Forsvarsministeriet
Holmens Kanal 9
1060 København K

# Rådet for Digital Sikkerheds høringssvar til Lov om ændring af Lov om Center for Cybersikkerhed

Rådet for Digital Sikkerhed (herefter Rådet) takker for muligheden for at afgive bemærkninger til udkastet til Lov om ændring af Lov om Center for Cybersikkerhed, som er sendt i offentlig høring d. 8. januar d.å.

Rådet har først og fremmest noteret sig, at regeringen har god fokus på informations- og cybersikkerhed. Der er gennem det seneste år iværksat mange gode tiltag. Finansministeriets strategi for cyber- og informationssikkerhed, Digitaliseringsstyrelsens portal Sikker Digital, Erhvervsstyrelsen og Rådets Sikkerhedstjekket, Erhvervsstyrelsens Privacy-kompas, som er ved at blive moderniseret, Justitsministeriets revision af Lov om TV-overvågning, Sektorstrategierne for sikkerhed og senest men ikke mindst nu revisionen af Lov om Center for Cybersikkerhed. Rådet er meget tilfredse med regeringens fokus. Det er afgørende for, at borgerne kan have tillid til digitalisering af samfundet, at der er god fokus på informationssikkerhed i både den offentlige og private sektor. Alle regeringens tiltag bidrager på forskellig vis hertil.

Rådets skal med dette brev komme med sine bemærkninger til ovennævnte lov.

## Bemærkninger til Lov om ændring af Lov om Center for Cybersikkerhed

Rådet har overordnet noteret sig, at Center for Cybersikkerhed (herefter CFCS) har et ønske om at udvide sine muligheder for at gribe ind forskellige steder i den digitale infrastruktur med det formål at understøtte et højt informationssikkerhedsniveau ved at opdage, analysere og bidrage til at imødegå sikkerhedshændelser. Rådet mener, at de udfordringer CFCS søger at løse er af kritisk betydning for rigets sikkerhed og stabilitet, hvorfor vi støtter op om behovet for at øge sikkerheden på den kritiske infrastruktur, hvor dette lovforslag er en ud af flere potentielle løsninger. Rådet mener samtidig, at det er vigtigt løbende at vurdere, om CFCS har de rette midler for at beskytte danske interesser i lyset af den teknologiske udvikling tillige med udviklingen i trusselsbilledet. Det er ved en sådan vurdering helt centralt, at midlerne er proportionale henset til borgernes fundamentale rettigheder i et demokratisk samfund og private virksomheders

interesser og behov for at holde deres data fortrolige. En række af de midler, som fremgår af lovforslaget, kan i Rådets optik ikke anses for at leve op til et sådant proportionalitetsprincip.

Rådet bemærker dog, at hvor lovforslaget har en række fundamentale problemer, så er den underliggende problemstilling, der søges adresseret af en sådan vigtighed, at det er afgørende, at der findes holdbare løsninger hertil. Hvor det er Rådets opfattelse, at lovforslaget som det foreligger ved høringen ikke er denne løsning, kan elementer heraf alligevel danne inspiration for løsninger. Eksempelvis kunne man overordnet opnå den underliggende målsætning ved at 1) Sætte minimumskrav til sikkerhed og beredskab for de organisationer, der indgår i den kritiske infrastruktur; 2) Opsætte CFCS services til krypteret modtagelse af relevante anonymiserede sikkerhedshændelser og/eller logninger; 3) Opsætte en statslig pulje af økonomiske midler til finansiering af de nødvendige tiltag og værktøjer ude i de enkelte organisationer. På denne vis opnås det ønskede formål, samtidig med at virksomheder og privates rettigheder respekteres, og tilgang til reel data stadig kan betinges af en dommerkendelse.

Med en sådan alternativ tilgang i tankerne findes nedenfor Rådets øvrige bemærkninger til lovforslaget, som det foreligger ved høringen.

