FORSVARSMINISTERIET

Folketinget
Christiansborg
1240 København K

Den 29. juni 2022

FØLGESKRIVELSE

Den 18. december 2022 er det 10 år siden, Center for Cybersikkerhed (CFCS) blev oprettet. CFCS blev sat i verden for at beskytte de vigtigste dele af det danske samfund mod cyberangreb. CFCS blev placeret ved Forsvarets Efterretningstjeneste (FE), hvormed centret fik adgang til efterretningstjenestens viden om det internationale trusselsbillede på cyberområdet og særlig adgang til oplysninger om cybertrusler fra udlandet.

CFCS fik et nyt, samlet lovgrundlag den 1. juli 2014. I takt med den digitale og teknologiske udvikling samt udviklingen i cybertruslen, har CFCS gennem årene udvidet sin kapacitet og opgaveportefølje. Folketinget vedtog på den baggrund i 2019 et lovforslag om ændring af CFCS-loven, der havde til formål at tilpasse CFCS' lovgrundlag det aktuelle trusselsbillede og den teknologiske udvikling, således at CFCS fik bedre muligheder for at løse sine opgaver. Lovændringen trådte i kraft d. 1. juli 2019. I bemærkningerne til loven fremgår, at der senest tre år efter lovens ikrafttrædelse skal udarbejdes en rapport til Folketinget med erfaringerne med den nye lovgivning.

Forsvarsministeriet har bedt CFCS evaluere de erfaringer, som CFCS har gjort med de nye tiltag med lovændringen fra 2019 samt enkelte af de videreførte dele af loven fra 2014. Erfaringerne fremgår af vedlagte rapport.

Forsvarsministeriet kan konstatere, at CFCS generelt vurderer, at de nye tiltag med lovændringen i 2019 har bidraget positivt til CFCS' opgave med at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder, der understøtter samfundsvigtige funktioner. Samtidig kan Forsvarsministeriet konstatere, at CFCS finder, at loven på nogle punkter kunne styrke CFCS' muligheder for at løse sine opgaver.

Henset til den hastige teknologiske udvikling på cybersikkerhedsområdet, ikke mindst set i lyset af krigen i Ukraine, arbejder Forsvarsministeriet løbende på at styrke sikkerhed og forsvar på cyberområdet. Det indebærer blandt andet, at CFCS har de rigtige værktøjer og muligheder for at kunne bidrage til et højt cybersikkerhedsniveau i den digitale infrastruktur.

CFCS' erfaringer med CFCS-loven vil blive medtaget i Forsvarsministeriets løbende arbejde med at skabe de rette rammer for beskyttelsen af Danmark i cyberspace.

Erfaringerne med lov om Center for Cybersikkerhed

1. Indledning 2

2. Erfaringer med lov om Center for Cybersikkerhed 2

2.1. Udveksling af data med Forsvarets Efterretningstjeneste 2
2.2. Nye datadefinitioner 2
2.3. Center for Cybersikkerheds netsikkerhedstjeneste 4
2.3.1. Tilslutning til netsikkerhedstjenesten ved tilslutningsaftale 4
2.3.2. Sikkerhedssoftware på lokale enheder og netværk 4
2.3.3. Overførsel af løbende logoplysninger 5
2.3.4. Påbud om tilslutning til netsikkerhedstjenesten 5
2.4. Indgreb omfattet af grundlovens § 72 5
2.4.1. Bistand fra netsikkerhedstjenesten til myndigheder og virksomheder, der ikke er tilsluttet netsikkerhedstjenesten 5
2.4.2. Aktivt cyberforsvar 6
2.4.3. Forebyggende sikkerhedstekniske undersøgelser 7
2.4.4. Honey Pots 7
2.4.5. Sinkholes 7
2.5. Edition 8
2.6. Analyse, videregivelse og sletning af data 8
2.6.1. Analyse af data 8
2.6.2. Videregivelse af data 9
2.6.3. Sletning af data 10
2.7. Andre forhold 12

3. Tilsynet med Efterretningstjenesternes tilsyn med behandling af personoplysninger i CFCS 12

3.1. Tilsynet med Efterretningstjenesterne 12
3.2. Tilsynet med Efterretningstjenesternes årsredegørelser 12

1. Indledning

Denne rapport vedrører erfaringerne med lov nr. 555 af 7. maj 2019 om Center for Cybersikkerhed (CFCS-loven).

Den 27. marts 2019 fremsatte den daværende regering forslag til lov om ændring af lov om Center for Cybersikkerhed[1]. Forslaget blev vedtaget af et bredt flertal i Folketinget den 2. maj 2019 og lov nr. 555 af 7. maj 2019 om Center for Cybersikkerhed trådte i kraft den 1. juli 2019. Formålet med at opdatere CFCS-loven var at tilpasse lovgrundlaget til det aktuelle trusselsbillede og den teknologiske udvikling for at give Center for Cybersikkerhed (CFCS) bedre muligheder for at løse opgaver med at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af, jf. CFCS-lovens § 1. Af den politiske aftale, der er gengivet i den skriftlige fremsættelsestale og omtales i bemærkningerne til loven[2], fremgik, at der, henset til den hastige udvikling på cybersikkerhedsområdet, senest tre år efter lovens ikrafttræden skal udarbejdes en rapport om erfaringerne med den nye lovgivning, som skal oversendes til Folketinget.

Rapporten omhandler erfaringerne med de nye tiltag fra 2019 samt relevante dele videreført fra den tidligere CFCS-lov[3]. I rapporten berøres alle nye tiltag i 2019-loven, idet CFCS' undtagelse fra §§ 3, 5 og 8, stk. 2, i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter, jf. CFCS-lovens § 8, stk. 1, 2. pkt., forholdet til databeskyttelsesloven og persondatabeskyttelsesforordningen, jf. CFCS-lovens § 8, stk. 1, forholdet til arkivlovgivningen, jf. CFCS-lovens § 8 a, og forholdet til bestemmelser om tavshedspligt fastsat ved lov eller med hjemmel i lov, jf. CFCS-lovens § 8 b, dog ikke behandles i rapporten. Rapportens fokus er således på de ændringer, der vedrører CFCS' kernevirksomhed.

