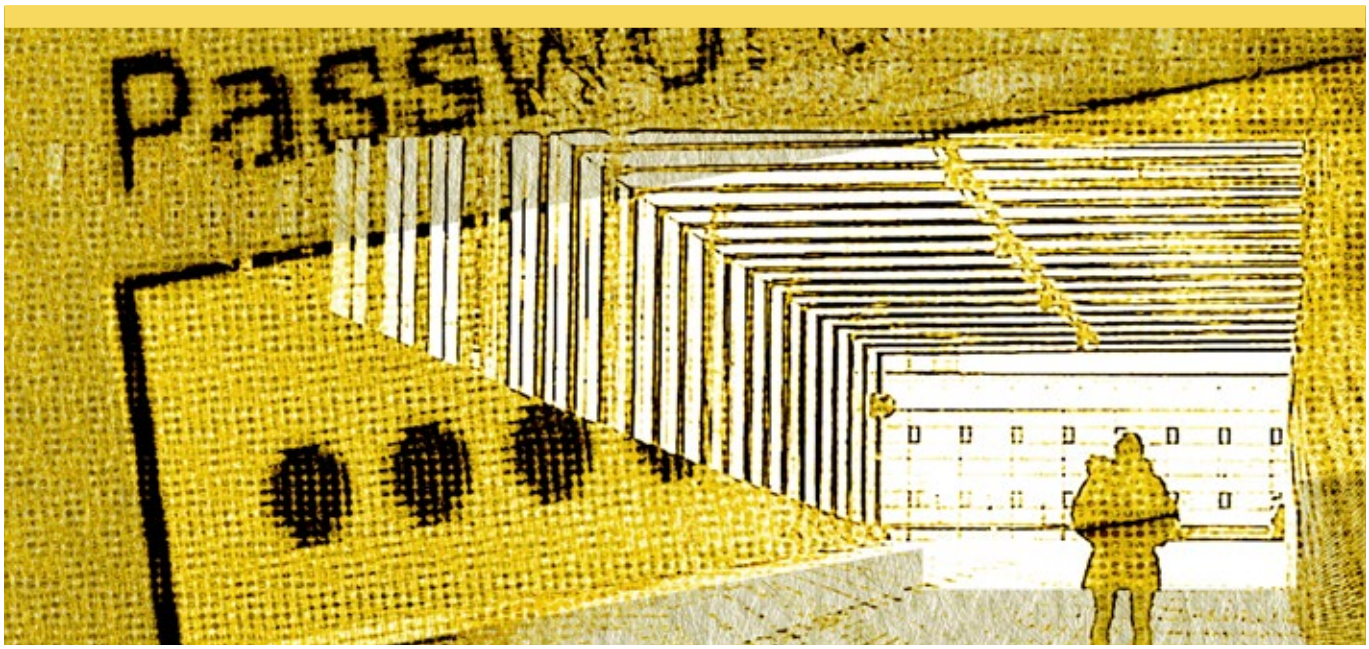
tet

Tilsynet med Efterretningstjenesterne



Årsredegørelse 2020

Center for Cybersikkerhed

Indhold

APPENDIKS

Til forsvarsministeren

I overensstemmelse med § 24 i lov om Center for Cybersikkerhed (lovbekendtgørelse nr. 836 af 7. august 2019) afgiver Tilsynet med Efterretningstjenesterne hermed redegørelse om sin virksomhed vedrørende Center for Cybersikkerhed for 2020. Redegørelsen skal offentliggøres.

København, august 2021

Michael Kistrup
Formand for Tilsynet med Efterretningstjenesterne

Resumé

Sigtet med redegørelsen er at give en generel information om karakteren af det tilsyn, der udøves med CFCS.

Tilsynet påser, at CFCS overholder lovens regler om

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

Redegørelsen indeholder blandt andet oplysninger om de forhold, som tilsynet har valgt at interessere sig for, og om i hvor mange tilfælde tilsynet har fundet, at CFCS' behandling af personoplysninger ikke har været i overensstemmelse med reglerne. For 2020 fremhæves følgende centrale og principielle dele af redegørelsen:

! Tilsynets kontrol af CFCS i 2020 viste, at centret **generelt har overholdt CFCS-lovgivningens bestemmelser om indgreb i meddelelseshemmeligheden, om behandling af personoplysninger samt om analyse og videregivelse**.

! Tilsynet har imidlertid på baggrund af sin kontrol af CFCS' anvendelse af centrets sensornetværk, jf. afsnit 1.2.1, konstateret, at centret **behandlede sensordata** på to af de tilfældigt udtrukne sensorer på sensornetværket i strid med CFCS-lovens § 17, stk. 2.

! Tilsynet har desuden på baggrund af sin kontrol af oplysninger i CFCS' separate it-miljøer og analyseværktøjer, jf. 1.2.2, konstateret, at centret **behandlede 13 filer** i strid med CFCS-lovens § 17, stk. 1, samt at oplysningerne i to analysesystemer ikke behandles i overensstemmelse med tilsynets fortolkning af CFCS-lovens § 17, stk. 1, henset til, at centret ikke foretager en løbende vurdering af, om der fortsat er behov for at behandle sensordata i analysesystemerne.

! Tilsynet har i forbindelse med en afsluttet kontrol fra 2019 vedrørende CFCS' anvendelse af centrets sensornetværk efterfølgende drøftet fortolkningen af sletteforpligtelsen i CFCS-lovens § 17, stk. 1, med centret, som er uenig i tilsynets vurdering og derfor i juli 2020 har **indbragt spørgsmålet for forsvarsministeren**. Tilsynet har efter indbringelse af spørgsmålet for forsvarsministeren ikke foretaget fokuseret kontrol af CFCS' overholdelse af sletteforpligtelsen i CFCS-lovens § 17, stk. 1, da tilsynet afventer forsvarsministerens afgørelse. Tilsynets fortolkning af CFCS-lovens § 17, stk. 1, er behandlet nærmere i afsnit 2.

! Tilsynet har i 2020 **ikke kunne foretage den ønskede kontrol af CFCS' videregivelser af data** indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, på grund af forhold hos centret. Tilsynet finder det problematisk, at CFCS ikke har etableret logning af systemer, som anvendes til videregivelse af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden umiddelbart efter tilsynets anmodning i januar 2020.

Det bemærkes, at ovenstående henvisninger alene udgør et mindre udsnit af tilsynets kontrol af CFCS i 2020, hvor tilsynet har haft særlige eller principielle bemærkninger. For det fulde billede af tilsynets kontrol af CFCS skal redegørelsen læses i sin helhed.

Forord

Tilsynet med Efterretningstjenesterne er et særligt uafhængigt kontrolorgan, der blandt andet fører tilsyn med, at Center for Cybersikkerhed (CFCS) behandler oplysninger om fysiske personer i overensstemmelse med lovgivningen. Tilsynet blev oprettet ved lov om Politiets Efterretningstjeneste (PET), der trådte i kraft den 1. januar 2014.

Sigtet med nærværende redegørelse er at informere om karakteren af det tilsyn, der udøves vedrørende CFCS. Redegørelsen indeholder oplysninger om de forhold, som tilsynet i 2020 har valgt særligt at interessere sig for, og om i hvor mange tilfælde tilsynet har fundet, at CFCS' behandling af personoplysninger ikke har været i overensstemmelse med reglerne.

Som i de forgangne år har tilsynet i 2020 haft fokus på at konsolidere og styrke grundlaget for tilsynets kontrol af henholdsvis CFCS, Forsvarets Efterretningstjeneste (FE), PET og Rigspolitiets PNR-enhed (RPNR), herunder ved løbende udvikling af tilsynets risiko- og væsentlighedsvurdering af tjenesterne, centret og enheden samt de standarder og metoder, som anvendes i den retlige kontrol heraf. Det er afgørende for tilsynet, at de enkelte kontroller er velunderbyggede og -dokumenterede, og at de er tilrettelagt på baggrund af en tilstrækkelig efterretningsfaglig og teknisk forståelse.

Tilsynet virksomhed har i 2020 været påvirket af COVID-19-pandemien, da tilsynet har været lukket ned fra den 13. marts 2020 til den 10. maj 2020 samt fra den 9. december 2020 til den 6. april 2021. Tilsynets medarbejdere har i perioderne ikke haft mulighed for at arbejde hjemmefra. Tilsynet har imidlertid gennemført samtlige planlagte kontroller af CFCS i 2020.

Tilsynet har i 2020 gennemført omfattende og intensive kontroller med CFCS' behandling af oplysninger om fysiske personer. Som i de foregående år har tilsynet prioriteret kontroller med fokus på CFCS' overholdelse af reglerne om analyse, videregivelse og sletning af data tilvejebragt ved indgreb i meddelelseshemmeligheden samt centrets behandling af personoplysninger i øvrigt.

Tilsynet har i forbindelse med en afsluttet kontrol fra 2019 vedrørende CFCS' anvendelse af centrets sensornetværk efterfølgende drøftet fortolkningen af sletteforpligtelsen i CFCS-lovens § 17, stk. 1, med centret, som er uenig i tilsynets vurdering og derfor i juli 2020 har indbragt spørgsmålet for forsvarsministeren. Tilsynets fortolkning af CFCS-lovens § 17, stk. 1, er behandlet nærmere i afsnit 2.

Ved anordning nr. 1658 af 20. november 2020 er lov om Center for Cybersikkerhed sat i kraft for Grønland. Da anordningen først er trådt i kraft den 1. januar 2021, har tilsynet ikke henset hertil ved sin kontrol af CFCS i 2020.

Tilsynet har i 2020 fortsat sit samarbejde med andre europæiske tilsynsmyndigheder, som udfører kontrol med efterretnings- eller sikkerhedstjenester i Holland, Belgien, Norge, Sverige, Schweiz og Storbritannien. Samarbejdet har i 2020 imidlertid været væsentligt påvirket af COVID-19-pandemien.

I efteråret 2020 har tilsynet desuden fået et nyt medlem.

