CENTER FOR CYBERSIKKERHED

Redegørelse om data i sensornetværket

Dato: 19. juli 2023

Sagsnr.: 2023/002920
Dok. nr.: 28230

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

Center for Cybersikkerhed (CFCS) under Forsvarets Efterretningstjeneste (FE) underrettede på et møde den 16. juni 2023 Forsvarsministeriet om, at CFCS i forbindelse med arbejdet om at belyse CFCS' muligheder for at genskabe slettede SMS-beskeder mv. er blevet opmærksom på, at CFCS i forbindelse med implementering af en ændring af CFCS-loven i 2019 har begået en beklagelig fejl.

Fejlen består i, at CFCS for en myndigheds vedkommende har anvendt en forkert slettefrist i forhold til data fra denne myndighed i sensornetværket.

Omvendt har CFCS for visse andre myndigheders vedkommende ikke udnyttet den forlængede slettefrist, som den pågældende lovændring medførte.

Forsvarsministeren bad på det pågældende møde om, at CFCS skulle udarbejde en samlet redegørelse vedrørende forløbet.

Der redegøres nærmere for forløbet herunder. Pkt. 1 handler om opbygningen af sensornetværket, i pkt. 2 redegøres der for de relevante regler i CFCS-loven, pkt. 3 handler om de omfattede sikkerhedsmyndigheder (og fejlen i den forbindelse), i pkt. 4 omtales CFCS' egenkontrol og det eksterne tilsyn, og CFCS' læringspunkter er beskrevet i pkt. 5.

1. Sensornetværket

1.1. CFCS har bl.a. til opgave at drive et sensornetværk med henblik på at varsle myndigheder og visse virksomheder, der beskæftiger sig med f.eks. kritisk infrastruktur, om cyberangreb. Formålet med sensornetværket er at detektere ondartet trafik og understøtte CFCS' opgaveløsning og ikke i anden forbindelse at logge aktiviteter på de monitorerede netværk.

Sensornetværket virker ved, at en række sensorer via automatiserede processer monitorerer datatrafikken ind og ud af de pågældende myndigheders og virksomheders netværk. Der holdes løbende øje med, om malware eller anden mistænkelig data indgår i trafikken, og hvis dette er tilfældet, går en alarm hos CFCS. CFCS kan herefter tilgå de pågældende data på sensoren og undersøge den mistænkelige trafik nærmere.

Sensornetværket monitorerer ikke data, som sendes via mobilnetværk fra f.eks. en telefon. Hvis telefonen imidlertid har været koblet på et wifi-netværk, der er tilsluttet sensornetværket, og der har været anvendt en internetbaseret chatfunktion som f.eks. iMessage, vil data knyttet hertil blive lagret i sensornetværket.

Data fra sensornetværket opbevares på de sensorer, der monitorer datatrafikken, og i et vist omfang også på en særskilt dataanalyseplatform (DAP), jf. herom nedenfor.

1.2. På sensorerne opbevares såkaldt pakkedata og trafikdata.

Pakkedata er indholdsdata, f.eks. indholdet af en e-mail. Trafikdata er metadata, som f.eks. er oplysninger som IP-adresser og tidspunktet for eventuel trafik til og fra disse adresser.

En sensor kan godt dække mere end en myndighed, og der opbevares under alle omstændigheder betydelige datamængder på sensorerne. Data fra én myndighed kan desuden være fordelt over flere sensorer. Lagringskapaciteten på de enkelte sensorer bliver derfor reelt den begrænsende faktor i forhold til, hvor længe data opbevares. Når 95 pct. af sensorens lagringskapacitet er nået, bliver ældste data således overskrevet af ny data og dermed slettet, selv om den absolutte slettefrist endnu ikke måtte være nået.

Til illustration kan oplyses, at ældste data på de sensorer, som bl.a. dækker Statsministeriet, pr. 28. juni 2023 er fra den 3. juni 2022. Den tilsvarende dato for Justitsministeriet er den 7. november 2022.

Slettet data fra sensorerne kan ikke genskabes.

1.3. Ud over i sensornetværket opbevares visse data som nævnt også på DAP, som CFCS anvender til at foretage tværgående analyser af mønstre i datatrafik.

