene side og hensynet til **efterretningsbaseret viden** på den anden side i forhold til en mulig **reorganisering** eller **organisatorisk opsplitning** af CFCS.
- Flere af høringssvarene peger på et behov for en **større analyse af cyberområdet** for at kunne fastlægge en mere effektiv virksomhedsbaseret indsats på området.

FORSVARSMINISTERIET

BILAG 3

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.

Hvordan kan eventuelle ovenstående udfordringer løses?
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

FORSVARSMINISTERIET

BILAG 4

DI

Den 24. februar 2022
MORV

Den private sektors samarbejde med CFCS - bidrag fra DI

1. Generelt

DI takker for muligheden for at bidrage til Forsvarsministeriets analyse af CFCS' virke med særligt fokus på at øge den samlede indsats over for den private sektor. Center for Cybersikkerhed (CFCS) har siden sin etablering i 2012 haft en betydelig rolle i det danske samfunds øgede fokus på at styrke cybersikkerheden. Det gælder også for virksomhedernes arbejde med cybersikkerhed – i særdeleshed for virksomheder i samfundskritiske sektorer.

DI vil gerne kvittere for denne indsats og for Center for Cybersikkerheds villighed til at stille op til konferencer, i netværk og lignende for at udbrede viden om cybertruslen. I det hele taget har CFCS været aktive i den offentlige debat og i projekter, der skal styrke dansk cybersikkerhed eksempelvis opbygning af cyberkompetencer fra børn og unge til bestyrelser.

Generelt set har der været en vis usikkerhed om, hvad CFCS er i stand til at hjælpe private virksomheder med, når der ikke specifikt er tale om virksomheder, der betragtes som samfundskritiske, eller der varetager samfundskritiske funktioner, ligesom det også opleves som uklart, hvornår en virksomhed varetager samfundsvigtige funktioner i CFCS' perspektiv. Rollefordelingen på tværs af de mange myndigheder, der i Danmark er inde over cyberdomænet – f.eks. mellem politiet, Erhvervsstyrelsen og CFCS – opleves også som uklar.

Samtidig er det en generel opfattelse, at CFCS igennem tiden har lagt mere vægt på at modtage og indsamle oplysninger fra virksomhederne end at give noget konkrete informationer og hjælp tilbage til virksomhederne. På den anden side er der blandt DI's medlemmer i samfundskritiske sektorer også flere meget positive oplevelser af hjælpen fra CFCS i forbindelse med enkeltstående angreb på virksomheden – særligt indenfor de samfundskritiske sektorer.

CFCS's direkte linje til både nationale og internationale efterretninger på cyberområdet skal ses i sammenhæng med, at cybertruslen i høj grad er international, og der sker en stadig stigende sammenblandingen mellem forskellige aktører. F.eks. har kriminelle grupper og fremmede efterretningstjenester samme interesser og samarbejder nogle gange direkte. Derfor bør der være en stor værdi – også for civile virksomheder – i den viden og efterretning, som CFCS/FE har adgange til. Fremadrettet tyder meget også på, at bekæmpelsen af cyberkriminalitet kommer til at ske mere offensivt fra bl.a. efterretningstjenesterne. Men der er også en oplevelse af, at CFCS bliver fanget mellem to verdener – den civile verden og efterretningsverdenen, når de skal forsøge at hjælpe virksomheder. Og den tætte relation til forsvaret har også fået virksomheder til at fravælge CFCS – f.eks. tilslutning til netsikkerhedstjenesten.

2. Udfordringer

Ansvaret for cyber- og informationssikkerhed er spredt ud på en række forskellige myndigheder som bl.a. er CFCS (forsvar), NC3 (politi), DIGST (borger), ERST (virksomhed) – dertil kommer ressortansvar og DCIS'er hos samfundskritiske sektorer (sundhed, tele, transport, finans, energi osv.).

Virksomhederne bør ikke først sætte sig ind i den gældende ressortfordeling og dennes udfordringer for at finde den rette indgang til myndighederne, den rette information eller det rette samarbejde. Grundlæggende skal rollefordelingen og myndighedssamarbejdet give borgerne og virksomhederne mest mulig cybersikkerhed for pengene, og man kan stille spørgsmålstegn ved, om det sker bedst ved at holde fast i sektoransvarsprincippet, ressortkampe, uklar rollefordeling, manglende prioritering og koordination etc., eller om det er på tide at centralisere arbejdet med cybersikkerhed i den offentlige sektor som f.eks. Finland eller Israel har gjort.

Denne udfordring og overvejelser er man nødt til at tage med i ligningen, når CFCS's samarbejde med den private sektor skal vurderes. Analysen bør heller ikke have som forudsætning, at en eventuel ny civil organisation skal etableres på Forsvarsministeriets ressort, men være åben for, at myndighedernes samarbejde med den private sektor kan forankres på andre ressort, hvor det nu er mest optimalt for et frugtbart samarbejde.

Danmark er et lille land, og efterspørgslen efter medarbejdere med cyberkompetencer er høj. Vi bør for nuværende koncentrere vores kompetencer frem for at sprede dem tyndt ud på mange myndigheder. Det taler ikke for, at der oprettes endnu en myndighed på området uden at se på den samlede organisering på området.

Center for Cybersikkerhed har løbende fået udvidet sin opgaveportefølje på rådgivningsområdet, og ganske som DI havde frygtet i vores høringssvar til ændring af lov om center for cybersikkerhed i 2019, ser vi, at der bliver brugt offentlige midler på at tilbyde forebyggende it-sikkerhedsydelser som f. eks. penetrationstest, som der også tilbydes på det private marked. Det er forkert og konkurrenceforvridende i sig selv, og ressourcerne burde i stedet bruges på samarbejde med den private sektor og på opgaver, der i forvejen ikke løftes af det private marked.

I vurderingen af CFCS's samarbejde med en private sektor er det en vigtig faktor, at de fremadrettede opgaver ikke er opgaver, der allerede løftes af andre.

3. Behov

Det er positivt, at politiet får flere ressourcer til efterforskning og disruption af cyberkriminalitet i den nye nationale strategi for cyber- og informationssikkerhed, og at den internationale dimension af politiets arbejde prioriteres. Men det er afgørende, at det ikke er en symbolsk satsning. Stadig mere kriminalitet og svindel bliver digital, og det er populært sagt kun de dumme kriminelle, der ikke er digitale, når udbyttet er højt, indsatsen lille og risikoen for at blive opdaget er minimal.

Uanset, hvor meget ansvar, som myndigheder vil lægge over på virksomhederne, er det stadig en forbrydelse, hver gang cyberkriminelle har held med deres foretagender. Der er med andre ord brug for en væsentlig ressourcetilførsel til område for efterforskning og bekæmpelse af cyberkriminalitet – og hvis CFCS har kompetencer og ressourcer, som politiet har brug for, er det et område, der er behov for at prioritere – samtidig med at der etableres og kommunikeres en klar rollefordeling mellem politi, forsvar og efterretningsvæsen.

Virksomhedernes efterspørger også større klarhed og gennemsigtighed om kriterier, når CFCS vurderer sikkerhedsniveau – f.eks. som myndighed for telesektoren. Det kan f.eks. være i forhold til:

- Krav til ledelsen
- Leverandørsikkerhed
- Anbefalinger i forhold til krav om kryptering

Andre specifikke områder, som virksomhederne efterspørger en indsats fra CFCS på, er eksempelvis hjælp til håndtering af supply chain trusler og hjælp til danske cybersikkerhedsvirksomheder med eksportpotentiele, så CFCS er med til at gøre cybersikkerhed til en dansk styrkeposition for branchen. Man kunne eksempelvis prioritere at gøre det til en dansk styrkeposition at

udvikle kryptering til en verden med kvanteteknologi, når vi i forvejen har et stærk forskningsmiljø indenfor kryptering.

