FORSVARETS EFTERRETNINGSTJENESTE

Til Forsvarsministeriet
Center for Cyber og Digitalisering

Att. Niels Poul Petersen, Nicklas Schreiber Echsner-Rasmussen, Lea Møberg og Christine E. Christensen

Kopi til:
Center for Sikkerhed og Operationer
Peter Kim Laustsen og Pelle Holager

Bidrag til besvarelse af REU-spørgsmål nr. 274

Dato: 26. november 2021

Sagsnr.: 2021/003688

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 66
E-mail: FE-MYN@fe-ddis.dk
www.fe-ddis.dk

Forsvarsministeriet har den 24. november 2021 anmodet Forsvarets Efterretningstjeneste (FE) om bidrag til Justitsministeriets besvarelse af følgende spørgsmål nr. 274 (alm. del) fra Folketingets Retsudvalg:

"Vil ministeren redegøre for, om det er undersøgt med CFCS, om CFCS er i besiddelse af data, der potentielt kunne indeholde de slettede SMS'er?"

FE kan oplyse følgende:

"FE har forstået spørgsmålet således, at det vedrører SMS-beskeder sendt til og fra visse medarbejdere i Statsministeriet og Justitsministeriet med relevans for den igangværende granskningskommission om sagen om aflivning af mink.

FE's Center for Cybersikkerhed (CFCS) kan oplyse, at CFCS ikke er blevet anmodet om at undersøge, om CFCS måtte være i besiddelse af data, der potentielt kunne indeholde alle eller visse dele af den relevante SMS-korrespondance.

Det kan i øvrigt oplyses, at CFCS ikke har hjemmel til at se efter indholdsdata, som måtte ligge i CFCS' sensornetværk, for at undersøge, om der i sensornetværket eventuelt er oplysninger af relevans for granskningskommissionens opgave."

Med venlig hilsen

Forsvarets Efterretningstjeneste

FORSVARETS
EFTERRETNINGSTJENESTE

Til Forsvarsministeriet,
Center for Cyber og Digitalisering,
Att.: Christine E. Christensen, Lea Møberg Kristensen og
Niels Poul Petersen
Kopi til: Center for Sikkerhed og Operationer,
Att.: Peter Kim Laustsen og Kristoffer Breindal

Bidrag til besvarelse af REU spørgsmål nr. 307

Dato: 2. december 2021

Sagsnr.: 2021/003754
Dok. nr.: 258942

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 66
E-mail: FE-MYN@fe-ddis.dk
www.fe-ddis.dk

Forsvarsministeriet har den 1. december 2021 anmodet Forsvarets Efterretningstjeneste (FE) om bidrag til besvarelse af spørgsmål nr. 307 (alm. del) fra Folketingets Retsudvalg:

"Vil ministeren redegøre for, om Center for Cybersikkerhed monitorerer Statsministeriets netværk samt intern og ekstern trafik? I bekræftende fald bedes ministeren redegøre for, hvor længe dette materiale gemmes, samt om det er undersøgt, om der i denne monitorering foreligger en kopi af de slettede SMS'er fra minksagen?"

Forsvarets Efterretningstjeneste kan oplyse følgende:

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) monitorerer Statsministeriets netværk, herunder den interne og eksterne trafik, gennem en opstillet sensor.

Data hidrørende fra monitoreringen af Statsministeriets netværk gemmes op til slettefristerne i CFCS-loven, dog for visse typer data i kortere tid grundet kapacitetshensyn vedrørende lagring. Den eksakte information om, hvilke data fra tilsluttede myndigheder og virksomheder der gemmes hvor længe, vil oftest være klassificeret.

CFCS kan i henhold til slettefristerne i CFCS-loven opbevare data, der knytter sig til en sikkerhedshændelse, i op til 5 år. Data, der ikke knytter sig til en sikkerhedshændelse, men som stammer fra myndigheder, der i særlig grad beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold, samt virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold, kan opbevares i op til 3 år. Øvrige data, der ikke knytter sig til en sikkerhedshændelse, må højst opbevares i 13 måneder.

CFCS har ikke undersøgt, om der i sensornetværket findes data, der potentielt kan indeholde alle eller visse dele af den relevante sms-korrepondance. I praksis ville dette kunne ske, hvis beskeder sendes via internettet – f.eks. via iMessage – ved anvendelse af et wifi-netværk. CFCS har imidlertid alene hjemmel til at tilgå oplysningerne i sensornetværket i helt særlige tilfælde, jf. herved paragraf 15 i lov om Center for Cybersikkerhed. CFCS har på denne baggrund ikke fundet at have

det fornødne retlige grundlag for at undersøge, om der i sensornetværket findes data vedrørende de slettede sms'er fra minksagen.