Mens sensorerne anvendes til at opbevare pakkedata og trafikdata, benyttes DAP alene til at opbevare trafikdata, dvs. metadata med oplysninger om den måde, som kommunikationen er sket på. Denne data anvendes til at analysere datastrømmene, og kun hvis der er mistanke om en IT-sikkerhedshændelse (cyberangreb mv.), tilgår CFCS pakkedata på sensoren, som så i relevant omfang kan flyttes midlertidigt via DAP og herefter til særlige PC'er med henblik på nærmere analyse. Analytikerne kan ikke se pakkedata i DAP, og det slettes på de særlige PC'er efter endt analyse. Hvis CFCS konstaterer, at der er tale om en IT-sikkerhedshændelse, vil CFCS varsle den tilsluttede myndighed eller virksomhed, der er ramt.

Udgangspunktet er, at data på DAP slettes automatisk, når slettefristerne i CFCS-loven på henholdsvis 13 måneder og 3 år indtræder, mens der gælder særlige slettefrister for data, der knytter sig til konkrete sikkerhedshændelser.

Ligesom for data på sensorerne gælder det for slettede data fra DAP, at disse ikke kan genskabes.

2. CFCS-loven

2.1. Det fremgår af slettefristerne i CFCS-loven, at data, som stammer fra myndigheder, der i særlig grad beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold (sikkerhedsmyndigheder), og virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold, som udgangspunkt kan opbevares i højst 3 år.

Data fra andre myndigheder mv. end sikkerhedsmyndighederne må som udgangspunkt højst opbevares i 13 måneder.

Slettefristen på 3 år blev indført ved en lovændring pr. 1. juli 2019, jf. nærmere herunder. Inden da var slettefristen 13 måneder for alle.

Der gælder særlige slettefrister for data, der knytter sig til konkrete sikkerhedshændelser.

Det bemærkes, at slettefristerne i CFCS-loven regulerer, hvor længe CFCS må opbevare data, og ikke hvor længe data skal opbevares.

2.2. Forlængelsen af slettefristen for sikkerhedsmyndigheder mv. blev indført ved lov nr. 555 af 7. maj 2019, som trådte i

kraft den 1. juli 2019. Begrundelsen for lovændringen var et ønske fra CFCS om at kunne beholde data i længere tid for visse særligt udsatte myndigheder, virksomheder og organisationer for derved at forbedre mulighederne for at detektere avancerede cyberangreb.

Hvilke myndigheder, virksomheder og organisationer, som denne den forlængede slettefrist gælder for, er uddybet i lovforslagets bemærkninger[1], hvor der bl.a. er anført følgende:

> *"Der er tale om en ny bestemmelse, som etablerer en særlig ordning for data, der hidrører fra en mindre gruppe af myndigheder, virksomheder og organisationer. Det vil eksempelvis dreje sig om udvalgte ministerier og om organisationer, herunder forskningsinstitutioner, der bidrager til den danske udenrigspolitik eller varetager opgaver i den forbindelse, og virksomheder, der leverer materiel og ydelser til Forsvaret.*
>
> *Der er tale om særligt sensitive data for staten, og det er data, der i særlig grad kan være af interesse for statsstøttede aktører, der spionerer mod Danmark. Den længere slettefrist indebærer en forbedring af mulighederne for at undersøge længerevarende eller ældre sikkerhedshændelser. Der kan således særligt i forbindelse med opdagelse af avancerede cyberangreb fra statsstøttede aktører opstå behov for at tilgå ældre data med henblik på at afdække angrebets iværksættelse og varighed, herunder eventuelt identificere andre ofre for angrebet.*
>
> *Det vil fremgå af tilslutningsaftalen med centerets netsikkerhedstjeneste – eller i tilfælde af påbud om tilslutning, af afgørelsen herom – hvorvidt centeret anser den pågældende myndighed eller virksomhed for omfattet af bestemmelsen."*

CFCS betragter bl.a. sikkerhedsministerierne (Statsministeriet, Forsvarsministeriet, Udenrigsministeriet og Justitsministeriet), PET og Forsvaret som sådanne sikkerhedsmyndigheder.

Det bemærkes, at TET fører tilsyn med, at CFCS overholder sletteglerne i CFCS-loven. Således gennemførte TET i 2022 en stikprøvekontrol af en sensor med data fra en række enheder i Forsvaret, herunder Forsvarskommandoen, og havde i den forbindelse ingen bemærkninger.