2. Erfaringer med lov om Center for Cybersikkerhed

2.1. Udveksling af data med Forsvarets Efterretningstjeneste

Forsvarsministeriet har i cirkulære nr. 9741 af 21. august 2019 om behandling af data i og fra CFCS' netsikkerhedstjeneste fastsat regler for bl.a. udveksling af oplysninger fra CFCS til de øvrige dele af FE.

Det bemærkes hertil, at formålet med at udveksle oplysninger med FE er at undersøge, om der i FE's efterretningsmæssige indhentning er informationer, der yderligere kan kvalificere en konkret sag. Den bistand, som den efterretningsmæssige del af FE yder til netsikkerhedstjenestens videre arbejde, er nødvendig for at understøtte et højt informationssikkerhedsniveau hos myndigheder og virksomheder.

2.2. Nye datadefinitioner

Ved ændringen af CFCS-loven i 2019 blev der introduceret nye datadefinitioner. Konkret blev det fastsat i CFCS-lovens § 2, nr. 4, at stationære data defineres som data, der opbevares på servere, cloudtjenester, pc'ere, lagerenheder, netværksenheder, mobile enheder og tilsvarende. Ligeledes blev det fastsat i CFCS-lovens § 2, nr. 5, at malware defineres som trafikdata- og pakkedata samt stationære data, hvor der er særlig bestyrket

[1] Lovforslag nr. 215 af den 27. marts 2019 om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden)

[2] Lovforslag nr. 215 af den 27. marts 2019 om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden) punkt 1.

[3] Lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed

mistanke om, at data er anvendt af en angrebsaktør med det formål at forårsage brud på informationssikkerheden.

Begrebet stationære data blev introduceret i lovændringen, da CFCS samtidig fik muligheden for monitorering bl.a. ved at installere sikkerhedssoftware på lokale enheder og netværk i medfør af CFCS-lovens § 4, ligesom der som en særlig variant af tilslutning til netsikkerhedstjenesten blev mulighed for, at myndigheder og virksomheder løbende overfører logoplysninger m.v., jf. CFCS-lovens § 3.

Det fremgår af lovens forarbejder, at logoplysninger, der overføres løbende fra en myndighed eller virksomhed, vil have karakter af stationære data.[4] Som følge af de nye muligheder for tilslutning til netsikkerhedstjenesten, herunder monitorering, blev der tilsvarende indsat særlige hjemler for analyse og videregivelse af stationære data. De særlige hjemler er med til at sikre, at data som f.eks. sundhedsdata, e-mailkorrespondancer m.v. kun kan analyseres manuelt, hvis det er nødvendigt, og alene ved begrundet mistanke om en sikkerhedshændelse. Endvidere sætter videregivelseshjemlen grænser for, hvornår stationære data kan videregives, herunder at det alene kan ske til politiet, den berørte myndighed eller virksomhed samt til andre netsikkerhedstjenester. Disse rammer sikrer, at CFCS kan berige politiet med oplysninger, der kan være grundlag for iværksættelsen af en strafferetlig efterforskning, ligesom CFCS kan indgå i dialog med den berørte myndighed eller virksomhed om, hvorvidt data rent faktisk er ondartet m.v.

Den forholdsvis brede definition af begrebet stationære data, der fokuserer på, hvordan CFCS tilgår data, frem for, hvilken datatype der faktisk er tale om, har i praksis medført visse udfordringer i forhold til CFCS' muligheder for at analysere data tilvejebragt efter CFCS-lovens kapitel 4. Det skyldes bl.a., at der forudsættes at foreligge en begrundet mistanke om en sikkerhedshændelse, før manuel analyse af stationære data kan finde sted.

CFCS modtager i stigende grad løbende logoplysninger fra tilsluttede myndigheder og virksomheder med henblik på at opdage, analysere og imødegå cybersikkerhedshændelser i medfør af CFCS-lovens § 3, stk. 1. Det bemærkes, at data fra logs er sammenlignelige med CFCS-lovens definition af trafikdata, jf. CFCS-lovens § 2, nr. 3. Manuel analyse af trafikdata følger af CFCS-lovens § 15, nr. 1, hvor kravet for at kunne analysere er mere lempeligt end kravene for manuel analyse af stationære data, jf. CFCS-lovens § 15, nr. 2.

Ligeledes kan det oplyses, at manuel analyse af data, der er tilvejebragt på baggrund af installation af sikkerhedssoftware på pc'er og lignende, medfører udfordringer, da dette data tilsvarende betragtes som stationære data på trods af, at der er tale om tekniske logs genereret af sikkerhedssoftwaren.

En afledt effekt ved indsættelsen af datadefinitionerne er bedre muligheder for, at CFCS kan videregive data tilvejebragt efter CFCS-lovens kapitel 4. Det har eksempelvis været muligt for CFCS ikke alene at videregive oplysninger om tidspunkter og anvendte IP-adresser i forbindelse med en it-sikkerhedshændelse, men også at dele selve de ondsindede data, som har været anvendt i sikkerhedshændelsen. CFCS anser dette som et væsentligt positivt bidrag til både kvaliteten og effekten af CFCS' håndtering af it-sikkerhedshændelser.

[4] Lovforslag nr. 215 fremsat den 27. marts 2019 ændring af lov om Center for Cybersikkerhed, bemærkningerne til § 3.

2.3. Center for Cybersikkerheds netsikkerhedstjeneste

2.3.1. Tilslutning til netsikkerhedstjenesten ved tilslutningsaftale
Også efter ændringen af CFCS-loven i 2019 skal tilslutning til netsikkerhedstjenesten, jf. CFCS-lovens § 3, ske ved indgåelse af en tilslutningsaftale. Det følger af lovens forarbejder, at en tilslutningsaftale kan være tidsbegrænset.[5]

Endvidere bemærkes, at gebyret for tilslutning til netsikkerhedstjenesten blev afskaffet med den seneste ændring af CFCS-loven med henblik på at øge antallet af tilslutninger til netsikkerhedstjenesten. Afskaffelsen af gebyret for tilslutning til netsikkerhedstjenesten er blevet positivt modtaget af tilsluttede myndigheder og virksomheder, og afskaffelsen af gebyret for tilslutning har bidraget til at smidiggøre processen og dialogen med myndigheder og virksomheder om potentiel tilslutning. Der er således sket en stigning i antallet af tilsluttede private virksomheder fra fem tilsluttede private virksomheder i 2019 til 17 tilsluttede private virksomheder i 2021. Det er CFCS' vurdering, at der ville være sket en yderligere stigning i antallet af tilsluttede private virksomheder, såfremt COVID-19-pandemien ikke havde forsinket beslutningsprocessen hos potentielle myndigheder og virksomheder.