Med venlig hilsen

Forsvarets Efterretningstjeneste

FORSVARETS
EFTERRETNINGSTJENESTE

Til Forsvarsministeriet,
Center for Cyber og Digitalisering,
Att.: Christine E. Christensen, Lea Møberg Kristensen og
Niels Poul Petersen
Kopi til: Center for Sikkerhed og Operationer,
Att.: Peter Kim Laustsen og Kristoffer Breindal

Forsvarsministeriet har den 3. december 2021 anmodet FE's Center for Cybersikkerhed (CFCS) om en udtalelse vedrørende en undersøgelse, som Rigspolitiets Nationale Cyber Crime Center (NC3) har foretaget af et antal telefoner, iPads og simkort. Undersøgelsen har haft til formål at søge at genskabe SMS-beskeder og iMessage-beskeder sendt og modtaget i perioden 1. april 2020 til 31. december 2020.

FE's udtalelse baserer sig på en beskrivelse af NC3's opgaveløsning, som FE har modtaget fra Rigspolitiet. FE har lagt til grund, at de relevante enheder (dvs. telefoner mv. og evt. tilknyttede PC'er og MAC's, som kan have taget backup af mobiltelefoner mv.) er blevet sendt til Rigspolitiet.

På denne baggrund kan CFCS oplyse, at CFCS ville have fulgt den samme fremgangsmåde og anvendt de samme værktøjer, som er beskrevet i NC3's opgaveløsning.

FE kan på det foreliggende grundlag ikke pege på yderligere undersøgelser, som kunne være iværksat for at fremfinde og evt. genskabe de pågældende beskeder.

Med venlig hilsen

Forsvarets Efterretningstjeneste

Dato: 5. december 2021

Sagsnr.: [Sagsnr.]
Dok. nr.: [Dokumentnr.]

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 66
E-mail: FE-MYN@fe-ddis.dk
www.fe-ddis.dk

From: FMN <FMN@FMN.dk>
Sent: 13-12-2021 08:50:29 (UTC +02)
To: FMN-NPP Petersen, Niels Poul <NPP@1net.fmn.dk>; FMN-FWI Wind-Hansen, Frederikke Ravnborg <FWI@1net.fmn.dk>; FMN-DCE Elver, Dan Christian <DCE@1net.fmn.dk>; FMN-KTO Olsen, Kasper Thams <KTO@1net.fmn.dk>; FMN-ANB Jensen, Anders Bager <ANB@1net.fmn.dk>; 'Beredskabsstyrelsen' <brs@brs.fiin.dk>; FMN-EWS Stoustrup, Esben Wiingaard <EWS@1net.fmn.dk>; FMN-AJA Jakobsen, Anders <AJA@1net.fmn.dk>; FMN-CEC Christensen, Christine Engel <CEC@1net.fmn.dk>; FMN-ANK Kjær, Anna Nielsen <ANK@1net.fmn.dk>; FMN-ATE Teppel, Anne <ATE@1net.fmn.dk>; FMN-BHO Holmer, Birgitte <BHO@1net.fmn.dk>; FMN-BML Lund, Beinta Maria Joensen <BML@1net.fmn.dk>; FMN-CAT Thrane, Casper <CAT@1net.fmn.dk>; FMN-CEK Karstensen, Christian Ejby Strøm <CEK@1net.fmn.dk>; FMN-HRA Rasmussen, Helene <HRA@1net.fmn.dk>; FMN-IHO Holst, Ida <IHO@1net.fmn.dk>; FMN-JAK Kanto, Jakob <JAK@1net.fmn.dk>; FMN-JBH Holm, Jon Bach <JBH@1net.fmn.dk>; FMN-KBN Nielsen, Kenneth Bo <KBN@1net.fmn.dk>; FMN-KBR Breindal, Kristoffer <KBR@1net.fmn.dk>; FMN-KHJ Høeg-Jensen, Kasper <KHJ@1net.fmn.dk>; FMN-KTH Thorsen, Kåre Teis <KTH@1net.fmn.dk>; FMN-LBO Olsen, Lars Bo <LBO@1net.fmn.dk>; FMN-LIL Liboriussen, Linda <LIL@1net.fmn.dk>; FMN-LMK Kristensen, Lea Møberg <LMK@1net.fmn.dk>; FMN-LSA Salquist, Lars Rasmus <LSA@1net.fmn.dk>; FMN-DC Bæk, Morten <MOB@1net.fmn.dk>; FMN-PJA Jans, Pernille <PJA@1net.fmn.dk>; FMN-PJM Holager, Pelle Jacob Mølgaard <PJM@1net.fmn.dk>; FMN-KTP-Ministersekretariat <mns@1net.fmn.dk>; FMN-TLB Bøgh, Tony Lindemann <TLB@1net.fmn.dk>; FE-MYN-Forsvarets Efterretningstjeneste <FE-MYN@fe-ddis.fiin.dk>; FIR-MYN-FORSVARSMINISTERIETS INTERNE REVISION <FIR-MYN@fiin.dk>; 'Forsvarskommandoen' <fko@fiin.dk>; 'HJK' <hjk@hjv.dk>; FMN-JGK Kristensen, Jan Graugaard <JGK@1net.fmn.dk>; FMN-JCA Alexa, Jacob Christian <JCA@1net.fmn.dk>; FMN-JDP Petersen, Jonas Dramsgaard <JDP@1net.fmn.dk>; FMN-MEC Ecklon, Mads <MEC@1net.fmn.dk>; FMN-MIM Müller, Maja Isabella <MIM@1net.fmn.dk>; FMN-NBR Rasmussen, Nis Blach <NBR@1net.fmn.dk>; FMN-PVL Langeberg, Pernille Vedsgaard <PVL@1net.fmn.dk>; FMN-PTH Thiesen, Peter <PTH@1net.fmn.dk>; FMN-SGA Gandrup, Søren <SGA@1net.fmn.dk>; FMN-TKR Kristiansen, Trine <TKR@1net.fmn.dk>
Subject: Besvarelse af GRA spm. 8 vedr. slettet sms-korresponmdance
Categories: N