[1] De specielle bemærkninger til forslaget til § 17, stk. 2, nr. 2, i lovforslag nr. L 215 af 27. marts 2019

3. Omfattede sikkerhedsmyndigheder

3.1. Betingelsen for at anvende slettefristen på 3 år er for det første, at myndigheden mv. kan anses for omfattet af den pågældende bestemmelse i CFCS-loven, og at dette for det andet også fremgår af den tilslutningsaftale, som CFCS indgår med myndigheden mv.[2] Da CFCS er IT-sikkerhedsmyndighed for Forsvarsministeriets område, er der dog ikke noget krav om tilslutningsaftaler for myndigheder på dette område.

En samlet liste over myndigheder, virksomheder og organisationer, som CFCS har indgået sådanne aftaler med, er klassificeret. Men det kan oplyses, at både Statsministeriet, Udenrigsministeriet og Justitsministeriet er blandt disse myndigheder.

3.2. CFCS er i forbindelse med arbejdet om at belyse centrets muligheder for at genskabe slettede SMS-beskeder mv. blevet opmærksom på, at CFCS i forbindelse med implementering af lovændringen i 2019 har begået en beklagelig fejl.

Fejlen består i, at CFCS uberettiget har implementeret den 3-årige slettefrist i forhold til data fra Danmarks Meteorologiske Institut (DMI). Der blev således den 6. januar 2021 indgået en ændret tilslutningsaftale med DMI med en slettefrist på 3 år. Fristen blev manuelt forlænget fra 13 måneder til 3 år i DAP den 30. juni 2021.

Efterfølgende blev CFCS opmærksom på, at DMI ikke kan anses for omfattet af kredsen af myndigheder mv., som den 3-årige slettefrist gælder for.

På den baggrund blev tilslutningsaftalen den 8. december 2021 ændret tilbage til en slettefrist på 13 måneder, men ved en beklagelig fejl blev slettefristen ikke manuelt ændret igen i DAP.

En forlængelse af slettefristen til 3 år forudsætter som nævnt ovenfor, at dette også er aftalt med DMI og således fremgår af tilslutningsaftalen. CFCS har dermed opbevaret data fra DMI en længere periode, end hvad der er berettiget efter CFCS-loven.

Det kan oplyses, at CFCS pr. 17. juni 2023 opbevarede trafikdata fra DMI på DAP, som var knap 3 år gammel (den ældste pakke- og trafikdata fra DMI på sensorerne var på grund af kapacitetsbegrænsningen knap 4 måneder gammel).

---

[2] Jf. også § 1, stk. 3, i bekendtgørelse nr. 896 af 21. august 2019 om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste

CFCS har den 17. juni 2023 underrettet DMI og TET om fejlen og har samme dag rettet slettefristen tilbage til 13 måneder og slettet de data, som er for gamle.

CFCS har gennemgået de øvrige myndigheder mv., hvor slettefristen er sat til 3 år i DAP, og har ikke konstateret yderligere fejl i den forbindelse. Alle de pågældende myndigheder mv. må således anses for omfattet af bestemmelsen i CFCS-loven om forlænget slettefrist i overensstemmelse med de respektive tilslutningsaftaler.

3.3. CFCS er i samme forbindelse blevet opmærksom på, at CFCS i forhold til visse myndigheder ikke har fået fulgt tilfredsstillende op på de forbedrede muligheder for at opbevaredata i længere tid, som lovændringen i 2019 medførte.

Det er således CFCS' opfattelse, at den forlængede slettefrist på 3 år i hvert fald burde have været anvendt for de myndigheder, som direkte beskæftiger sig med regeringens sikkerhedssager. Dette er også sket for en række af disse myndigheder, herunder Udenrigsministeriet og PET, men ikke i forhold til f.eks. Statsministeriet og Justitsministeriet. For disse to myndigheders vedkommende er der således hhv. 10. marts 2020 og 21. januar 2021 ændret i tilslutningsaftalerne, så den forlængede slettefrist fremgår heraf, men ændringen er ikke blevet implementeret i DAP.

Dette har haft betydning for, hvor længe CFCS har haft trafikdata fra de to myndigheder, idet disse data er blevet slettet automatisk fra DAP efter 13 måneder. Det har derimod ikke haft betydning for, hvor længe CFCS har haft pakkedata, idet lagringskapaciteten på de enkelte sensorer som nævnt ovenfor reelt har været den begrænsende faktor i forhold til, hvor længe data har været opbevaret.