I forlængelse heraf er der også behov for, at CFCS spiller en tydeligere rolle i vurderingen af nye teknologiers betydning for udvikling af cybertruslen.

For borgere og virksomheder er der tæt sammenhæng mellem it-sikkerhed og databeskyttelse. Borgere skelner typisk ikke mellem it-sikkerhed og databeskyttelse eller blander det sammen og forveksler det ene med det andet. For virksomhederne er det ikke et valg. De er nødt til at tænke it-sikkerhed og databeskyttelse sammen i regi af GDPR, og når de sikrer persondata, sikrer de typisk også andre forretningsdata. Fra et myndighedsperspektiv er it-sikkerhed og databeskyttelse overraskende skarpt opdelt. Udgangspunktet er, at begge dele i bund og grund oftest handler om at have styr på sine data og passe på dem. CFCS bør tage større ansvar for at tænke it-sikkerhed og GDPR sammen.

4. Løsninger

Etablering af processer for informationsdeling - klassificerede informationer skal bedre i spil
Fremadrettet skal der findes bedre muligheder for at dele klassificeret informationer – f.eks. i form af deklassificering etc. Leverandørerne oplever ikke, at det i dag er muligt at drage nytte af den værdi, der ligger i, at CFCS er placeret ved FE udenfor CFCS. I det hele taget bør der være mere fokus på informationsdeling og etablering af processer, der understøtter dette.

Etablering af et formaliseret samarbejde mellem CFCS og it-sikkerhedsbranchen
Samarbejdet mellem CFCS og den it-sikkerhedsbranchen i Danmark skal gå fra den ad-hoc praksis, der opleves i dag til et mere formaliseret samarbejde om f.eks. systematisk deling af informationer. Det er vigtigt, at der i den forbindelse opbygges den nødvendige tillid parterne imellem.

Tydelig forventningsafstemning omkring den virksomhedsrettede indsats
Den virksomhedsrettede indsats i CFCS, som ikke er målrettet samfundskritiske sektorer eller virksomheder med samfundsvigtige funktioner, bør være en tydeligt prioriteret opgave i CFCS. Der bør formuleres en målsætning for den virksomhedsrettede indsats, så der kommer en bedre forventningsafstemning med samarbejdspartnere og virksomhederne selv.

Bredere fokus i analysen end Forsvarsministeriets ressort

Den forestående analyse, som vi hermed bidrager til , bør ikke afgrænse sig til at se på Forsvarsministeriets ressort. Når det handler om understøttelse af virksomhedernes cybersikkerhed fra danske myndigheders side, er det afgørende, at det fragmenterede landskab af myndigheder på området tages i betragtning. Grundlæggende giver analysen kun mening, hvis der tages udgangspunkt i den samlede myndighedsindsats overfor virksomhederne, og i den forbindelse opfordrer DI til, at der tænkes på tværs af ressortområder, hvis virksomhedsindsatsen skal forankres i en ny organisation, så virksomhederne skal forholde sig til færre myndigheder, så der drages bedre nytte af meget efterspurgte cybersikkerhedskompetencer, og så der sikres bedre koordination og ressourceforbrug.
Det er en væsentlig faktor i disse overvejelser, at kontakten til efterretningstjenesterne medtænkes, at den etablerede synergi ikke mistes. Der kan eksempelvis skeles til den måde, som et land som Israel har organiseret sig på.

CFCS skal prioritere medvirken i offentlig/privat SMV-samarbejde

DI har længe argumenteret for, at der skal opbygges et proaktivt, praktisk orienteret og kompetent videns- og overvågningscenter (SMV-CERT), der i et tæt samspil med alle væsentlige interessenter kan bistå danske SMV'er med at styrke deres IT-sikkerhed og evnen til at forebygge relevante cyberrisici og dermed nedbringe antallet af succesfulde cyberangreb. Samspillet mellem CFCS, andre myndigheder, erhvervsorganisationer og virksomheder er afgørende for, at det kan realiseres og gøre en forskel. Prioriteringen af CFCS's bidrag, selvom organiseringen sker udenfor myndighederne, vil derfor være nødvendig.

FORSVARSMINISTERIET

BILAG 5

IT-Branchens høringssvar vedr. den private sektors samarbejde med CFCS

Hvad fungerer godt i samarbejdet med CFCS mht. den virksomhedsrettede indsats?
Overordnet skal CFCS have ros for sit arbejde med vejledninger, rapporter og trusselsvurderinger og andre udadvendte, virksomhedsrettede aktiviteter, og som organisation oplever IT-Branchen, at CFCS er tilgængelig for dialog og en god samarbejdspartner.

Med CFCS's nuværende placering har CFCS en unik, direkte adgang til viden om det internationale trusselsbillede på cyberområdet, herunder særlig adgang til efterretninger om cybertrusler fra udlandet. Der er over de seneste år skabt et stærkt CFCS, der har opbygget stærke kompetencer på cyberområdet, har skarpt fokus på rigets sikkerhed, de offentlige myndigheder og de samfundskritiske sektorer – og som fungerer som et væsentligt videncenter i kampen mod internationale cybertrusler. Disse styrker bør der bygges videre på med fokus på øget videndeling og øget hjælp til cybersikkerhed til det brede danske erhvervsliv og SMV'erne.

Derfor er vejen frem ikke nødvendigvis en entydig opsplitning af CFCS i en militær enhed under FE og en civil enhed udenfor FE, men den virksomhedsrettede indsats på cyberområdet – herunder ikke mindst videndelingen med virksomhederne – er i dag utilstrækkelig.

Hvilke udfordringer opleves i relation til CFCS mht. den virksomhedsrettede indsats?
Som kommissoriet for analysen af CFCS' forankring under FE også antyder, er der behov for at styrke det civile arbejde med cybersikkerhed, og herunder i højere grad at hjælpe de danske virksomheder med at løfte opgaven ift. cyberbeskyttelse.

IT-Branchens medlemmer deler tillige den i kommissoriet nævnte opfattelse af, at CFCS' organisering ikke befordrer en tilstrækkelig videndeling og åbenhed ift. hjælpe de danske virksomheder med at imødegå og tackle aktuelle cybertrusler.

IT·BRANCHEN

IT-Branchens medlemmer oplever ikke de tiltænkte synergieffekter mellem CFCS' adgang til efterretninger om cybertrusler fra udlandet og viden om det internationale trusselsbillede på cyberområdet på den ene side, og en øget videndeling og konkret hjælp og rådgivning til virksomhederne på den anden side. Tværtimod mener IT-Branchens medlemmer, at den gensidige videndeling med virksomhederne kan styrkes ved, at viden ikke hemmelighedsstemples unødigt, så virksomhederne i højere grad kan modtage aktuel og relevant/vedkommende viden, der kan bruges operationelt i virksomhedernes egne, konkrete trusselsvurderinger og sikkerhedsforanstaltninger.

Der er samtidig behov for større åbenhed omkring, hvad CFCS ønsker at bruge indsamlet data fra virksomhederne til, hvis der skal skabes en tillidsfuld og værdiskabende relation mellem CFCS og virksomhederne. En udfordring der fx viste sig, da CFCS ønskede at etablere et sensornetværk hos private virksomheder uden gennemsigtighed omkring, hvordan disse sensordata ville blive brugt, og hvem de ville blive delt med.

