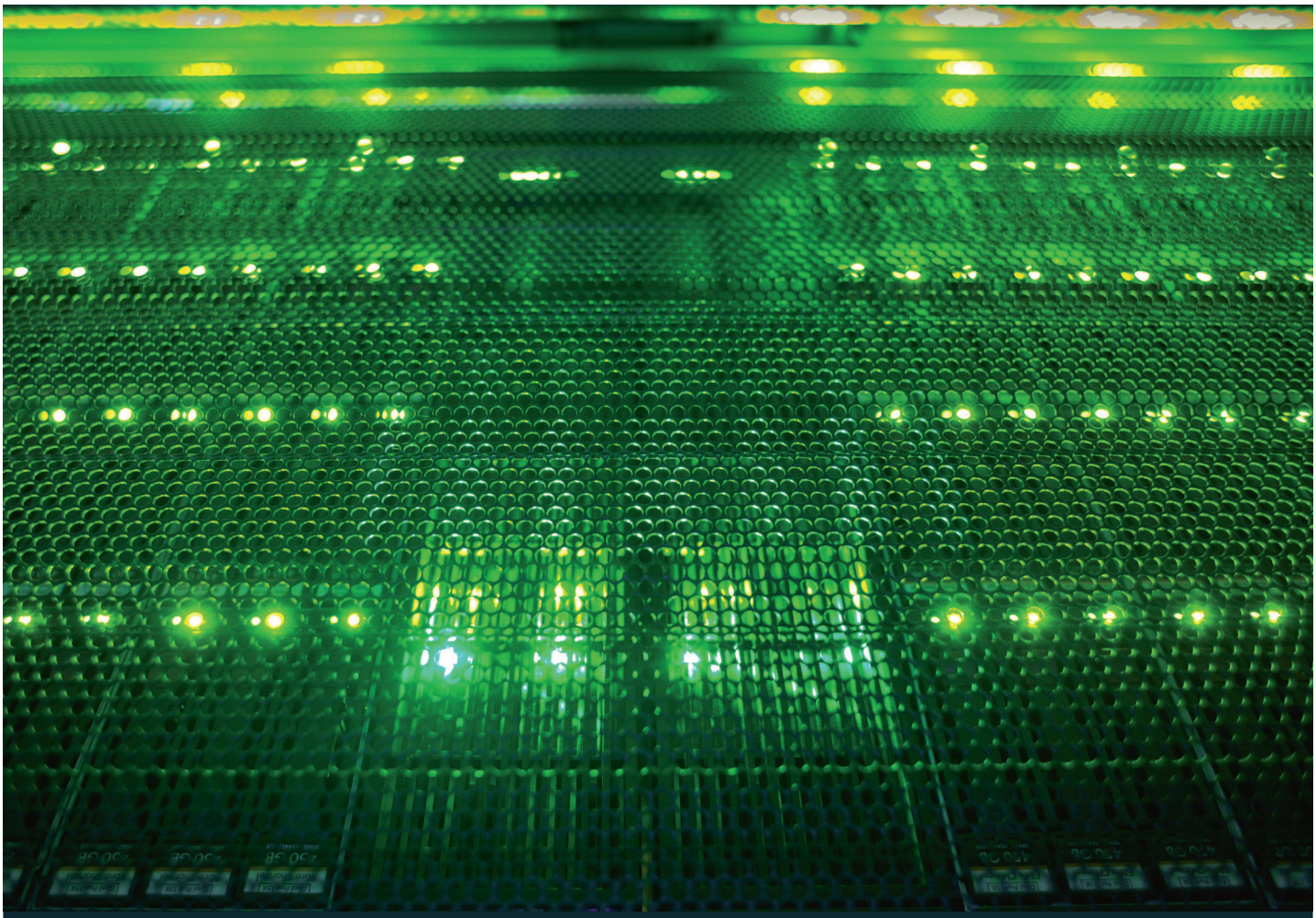
Forsvarsudvalget 2016-17
FOU Alm.del Bilag 97
Offentligt

FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE



Rapport om erfaringerne med lov om Center for Cybersikkerhed

Indholdsfortegnelse

Bilag 1 - Tilsynet med Efterretningstjenesternes bidrag til evalueringen af 25. april 2017.

Bilag 2 – Professor, dr. jur. Henrik Udsens bidrag til evalueringen af 10. maj 2017.

Bilag 3 – Center for Cybersikkerheds bidrag til evalueringen af 12. juni 2017.

1. Indledning

Forslag til lov om Center for Cybersikkerhed[1] blev fremsat den 2. maj 2014 på baggrund af en politisk aftale mellem den daværende regering (Socialdemokratiet og Radikale Venstre), Dansk Folkeparti, Det Konservative Folkeparti, Socialistisk Folkeparti og Venstre. Forslaget blev efterfølgende vedtaget den 11. juni 2014 af et bredt flertal i Folketinget, og den 1. juli 2014 trådte lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed (CFCS-loven) i kraft.

Af den politiske aftale, der er gengivet i den skriftlige fremsættelsestale og omtales i bemærkningerne til lovens § 24, fremgår, at der senest 3 år efter lovens ikrafttræden skal udarbejdes en rapport om erfaringerne med loven, som skal oversendes til Folketinget. Af den politiske aftale fremgår endvidere, at der til brug for rapporten skal indhentes bidrag fra Center for Cybersikkerhed (CFCS) om centerets almindelige erfaringer med hensyn til den nye lovgivning og Tilsynet med Efterretningstjenesterne om centerets overholdelse af den nye lovgivning. Endelig fremgår det, at Forsvarsministeriet i forbindelse med evalueringen vil indhente bidrag fra en eller flere uafhængige eksperter på cyberområdet, der skal medvirke til at belyse den nye lovgivnings betydning for kvaliteten og effektiviteten af CFCS' opgavevaretagelse.

Forsvarsministeriet har på den baggrund til brug for nærværende rapport indhentet bidrag fra henholdsvis Tilsynet med Efterretningstjenesterne (bilag 1), professor, dr. jur. Henrik Udsen fra Center for Informations- og innovationsret ved Københavns Universitet, der har mange års erfaring med cyberområdet og persondataret (bilag 2), og CFCS (bilag 3).

2. Oprettelsen af Center for Cybersikkerhed

Ved kongelig resolution af 3. oktober 2011 blev ressortansvaret for sager om beskyttelse af kritisk it-infrastruktur samt statens varslingstjeneste for internettrusler – det daværende GovCERT – overført til Forsvarsministeriet. CFCS blev efterfølgende oprettet som en del af Forsvarets Efterretningstjeneste (FE) den 18. december 2012, og den 1. juli 2014 trådte CFCS-loven med tilhørende retningslinjer vedrørende behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste af 30. juni 2014 (CFCS-retningslinjerne)[2] i kraft. Dele af CFCS's virksomhed var frem til CFCS-lovens ikrafttræden reguleret af lov nr. 596 af 14. juni 2011 om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v. (GovCERT-loven).

CFCS' hovedopgave som national it-sikkerhedsmyndighed er at bidrage til et højt sikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur (ikt-infrastruktur), som samfundsvigtige funktioner er afhængige af. Denne opgave løses bl.a. ved, at CFCS' netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder på Forsvarsministeriets område samt hos øvrige myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenestens netværk af alarmenheder.

Netsikkerhedstjenesten monitorerer løbende aktiviteterne på de tilsluttede myndigheders og virksomheders forbindelser til eksterne netværk, herunder internettet. Indsamlingen af data sker primært ved hjælp af

[1] L 192 FT 2013/14.
[2] https://fe-ddis.dk/cfcs/CFCSDocuments/Administrativeretningslinjer.pdf

elektroniske alarmenheder, som er opsat hos de enkelte myndigheder og virksomheder, hvor de monitorerer ind- og udgående netværkskommunikation, herunder internetkommunikation.

Som national it-sikkerhedsmyndighed varetager centeret desuden en række opgaver af både forebyggende og afhjælpende karakter, herunder oplysning, vejledning og rådgivning af danske myndigheder og virksomheder i at styrke cybersikkerheden, så risikoen for cyberangreb mindskes og imødegås – såfremt et angreb lykkes – på den mest hensigtsmæssige måde. I forlængelse heraf har centeret en løbende dialog med relevante interessenter.

Som national it-sikkerhedsmyndighed – herunder ligeledes i relation til EU og NATO – er det endvidere CFCS' opgave at sikkerhedsgodkende og føre tilsyn med klassificerede produkter, systemer og installationer inden for informations- og kommunikationsteknologi.

Endelig har CFCS ressortansvaret for informationssikkerhed og beredskab i telesektoren, og som led heri fører CFCS tilsyn med overholdelsen af lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed (NIS-loven), der trådte i kraft den 1. juli 2016, og tilhørende bekendtgørelser[3].

CFCS offentliggør hvert år en beretning, der gengiver centerets resultater det pågældende år. Indtil videre er der udgivet beretninger for 2014 og 2015, som er tilgængelige på centerets hjemmeside[4], og beretningen for 2016 forventes offentliggjort i juli 2017.

3. Erfaringer med lov om Center for Cybersikkerhed

3.1. Placering ved Forsvarets Efterretningstjeneste

Det fremgår af CFCS-lovens § 1, at CFCS organisatorisk er en del af Forsvarets Efterretningstjeneste (FE). CFCS blev placeret ved FE, da man dermed kunne drage nytte af FE's erfaringer inden for it-sikkerhedsområdet, tjenestens viden om det internationale trusselsbillede samt særlige adgang til oplysninger fra udlandet om cybertrusler[5].

Som det fremgår af "Efterretningsmæssig Risikovurdering 2016"[6], er cybertruslen, særligt fra cyberspionage, men også fra cyberkriminalitet, mod Danmark meget høj. Cyberspionage mod offentlige myndigheder og private virksomheder udgør fortsat den alvorligste cybertrussel mod Danmark og danske sikkerhedspolitiske og samfundsøkonomiske interesser. Der er tale om en særdeles aktiv trussel, og danske myndigheder og virksomheder er løbende udsat for forsøg på cyberspionage. Truslen er især kommet til udtryk over for

[3] Bekendtgørelse nr. 564 af 1. juni 2016 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv., bekendtgørelse nr. 565 af 1. juni 2016 om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet, bekendtgørelse nr. 566 af 1. juni 2016 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed og bekendtgørelse nr. 567 af 1. juni 2016 om informationssikkerhed og beredskab i net og tjenester.
[4] https://fe-ddis.dk/cfcs/publikationer/Pages/publikationer.aspx
[5] Lovforslag nr. 192 fremsat den 2. maj 2014 om Center for Cybersikkerhed, afsnit 2.1.
[6] https://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/Risikovurdering2016.pdf

myndigheder af betydning for dansk udenrigs- og sikkerhedspolitik samt private virksomheder inden for forskningstunge og højteknologiske industrier og sektorer.

Det fremhæves videre, at en række lande systematisk benytter cyberspionage som et middel til at opnå industrielle og forretningsmæssige fordele samt til at understøtte deres politiske og økonomiske interesser. Det er sandsynligt, at aktørerne bag cyberspionagen er knyttet til disse landes sikkerheds- og efterretningstjenester. Truslen mod Danmark udspringer især fra lande, der forsøger at positionere sig politisk og økonomisk, og hvor landenes sikkerheds- og efterretningstjenester har en central magtposition.

Det er på den baggrund af afgørende betydning for centerets muligheder for at imødegå cyberangreb rettet mod Danmark, at man har adgang til den viden, som FE i kraft af funktionen som udenrigsefterretningstjeneste har om udenlandske aktører på området samt tjenestens veletablerede samarbejde med udenlandske efterretningstjenester.

Placeringen ved FE skaber således en række synergieffekter og sikrer samtidig, at centeret i indsatsen for at styrke Danmarks robusthed mod cyberangreb har adgang til den særlige efterretningsmæssige viden, som tjenesten råder over på cyberområdet.

3.2. Center for Cybersikkerheds netsikkerhedstjeneste

3.2.1. Netsikkerhedstjenestens opgaver

Netsikkerhedstjenestens opgaver er beskrevet nærmere i CFCS-lovens § 3, hvoraf fremgår, at netsikkerhedstjenestens opgave er at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos de tilsluttede virksomheder og myndigheder, samt myndigheder på Forsvarsministeriets område.

I praksis betyder dette typisk, at netsikkerhedstjenesten ved hjælp af elektroniske alarmenheder opsat lokalt hos de tilsluttede myndigheder og virksomheder løbende monitorerer aktiviteterne på forbindelser til eksterne netværk, herunder internettet. Netsikkerhedstjenesten monitorerer således ind- og udgående netværkskommunikation, herunder internetkommunikationen. Derudover udsender netsikkerhedstjenesten varslinger samt yder bistand, hvis en tilsluttet myndighed eller virksomhed rammes af en alvorlig sikkerhedshændelse.

Netsikkerhedstjenesten blev etableret bl.a. ved en sammenlægning af den daværende statslige varslingstjeneste for internettrusler (GovCERT), der blev oprettet som en del af IT- og Telestyrelsen i 2009, samt varslingstjenesten på Forsvarsministeriets område (MILCERT), der blev oprettet i 2010 som en del af FE. De to CERT'er (Computer Emergency Response Teams) udførte grundlæggende set de samme opgaver på henholdsvis det civile og det militære område, og en sammenlægning gjorde det derfor muligt at udnytte ressourcerne bedre, ligesom man også fik mulighed for at dele relevant viden om trusler med både civile og militære samarbejdspartnere samt deltage i både civile og militære samarbejdsfora. Som det fremhæves af CFCS, har den danske tilgang desuden vakt interesse i udlandet, ligesom den også er blevet brugt som inspiration til oprettelse af tilsvarende enheder i andre lande.

3.2.2. Kredsen af myndigheder og virksomheder der kan anmode om tilslutning til netsikkerhedstjenesten

Det følger af CFCS-lovens § 3, stk. 2, at de øverste statsorganer og statslige myndigheder, dvs. Folketinget med tilhørende institutioner, regenten og domstolene, efter anmodning kan blive tilsluttet netsikkerhedstjenesten. Det samme gælder efter CFCS-lovens § 3, stk. 3, for regioner og kommuner samt virksomheder, der er beskæftiget med samfundsvigtige funktioner, hvis CFCS konkret vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

CFCS-lovens § 3, stk. 3, var en delvis videreførelse af den tilsvarende bestemmelse i GovCERT-lovens[7] § 2, stk. 1, idet kredsen af virksomheder, der kan tilsluttes, blev udvidet fra at omfatte virksomheder, der er beskæftiget med kritisk infrastruktur, til at omfatte virksomheder, der er beskæftiget med samfundsvigtige funktioner. Som fremhævet af professor, dr. jur. Henrik Udsen, mødte denne udvidelse af kredsen af muligt tilslutningsberettigede virksomheder kritik i forbindelse med den offentlige høring, idet der blev udtrykt bekymring for, om kredsen af muligt tilsluttede blev for bred.