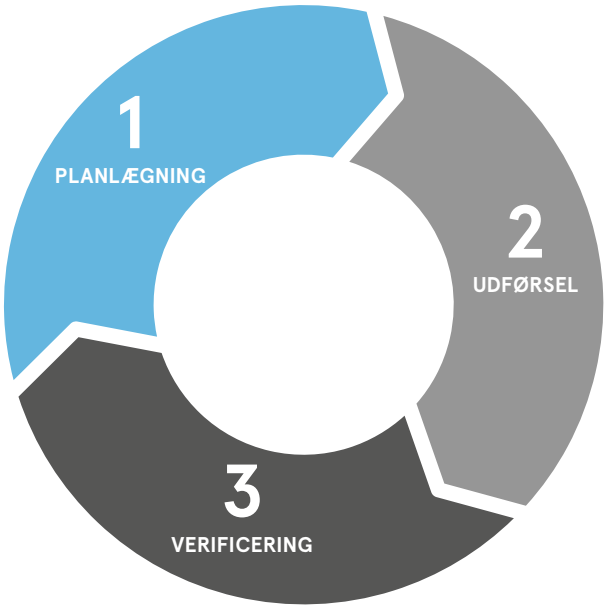
Michael Kistrup
Formand for Tilsynet med Efterretningstjenesterne

1. Tilsynets kontrol

1.1 Kontrolmetode

Tilsynet arbejder kontinuerligt med at forbedre de metoder, som tilsynet anvender i planlægningen og udførelsen af kontrollen af CFCS med henblik på, at kontrollen får den størst mulige effekt inden for de rammer, som er sat for tilsynets virke.

Tilsynets kontrol af CFCS består overordnet af følgende tre delelementer:



Tilsynets **1)** planlægning af kontroller for det kommende år sker på baggrund af en årlig risiko- og væsentlighedsvurdering af processer og systemer i CFCS. Formålet hermed er at vurdere risici for lovbrud i relation til centrets aktiviteter, der er omfattet af tilsynets kompetence. På baggrund heraf udarbejder tilsynet risikoanalyser, som danner grundlag for udvælgelsen af det kommende års kontroller.

Formålet med risikoanalyserne er at sikre, at tilsynets kontrol fokuseres på de områder, hvor der er størst risiko for fejl, samt at der tages højde for andre relevante faktorer, eksempelvis områder hvor tilsynets kontrol fra lovgivers side er tillagt særlig vægt, såsom reglerne om videregivelse og udveksling af oplysninger.

Områder, hvor der vurderes at være en lav risiko for fejl, kontrolleres som hovedregel en gang hvert tredje år med henblik på at skabe fuldstændighed i kontrollen af CFCS og sikre, at vurderingen af risiko for fejl på området fortsat er retvisende.

Tilsynets kontroller **2)** udføres løbende hen over året på baggrund af tilsynets beslutning om kontrolplan vedrørende CFCS. Tilsynet fastlægger ikke metoder for de enkelte kontroller i forbindelse med udarbejdelsen af risikovurderinger og -analyser, hvorfor metodevalget skal afklares forud for igangsættelse af en specifik kontrol.

Tilsynet benytter sig af en række forskellige metoder i kontrollen af de enkelte områder, heriblandt fuldstændig kontrol, tilfældige eller målrettede stikprøver, indholdsscreening, inspektioner og interviewbaseret kontroller.

Tilsynets valg af kontrolmetode sker på baggrund af en konkret risikovurdering af kontrolområdet, erfaringer fra tidligere kontroller samt de faktiske forhold, som tilsynet konstaterer i forbindelse med den specifikke kontrol. I den sammenhæng afholder tilsynet forud for en kontrol af ikke tidligere kontrollerede områder tekniske møder og opstartsmøder med relevante medarbejdere i CFCS med henblik på at sikre en tilstrækkelig teknisk forståelse af området, således at kontrollen kan tilpasses og gennemføres hensigtsmæssigt.

Endelig foretager tilsynet **3)** verificering ved løbende kortlægning af CFCS' it-infrastruktur på server-, komponent- og applikationsniveau med henblik på at kunne foretage fuldstændige risikovurderinger af samtlige processer og systemer i centret. Formålet med verificeringen er at sikre, at tilsynets kontrol beror på oplysninger fra CFCS, hvis rigtighed tilsynet har efterprøvet.

Tilsynets direkte adgang til CFCS' systemer sikrer, at centret ikke kan forudse, hvilke sager og oplysninger der bliver genstand for tilsynets kontrol. I nogle tilfælde er det imidlertid nødvendigt for tilsynet at varsle CFCS om tidspunktet og metoden for en kontrol, eksempelvis hvis tilsynet skal have adgang til særlige fysiske lokaliteter eller skal interviewe specifikke medarbejdere.

Tilsynet deler forud for påbegyndelsen af årets kontroller sin risikoanalyse og kontrolplan med CFCS med henblik på blandt andet at sikre åbenhed om tilsynets vurdering af forholdene i centret. Åbenheden giver endvidere CFCS mulighed for at tage højde for tilsynets kontrol i tilrettelæggelsen af centrets interne kontrol, hvilket bidrager til, at tilsynets kontrol og centrets interne kontrol samlet dækker en større del af centrets virksomhed. Endelig sikrer åbenheden, at CFCS kan afsætte tilstrækkelige ressourcer til at servicere tilsynet.

For yderligere information om tilsynets kontrolmetodik henvises til de af tilsynet udarbejdede standarder herfor, som findes på tilsynets hjemmeside.

1.2 Kontrol af CFCS i 2020

Med henblik på at kontrollere at CFCS i forbindelse med behandling af oplysninger om fysiske personer overholder reglerne i CFCS-loven, har tilsynet i 2020 foretaget kontrol af centrets

- anvendelse af centrets sensornetværk (1.2.1),
- behandling af oplysninger i separate it-miljøer og analyseværktøjer (1.2.2),
- drev (1.2.3),
- arbejdsstationer (1.2.4),
- videregivelse af oplysninger til andre myndigheder, virksomheder og samarbejdspartnere (1.2.5),
- udveksling af oplysninger med den øvrige del af FE (1.2.6),
- behandling af personoplysninger (1.2.7),
- interne kontrol (1.2.8) og
- opfølgning på tilsynets kontrol af CFCS i 2019 (1.2.9).

SAMMENFATNING AF TILSYNETS KONTROLLER I 2020

Tilsynets kontrol af CFCS i 2020 viste, jf. afsnit 1.2.3, 1.2.4, 1.2.6 og 1.2.7, at centret generelt overholder CFCS-lovgivningens bestemmelser om indgreb i meddelelseshemmeligheden, om behandling af personoplysninger samt om analyse, videregivelse og udveksling.

Tilsynets kontrol af CFCS' sensornetværk viste imidlertid, jf. afsnit 1.2.1, at centret behandlede sensordata på to af de tilfældigt udtrukne sensorer på sensornetværket i strid med lovgivningens krav om sletning, jf. CFCS-lovens § 17, stk. 2.

Tilsynets kontrol af CFCS' behandling af oplysninger i separate it-miljøer og analyseværktøjer viste, jf. afsnit 1.2.2, at centret behandlede 13 filer i strid med CFCS-lovens § 17, stk. 1, samt at oplysningerne i to analysesystemer ikke behandles i overensstemmelse med tilsynets fortolkning af CFCS-lovens § 17, stk. 1, henset til, at centret ikke foretager en løbende vurdering af, om der fortsat er behov for at behandle sensordata i analysesystemerne.

Vedrørende tilsynets kontrol af CFCS' videregivelse af data i 2020, jf. afsnit 1.2.5, har det ikke været muligt for tilsynet at foretage den ønskede kontrol på grund af forhold hos centret. Tilsynet finder det problematisk, at CFCS ikke har etableret logning af systemer, som anvendes til videregivelse af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden umiddelbart efter tilsynets anmodning i januar 2020.

Endvidere viste kontrollen af CFCS' interne kontrol, jf. afsnit 1.2.8, at centret generelt har tilrettelagt og gennemført sin interne kontrol tilfredsstillende.

1.2.1 Kontrol af CFCS' anvendelse af centrets sensornetværk

CFCS' sensornetværk overvåger internettrafik hos tilsluttede myndigheder og virksomheder. Sensorerne indeholder en række regler, der bruges til at genkende forsøg på cyberangreb. Når der via sensorerne registreres potentielt ondsindet trafik, som passer på en regel, modtager CFCS en alarm. Medarbejdere i CFCS henter derefter et relevant udsnit af internettrafikken med henblik på at foretage en undersøgelse af årsagen hertil.

Tilsynet har i 2020 foretaget kontrol af CFCS' behandling, herunder sletning, af oplysninger på centrets sensornetværk.

Tilsynet foretog en stikprøve af et antal tilfældigt udvalgte sensorer på sensornetværket med henblik på at kontrollere, om oplysningerne blev slettet i overensstemmelse med CFCS-lovens § 17, stk. 2.

Tilsynet afventer fortsat svar fra forsvarsministeren vedrørende fortolkningen af CFCS-lovens § 17, stk. 1 (se afsnit 2), hvorfor tilsynet i 2020 ikke har foretaget kontrol af CFCS' iagttagelse af CFCS-lovens § 17, stk. 1, på sensornetværket.

TILSYNETS BEMÆRKNINGER

Tilsynets kontrol af CFCS' anvendelse af centrets sensornetværk viste, at centret behandlede sensordata på to af de tilfældigt udtrukne sensorer i strid med lovgivningens krav om sletning, jf. CFCS-lovens § 17, stk. 2.

1.2.2 Kontrol af CFCS' behandling af oplysninger på separate it-miljøer og analyseværktøjer

CFCS anvender en række separate it-miljøer og analyseværktøjer i forbindelse med centrets tekniske analyse af angreb og malware. CFCS behandler og lagrer sensordata i disse it-miljøer og analyseværktøjer i forbindelse med centrets analyse heraf.

Tilsynet har i 2020 foretaget kontrol af udvalgte dele af CFCS' separate it-miljøer og analyseværktøjer.

Tilsynet foretog kontrol af et separat it-miljø og to analyseværktøjer. Kontrollen af det separate it-miljø blev gennemført ved en fuldstændig kontrol af oplysningerne, mens kontrollerne af analyseværtøjerne blev gennemført ved indholdsscreening af de pågældende oplysninger.

TILSYNETS BEMÆRKNINGER

Tilsynets kontrol af CFCS' separate it-miljø og analyseværktøjer viste, at centrets behandling af oplysninger i analysesystemer var i overensstemmelse med CFCS-loven.

Kontrollen af et separat it-miljø viste imidlertid, at 13 filer blev behandlet i strid med CFCS-lovens § 17, stk. 1, hvilket CFCS erklærede sig enig i.