Hvordan kan eventuelle ovenstående udfordringer løses? Hvilke tiltag vil kunne styrke CFCS' virksomhedsrettede indsats?

For at styrke den overordnede videndeling og gøre vigtig information på cybersikkerhedsområdet mere nærværende for det brede danske erhvervsliv, herunder ikke mindst SMV'erne, bør det overvejes at styrke og udbygge allerede etablerede fora som fx Cybersikkerhedsrådet og Virksomhedsforum for Digital Sikkerhed som informations- og formidlingskanaler. Disse fora, hvor både cybersikkerhedsindustrien og det generelle erhvervsliv er repræsenteret, har flere eksempler på succesfuldt at være nået ud med information til den bredere offentlighed og de danske virksomheder. Der er behov for at gentænke både indhold og formidlingsformat for viden og vejledninger på cybersikkerhedsområdet samt hvem, der er den rette afsender, hvis vi skal nå bredt ud til erhvervslivet. Og her vil det ikke være tilstrækkeligt med tilgængelig viden på en hjemmeside.

Såfremt CFCS' virksomhedsrettede indsats placeres udenfor FE vil det være centralt, at der kan trækkes på den viden og de kompetencer, der allerede er opbygget, og at der i videst muligt omfang kan drages nytte af de efterretninger på cyberområdet, der tilgår FE. Det kan dog i sagens natur vise sig svært/umuligt for en civil enhed udenfor FE at blive delagtiggjort i – og hermed kunne drage nytte af – de pågældende efterretninger.

Omvendt er det svært at se for sig, at CFCS' nuværende organisering og kultur kan levere på den øgede åbenhed og videndeling med det brede danske erhvervsliv og SMV'erne, som den stigende cybertrussel kræver. Det vil blandt andet indebære en mere klar myndighedsadskillelse i CFCS, så

kritisk og værdifuld markedsinformation til virksomhedernes ikke tilbageholdes efter samme fortroligheds-/ forsigtighedsprincip som efterretningsdata.

I tillæg til CFCS' samlede arbejde på cyberområdet – militært såvel som civilt – foreslår IT-Branchen, at der etableres en uvildig organisation bestående af repræsentanter fra både myndigheder og virksomheder, der skal varetage opgaven med at indsamle og dele viden om cybertrusler og komme med råd og aktuelle anbefalinger, som både det offentlige og private virksomheder – ikke kun i samfundskritiske/-vigtige sektorer – kan tilgå og agere proaktivt på. Organisationen skal fungere som koordinerende organ på tværs af eksisterende aktører og fora på cybersikkerhedsområdet, men skal samtidig have en aktiv og udøvende rolle ift. at indsamle, koordinere og validere viden og yde vejledning om beredskab og forebyggende sikkerhedsforanstaltninger samt rådgivning og hjælp til håndtering af sikkerhedshændelser i samspil med private cybersikkerhedseksperter.

Særlige bemærkninger vedr. CFCS' opgaver og beføjelser ift. telesektoren

I kommissoriet for analysen af CFCS' forankring under FE fremgår følgende tekst:

a. Som led i ovenstående, analyseres de særlige opgaver og beføjelser, som CFCS er tillagt i forhold til telesektoren. Her vil det specifikt blive belyst, hvilke fordele og ulemper, herunder i forhold til gældende sektorlovgivning og til de nuværende særlige lovgivningsmæssige undtagelser for CFCS, der vil være ved flytning af denne virksomheds- og sektorrettede opgave til en civil enhed på Forsvarsministeriets område.

CFCS påtager sig rollen ift. at regulere og føre tilsyn med teleudbydere – ikke med udstyrsleverandører. Imidlertid er CFCS blevet særdeles relevant for udstyrsleverandører efter vedtagelsen af "Lov om leverandørsikkerhed in den kritiske teleinfrastruktur" fra maj 2021.

På vegne af udstyrsleverandørerne vil IT-branchen sætte pris på, at følgende to inputs kan medtages i opgaverne for kommissoriet:

- *Mere objektive krav til telesikkerhed:* CFCS har i loven en rolle, hvor de kan forbyde leverandøraftaler, men loven foreskriver ikke operationelle kriterier for CFCS' afgørelser. På grund af CFCS' placering i FE har markedet ikke adgang til indsigt i, hvilke kriterier CFCS i praksis anvender for deres afgørelser. Vi vil foreslå, at det i arbejdet også vurderes, om en placering udenfor FE kan bidrage til en mere præcis beskrivelse af objektive krav til

udstyrsleverandører, hvilket vil gøre det enklere for både teleudbydere og leverandører at navigere i henhold til lovens krav

- *Mere samling af telereguleringen*: Udover CFCS som sikkerhedsmyndighed for telesektoren er Energistyrelsen og Erhvervsstyrelsen også væsentlige myndigheder for telesektoren. Vi vil derfor foreslå, at der også ses på, om der er fordele ved at lægge teleopgaverne i CFCS sammen med disse øvrige myndigheder for telesektoren i stedet for blot at vurdere en placering i en civil enhed under Forsvarsministeriet. Vi forventer, at dette vil medføre en øget effektivitet og en øget åbenhed til gavn for både myndigheder og marked.

FORSVARSMINISTERIET

BILAG 6

Rådet for Digital Sikkerhed

23.06.2022

Rådet for Digital Sikkerheds bemærkninger til Virksomhedsindsatsen på Cybersikkerhedsområdet

Rådet for Digital Sikkerhed skal hermed fremkomme med sine bemærkninger til høringen om Virksomhedsindsatsen på Cybersikkerhedsområdet og CFCS placering.

Baggrund

Regeringen har med Aftale om et Styrket Cyberforsvar af 24. juni 2021 besluttet at igangsætte en analyse af CFCS forankring under FE. Analysen skal omfatte CFCS ansvar opgaver og snitflader til andre myndigheder, CFCS opgavevaretagelse i forhold til den private sektor og CFCS forankring under FE herunder fordele og ulemper ved at rykke virksomhedsindsatsen udenfor FE.

RfDS vil indledningsvist kvittere for det væsentlige bidrag, som CFCS gennem tiden har givet til at styrke den nationale sikkerhed og danske virksomheders sikkerhed. Der er en høj kvalitet, af de materialer der udarbejdes, CFCS spiller en vigtig rolle i forhold til den offentlige debat og f.eks. etablering af uddannelse, og CFCS stiller også ofte og beredvilligt op som taler på ved række konferencer. RfDS og omverdenen i øvrigt er efterladt med et godt indtryk af solid faglighed i CFCS.

Rådets bemærkninger

I forhold til det private erhvervslivs forventninger er der en oplevelse af, at CFCS gerne vil modtage data om hændelser m.v. og i vid udtrækning også gerne vil installere prober, logningssystemer m.v., men at der er en betydelig tilbageholdenhed med at levere data tilbage erhvervslivet. Når der kommer tilbagemeldinger, er disse ofte på et meget overordnet niveau i form af vejledninger mere end på operationelt niveau i form af konkrete risikovurderinger og konkrete tekniske data.

Et konkret eksempel som er aktuelt i skrivende stund: Giver situationen i Ukraine anledning til ændringer i danske virksomheders risikovurderinger, hvilke trusler forudses, hvad er sandsynlighed og konsekvens for at disse materialiserer sig i en hændelse for danske virksomheder, fra hvilke sider kan truslerne komme, er der IP-adresser, processer eller andet som virksomhederne skal rette deres opmærksomhed imod og evt. blokere?

Et andet konkret eksempel er, at når data først er blevet opsamlet og kommet ind i CFCS regi, så opnår de sådan klassificering, at de ikke kan benyttes til at hjælpe de virksomheder, som i første omgang stillede dem til rådighed.