(FMI-KI besked: Denne mail kommer fra Internettet.)

Kvittering på afsendelse af GRA spørgsmål.

FORSVARSMINISTERIET
Holmens Kanal 9, DK-1060 København K
Telefon + 45 72 81 00 00
Fax + 45 72 81 03 00
E-mail: fmn@fmn.dk
www.fmn.dk

Fra: FMN [mailto:FMN@FMN.dk]
Sendt: 13. december 2021 08:49
Til: 'udvfor@ft.dk'
Emne: ¤¤ ££ Besvarelse af GRA spm. 8 vedr. slettet sms-korresponmdance

FORSVARSMINISTERIET
Holmens Kanal 9, DK-1060 København K
Telefon + 45 72 81 00 00
Fax + 45 72 81 03 00
E-mail: fmn@fmn.dk

www.fmn.dk

FORSVARSMINISTEREN

Folketingets Granskningsudvalg
Christiansborg

Folketingets Granskningsudvalg har den 7. december 2021 stillet følgende spørgsmål nr. 8, som hermed besvares.

Spørgsmål nr. 8:
Vil ministeren oversende sit talepapir fra det lukkede samråd den 7. december 2021 om muligheder for at gendanne slettet sms-korrespondancer, jf. GRA alm. del – samråds-spørgsmål A, B og C?

Svar:
Vedlagt fremsendes i fortrolighed det udkast til talepapir, som dannede grundlag for min besvarelse af samrådsspørgsmål C den 7. december 2021. Der gøres opmærksom på, at det talte ord gælder.

Med venlig hilsen

Trine Bramsen

Dato: 13. december 2021

Enhed: CNI
Sagsnr.: 2021/008780
Dok.nr.: 320356
Bilag: 1

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

FORSVARSMINISTERIET

DET TALTE ORD GÆLDER

TALESEDDEL TIL BRUG FOR BESVARELSEN AF GRANSKNINGSUDVALGETS SAMRÅDSSPØRGSMÅL C

Samråd C: Ministrene bedes redegøre for, om de har kendskab til eller har undersøgt andre muligheder, metoder, private virksomheder eller andre myndigheder, herunder Center for Cybersikkerhed, der vil kunne gendanne de slettede sms-korrespondance i lyset af, at dette i nogle tilfælde ikke var muligt for politiet?

[Justitsministeren og CH NC3 taler først derefter forsvarsministeren]

Tak for lejligheden til at bidrage til denne sag. Det glæder mig, at rammen er et lukket samråd, og at Rigspolitiet her har kunnet gå et spadetik dybere om genskabelse af de slettede SMS end vi ellers ville have kunnet i et åbent samråd.

Der bliver i samrådsspørgsmål C spurgt til, om Forsvarets Efterretningstjeneste (FE) og Center for Cybersikkerhed (CFCS) vil kunne bidrage til at gendanne de slettede SMS-beskeder.