Endvidere viste kontrollen af analyseværktøjer, at oplysningerne i begge analysesystemer behandles i strid med tilsynets fortolkning af CFCS-lovens § 17, stk. 1, henset til, at CFCS ikke foretager en løbende vurdering af, om der fortsat er behov for at behandle sensordata i analysesystemet. Tilsynet afventer forsvarsministerens afgørelse vedrørende tilsynets fortolkning af § 17, stk. 1, se afsnit 2.

1.2.3 Kontrol af drev

CFCS anvender drev til opbevaring af oplysninger, som anvendes i centrets afdelinger og sektioner, men som ikke nødvendigvis registreres i centrets centrale systemer.

Tilsynet har i 2020 foretaget kontrol af CFCS' behandling af oplysninger på drev.

Tilsynet foretog løbende kontrol af et drev, som anvendes af medarbejdere tilknyttet CFCS' netsikkerhedstjeneste. Kontrollen blev gennemført ved en fuldstændig gennemgang af indholdet af drevet.

TILSYNETS BEMÆRKNINGER

Tilsynets kontrol af CFCS' behandling af oplysninger på drev viste, at centret generelt har iagttaget lovgivningens bestemmelser herom.

1.2.4 Kontrol af arbejdsstationer

Tilsynet har i 2020 foretaget kontrol af et antal medarbejderes arbejdsstationer.

Tilsynets foretog kontrol af et antal tilfældigt udvalgte arbejdsstationer, herunder af personlige drev, mailsystemer, eksterne lagringsenheder og fysiske dokumenter. I forbindelse med den stikprøvevise gennemgang af oplysningerne på den enkelte arbejdsstation stillede tilsynet spørgsmål til vedkommende medarbejder om pågældendes kendskab til reglerne om behandling, herunder sletning, af oplysninger vedrørende fysiske personer.

TILSYNETS BEMÆRKNINGER

Tilsynets kontrol af udvalgte arbejdsstationer viste, at CFCS' medarbejdere overholdt CFCS-loven og centrets interne retningslinjers regler om behandling af oplysninger. Kontrollen viste endvidere, at medarbejderne var opmærksomme på, at behandling af oplysninger sker i overensstemmelse med CFCS-lovgivningen og centrets interne retningslinjer.

1.2.5 Kontrol af CFCS' videregivelse af oplysninger til andre myndigheder, virksomheder og samarbejdspartnere

Tilsynet har i 2020 ikke foretaget den planlagte kontrol af CFCS' videregivelse af data indeholdende personoplysninger til andre myndigheder, virksomheder og udenlandske samarbejdspartnere med fokus på centrets overholdelse af CFCS-lovens §§ 10 og 16.

Tilsynet anmodede i januar 2020 CFCS om, at etablere logning af systemer, som anvendes til videregivelse af personoplysninger med henblik på at anvende logudtræk fra disse til kontrol af centrets videregivelse af data indeholdende personoplysninger til andre myndigheder, virksomheder og udenlandske samarbejdspartnere i 2020.

CFCS oplyste i oktober 2020, at centret ikke har etableret den logning, som tilsynet anmodede om i januar 2020. I maj 2021 har CFCS fremsendt logmateriale for de pågældende systemer.

TILSYNETS BEMÆRKNINGER

Tilsynet finder, at det ikke i 2020 har været muligt for tilsynet at foretage den ønskede kontrol af CFCS' videregivelser af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, på grund af forhold hos centret.

Tilsynet finder det problematisk, at CFCS ikke har etableret logning af systemer, som anvendes til videregivelse af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden umiddelbart efter tilsynets anmodning i januar 2020.

1.2.6 Kontrol af CFCS' udveksling af oplysninger med den øvrige del af FE

Tilsynet har i 2020 foretaget kontrol af CFCS' udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE.

CFCS er organisatorisk en del af FE, og derfor er den interne udveksling af oplysninger mellem centret og de øvrige dele af FE ikke omfattet af CFCS-lovens regler om videregivelse. Forsvarsministeriet har i cirkulære nr. 9741 af 21. august 2019 om behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste (CFCS-cirkulæret) fastsat regler for udveksling af oplysninger fra CFCS til FE.

Tilsynet har i 2020 foretaget en fuldstændig kontrol af CFCS' udveksling af oplysninger med den øvrige del af FE.

TILSYNETS BEMÆRKNINGER

Tilsynets kontrol af CFCS' udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE viste, at centret har iagttaget CFCS-cirkulærets bestemmelser herom.

1.2.7 Kontrol af CFCS' behandling af personoplysninger

Tilsynet har ved sin kontrol af CFCS i 2020 foretaget kontrol af centrets behandling af personoplysninger.

Kontrollen er foranlediget af tilsynets kontrol af udvalgte arbejdsstationer i 2019 (se tilsynets redegørelse for 2019, afsnit 1.2.4) som viste, at en medarbejder i et tilfælde behandlede oplysninger i strid med CFCS-loven, idet tilsynet fandt, at det af centret oplyste formål ikke var tilstrækkeligt grundlag for behandlingen. Kontrollen har haft til formål at undersøge, om CFCS generelt behandler personoplysninger til formål, som er i strid med CFCS-lovgivningen.

TILSYNETS BEMÆRKNINGER

Tilsynets kontrol af CFCS' behandling af personoplysninger i 2020 viste, at centret har iagttaget lovgivningens krav til behandling af oplysninger.

I forlængelse af kontrollen fandt tilsynet imidlertid anledning til af bemærke, at bevaring og behandling af personoplysninger til andre formål, efter at det oprindelige formål med behandlingen er afsluttet, efter tilsynets opfattelse vil være i strid med CFCS-lovens § 9 og § 14.

1.2.8 Kontrol af CFCS' interne kontrol

Tilsynet har ved sin kontrol af CFCS i 2020 foretaget kontrol af centrets interne kontrol. Kontrollen har omfattet CFCS' interne kontrol samt centrets planlægning heraf for 2020 og er foretaget ved gennemgang af udleveret dokumentation.

TILSYNETS BEMÆRKNINGER

Tilsynets kontrol af CFCS' interne kontrol i 2020 viste, at centret generelt har tilrettelagt den interne kontrol tilfredsstillende.

1.2.9 Opfølgning på tilsynets kontrol af CFCS i 2019

Tilsynet foretager årligt kontrol af, at CFCS har foretaget de handlinger, som centret på baggrund af tilsynets kontrol i det foregående år har tilkendegivet at ville gennemføre.

I tilsynets redegørelse for 2019, afsnit 1.2.4, beskrev tilsynet, at CFCS havde tilkendegivet, at centret på baggrund af tilsynets kontrol af arbejdsstationer i 2019 har besluttet at udarbejde nye retningslinjer vedrørende medarbejderes behandling af oplysninger om fysiske personer.

TILSYNETS BEMÆRKNINGER

Opfølgning på tilsynets kontrol af CFCS i 2019 har givet anledning til høring af centret om, hvorvidt centret har udarbejdet de retningslinjer, som centret i forbindelse med tilsynets kontrol i 2019 havde tilkendegivet, at ville udarbejde. CFCS har på tidspunktet for udarbejdelse af tilsynets redegørelse ikke udarbejdet de pågældende retningslinjer.

2. Sletning efter CFCS-lovens § 17, stk. 1

Tilsynet foretog i 2019 kontrol af CFCS' tilvejebringelse af oplysninger fra centrets sensornetværk på baggrund af alarmer samt den efterfølgende behandling, herunder sletning, af hentet sensordata, se tilsynets redegørelse for 2019, afsnit 1.2.1. Ved sensordata forstås data hentet fra CFCS' sensornetværk, se afsnit 1.2.1.

Tilsynet foretog en stikprøve af et antal tilfældigt udvalgte hentninger fra sensornetværket med henblik på at kontrollere, om oplysningerne efterfølgende blev slettet i overensstemmelse med CFCS-lovens § 17, stk. 1, hvoraf det følger, at data, der behandles efter lovens kapitel 4 om indgreb i meddelelseshemmeligheden §§ 4-6, skal slettes, når formålet med behandlingen er opfyldt. Tilsynet havde spørgsmål til 67 procent af de udtrukne tilfælde, hvor CFCS havde afsluttet sin behandling af de alarmer, som den pågældende pakkedata var indhentet på baggrund af, men ikke foretaget sletning af det hentede pakkedata. Ved pakkedata forstås indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester.

CFCS besvarede tilsynets spørgsmål og oplyste i sit høringssvar blandt andet, at formålet med behandlingen af pakkedata i de sager, som tilsynet har haft spørgsmål til, endnu ikke er opfyldt. CFCS har således fortsat behov for at kunne fremfinde tidligere behandlet pakkedata blandt andet med henblik på at kunne identificere, om tidligere aktører på ny er aktive, eller om data, der ser mistænkelig ud, tidligere har været analyseret som falske positiver. Pakkedata opbevares frem til det tidspunkt, hvor data skal slettes efter CFCS-lovens § 17.

Tilsynet konstaterede på baggrund af kontrollen, at CFCS' behandling af sensordata i 67 procent af de udtrukne tilfælde ikke var i overensstemmelse med lovgivningens krav om løbende sletning, jf. CFCS-lovens § 17, stk. 1, idet tilsynet fandt, at det af centret oplyste formål ikke var tilstrækkeligt grundlag for behandlingen.

CFCS oplyste efterfølgende, at centret var uenig i tilsynets vurdering og indbragte spørgsmålet for forsvarsministeren i juli 2020.

Tilsynet har på tidspunktet for udarbejdelsen af tilsynets redegørelse ikke modtaget en afgørelse fra forsvarsministeren.

