Retsudvalget 2022-23 (2. samling)
REU Alm.del - Bilag 215
Offentligt

FORSVARSMINISTEREN

Folketingets Retsudvalg
Folketingets Forsvarsudvalg
Folketingets Granskningsudvalg
Christiansborg

Orientering om mulighederne for at tilgå beskeder fra Center for Cybersikkerheds sensornetværk samt om konstateret opsætningsfejl hos centeret

Dato: 19. juni 2023

Enhed: CCD
Sagsnr.: 2023/005054
Dok.nr.: 567648
Bilag: Ingen

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Tlf.: +45 7281 0000
Fax: +45 7281 0300
E-mail: fmn@fmn.dk
www.fmn.dk

EAN: 5798000201200
CVR: 25 77 56 35

1. Der har politisk været rejst spørgsmål om, hvorvidt Folketinget blev informeret om, at Center for Cybersikkerhed ikke havde lovhjemmel til at tilgå beskeder, der måtte være lagret i centerets sensornetværk.

Jeg kan i den forbindelse henvise til følgende, der fremgår af den taleseddel, som den daværende forsvarsminister anvendte under det lukkede samråd C i Folketingets Granskningsudvalg den 7. december 2021:

> "CFCS-loven giver dermed ikke hjemmel til at se efter indholdsdata i den konkrete sag. Det må der ikke herske tvivl om.
>
> CFCS har til opgave at finde og bremse malware. For at kunne varsle om angreb på landets myndigheder og landets virksomheder i den kritiske infrastruktur.
>
> Vi skal have tiltro til, at CFCS kan behandle sensitive og forretningskritiske data samt persondata i fuld diskretion. Når det er sagt, så har vi faktisk rakt ud til CFCS om spørgsmålet for at kunne komme til bunds i denne sag. Og budskabet fra CFCS er meget klart. Lad mig citere fra min besvarelse af Retsudvalgets spørgsmål nr. 307, som blev oversendt i går:
>
> *'CFCS' monitorering [af statsministeriets netværk] omfatter ikke SMS'er, der sendes gennem mobiloperatørernes mobilnetværk. Beskeder, der sendes via internettet – f.eks. via iMessage – ved anvendelse af et wifi-netværk, som CFCS monitorerer, vil potentielt blive kunne opfanget af CFCS' sensor.*
>
> *Det er CFCS' forventning, at der blandt andet pga. kryptering af evt. relevant trafik ikke kan findes materiale i form af iMessages af relevans for Granskningskommissionen.'"*

Den daværende forsvarsministers taleseddel blev endvidere oversendt til Folketingets Granskningsudvalg den 13. december 2021 som svar på spørgsmål nr. 8 (Alm. del). Folketinget er således både mundtligt og skriftligt blevet udtrykkeligt orienteret om hjemmelsspørgsmålet.

2. Der har herudover været rejst spørgsmål om, hvorvidt det på nuværende tidspunkt ville være muligt at tilgå beskeder, der stadig er lagret i Center for Cybersikkerheds sensornetværk, såfremt der blev skabt den fornødne lovhjemmel til at tilgå eventuelle beskeder, som kunne have været af relevans for Minkkommissionens undersøgelser.

Forsvarets Efterretningstjeneste, hvorunder Center for Cybersikkerhed hører, har oplyst følgende:

> "Center for Cybersikkerhed (CFCS) har bl.a. til opgave at drive et sensornetværk, som beskytter myndigheder og visse virksomheder, der beskæftiger sig med f.eks. kritisk infrastruktur, mod cyberangreb. Formålet med sensornetværket er at detektere ondsindet trafik, og ikke at logge aktiviteterne 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 derimod har været koblet på et wifi-netværk, der er tilsluttet sensornetværket, og der har været anvendt en databaseret chatfunktion som f.eks. iMessage, vil data knyttet hertil blive lagret i sensornetværket.
>
> Såkaldte pakkedata og trafikdata fra sensornetværket - og herunder eventuelle data hidrørende fra iMessages - opbevares på de sensorer, der monitorerer datatrafikken. Trafikdata opbevares desuden på en særskilt dataanalyseplatform, og kun ved konkrete IT-sikkerhedshændelser hentes de berørte pakkedata til analyseplatformen og herfra videre til særlige analyseværktøjer. Pakkedata er indholdsdata, f.eks. om indholdet af en e-mail eller en iMessage. Trafikdata er f.eks. oplysninger om de tilsluttedes enheders IP-adresser og tidspunktet for eventuel trafik til og fra disse adresser.
>
> En sensor kan godt dække mere end én myndighed, og der opbevares betydelige datamængder på sensorerne. 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 overskrevet af ny data og dermed slettet, selv om slettefristen endnu ikke måtte være nået. Således er ældste data på de sensorer, som bl.a. dækker Statsministeriet, pr. 16. juni 2023 fra den 22. maj 2022. Den tilsvarende dato for Justitsministeriet er den 25. oktober 2022."