FE er Danmarks udenrigsefterretningstjeneste. De retter dermed sine aktiviteter uden for Danmarks grænser og mod andre landes statsborgere. Elektronisk indhentning og analyse af data er et væsentligt grundlag for FE's virke.

CFCS er organiseret under FE og er Danmarks netsikkerhedstjeneste. CFCS har til opgave at understøtte et højt informationssikkerhedsniveau og beskytte danske myndigheder og dansk infrastruktur mod cyberangreb.

Jeg er blevet oplyst, at der er en dialog mellem Minkkommissionen og bisidderne for de relevante personer, om den videre proces i lyset af resultatet af politiets teknikeres forsøg på at genskabe relevante SMS'er.

Som justitsministeren netop har redegjort for, har nogle af Danmarks dygtigste IT-teknikere fra Rigspolitiet været på sagen.

FE bidrager altid gerne teknisk til politiets opgaveløsning, når der er behov for det - for ligesom politiet har FE en række tekniske kapaciteter til gendannelse af slettet data. Der sker løbende erfaringsudveksling mellem myndighederne på det tekniske område.

Der har i anledning af dette samråd været kontakt mellem myndighederne. Det har handlet om at afdække, om det er sandsynligt, at FE vil kunne noget mere med de konkrete enheder, end politiet har kunnet.

Statsministeriet har oplyst i svar til Folketinget, at forsøget på genskabelse af SMS-beskeder er sket fra de enheder, som ministeriet kunne identificere [spørgsmål nr. 180 fra Retsudvalget og spørgsmål nr. 3 fra Granskningsudvalget]. Justitsministeren har oplyst det samme til Folketinget [mundtlig besvarelse af spørgsmål nr. S 223]. Som jeg er oplyst, omfatter det telefoner, iPads, simkort og icloud-konti. Der er ikke udleveret computere, fordi ministerierne ikke har grund til at tro, at SMS'erne skulle være gemt på computere.

FE har på den baggrund afgivet følgende udtalelse, som jeg nu vil citere:

"FE's udtalelse baserer sig på en beskrivelse af NC3's opgaveløsning, som FE har modtaget fra Rigspolitiet. FE har lagt til grund, at de relevante enheder - dvs. telefoner mv. og evt. tilknyttede PC'er og MAC's, som kan have taget backup af mobiltelefoner mv. - er blevet sendt til Rigspolitiet.

På denne baggrund kan CFCS oplyse, at CFCS ville have fulgt den samme fremgangsmåde og anvendt de samme værktøjer, som er beskrevet i NC3's opgaveløsning.

FE kan på det foreliggende grundlag ikke pege på yderligere undersøgelser, som kunne være iværksat for at fremfinde og evt. genskabe de pågældende beskeder."

Som justitsministeren var inde på, har politiet altså benyttet de værktøjer, der også benyttes internationalt af specialierede politimyndigheder og efterretningstjenester.

Der har også været spurgt til, om CFCS monitorerer Statsministeriets netværk og datatrafik, og om de slettede SMS'er vil kunne findes i denne monitorering.

Ja, det gør CFCS for at kunne opdage og varsle mod cyberangreb. For CFCS's største og vigtigste opgave er at beskytte danske myndigheder og dansk infrastruktur mod cyberangreb.

Folketinget har vedtaget en lov om Center for Cybersikkerhed, som stiller præcise krav til og rammer for, hvad den monitorerede data må anvendes til.

Det har vi gjort for at beskytte data og privatlivets fred. Og et bredt flertal af Folketingets partier stod bag CFCS-loven.

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 Granskningskommissonen."

Som nævnt bidrager FE gerne teknisk til Rigspolitiets opgaveløsning. Og det gælder selvsagt også, hvis der er yderligere FE kan gøre i denne sag.

Tak for ordet.

FORSVARSMINISTERIET

Ekstraherede oplysninger i dokumenter vedrørende korrespondancer mellem Forsvarsministeriet og Forsvarets Efterretningstjeneste, herunder Center for Cybersikkerhed, om myndighedernes forsøg på at genskabe slettede SMS'er i Minksagen.

Dok. nr.	Titel	Brevdato
320943	20211201 Svar på anmod	01-12-2021

Forsvarsministeriet har anmodet FE om at sikre et øjeblikkeligt stop for overskrivning af data i sensornetværket.