2.1 Tilsynets vurdering

Følgende fremgår af bemærkningerne til CFCS-lovens § 17:

> *"Den foreslåede § 17 fastsætter de tidsmæssige rammer for Center for Cybersikkerheds opbevaring af de data, der behandles i medfør af det foreslåede kapitel 4 og dermed behandles på baggrund af indgreb i meddelelseshemmeligheden. Bestemmelsen skal ses i sammenhæng med den foreslåede § 14, hvorefter indsamlede personoplysninger generelt ikke må opbevares på en måde, der giver mulighed for at identificere den pågældende person i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. Mens § 14 finder anvendelse på al behandling af personoplysninger i Center for Cybersikkerhed, finder de særlige regler i § 17 som nævnt alene anvendelse på de data, der behandles på baggrund af indgreb i meddelelseshemmeligheden. Bestemmelsen er en delvis videreførelse af GovCERT-lovens § 4, stk. 2-4. Efter det foreslåede stk. 1 vil data skulle slettes, når formålet med behandlingen er opfyldt, hvilket er en videreførelse af GovCERT-lovens § 4, stk. 2, idet bestemmelsen dog foreslås udvidet til at omfatte alle former for data, der behandles på baggrund af indgreb i meddelelseshemmeligheden. Der vil på den baggrund ske en løbende vurdering af de behandlede data med henblik på at sikre, at data, der ikke længere er relevante i forhold til netsikkerhedstjenestens formål og aktiviteter, straks slettes."*

Bestemmelsen en delvis videreførelse af GovCERT-lovens § 4, stk. 2-4. Følgende fremgår af bemærkningerne til GovCERT-lovens § 4:

> *"Det er i den forbindelse væsentligt at være opmærksom på, at GovCERT med den foreslåede lov kun får hjemmel til at analysere pakkedata ved begrundet mistanke om en stedfunden eller forventet sikkerhedshændelse. Adgangen til pakkedata er yderligere begrænset af, at kun den del af de indsamlede pakkedata, som er relevant for den pågældende analyse af sikkerhedshændelsen, vil kunne analyseres. Adgangen for GovCERT til pakkedata er herved begrænset mest muligt for at imødekomme hensynet til privatlivets fred.*
>
> *[...]*
>
> *Opbevaringsperioden for indsamlede oplysninger om de tilsluttede myndigheders ind- og udgående internetkommunikation vil højst være tre år for så vidt angår pakke- og trafikdata, der knytter sig til en sikkerhedshændelse. Opbevaringsperioden påregnes dog i de mange tilfælde at være væsentligt kortere, idet GovCERT er forpligtet til at slette data, så snart data ikke længere er relevant i forhold til GovCERT's formål og aktiviteter."*

Derudover fremgår følgende af de almindelige bemærkninger til GovCERT-loven:

> *"Pakkedata vil blive slettet umiddelbart efter GovCERT's analyse, hvis denne ikke viser tegn på en sikkerhedshændelse. Analyseret pakkedata vil således kun blive opbevaret i GovCERT's system til at registrere sikkerhedshændelser, hvis data er knyttet til en sikkerhedshændelse."*

Det er på den baggrund tilsynets vurdering, at CFCS-lovens § 17 er udtryk for et dataminimeringsprincip, således at CFCS i videst muligt omfang skal slette pakkedata, når centret ikke længere har behov for at behandle den pågældende data.

CFCS har i sit høringssvar gjort gældende, at formålet med behandling af de pågældende pakkedata fortsat er opfyldt, på trods af at centret har afsluttet sin behandling af de alarmer, som den pågældende pakkedata er indhentet på baggrund af. Det skyldes, ifølge CFCS, at der fortsat er behov for at kunne fremfinde tidligere behandlet pakkedata, blandt andet med henblik på at kunne identificere, om tidligere aktører på ny er aktive, eller om data, der ser mistænkelig ud, tidligere har været analyseret som falske positiver.

Det er tilsynets vurdering, at et generelt behov for at kunne fremfinde tidligere behandlet pakkedata, uanset om pakkedata vedrører eller ikke vedrører en sikkerhedshændelse, ikke er en tilstrækkelig begrundelse for at undlade sletning efter CFCS-lovens § 17, stk. 1.

Det er endvidere tilsynets vurdering, at en udstrækning af slettefristen i CFCS-lovens § 17, stk. 1, til i alle tilfælde at være sammenfaldende med de absolutte slettefrister i CFCS-lovens § 17, stk. 2, vil betyde at CFCS-lovens § 17, stk. 1, ikke har et selvstændigt indhold samt være i strid med det dataminimeringsprincip, som CFCS-lovens § 17 er udtryk for.

CFCS vil fortsat kunne behandle den del af pakkedata, som centret konkret vurderer er nødvendig at behandle.

Det er desuden tilsynets vurdering, at pakkedata, som er hentet på baggrund af en alarm, og som CFCS efterfølgende vurderer er indhentet på grund af en falsk alarm, i alle tilfælde ikke er omfattet af 5-årsfristen i CFCS-lovens § 17, stk. 2, nr. 1, men kun vil kunne opbevares ind til udløbet af slettefristerne i CFCS-lovens § 17, stk. 2, nr. 2 og 3 (henholdsvis 3 år eller 13 måneder), idet centret ved analysen har konstateret, at den pågældende data ikke vedrører en sikkerhedshændelse.


PASSWORD

3. Eksempler på CFCS' håndtering af cyberangreb

Ifølge forarbejderne til CFCS-loven skal tilsynets årlige redegørelse om sin virksomhed vedrørende CFCS blandt andet indeholde en fuldt ud anonymiseret beskrivelse af et eller flere konkrete cyberangreb.

CFCS har bidraget med følgende beskrivelse af cyberangreb i 2020:

Center for Cybersikkerheds (CFCS) Netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at håndtere it-sikkerhedshændelser hos de offentlige myndigheder og private virksomheder, der er tilsluttet sensornetværket. Denne indsats er bredt fokuseret og omfatter derfor både håndtering af almene angreb, der typisk udføres af mindre kriminelle grupper samt de mest avancerede spionageangreb, der typisk udføres af statsstøttede aktører.

CFCS' døgnbemandede Cybersituationscenter, som er en del af Netsikkerhedstjenesten, indgår i håndteringen og analysen af sikkerhedshændelser hos de tilsluttede kunder. Derudover har Cybersituationscenteret også et særligt fokus på at indsamle, analysere og dele viden om aktuelle cyberangreb, der påvirker dansk kritisk infrastruktur, herunder de seks samfundskritiske sektorer i Danmark.

I forbindelse med Coronakrisens indtog opbyggede CFCS i 2020 en kapacitet til at identificere og varsle mod phishingdomæner, som var målrettet mod danske interesser, herunder bl.a. COVID-19-forskning, -oplysning og -vacciner, NemID, danske banker, pakketransportører m.fl. Fælles for mange af domænerne var, at de forsøgte at franarre NemID-login eller andre personlige oplysninger fra de besøgende.

Domæner, som har haft relation til COVID-19 situationen, har CFCS haft succes med at DNS-blokere i tæt samarbejde med Nationalt Cyber Crime Center (NC3) i Rigspolitiet, der har en særlig lovhjemmel til blokering af datatrafik mod disse hjemmesider, jf. lov nr. 349 af 2. april 2020. Derudover har CFCS også anmodet

hosting-udbydere om at tage hjemmesider ned, hvis phishingdomænet ikke direkte var relateret til COVID-19, men relateret til øvrig online svindelforsøg.

Derudover har Netsikkerhedstjenesten og Cybersituationscenteret håndteret og observeret en lang række it-sikkerhedshændelser i 2020. Størstedelen af disse hændelser omhandlede primært rekognosceringsforsøg, forskellige former for social engineering samt forsøg på udnyttelse af sårbarheder og fejlkonfigurationer i software, der er eksponeret mod internettet. CFCS har derudover også observeret og behandlet et antal angrebsforsøg med relation til ransomware.

Baseret på CFCS' observationer, anses angrebsforsøg via phishingmails fortsat som en alvorlig trussel mod centerets kunder. Dette kan eksempelvis være mails fra forskellige ondsindede aktører, der forsøger at lokke modtageren til at aktivere eller tilgå indhold i mailen, som enten kan føre til inficeringer eller som forsøger at franarre adgangsoplysninger fra ofret.

Ransomware fortsatte som en trussel i 2020, og der er observeret en mere struktureret fremgangsmåde i hvorledes angreb bliver orkestreret. Virksomheder eller myndigheder, som rammes af ransomware, oplever ofte store driftsforstyrrelser med betydelige økonomiske konsekvenser til følge. Udviklingen inden for ransomware er derfor et område, som har haft Netsikkerhedstjenestens fokus i 2020.

Desuden har CFCS som nævnt observeret forskellige typer forsøg på at udnytte eventuelle fejlkonfigurationer og sårbarheder i softwaretjenester. Dette indebærer eksempelvis også regulære brute force-angrebsforsøg rettet mod eksponerede it-systemer hos kunderne, som angriberen forsøger at tiltvinge sig adgang til.

4. Statistik vedrørende CFCS' behandling af oplysninger

Det fremgår af forarbejderne til CFCS-loven, at tilsynets årlige redegørelse om sin virksomhed vedrørende CFCS skal indeholde statistiske oplysninger om centrets behandling af personoplysninger, herunder oplysninger om antallet af modtagne klagesager i såvel centret 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 centret.

Redegørelsen skal endvidere indeholde statistik over antallet af tilfælde, hvor en analytiker fra CFCS på baggrund af indgreb i meddelelseshemmeligheden har foretaget en analyse af data. Denne statistik skal indeholde en overordnet kategorisering af, hvor alvorlige disse tilfælde har været.

CFCS har bidraget med følgende data for 2020:

TABEL 1

Modtagne klagesager over CFCS' behandling af personoplysninger

Kategorier	2020
Klager til CFCS over behandling af personoplysninger	0
Klagesager modtaget i tilsynet	0

TABEL 2

Aktindsigtssager

Kategorier	2020
Fuld aktindsigt	1
Delvis aktindsigt	1
Afslag på aktindsigt	6
Ingen dokumenter lokaliseret til at give eller afslå aktindsigt i	1
Total	**9**

TABEL 3

Sikkerhedshændelser* efter alvorlighedsgrad

Kategorier	2020
Alvorlige cyberangreb	1
Større cyberangreb	2
Moderate cyberangreb	31
Mindre cyberangreb	443
Ingen/begrænset effekt**	4.503
Total	**4.980**

* Sikkerhedshændelser defineres i overensstemmelse med § 2, nr. 1, i lov om Center for Cybersikkerhed.

** Kategorien "Ingen/begrænset effekt" inkluderer alle sikkerhedshændelser, som ikke har haft indvirkning på kunden.

TABEL 4

CFCS' videregivelse* og udveksling af oplysninger

Kategorier	2020
Videregivelser	100
Udvekslinger	19

* Antallet af CFCS' netsikkerhedstjenestes videregivelser af oplysninger, herunder oplysninger, der stammer fra indgreb i meddelelseshemmeligheden, omfatter samtlige videregivne oplysninger, herunder om fysiske og juridiske personer, samt oplysninger, der ikke er personhenførbare. Se desuden tilsynets kontrol heraf, jf. afsnit 1.2.5.