Det nytter ikke noget, at CFCS på den ene side er meget kompetent og qua sin placering i FE har adgang til gode datakilder, hvis på den anden side sådanne oplysninger ikke kan stilles til rådighed for erhvervslivet i bred forstand.

Formålet med dataindsamlingen i CFCS er meget abstrakt f.eks. i forhold til at beskytte danske interesser mens den konkrete anvendelse af data er uigennemsigtig f.eks. hvor ender virksomhedernes data. CFCS opfattes således af mange virksomheder som en blackbox. Dette underbygges yderligere af, at der med centerets placering er en undtagelse for de love, som generelt skal sikre, at forvaltningen går ordentligt for sig forvaltningsloven, offentlighedsloven og de persondataretlige regler, og dels af at det er RfDS opfattelse af Tilsynet med Efterretningstjenester er et forholdsvist svagt Tilsyn.

Rådet for Digital Sikkerhed
Vester Farimagsgade 37B, 1.th., 1606 København V
Telefon: +45 53 36 02 23 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

Samarbejdet med sikkerhedsleverandører får også en meget blandet anmeldelse, men historien er den samme: Der synes at være et ønske om, at der tilflyder CFCS en masse data, men der er ikke et tilsvarende ønske om at data flyder tilbage til sikkerhedsleverandørerne. Sikkerhedsleverandørerne har ellers gennem en række af de tekniske løsninger, som udbydes, mulighed for at beskytte store dele af erhvervslivet under eet – f.eks. en DNS-blacklist, der sikrer blokering af skadelige IP-adresser.

De kompetencer, der er oparbejdet i CFCS stilles fortrinsvis til rådighed for privat erhvervsliv, der er defineret ved at være kritisk infrastruktur. Især SMV-segmentet, som udgør en stor del af dansk erhvervsliv, kan således ikke drage nytte af CFCS – evt. mere konkrete hjælp.

Eksistensen af CFCS har i den senere tid givet anledning til misforståelser og urealistiske forventninger hos en række private aktører – uden at CFCS er skyld i dette! Flere aktører har således haft en forventning om af CFCS kavaleriet ville komme ridende og redde virksomheder, der havde været udsat for et cyberangreb. Det er vigtigt, at det fra Regeringen m.fl. præciseres, hvilken hjælp private virksomheder kan forvente at modtage fra myndighederne – og ikke mindst at det præciseres hvilke myndigheder, der gør hvad.

Virksomhedernes behov

Der er behov for et mere formaliseret samarbejde med de konkrete virksomheder og en national myndighed, således at der kan laves mere konkret (og dermed mindre abstrakt og generel) erfaringsudveksling, opbygges tillid på forhånd inden en hændelse materialiserer sig og sikres en passende gennemsigtighed om selve samarbejdsrelationen.

Der er ligeledes behov for, at oplysninger om trusler gøres så konkrete, at de kan bruges dels i risikovurderinger og dels direkte som input til eksisterende tekniske foranstaltninger – evt. gennem leverandører.

Videre er der behov for at oplysninger de-klassificeres, så de kan komme i spil de steder, hvor de kan skabe værdi for erhvervslivet.

I det omfang, hvor en hændelse er at betragte som en kriminel handling, er det vigtigt for virksomhederne at kunne have en dialog med politiet om efterforskningen og at virksomhederne betrygges i, at politiet tager efterforskningen alvorligt – også selv om der er tale om grænseoverskridende kriminalitet.

Yderligere er der behov for at skabe meget mere gennemsigtighed med, hvad der sker med data, som kommer fra det private til CFCS, og der er behov for at data som opsamles af myndighederne i bred forstand (f.eks. også af Rigspolitiet og Datatilsynet), bearbejdes og stilles til rådighed for erhvervslivet.

Endelig er der behov for at det tydeliggøres hvilke myndigheder der gør hvad, når virksomhederne – også SMV'erne – har været udsat for en hændelse.

Rådets anbefalinger

RfDS anbefaler derfor, at der etableres en organisation bestående af repræsentanter fra både myndigheder og virksomheder, der varetager opgaven med at indsamle og dele cybertrusler og komme med råd og konkrete operationelle anbefalinger, som alle kan få glæde af og reagere proaktivt på. En sådan organisation kunne bl.a. en aktivitet udbyde en SMV-CERT, således at der udgik konkrete varslinger herfra til virksomhederne. Som en anden aktivitet bør der oparbejdes netværk til vidensdeling og tillidsopbygning efter inspiration fra NC3 Skyt, således at der opbygges et landsdækkende netværk baseret på både lokalområder og tværgående på tværs af sektorer og teknologier. Som en tredje aktivitet bør organisationen

samarbejde med Rigspolitiet om anmeldelse og efterforskning af kriminalitet. Aktører som Cybersikkerhedsrådet, Virksomhedsforum og erhvervsorganisationerne kunne bidrage til opbygningen af en sådan organisation. Der skal sikres høj grad af gennemsigtighed med anvendelse af data i organisationen. Placeringen af organisationen bør være i civilsamfundet – måske hos Rigspolitiet eller i Erhvervsstyrelsen – og nogle af de enkelte aktiviteter behøver ikke foregå direkte hos en myndighed – f.eks. kunne en SMV-CERT udmærket bo hos en erhvervsorganisation.

Baseret på erfaringen og de tilbagemeldinger der løbende har været fra CFCS synes den nuværende klassificeringskultur (hemmelighedskultur) hos CFCS at være et problem for, at CFCS kunne opfylde disse opgaver. RfDS hælder derfor til, at alle de opgaver, som kan varetages udenfor FE, bør varetages i civilsamfundet udenfor FE i et bredt samarbejde med andre aktører. Det betyder, at vejledende, rådgivende, netværksopbyggende og kriminalitetsbekæmpende indsatser rettet mod det private erhvervsliv med fordel kan foretages udenfor FE. De data FE så kan stille til rådighed, kan så tilflyde den foreslåede organisation.

De tilbageværende opgaver som vedrørende nationens sikkerhed og som fordrer klassifikation bør forblive under FE's organisation.

RfDS står naturligvis til rådighed for en uddybelse af ovenstående synspunkter.

På bestyrelsens vegne

Henning Mortensen

Formand, RfDS

FORSVARSMINISTERIET

BILAG 7

De private medlemmer af Cybersikkerhedsrådet

1. marts 2022

Høringssvar på FMN høring vedr. CFCS fra de private medlemmer i Cybersikkerhedsrådet.

Forsvarsministeriet har med mail af 21. februar 2022 bedt bl.a. de private medlemmer af Cybersikkerhedsrådet om at bidrage med høringssvar vedrørende den private sektors samarbejde med CFCS. Høringen skal indgå som et bidrag til en analyse af CFCS' forankring under Forsvarets Efterretningstjeneste som har den specifikke præmis, at en alternativ forankring skal være en selvstændig enhed indenfor Forsvarsministeriets område.

De private medlemmer af Cybersikkerhedsrådet takker for muligheden for at indgå som høringspart, og ønsker indledningsvist at slå fast, at højt niveau indenfor cyber- og informationssikkerhed er en grundlæggende forudsætning for et gennemdigitaliseret samfund som det danske. De private medlemmer af Cybersikkerhedsrådet er af den opfattelse, at CFCS spiller en vigtig rolle i beskyttelse af Danmark og danske interesser mod cybertrusler. Det er i alles interesse, at der er et tæt og velfungerende samarbejde mellem CFCS og interessenter - herunder private virksomheder, i forhold til at kunne øge robustheden i samfundet.