**Sikkerhedssoftware og adgang til stationære data**
Forslagets § 3, stk. 1 indebærer jf. bemærkningerne p. 50, at CFCS fremadrettet skal kunne monitorere de tilsluttedes forbindelse til internettet, skal kunne installere sikkerhedssoftware på lokale enheder hos de tilsluttede og overføre oplysninger fra den tilsluttedes egne sikkerhedssystemer til CFCS. Videre fremgår det af § 4, at der lægges op til, at CFCS får adgang til stationære data – foruden de trafik- og pakkedata, som CFCS allerede har adgang til. I § 15 lægges der videre op til, at CFCS kan foretage automatiserede analyser af trafikdata, pakkedata og stationære data. Disse kan suppleres af manuelle analyser.

Rådet noterer sig, at det er en betydelig udvidelse af de beføjelser, som CFCS har i dag. I dag kan CFCS alene opsamle trafik- og pakkedata på ydersiden af den tilsluttedes firewall. I fremtiden er det med forslaget tanken, at CFCS kommer dybt ind i den tilsluttedes infrastruktur og kan tilgå alle data. CFCS vil dermed få adgang til forretningshemmeligheder, alle oplysninger om ansatte, kunder og borgere, de ansattes private filer m.v. Rådet har noteret sig, at CFCS ikke får adgang til internetudbydernes kunders kommunikation og dermed som udgangspunkt ikke borgernes private kommunikation med hinanden.

I forslaget præciseres det ikke, hvilken sikkerhedssoftware CFCS har i tankerne at installere i de tilsluttede myndigheder og virksomheders infrastruktur. Der gives dog flere steder indikationer af softwarens funktionalitet[1], der bl.a. omfatter:

[1] "unormal aktivitet" (p. 12), "blokere, omdanne eller omdirigere" (p. 16), "reagere på kendte signaturer" (p.17), "opdage uregelmæssigheder… på enkelte enheder (f.eks. pc'er)" (p. 18) og "servere, smartphones og tablets" (p. 18), "beskyttelse af netværk, der ikke er forbundet til internettet" (p. 18), "tilgå data, som opbevares på en lokal enhed" (p. 18), sammenligning med "antivirus-software" (p. 19), "uregelmæssigheder i de processer, der er aktiveret på enheden eller i de netværk, som enheden er tilknyttet" (p. 19), "opdage afvigelser fra normalbilledet" (p. 19), "forebyggende sikkerhedstekniske undersøgelser… [der]… afdække[r] områder og sårbarheder (p. 21), "simuleret

Logopsamling fra systemer og end-points og opsamling af flowdata på indersiden af firewallen, således at der kan reageres på baggrund af på forhånd definerede genkendelse af trafikmønstre og angrebsvektorer. Der er formodentlig desuden tale om forskellige produkter til overvågning af end-points, hvor der søges efter malware, kontakt til skadelige sider og analyseres afvigende brugeradfærd (logon på mærkelige tidspunkter, kopiering af større mængder filer, osv.). Der er videre formodentlig tale om analyse af netværkstrafik og for så vidt angår den aktive software, mulighed for at reagere på cyberangreb i realtid. På netværk og endpoints kan der søges efter bestemte signaturer. Der tales videre om at gennemføre skanninger på ydersiden af firewallen med henblik på at identificere og udnytte sårbarheder. Der tales om at overvåge systemprocesser og services. Videre nævnes der nogle få sikkerhedsteknologier eller begreber: spearphishing mails, spredning af skadelige usb-nøgler, anvendelsen af honeypots og sinkholes samt social engineering. Der er med andre ord tale om en bred vifte af teknologier med funktionalitet, som allerede udbydes af det private marked, og allerede mange steder er installeret af myndigheder og virksomheder.

Rådet finder, at anvendelsen af disse teknologier er rigtig fornuftige sikkerhedstiltag. Anvendelsen af dem bør baseres på en risikovurdering, og hvor risici tilsiger det, kan de med fordel implementeres som korrigerende foranstaltninger.