Udviklingen i antallet af tilsluttede kunder fremgår af CFCS' årlige beretninger[8]:

	2014	2015	2016
Tilsluttede kunder (civile / militære)	25/6	28/9	29/9
Sensorer / alarmenheder[9]	18/11	22/13	21/11
Midlertidigt tilsluttede virksomheder og myndigheder	1	0	0

I relation til antallet af midlertidigt tilsluttede virksomheder og myndigheder skal det bemærkes, at disse oplysninger ikke fremgik udtrykkeligt af beretningerne for 2014 og 2015, som påpeget af professor, dr. jur. Henrik Udsen. CFCS har i den forbindelse oplyst, at der var en midlertidigt tilsluttet virksomhed i 2014, som dog ikke fremgår af beretningen for 2014, men at der ellers ikke har været midlertidigt tilsluttede myndigheder eller virksomheder i hverken 2015 eller 2016, hvilket nu vil blive tydeliggjort, for så vidt angår 2016, i den kommende beretning for 2016.[10]

[7] Lov nr. 596 af 14. juni 2011 om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v.
[8] Center for Cybersikkerheds årsberetninger for 2014 og 2015.
[9] Det bemærkes, at antallet af tilsluttede kunder ikke er identisk med antallet af alarmenheder, da der kan være anvendt flere sensorer pr. kunde, ligesom en enkelt alarmenhed placeret hos en central it-leverandør kan dække flere kunder.
[10] Årsberetningen for 2016 forventes offentliggjort i juli 2017.

3.2.3. Omkostninger forbundet med tilslutning

Det er forudsat i bemærkningerne til CFCS-loven[11], at regioner, kommuner og virksomheder, der ønsker at blive tilsluttet netsikkerhedstjenesten, dækker de udgifter, der er forbundet med indkøb og/eller udvikling af evt. monitoreringsudstyr, samt centerets udgifter til monitoreringen.

Det er på den baggrund i bekendtgørelse nr. 1568 af 12. december 2016 om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste fastsat, at en tilsluttet region, kommune eller virksomhed betaler et årligt gebyr til dækning af udgifter, der er forbundet med tilslutningen og driften af alarmenheden. For 2017 udgør gebyret 300.000 kr. excl. moms pr. alarmenhed af typen NSS-1 og 400.000 kr. excl. moms pr. alarmenhed af typen NSS-2. De to typer af alarmenheder adskiller sig alene ved mængden af data, der kan håndteres ved kunden.

Det er CFCS' oplevelse, at regioner, kommuner og virksomheder, der ellers opfylder betingelserne for at blive tilsluttet i medfør af § 3, stk. 3, i visse tilfælde afholder sig fra at blive tilsluttet, som følge af størrelsen af det årlige gebyr forbundet med tilslutning, samt at dette er baggrunden for, at der kun har været en begrænset stigning i antallet af tilsluttede myndigheder og virksomheder i perioden siden centerets oprettelse.

CFCS har endvidere fremhævet, at en yderligere udbredelse af netværket af alarmenheder, vil sætte centeret i stand til at varsle hurtigere og bredere om trusler. Ligesom et forbedret datagrundlag vil styrke centerets trusselsvurderinger og centerets rådgivning til myndigheder og virksomheder om risici og passende sikkerhedstiltag.

Som fremhævet af professor, dr. jur. Henrik Udsen, var det et kritikpunkt i forbindelse med den offentlige høring, at CFCS ved udvidelsen af kredsen af tilslutningsberettigede virksomheder ville bevæge sig ind på det private marked, hvilket efter det oplyste fortsat er DI og IT-Branchens vurdering, såfremt prisen for tilslutning sænkes. CFCS oplever sig dog ikke som en konkurrent til det private marked – men derimod som et supplement – idet centeret primært beskæftiger sig med avancerede angreb samt anvender en efterretningsbaseret tilgang.

3.3. Indgreb i meddelelseshemmeligheden

3.3.1. Generelt om muligheden for at foretage indgreb i meddelelseshemmeligheden

GovCERT's adgang til uden retskendelse at behandle pakke- og trafikdata hidrørende fra netværk hos tilsluttede myndigheder og virksomheder på civile område efter GovCERT-lovens § 4, stk. 1, blev videreført med CFCS-lovens § 4 samt udvidet til også at omfatte det militære område, midlertidigt tilsluttede myndigheder og virksomheder samt informationssystemer med CFCS-lovens §§ 5 - 7.

CFCS fremhæver i den forbindelse, at det generelt har stor betydning, at en netsikkerhedstjeneste har adgang til at analysere den trafik, som tilgår de tilsluttede myndigheder og virksomheder fra internettet, og at der fortsat er tale om et uundværligt værktøj i centerets arbejde med at analysere internettrafikken og varsle om

[11] Lovforslag nr. 192 fremsat den 2. maj 2014 om Center for Cybersikkerhed, bemærkningerne til § 3.

sikkerhedshændelser og trusler. CFCS pointerer videre, at adgangen til at analysere data har betydet, at centeret bl.a. har kunnet identificere og efterfølgende medvirke til standsning af adskillige cyberangreb, der, hvis angrebene ikke var blevet standset, havde medført omfattende tab af beskyttelsesværdig information om beslutningsprocesser, men også tab af sensitiv information om danskere.

3.3.2. Sikkerhedstekniske undersøgelser

CFCS fremhæver, at centeret særligt efter oprettelsen af kompetencecenteret på SCADA-området[12] – men også generelt – oplever en stigende efterspørgsel efter, at centeret kommer ud til både myndigheder og virksomheder og hjælper disse med at vurdere sikkerheden i deres ikt-infrastruktur, herunder tester sikkerheden. Der er imidlertid ikke i dag hjemmel til at foretage indgreb i meddelelseshemmeligheden i forbindelse med gennemførelsen af sikkerhedstekniske undersøgelser, hvilket efter det oplyste begrænser centerets muligheder for at gennemføre de nødvendige sikkerhedstekniske undersøgelser.

3.3.3. Hostingselskaber

CFCS oplever i stigende grad udfordringer i forbindelse med, at myndigheder og virksomheder anvender hostingselskaber eller andre it-fællesskaber til at administrere og hoste deres systemer. Det skyldes, at de fleste af disse anvender såkaldte shared services, hvor flere kunder deler en server. Hvis en enkelt myndigheds eller virksomheds løsning er kompromitteret, og CFCS skal bistå myndigheden eller virksomheden med afhjælpning af angrebet ved at hjemtage den pågældende server til nærmere analyse, kræver dette skriftligt samtykke fra hver enkelt myndighed eller virksomhed. CFCS oplyser imidlertid, at denne udfordring er under håndtering via en styrkelse af samarbejdet med relevante myndigheder.

3.3.4. Monitorering på lokale netværk

Som nævnt monitorerer netsikkerhedstjenesten ved hjælp af elektroniske alarmenheder opsat lokalt hos de tilsluttede myndigheder og virksomheder løbende aktiviteterne på forbindelser til eksterne netværk, herunder internettet. Netsikkerhedstjenesten monitorerer således alene den ind- og udgående netværkskommunikation og ikke aktivitet, der foregår på de enkelte enheder på det lokale netværk hos de tilsluttede myndigheder og virksomheder, da disse ikke transporteres gennem alarmenheden. Dertil kommer, at den teknologiske udvikling har betydet, at indholdet af stadig mere netværkstrafik er utilgængeligt på grund af kryptering, hvilket i forhold til alarmenhederne kan betyde, at de indikatorer, som alarmenhederne er indstillet til at reagere på, ikke udløser en alarm.

CFCS-loven indeholder ikke hjemmel til monitorering af enheder på de lokale netværk, men en sådan løsning ville efter CFCS' opfattelse styrke centerets arbejde med at opdage og imødegå cyberangreb betydeligt på flere måder

[12] Ved SCADA-systemer forstås de industrielle styresystemer, der anvendes i en lang række industrielle processer, forsyningsinfrastrukturer (el, gas, vand, vind m.v.) og i større anlæg (jernbaner, lufthavne m.v.). SCADA-systemer anvendes f.eks. til fjernstyring af generatorer, pumper, ventilation m.v. Ofte er systemerne udviklet for en række år siden uden sikkerhed for øje, da systemerne typisk ikke var forbundne til omverdenen. I dag anvendes de samme systemer stadig, men nu vil de ofte være blevet forbundne med internettet med henblik på at kunne overvåge og styre processerne.

og dermed komplementere beskyttelsen fra alarmenhederne samt derudover muliggøre, at man kan se data efter dekryptering hos brugeren.

3.3.5. Aktivt netværk af alarmenheder

Alarmenhederne i netværket af alarmenheder er passive, hvilket betyder, at de alene kopierer den ind- og udgående trafik, hvorefter trafikken analyseres for ondsindet aktivitet. Hvis der udløses en alarm i alarmenhederne, håndteres denne efterfølgende af CFCS' netsikkerhedstjeneste. CFCS har i den forbindelse fremhævet, at CFCS-loven og den nuværende indretning af netværket af alarmenheder i dag ikke gør det muligt at imødegå ondsindede aktørers angrebsmetoder og værktøjer ved for eksempel aktivt – og evt. automatiseret – at standse igangværende angreb. CFCS vurderer, at en sådan løsning vil kunne sikre en bedre beskyttelse af de tilsluttede myndigheder og virksomheder.

3.4. Forholdet til offentlighedsloven og forvaltningsloven

Det følger af CFCS-lovens § 8, stk. 1, at CFCS' virksomhed er undtaget fra offentlighedsloven[13] (dog med undtagelse af offentlighedslovens § 13 om notatpligt) samt fra forvaltningslovens[14] kapitel 4-6 om partsaktindsigt, partshøring og begrundelse. Det fremgår imidlertid også af forarbejderne til bestemmelsen[15], at CFCS i videst muligt omfang forudsættes at efterleve principperne i de to love.

Antallet af aktindsigtsanmodninger, som CFCS har modtaget i perioden fra CFCS-lovens ikrafttræden og indtil udgangen af 2015, er nævnt i Tilsynet med Efterretningstjenesternes årsredegørelse[16]. Af TET's opgørelse fremgår endvidere, i hvilket omfang der er meddelt aktindsigt eller givet afslag:

	2. halvår 2014	2015
Fuld aktindsigt	0	0
Delvis aktindsigt	10	0
Afslag på aktindsigt	0	0
Ingen dokumenter lokaliseret til at give eller afslå aktindsigt	1	4

Efter det oplyste, er der ikke sket væsentlige ændringer i antallet af aktindsigtsanmodninger i 2016.

[13] Lov nr. 606 af 12. juni 2013 om offentlighed i forvaltningen (offentlighedsloven).
[14] Forvaltningsloven, jf. lovbekendtgørelse nr. 433 af 22. april 2014.
[15] Lovforslag nr. 192 fremsat den 2. maj 2014 om Center for Cybersikkerhed, punkt. 3.3.3 samt bemærkningerne til § 8.
[16] Se årsredegørelse for 2014 og 2015, side 18.

Som professor, dr. jur. Henrik Udsen fremhæver, har centeret kun i meget begrænset omfang modtaget anmodninger om aktindsigt, og der er ikke givet afslag på aktindsigt i perioden.

CFCS efterlever efter det oplyste principperne i både offentlighedsloven og forvaltningsloven, medmindre der er tale om en anmodning om adgang til netsikkerhedstjenestens indsamlede data eller dokumenter, der vedrører øvrige dele af FE, og som dermed har efterretningsmæssig karakter, hvilket er i overensstemmelse med bemærkningerne til loven[17].

Professor, dr. jur. Henrik Udsen fremhæver endvidere, at Forsvarsministeriet ikke har udnyttet muligheden efter CFCS-lovens § 8, stk. 2, for at sætte reglerne i offentlighedsloven og forvaltningsloven i kraft i forhold til 1) centerets behandling af anmodninger om tilslutning, 2) centerets virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet og 3) centerets personalesager. Han foreslår derfor, at det overvejes, om muligheden for at udstede en bekendtgørelse herom bør udnyttes. Forsvarsministeriet har imidlertid vurderet, at der ikke behov for dette, da alle sager er blevet behandlet efter principperne i de to love.

I relation til adgangen til aktindsigt skal det endelig bemærkes, at IT-Branchen over for professor, dr. jur. Henrik Udsen har påpeget, at nogle af organisationens medlemmer finder det uhensigtsmæssigt, at det ikke er muligt at få oplyst baggrunden for CFCS' trusselvurderinger.

3.5. Forholdet til persondataloven

CFCS er, som det fremgår af persondatalovens § 2, stk. 11 og CFCS-lovens § 8, stk. 1, undtaget fra persondatalovens regler om behandling af personoplysninger. Dette følger også af persondatalovens[18] § 2, stk. 11, da CFCS er en del af FE.

CFCS' behandling af personoplysninger er i stedet reguleret i CFCS-lovens kapitel 6, der er udformet med udgangspunkt i persondatalovens centrale principper for behandling af personoplysninger. Kapitel 6 suppleres endvidere af CFCS-lovens kapitel 7, der regulerer netsikkerhedstjenestens behandling af data, herunder personoplysninger, der indsamles ved monitorering af netværkskommunikation eller i øvrigt tilvejebringes ved indgreb i meddelelseshemmeligheden efter kapitel 4.

Baggrunden for de særlige regler i kapitel 7 var at begrænse behandlingen af disse oplysninger til situationer, hvor der er begrundet mistanke om en sikkerhedshændelse. Reglerne er således generelt mere detaljerede og restriktive end persondatalovens regler.

Reglerne om indsigtsret og oplysningspligt i persondataloven blev ikke medtaget i CFCS-loven, da dette ville medføre en række uhensigtsmæssigheder. Som et eksempel herpå nævnes i den kommenterede høringsoversigt[19], at netsikkerhedstjenesten i overensstemmelse med sit formål behandler store mængder data, hvor behandlingen alene har karakter af en rent teknisk behandling. De store mængder data indsamlet i alarmenhederne anvendes således til at danne et normalbillede af netværkskommunikation hos den tilsluttede myndighed eller virksomhed.