CFCS' virksomhedsrettede indsats består af udgivelse af specifikke trusselsvurderinger mod de kritiske sektorer i Danmark, udsendelse af generelle varsler om trusler, samt udgivelse af generelle vejledninger indenfor cyber- og informationssikkerhed. Derudover tilbydes netværksmonitorering af visse virksomheder indenfor de kritiske sektorer med udsendelse af specifik alarmering for tilsluttede virksomheder. Etablering af de såkaldte DCIS'er i de kritiske sektorer, har også været tænkt som en informationsdelingskanal mellem CFCS og de private virksomheder indenfor de kritiske sektorer.

Meget af denne information forudsætter, at der i virksomheder er dedikerede ressourcer til at forstå og tolke meldingerne for CFCS, hvilket ikke er tilfældet i alle dele af SMV-segmentet. Der er således behov for at mere håndholdt indsats overfor SMV'ere.

For virksomheder med dedikerede sikkerhedsressourcer, yder de generelle trusselsvurderinger, varsler og vejledninger et vigtigt bidrag til at højne opmærksomheden omkring cyber- og Informationssikkerhed i de private virksomheder.

Generelt ses dog betydelige udfordringer med deling af konkret, operativ information, samt med etablering af et gensidigt, operativt samarbejde mellem CFCS og de private virksomheder, herunder ikke mindst private sikkerheds- og rådgivningsvirksomheder. En tættere, operativt samarbejde med aktiv deling af information og indikatorer vil kunne styrke samfundets robusthed, da sikkerheds- og rådgivningsfirmaer er i daglig berøring med mange typer af virksomheder og bistår med konkret imødegåelse af trusler mod cyber- og informationssikkerheden.

De udfordringer som ses i CFCS' virksomhedsrettede arbejde ses ikke relateret til placeringen af CFCS' virksomhedsrettede indsats, men til CFCS' tilgang til samarbejde med private virksomheder.

Det er de private medlemmer af Cybersikkerhedsrådets vurdering, at der er behov for at en hurtig og konkret styrkelse af CFCS' operative samarbejde med de private virksomheder og behov for at CFCS går væsentligt længere med informationsdeling end hidtil.

For at styrke den generelle robusthed i Danmark, bør samarbejde mellem offentlige og private sikkerhedskompetencer styrkes. Konkret anbefaler de private medlemmer af Cybersikkerhedsrådet, at CFCS sætter sig i spidsen for følgende initiativer for at styre det operative samarbejde:

a. CFCS bør styrke evnen til at afklassificere information så mængde og frekvens af informationsdeling kan øges og stille en informationsdelingsplatform i stil med MISP til rådighed, hvor virksomheder kan hente informationen og bringe den i anvendelse. En informationsdelingsplatform vil også kunne lette virksomhedernes arbejde med at dele tekniske indikatorer om egne hændelser.

b. CFCS bør i samarbejde med private sikkerheds- og rådgivningsvirksomheder finde en model for deling og af klassificeret information, som eksempelvis kan tage udgangspunkt i den norske kvalitetsordning for leverandører som håndterer IKT-hændelser[1]. Godkendte virksomheder kunne eksempelvis også få godkendt installationer og personel som kan få adgang til klassificeret information og derved kunne anvende information ved sikkerhedshændelser eller ved rådgivning om cyber- og informationssikkerhed.

c. CFCS bør styrke evnen til at bearbejde den information som indsamles på tværs af andre offentlige myndigheder så som Datatilsynet og Rigspolitiet og stille et situationsbillede til rådighed for private virksomheder.

d. CFCS bør styrke evnen til at rådgive SMV'ere ved i samarbejde med Erhvervsstyrelse at etablere en SMV-CERT som kan medvirke til at øge den generelle robusthed hos SMV'ere.

e. Det offentlige formandskab anvender Cybersikkerhedsrådet til jævnlige drøfter den samlede virksomhedsrettede indsats indenfor styrkelse af cyber- og informationssikkerhed f.eks. med inddragelse af Virksomhedsrådet.

De private medlemmer af Cybersikkerhedsrådet står naturligvis til rådighed for en uddybelse af ovenstående synspunkter.

Med venlig hilsen

Per Olsen

Formand for de private medlemmer af Cybersikkerhedsrådet.

[1] https://nsm.no/fagomrader/sikkerhetsstyring/leverandorforhold/kvalitetsordning-for-leverandorer-som-handterer-ikt-hendelser

FORSVARSMINISTERIET

BILAG 8

- **Hvad fungerer godt i samarbejdet med CFCS mht. den virksomhedsrettede indsats?**
  - Vi oplever en god villighed fra CFCS's side til at række ud og deltage i projekter og tiltag, der måske ligger lidt på kanten af kerne-opgaveporteføljen for CFCS.
  - Vi har i Industriens Fond haft et godt samarbejde med CFCS om en række af vores projekter, herunder:
    - Styrkelse af Strategiske Cyberkompetencer med fokus på at styrke cyberkompetencer blandt bestyrelser, hvor CFCS er indgået med viden og kompetencer samt stillet op ifbm. undervisningsforløb.
    - De Danske Cybermesterskaber 2021 – 2024, hvor CFCS og andre dele af FE har stillet op med mandskab og kompetencer til både udvikling af opgaver samt deltagelse i arrangementer.
    - Danish Hub for Cybersecurity, hvor CFCS sidder I bestyrelsen som repræsentant for myndighederne.

- **Hvilke udfordringer opleves i relation til CFCS mht. den virksomhedsrettede indsats?**
  - Vi har ikke oplevet nogle udfordringer i forbindelse med vores projekter.
  - I vores generelle arbejde for at fremme SMV'ers cybersikkerhed har det undertiden været uklart, hvilke opgaver ift. virksomheder som CFCS står for, og hvilke opgaver som ERST har ansvaret for. Det er afgørende, at en fremadrettet model/struktur ikke forhindrer udviklingen af og afprøvningen af nye løsninger for at styrke cybersikkerheden blandt danske virksomheder i et offentligt-privat samarbejde.

- **Hvordan kan eventuelle ovenstående udfordringer løses?**
  - Det kommer ikke til at blive mindre komplekst og vigtigt med klare ansvarsdelinger med det kommende NIS2, hvor endnu flere sektorer, virksomheder og myndigheder inddrages. Der skal rammes en god balancer mellem sektoransvaret og informations- og erfaringsdeling på tværs.

- **Hvilke tiltag vil kunne styrke CFCS' virksomhedsrettede indsats?**
  - Vi kunne godt ønske os, at noget af al den unikke viden som CFCS har om hændelser og trusler kunne formidles i en mere tilgængelig form – fx via andre aktører – til virksomhederne. Vi arbejder i Fonden pt. i samarbejde med forskellige offentlige og private aktører omkring udvikling af en varslingstjeneste for SMV'er, der skal tilvejebringe målrettede varslinger og tilpasset vejledning vil virksomhederne. Det vil være af stor værdi, hvis CFCS kunne bidrage til den slags arbejde.

MALENE STIDSEN
Programchef

INDUSTRIENS FOND

Frederiksgade 17, 3. sal
DK-1265 København K
+45 70209208

FORSVARSMINISTERIET

BILAG 9

Til Forsvarsministeriet

Sendt pr. mail til aso@fmn.dk, ner@fmn.dk og llc@fmn.dk

24. februar 2022

Høring over den private sektors samarbejde med Center for Cybersikkerhed

Ved mail d. 4. februar 2022 har Forsvarsministeriet fremsendt høring over den private sektors samarbejde med Center for Cybersikkerhed (CFCS).