CFCS bemærker mere generelt, at tilslutningsaftalerne med offentlige myndigheder giver udfordringer, når der sker ressortomlægninger, da aftalerne herefter skal revideres og underskrives på ny, hvilket er en omfangsrig og tidskrævende proces for både den pågældende myndighed og CFCS. I 2014 blev truffet regeringsbeslutning om, at alle statslige myndigheder, der anvender Statens It som internetleverandør, fra 1. september 2014, skal tilsluttes netsikkerhedstjenesten.[6] Udfordringerne med tilslutningsaftalerne ved ressortomlægninger løses delvist ved at samle de tilsluttede myndigheder hos Statens It. Udviklingen i antallet af tilsluttede myndigheder og virksomheder fremgår af CFCS' årlige beretninger[7]:

	2017	2018	2019	2020	2021
Tilsluttede myndigheder og virksomheder (civile / militære) *	27 / 12	30 / 34	34 / 36	209 / 36	229 / 36
Midlertidigt tilsluttede virksomheder og myndigheder	0	0	0	N/A	N/A

** CFCS opgjorde indtil 2020 tilslutninger til sensornetværket med udgangspunkt i antal tilslutningsaftaler, hvoraf en aftale kunne dække flere underliggende myndigheder. Fra 2020 har CFCS opgjort tilslutninger med udgangspunkt i antal monitorerede organisationer. Dette forklarer en væsentlig del af stigningen fra 2019 til 2020.*

2.3.2. Sikkerhedssoftware på lokale enheder og netværk
Ved ændringen af CFCS-loven i 2019 blev der indsat hjemmel til at monitorere netværkstrafikken hos tilsluttede myndigheder og virksomheder bl.a. ved at installere sikkerhedssoftware på lokale enheder og netværk. Der kan i den forbindelse anvendes passiv sikkerhedssoftware, som på mange måder ligner den passive monitorering af netværkstrafikken, der sker, når myndigheder/virksomheder tilsluttes netsikkerhedstjenesten. Passiv sikkerhedssoftware bremser ikke cyberangreb, men opdager dem, hvorefter de kan håndteres. Der kan endvidere anvendes aktiv sikkerhedssoftware, der indebærer automatiske reak-

[5] Lovforslag nr. 215 fremsat den 27. marts 2019 ændring af lov om Center for Cybersikkerhed, bemærkningerne til § 3, stk. 1

[6] Forsvarsministeriets brev af den 22. juli 2014

[7] CFCS' årsberetninger er tilgængelige på hjemmesiden www.cfcs.dk

tioner på bestemte alarmer med det formål at forebygge, stoppe eller begrænse cyberangreb.[8]

CFCS har ikke anvendt muligheden for at installere sikkerhedssoftware på lokale enheder og netværk som led i tilslutning til netsikkerhedstjenesten. Det skyldes, at centret afventer udvikling af en passende teknisk løsning. CFCS vurderer, at hjemlen er relevant at beholde, da den fortsat understøtter et operativt behov.

2.3.3. Overførsel af løbende logoplysninger
Ved ændringen af CFCS-loven i 2019 blev der skabt mulighed for, at tilsluttede myndigheder/virksomheder løbende overfører logoplysninger og oplysninger om konstaterede og mulige sikkerhedshændelser fra myndighedens eller virksomhedens eget sikkerhedssystem. Såfremt en sådan løbende overførsel sker, anses myndigheden/virksomheden som tilsluttet netsikkerhedstjenesten, og der indgås en tilslutningsaftale.[9]

CFCS har gjort brug af denne særlige tilslutningsvariant i udvalgte tilfælde, hvor den har været formålstjenstlig.

Løbende overførsel af logoplysninger udgør et væsentligt supplement til data, der er omfattet af CFCS-lovens kapitel 4, fra et allerede monitoreret (tilsluttet) it-system eller som alternativ til monitorering (tilslutning) i de tilfælde, hvor et it-system eksempelvis er placeret i en cloudløsning. Løbende overførsel af logoplysninger bidrager dermed til at opdage, analysere og imødegå sikkerhedshændelser mod kritiske it-systemer hos tilsluttede virksomheder og myndigheder.

2.3.4. Påbud om tilslutning til netsikkerhedstjenesten
Ved ændringen af CFCS-loven i 2019 blev der endvidere indført mulighed for, at CFCS i særlige tilfælde kan påbyde virksomheder, der har særlig samfundsvigtig karakter, og regioner og kommuner, at blive tilsluttet netsikkerhedstjenesten med henblik på monitorering af netværkskommunikation, jf. CFCS-lovens § 3, stk. 4, 1. pkt. Et påbud kan kun omfatte de dele af virksomheden, regionen eller kommunen, der har en væsentlig betydning for Danmarks kritiske infrastruktur, jf. CFCS-lovens § 3, stk. 4, 2. pkt. CFCS skal mindst hvert halve år vurdere, om et meddelt påbud skal opretholdes, jf. CFCS-lovens § 3, stk. 4, 3. pkt. Det bemærkes hertil, at forsvarsministeren i medfør af CFCS-lovens § 3, stk. 5, 2. pkt., har fastsat nærmere regler for påbud efter stk. 4 i bekendtgørelse nr. 896 af 21. august 2019 om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

Der er, som ovenfor nævnt, en positiv udvikling i antallet af frivilligt tilsluttede virksomheder m.v. og CFCS har ikke anvendt muligheden for at påbyde virksomheder, der har særlig samfundsvigtig karakter, og regioner og kommuner, at blive tilsluttet netsikkerhedstjenesten. CFCS vurderer desuagtet fortsat, at hjemlen kan blive relevant.