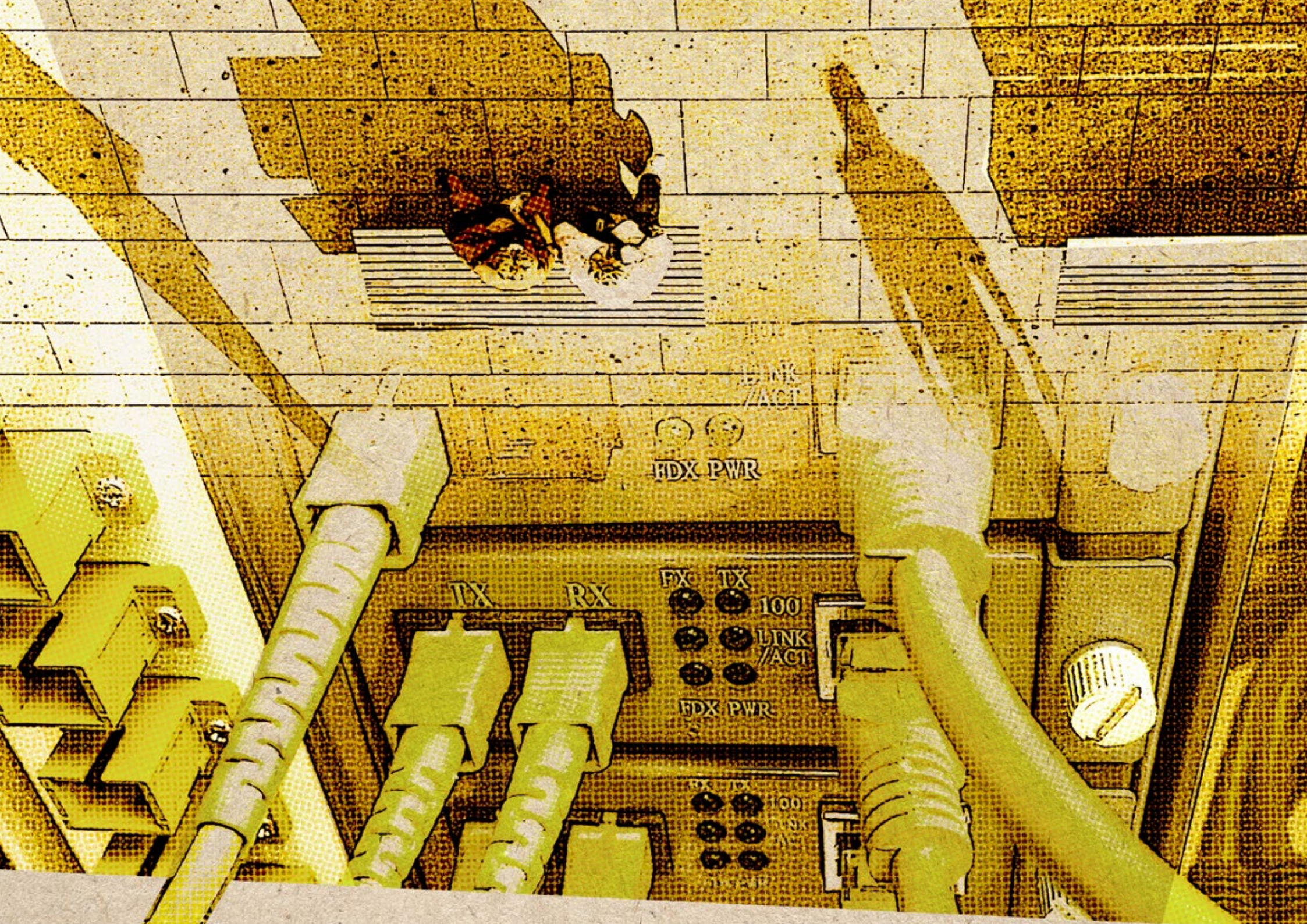
5. Presseomtale i 2020

CFCS' virksomhed, samt de rammer som Folketinget og regeringen sætter for denne, heriblandt tilsynets kontrol, er løbende genstand for omtale i de danske medier.

Tilsynet ønsker i videst muligt omfang at bidrage til, at pressen og dermed offentligheden får den bedst mulige indsigt i tilsynets kontrol af CFCS, under hensyntagen til det behov for hemmeligholdelse som følger af centrets særlige funktion.

Tilsynet følger løbende med i den offentlige debat om tilsynets kontrol af CFCS, med henblik på at vurdere om tilsynet kan bidrage til en bedre forståelse af tilsynets rolle og kontrolmuligheder samt resultaterne af tilsynets kontrol.

Tilsynets betydning som kontrolorgan har ikke været fremhævet i den offentlige debat i 2020.


FDX PWR
TX
RX
FX TX
100
LINK
/ACT
FDX PWR

Appendiks 1. Om Center for Cybersikkerhed

Center for Cybersikkerhed (CFCS) blev oprettet i 2012 som en del af Forsvarets Efterretningstjeneste (FE) og har som hovedopgave at være

- statslig og militær varslingstjeneste for internettrusler,
- national it-sikkerhedsmyndighed (bortset fra Justitsministeriets område, hvor Politiets Efterretningstjeneste (PET) varetager opgaven) og
- myndighed for informationssikkerhed og beredskab på teleområdet.

Det er CFCS' opgave som statslig og militær varslingstjeneste for internettrusler at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af. Denne opgave løses blandt andet ved, at CFCS' netsikkerhedstjeneste opdager, analyserer og bidrager til at imødegå avancerede cyberangreb hos Forsvaret samt de statslige myndigheder og virksomheder, der er tilsluttet centrets sensornet.

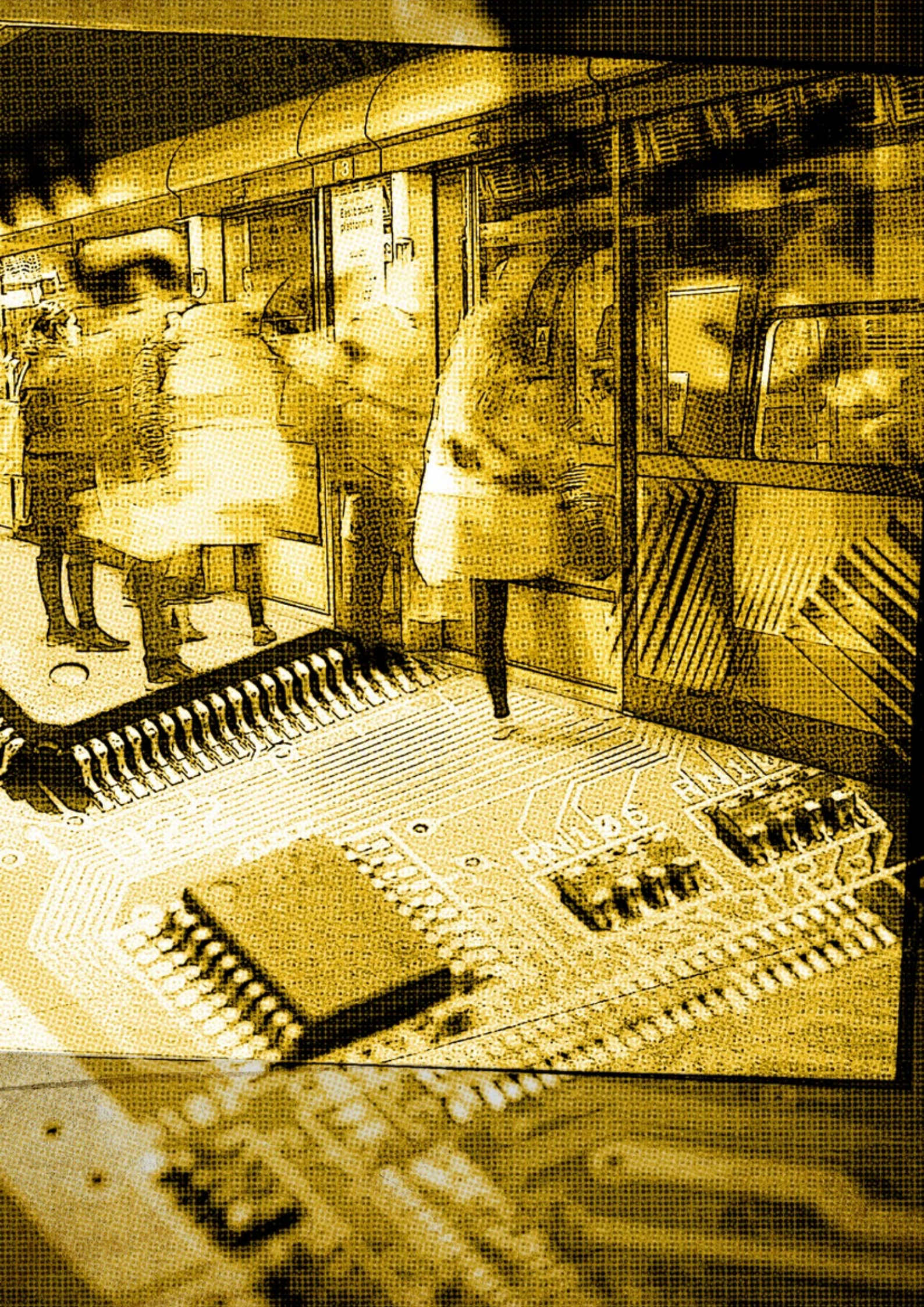
CFCS' opgave som national it-sikkerhedsmyndighed indebærer, at centret oplyser, vejleder og rådgiver danske myndigheder og virksomheder om it-sikkerhed og fungerer som nationalt kompetencecenter på cybersikkerhedsområdet. Som national it-sikkerhedsmyndighed er det tillige CFCS' opgave at sikkerhedsgodkende og føre tilsyn med klassificerede produkter, systemer og installationer inden for informations- og kommunikationsteknologi.

CFCS' varetagelse af opgaven som myndighed for informationssikkerhed og beredskab på teleområdet indebærer, at centret blandt andet fører tilsyn på området og rådgiver samfundets beredskabsaktører om teleberedskab. Herunder udsteder CFCS med bemyndigelse i lov om net- og informationssikkerhed (herefter NIS-loven) bekendtgørelser og har til opgave at føre tilsyn på området samt på overordnet niveau at koordinere håndteringen af særlige trusler, som kan påvirke informationssikkerheden i telesektoren.

De juridiske rammer for CFCS' virksomhed følger i det væsentlige af CFCS-loven med tilhørende bekendtgørelse og cirkulære samt NIS-loven.