CFCS vil med disse softwareteknologier kunne få adgang til alle de tilsluttede myndigheder og virksomheders data – herunder forretningskritiske data, strategiske data, intellectual property rights, personoplysninger i form af sundhedsoplysninger, biometriske data, genetiske data, sagsbehandling relateret til etnisk tilhørsforhold, oplysninger om seksuelt, politisk, religiøst og filosofisk tilhørsforhold om ansatte hos de tilsluttede (følsomme personoplysninger) (se f.eks. bemærkningerne p. 18, 24, 61 og 62) (endda med mulige ansættelsesretlige konsekvenser), sagsbehandling om landets mest udsatte borgere (se f.eks. beskrivelsen p. 59), CPR-numre, personalefiler for de ansatte hos tilsluttede (fortrolige personoplysninger) og en lang række andre oplysninger – f.eks. fra de ansatte eller data om kunder, som er lagret (almindelige personoplysninger). Teknologierne kan således i vid udstrækning anvendes til at krænke privatlivets fred, som adresseret i Grundlovens § 72. I lovforslaget bemærkes det da også, at installation af software og undersøgelse af data på lokale enheder kræver særskilt lovgivning for ikke at være i modstrid med Grundlovens § 72. Udgangspunktet for § 72 er, at myndighederne ikke må krænke privatlivets fred. Helt undtagelsesvist kan der laves lovgivning, som under særligt vigtige omstændigheder kan tilsidesætte borgerens ret efter Grundloven – f.eks. hvis politiet jager en forbryder i et hus, og ikke kan nå at indhente dommerkendelse. Der skal således foretages en proportionalitetsvurdering mellem to hensyn. Rådet bemærker, at de grænser, der i lovforslagets bemærkninger pp. 55-60 søges opstillet for CFCS adgang til de tilsluttedes data, er uklare. Rådet er således usikker på, i hvilket omfang CFCS foruden søgning med software faktisk vil have adgang til

angreb" (p. 21), "dokumentere potentielle angrebsvektorer og sårbarheder" (p. 21), "skanninger på ydersiden… i søgen efter åbne netværksadgange, tjenester og sårbare applikationer" (p. 23 og p. 60), "social engineering" (p. 23 og p. 61), "spear-phishing" mails (p. 24 og p. 61), usb-nøgler, "honeypots og sinkholes" (p. 26 og p. 62), "monitorering af netværkstrafik og monitorering via lokal sikkerhedssoftware" (p. 55), "kørende systemprocesser og services" (p. 55), "logfiler" (p. 55), "reagere på cyberangreb i realtid" (p. 58).

med andre - herunder manuelle midler - at tilgå de tilsluttedes data. Rådet bemærker videre, at denne præcisering bør fremgå af loven og ikke alene af bemærkningerne.

Foruden privacy problemet vil det for internationale virksomheder være problematisk at lagre data om udviklingsprojekter i et land, hvor efterretningstjenesten systematisk tilgår data. Tilsvarende vil det være problematisk at iværksætte udviklingsprojekter i sådanne lande. Endelig er der en risiko for, at danske virksomheder ikke kan indgå som partner i sådanne udviklingsprojekter. Der er derfor en risiko for, at internationale virksomheder vil gå uden om Danmark, når der skal besluttes, hvor udviklingsprojekter kan foregå.

*Rådet mener, at de foreslåede adgange for en myndighed i en efterretningstjeneste ikke lever op til et gængs proportionalitetsprincip for et demokratisk samfund, givet mængden af kritiske data og personoplysninger der søges tilgået uden dommerkendelse. Rådet anbefaler, at det præciseres og afgrænses præcist i hvilket omfang og med hvilke midler, CFCS kan tilgå de tilsluttedes data. Videre er det en udfordring for danske virksomheder, at CFCS kigger med i fortrolige internationale projekter.*

**Påbud**
I henhold til forslagets § 3, stk. 4 er det hensigten, at CFCS kan påbyde, virksomheder, regioner og kommuner, der har særligt samfundsvigtig karakter at blive tilsluttet netsikkerhedstjenesten. Videre følger det af § 3, stk. 4 at de parter, der har modtaget påbud skal medvirke til netsikkerhedstjenestens opsætning og drift af hardware og software.