[17] Lovforslag nr. 192 fremsat den 2. maj 2014 om Center for Cybersikkerhed, punkt. 3.3.3.
[18] Lov nr. 429 31. maj 2000 om behandling af personoplysninger (persondataloven).
[19] Se høringsoversigten af april 2014, punkt. 2.

Det er kun i tilfælde af en konkret sikkerhedshændelse, at eksempelvis e-mails åbnes og analyseres, men hvis eksempelvis persondatalovens § 28, stk. 1, om oplysningspligt fandt anvendelse, ville centeret være nødsaget til at gennemse samtlige opbevarede data med henblik på at kunne orientere den registrerede om formålet med behandlingen af oplysningerne. En ikraftsættelse af eksempelvis reglerne om oplysningspligt ville således indebære et så stort ressourcebehov hos centeret, at det i praksis ikke ville være muligt at drive netsikkerhedstjenesten.

Professor, dr. jur. Henrik Udsen fremhæver i sit bidrag, at netop undtagelsen fra persondatalovens regler var et af de punkter, der mødte kritik og betænkeligheder i forbindelse med den offentlige høring[20]. Han nævner imidlertid også under henvisning til Tilsynet med Efterretningstjenesternes årsredegørelser, at denne kritik umiddelbart synes ubegrundet, idet centeret generelt set har efterlevet CFCS-lovens bestemmelser om behandling af personoplysninger, og at der i øvrigt ikke er fremkommet oplysninger, der kunne indikere, at personoplysninger ikke er blevet tilstrækkeligt beskyttet ved CFCS-lovens regulering. Tilsynet med Efterretningstjenesterne har ej heller modtaget klager over centerets behandling af personoplysninger[21].

I relation til muligheden for at sætte persondatalovens bestemmelser i kraft i forhold til 1) centerets behandling af anmodninger om tilslutning til netsikkerhedstjenesten, 2) centerets virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet og 3) centerets personalesager, påpeger professor, dr. jur. Henrik Udsen, at det bør overvejes, om denne hjemmel skal udnyttes.

Endelig påpeger professor, dr. jur. Henrik Udsen, at det i forbindelse med, at persondataforordningen[22] får virkning i maj 2018, selvom centerets aktiviteter falder uden for forordningens anvendelsesområde, bør overvejes, om der skal ske en tilpasning af CFCS-loven, så den afspejler de ændringer, der indføres med de nye persondataregler. Alternativt om man eventuelt skal tilpasse reglerne til direktivet om retshåndhævende myndigheders behandling af persondata[23], der blev implementeret ved lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger, der dog ej heller finder direkte anvendelse på CFCS' virksomhed.

3.6. Analyse, videregivelse og sletning af data

3.6.1. Analyse af data ved opsætning og kontrol af alarmenheder

Analyse af pakkedata og videregivelse af pakke- og trafikdata, der stammer fra alarmenhederne, forudsætter efter de nuværende regler i CFCS-lovens § 15 begrundet mistanke om en sikkerhedshændelse.

CFCS har i den forbindelse fremhævet, at den nuværende lovgivning skaber en række udfordringer i forbindelse med opsætning og efterfølgende kontrol af alarmenheder hos tilsluttede myndigheder og virksomheder, idet der i

---

[20] Se høringsoversigten af april 2014, punkt 2.
[21] Se årsredegørelse for 2014 og 2015, side 18.
[22] Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).
[23] Direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om for udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA.

forbindelse hermed kan være behov for at videregive data til den tilsluttede myndighed eller virksomhed for at identificere den service, der ligger bag en intern IP-adresse, og hvad der dermed genererer det pågældende datamønster i netværket. Det kan endvidere være relevant at analysere pakke- og trafikdata med henblik på at teste, at alarmenheden reagerer, som den skal. Kravet om begrundet mistanke om en sikkerhedshændelse betyder således i praksis, at det ikke i tilstrækkeligt omfang er muligt at foretage den beskrevne kontrol af, at alarmenheden fungerer efter hensigten.

3.6.2. Videregivelse af data

Ved begrundet mistanke om en sikkerhedshændelse har CFCS i medfør af CFCS-lovens § 16 mulighed for at videregive trafikdata til en afgrænset kreds af samarbejdspartnere samt til at udsende sikkerhedsvarslinger, der indeholder trafikdata. I forhold til det tidligere lovgrundlag er kredsen af samarbejdspartnere, hvortil der kan videregives trafikdata[24], nu udvidet til også at omfatte bl.a. teleselskaber. CFCS kan desuden videregive både trafik- og pakkedata[25] om sikkerhedshændelser til politiet, ligesom politiet underretter CFCS, når politiet bliver opmærksomt på relevante sager.

CFCS fremhæver i den forbindelse, at muligheden for at videregive data har været med til at understøtte centerets opgavevaretagelse. Sammenlignet med det øvrige FE har centeret en meget offentlig profil samt et aktivt udadvendt virke med stor fokus på at formidle viden, der kan bidrage til at understøtte et højt informationssikkerhedsniveau i den ikt-infrastruktur, som samfundsvigtige funktioner er afhængige af.

CFCS har et tæt samarbejde med netsikkerhedstjenester i udlandet, som bidrager med vigtige informationer, der øger centerets muligheder for at forebygge sikkerhedshændelser i Danmark. CFCS fremhæver i den forbindelse, at et effektivt internationalt samarbejde på myndighedsniveau er blevet muligt ved, at Danmark også kan videregive oplysninger til netsikkerhedstjenester i udlandet med henblik på, at dette kan bidrage til at stoppe grænseoverskridende cyberangreb rettet mod Danmark.

Antallet af sager, hvor der er sket videregivelse af oplysninger, er anført i Tilsynet med Efterretningstjenesternes årsredegørelser samt CFCS' bidrag til evalueringen.

CFCS påpeger dog også, at der har vist sig at være en række udfordringer forbundet med informationsdeling og muligheder for videregivelse af data efter de nuværende regler. Det er eksempelvis ikke muligt at videregive bl.a. malware[26], der er anvendt i forbindelse med et cyberangreb, til eksempelvis udenlandske partnere for at undersøge, om der kan tilvejebringes information, der yderligere kan kvalificere den konkrete sag. Det skyldes, at det ikke efter de nuværende regler er muligt at videregive malware, da malware som oftest er indeholdt i pakkedata, dvs. eksempelvis indholdet af en e-mail.

---

[24] Trafikdata er i CFCS-lovens § 2, nr. 3, defineret som data, der behandles med henblik på at transmittere pakkedata. Det vil sige data, som beskriver oprindelse, destination og rutestyringsinformation, herunder oprindelsesdomænet eller den oprindelige elektroniske adresse samt anden tilsvarende information. Som eksempler herpå kan nævnes e-mailadresser og hjemmesideadresser.

[25] Pakkedata er i CFCS-lovens § 2, nr. 2, defineret som indholdet af den kommunikation, der transmitteres gennem digitale netværk eller tjenester. Som eksempel herpå kan nævnes indholdet af en mail eller indholdet af tilgåede hjemmesider.

[26] Begrebet malware (sammentrækning af det engelske udtryk malicious software) er en samlebetegnelse for programkoder, der gør skadelige eller uønskede ting på de computere, hvorpå de kører.

3.6.3. Udveksling af data med de øvrige dele af Forsvarets Efterretningstjeneste

Da CFCS organisatorisk og i forvaltningsmæssig forstand er placeret under FE, er det almindelige udgangspunkt efter de forvaltningsretlige principper, at der kan ske intern udveksling af data. Den interne udveksling af data mellem CFCS og de øvrige dele af FE er ikke reguleret i CFCS-loven men derimod i Forsvarsministeriets retningslinjer vedrørende behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste af 30. juni 2014. Det betyder i praksis, at centeret kun under visse betingelser kan udveksle data med de øvrige dele af FE, og at FE kun i begrænset omfang kan videregive disse oplysninger til samarbejdspartnere.

Som anført af CFCS, er formålet med at udveksle oplysninger med FE at undersøge, om der i den efterretningsmæssige indhentning er informationer, der yderligere kan kvalificere den konkrete sag, herunder identifikation af angrebsaktør, oplysninger om angriberens kapaciteter og metoder. CFCS oplyser endvidere, at den bistand, som den efterretningsmæssige del af FE kan yde til netsikkerhedstjenestens videre arbejde i en konkret sag, er nødvendig for at understøtte et højt informationssikkerhedsniveau hos myndigheder og virksomheder fremadrettet.

Antallet af sager, hvor der er sket udveksling med de øvrige dele af FE, er anført i Tilsynet med Efterretningstjenesternes årsredegørelse samt CFCS' bidrag til evalueringen.

CFCS oplyser, at udviklingen i antallet af udvekslinger skal ses som udtryk for, at det i praksis har vist sig at være gavnligt for centerets opgaveløsning at kunne udveksle konkret information om angribernes redskaber og metodikker, idet der ofte kommer ny viden om angriberen, om andre berørte myndigheder eller virksomheder, som skal varsles og hjælpes, eller om nye hidtil ukendte redskaber fra angriberens side.

3.6.4. Muligheder for at gemme data

Det følger af CFCS-lovens § 17, at data, der er indhentet ved indgreb i meddelelseshemmeligheden og knytter sig til en konkret sikkerhedshændelse, kan opbevares i tre år, mens data, der ikke knytter sig til en sikkerhedshændelse, må opbevares i 13 måneder. Fristen for opbevaring af data, der ikke knytter sig til en sikkerhedshændelse, blev således i forhold til de gældende regler forlænget fra 14 dage til 13 måneder.

CFCS fremhæver i den forbindelse, at adgangen til historiske data har medført en betydelig styrkelse af centerets arbejde, da man på baggrund af disse data kan tegne et normalbillede af netværksaktiviteterne hos den enkelte myndighed eller virksomhed med henblik på at kunne konstatere, når der afviges herfra. Jo længere perioden, hvor der er adgang til at søge efter karakteristika, er, jo større er muligheden endvidere for at opdage hidtil uopdagede cyberangreb. Professor, dr. jur. Henrik Udsen lægger på den baggrund til grund, at lovbemærkningernes forudsætninger for at udvide slettefristen har vist sig at være relevante.

Centeret påpeger imidlertid også, at den nuværende begrænsede adgang til opbevaring af historiske data betyder, at CFCS ikke fuldt ud kan udnytte den viden om angriberens adfærd, som opbygges, når centeret har afdækket et angreb eller angrebsforsøg. Centeret oplyser i den forbindelse, at denne adfærd typisk vil ændre sig over tid, men at en angriber fra tid til anden typisk vender tilbage til velkendte og afprøvede teknikker, nogle gange med ganske lidt variation. Det er derfor væsentligt for centerets mulighed for at opdage og imødegå fremtidige angreb, at oplysninger om tidligere angreb i videst muligt omfang kan bevares.

Endelig oplyser CFCS, at forpligtelsen til sletning af oplysninger giver en række praktiske udfordringer i relation til muligheden for at tage back-up af oplysninger i centerets systemer og platforme og dermed sikre, at vigtige data ikke mistes.

3.7. Tilsynet med behandling af personoplysninger

3.7.1. Tilsynet med Efterretningstjenesterne

Tilsynet med Efterretningstjenesterne (TET) blev oprettet den 1. januar 2014[27] og er et uafhængigt kontrolorgan, der oprindelig alene havde til formål at føre tilsyn med, at Politiets Efterretningstjeneste (PET) og FE behandler oplysninger om fysiske og juridiske personer i overensstemmelse med lovgivningen. Ved CFCS-lovens ikrafttræden den 1. juli 2014 blev tilsynets opgaver udvidet til også at omfatte CFCS' behandling af personoplysninger.

TET påser på den baggrund, at CFCS overholder CFCS-lovens regler om indgreb i meddelelseshemmeligheden (kapitel 4), behandling (kapitel 6), analyse, videregivelse og sletning af personoplysninger (kapitel 7 og CFCS-retningslinjerne) samt kravene til sikkerhedsforanstaltninger (kapitel 8).

TET bistås i den forbindelse af et sekretariat, der alene er undergivet tilsynets instruktion. Tilsynet beslutter selv, hvordan sekretariatet sammensættes, og der lægges i den forbindelse – som fremhævet af professor, dr. jur. Henrik Udsen – særlig vægt på at sikre de fornødne it-kompetencer.

TET har mulighed for at kræve enhver oplysning og alt materiale, der har betydning for tilsynets arbejde, ligesom tilsynet også har ret til adgang til alle lokaler, hvorfra der er adgang til de behandlede oplysninger, samt hvor tekniske hjælpemidler anvendes. Endvidere kan tilsynet afkræve CFCS skriftlige udtalelser om faktiske og retlige forhold.

CFCS har således siden oprettelsen i juli 2014 været underlagt et særligt tilsyn med henblik på at sikre, at centeret behandler personoplysninger i overensstemmelse med CFCS-loven og CFCS-retningslinjernes bestemmelser herom.

TET har indtil nu afgivet én årsredegørelse til forsvarsministeren om tilsynets kontrol med CFCS for perioden 2014-2015, der er offentliggjort på TET's hjemmeside[28].

Tilsynets kontroller viser, som det også fremgår af tilsynets bidrag til nærværende rapport, at CFCS generelt har iagttaget lovgivningens bestemmelser vedrørende indgreb i meddelelseshemmeligheden, intern behandling af personoplysninger samt analyse, videregivelse og sletning af data, men at centeret fortsat er i proces med at implementere ISO 27001-standarden i forhold til sikkerhedsforanstaltninger.