2.4. Indgreb omfattet af grundlovens § 72

2.4.1. Bistand fra netsikkerhedstjenesten til myndigheder og virksomheder, der ikke er tilsluttet netsikkerhedstjenesten
Det fulgte af § 6 i den tidligere CFCS-lov, at der for myndigheder og virksomheder, som ikke var tilsluttet netsikkerhedstjenesten, kunne ske midlertidig tilslutning til netsikkerhedstjenesten ved begrundet mistanke om en sikkerhedshændelse, hvorefter netsikker-

[8] Lovforslag nr. 215 fremsat den 27. marts 2019 om ændring af lov om Center for Cybersikkerhed, afsnit 3.3.

[9] Lovforslag nr. 215 fremsat den 27. marts 2019 ændring af lov om Center for Cybersikkerhed, bemærkningerne til § 3, stk. 1

hedstjenesten kunne behandle pakke- og trafikdata hidrørende fra myndigheden eller virksomhedens netværk, når myndigheden eller virksomheden havde anmodet CFCS om at blive midlertidigt tilsluttet og givet skriftligt samtykke til behandlingen (nr. 1), behandlingen blev vurderet til at kunne bidrage væsentligt til CFCS' muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner var afhængige af (nr. 2), og den midlertidige tilslutning havde en varighed på højst 2 måneder (nr. 3).

Muligheden for midlertidigt at blive tilsluttet netsikkerhedstjenesten er som nævnt videreført i CFCS-lovens § 3. Det følger af lovens forarbejder hertil, at en tilslutningsaftale kan være tidsbegrænset.

Det fulgte af § 7 i den tidligere CFCS-lov, at CFCS' netsikkerhedstjeneste uden retskendelse kunne behandle data, der var indeholdt i eller hidrørende fra et informationssystem, der blev anvendt af en myndighed eller virksomhed, ved begrundet mistanke om en sikkerhedshændelse, når 1) myndigheden eller virksomheden havde anmodet CFCS om bistand, stillet informationssystemet eller dataene herfra til rådighed for netsikkerhedstjenesten og givet skriftligt samtykke til, at netsikkerhedstjenesten kunne behandle dataene, og 2) behandlingen vurderedes at kunne bidrage væsentligt til CFCS' muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner er afhængige af.

Muligheden for at modtage CFCS' netsikkerhedstjenestes bistand, uagtet myndigheden eller virksomheden ikke er tilsluttet netsikkerhedstjenesten, er videreført i CFCS-lovens § 5, dog med den begrænsning, at bistanden alene gælder for netsikkerhedstjenestens behandling af stationære data.

Det følger således af CFCS-lovens § 5, at netsikkerhedstjenesten ved begrundet mistanke om en sikkerhedshændelse uden retskendelse efter anmodning kan behandle stationære data fra myndigheder og virksomheder, der ikke er tilsluttet netsikkerhedstjenesten, når myndigheden eller virksomheden har stillet de stationære data til rådighed for netsikkerhedstjenesten og givet skriftligt samtykke til behandlingen (1), og behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet (2). Bestemmelsen omfatter også incident response (bistand til håndtering af konkrete sikkerhedshændelser).

Hjemlen i CFCS-lovens § 5 har bidraget væsentligt til at smidiggøre processen med at modtage supplerende data fra ikke-tilsluttede myndigheder og virksomheder i forbindelse med en sikkerhedshændelse. CFCS har anvendt hjemlen i en række sager siden 2019.

2.4.2. Aktivt cyberforsvar

Ved ændringen af CFCS-loven i 2019 blev der givet mulighed for at udøve aktivt cyberforsvar, jf. CFCS-lovens § 6. Det følger således af CFCS-lovens § 6, stk. 1, at netsikkerhedstjenesten, efter aftale med en tilsluttet myndighed eller virksomhed, ved begrundet mistanke om en sikkerhedshændelse uden retskendelse kan blokere, omdanne eller omdirigere trafik-og pakkedata hidrørende fra netværk hos myndigheden eller virksomheden med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet. Det følger af § 6, stk. 2, at stk. 1 finder tilsvarende anvendelse ift. stationære data, og at netsikkerhedstjenesten ved en konstateret sikkerhedshændelse kan slette stationære data, der har forårsaget sikkerhedshændelsen.

CFCS har ikke anvendt aktivt cyberforsvar, hvilket skyldes, at centret afventer den understøttende tekniske løsning. CFCS vurderer fortsat, at hjemlen er relevant.

2.4.3. Forebyggende sikkerhedstekniske undersøgelser
Ved ændringen af CFCS-loven i 2019 blev der skabt hjemmel til efter anmodning at udføre forebyggende sikkerhedstekniske undersøgelser hos myndigheder og virksomheder med henblik på at rådgive myndigheden eller virksomheden, jf. CFCS-lovens § 6 a. Det følger af § 6 a, stk. 1, at forebyggende sikkerhedstekniske undersøgelser består af den sikkerhedstekniske undersøgelse, der kan suppleres af de i stk. 2 nævnte tiltag: Behandling af trafikdata, pakkedata og stationære data hos myndigheden eller virksomheden, uden retskendelse (nr. 1), behandling af offentligt tilgængelige oplysninger om myndigheden eller virksomheden og dennes medarbejdere (nr. 2) og forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder i myndigheden eller virksomheden (nr. 3).

CFCS har i 2021 gennemført 26 sikkerhedstekniske undersøgelser og oplever en fortsat stigende efterspørgsel fra myndigheder og virksomheder efter CFCS' bistand til at udføre forebyggende sikkerhedstekniske undersøgelser. Udviklingen i antallet af sikkerhedstekniske undersøgelser fremgår af CFCS' årlige beretninger[10]:

	2019	**2020**	**2021**
Sikkerhedstekniske undersøgelser	7	16	26

Muligheden for at gennemføre forebyggende sikkerhedstekniske undersøgelser har styrket CFCS' forebyggende indsats væsentligt, hvilket til dels skyldes muligheden for at udøve indgreb omfattet af grundlovens § 72 i forbindelse med undersøgelserne. Muligheden for at anvende elementer af social engineering som for eksempel spear-phishing med henblik på at skabe eller eskalere adgang til systemer har gjort, at CFCS kan udføre mere komplekse undersøgelser af høj kvalitet.