Rådet noterer sig, at det foreslåede påbud gælder tilslutning til CFCS. Rådet skal igen bemærke, at man kunne forestille sig alternative veje til at arbejde med påbud. F.eks. kunne man give myndigheder og virksomheder indenfor kritisk infrastruktur påbud om at udarbejde risikovurderinger og/eller påbud om at installere konkrete tekniske sikkerhedsforanstaltninger, som de selv administrerer, uden at CFCS skal have adgang til data eller kun begrænset anonymiseret adgang. Det er vigtigt at overveje, hvordan man kan gøre påbud så lidet indgribende overfor data, som muligt. Slutteligt kunne man igen gøre disse tiltag statsfinansieret igennem en pulje, hvorfra virksomhederne kan søge omkostningsdækning for tilslutningsomkostninger. Dette vil bidrage til en tættere tilslutning og derved øget sikkerhed i den kritiske infrastruktur.

*Rådet mener, at det bør være op den enkelte myndighed eller virksomhed, hvilke sikkerhedsforanstaltninger de ønsker at tage – herunder om de ønsker tilslutning til CFCS. Rådet anbefaler, at hvis man vil påbyde myndigheder og virksomheder sikkerhedsforanstaltninger, at dette så gøres på så lidet en indgribende måde som muligt, og hvor omkostninger hertil afholdes af staten.*

**Aktiv versus passiv sikkerhedssoftware**
Forslagets § 6, stk. 1 lægger op til, at den software, som installeres hos myndigheder og virksomheder, kan være aktiv og blokere, omdanne eller omdirigere trafik- og pakkedata. I § 6, stk. 2 fastslås det, at tilsvarende finder anvendelse for stationære data – tillige med sletning.

Endelig lægges der i §§ 6a-c op til, at CFCS kan gennemføre sikkerhedstekniske undersøgelser, installere sikkerhedssoftware, tilgå offentlige informationer andre steder og rette forebyggelsesaktiviteter mod enkelte medarbejdere, tillige med muligheden for at gøre brug af honeypots og sinkholes.

*Rådet bemærker igen, at vi ikke finder det proportionalt at gennemføre de skitserede tiltag og anbefaler i stedet alternative tilgange med samme målsætning.*

**Sletning ved videregivelse**
I § 17 lægges der op til en forlængelse af slettefristerne.

*Henset til den tid, der som gennemsnit går før en sikkerhedshændelse opdages, og i tilknytning hertil, hvor længe det tager at efterforske en sag – særligt APT-angreb, som må antage at være CFCS fokus-område – har Rådet ikke overordnet bemærkninger til de forlængede slettefrister.*

I henhold til § 17, stk. 5 lægges der op til, at hvis data er videregivet, skal slettefristerne angivet i § 16 ikke gælde. Herefter gælder der jf. forslagets § 17, stk. 6, at personoplysninger skal slettes, når de sikkerhedstekniske undersøgelser er afsluttet. Det præciseres videre p. 34, at data i medfør af § 17, stk. 1 skal slettes, når formålet med behandlingen efter konkret vurdering er udtømt. Det forekommer på den baggrund uklart, i hvilket omfang videregivne data skal slettes.

*Rådet mener ikke, at videregivelse kan fravige sletningskrav for data, hvis formål er opfyldt. Rådet skal derfor henstille til 1) at det fastslås at alle data – inkl. videregivne data – slettes når formålet er opfyldt og 2) at der ligesom på det persondataretlige område fastlægges et krav om underretning ved sletning, således at de aktører, til hvem data er videregivet, underrettes om at CFCS har foretaget sletning, og at modtagere derfor skal overveje, om de forsat skal lagre data.*

**Andre forhold**
Med forslaget lægges der i § 7 samt §§ 7a-f op til at vedtage editionsbestemmelser og i § 8 op til at undtage CFCS fra Lov om retssikkerhed.