CFCS-loven regulerer blandt andet centrets opgaver samt indgreb i meddelelseshemmeligheden, behandling, analyse, videregivelse og sletning af personoplysninger. Med loven er det yderligere bestemt, at Tilsynet med Efterretningstjenesterne, der som et uafhængigt kontrolorgan fører tilsyn med PET og FE, tillige skal føre tilsyn med, at CFCS' behandling af oplysninger om fysiske personer er i overensstemmelse med lovgivningen.

CFCS er tillige undergivet ekstern kontrol af Forsvarsministeriet, domstolene og Folketingets Ombudsmand.



2. Tilsynet med Efterretningstjenesterne

Tilsynet er et særligt uafhængigt kontrolorgan, der fører tilsyn med, at PET, FE, CFCS og Rigspolitiets PNR-enhed (RPNR) behandler personoplysninger i overensstemmelse med lovgivningen.

Tilsynet udøver sine funktioner i fuld uafhængighed og er således ikke undergivet tjenestebefalinger fra Forsvarsministeriet eller andre administrative myndigheder med hensyn til udøvelsen af sin virksomhed.

Tilsynet består af fem medlemmer, der er udpeget af justitsministeren efter forhandling med forsvarsministeren. Formanden, der skal være landsdommer, er udpeget efter indstilling fra præsidenterne for Østre Landsret og Vestre Landsret, mens de øvrige medlemmer er udpeget efter drøftelser med Folketingets Udvalg vedrørende Efterretningstjenesterne.

Medlemmerne var ved udgangen af 2020:

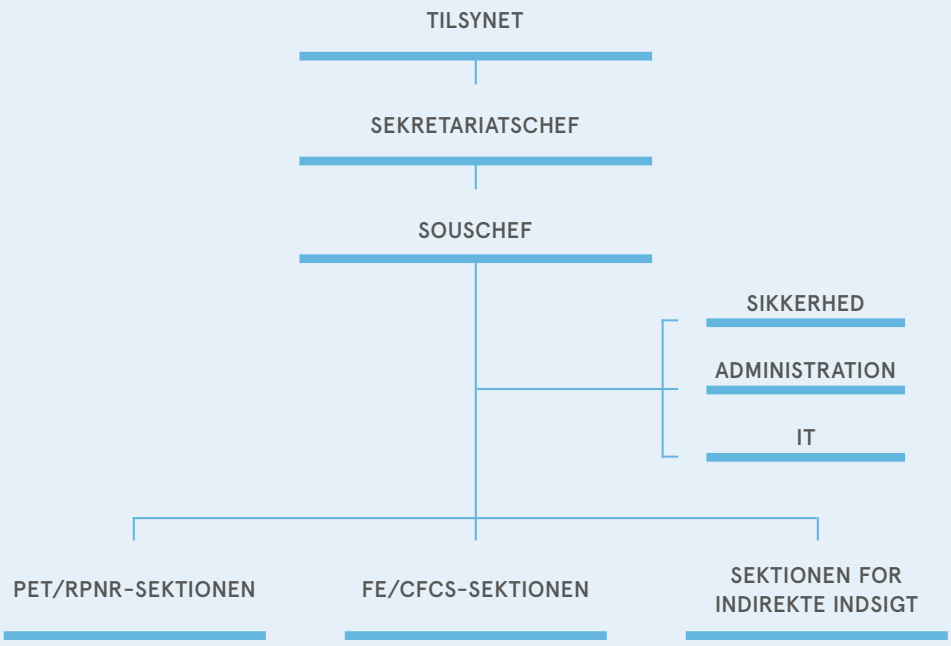
- Landsdommer Michael Kistrup, Østre Landsret (formand)
- Juridisk chef Pernille Christensen, Kommunernes Landsforening
- Professor Henrik Udsen, Københavns Universitet
- Professor Rebecca Adler-Nissen, Københavns Universitet
- Koncerndirektør David Hellemann, Nykredit

Medlemmerne udpeges for en periode på fire år med mulighed for genbeskikkelse for yderligere fire år. Ved tilsynets etablering i 2014 blev to medlemmer udpeget for to år med mulighed for genbeskikkelse for yderligere fire år med henblik på at sikre mod en samtidig og fuldstændig udskiftning af tilsynets medlemmer, idet de efterfølgende funktionsperioder er forskudt to år i forhold til hinanden.

Tilsynet bistås af et sekretariat, der alene er undergivet tilsynets instruktion. Tilsynet bestemmer selv, hvem der skal ansættes til sekretariatet, herunder hvilken uddannelsesmæssig baggrund og øvrige kvalifikationer de pågældende skal have. Ved udgangen af 2020 bestod sekretariatet af en sekretariatschef, der varetager den daglige ledelse af sekretariatet, en souschef, fire jurister, to it-konsulenter og en kontorfunktionær.

Sekretariatet er opdelt i sektioner, der beskæftiger sig med henholdsvis PET/RPNR, FE/CFCS og anmodninger om indirekte indsigt. Med henblik på at sikre faglig koordinering og erfaringsudveksling arbejder tilsynets medarbejdere på tværs af sektionerne.

Organisation 2020



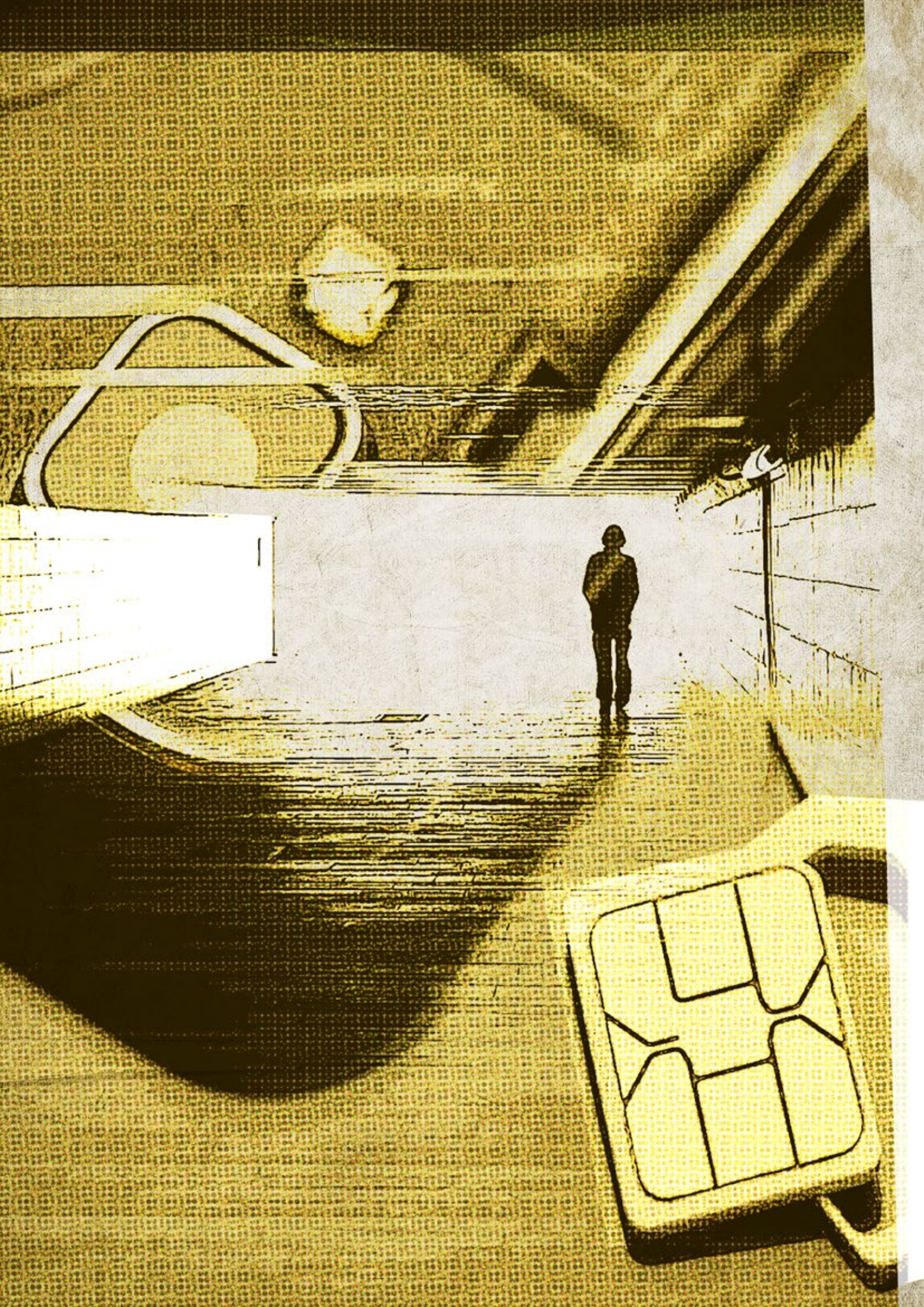
2.1 Tilsynets opgaver i forhold til CFCS

Ifølge CFCS-loven skal tilsynet efter klage eller af egen drift påse, at CFCS behandler oplysninger om fysiske personer i overensstemmelse med de nærmere bestemmelser herom i CFCS-loven samt regler udstedt i medfør heraf. Tilsynet påser, at CFCS overholder lovens regler om

- indgreb i meddelelseshemmeligheden,
- behandling af personoplysninger i centret,
- 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 oplysninger om fysiske personer i overensstemmelse med lovgivningen, og tilsynet skal således ikke påse, hvorvidt centret 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. Der er ikke givet nærmere retningslinjer for tilsynets udførelse af sin kontrol.



2.2 Tilsynets adgang til oplysninger i CFCS

Tilsynet kan hos CFCS kræve enhver oplysning og alt materiale, der er af betydning for tilsynets virksomhed, og tilsynet har til enhver tid adgang til alle lokaler, hvorfra der er adgang til de oplysninger, som behandles, eller hvor tekniske hjælpemidler anvendes. Tilsynet kan endvidere afkræve CFCS skriftlige udtalelser om faktiske og retlige forhold af betydning for tilsynets kontrolvirksomhed, ligesom tilsynet kan anmode om, at en repræsentant for centret er til stede med henblik på at redegøre for de behandlede sager.

CFCS har stillet lokaler til rådighed for tilsynet, hvorfra tilsynet på egen hånd kan foretage søgninger i centrets it-systemer.