3.7.2. Tilsynet med Efterretningstjenesternes årsredegørelse

I 2014 og 2015 foretog TET bl.a. kontrol af centerets videregivelse af oplysninger indhentet ved indgreb i meddelelseshemmeligheden til andre myndigheder, virksomheder eller samarbejdspartnere samt centerets

[27] Lov nr. 604 af 12. juni 2013 om Politiets Efterretningstjeneste (PET) § 16.
[28] www.tet.dk

udveksling af sådanne oplysninger med det øvrige FE. Begge dele viste, at centeret i alle tilfælde havde efterlevet lovgivningens krav. Tilsynet foretog derudover en kontrol af udvalgte arbejdsstationer, der viste, at centeret med undtagelse af ét enkelt tilfælde generelt set havde efterlevet lovgivningen. Det drejede sig mere konkret om manglende sletning af en række IP-adresser, der burde have været slettet, idet formålet med behandlingen var opfyldt. Endvidere gennemførte tilsynet en stikprøvekontrol af centerets behandling af personoplysninger i centerets elektroniske hændelseshåndteringssystem, der viste, at centeret fuldt ud havde efterlevet lovgivningen.[29]

Endelig gennemførte tilsynet en kontrol vedrørende centerets sikkerhedsforanstaltninger i forbindelse med behandlingen af personoplysninger, der også omtales i tilsynets bidrag til nærværende rapport. Der blev ved kontrollen taget udgangspunkt i ISO 27001-standarden samt de krav, der stilles i sikkerhedsbekendtgørelsen[30] og Datatilsynets vejledning herom[31], selvom disse i medfør af CFCS-lovens § 8 ikke finder direkte anvendelse. Kontrollen viste, at CFCS ikke fuldt ud levede op til kravene til sikkerhedsforanstaltninger indenfor 9 ud af 38 kontrollerede områder fra annex A i ISO 27001:2013. Hovedparten af disse risici blev imidlertid afhjulpet i løbet af 2015, og der er efterfølgende afgivet kvartalsvise orienteringer til tilsynet.[32] TET har endvidere efterfølgende oplyst, at man i 2016 havde afhjulpet hovedparten af de omhandlede risici, samt at centeret efter det oplyste var i gang med at afhjælpe de resterende.

4. Sammenfatning

Sammenfattende viser erfaringerne med lov om Center for Cybersikkerhed, at der med loven er blevet skabt et velfungerende retsgrundlag for CFCS' virksomhed, som har givet centeret nye muligheder for at yde et værdifuldt bidrag til at beskytte samfundsvigtige funktioner mod cyberangreb. Samtidig viser erfaringerne, at CFCS generelt har iagttaget lovgivningens krav til behandling af personoplysninger, ligesom en række af de bekymringer, der blev givet udtryk for i forbindelse med behandlingen af lovforslaget, har vist sig ubegrundede.

Det kan imidlertid også konstateres, at loven på en række områder begrænser CFCS' muligheder for at yde en optimal indsats. Samtidig er der de seneste år sket en betydelig stigning i omfanget af cyberangreb mod Danmark, og cybertruslen mod Danmark er i dag meget høj, ligesom der også i takt med den teknologiske udvikling vil forekomme nye og mere avancerede forsøg på cyberangreb. Der er derfor behov for at sikre, at CFCS fortsat har de rigtige værktøjer og muligheder for at kunne bidrage til et højt sikkerhedsniveau i den infrastruktur, som samfundsvigtige funktioner er afhængige af.

Forsvarsministeriet vil derfor i den kommende tid analysere de områder, hvor der i forbindelse med udarbejdelsen af denne rapport er blevet peget på et behov for tilpasning af lovgivningen. På baggrund af den analyse vil Forsvarsministeriet vurdere, om der er behov for lovændringer.

---

[29] Årsredegørelsen for 2014 og 2015, side 10-15.
[30] Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.
[31] Datatilsynets vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger.
[32] Årsredegørelsen for 2014 og 2015, side 12.

Tilsynet med Efterretningstjenesterne

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Dato: 25. april 2017
Sagsnr.: 2017-152-25
Dok.: 10349

Ved brev af 20. marts 2017 har Forsvarsministeriet anmodet Tilsynet med Efterretningstjenesterne om bidrag til en rapport om erfaringerne med lov om Center for Cybersikkerhed (CFCS-loven), som ifølge lovforslagets bemærkninger skal oversendes til Folketinget 3 år efter lovens ikrafttræden den 1. juli 2014, og hvortil tilsynet skal bidrage med oplysning om tilsynet med CFCS' overholdelse af den nye lovgivning.

I den anledning skal tilsynet bemærke følgende:

Om CFCS' overholdelse af lovgivningen
Tilsynets opgave er at føre legalitetskontrol med, at CFCS behandler oplysninger om *fysiske* personer i overensstemmelse med CFCS-lovgivningen. Tilsynets kontroller er beskrevet i tilsynets redegørelse om sin virksomhed vedrørende CFCS for 2014 og 2015 og i redegørelsen for 2016, som forventes afgivet i maj 2017.

Kontrollerne vedrørende CFCS' behandling af oplysninger om fysiske personer har vist, at centret generelt har iagttaget lovgivningens bestemmelser vedrørende indgreb i meddelelseshemmeligheden, intern behandling af personoplysninger samt analyse, videregivelse og sletning af data.

En kontrol vedrørende sikkerhedsforanstaltninger i forbindelse med CFCS' behandling af oplysninger om fysiske personer viste i 2015, at CFCS ikke fuldt ud levede op til lovgivningens krav om sikkerhedsforanstaltninger eller internt fastsatte retningslinjer herom i forhold til et antal observationer med tilhørende risici inden for 9 ud af 38 kontrollerede områder. En opfølgning på kontrollen i 2016 viste, at der fortsat udestod implementering af nødvendige sikkerhedsforanstaltninger i forhold til risici forbundet med et antal observationer inden for flere af områderne.

Om CFCS' data
Som anført skal tilsynet kontrollere, at CFCS behandler oplysninger om *fysiske* personer i overensstemmelse med lovgivningen. I mange tilfælde er det imidlertid van-

Borgergade 28, 1.
DK-1300 København K
t 25 50 10 34
www.tet.dk

skeligt eller slet ikke muligt at fastslå, hvorvidt data indeholder oplysninger om fysiske personer og dermed er omfattet af tilsynets kontrol. Det er dog tilsynets vurdering, at en stor del af de data, som CFCS behandler, ikke kan henføres til fysiske personer og derfor ikke er omfattet af tilsynets kontrol. Således viste en kontrol i 2016 af centrets videregivelse af data, der stammede fra indgreb i meddelelseshemmeligheden, at kun ca. 30 procent af videregivelserne kunne fastslås at indeholde oplysninger om fysiske personer.

Med venlig hilsen

Ulla Staal

Bidrag til rapport om erfaringer med Lov om Center for Cybersikkerhed

notat udarbejdet til Forsvarsministeriet

1. Indledning

Lov om Center for Cybersikkerhed (lov nr. 713 af 25. juni 2014, herefter "CFCS-loven") trådte i kraft den 1. juli 2014. Det følger af den daværende forsvarsministers fremsættelsestale til lovforslaget (L 192, FT 2013/14), at der mellem en række partier i Folketinget var indgået en politisk aftale om lovforslaget. Som led heri var det aftalt, at der tre år efter lovens ikrafttræden skulle udarbejdes en rapport om erfaringerne med den nye lov. I fremsættelsestalen angives følgende: "Endelig er aftaleparterne enige om, at der skal udarbejdes en rapport om erfaringerne med den nye lovgivning, som oversendes til Folketinget 3 år efter lovens ikrafttræden. Til brug for rapporten vil der blive indhentet bidrag fra Center for Cybersikkerhed, der vil kunne oplyse om centerets almindelige erfaringer med hensyn til den nye lovgivning, og fra Tilsynet med Efterretningstjenesterne, der vil kunne oplyse om tilsynet med Center for Cybersikkerheds overholdelse af den nye lovgivning. Endelig vil Forsvarsministeriet indhente bidrag fra en eller flere uafhængige eksperter på cyberområdet, der kan medvirke til at belyse den nye lovgivnings betydning for kvaliteten og effektiviteten af Center for Cybersikkerheds opgavevaretagelse". Denne passus er ligeledes gengivet i bemærkningerne til CFCS-lovens § 24.

Forsvarsministeriet har bedt mig som uafhængig ekspert udarbejde et bidrag til den nævne rapport i overensstemmelse med den politiske aftale. Nærværende notat udgør dette bidrag. Opdraget blev givet den 19. april 2017 med frist for aflevering af bidraget den 10. maj 2017. Notatet er udarbejdet i dette tidsrum.

2. Indhold og afgrænsning

Beskrivelsen af ekspertbidraget til rapporten om erfaringer med CFCS-loven er holdt på et overordnet plan i den politiske aftale som netop citeret. Lovforslaget var genstand for en betydelig debat og en række ganske kritiske høringssvar blev indgivet af en række organisationer[1]. Kritikken kredsede navnlig om, at Center for Cybersikkerhed (herefter "CFCS") ifølge lovforslaget ikke var omfattet af persondataloven, offentlighedsloven og forvaltningslovens regler om bl.a. aktindsigt, hvilket en række organisationer fandt retssikkerhedsmæssigt betænkeligt. Det politiske ønske om en evaluering af loven efter tre år må ses i dette lys. På den baggrund er det aftalt med Forsvarsministeriet, at udgangspunktet for nærværende notat er en række af de centrale kritikpunkter og bekymringer, der blev fremført i forbindelse med lovens vedtagelse og den dertil knyttede høringsproces.

Notatet forholder sig til, hvordan de anførte kritik- og bekymringspunkter efterfølgende er adresseret i administrationen af loven og CFCS's virke og eventuelle praktiske erfaringer hermed. Som grundlag herfor er anvendt de angivne høringssvar, den hertil hørende kommenterede høringsoversigt udarbejdet af Forsvarsministeriet i april 2014 (herefter "Høringsoversigten")[2], CFCS' årsberetninger, Tilsynet med Efterretningstjenesternes (herefter "Tilsynet") redegørelse for 2014 og 2015 for CFCS (herefter "Tilsynets Redegørelse") og det statistiske materiale, der indgår i disse dokumenter. Der er endvidere gennemført telefoninterviews med chef for CFCS, Thomas Lund-Sørensen, formand for Tilsynet, landsdommer Ulla Staal og repræsentanter for en række af de organisationer, der afgav høringssvar i forbindelse med CFCS-lovens tilblivelse. Ingen af disse personer og organisationer kan tages til indtægt for notatets synspunkter og konklusioner. Der er ikke gennemført konsekvensanalyser af loven, brugerundersøgelser eller anden

[1] Høringssvarene kan findes på Høringsportalen, http://hoeringsportalen.dk/Hearing/Details/17582

[2] Høringsoversigten kan findes på Høringsportalen, http://hoeringsportalen.dk/Hearing/Details/17582

form for egenudarbejdet datamateriale. Notatet og de heri indeholdte vurderinger og konklusioner er således alene baseret på de netop nævnte kilder.

Formålet med notatet er ikke at foretage en generel vurdering af, om CFSC overholder sine forpligtelser under loven. Denne vurdering foretages i vid udstrækning af Tilsynet. Det er endvidere ikke notatets formål at forhold sig til de overordnede principielle spørgsmål om balancen mellem på den ene side borgernes privatliv og offentlighedens adgang til indsigt og på den anden side myndighedernes (in casu CFCS') beføjelser.

I de følgende afsnit 3-9 gennemgås inden for den netop beskrevne ramme en række af de kritikpunkter, der blev fremført i de indkomne høringssvar. I afsnit 10 anføres notatets sammenfattende konklusioner.

3. Reguleringen af CFCS' behandling af personoplysninger

3.1. CFCS' undtagelse fra persondataloven

Det følger af persondataloven § 2, stk. 11, at Forsvarets Efterretningstjeneste (herefter "FE"), og dermed også CFCS, ikke er omfattet af loven. Dette er også fastslået i CFCS-loven § 8, stk. 1. Det fremgår dog af de generelle bemærkninger til CFCS-loven, at Forsvarsministeriet finder, at de centrale principper i persondataloven så vidt muligt bør gælde for CFCS. CFCS-lovens kapitel 6 rummer derfor en række bestemmelser om CFCS' behandling af personoplysninger, der er udformet med udgangspunkt i persondatalovens centrale bestemmelser. Tilsvarende indeholder loven i § 18, stk. 1, krav om sikkerhedsforanstaltninger, der svarer til persondatalovens § 41, stk. 3, og i stk. 2 en bestemmelse, der svarer til "krigsreglen" i persondatalovens § 41, stk. 4. Persondatalovens regler om oplysningspligt og indsigelsesret er ikke medtaget i CFCS-loven.

Efter § 8, stk. 2, kan forsvarsministeren bestemme, at persondatalovens kapitel 8-10 (om den registreredes rettigheder) helt eller delvist skal finde anvendelse vedrørende CFCS' 1) behandling af anmodninger om tilslutning til netsikkerhedstjenesten, 2) virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet og 3) egne personalesager. Forsvarsministeriet har ikke udnyttet denne hjemmel.

En række foreninger udtrykte i deres høringssvar kritik af eller betænkeligheder ved, at CFCS ikke omfattes af persondataloven, jf. Høringsoversigten, pkt. 2.

Denne kritik kan have en mere principiel karakter og angå den overordnede balance mellem de beføjelser, der tildeles statsmagten, og de rettigheder og beskyttelsesmekanismer som tildeles borgerne. Det ligger som allerede beskrevet ikke inden for notatets rammer at vurdere denne overordnede balance, der primært er et politisk spørgsmål. På et mere konkret plan kan det konstateres, at hverken CFCS eller Tilsynet har modtaget klager over CFCS' behandling af personoplysninger, jf. statistikken i Tilsynets Redegørelse, pkt. 5. Af samme redegørelse, pkt. 3, fremgår, at CFCS' behandling af personoplysninger generelt fandt sted i overensstemmelse med CFCS-lovens bestemmelser, idet redegørelsen dog har peget på enkelte punkter, som der skulle rettes op på, hvilket efterfølgende er sket. Jeg er endvidere ikke i mine samtaler med høringsparter blevet gjort bekendt med konkrete sager, hvor myndigheder, virksomheder eller enkeltpersoner har oplevet, at personoplysninger ikke er blevet tilstrækkeligt beskyttet ved CFCS-lovens regulering. Disse observationer udelukker ikke, at der kan bestå sådanne sager, men samlet tegner der sig ikke et billede af, at CFCS's behandling af personoplysninger og CSCS-lovens regulering heraf hidtil har medført en manglende beskyttelse af borgere. Det skal dog understreges, at denne konklusion alene er draget på baggrund af de netop nævnte kilder og som angivet ikke retter sig mod det mere principielle spørgsmål om balancen mellem privatlivsbeskyttelse og CFCS' beføjelser.