Teleindustrien (TI) takker for muligheden for at bidrage til høringen og glæder sig over, at Forsvarsministeriet ønsker at afdække mulighederne for et styrket samarbejde mellem det offentlige og private på dette særdeles vigtige område.

Det er generelt TI's opfattelse, at et velfungerende CFCS - med god og værdifuld videndeling og rådgivning - ikke kun vil være til gavn for telebranchen, men generelt for det danske samfund, som bliver mere og mere digitaliseret og står over for mange af de samme typer trusler i cyberspace.

TI har valgt at strukturere høringssvaret efter den af Forsvarsministeriet anviste struktur ved så vidt muligt at besvare de fire vejledende spørgsmål. TI skal endvidere bemærke, at Forsvarsministeriet er mere end velkomne til at rette henvendelse med henblik på supplering af det skriftlige bidrag.

TI har nedenstående bemærkninger til høringen:

1. **Hvad fungerer godt i samarbejdet med CFCS mht. den virksomhedsrettede indsats?**

TI noterer sig, at det er en helt afgørende faktor i kampen mod cybertruslen, at vi tager ved lære, deler erfaringer og koordinerer indsatsen – på tværs af myndigheder, virksomheder og sektorer.

CFCS vurderer selv i deres seneste trusselvurdering, at truslen for cyberkriminalitet- og spionage mod Danmark er *meget høj* - og der er ikke umiddelbart noget, der tyder på, at trusselsniveauet bliver mindre over de kommende år.

På denne baggrund værdsætter TI overordnet den sparring og løbende dialog, som CFCS prioriterer at have med virksomhederne i telesektoren. TI bemærker, at interaktionen med CFCS er kendetegnet ved en positiv dialog, og vi oplever, at CFCS løbende er involveret i - og står aktivt til rådighed for TI og branchens selskaber, bl.a. ved

deltagelse i TI's Sikkerhedsgruppe, ved spørgsmål i branchen, samt ikke mindst ved en aktiv deltagelse og støtte til TeleDCIS-branchesamarbejdet.

Denne tilgængelighed, mener vi, er med til at styrke samarbejdet og dette skal CFCS have stor ros og tak for.

TI vurderer desuden, at det operationelle samarbejde med CFCS generelt fungerer godt. Selskaberne oplever samarbejdet med CFCS som dialogsøgende og konstruktivt. Gennem løbende operationelle statusmøder med CFCS sikres en fælles faglig forståelse på området – og der opfordres til, at dette fortsat prioriteres, da det muliggør et smidigt og konstruktivt samarbejde. TI hilser generelt en tæt dialog med CFCS velkomment og finder det afgørende for at sikre forståelse og gensidig tillid.

2. Hvilke udfordringer opleves i relation til CFCS mht. den virksomhedsrettede indsats?

TI oplever forskellige udfordringer i relation til CFCS med hensyn til den virksomhedsrettede indsats. Størstedelen af udfordringerne, som identificeres af TI, har rod i, at CFCS varetager flere funktioner og roller som både IT-sikkerhedsmyndighed, kompetencecenter, rådgivningsfunktion, tilsynsmyndighed og ikke mindst som efterretningstjeneste.

Dette medfører, at der ses flere eksempler på forvirrende dobbeltroller i CFCS, hvilket fører til en række konkrete udfordringer i det løbende samarbejde. Udfordringerne relateret hertil skitseres i punktform herunder:

- Det kan opleves som en hæmmende faktor for samarbejdet mellem CFCS og telebranchen, at det kan være vanskeligt at skelne mellem, i hvilken konkret rolle CFCS optræder i en given situation. Hvorvidt CFCS optræder som tilsyn, som rådgivningsfunktion eller som efterretningstjeneste, eller med fokus på statens sikkerhed, har stor indflydelse på naturen af samarbejdet og dialogen.

- CFCS kan opleves som tilbageholdende i forhold til deling af informationer og viden, der ellers kan potentielt kunne medvirke til at styrke det daglige og taktiske samarbejde og dermed øget cybersikkerhedsniveauet generelt i Danmark og specifikt i telebranchen. Det kan blandt andet skyldes, at den information, som CFCS har adgang til via efterretningssamarbejdet, er klassificeret og ikke kan deles med private aktører.

- Den rådgivende funktion i CFCS kan være begrænset i forhold til konkret rådgivning og deling af viden, hvilket ligeledes vurderes at være en afledt effekt af den organisatoriske forankring under efterretningstjenesten. Dette antages at medføre en kultur for hemmeligholdelse og -stempling af information generelt set. Det kan derfor opleves, at der er et asymmetrisk informationsflow, hvor virksomhederne leverer information og data til CFCS, mens CFCS i mindre omfang leverer operationelle og taktiske informationer til selskaberne. Dette medfører, at CFCS ikke realiserer den (synlige) værdi for virksomhederne, som Centeret potentielt kan.

- CFCS tilbyder officielt rådgivning til virksomheder i forbindelse med kriser, hvilket potentielt er et ekstremt værdifuldt redskab, som stort set alle virksomheder i Danmark vil kunne nyde godt af. Dog opleves det ikke, at CFCS i praksis fuldt ud udfører denne form for rådgivning og krisehjælp. Derimod opleves det primært, at virksomheder skal udlevere så meget information som muligt til CFCS, hvis krisen rammer. Det fremstår sandsynligt, at den manglende funktionsdygtighed i rådgivningen i krisesituationer kan skyldes den træghed informationsdeling og lignende, der opstår i en efterretningstjeneste med stramme juridiske processer.

- CFCS stiller vigtige værktøjer til rådighed, herunder fx Red Team-øvelser, men Centrets funktion(er), som både tilsyn og rådgivende organ, kan potentielt lede til en interessekonflikt.

- Processen omkring clearing og klassifikation af informationer i Forsvarets Efterretningstjeneste (FE) er af og til en barriere og forsinkende faktor for deling af informationer til virksomhederne. Dette kan fx være trusselvurderinger eller informationer om specifikke hændelser af særlig relevans.

- I nogle tilfælde mangler CFCS' forståelse for selskabernes og branchens mulighed for indsamling af data, hvilket har ført til manglende proportionalitet mellem typen/mængden af dataindsamling og svarfrister fra CFCS, hvor svarfristerne er for korte.

Af øvrige kommentarer til udfordringer i CFCS' virksomhedsrettede indsats bemærkes det, at det potentielt kan være en udfordring at skelne mellem, hvad der er "sikkerhedskrav" og "gode sikkerhedsråd". Mangel på klar specifikation kan føre til, at vi som branche risikerer at fortolke regelgrundlag forskelligt og dermed efterleve krav på forskellig vis.

3. Hvordan kan eventuelle ovenstående udfordringer løses?
4. Hvilke tiltag vil kunne styrke CFCS' virksomhedsrettede indsats?

TI har vurderet, at der ikke vil være de store forskelle i besvarelsen af de vejledende spørgsmål 3 og 4. Derfor bedes Forsvarsministeriet se disse to spørgsmål i sammenhæng, da TI's besvarelse herunder både indeholder konkrete forslag til løsninger og tiltag, som både kan løse de ovennævnte udfordringer (spørgsmål 2) samt styrke CFCS' virksomhedsrettede indsats.

Besvarelsen af disse spørgsmål struktureres ud fra to overordnede 'områder' i relation til løsninger og tiltag: Organisatoriske og operationelle løsningsforslag/tiltag.

De rejste løsningsforslag og tiltag under besvarelse af spørgsmål 3 og 4 er ikke gensidigt udelukkende.