2.3 Tilsynets reaktionsmuligheder

Tilsynet har ikke kompetence til at påbyde CFCS bestemte foranstaltninger i forhold til behandling af oplysninger. Tilsynet kan derimod afgive udtalelser over for CFCS, hvori tilsynet blandt andet kan tilkendegive sin opfattelse af, om centret overholder reglerne om behandling af personoplysninger. Hvis CFCS undtagelsesvis måtte beslutte ikke at følge en henstilling i en udtalelse fra tilsynet, skal centret underrette tilsynet herom og straks forelægge sagen for forsvarsministeren til afgørelse.

Tilsynet skal underrette forsvarsministeren om forhold, som ministeren efter tilsynets opfattelse bør have kendskab til.

Tilsynet afgiver en årlig redegørelse om sin virksomhed til forsvarsministeren. Redegørelsen, der desuden offentliggøres, giver information om karakteren af det tilsyn, der udøves med CFCS. Det fremgår således af forarbejderne til loven, at sigtet med den årlige redegørelse er at give information om karakteren af det tilsyn, der udøves vedrørende CFCS, herunder en generel beskrivelse af, hvilke forhold tilsynet måtte have valgt særligt at interessere sig for. Redegørelsen skal indeholde statistiske oplysninger om CFCS' behandling af personoplysninger, herunder oplysninger om antallet af modtagne klagesager i såvel centret 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 centret. Tilsynet vil også skulle medtage oplysninger om, i hvor mange tilfælde tilsynet har fundet, at CFCS' behandling af personoplysninger ikke har været i overensstemmelse med reglerne. Redegørelsen skal ligeledes indeholde en fuldt ud anonymiseret beskrivelse af et eller flere konkrete cyberangreb samt en statistik over antallet af tilfælde, hvor en analytiker fra CFCS 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.

Tilsynet afgav senest en årlig redegørelse om sin virksomhed til forsvarsministeren i august 2020. Redegørelsen blev offentliggjort i september 2020.

3. Retsgrundlag

1) Lov om Center for Cybersikkerhed (CFCS) (lovbekendtgørelse nr. 836 af 7. august 2019) (CFCS-loven)

2) Forsvarsministeriets cirkulære om behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste (cirkulære nr. 9741 af 21. august 2019) (CFCS-cirkulæret)

3) Anordning nr. 1658 af 20. november 2020 om ikrafttræden for Grønland af lov om Center for Cybersikkerhed

3.1 CFCS' netsikkerhedstjeneste

3.1.1 Om CFCS' netsikkerhedstjeneste, jf. CFCS-lovens § 3

Det følger af lovens § 3, at CFCS' netsikkerhedstjenestes opgave er at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder. Det er de øverste statsorganer samt statslige myndigheder, der efter anmodning kan blive tilsluttet netsikkerhedstjenesten, mens regioner og kommuner samt virksomheder, der er beskæftiget med samfundsvigtige funktioner, efter anmodning kan blive tilsluttet netsikkerhedstjenesten, såfremt CFCS konkret vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet. I særlige tilfælde kan CFCS påbyde virksomheder, der har særlig samfundsvigtig karakter, samt regioner og kommuner at blive tilsluttet netsikkerhedstjenesten.

CFCS' netsikkerhedstjeneste er betegnelsen for centret samlede aktiviteter i forbindelse med at opdage, analysere og bidrage til at imødegå sikkerhedshændelser, herunder CERT-aktiviteterne på det civile område (GovCERT), CERT-aktiviteterne på det militære område (MILCERT), sikkerhedstekniske aktiviteter (f.eks. analyse af malware) og støttefunktioner. Ved myndigheders og virksomheders tilslutning til netsikkerhedstjenesten bliver der indgået en tilslutningsaftale, der nærmere regulerer specifikke forhold i relationen mellem netsikkerhedstjenesten og den enkelte tilsluttede myndighed eller virksomhed. På Forsvarsministeriets område er det den militære it-sikkerhedsmyndighed, som pålægger myndigheder at blive tilsluttet netsikkerhedstjenesten, og på dette område indgås ikke tilslutningsaftaler.

3.2 Indgreb i meddelelseshemmeligheden og edition

3.2.1 Om indgreb i meddelelseshemmeligheden, jf. CFCS-lovens §§ 4-6 c

CFCS-lovens § 4 indebærer, at CFCS' netsikkerhedstjeneste uden retskendelse kan behandle pakkedata, trafikdata og stationære data hidrørende fra tilsluttede myndigheder og virksomheder med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet. Ved pakkedata forstås indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester, jf. lovens § 2, nr. 2, og ved trafikdata forstås data, som behandles med henblik på at transmittere pakkedata, jf. lovens § 2, nr. 3. Ved stationære data forstås data, som opbevares på servere, cloudtjenester, pc'er, lagerenheder, netværksenheder, mobile enheder og tilsvarende, jf. lovens § 2, nr. 3.

Det følger af lovens § 5, at CFCS ved en begrundet mistanke om en sikkerhedshændelse uden retskendelse kan behandle stationære data fra en myndighed eller virksomhed, som ikke er tilsluttet netsikkerhedstjenesten, når

1) myndigheden eller virksomheden har anmodet CFCS om bistand, stillet de stationære data til rådighed og givet skriftligt samtykke til behandlingen, og

2) behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

Det følger af lovens § 6, at CFCS efter aftale med en myndighed eller virksomhed, som er tilsluttet centrets netsikkerhedstjeneste, ved begrundet mistanke om en sikkerhedshændelse uden retskendelse kan blokere, omdanne eller omdirigere trafikdata, pakkedata og stationære data hidrørende fra netværk hos myndigheden eller virksomheden med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet. Ved en konstateret sikkerhedshændelse kan CFCS slette stationære data, der har forårsaget sikkerhedshændelsen.

Efter lovens § 6 a kan CFCS gennemføre sikkerhedstekniske undersøgelser med henblik på at kunne rådgive myndigheder og virksomheder om forebyggelse af sikkerhedshændelser, når en myndighed eller virksomhed har anmodet centret herom. I forbindelse med en sikkerhedsteknisk undersøgelse kan CFCS uden retskendelse behandle trafikdata, pakkedata og stationære data hos myndigheden eller virksomheden, behandle offentligt tilgængelige data om myndigheden eller virksomheden og dennes medarbejdere og iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder i myndigheden eller virksomheden.

Efter lovens § 6 b kan CFCS med henblik på at opnå viden om angrebsaktørers metoder og værktøjer opsætte fiktive angrebsmål, såfremt opsætningen vurderes at kunne bidrage væsentligt til centrets muligheder for at understøtte et højt informationssikkerhedsniveau i samfundet. Såfremt angrebsaktører benytter et fiktivt angrebsmål til at deponere data, kan CFCS uden retskendelse behandle de deponerede data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.

Det følger af lovens § 6 c, at CFCS med henblik på at forhindre, standse eller begrænse en nært forestående eller igangværende sikkerhedshændelse 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. Såfremt CFCS i forbindelse med anvendelsen af it-infrastruktur modtager data fra tredjemand, kan centret uden retskendelse behandle de modtagne data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.

3.2.2 Om edition, jf. CFCS-lovens § 7

Med henblik på at afdække sikkerhedshændelser kan der efter lovens § 7 meddeles en juridisk eller fysisk person pålæg om at forevise eller udlevere oplysninger om brugeren af en e-mailkonto, ip-adresse eller et domænenavn, såfremt oplysningerne er undergivet den pågældendes rådighed, medmindre indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre.

3.3 Behandling af personoplysninger

3.3.1 Om behandling af personoplysninger, jf. CFCS-lovens §§ 9-14

Efter lovens § 9 skal CFCS' indsamling af personoplysninger ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål. Senere behandling af personoplysninger, der alene sker i historisk, statistisk eller videnskabeligt øjemed, anses ikke for uforenelig med de formål, hvortil oplysningerne er indsamlet. Personoplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Behandling af personoplysninger må efter lovens § 10 kun finde sted, hvis

1) den pågældende person har givet sit udtrykkelige samtykke hertil,

2) behandlingen er nødvendig af hensyn til opfyldelsen af en aftale, som den pågældende person er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den pågældende persons anmodning forud for indgåelsen af en sådan aftale,

3) behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse,

4) behandlingen er nødvendig til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar,

5) behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som CFCS eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt,

6) behandlingen er nødvendig for, at CFCS eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den pågældende person ikke overstiger denne interesse, eller

7) behandlingen vedrører personoplysninger, der er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden).

Lovens § 10, nr. 1, 2, 3, 5 og 6 er med sproglige tilpasninger identiske med de tilsvarende bestemmelser i Europa-Parlamentets og Rådets forordning 2016/679 artikel 6 og skal fortolkes i overensstemmelse med disse bestemmelsers forarbejder og relevante praksis. Anvendelse af bestemmelsens nr. 4 forudsætter, at der er fare for, at statens sikkerhed eller rigets forsvar vil lide skade, hvilket eksempelvis kan være tilfældet i forbindelse med cyberangreb mod danske myndigheders informationssystemer. Hensynet til statens sikkerhed eller rigets forsvar skal fortolkes i overensstemmelse med det tilsvarende udtryk i offentlighedslovens § 31. Med bestemmelsens nr. 7 fastsættes en generel hjemmel til at behandle personoplysninger, hvis de er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden), hvorved bemærkes, at der med lovens § 15 er fastsat nærmere rammer for analyse af pakkedata, der er omfattet af lovens §§ 4, 6 og 7, mens der i lovens § 17 er fastsat regler for sletning af de pågældende data.

Der må ikke behandles personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og personoplysninger om helbredsmæssige og seksuelle forhold, jf. lovens § 11, stk. 1. Efter bestemmelsens stk. 2 gælder dette dog ikke, hvis

1) den pågældende person har givet sit udtrykkelige samtykke til en sådan behandling,

2) behandlingen vedrører personoplysninger, som er blevet offentliggjort af den pågældende person,

3) behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares,

4) behandlingen er nødvendig til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar, eller

5) behandlingen vedrører personoplysninger, der er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden).

Det følger af lovens § 12, stk. 1, at der ikke må behandles personoplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 11, stk. 1, nævnte, medmindre det er nødvendigt for varetagelsen af CFCS' opgaver. Efter bestemmelsens stk. 2 må de i stk. 1 nævnte personoplysninger ikke videregives, medmindre

1) den pågældende person har givet sit udtrykkelige samtykke til videregivelsen,

2) videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår,

3) videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe,

4) videregivelsen er nødvendig for udførelsen af en persons eller virksomheds opgaver for det offentlige, eller

5) videregivelsen omfatter personoplysninger, der er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden).