Tilbagemeldingerne fra myndigheder og virksomheder, der har fået gennemført forebyggende sikkerhedstekniske undersøgelser af CFCS, har generelt været meget positive, og CFCS vurderer, at undersøgelserne og CFCS' opfølgende anbefalinger har stor værdi i forhold til at højne sikkerheden ved de undersøgte myndigheder og virksomheder. Myndigheder og virksomheder, der har fået gennemført forebyggende sikkerhedstekniske undersøgelser af CFCS, har i flere tilfælde efterfølgende efterspurgt andre ydelser fra CFCS, herunder rådgivning samt tilslutning til CFCS' netsikkerhedstjeneste.

2.4.4. Honey Pots
Ved ændringen af CFCS-loven i 2019 blev der skabt hjemmel til, at CFCS kan opsætte fiktive angrebsmål – såkaldte honeypots – med henblik på at opnå viden om angrebsaktørers metoder og værktøjer, såfremt opsætningen vurderes at kunne bidrage væsentligt til CFCS' muligheder for at understøtte et højt informationssikkerhedsniveau i samfundet, jf. CFCS-lovens § 6 b. Honeypots er fiktive angrebsmål, der er udstyret med potentielle sårbarheder, med det formål at tiltrække angrebsaktører.

CFCS har ikke anvendt muligheden for at opsætte honeypots, da centret afventer den nødvendige tekniske løsning. CFCS vurderer, at hjemlen fortsat er relevant.
2.4.5. Sinkholes
Ved ændringen af CFCS-loven i 2019 blev der skabt mulighed for, at CFCS kan gøre brug af domænenavne og tilsvarende it-infrastruktur, som anvendes eller har været anvendt af en angrebsaktør, forudsat at disse er ledige til registrering, med henblik på at forhindre,

[10] CFCS' årsberetninger kan findes på hjemmesiden, www.cfcs.dk

standse eller begrænse en nært forestående eller igangværende sikkerhedshændelse – såkaldte sinkholes – jf. CFCS-lovens § 6 c. Sinkholes anvendes til at overtage en ondsindet aktørs angrebsinfrastruktur med henblik på at standse eller begrænse et angreb.

CFCS har i ét tilfælde benyttet sig af hjemlen i § 6 c til at overtage dele af en aktørs angrebsinfrastruktur. Anvendelsen af hjemlen bidrog med større indsigt i aktørens angrebsmetoder samt til at udfinde yderligere ofre i Danmark, som herefter kunne varsles om angrebet. Viden fra sinkholet bidrog desuden til en malwareanalyserapport, som blev offentliggjort på CFCS' hjemmeside og delt bredt.

CFCS vurderer, at hjemlen fortsat er relevant både i forhold til at opnå viden om angrebsaktørerne og identificere ofre for angreb.

2.5. Edition

Ved ændringen af CFCS-loven i 2019 blev der skabt adgang til at gøre brug af edition, jf. kapitel 4 a (§§ 7-7 d). Det indebærer, at retten efter begæring fra CFCS kan pålægge personer og virksomheder at udlevere oplysninger om brugeren af en e-mailkonto, ip-adresse eller et domænenavn til CFCS, hvis det er nødvendigt for at afdække forhold vedrørende en sikkerhedshændelse.

Centret har anvendt hjemlen og indtil videre indhentet seks kendelser. Muligheden for at anvende edition har gjort CFCS i stand til selvstændigt at arbejde med identifikation af mål for it-sikkerhedshændelser. Muligheden anvendes i de tilfælde, hvor der mangler oplysninger om, hvem der på et givet tidspunkt har været bruger af en specifik internetprotokoladresse. Dette er en særlig værdifuld mulighed i forbindelse med undersøgelse af cyberangreb foretaget af udenlandske – eventuelt statsstøttede – aktører eller sikkerhedshændelser.

Processen med varsling, analyse og imødegåelse af en sikkerhedshændelse kan først iværksættes, når selve målet for angrebet er identificeret. Ved at anvende edition i en hurtig og effektiv sagsgang kan CFCS hurtigt vurdere, hvorvidt der har været tale om et målrettet angreb mod et sårbart mål. Det gør CFCS i stand til at kunne imødegå sikkerhedshændelser hurtigt og effektivt. Dette har stor betydning ift. ikke bare at imødegå hændelsen, men også at sikre relevant data før disse slettes.

2.6. Analyse, videregivelse og sletning af data

2.6.1. Analyse af data

Ved ændringen af CFCS-loven i 2019 blev der indsat en bestemmelse om automatiserede og manuelle analyser af data, jf. CFCS-lovens § 15. Bestemmelsen er videreført fra den tidligere CFCS-lov, men er blevet udvidet, således at der er flere muligheder for at analysere data, og det er præciseret, at der skelnes mellem automatiserede og manuelle analyser.

CFCS' muligheder for at foretage automatiserede og manuelle analyser af data tilvejebragt efter CFCS-lovens kapitel 4 fremgik ikke eksplicit af den tidligere CFCS-lovs § 15. Med den nye bestemmelse i CFCS-lovens § 15, stk. 1, 1. pkt., er der skabt udtrykkelig hjemmel til, at CFCS kan foretage automatiserede analyser af trafik- og pakkedata samt stationære data tilvejebragt efter CFCS-lovens kapitel 4. CFCS anvender i høj grad automatiserede analyser af data med henblik på at scanne store mængder af data for kendte angrebsformer, der udløser alarmer, hvorefter data udtages til manuel analyse, såfremt betingelserne herfor er opfyldt. Med den nye bestemmelse i CFCS-lovens § 15, stk. 1, 2. pkt., er der fastsat udtrykkelige regler for, hvornår CFCS må foretage manuelle analyser af data,

der er omfattet af CFCS-lovens kapitel 4, herunder fsva. trafik- og pakkedata samt stationære data samt fsva. data tilvejebragt i forbindelse med forebyggende sikkerhedstekniske undersøgelser m.v.