*Rådet har ikke bemærkninger til disse undtagelser.*

**Konkurrence**
I tal kan man af CFCS' årsberetning for 2017 se, at der var 39 tilslutningsaftaler fordelt på 25 civile myndigheder, 12 militære myndigheder og 2 private virksomheder[2]. I høringsmaterialets side 11 fastslås det, at "relativt få myndigheder og virksomheder er tilsluttet netsikkerhedstjenesten, og at der dermed er mange samfundsvigtige virksomheder, som ikke får monitoreret deres internettrafik for avancerede cybertrusler". Det lægges således til grund af Forsvarsministeriet, at fordi der er så relativt få tilslutninger, så sker der ikke en monitorering af internettrafik for avancerede cybertrusler. For at løse dette problem lægges der p. 14 op til at gøre tjenesten gratis.

[2] https://fe-ddis.dk/cfcs/publikationer/Documents/CFCS_Beretning_2017.pdf, p. 4.

*Rådet vil gerne rejse tvivl om, hvorvidt mange samfundsvigtige myndigheder ikke får monitoreret deres internettrafik for avancerede trusler. Rådet er af den opfattelse, at der på det private marked findes mange sikkerhedsteknologier, der monitorerer internettrafik for avancerede cybertrusler. Rådet finder, at det er uheldigt signal, at Forsvarsministeriet ikke tillægger nogen videre vægt til den betydelige effekt disse private leverandører har på sikkerheden i Danmark. Det bemærkes, at den lavere tilslutning til CFCS ligeledes kunne skyldes, at det udbudte produkt står konkurrencemæssigt svagere på funktionalitet og/eller pris ift. det private marked, eller at CFCS' formål som efterretningstjeneste opfattes som i uoverensstemmelse med de kommercielle virksomheders interesser. Det er meget tænkeligt, at CFCS' produkt ikke foretrækkes af virksomheder og myndigheder, i forhold til alternativer fra det private marked.*

Forsvarsministeriet hævder flere steder i høringsmaterialet at både de eksisterende tiltag med monitorering af trafik via sensorer såvel som de fremtidige tiltag, hvor der skal installeres software, der kan reagere aktivt og tilgå stationære data, ikke påvirker det private marked for IT-sikkerhedsprodukter og -services - f.eks. pp. 14, 16, 19, 22, 25 og 29. Argumentet som gives af Forsvarsministeriet er bl.a., at den tjeneste, som CFCS stiller til rådighed, er efterretningsbaseret, hvilket de private tjenester ikke er. Da de nødvendige tekniske tiltag for at opnå CFCS' ønskede formål er tilgængelige på det private marked, finder Rådet ikke dette argument overbevisende.

*Rådet er af den opfattelse, at lovforslaget vil have en meget betydelig konkurrenceforvridende effekt. Rådet skal derfor anbefale, at CFCS i stedet for at tilbyde software, tilbyder efterretningsmæssig information og lader denne indgå i den software, der allerede findes på markedet. Konkret foreslås det, at CFCS stiller f.eks. efterretningsbaseret information om skadelige IP-adresser, signaturer af malware m.v. til rådighed for de tilsluttede myndigheder og virksomheder til indlejring i deres sikkerhedssoftware.*

Rådet noterer sig videre, at det p. 15 nævnes, at CFCS i visse tilfælde alene vil tilbyde sin gratis service til én virksomhed i en given branche. Rådet skal bemærke, at i henhold til GDPR pålægges myndigheder og virksomheder at implementere betydelige organisatoriske og tekniske sikkerhedsforanstaltninger. Dette har betydelige omkostninger for virksomhederne. Med forslaget p. 15 er der altså én virksomhed i hver branche, som potentielt kan spare millioner af kroner på at foretage investering i sikkerhedsprodukter ved blot at anvende CFCS i stedet. Dette vil også medvirke til at skabe konkurrenceforvridning i disse brancher.

*Rådet er af den opfattelse, at forslaget ikke alene vil skabe konkurrenceforvridning på IT-sikkerhedsmarkedet, men også potentielt på de markeder, der er omfattet af kritisk infrastruktur.*

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

På bestyrelsens vegne

Henning Mortensen
Formand, Rådet for Digital Sikkerhed