CFCS har den 17. juni 2023 ændret slettefristen fra 13 måneder til 3 år for Statsministeriet og Justitsministeriet.

Det bemærkes i øvrigt, at CFCS den 19. juni 2023 ligeledes ændrede slettefristen fra 13 måneder til 3 år for Forsvarsministeriet, således er den forlængede slettefrist nu implementeret korrekt for alle sikkerhedsministerierne.

CFCS vil desuden hurtigst muligt følge op på at få ændret tilslutningsaftaler og implementeret den forlængede slettefrist for andre

myndigheder, virksomheder og organisationer, som efter CFCS' opfattelse bør være omfattet heraf.

CFCS har ikke indikationer på, at den utilstrækkelige implementering af den forlængede slettefrist har haft betydning for detektionen af konkrete cyberangreb mv. CFCS kan imidlertid i sagens natur ikke udelukke, at det kunne have været tilfældet.

4. Egenkontrol og tilsyn

4.1. CFCS fører en omfattende egenkontrol for at sikre overholdelse af CFCS-lovens regler. Der er i den forbindelse en særlig opmærksomhed på data i sensornetværket.

Egenkontrolplanen udarbejdes på baggrund af et risikostyringssystem på tværs af FE. De juridiske risici identificeres og vurderes løbende og prioriteres med hensyn til kontroltryk og audits. I forhold til sensordata er fokus navnlig på, at data ikke opbevares længere, end slettefristerne tillader. Egenkontrolplanen deles med TET.

Det kan i den forbindelse oplyses, at CFCS i henhold til egenkontrolplanerne i 2023 og årene før har udført en række kontroller med hensyn til sensordata både på sensorerne og i DAP. Kontrollerne har primært bestået i stikprøvevis gennemgang af sensorer, hvor tidspunktet for indsamling af data har været kontrolleret og i tilsvarende kontroller i DAP.

Fejlen vedr. DMI blev ikke konstateret gennem egenkontrollerne, men kunne muligvis være blevet opdaget tidligere, hvis der ved stikprøven havde været udtaget data fra DMI.

I henhold til den juridiske risikostyring og den aktuelle egenkontrolplan er rettidig sletning og procedurerne herfor et fortsat fokusområde i 2023.

4.2. TET fører bl.a. tilsyn med, at CFCS overholder sletteregleme i CFCS-loven og fører hvert år stikprøvevis kontrol med slettefristerne i DAP og/eller sensorer.

TET udførte senest i 2022 en sådan kontrol og kontrollerede bl.a. om slettefristerne i loven overholdes på visse data i sensornetværket, hvilket TET ikke havde bemærkninger til.

TET-kontrollerne har i lighed med CFCS' egenkontrol ikke konstateret fejlen med DMI.

5. Læringspunkter

Som det fremgår ovenfor, har CFCS i forbindelse med implementering af en ændring af CFCS-loven i 2019 begået en beklagelig fejl. Fejlen består i, at CFCS for DMI har anvendt en for lang slettefrist i forhold til data herfra i sensornetværket.

Som det ligeledes er beskrevet ovenfor, fører CFCS en omfattende egenkontrol på området med en særlig fokus på, at sensordata slettes senest, når slettefristerne i CFCS-loven indtræder. Dette fokus har imidlertid navnlig rettet sig mod efterfølgende datahåndtering (back end) og mindre mod sikring af korrekt registrering af data i henhold til de indgåede tilslutningsaftaler (front end).

Den konstaterede fejl skyldtes manglende klare procedurer og i det konkrete tilfælde opmærksomhed på, hvilke lovkrav der skulle være opfyldt, før slettefristen kunne forlænges i det konkrete tilfælde. Fejlen er nu rettet, og data, som ikke længere må opbevares, er nu slettet.

Som nævnt ovenfor har CFCS herudover i forhold til visse myndigheder ikke fulgt tilfredsstillende op på de forbedrede muligheder for at beholde opbevare data i længere tid, som lovændringen i 2019 medførte.

CFCS vil på baggrund af ovenstående nu styrke governance på området, herunder sikre, at der udarbejdes fyldestgørende procesbeskrivelser for tilslutning til sensornetværket, og at de indgåede aftaler implementeres korrekt.

Desuden vil CFCS styrke det ledelsesmæssige fokus på at få rettet og modvirke den pågældende type af fejl, ligesom egenkontrollen i højere grad også vil rette sig mod front end.