Det bemærkes, at definitionen af stationære data i CFCS-lovens § 2, nr. 4, sammenholdt med betingelserne for manual analyse af bl.a. stationære data i CFCS-lovens § 15, nr. 2, efter CFCS' opfattelse, begrænser centrets muligheder for at opdage, analysere og imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder. Udfordringerne med definitionen af stationære data er beskrevet yderligere i afsnit 2.2. Det bemærkes endvidere, at centret finder det uhensigtsmæssigt, at det ikke er muligt at foretage manuelle analyser af stationære data i det løbende arbejde med at understøtte et højt informationssikkerhedsniveau på Forsvarsministeriets område.

Ved ændringen af CFCS-loven i 2019 blev endvidere givet mulighed for at analysere trafik- og pakkedata i forbindelse med test og konfiguration af netsikkerhedstjenestens alarmenheder, jf. CFCS-lovens § 15, nr. 5. Analysen må foretages, uden at der foreligger begrundet mistanke om en sikkerhedshændelse. Hjemlen giver mulighed for at teste, hvorvidt opsætning og/eller nyudviklede funktioner virker efter hensigten. Centret anvender i høj grad hjemlen i CFCS-lovens § 15, nr. 5. Dette sker både i forbindelse med opsætning af alarmenheder hos nytilsluttede og allerede tilsluttede myndigheder og virksomheder og i forbindelse med udvikling af nye funktioner eller ved opdateringer på alarmenhederne.

Det bemærkes, at centret oplever at være begrænset af, at der efter bestemmelsen alene må ske manuel analyse af trafik-og pakkedata. CFCS modtager i stigende grad logoplysninger fra tilsluttede myndigheder og virksomheder, og da disse anses for stationære data, jf. CFCS-lovens § 2, nr. 4, har centret ikke mulighed for at analysere oplysningerne, medmindre der foreligger en sikkerhedshændelse. De samme omstændigheder gør sig gældende for data modtaget fra installeret sikkerhedssoftware på lokale enheder og netværk hos tilsluttede myndigheder og virksomheder.

2.6.2. Videregivelse af data

CFCS-loven fra 2019 giver mulighed for at videregive trafik- og pakkedata samt stationære data og malware, jf. CFCS-lovens § 16, stk. 1-4. Bestemmelsen er videreført fra den tidligere CFCS-lov, men er blevet udvidet, således at der er en videregivelseshjemmel for hver datatype. Endvidere regulerer bestemmelsen, hvornår der må ske videregivelse af hhv. malware og trafikdata, når denne type data stammer fra tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder. Hjemlen i den seneste CFCS-lov er blevet udvidet, således at der er en bredere mulighed for at videregive data – og dermed et bredere udvalg af datatyper relateret til it-sikkerhedshændelser. Dette har medført, at CFCS har fået bedre muligheder for at varsle myndigheder og virksomheder samt generelt dele mere indsigtsgivende viden med myndigheder og virksomheder. Muligheden for at videregive en bredere del af data relateret til en it-sikkerhedshændelse har været udnyttet og anses som et væsentlig positivt bidrag til både kvaliteten og effekten af CFCS' håndtering af it-sikkerhedshændelser.

Mulighederne for videregivelse af trafik- og pakkedata samt stationære data, jf. CFCS-lovens § 16, stk. 1-3, anvendes i centrets daglige håndtering af it-sikkerhedshændelser og har derfor haft afgørende betydning for centrets opgave med at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder. Muligheden for at videregive trafik- og pakkedata samt stationære data til den myndighed eller virksomhed, der er berørt af en sikkerhedshændelse, understøtter, at CFCS kan kommunikere meningsfuldt med de berørte parter i en tæt, teknisk dialog med henblik på at

afdække sikkerhedshændelsen. Dette muliggør, at myndigheden eller virksomheden kan træffe de nødvendige forholdsregler.

I forbindelse med CFCS' udsendelse af sikkerhedsvarslinger sker videregivelse af malware i medfør af CFCS-lovens § 16, stk. 4 ofte til såvel den myndighed eller virksomhed, hvorfra data stammer, som til andre netsikkerhedstjenester, myndigheder og virksomheder i øvrigt. Muligheden for at videregive malware medfører, at CFCS kan varsle bredt om erkendte angrebsmetoder, mål eller sårbarheder. CFCS fremhæver, at centret har videregivet malwaresamples som gør, at virksomheder og myndigheder i øget omfang kan ruste sig mod et cyberangreb, hvor den pågældende malware anvendes.

Centret har i vidt omfang anvendt muligheden for videregivelse af data, der stammer fra tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder i dialogen med myndigheder og virksomheder med henblik på at sikre, at der alene ydes den aftalte netværksdækning samt til kvalitetssikring af de indkomne data. Muligheden for at anvende data i dialogen med myndigheden eller virksomheden har haft en stor positiv effekt på onboardingprocessen for nye myndigheder og virksomheder

CFCS' videregivelse af oplysninger vedrørende myndighedens eller virksomhedens medarbejdere i forbindelse med en forebyggende sikkerhedsteknisk undersøgelse i medfør af CFCS-lovens § 6 a sker alene i anonymiseret form, jf. CFCS-lovens § 16, stk. 6.
Kravet om anonymisering af disse oplysninger vurderes ikke at medføre væsentlige begrænsninger i forhold til værdien af den afrapportering, som myndigheder og virksomheder, der får udført sikkerhedstekniske undersøgelser af CFCS, modtager.

2.6.3. Sletning af data
CFCS-loven indeholder i lovens § 17, stk. 1, en formålsbestemt slettefrist. Det følger heraf, at data, der er omfattet af kapitel 4, slettes, når formålet med behandlingen er opfyldt. Endvidere angiver den nugældende CFCS-lov absolutte slettefrister, jf. CFCS-lovens § 17, stk. 2, der indtræder efter hhv. 5 år (nr. 1), 3 år (nr. 2) eller 13 mdr. (nr. 3), uanset at formålet med behandlingen af data ikke er opfyldt, jf. stk. 1.