Forsvarets Efterretningstjeneste har endvidere oplyst, at allerede slettede data fra sensorerne ikke kan gendannes. Forsvarets Efterretningstjeneste konkluderer på den baggrund, at Center for Cybersikkerhed ikke er i besiddelse af sensordata – hverken trafikdata eller pakkedata – fra den periode, som Minkkommissionen havde til opgave at undersøge.

Herudover har Forsvarets Efterretningstjeneste tidligere oplyst, at selv hvis de pågældende data fortsat var tilgængelige, så ville krypteringen gøre, at Center for Cybersikkerhed ikke ville forvente at kunne se indholdet af iMessages af relevans for Minkkommissionen. På et møde i Forsvarsministeriet den 19. juni 2023 har den fungerende chef for Forsvarets Efterretningstjeneste og chefen for Center for Cybersikkerhed oplyst, at Forsvarets Efterretningstjeneste – efter at have undersøgt spørgsmålet yderligere – nu vurderer, at det ikke ville være muligt for Center for Cybersikkerhed at se indholdet af iMessages af relevans for Minkkommissionen.

3. Forsvarets Efterretningstjeneste har endvidere oplyst, at Center for Cybersikkerhed i forbindelse med kortlægningen af, hvilke sensordata fra Statsministeriet og Justitsministeriet, der aktuelt er lagret, er blevet opmærksom på, at centeret uberettiget har implementeret en tre-årig slettefrist i forhold til data fra Danmarks Meteorologiske institut (DMI).

Forsvarets Efterretningstjeneste har oplyst, at fejlen er opstået i forbindelse med implementeringen af en lovændring i 2019.

Lovændringen indførte differentierede frister for, hvornår Center for Cybersikkerhed *senest* skal slette data fra centerets sensornetværk. Med lovændringen er udgangspunktet, at data kan opbevares i op til 13 måneder, men for 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, kan data efter aftale med den pågældende myndighed eller virksomhed opbevares i op til tre år. Der er ikke tale om, at Center for Cybersikkerhed er forpligtet til at opbevare data i disse perioder, men alene, at centeret *senest* skal slette data efter disse perioders udløb.

Forsvarets Efterretningstjeneste har om fejlen oplyst følgende:

> ”CFCS er blevet opmærksom på, at centeret i forbindelse med implementeringen af ændringen i CFCS-loven i 2019 har begået en beklagelig fejl. Fejlen består i, at CFCS for én myndigheds vedkommende har anvendt en forkert slettefrist. Således har CFCS uberettiget implementeret den 3-årige slettefrist i forhold til data fra Danmarks Meteorologiske institut (DMI).

> Omvendt har CFCS for andre myndigheders vedkommende ikke udnyttet den forlængede slettefrist, som lovændringen medførte. Således er muligheden for at opbevare data i op til 3 år ikke blevet implementeret i forhold til bl.a. Statsministeriet, Justitsministeriet og Forsvarsministeriet. Dette har haft betydning for, hvor længe CFCS har haft trafikdata fra disse myndigheder, da data herfra er blevet slettet fra dataanalyseplatformen efter 13 måneder. Det har derimod ikke haft betydning for, hvor længe CFCS har haft pakkedata, idet lagringskapaciteten på de enkelte sensorer som nævnt reelt har været den begrænsende faktor i forhold hertil.
>
> Statsministeriet indgik den 10. marts 2020 aftale med CFCS om at ændre slettefristen til 3 år, og for Justitsministeriets vedkommende skete dette den 21. januar 2021. Som følge af fejl i sagsbehandlingen i CFCS blev de ændrede slettefrister imidlertid ikke implementeret i sensornetværket. Trafikdata fra disse ministerier er derfor fortsat blevet slettet i dataanalyseplatformen efter 13 måneder, selv om CFCS efter lovændringen havde mulighed for at gemme data i op til 3 år.
>
> De pågældende trafikdata ville ikke kunne give mulighed for at se hverken indhold, afsender eller modtager af en besked sendt via iMessage."

Jeg finder det naturligvis kritisabelt, at en sådan fejl kan opstå, og dette har jeg meddelt chefen for Forsvarets Efterretningstjeneste.

Jeg har noteret mig, at Center for Cybersikkerhed straks vil bringe fejlen til ophør, og at centeret vil sikre, at data, der er blevet opbevaret i strid med lovgivningen, straks slettes. Endvidere har jeg noteret mig, at Forsvarets Efterretningstjeneste straks har orienteret Tilsynet med Efterretningstjenesterne om fejlen, ligesom Forsvarsministeriet også retter henvendelse til Tilsynet. Herudover har Forsvarets Efterretningstjeneste oplyst, at tjenesten har sikret, at den berørte myndighed – DMI – straks orienteres om fejlen.

Jeg har anmodet Forsvarets Efterretningstjeneste om at udarbejde en samlet redegørelse vedrørende forløbet i forbindelse med denne fejl.

Med venlig hilsen

Troels Lund Poulsen