Organisatoriske:

TI opfordrer til, at det afdækkes nærmere, hvordan der kan findes en organisatorisk løsning på, at centeret har flere funktioner og roller som tilsynsmyndighed, rådgivningsfunktion og efterretningstjeneste, hvor der kan være modsatrettede interesser. Som det fremgår ovenfor, er de forskellige roller og funktioner årsagen til størstedelen af de

udfordringer, som TI oplever ved CFCS's opgavevaretagelse. Det formodes, at en organisatorisk løsning, og adskillelse af funktioner, muligvis vil kunne skabe mere klarhed og styrke effektivt og værdifuldt samarbejde med erhvervslivet.

Det bør analyseres nærmere, hvordan CFCS kan få en stærkere civil forankring. Det bør i den forbindelse analyseres, om der eventuelt kunne være fordele ved at udskille den civile myndighed fra efterretningstjenesten. Dette kunne potentielt skabe et mere effektivt informationsflow mellem civile del og erhvervslivet, da barriererne i efterretningstjenesten ikke længere står i vejen for en deling af informationer og viden. På den anden side, skal det analyseres nærmere, i hvilket omfang dette ville føre til et tab af informationer, som indhentes via samarbejde med andre efterretningstjenester, som så på ingen måde ville kunne gøres tilgængeligt i samarbejdet.

Derudover bør det konsekvensanalyseres, i hvilket omfang der risikeres kompetencetab og rekrutteringsudfordringer ved udskilning af civil myndighed, som primært vil varetage enten tilsyns- eller rådgivningsopgaver. Det skal noteres, at TI og selskaberne i branchen meget gerne samarbejder med efterretningstjenesten og leverer data, når det vurderes nødvendigt – men der ønskes, at den civile myndighed i højere grad får mulighed for at yde en værdifuld rådgivning, og at koordinationen og interaktionen skaber endnu større værdi for virksomhederne.

TI har følgende *konkrete* bud på organisatoriske løsningsforslag:

TI og dets medlemmer er opmærksomme på, at det i Kommissoriet for analysen fremgår, at man skal analysere *"fordele og ulemper ved at lægge en del af virksomhedsindsatsen i en civil enhed på Forsvarsministeriets område"*.

1) Hvis det vurderes hensigtsmæssigt at adskille tilsynsmyndigheden fra den resterende del af CFCS, herunder efterretningstjeneste og rådgivningsfunktion, så vil TI opfordre til, at man undersøger muligheden for at indarbejde tilsynet i en eksisterende struktur. På denne baggrund noterer TI sig, at Erhvervsstyrelsen varetager forskellige tilsynsroller i forhold til IT-sikkerhed i erhvervslivet (domæner, servere, NIS, platforme, mv.). Samtidig må det forventes, at der over de kommende år vil komme yderligere digitale, erhvervsrettede tilsynsopgaver, fx som følge af kommende EU-retsakter om data og kunstig intelligens. På denne måde kan man samle én fælles IT- og cybersikkerheds-tilsynsmyndighed – og denne model har flere fordele, fx mindsket kompleksitet blandt forskellige offentlige tilsynsmyndigheder, samt sikring af nødvendig adskillelse mellem CFCS' rolle som både rådgivende myndighed og tilsynsmyndighed.

2) Det er derudover TI's forståelse, at der allerede ligger en række kompetencer inden for cyber- og informationssikkerhed i Digitaliseringsstyrelsen, som bl.a. deler sekretariatsrollen i Cybersikkerhedsrådet. Det bør derfor indgå i analysen, at man eventuelt kan placere en eller flere rådgivningsfunktioner her. Med Digitaliseringsstyrelsens kompetencer inden for offentlig-privat samarbejde, deres rolle i udformning af Den nationale strategi for cyber- og informationssikkerhed samt deres erfaring med cybersikkerhedsrådgivning af offentlige myndigheder, vurderes det, at en civil myndighed og/eller rådgivningsfunktion vil kunne være passende forankret her. Omvendt kan der være en udfordring i forhold til, om Digitaliseringsstyrelsen vil have adgang til efterretninger om cyberangreb, som kan tages i anvendelse i varetagelsen

af opgaverne. Endvidere har Digitaliseringsstyrelsen hidtil varetaget opgaver, der primært retter sig mod den offentlige sektor, og har ikke stor erfaring med erhvervsrettet rådgivning.

TI forstår afgrænsningen i kommissoriet, men vurderer det hensigtsmæssigt at få analyseret, om placering af enten et separat tilsyn i fx Erhvervsstyrelsen eller en separat rådgivningsfunktion fx i Digitaliseringsstyrelsen kan være mere hensigtsmæssigt end en placering under Forsvarsministeriets ressort, da der i forvejen eksisterer et ekstensivt fagligt miljø og forbindelser til erhvervslivet og telesektoren her.

Helt overordnet ønsker TI – hvilket vi også håber, at forslagene her afspejler – at vi undgår forvirrende 'dobbeltroller', således at vi får placeret de forskellige funktioner i forskellige organisationer. TI mener, at et stærkt, effektivt og fortroligt samarbejde mellem CFCS og telesektoren – og i øvrigt de øvrige kritiske sektorer – vil kunne skabe en enorm værdi for ikke blot virksomhederne, men for Danmarks samlede cyberforsvar.

Operationelle:

TI vil herunder komme ind på nogle mere operationelle løsningsforslag, som - under CFCS' nuværende organisering - kan tages til efterretning for at mitigere en række af de udfordringer, som TI har skitseret under spørgsmål 2. Fastholdes den nuværende organisering af CFCS, opfordrer TI på det kraftigste til en række operationelle tiltag:

- CFCS opfordres til fremadrettet at tage øget initiativ til at sikre en mere åben vidensdeling på de områder, hvor det kan lade sig gøre, og hvor der er en gevinst for de væsentlige teleudbydere ved at kende til den viden, som CFCS har. Det kunne fx være tilfælde, hvor information, som CFCS har, kan hjælpe sektoren med at inkorporere særlige fokuspunkter i den fremadrettede indsats på cybersikkerhedsområdet.

- I forlængelse af ovenstående opfordres CFCS videre til at være mere åben i forhold til deling af viden om kendte cyberangreb, kommende trusler (aktuelt trusselsbillede) og trusselsscenarier med de væsentlige teleudbydere. Denne mere værdifulde og fortrolige videndeling kan eventuelt foregå i en tillidsbaseret dialog mellem myndighederne og grupper af sikkerhedsgodkendte medarbejdere fra de væsentlige teleudbydere, herunder eventuelt i lukkede grupper eller ved både formelle og/eller uformelle fysiske møder.

- TI oplever, at hastigheden for distribution af trusler og sårbarheder ofte foregår i et tempo, så teleudbyderne får informationerne via andre kanaler, før de meldes ud fra CFCS. Derfor opfordres CFCS til i videst muligt omfang at sætte hastigheden for distribution af vigtige informationer til virksomhederne op.

- TI efterlyser slutteligt mere information om CFCS' kompetencer og virksomhedernes muligheder for at gøre brug af disse. En forklaring på den manglende viden om disse forhold i CFCS formodes at skyldes et hensyn til, at man hører til under en efterretningstjeneste.

- Et tiltag, der antages at kunne styrke CFCS' virksomhedsrettede indsats er, at CFCS fik mere konkret kendskab til de mekanismer og måder at agere på, der

kendetegner større private virksomheder, herunder kommercielle aspekter og overvejelser samt hierarkiske beslutningsgange. En myndighed og en privat virksomhed tænker og agerer ofte forskelligt på mange områder. Derfor kan et øget kendskab og forståelse for private virksomheders vilkår være en vej frem, da det kan skabe en bedre forståelse, som vil styrke samarbejdet.