Fsva. videreførelsen af kravet om sletning af data, når formålet med behandlingen er videreført, jf. CFCS-lovens § 17, stk. 1, bemærkes, at det efter CFCS' opfattelse er en væsentlig forudsætning for at kunne løse opgaven med at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder, at CFCS har hjemmel til at opbevare store mængder af data i længere tid. Det bemærkes, at dette ligeledes gør sig gældende i situationer, hvor opbevaringen af data alene sker med henblik på en potentiel senere anvendelse. Der opstår alene i meget få tilfælde situationer, hvor formålet med behandlingen anses for opfyldt, inden de absolutte slettefrister indtræder.

Videreførelse af kravet om sletning af data, når formålet med behandlingen er opfyldt, indebærer desuden, at data snarest muligt slettes, såfremt en myndighed eller virksomhed opsiger en tilslutningsaftale. Det omfatter som udgangspunkt al data, som CFCS har behandlet på baggrund af tilslutningsaftalen, dog ikke data, der konkret knytter sig til en sikkerhedshændelse.

Der er i den forbindelse grund til at fremhæve, at centrets arbejde omfatter en løbende indsats for at opnå viden om centrale aktører og deres metoder og værktøjer. Ny viden fra partnertjenester eller fra en konkret sikkerhedshændelse kan betyde, at CFCS får indsigt i metoder og værktøjer, der kan identificere sikkerhedshændelser i data, som ikke har været erkendt på et tidligere tidspunkt. Data, som er kommet til CFCS' kendskab, men som ikke tidligere har medvirket til at afdække sikkerhedshændelser, kan dermed på et senere tidspunkt medvirke til afdækning af fjendtligsindet aktivitet imod danske myndigheder og virksomheder. Sletning af data i forbindelse med opsigelse af en tilslutningsaftale

kan medføre, at CFCS ikke kan opdage og dermed varsle en tilsluttet virksomhed eller myndighed om angreb, der er pågået i tilslutningsperioden, i de tilfælde, hvor angrebet først opdages på et senere tidspunkt.

CFCS-lovens § 17, stk. 2, nr. 3 viderefører en bestemmelse fra den tidligere CFCS-lov, der ligeledes angav en slettefrist på 13 mdr. for data, der ikke knytter sig til en sikkerhedshændelse. Slettefristen for data, der knytter sig til en sikkerhedshændelse, blev med den seneste CFCS-lov udvidet fra 3 år til 5 år, jf. CFCS-lovens § 17, stk. 2, nr. 1. Endvidere blev der indført en særskilt absolut slettefrist på 3 år for data, der stammer fra myndigheder, som i særlig grad beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold, samt virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold, jf. CFCS-lovens § 17, stk. 2, nr. 2. Tidligere var denne omfattet af slettefristen på 13 mdr. for data, der ikke knytter sig til en sikkerhedshændelse.
De absolutte slettefrister giver udfordringer i tilfælde, hvor eksempelvis myndigheder er genstand for længerevarende angrebskampagner, der først opdages efter 13 mdr. eller senere. Særligt når det gælder opdagelse af avancerede cyberangreb fra statsstøttede aktører har CFCS erfaret, at det har stor betydning, at centret kan tilgå ældre data med henblik på f.eks. at afdække angrebets iværksættelse og varighed. Statsstøttede angrebsaktører arbejder ofte politisk styret og mod strategiske mål. Det betyder, at deres indsatser er langvarige angrebskampagner, der kan strække sig over flere år. Sletning af data efter 13 mdr. øger risikoen for, at CFCS sletter væsentlig viden om angreb og angrebsaktører, som endnu ikke er opdaget. Centret har i flere tilfælde været nødsaget til at slette meget værdifulde oplysninger om statsstøttede aktørers infrastruktur eller malware grundet de absolutte slettefrister i CFCS-lovens § 17, stk. 2, nr. 1.

Udvidelsen af slettefristen fra 3 år til 5 år, jf. CFCS-lovens § 17, stk. 2, nr. 1, og udvidelsen af slettefristen fra 13 mdr. til 3 år, jf. CFCS-lovens § 17, stk. 2, nr. 2, har overordnet set betydet, at CFCS i højere grad end tidligere er i stand til at opdage og dermed bidrage til at imødegå og analysere sikkerhedshændelser.

Den reviderede bestemmelse i CFCS-lovens § 17, stk. 4 giver mulighed for backup af data, hvilket er en vigtig del af at sikre et robust it-miljø ved CFCS. Backup vil i nogle tilfælde indeholde data, der er blevet slettet efter det tidspunkt, hvor backuppen er taget. I tilfælde af at en backup gendannes, sikrer CFCS, at data slettes igen som en del af genskabelsesproceduren.

Efter CFCS-lovens § 17, stk. 6, 1. pkt., skal personoplysninger i data, som CFCS får adgang til som led i forebyggende sikkerhedstekniske undersøgelser, jf. CFCS-lovens § 6 a, slettes eller anonymiseres, når den sikkerhedstekniske undersøgelse er afsluttet. Konstaterer CFCS, at der i de pågældende data indgår følsomme personoplysninger, skal disse slettes uden unødigt ophold, jf. CFCS-lovens § 17, stk. 6, 2. pkt. Data, som behandles af centret i forbindelse med gennemførelse af en forebyggende sikkerhedstekniske undersøgelse, behandles i overensstemmelse med CFCS-loven. Data slettes således, når formålet med behandlingen er opfyldt, jf. CFCS-lovens § 17, stk. 1. Centret sikrer sig desuden, at eventuelle data, der indeholder personoplysninger, slettes eller anonymiseres, jf. CFCS-lovens § 17, stk. 6. Som udgangspunkt opbevarer CFCS data på arbejdsklienter og eksterne medier i 3 mdr. efter gennemførelse af en sikkerhedsteknisk undersøgelse, hvorefter undersøgelsen betragtes som afsluttet. Fristen på 3 mdr. er fastsat for at give en myndighed eller virksomhed tilstrækkelig tid til at analysere CFCS' undersøgelsesrapport og indgå i dialog med CFCS om eksempelvis opfølgende spørgsmål til undersøgelsens data.