3.2. Tilpasning til de nye og kommende persondataregler

De hidtil gældende persondataregler, persondataloven og det bagvedliggende persondatadirektiv (dir. 46/95) er på vej til at blive afløst af persondataforordningen (forordning 2016/679), der får virkning fra den 25. maj 2018. Behandling af personoplysninger, der foretages af politi, anklagemyndighed og domstole, omfattes som udgangspunkt ikke af persondataforordningen men reguleres i direktivet om retshåndhævende myndigheders behandling af personoplysninger (dir. 2016/680). Dette direktiv er implementeret i dansk ret med lov om retshåndhævende myndigheders behandling af personoplysninger (lov nr. 410 af 27. april 2017), der trådte i kraft 1. maj 2017. Det følger af lovens § 1, stk. 2, at den ikke finder anvendelse på FE's, og dermed CFCS's, behandling af personoplysninger. Heller ikke persondataforordningen vil gælde for FE og CFCS. Retstilstanden vil derfor fortsat være den, at CFCS' behandling af personoplysninger kun er omfattet af særskilt lovregulering, i det omfang behandlingen er reguleret i CFCS-loven (eller anden særlovgivning).

Da den omtalte regulering af CFCS' behandling af personoplysninger i CFCS-loven ifølge lovbemærkningerne så vidt muligt bør følge persondatalovens centrale principper, må det anbefales at foretage en justering af loven, så den afspejler de ændringer, der indføres med de nye persondataregler. Da der fremadrettet vil eksisterer to regelsæt, et for behandling foretaget af de retshåndhævende myndigheder (det nævnte direktiv og den tilhørende danske implementeringslov), og et for behandling foretaget af andre (persondataforordningen og den forventede kommende persondatalov), må der tage stilling til, hvilket af de to regelsæt, der skal danne udgangspunkt for reglerne i CFCS-loven, i det omfang de to regelsæt indeholder forskellige reguleringer. Denne vurdering kan først foretages, når den nye persondatalov foreligger, og det vil i sidste ende være et politisk/administrativt spørgsmål, hvilket regelsæt man ønsker at følge, da CFCS som nævnt hverken er omfattet af persondataforordningen eller af direktivet.

4. CFCS' undtagelse fra offentlighedsloven og forvaltningsloven

Det følger af CFCS-loven § 8, stk. 1, at CFCS' virksomhed er undtaget fra offentlighedsloven og forvaltningslovens kapitel 4-6 (om aktindsigt, partshøring og begrundelse). En række foreninger udtrykte i deres høringssvar betænkeligheder ved, at CFCS ikke er omfattet af disse regler, jf. Høringsoversigten, pkt. 2.

Efter § 8, stk. 2, kan forsvarsministeren bestemme, at offentlighedsloven og forvaltningslovens kapitel 4-6 helt eller delvist skal finde anvendelse vedrørende CFCS' 1) behandling af anmodninger om tilslutning til netsikkerhedstjenesten, 2) virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet og 3) egne personalesager. Forsvarsministeriet har ikke udnyttet denne hjemmel.

Det forudsættes endvidere af bemærkningerne til bestemmelsen, at CFCS i videst muligt omfang efterlever principperne i offentlighedsloven og forvaltningslovens kapitel 4-6, herunder at CFCS som led i alle afgørelsessager konkret vurderer, om det er muligt at anvende forvaltningslovens principper om partens aktindsigt, partshøring og begrundelse mv. Tilsvarende forudsættes det, at anmodninger om aktindsigt i videst muligt omfang behandles efter principperne i offentlighedsloven. Chef for CFCS, Thomas Lund-Sørensen, har over for mig bekræftet, at CFCS i praksis følger reglerne i offentlighedsloven og forvaltningsloven, medmindre der er tale om anmodning om adgang til netsikkerhedstjenestens indsamlede data eller dokumenter, der vedrører øvrige dele af FE, og som dermed har efterretningsmæssig karakter. At der ikke gives aktindsigt for disse to typer af data er i overensstemmelse med de almindelige bemærkninger til CFCS-loven, hvoraf fremgår, at CFCS "ikke [vil] foretage en søgning i de store mængder data, som centerets netsikkerhedstjeneste til enhver tid opbevarer, eller i dokumenter, der vedrører øvrige dele af Forsvarets Efterretningstjeneste".

I Tilsynets Redegørelse, s. 18, er angivet en statistik over aktindsigtssager. Det fremgår heraf, at der i 2. halvår af 2014 ikke er givet afslag på nogen sager om aktindsigt, i 10 sager er givet delvis aktindsigt, og der er ingen sager, hvor der er givet fuld aktindsigt. I én sag har der ikke været lokaliseret dokumenter til at give eller afslå aktindsigt i. I 2015 er der hverken givet fuld, delvis eller afslag på aktindsigt i nogen sager. I fire sager har der ikke været lokaliseret dokumenter til at give eller afslå aktindsigt. Ifølge oplysninger fra CFCS, har der været tre anmodninger om aktindsigt i 2016 og én i 2017. Der er således kun anmodet om aktindsigt i et ganske begrænset antal tilfælde.

Samlet set efterlader oplysningerne fra CFCS og statistikmaterialet ikke indtryk af, at CFCS-lovens regler med tilhørende bemærkninger og CFCS's administration heraf har givet anledning til praktiske vanskeligheder eller en utilsigtet begrænsning i adgangen til oplysninger. Det skal dog understreges, at denne konklusion alene er draget på baggrund af de netop nævnte kilder. Det statistiske materiale siger således ikke noget om, hvorvidt der er undladt at søge aktindsigt i forventning om et afslag. Der er heller ikke hermed taget stilling til, i hvilket omfang det er hensigtsmæssigt at undtage adgangen til oplysninger af efterretningsmæssig karakter, herunder de data der indsamles i netsikkerhedstjenesten, idet dette først og fremmest er en politisk beslutning. IT-Branchen har i den forbindelse oplyst, at nogle af organisationens medlemmer finder det uhensigtsmæssigt, at det ikke er muligt at få oplyst baggrunden for CFCS' trusselsvurderinger.

Da CFCS i praksis følger offentlighedslovens og forvaltningslovens regler i de situationer, der er angivet i CFCS-lovens § 8, stk. 2, bør det overvejes at udnytte bestemmelsens mulighed for at udstede en bekendtgørelse herom. Dette vil give en mere fast og gennemsigtig regulering af den adgang til aktindsigt, som allerede følges i CFCS' praksis og lovbemærkningernes forudsætninger.

5. Intern udveksling af data mellem CFCS og øvrige dele af FE

Flytningen af CFCS fra IT- og Telestyrelsen til FE i 2012 indebar, at CFCS organisatorisk og i forvaltningsmæssig forstand blev en del af FE. Bemærkningerne til CFCS-loven fastslår, at de begrænsninger, der gælder for CFCS's videregivelse af data efter CFCS-lovens § 16, derfor – i overensstemmelse med almindelige forvaltningsretlige principper - ikke gælder for CFCS's interne udveksling af data med øvrige dele af FE. Dette gav anledning til en markant kritik af, at der hermed var åbnet for fri udveksling af data fra CFCS til resten af FE med efterfølgende mulighed for videregivelse til FE's samarbejdspartnere. Som svar på denne bekymring blev anført i bemærkningerne til loven, at Forsvarsministeriet i forbindelse med lovens ikrafttræden ville udstede administrative retningslinjer, der begrænsede adgangen til intern udveksling. Det fremgår således af lovbemærkningerne:

> *"Forsvarsministeriet vil imidlertid i forbindelse med lov om Center for Cybersikkerheds ikrafttræden udstede administrative retningslinjer, der sikrer, at den interne udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste også fremadrettet sker med respekt for retssikkerheden og den personlige frihed. Center for Cybersikkerhed behandler data på baggrund af indgreb i meddelelseshemmeligheden, og retningslinjerne vil blandt andet indeholde bestemmelser om, at sådanne data på det civile område (uden for Forsvarsministeriets myndighedsområde) kun kan videreformidles til den øvrige del af Forsvarets Efterretningstjeneste, hvis de pågældende data er knyttet til en cybersikkerhedshændelse. Disse retningslinjer vil endvidere indeholde bestemmelser om, at data, der er videreformidlet fra Center for Cybersikkerhed til den øvrige del af Forsvarets Efterretningstjeneste, fortsat alene vil kunne videregives efter de regler, der gælder for Center for Cybersikkerhed. Dette indebærer, at den øvrige del af Forsvarets Efterretningstjeneste ikke vil*

kunne videregive pakkedata til andre end dansk politi, ligesom trafikdata udelukkende vil kunne videregives til den kreds af aktører, som er omfattet af den foreslåede § 16, nr. 2. Desuden vil retningslinjerne fastsætte, at medarbejdere, der varetager efterretningsmæssige opgaver i den øvrige del af Forsvarets Efterretningstjeneste, ikke må have adgang til de it-systemer, hvor Center for Cybersikkerhed behandler data på baggrund af indgreb i meddelelseshemmeligheden. Ud over bestemmelser om behandlingen af data på det civile område vil retningslinjerne også indeholde bestemmelser om behandling af data på det militære område (Forsvarsministeriets myndighedsområde)".

I overensstemmelse hermed udstedte Forsvarsministeriet "Retningslinjer vedrørende behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste" den 30. juni 2014 med ikrafttræden 1. juli 2014. En gennemgang af retningslinjerne viser, at de indeholder den regulering, der er beskrevet i lovbemærkningerne, herunder de angivne begrænsninger i den interne udveksling mellem CFCS og øvrige dele af FE. Efter retningslinjernes § 2 forudsætter udveksling af data med den øvrige del af FE således, at følgende kriterier er opfyldt: 1) udvekslingen er nødvendig for at understøtte et højt informationssikkerhedsniveau, 2) udvekslingen sker med udtrykkeligt angivne og saglige formål og 3) der er begrundet mistanke om en sikkerhedshændelse. Det sidstnævnte kriterie svarer til det kriterie, der gælder for at CFCS må videregive data til politiet efter CFCS-lovens § 16, stk. 1, nr. 1. De to førstnævnte kriterier følger ikke af § 16. Hermed indeholder retningslinjerne skærpede krav til intern udveksling med FE i forhold til adgangen til videregivelse til politiet efter CFCS-lovens § 16.

Det følger endvidere af lovbemærkningerne, at også den interne udvekling af data vil være underlagt Tilsynet, som således fører tilsyn med, om de administrative retningslinjer overholdes. Det følger af Tilsynets Redegørelse, pkt. 3.1.4, at Tilsynet i 2015 i samarbejde med CFCS fastlagde en procedure, hvorefter Tilsynet løbende modtager orientering fra CFCS, når der foretages intern udveksling af data, der stammer fra indgreb i meddelelseshemmeligheden, med øvrige dele af FE. Det fremgår endvidere af redegørelsen, at Tilsynet havde modtaget 15 orienteringer med udgangen af 2015.

Det følger af bemærkningerne til CFCS-loven, at retningslinjerne vil blive gjort offentligt tilgængelige via CFCS´s hjemmeside, hvilket også er sket[3]. Offentligheden vil således have mulighed for at følge med i eventuelle ændringer af retningslinjerne.

Samlet set er der således administrativt etableret en ordning, hvorefter udveksling af data mellem CFCS og øvrige dele af FE i relation til adgang til udveksling af oplysninger, tilsyn og offentlig kontrol svarer til CFCS's videregivelse af data til politiet efter CFCS-loven, idet adgangen til udveksling af oplysninger med øvrige dele af FE dog er skærpet i retningslinjerne, jf. ovenfor. Det følger endvidere af Tilsynets Redegørelse, pkt. 3.1.4, at CFCS har efterlevet disse retningslinjer. Af redegørelsens pkt. 5 fremgår, at CFCS fem gange i 2014 og 14 gange i 2015 har udvekslet oplysninger med øvrige dele af FE.

6. Opbevaring og sletning af data

Med CFCS-loven blev den maksimale periode for opbevaring af pakkedata, som ikke knytter sig til en sikkerhedshændelse, forlænget fra 14 dage til 13 måneder, jf. lovens § 17, stk. 2, nr. 2. En række høringssvar kritiserede denne forlængelse, jf. Høringsoversigten, pkt. 7.

Af de generelle lovbemærkninger fremgår, at forlængelsen for det første skyldes, at de historiske data giver mulighed for at tegne et normalbillede hos den enkelte myndighed eller virksomhed og dermed bidrager til vurderingen af, om der foreligger en potentiel sikkerhedshændelse. For det andet vil adgang

[3] Se https://fe-ddis.dk/cfcs/CFCSDocuments/Administrativeretningslinjer.pdf

til yderligere historiske data give netsikkerhedstjenesten langt bedre muligheder for at spore cyberangreb, som ikke tidligere er blevet opdaget af de ramte myndigheder eller virksomheder.

CFCS har i forbindelse med udarbejdelsen af nærværende notat over for mig oplyst, at der er eksempler på, at data er blevet brugt i forbindelse med undersøgelse af sikkerhedshændelser tæt på 13-månedersfristen. CFCS fører dog ikke statistik over alderen af de data, der indgår i efterforskning af sikkerhedshændelser, og kan derfor heller ikke oplyse, hvor ofte der er anvendt data, som ville være have været slettet under de tidligere regler. Da efterforskning som regel indebærer analyse af pakkedata i form af malware-filer o.lign., har det dog nok formodningen for sig, at dette sker ofte, og CFCS har over mig oplyst, at man oplever den udvidet slettefrist som vigtig for CFCS's efterforskningsarbejde. På baggrund af disse oplysninger må det lægges til grund, at lovbemærkningernes forudsætninger for at udvide slettefristen har vist sig relevante.

7. Kredsen af virksomheder, der kan tilsluttes CFCS's netsikkerhedstjeneste og konsekvenserne for private sikkerhedsleverandører

Med CFCS-loven blev kredsen af virksomheder, der kan tilsluttes CFCS's netsikkerhedstjeneste udvidet, således at virksomheder, der er beskæftiget med samfundsvigtige funktioner, kan tilsluttes, jf. lovens § 3, stk. 3. Det følger af lovbemærkningerne, at der med begrebet "samfundsvigtige funktioner" forstås funktioner, som er særligt vigtige for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed, herunder funktioner inden for sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet. Som eksempler på nye typer af virksomheder, der vil få mulighed for at blive tilsluttet netsikkerhedstjenesten, nævnes i lovbemærkningerne medicinalvirksomheder, fødevarevirksomheder, virksomheder, der leverer vigtige komponenter til Forsvaret, og virksomheder, der varetager driften af administrative it-systemer for det offentlige. Efter den tidligere GovCERT-lov, var det alene virksomheder, der beskæftigede sig med kritisk infrastruktur, der kunne tilsluttes.