Behandling af personoplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne, jf. lovens § 13. Der skal endvidere foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende personoplysninger. Personoplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

Indsamlede personoplysninger må ikke opbevares på en måde, der giver mulighed for at identificere den pågældende person i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles, jf. lovens § 14. I den forbindelse bemærkes, at der i lovens § 17 er fastsat særlige bestemmelser om sletning af data, der er omfattet af lovens kapitel 4 (indgreb i meddelelseshemmeligheden).

3.3.2 Om sikkerhedsforanstaltninger i forbindelse med behandling af personoplysninger, jf. CFCS-lovens § 18

Ifølge lovens § 18 træffer CFCS passende tekniske og organisatoriske foranstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, og mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. For oplysninger, som er af særlig interesse for fremmede magter, skal CFCS træffe foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

3.4 Analyse og sletning af data omfattet af CFCS-lovens kapitel 4

3.4.1 Om analyse af data, jf. CFCS-lovens § 15

Det følger af lovens § 15, at CFCS kan foretage automatisk analyse af trafikdata, pakkedata og stationære data, der er omfattet af lovens kapitel 4 om indgreb i meddelelseshemmeligheden (§§ 4-6 c). CFCS må alene foretage manuelle analyser af kapitel 4 data i følgende tilfælde:

1) For at opdage, analysere og bidrage til at imødegå sikkerhedshændelser kan trafikdata analyseres i det omfang, det er nødvendigt.

2) Ved begrundet mistanke om en sikkerhedshændelse kan pakkedata og stationære data analyseres i det omfang, det er nødvendigt for at afklare forhold vedrørende hændelsen.

3) Som led i forebyggende sikkerhedstekniske undersøgelser efter § 6 a kan trafikdata, pakkedata og stationære data analyseres i det omfang, det er nødvendigt for at gennemføre undersøgelserne.

4) Som led i det løbende arbejde med at understøtte et højt informationssikkerhedsniveau på Forsvarsministeriets område, herunder ved kontrol af om kommunikation indeholder klassificeret materiale, kan trafikdata og pakkedata, der hidrører fra myndigheder på Forsvarsministeriets område, analyseres.

5) Som led i tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder kan trafikdata og pakkedata analyseres i det omfang, det er nødvendigt for at gennemføre testen. Testen skal afsluttes, så snart formålet med testen er opfyldt. Analysen må alene foretages af medarbejdere, der varetager tekniske drifts- og udviklingsopgaver for CFCS. Øvrige medarbejdere må ikke tilgå oplysninger, der hidrører fra test. Malware, der ved en tilfældighed opdages som led i en teknisk test, må dog analyseres af øvrige medarbejdere i CFCS efter nr. 2.

3.4.2 Om sletning af data, jf. CFCS-lovens § 17

Ifølge lovens § 17, stk. 1, skal data, der behandles efter lovens kapitel 4 om indgreb i meddelelseshemmeligheden (§§ 4-6 c), slettes, når formålet med behandlingen er opfyldt. Bestemmelsen skal ses i sammenhæng med lovens § 14, hvorefter indsamlede personoplysninger generelt ikke må opbevares på en måde, der giver mulighed for at identificere den pågældende person i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. Mens lovens § 14 finder anvendelse på al behandling af alle personoplysninger i CFCS, finder de særlige regler i lovens § 17 alene anvendelse på de data, der behandles på baggrund af indgreb i meddelelseshemmeligheden.

Ifølge lovforslagets bemærkninger til § 17 vil der på baggrund af bestemmelsen ske en løbende vurdering af de behandlede data med henblik på at sikre, at data, der ikke længere er relevante i forhold til netsikkerhedstjenestens formål og aktiviteter, straks slettes.

Af lovens § 17, stk. 2, fremgår, at uanset at formålet med behandlingen ikke er opfyldt, jf. stk. 1, må

1) data, der knytter sig til en sikkerhedshændelse, højst opbevares i fem år,

2) data, der ikke knytter sig til en sikkerhedshændelse, men som strammer 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, højst opbevares i tre år, og

3) data, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 13 måneder.

Bestemmelsen fastsætter øvre grænser for, hvor længe data, der ikke er slettet efter lovens § 17, stk. 1, kan opbevares, og bestemmelsen finder dermed anvendelse på data, hvor det er blevet vurderet, at der fortsat er behov for behandling i netsikkerhedstjenesten. Uanset at formålet med behandlingen således i disse tilfælde endnu ikke er opfyldt, vil data skulle slettes inden for de absolutte frister, som er fastsat i bestemmelsen. Såfremt data, der knytter sig til en sikkerhedshændelse, inden for den femårige periode igen

konstateres anvendt i forbindelse med en sikkerhedshændelse, vil en ny femårig periode begynde. Fristerne i stk. 2 regnes fra tidspunktet for CFCS' registrering af de pågældende data, jf. stk. 3.

Lovens § 17, stk. 1 og 2, finder ikke anvendelse på data, der er videregivet til andre end den myndighed eller virksomhed, som data hidrører fra, jf. lovens § 17, stk. 5.

Personoplysninger i data, som CFCS får adgang til som led i forebyggende sikkerhedstekniske undersøgelser efter § 6 a, skal ifølge lovens § 17, stk. 6, slettes eller anonymiseres, når den sikkerhedstekniske undersøgelse er afsluttet. Konstaterer CFCS, at der i de pågældende data er indeholdt følsomme personoplysninger, skal disse slettes uden unødigt ophold.

I helt særlige tilfælde kan de ovenfor beskrevne slettefrister kortvarigt suspenderes, hvis væsentlige hensyn til varetagelsen af CFCS' opgaver gør det nødvendigt, jf. § 17, stk. 7. CFCS skal straks underrette tilsynet om suspensionen og baggrunden herfor.

Ifølge lovens § 17 a finder bestemmelserne i lovens § 17 ikke 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 i stedet hurtigst muligt.

3.5 Videregivelse og udveksling af oplysninger omfattet af CFCS-lovens kapitel 4

3.5.1 Om videregivelse, jf. CFCS-lovens § 16

Efter lovens § 16 kan CFCS i en række nærmere definerede tilfælde videregive data, der er omfattet af lovens kapitel 4 om indgreb i meddelelseshemmeligheden (§§ 4-6 c). Kravene til videregivelsen afhænger både af, hvem der er tiltænkt som modtager af data, samt af hvilken type af data der videregives.

CFCS kan ifølge lovens § 16, stk. 1, videregive trafikdata, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.

2) Den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse, og hvis det er nødvendigt for udførelsen af CFCS' opgaver.

3) Danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt myndigheder og virksomheder i øvrigt i forbindelse med CFCS' udsendelse af sikkerhedsvarslinger, såfremt der er begrundet mistanke om en sikkerhedshændelse, og såfremt det er nødvendigt for udførelsen af centrets opgaver.

CFCS kan ifølge lovens § 16, stk. 2, videregive pakkedata, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.

2) Den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse.

CFCS kan ifølge lovens § 16, stk. 3, videregive stationære data, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.

2) Den myndighed, virksomhed eller borger, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse.

3) Andre netsikkerhedstjenester, såfremt CFCS har modtaget de pågældende data i medfør af § 6 b eller § 6 c.

CFCS kan ifølge lovens § 16, stk. 4, videregive malware, der er omfattet af kapitel 4, til:

1) Politiet.

2) Den myndighed eller virksomhed, hvorfra de pågældende data hidrører.

3) Danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt myndigheder og virksomheder i øvrigt i forbindelse med CFCS' udsendelse af sikkerhedsvarslinger.

CFCS kan ifølge lovens § 16, stk. 5, alene videregive data, som stammer fra tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder i følgende tilfælde:

1) Malware, der er opdaget ved en tilfældighed, kan videregives til politiet, til den myndighed eller virksomhed, hvorfra de pågældende data hidrører, til danske myndigheder, til udbydere af offentlige elektroniske kommunikationsnet og -tjenester og til andre netsikkerhedstjenester samt til myndigheder og virksomheder i øvrigt i forbindelse med CFCS' udsendelse af sikkerhedsvarslinger.

2) Trafikdata kan videregives til den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører.

CFCS må ifølge lovens § 16, stk. 6, i forbindelse med forebyggende sikkerhedstekniske undersøgelser efter § 6 a alene videregive oplysninger vedrørende myndighedens eller virksomhedens medarbejdere, hvis det sker i anonymiseret form.

3.5.2 Om udveksling af data med FE, jf. CFCS-cirkulærets § 2

I de almindelige bemærkninger til CFCS-loven anføres om den interne udveksling af data i FE, at denne i overensstemmelse med almindelige forvaltningsretlige principper ikke er lovreguleret.

Dette indebærer, at der som udgangspunkt er fri adgang til at udveksle data internt i FE, herunder mellem CFCS og den øvrige del af efterretningstjenesten, hvis dette er nødvendigt for at løse myndighedens opgaver, og der i øvrigt er tale om et sagligt formål. Det sikrer, at alle de relevante ressourcer i FE hurtigt og effektivt kan indsættes ved den meget store andel af cyberangreb mod Danmark, som hidrører fra udlandet,

og hvor FE som udenrigsefterretningstjeneste kan bidrage med en række værdifulde oplysninger.

I overensstemmelse hermed er det i § 2, stk. 1, i CFCS-cirkulæret fastsat, at CFCS kun må udveksle data, der er omfattet af lovens kapitel 4, med den øvrige del af FE, når

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.

Efter bestemmelsens stk. 2 finder stk. 1, nr. 3, ikke anvendelse på data, der hidrører fra myndigheder på Forsvarsministeriets område.

Det følger af bestemmelsens stk. 3, at enhver udveksling af data skal registreres af CFCS.

Årsredegørelse 2020
Center for Cybersikkerhed
Udgivet af Tilsynet med Efterretningstjenesterne, august 2021

Layout + illustrationer: Eckardt ApS
Portrætfotos: Lars Engelgaar / Sophie Kalckar

Publikationen kan downloades fra tilsynets hjemmeside på www.tet.dk

Medlemmer af Tilsynet med Efterretningstjenesterne

Landsdommer Michael Kistrup, Østre Landsret (formand)
Juridisk chef Pernille Christensen, Kommunernes Landsforening
Professor Henrik Udsen, Københavns Universitet
Professor Rebecca Adler-Nissen, Københavns Universitet
Koncerndirektør David Hellemann, Nykredit

Tilsynet med Efterretningstjenesterne
Borgergade 28, 1. sal, 1300 København K
www.tet.dk