Kravet om sletning eller anonymisering af personoplysninger, der er indeholdt i data fra sikkerhedstekniske undersøgelser, vurderes ikke at medføre begrænsninger i forhold til værdien af CFCS' forebyggende sikkerhedstekniske undersøgelser.

Slettefristerne kan i helt særlige tilfælde kortvarigt suspenderes, jf. CFCS-lovens § 17, stk. 2, nr. 2 og 3, såfremt væsentlige hensyn til varetagelsen af CFCS' opgaver gør det nødvendigt, jf. CFCS-lovens § 17, stk. 7. Ved suspension skal Tilsynet med Efterretningstjenesterne (TET) straks underrettes og oplyses om baggrunden herfor. Hjemlen forudsættes anvendt i tilfælde, hvor der er mistanke om en sikkerhedshændelse, og hvor der er fare for, at relevant data, der endnu ikke er analyseret, slettes i medfør af de absolutte slettefrister. Centret har ikke gjort brug af hjemlen.

Afslutningsvist bemærkes det, at det følger af CFCS-lovens § 17 a, at § 17 ikke finder anvendelse på data, der er deponeret på fiktive angrebsmål efter § 6 b eller modtaget via infrastruktur omfattet af § 6 c, såfremt CFCS ikke udtager disse data til nærmere vurdering. Disse data slettes hurtigst muligt. Udtager CFCS data til nærmere vurdering, skal sletning ske efter reglerne i § 17. Grundet CFCS begrænsede erfaring med anvendelsen af honeypots og sinkholes, jf. ovenfor, har centret ingen bemærkninger til denne bestemmelse.

2.7. Andre forhold

	2016	2017	2018	2019	2020	2021
Fuld aktindsigt	1	0	1	0	1	0
Delvis aktindsigt	1	0	0	2	1	1
Afslag på aktindsigt	0	1	7	3	6	3
Ingen dokumenter lokaliseret til at give eller afslå aktindsigt	1	1	2	1	1	2
Samlet antal	3	2	10	6	9	6

Antallet af aktindsigtsanmodninger, som CFCS har modtaget i perioden fra 2016 indtil udgangen af 2020, er ligeledes nævnt i TET's årsredegørelser for de pågældende år[11].

3. Tilsynet med Efterretningstjenesternes tilsyn med behandling af personoplysninger i CFCS

3.1. Tilsynet med Efterretningstjenesterne

TET er et særligt uafhængigt kontrolorgan, der har ført tilsyn med CFCS' behandling af personoplysninger siden 1. juli 2014, hvor lov om Center for Cybersikkerhed trådte i kraft. Det følger af CFCS-lovens § 20, at TET efter klage eller af egen drift påser CFCS' overholdelse af de gældende regler i CFCS-lovens kapitel 4, 4 a, 6 og 7, vedrørende behandling af personoplysninger.

3.2. Tilsynet med Efterretningstjenesternes årsredegørelser

Det følger af CFCS-lovens § 24, at TET afgiver en årlig redegørelse om sin virksomhed til forsvarsministeren og at denne redegørelse offentliggøres. TET's årlige redegørelser kan findes på TET's hjemmeside, www.tet.dk.

TET har i en række tilfælde over de seneste år tilkendegivet i tilsynets årsredegørelser, at TET's kontroller af CFCS i de pågældende år viste, at CFCS generelt overholder CFCS-

[11] Se årsredegørelser for 2016-2020

lovgivningens bestemmelser om indgreb i meddelelseshemmeligheden, behandling af personoplysninger samt bestemmelserne om analyse og videregivelse af oplysninger.

Af relevans for erfaringerne med CFCS-loven fra 2019 har TET anført følgende:

- For så vidt angår sletning i medfør af CFCS-lovens § 17, stk. 1, har TET anført, at kontrollen i 2019 viste, at oplysninger, der var omfattet af lovens kapitel 4, ikke var slettet i overensstemmelse med § 17, stk. 1. For så vidt angår kontrollen i 2020 har TET anført, at 13 filer i et separat it-miljø ikke var slettet i overensstemmelse med lovens § 17, stk. 1. Fortolkningen af CFCS-lovens § 17, stk. 1, blev i 2020 indbragt for forsvarsministeren af CFCS. Forsvarsministeren har ved afgørelse tiltsluttet sig CFCS' fortolkning af bestemmelsen, hvilket omtales nærmere i TET's årsredegørelse for CFCS for 2021. TET's kontroller af CFCS i 2021 har ikke givet anledning til bemærkninger i forhold til CFCS' sletning af data i medfør af § 17, stk. 1.

- For så vidt angår sletning i medfør af CFCS-lovens § 17, stk. 2, har TET anført, at kontrollen i 2020 viste, at CFCS på to tilfældigt udtrukne sensorer på sensornetværket ikke havde slettet data, der var omfattet af lovens kapitel 4, i medfør af § 17, stk. 2. TET's kontroller af CFCS i 2021 har ikke givet anledning til bemærkninger i forhold til CFCS' sletning af data i medfør af § 17, stk. 2.

- Endvidere har TET anført, at CFCS-medarbejdere i én afdeling i både 2019 og 2020 behandlede oplysninger på drev i overensstemmelse med CFCS-lovgivningen. CFCS-medarbejdere var både i 2019 og 2020 generelt opmærksomme på, at behandling af oplysninger skal ske i overensstemmelse med CFCS-loven. For så vidt angår kontrollen i 2019 har TET anført, at CFCS i ét tilfælde ikke behandlede oplysninger i overensstemmelse med CFCS-loven. TET har ikke gennemført kontroller på dette område i 2021.

- TET førte i 2019 i øvrigt kontrol med CFCS' behandling, videregivelse og udveksling af oplysninger. Kontrollerne har ikke givet anledning til bemærkninger fra TET. TET førte ligeledes i 2020 kontrol med CFCS' behandling, videregivelse, og udveksling af oplysninger, men kunne ikke gennemføre kontrol af videregivelse af data pga. forhold hos CFCS. I øvrigt har kontrollerne ikke givet anledning til bemærkninger fra TET. TET's kontrol med behandling, videregivelse og udveksling af oplysninger har i 2021 ikke givet anledning til bemærkninger.