Denne udvidelse gav anledning til kritik i en række høringssvar, jf. Høringsoversigten, pkt. 3. På et generelt plan gik kritikken på, at en større del af den samlede internetkommunikation med udvidelsen ville blive omfattet af CFCS's indsamling af oplysninger. Ved CFCS-lovens ikrafttræden var tre privat virksomheder tilsluttet netsikkerhedstjenesten. Det samme antal er tilsluttet i dag. Det kan på den baggrund konstateres, at den udvidet mulighed for tilslutning i hvert fald ikke indtil videre har haft betydning for det samlede omfang af den internetkommunikation, der indsamles af CFCS.

Der blev endvidere blev fra visse organisationer rejst en kritik af, at CFCS med udvidelsen ville bevæge sig ind på et marked, hvor private aktører også befandt sig og hermed konkurrere med disse. Denne bekymring består fortsat, om end konkurrencesituationen nok ikke opleves som aktuelt presserende. DI Digital har i forbindelse med udarbejdelsen af nærværende notat således givet udtryk for, at CFCS af nogle medlemmer opfattes som en potentiel konkurrent på markedet. IT-Branchen har tilsvarende givet udtryk for, at CFCS's netsikkerhedstjeneste af deres medlemmer opleves som en ydelse, der også tilbydes af det private marked. Prisen for tilslutning til CFCS' netsikkerhedstjeneste er dog så høj, at dette ikke på nuværende tidspunkt opleves som et praktisk problem, men der er bekymring for, at dette vil ændre sig, såfremt priserne sænkes. Chef i CFCS, Thomas Lund-Sørensen, har givet udtryk for, at CFCS ikke oplever sig som en konkurrent til det private marked men som et supplement, idet CFCS primært beskæftige sig med en anden type angreb, end dem, som private aktører beskæftiger sig med, og idet CFCS har adgang til efterretningsoplysninger, som private aktører ikke har adgang til.

Som nævnt er antallet af tilsluttede virksomheder ikke steget i CFCS-lovens levetid, hvorfor den udvidet mulighed for tilslutning derfor indtil videre *i sig selv* ikke har haft betydning for konkurrencesituationen. I hvilket omfang der i øvrigt består en konkurrencesituation, og hvordan denne vil blive påvirket, såfremt flere virksomheder tilsluttes og priserne eventuelt sænkes, således som IT-Branchen udtrykker bekymring for, kan ikke vurderes her. En analyse af, om der består en reel konkurrencesituation mellem CFCS og private aktører og omfanget heraf, ligger uden for rammerne af nærværende rapport.

8. Generel information om CFCS's virke og behandling af personoplysninger

I forbindelse med behandlingen af forslaget til CFCS-loven angav flere høringssvar, at der løbende burde offentliggøres statistiske oplysninger om CFCS's virke, se Høringsoversigten pkt. 6. Dette ønske om gennemsigtighed afspejles i CFCS-lovens § 24, hvorefter Tilsynet skal afgive en årlig redegørelse om sit virke til forsvarsministeren. Redegørelsen skal offentliggøres. Om indholdet af denne redegørelse fremgår af lovbemærkningerne til § 24 bl.a.:

> *"Redegørelserne skal indeholde statistiske oplysninger om Center for Cybersikkerheds behandling af personoplysninger, herunder oplysninger om antallet af modtagne klagesager i såvel centeret som tilsynet, oplysninger om antallet af aktindsigtssager og afgørelsen af disse samt oplysninger om antallet af sager med relation til sikkerhedshændelser, der er behandlet i centeret. Tilsynet vil også skulle medtage oplysninger om, i hvor mange tilfælde tilsynet har fundet, at Center for Cybersikkerheds behandling af personoplysninger ikke har været i overensstemmelse med reglerne. Redegørelsen skal ligeledes indeholde en fuldt ud anonymiseret beskrivelse af en eller flere konkrete cyberangreb samt en statistik over antallet af tilfælde, hvor en analytiker fra Center for Cybersikkerhed på baggrund af indgreb i meddelelseshemmeligheden har foretaget en analyse af data. Denne statistik skal desuden indeholde en overordnet kategorisering af, hvor alvorlige disse tilfælde har været".*

Det fremgår endvidere af lovbemærkningerne til § 24, at Tilsynets redegørelse suppleres af en årlig beretning fra Center for Cybersikkerhed, der bl.a. skal beskrive centerets aktiviteter på det forebyggende område og bringer statistiske oplysninger herom, ligesom CFCS regelmæssigt vil offentliggøre en oversigt over de tilsluttede myndigheder og virksomheder, som også vil omfatte statistiske oplysninger om antallet af myndigheder og virksomheder, der midlertidigt er tilsluttet netsikkerhedstjenesten.

I overensstemmelse hermed indeholder Tilsynets Redegørelse en statistik vedrørende CFCS' behandling af personoplysninger. Statistikken er udarbejdet i overensstemmelse med de krav, der følger af § 24 og bemærkningerne til bestemmelsen. Af statistikken fremgår således 1) hvor mange klagesager CFCS henholdsvis Tilsynet har modtaget i perioden, 2) hvor mange gange der er givet fuld aktindsigt, delvist aktindsigt og afslag på aktindsigt, 3) sager om sikkerhedshændelser, hvori der er sket indgreb i meddelelseshemmeligheden og foretaget analyse af data, opdelt efter alvorlighed og 4) CFCS's videregivelse og udveksling af oplysninger, herunder personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden.

CFCS's årsberetning for 2015 indeholder en statistisk oversigt over sikkerhedshændelser i 2015 og en oversigt over antallet af udvalgte proaktive indsatser i 2015. Beretningen indeholder endvidere oversigt over antallet af tilsluttede myndigheder og virksomheder ved netsikkerhedstjenesten (9 militære og 28 civile ved udgangen af 2015). En opdateret oversigt over tilsluttede myndigheder er offentliggjort på CFCS' hjemmeside[4]. Oversigten indeholder dog ikke statistiske oplysninger om antallet af myndigheder

[4] https://fe-ddis.dk/cfcs/opgaver/Netsikkerhedstjenesten/Documents/Myndigheder%20og%20virksomheder.pdf

og virksomheder, der midlertidigt har været tilsluttet netsikkerhedstjenesten, som forudsat i lovbemærkningerne.

Samlet set tilvejebringer Tilsynet og CFCS de statistiske oplysninger, som fremgår af loven med tilhørende bemærkninger, idet oversigten over tilsluttede kunder dog bør suppleres med de nævnte statistiske oplysninger om midlertidige tilslutninger. Det kan overvejes, om det statistiske materiale burde samles på et statistisksite på CFCS' og/eller Tilsynets hjemmeside. Dette ville give en bedre mulighed for at skaffe sig et samlet overblik fremfor at skulle søge informationerne i de enkelte årsberetninger for de to enheder.

9. Tilsynet med Efterretningstjenesterne

En gennemgang af Tilsynets Redegørelse og samtale med Tilsynets formand, landsdommer Ulla Staal, efterlader indtryk af, at Tilsynet fungerer effektivt og har de beføjelser, der er nødvendige for at kunne foretage det af loven forudsatte tilsyn. Tilsynets formand peger dog på, at det kan være vanskeligt at begrænse tilsynet til behandlingen af personoplysninger, da det i praksis ofte ikke er muligt at adskille personoplysninger fra andre typer oplysninger. Det er ikke i øvrigt en del af nærværende notat at foretage en generel vurdering af Tilsynets virke.

I forbindelse med behandlingen af CFCS-loven blev der stillet spørgsmål ved Tilsynets kompetencer. Ved lovens ikrafttræden blev CFCS underlagt Tilsynet. Indtil da havde den del af CFCS, der forestod varslingstjenesten, været underlagt GovCERT-tilsynet. GovCERT-tilsynet var i overensstemmelse med kravene i den daværende GovCERT-lov bemandet med såvel juridisk, it-revisionsmæssige som sikkerhedsmæssig sagkundskab. CFCS-loven indeholder ikke et tilsvarende krav til, at Tilsynet med Efterretningstjenesterne skal have it-revisionsmæssig og sikkerhedsmæssig sagkundskab. Loven fastslår i § 19, stk. 1, at tilsynet føres af Tilsynet med Efterretningstjenesterne som etableret i henhold til § 16 i lov om Politiets Efterretningstjeneste (PET-loven). PET-lovens § 16 foreskriver blot, at tilsynet skal bestå af fem medlemmer, hvoraf formanden skal være landsdommer.

Da tilsynet med CFCS, og navnlig centres netsikkerhedstjeneste, forudsætter en vis it-faglig og teknisk indsigt, blev der i forbindelse med behandlingen af CFCS-loven rejst tvivl om, hvorvidt Tilsynet ville have de fornødne kompetencer til at føre tilsynet med denne del af FE, se herved pkt. 8 i Høringsoversigten. Som svar herpå anførte Forsvarsministeriet i Høringsoversigten (s. 26), at Tilsynet med Efterretningstjenesterne ville få tilført yderligere ressourcer, herunder til it-faglig og teknisk sagkundskab, som følge af udvidelsen af tilsynets virksomhed til også at omfatte CFCS.

Det følger af PET-lovens § 16, at Tilsynet har kompetence til at antage den fornødne sekretariatsbistand. Tilsynet beslutter selv, hvem der skal ansættes i sekretariatet, herunder hvilken uddannelsesmæssig baggrund og øvrige kvalifikationer, de pågældende skal have. Det fremgår af Tilsynets Redegørelse, at sekretariatet ved udgangen af 2015 bestod af seks personer, herunder en it-konsulent. Tilsynet har endvidere mulighed for at hyre ekstern bistand. På den baggrund må det konkluderes, at den nuværende tilsynsordning giver mulighed for at få inddraget de fornødne tekniske kompetencer. Denne opfattelse er bekræftet af Tilsynets formand, landsdommer Ulla Staal, ligesom Tilsynets sekretariat har oplyst, at der er stor fokus på at være bemandet med de fornødne it-kompetencer.

10. Sammenfattende konklusioner

I nærværende notat er gennemgået en række af de kritik- og bekymringspunkter, der blev anført i høringsfasen i forbindelse med vedtagelsen af CFCS-loven og det er blevet vurderet, hvordan disse efterfølgende er adresseret i administrationen af loven og CFCS's virke og eventuelle praktiske erfaringer her-

med. Der er ikke på baggrund af denne gennemgang med tilhørende vurderinger identificeret uhensigtsmæssigheder, der giver anledning til forslag om justeringer af CFCS-loven. Gennemgangen viser bl.a., at der i forbindelse med lovens ikrafttræden blev etableret en ordning for udveksling af oplysninger mellem CFCS og øvrige dele af FE, der i relation til adgang til udveksling, tilsyn og offentlig kontrol med visse skærpelser svarer til CFCS's videregivelse af data til politiet efter CFCS-loven. Den frie adgang til udveksling af oplysninger mellem CFCS og FE var et af de markante kritikpunkter i høringsfasen, som således er blevet adresseret.

Da CFCS' behandling af personoplysninger i CFCS-loven ifølge lovbemærkningerne så vidt muligt bør følge persondatalovens centrale principper, må det anbefales at foretage en justering af lovens kapitel 6 om behandling af personoplysninger i CFCS, så den afspejler de ændringer, der indføres med de nye persondataregler som nærmere beskrevet i afsnit 3.2.

Det følger af CFCS-loven § 8, stk. 1, at CFCS' virksomhed er undtaget fra offentlighedsloven og forvaltningslovens kapitel 4-6 (om aktindsigt, partshøring og begrundelse). Efter § 8, stk. 2, kan forsvarsministeren bestemme, at disse regler skal finde anvendelse i nærmere angivne situationer, der ikke vedrører CFCS' virke af efterforskningsmæssig karakter. Da CFCS i praksis følger offentlighedslovens og forvaltningslovens regler i disse situationer, som også forudsat i lovbemærkningerne, bør det overvejes at udnytte bestemmelsens mulighed for at udstede en bekendtgørelse herom. Dette vil give en mere fast og gennemsigtig regulering af den adgang til aktindsigt, som allerede følges i CFCS' praksis og lovbemærkningernes forudsætninger.

Der blev ved lovens tilblivelse fra visse organisationer rejst en kritik af, at CFCS med udvidelsen ville bevæge sig ind på et marked, hvor private aktører også befandt sig og hermed konkurrere med disse. Denne bekymring består fortsat, om end konkurrencesituationen nok ikke opleves som aktuelt presserende, bl.a. fordi prisen for at blive tilsluttet CFCS's netsikkerhedstjeneste er relativt høj. En analyse af, om der består en reel konkurrencesituation mellem CFCS og private aktører og omfanget heraf, ligger uden for rammerne af nærværende rapport.

Nærværende konklusioner skal læses i sammenhæng med den afgrænsning, der er anført i afsnit 2 og de uddybninger, der er anført i behandlingen af de enkelte punkter i notatets øvrige afsnit.

10. maj 2017

Henrik Udsen

CENTER FOR CYBERSIKKERHED

12. juni 2017
C/CP/CPI

CFCS' bidrag til evaluering af lov om Center for Cybersikkerhed

Baggrund for lov om Center for Cybersikkerhed (CFCS-loven)

Ved kongelig resolution af 3. oktober 2011 blev ressortansvaret for sager vedrørende beskyttelse af kritisk it-infrastruktur samt statens varslingstjeneste for internettrusler, GovCERT, overført til Forsvarsministeriet med henblik på at styrke beskyttelsen mod cyberangreb. På denne baggrund blev Center for Cybersikkerhed (CFCS) den 18. december 2012 oprettet som en del af Forsvarets Efterretningstjeneste (FE).

CFCS' opgaver

CFCS varetager bl.a. funktionen som Danmarks nationale it-sikkerhedsmyndighed[1], og centerets hovedopgave er at bidrage til at styrke sikkerheden i den informations- og kommunikationsteknologiske infrastruktur (ikt-infrastruktur), som samfundsvigtige funktioner er afhængige af.

CFCS´ netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder på Forsvarsministeriets område samt hos øvrige myndigheder og virksomheder, der er tilsluttet tjenestens netværk af alarmenheder.

Netsikkerhedstjenestens arbejde fokuserer på de mest avancerede angreb, der oftest udføres af statsstøttede aktører, eller cyberangreb, der i øvrigt kan påvirke det danske samfund i væsentlig grad.

Netsikkerhedstjenesten i CFCS blev etableret i 2014 blandt andet som en sammenlægning af varslingstjenesterne GovCERT og MILCERT.

[1] Politiets Efterretningstjeneste varetager funktionen som it-sikkerhedsmyndighed på Justitsministeriets område.