Med venlig hilsen

Jakob Willer
Direktør, TI

FORSVARSMINISTERIET

BILAG 10

Input fra SMVdanmark,

I SMVdanmark har vi tidligere spurgt vores medlemmer, om de var klar over, hvor de finder den relevante rådgivning inden for digitalisering. Her svarede 1 ud af 3, at de ikke vidste, hvor de kunne få rådgivning. Kun 1 ud af 4 virksomheder, som faktisk vidste hvor de kunne finde rådgivning, benyttede rådgivningen. Det skyldtes primært, at folk ikke mente, rådgivningen var relevant for deres virksomhed. De små og mellemstore virksomheder halter efter i brugen af de mest basale sikkerhedsforanstaltninger. Derfor bør der investeres i støre kampagner for sætte fokus på problemet.

I SMVdanmark efterspørger vi et øget samarbejde mellem myndighederne og erhvervslivet for at styrke indsatsen mod digital kriminalitet og for at øge vidensdelingen. Mange SMV'ers begrænsede størrelse betyder, at de har svært ved at få adgang til ressourcer, herunder talentfulde personer med den nyeste viden om teknologi, for at udnytte virksomhedens fulde potentiale.

Samtidig betyder de fraværende sikkerhedssystemer, at SMV'erne forholdsvis nemt kan adoptere gennemtestede sikkerhedssystemer hos de større virksomheder, idet de ikke er forhindret af ældre systemer og forældede strategier. Oven i det er SMV'erne i stand til at nytænke etablerede praksisser og skære igennem traditionelle branchebegrænsninger.

SMV'erne mangler konkrete værktøjer og forståelige guidelines til, hvordan de styrker deres cybersikkerhed og minimere risikoen for cyberangreb. Der skal handles hurtigts muligt. Vi står i en paradoksal situation, hvor virksomhederne har investeret massivt i digitalisering under covid-19, men hvor sikkerheden ikke er fuldt med. Nu står vi i en ny krise, hvor cybersikkerheden er afgørende for at minimere risikoen for russiske hackerangreb.

Venlig hilsen

Lasse Lundqvist
Konsulent

T +45 33 93 20 00

SMVdanmark

Islands Brygge 26 | 2300 Kbh. S | SMVdanmark.dk | T +45 33 93 20 00 |

FORSVARSMINISTERIET

BILAG 11

Sag

ERHVERVSSTYRELSEN
Dahlerups Pakhus
Langelinie Allé 17
2100 København Ø

Tlf. 35 29 10 00
Fax 35 29 10 01
CVR-nr 10 15 08 17
E-post erst@erst.dk
www.erst.dk

ERHVERVSMINISTERIET

Høringssvar fra Virksomhedsforum for Digital Sikkerheds medlemmer i 2021

Forsvarsministeriet sendte d. 4. februar en høring til Virksomhedsforum for Digital Sikkerhed, hvor forummet blev bedt om at give bidrag til følgende spørgsmål:

- Hvad fungerer godt i samarbejdet med CFCS mht. den virksomhedsrettede indsats?
- Hvilke udfordringer opleves i relation til CFCS mht. den virksomhedsrettede indsats?
- Hvordan kan eventuelle ovenstående udfordringer løses?
- Hvilke tiltag vil kunne styrke CFCS' virksomhedsrettede indsats?

Da forummet endnu ikke er genudpeget i forlængelse af den nye nationale cyber- og informationssikkerhedsstrategi fra 2022, er det ikke muligt at besvare høringen vegne af Virksomhedsforum for Digital Sikkerhed. Høringen er i stedet blevet delt med Virksomhedsforum for Digital Sikkerheds medlemmer sidste år, 2021, hvoraf nogle af dem har givet deres input. Bidragene repræsenterer derfor medlemmernes egne holdninger og ikke Virksomhedsforum for Digital Sikkerhed som helhed.

Medlemmernes bidrag findes nedenfor.

Bidrag fra Mette Stürup, Finans Danmark

"Jeg har fået dette feedback fra mit bagland. Beklager det sene svar men det var svært i forhold til vinterferien.

Der hvor jeg møder CFCS, og hvad jeg samtidig synes godt om, er:

- *Strategisk samarbejdsform*
- *Deres trusselvurderinger*
- *Div. publikationer med gode råd*
- *Deres twitter-profil, hvor de advarer om fx 0-day sårbarheder og*
- *Deres deltagelse i FSOR.*

Alle disse ting, må CFCS meget gerne fortsætte med.

Og dette input.

Hvad fungerer godt i samarbejdet med CFCS mht. den virksomhedsrettede indsats?

- *Det er en stor fordel, at CFCS har adgang til både åbne og lukkede kilder. Der er tilfælde, hvor de ikke kan fortælle hvorfor de kommer med en specifik vejledning, men man ved altid, at der er en særlig grund til denne vejledning. Dette er information som man ellers ikke ville have til rådighed.*
- *Derudover kan de i et lukket rum dele konkrete efterretninger på HEMMELIGT niveau*

Hvilke udfordringer opleves i relation til CFCS mht. den virksomhedsrettede indsats?

- *Der kan være lukkethed omkring nogle hændelser, men det er typisk hændelser man ikke ville have adgang til ellers.*

Hvordan kan eventuelle ovenstående udfordringer løses?

- *Jeg mener overordnet, at organiseringen er rigtig.*
- *Der er dog udfordringer ift. teleområdet. Her bør man overveje en anden organisering.*

Hvilke tiltag vil kunne styrke CFCS' virksomhedsrettede indsats?

- *Deres vejledninger er tit rettet mod store virksomheder. Der mangler mere til SMV segmentet. Her skal det være mere konkret, fx standarder osv."*

Bidrag fra Michael Warrer, CIO/IT-chef NRGi

"Fra min stol og virksomhed, kan jeg ikke mærke forskel fra før eller efter de berømte 500mdk kom til. Jeg synes CFCS er meget usynlige og savner at de er mere pro mod virksomheder af alle størrelser.

Ja der kommer noget på twitter, men kigger man det igennem er det meget lidt om varsler eller vidensdeling og ved godt de ikke må dele alt. Jeg ved også de ikke skal og kan konkurrere med private aktører om vidensdeling men jeg synes det kan gøres bedre. Den private vi bruger, kommer med 10-20 om ugen, CFCS har måske 1-3 om mdr.

Kan godt være jeg ikke har fulgt godt nok med, men afholder de netværksmøder, møder hvor viden kan deles, seminar om nyeste indenfor IT-sikkerhed mm altså proactive seminar

Jeg er sikker på CFCS gør et stort arbejde og stopper meget grimt trafik, men det burde de også vise / fortælle mere om. De laver en fin trusselvurdering, men den burde komme hvert kvartal hvor man på bagkant så kunne se alt det gode de gør og se en mere opdateret trusselvurdering.

Det er bare lige lidt fra min side, som jeg gerne uddyber over telefon eller møde, det er lidt nemmere."

Bidrag fra Tom Engly, Chief Security Officer, TRYG og Henning Mortensen, Formand, Rådet for Digital Sikkerhed

Henning Mortensen og Tom Engly har meddelt at høringssvaret fra Rådet for Digital Sikkerhed repræsenterer deres holdning til sagen.
Høringssvaret er vedlagt som bilag.

Bilag

- Bidrag fra Rådet for Digital Sikkerhed: ”CFCS placering og samarbejdsmuligheder – final”