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