GovCERT og MILCERT

GovCERT (Governmental Computer Emergency Response Team) var den statslige varslingstjeneste for internettrusler. GovCERT blev oprettet i 2009 og var tidligere en del af IT- og Telestyrelsen.

MILCERT (Military Computer Emergency Response Team) blev oprettet i 2010 som en del af Forsvarets Efterretningstjeneste og var varslingstjeneste for internettrusler på Forsvarsministeriets område.

Netsikkerhedstjenesten monitorerer løbende aktiviteterne på de tilsluttede myndigheders og virksomheders forbindelser til eksterne netværk, herunder internettet. Indsamlingen af data sker primært ved hjælp af elektroniske alarmenheder, som er opsat hos de enkelte myndigheder og virksomheder, hvor de monitorerer ind- og udgående netværkskommunikation, herunder internetkommunikation.

Netværk af alarmenheder

CFCS' netværksanalytikere indsamler løbende den nyeste viden om cyberangreb og finder de digitale spor og mønstre, der identificerer et angreb. Disse digitale fingeraftryk lægges ud i specialkonstruerede alarmenheder, som er placeret på de tilsluttede myndigheder og virksomheders internetforbindelser. Tilsammen danner alarmenhederne et netværk af alarmenheder, som alarmerer CFCS ved tegn på advancerede cyberangreb hos de tilsluttede myndigheder og virksomheder ved netsikkerhedstjenesten.

Som national it-sikkerhedsmyndighed varetager centeret en række opgaver af både forebyggende og afhjælpende karakter, herunder oplysning, vejledning og rådgivning af danske myndigheder og virksomheder i at styrke cybersikkerheden, så risikoen for cyberangreb mindskes og – såfremt angreb er lykkedes – imødegås på den mest hensigtsmæssige måde. I forlængelse heraf har centeret en løbende dialog med bl.a. statslige myndigheder, brancheorganisationer og større virksomheder inden for de sektorer, der beskæftiger sig med samfundsvigtige funktioner.

Som national it-sikkerhedsmyndighed er det endvidere Center for Cybersikkerheds opgave at sikkerhedsgodkende og føre tilsyn med klassificerede produkter, systemer og installationer inden for informations- og kommunikationsteknologi. Med opgaven som national it-sikkerhedsmyndighed følger også, at centeret er it-sikkerhedsmyndighed i relation til EU og NATO.

CFCS´placering hos FE

Forud for oprettelsen af CFCS havde FE allerede til opgave at beskytte Forsvarets kritiske infrastruktur mod cyberangreb, og dermed havde FE fået opbygget stærke kompetencer på netop it-sikkerhedsområdet. Med oprettelsen af CFCS blev en række eksisterende men spredte it-kompetencer og specialiserede kundskaber således samlet ét sted.

Baggrunden for placeringen af CFCS ved FE var endvidere at opnå synergieffekter i form af eksempelvis udnyttelse af FE's erfaringer inden for it-sikkerhedsområdet, viden om det internationale trusselsbillede på cyberområdet og særlig adgang til oplysninger fra udlandet om cybertrusler. Den største cybertrussel kommer fra udlandet, og som udenrigsefterretningstjeneste har FE stor viden om udenlandske aktører på cyberområdet samt et veletableret samarbejde med udenlandske efterretningstjenester. Det betyder, at placeringen i FE sikrer, at centeret har adgang til den særlige efterretningsbaserede viden, som FE råder over på cyberområdet med henblik på at styrke imødegåelsen af cyberangreb mod Danmark.

Compliance

CFCS har stort fokus på overholdelse af lovgivning og retningslinjer. I forbindelse med lovens ikrafttræden er der således etableret en intern compliance-funktion i FE's Juridiske Afdeling, der støtter centeret i at efterleve gældende lovgivning, retningslinjer og interne procedurer. Som led i compliance-arbejdet udarbejdes der løbende procedurer og rådgivningsmateriale, der sikrer implementering af reglerne i den daglige opgaveløsning, ligesom medarbejderne løbende undervises i retsgrundlaget. Derudover udarbejdes der afvigerapporter, når der konstateres hændelser, som vurderes at være i uoverensstemmelse med lovgivning, retningslinjer eller interne procedurer. Formålet med rapporterne er at sikre, at der sker indsamling, analyse og formidling af viden om utilsigtede hændelser, således at der skabes grundlag for en systematisk læring. Rapporterne udarbejdes uanset hændelsernes omfang og karakter og dermed også ved afvigelser, der vurderes som ikke alvorlige. Rapporterne tilgår Tilsynet med Efterretningstjenesterne.

Evaluering af CFCS-loven

I forbindelse med oprettelsen af CFCS besluttede S-R-SF-regeringen, at forsvarsministeren skulle fremsætte et lovforslag, der regulerer CFCS' virksomhed. I forlængelse heraf blev der den 1. maj 2014 indgået en politisk aftale om lovforslaget mellem den daværende S-R-regering, Dansk Folkeparti, Det Konservative Folkeparti, Socialistisk Folkeparti og Venstre. Formålet med loven var først og fremmest at etablere et samlet lovgrundlag for centeret, og herunder sikre, at de centrale principper i persondataloven også skulle finde anvendelse på CFCS' virksomhed.

Loven trådte i kraft den 1. juli 2014. Det fremgår af bemærkningerne til lovens § 24, at der skal udarbejdes en rapport om erfaringerne med den nye lovgivning, som oversendes til Folketinget 3

år efter lovens ikrafttræden. Det fremgår endvidere, at der til brug for rapporten bl.a. indhentes bidrag fra CFCS, der vil kunne oplyse om centerets almindelige erfaringer med hensyn til den nye lovgivning.

Tilsynet med Efterretningstjenesterne

Siden 1. juli 2014 har Tilsynet med Efterretningstjenesterne (TET) i medfør af CFCS-loven ført tilsyn med CFCS' behandling af personoplysninger. TET har på dette område erstattet det tidligere GovCERT-tilsyn. TET afgiver årlige redegørelser, der kan findes på TET's hjemmeside.

Ifølge CFCS-loven påser tilsynet efter klage eller af egen drift, at CFCS overholder reglerne om behandling af personoplysninger i CFCS-loven.

Tilsynet påser, at centret overholder lovens regler om:

- indgreb i meddelelseshemmeligheden,
- behandling af personoplysninger,
- analyse, videregivelse og sletning af data, og
- krav til sikkerhedsforanstaltninger i forbindelse med centrets behandling af personoplysninger.

Tilsynets opgave er at føre legalitetskontrol med, at CFCS behandler personoplysninger i overensstemmelse med lovgivningen, og tilsynet skal således ikke påse, om CFCS udfører sine opgaver på en hensigtsmæssig måde. Tilsynet afgør selv intensiteten af sin kontrol, herunder i hvilket omfang kontrollen skal være fuldstændig eller stikprøvevis, hvilke sagsområder der særskilt skal prioriteres, og i hvilket omfang tilsynet vil tage sager op af egen drift.

Konkrete erfaringer med CFCS-loven

Sammenlægning af GovCERT og MILCERT

CFCS-loven banede vejen for en sammenlægning af GovCERT og MILCERT i en enhed, netsikkerhedstjenesten. De to CERT'er udførte grundlæggende de samme opgaver i forhold til henholdsvis civile myndigheder/virksomheder og myndigheder på Forsvarsministeriets område. Sammenlægningen til én samlet netsikkerhedstjeneste muliggjorde en endnu bedre udnyttelse af de samlede ressourcer.

Denne sammenlægning har således konkret givet en række synergieffekter, ligesom den samlede kapacitet, som kan indsættes ved større cyberangreb, er væsentligt større. Eksempelvis har CFCS - modsat mange andre lande - kunnet deltage i både civile og militære samarbejdsfora. Det har i praksis betydet, at CFCS har kunnet modtage information fra både civile og militære myndigheder,

og har tilsvarende kunnet dele relevant viden om trusler med både civile og militære samarbejdspartnere. I andre lande er man afhængige af to eller flere forskellige myndigheders evne til gnidningsfrit at koordinere og dele oplysninger. Den danske model med en samlet netsikkerhedstjeneste har vakt interesse i udlandet, og blandt andre har Storbritannien efterfølgende gennemført en lignende model.

Indgreb i meddelelseshemmeligheden

Det er af stor betydning, at en netsikkerhedstjeneste har adgang til at analysere den trafik, som tilgår de tilsluttede myndigheder fra internettet. GovCERT-loven åbnede derfor op for, at GovCERT kunne bryde meddelelseshemmeligheden uden en retskendelse under visse, restriktive betingelser. Denne mulighed er videreført i CFCS-loven og er fortsat et uundværligt værktøj i centerets arbejde med at analysere internettrafikken til tilsluttede myndigheder og virksomheder og varsle om sikkerhedshændelser og trusler. Dette har betydet, at centeret bl.a. har kunnet identificere og efterfølgende medvirke til standsning af adskillige cyberangreb mod både myndigheder og virksomheder. Såfremt angrebene var fortsat, kunne de have resulteret i ikke kun omfangsrige tab af beskyttelsesværdig information om beslutningsprocesser, men også tab af sensitiv information om danskere. Se bl.a. undersøgelsesrapporten "Når Danmark sover – fjendtlig opmarch på usikre servere" på cfcs.dk

Videregivelse af data

Ved begrundet mistanke om en sikkerhedshændelse har CFCS mulighed for at videregive trafikdata til en afgrænset kreds af aktører, ligesom CFCS kan udsende sikkerhedsvarslinger, der indeholder trafikdata i forbindelse med sikkerhedshændelser. I forhold til det tidligere lovgrundlag er kredsen af samarbejdspartnere, hvortil der kan videregives trafikdata, udvidet til også at omfatte bl.a. teleselskaber. CFCS kan endvidere videregive både pakke- og trafikdata om sikkerhedshændelser til politiet. Tilsvarende underretter politiet CFCS, når politiet bliver opmærksomt på sager, der har relevans for centerets funktion.

Pakke- og trafikdata

Ved **pakkedata** forstås indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester. Det kan for eksempel være indholdet af en e-mailkorrespondance eller indholdet af tilgåede hjemmesider.

Ved **trafikdata** forstås data, som behandles med henblik på at transmittere pakkedata. Det vil sige data, som beskriver oprindelse, destination og rutestyringsinformation, herunder

oprindelsesdomænet eller den oprindelige elektroniske adresse samt anden tilsvarende information. Konkrete eksempler er e-mailadresser eller hjemmesideadresser.

CFCS har generelt stort fokus på at formidle viden, der bredt kan bidrage til at understøtte et højt informationssikkerhedsniveau i den ikt-infrastruktur, som samfundsvigtige funktioner er afhængige af. Det betyder, at centeret – sammenlignet med det øvrige FE – har en større offentlig profil og et meget aktivt udadvendt virke. Foruden udsendelsen af sikkerhedsvarslinger til netsikkerhedstjenestens kunder, offentliggør centeret undersøgelsesrapporter, vejledninger og trusselsvurderinger, bl.a. på baggrund af de erfaringer fra sikkerhedshændelser, som netsikkerhedstjenesten observerer i netværket af alarmenheder.[2]

Tabel 1: Udsendte varsler fra netsikkerhedstjenesten 2014-2016

Årstal	**2014**	**2015**	**2016**
Antal udsendte varsler	180	99	120

CFCS har udgivet følgende undersøgelsesrapporter:

- Når Danmark sover – fjendtlig opmarch på usikre servere
- KingofPhantom - bagdør til hovedmålet
- Phishing uden fangst - Udenrigsministeriet under angreb
- Outsourcing - hvem har ansvaret?
- Én aktør, mange angreb

CFCS har endvidere udgivet følgende vejledninger, der løbende opdateres:

- Cyberforsvar der virker
- Passwordvejledning
- Reducér risikoen for ransomware
- Logning - en del af et godt cyberforsvar
- Undgå DNS Amplification attacks
- SNMP Reflected Amplification DDOS-attacks
- Sådan kan du imødegå DDoS-angreb
- Webmasteren kan holde øje med cybersikkerheden
- Målepunkter for informationssikkerhed
- Styrkelse af informationssikkerheden i mainframeinstallationer
- Spear-phishing - et voksende problem
- It-sikkerhed på rejsen
- Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift

[2] De offentliggjorte produkter udgør imidlertid kun et udsnit af centerets produktion. Derudover udarbejdes produkter til en lukket kreds, herunder klassificerede rapporter.

CFCS anvender derudover sociale medier som platforme for formidling, og centerets medarbejdere holder mange oplæg i forskellige fora for både teknikere og strategiske beslutningstagere. Endvidere afholder CFCS kurser for sikkerhedschefer. På kurserne orienteres blandt andet om regler, CFCS' vejledninger, trusselsbilledet og netværket af alarmenheder.

CFCS har et tæt samarbejde med netsikkerhedstjenester i udlandet, for eksempel CERT'er og ikt-sikkerhedsmyndigheder, som bidrager med vigtige informationer, der øger centerets muligheder for at forebygge sikkerhedshændelser i Danmark. Et effektivt internationalt samarbejde på myndighedsniveau er blevet muligt ved, at Danmark også kan videregive oplysninger til netsikkerhedstjenester i udlandet, som kan bidrage til at stoppe grænseoverskridende cyberangreb rettet mod Danmark. Dette samarbejde med udenlandske netsikkerhedstjenester højner sikkerheden internationalt, idet information om angribernes redskaber og metodikker i et vist omfang har kunnet videregives, så angriberne generelt får vanskeligere ved at operere, og det dermed bliver dyrere og mere omkostningsfuldt for dem at foretage deres angreb.

Muligheden for at videregive data har endvidere understøttet CFCS' opgavevaretagelse, idet centeret har kunnet varsle myndigheder og virksomheder om erkendte angreb foretaget mod den/de pågældende.

Muligheder for at gemme data

CFCS-loven giver mulighed for, at data knyttet til en sikkerhedshændelse kan gemmes i tre år. Men det blev med loven også muligt at gemme data, der ikke knytter sig til en sikkerhedshændelse, i 13 måneder. Det er CFCS' vurdering, at denne adgang til historiske data har medført en betydelig styrkelse af CFCS' arbejde, da det har været muligt at tegne et normalbillede af internetaktiviteterne hos den enkelte myndighed eller virksomhed. Jo længere perioden er, hvor der er adgang til at søge efter karakteristika, jo større er muligheden endvidere for at opdage hidtil uopdagede cyberangreb. I flere tilfælde er der således opdaget indikationer på igangværende angreb, hvor det oprindelige angreb var foregået længere tilbage i tiden. I de situationer har adgangen til data i 13 måneder været afgørende for evnen til at reagere.

Mængderne af internettrafik stiger hele tiden, og angrebsteknikkerne bliver mere avancerede. Det stiller store krav til CFCS. CFCS har imidlertid fulgt med udviklingen ved bl.a. at implementere en helt ny generation af egenudviklede alamenheder med større lagringssystemer. Disse alarmenheder er pr. 1. december 2016 installeret hos alle centerets tilsluttede myndigheder og virksomheder.

Udveksling af data

Centeret kan under visse betingelser udveksle data med den øvrige del af FE. Formålet med udvekslingen er at undersøge, om der i FE's efterretningsmæssige indhentning er informationer, der yderligere kan kvalificere den konkrete sag, herunder identifikation af angrebsaktør, oplysninger om angriberens kapaciteter og metoder Den bistand, som den efterretningsmæssige del af FE kan yde til netsikkerhedstjenestens videre arbejde i en konkret sag, vurderes at være nødvendig for at understøtte et højt informationssikkerhedsniveau hos myndigheder og virksomheder fremadrettet.

Omfanget af udveksling og videregivelse af oplysninger fremgår af tabel 2, og det stigende omfang indikerer, at CFCS ofte benytter sig af mulighederne, fordi de vurderes at give betydelig merværdi for centerets arbejde. Det har i praksis vist sig at være overordentligt effektivt for centerets opgaveløsning at kunne udveksle konkret information om angribernes redskab og metodikker, idet der ofte kommer ny viden om angriberen tilbage til CFCS. Denne viden kan enten bestå af viden om nye myndigheder eller virksomheder, som skal varsles og hjælpes, eller nye hidtil ukendte redskaber fra angriberens side.

Udveksling og videregivelse

Udveksling
Den interne udveksling af pakke- og trafikdata fra Center for Cybersikkerhed til den øvrige del af Forsvarets Efterretningstjeneste.

Videregivelse
Den eksterne videregivelse af pakke- og trafikdata fra Center for Cybersikkerhed til øvrige myndigheder og virksomheder.

Tabel 2. CFCS' videregivelser og udvekslinger af oplysninger, herunder personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden[3]

Kategorier	**2. halvår 2014**	**2015**	**2016**
Sager, hvori der er sket videregivelse af oplysninger	50	39	427
Sager, hvori der er sket udveksling af oplysninger	5	14	49

[3]En sag kan indeholde flere videregivelser og/eller udvekslinger.

Udfordringer i forbindelse med CFCS-loven

Som det fremgår ovenfor, har CFCS-loven overordnet givet CFCS et solidt fundament for at understøtte et højt informationssikkerhedsniveau i den ikt-infrastruktur, som samfundsvigtige funktioner er afhængige af.

CFCS har imidlertid identificeret en række områder, hvor CFCS-loven i højere grad kunne bidrage til en effektiv løsning af centerets opgave med at understøtte et højt informationssikkerhedsniveau i den ikt-infrastruktur, som samfundsvigtige funktioner er afhængige af. Det skyldes blandt andet, at dele af den nuværende lovgivning ikke vurderes tilstrækkeligt i overensstemmelse med den teknologiske udvikling samt de nye opgaver, som centeret varetager, bl.a. som følge af cyber- og informationssikkerhedsstrategien af 2014.

Den nationale strategi for cyber-og informationssikkerhed

Den nationale strategi for cyber-og informationssikkerhed blev lanceret ultimo 2014. Strategien indeholder 27 konkrete initiativer på tværs af seks indsatsområder med henblik på at øge informationssikkerheden og styrke beskyttelsen mod cyberangreb.

Områderne, hvor den nuværende lovgivning har vist sig ikke at fungere optimalt, skitseres nedenfor.

Udbredelsen af netværket af alarmenheder

CFCS indsamler løbende den nyeste viden om cyberangreb og finder de digitale spor og mønstre, der identificerer et angreb. Disse digitale fingeraftryk lægges ud i specialkonstruerede alarmenheder, som er placeret på de tilsluttede myndigheder eller virksomheders internetforbindelser. Tilsammen danner alarmenhederne et netværk af alarmenheder, som alarmerer CFCS ved tegn på cyberangreb hos de tilsluttede kunder ved netsikkerhedstjenesten.

Det er forudsat i bemærkningerne til CFCS-loven, at regioner, kommuner og virksomheder, der ønsker at blive tilsluttet netsikkerhedstjenesten, dækker de udgifter, der er forbundet med indkøb og/eller udvikling af evt. monitoreringsudstyr, samt centerets udgifter til monitoreringen.

Det er på den baggrund fastsat i § 3 i bekendtgørelse nr. 1568 af 12. december 2016 om tilslutning til CFCS' netsikkerhedstjeneste, at en tilsluttet region, kommune eller virksomhed betaler et årligt gebyr til dækning af udgifter, der er forbundet med tilslutningen til CFCS' netsikkerhedstjeneste. For 2017 udgør gebyret 300.000 kr. excl. moms pr. alarmenhed af typen NSS-1 og 400.000 kr. excl.

moms pr. alarmenhed af typen NSS-2. De to typer alarmenheder adskiller sig alene ved mængden af data, som skal håndteres ved kunden.

Det følger endvidere af bemærkningerne til CFCS-loven, at de øverste statsorganer samt statslige myndigheder, som tilsluttes netsikkerhedstjenesten, modtager netsikkerhedstjenestens ydelser vederlagsfrit, men at en myndighed, som ønsker særlige ydelser, for eksempel monitorering af flere forskellige forbindelser til internettet, vil blive opkrævet betaling, som dækker udgifterne til indkøb og/eller udvikling af evt. monitoreringsudstyr og udgifter til driften heraf.

Yderligere udbredelse af netværket af alarmenheder vil sætte CFCS i stand til at varsle hurtigere og bredere om trusler. Endvidere vil et forbedret datagrundlag styrke centerets trusselsvurderinger og centerets rådgivning til myndigheder og virksomheder om risici og passende sikkerhedstiltag.

Sikkerhedstekniske undersøgelser

CFCS har i dag ikke hjemmel til at foretage indgreb i meddelelseshemmeligheden i forbindelse med gennemførelsen af sikkerhedstekniske undersøgelser, herunder test af sikkerheden, efter anmodning fra en civil myndighed eller virksomhed. I forbindelse med test af sikkerheden kan der opstå et behov for at bryde meddelelseshemmeligheden.

Efterspørgslen efter test af sikkerheden er stigende. I forbindelse med den nationale strategi for cyber- og informationssikkerhed i 2014 blev det besluttet at etablere et særligt kompetencecenter på SCADA-området hos CFCS. Kompetencecenteret bistår, tester sikkerhed og rådgiver både offentlige myndigheder og private virksomheder i forsyningssektorerne med viden om sårbarhederne ved SCADA-systemer SCADA (Supervisory Control And Data Acquisition) er betegnelsen for industrikontrolsystemer, der anvendes til styring og overvågning af processer og protokoller samt kommunikationen mellem et netværk og et fysisk domæne som f.eks. ventiler, pumper, varmestyring, generatorer m.v. Etableringen af kompetencecenteret har afstedkommet en yderligere efterspørgsel efter, at CFCS kommer ud til både offentlige myndigheder og private virksomheder og hjælper dem med at vurdere sikkerheden i deres ikt-infrastruktur, herunder teste sikkerheden.

Mulighed for monitorering af enheder på lokale netværk

CFCS-loven indebærer i dag en række begrænsninger ift. adgangen til og behandlingen af information. For eksempel monitorerer netsikkerhedstjenesten i dag løbende aktiviteter på tilsluttede myndigheder og virksomheders forbindelser til eksterne netværk, herunder internettet. De opsatte alarmenheder monitorerer således ind- og udgående netværkskommunikation, herunder internetkommunikation, mens aktivitet, der alene foregår på de enkelte enheder på det lokale netværk hos de tilsluttede myndigheder og virksomheder, ikke transporteres gennem alarmenheden og derfor ikke monitoreres. Samtidig indebærer den teknologiske udvikling, at indholdet af stadig mere netværkstrafik bliver utilgængeligt på grund af kryptering. Konsekvensen af kryptering kan

være, at de indikatorer, som alarmenhederne er indstillet til at reagere på, ikke udløser en alarm. Såfremt det var muligt at foretage monitorering af enheder på det lokale netværk, eksempelvis ved installation af host-baserede agenter[4] på de enkelte enheder hos tilsluttede myndigheder og virksomheder, ville det være muligt at se data efter dekryptering hos brugeren. Muligheden for monitorering af enheder på tilsluttede myndigheder og virksomheders lokale netværk ville således styrke centerets arbejde med at opdage og imødegå cyberangreb betydeligt på flere måder og dermed komplementere beskyttelsen fra alarmenhederne. CFCS-loven hjemler imidlertid ikke på nuværende tidspunkt en sådan monitorering af enheder på det lokale netværk.

Hostingselskaber

Stadigt flere myndigheder og virksomheder anvender hostingselskaber eller andre it-fællesskaber til at administrere og hoste deres systemer. De fleste af disse anvender shared services. Det vil sige, at flere kunder deler en server. Det kan for eksempel være en webserver, database eller lignende. Hvis en enkelt myndigheds eller virksomheds løsning er kompromitteret, kan CFCS som udgangspunkt bistå myndigheden eller virksomheden med afhjælpning af angrebet ved at hjemtage den pågældende server til nærmere analyse. Men hjemtagning kræver et skriftligt samtykke fra systemejeren, og der kan være hundredevis af kunder/systemejere på en enkelt server. Dermed er det i praksis vanskeligt at få et samtykke fra hver enkelt myndighed eller virksomhed. I dag løses problemstillingen via samarbejde med relevante myndigheder. Det har dog i visse tilfælde betydet en forsinkelse ift. CFCS' muligheder for at bidrage til at imødegå sikkerhedshændelser. Denne udfordring er under håndtering via styrkelse af samarbejdet med relevante myndigheder.

Videregivelse og opbevaring af pakke- og trafikdata

Der har i CFCS-loven vist sig at være en række udfordringer forbundet med informationsdeling og muligheder for videregivelse af data. Det kan for eksempel være relevant at videregive bl.a. malware, der er anvendt i forbindelse med et cyberangreb, til eksempelvis udenlandske partnere for at undersøge, om der kan tilvejebringes information, der yderligere kan kvalificere den konkrete sag, herunder identifikation af en angrebsaktør og oplysninger om angriberens kapaciteter og metoder, hvilket som udgangspunkt ikke er muligt, da malware oftest er indeholdt i pakkedata.

Det er desuden væsentligt for centerets mulighed for at opdage og imødegå fremtidige angreb, at oplysninger om tidligere angreb i videst muligt omfang kan bevares. Som nævnt oven for giver CFCS-loven mulighed for, at data knyttet til en sikkerhedshændelse kan gemmes i tre år, og data, der ikke knytter sig til en sikkerhedshændelse, kan gemmes i 13 måneder. Efter de nuværende regler skal alle data, der knytter sig til en sikkerhedshændelse, slettes senest efter 3 år, uanset om

[4] Hostbaserede agenter bærer mange af de samme karakteristika som anti-virus-software

disse data stadig måtte være relevante for centerets arbejde. Når CFCS har afdækket et angreb eller angrebsforsøg, giver det centeret viden om angriberens adfærd. Over tid vil denne adfærd typisk ændre sig, men fra tid til anden vender en angriber tilbage til velkendte og afprøvede teknikker, nogle gange med ganske lidt variation. Hvis data ikke er gemt, bliver det derfor vanskeligere at være på forkant med angriberne og forudsige deres næste træk. Det er på denne baggrund, at det er af stor betydning at kunne gemme data.
Forpligtelsen til sletning af oplysninger giver endvidere praktiske udfordringer i relation til muligheden for at tage back-up af oplysninger i centerets systemer og platforme, og dermed sikre, at vigtigt data ikke mistes.

Opsætning og test af alarmenheder

Det er i forbindelse med opsætning af en alarmenhed hos en tilsluttet myndighed eller virksomhed samt løbende efter behov relevant at kontrollere, at alarmenheden er korrekt og effektivt konfigureret. I den forbindelse kan der være behov for at videregive data til den tilsluttede myndighed eller virksomhed for at identificere, hvilken service, der ligger bag en intern IP-adresse, og hvad der dermed genererer det pågældende datamønster i netværket. Det kan endvidere være relevant at analysere pakke- og trafikdata med henblik på at teste, at alarmenheden reagerer, som den skal.

Analyse af pakkedata og videregivelse af pakke- og trafikdata, der stammer fra alarmenhederne forudsætter efter de nuværende regler begrundet mistanke om en sikkerhedshændelse. Det betyder, at det i praksis ikke i tilstrækkeligt omfang er muligt at foretage den beskrevne kontrol af, at alarmenheden fungerer efter hensigten.

Aktivt netværk af alarmenheder

Alarmenhederne i netværket af alarmenheder er passive. Det betyder, at de kopierer internettrafikken, hvorefter trafikken inspiceres for ondsindet aktivitet. Såfremt der udløses en alarm i alarmenhederne, håndteres denne efterfølgende af netsikkerhedstjenesten. Lovgivningen og netværket af alarmenheder giver således ikke i dag mulighed for at imødegå ondsindede aktørers angrebsmetoder og værktøjer ved for eksempel aktivt evt. automatiseret at standse igangværende angreb.

Erfaringer fra Incident Response

Med CFCS-loven fik CFCS mulighed for at få adgang til at analysere data fra en kompromitteret computer, server eller et andet informationssystem under forudsætning af bl.a. myndighedens eller virksomhedens skriftlige samtykke, for eksempel i forbindelse med Incident Response.

Når CFCS udfører Incident Response, sker det på baggrund af en dokumenteret mistanke om et igangværende hackerangreb. Forudsætningen for at kunne be- eller afkræfte mistanken er, at CFCS får adgang til logfiler fra netværkstrafikken og de potentielt inficerede maskiner. Ofte støder CFCS imidlertid på det problem, at den kompromitterede virksomhed eller myndighed ikke råder over logfiler i tilstrækkelig grad. Enten opsamles logs slet ikke, eller også slettes de efter kort tid. Derudover kan logfilerne være fejlbehæftede eller utilstrækkelige, som følge af forkert opsætning og manglende test og kontrol af filerne fra virksomhedens eller myndighedens side.

Med henblik på at styrke fastholdelsen af erfaringer, der gøres, udsender CFCS vejledninger, som løbende holdes opdateret.