Et øjeblikkeligt ophør af den automatisk overskrivning kan imidlertid i praksis kun ske ved at standse monitoreringen af CFCS' sensornetværk. Det skyldes, at lagringskapaciteten på de enkelte alarmenheder, udover den lovgivningsmæssige slettefrist, er den begrænsende faktor, som fører til automatisk sletning. Sletningen kan med andre ord kun stoppes ved at holde op med at gemme nye oplysninger. Øjeblikkelig standsning vil derfor betyde, at CFCS fra tidspunktet for standsning og fremefter ikke foretager monitorering, og deraf ikke er i stand til at detektere og varsle cyberangreb på de berørte netværk. Da monitorering af myndighedernes internetvendte trafik sker hos Statens IT, vil alle tilsluttede myndigheder ved Statens IT blive berørt af forholdet.

Dok. nr.	Titel	Brevdato
320945	Bidrag til besvarelse af samrådsspørgsmål C	02-12-2021

Til Forsvarsministeriet,
Center for Cyber og Digitalisering,
Christine E. Christensen, Lea Møberg Kristensen og Niels Poul Petersen
Kopi til: Center for Sikkerhed og Operationer, Peter Kim Laustsen og Kristoffer Breindal

Bidrag til besvarelse af samrådsspørgsmål C

Forsvarsministeriet har den 1. december 2021 anmodet Forsvarets Efterretningstjeneste (FE) om bidrag til besvarelse af samrådsspørgsmål C fra Granskningsudvalget og herunder besvare en række spørgsmål til brug for citatsvar.

Samrådsspørgsmål C
"Ministrene bedes redegøre for, om de har kendskab til eller har undersøgt andre muligheder, metoder, private virksomheder eller andre myndigheder, herunder Center for Cybersikkerhed, der vil kunne gendanne de slettede sms-korrespondance i lyset af, at dette i nogle tilfælde ikke var muligt for politiet?

FE kan til brug for besvarelsen oplyse følgende:

FE og CFCS' opgave, herunder særligt netsikkerhedstjenesten
FE er Danmarks udenrigs- og militære efterretningstjeneste og ansvarlig for at lede og kontrollere den militære sikkerhedstjeneste og varetage funktionen som national sikkerhedsmyndighed inden for Forsvarsministeriets område.

Derudover er FE national it-sikkerhedsmyndighed samt militær og statslig varslingstjeneste for internettrusler. Disse opgaver varetages af Center for Cybersikkerhed (CFCS) og er reguleret særskilt i CFCS-loven.

CFCS har til opgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

CFCS varetager en række opgaver, der spænder bredt fra ledelse af sikkerhedsarbejde, tilsyn, rådgivning og vejledning til myndigheder og virksomheder til imødegåelse af avancerede cyberangreb og international koordination af cybersikkerhedshændelser.

CFCS' netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser, f.eks. cyberangreb, hos de myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten.

CFCS' netsikkerhedstjeneste driver et sensornetværk, der er et alarmsystem bestående af alarmenheder og et 24/7- bemandet situationscenter, som monitorerer de tilsluttede myndigheder og virksomheder.

CFCS' hjemmel til opgaveløsning
CFCS' konkrete opgaver er specificeret i CFCS-lovens § 3, herunder netsikkerhedstjenestens opgaver.

Ved tilslutning til CFCS' netsikkerhedstjeneste indgås en aftale med den pågældende myndighed eller virksomhed om monitorering af bl.a. myndighedens forbindelse til digitale netværk, herunder internettet, gennem opsatte alarmenheder.

CFCS' netsikkerhedstjeneste kan i den forbindelse uden retskendelse behandle trafikdata, pakkedata og stationære data, jf. nedenfor, fra tilsluttede myndigheder med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet, jf. CFCS-lovens § 4.

Tilfælde hvor CFCS kan tilgå data fra sensornetværket
CFCS' behandling af data, der hidrører fra tilsluttede myndigheder, er nærmere reguleret i CFCS-lovens kapitel 7.

Det fremgår af CFCS-lovens § 15, at CFCS kan foretage automatiserede analyser af trafikdata, pakkedata og stationære data, der er omfattet af kapitel 4 (sensordata). Manuelle analyser af sensordata må alene finde sted 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 CFCS-lovens § 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.

I praksis udmøntes ovenstående således, at CFCS lægger en række regler i sensornetværket. Såfremt der forekommer trafik på alarmenhederne, der svarer til de

regler, der er lagt i sensornetværket, udløses en alarm. Ved alle alarmer foretages der en manuel analyse af en analytiker i netsikkerhedstjenesten.

CFCS frister for sletning af data fra monitorerede netværk (iht. loven og i praksis)
CFCS-lovens § 17 fastsætter de tidsmæssige rammer for CFCS' opbevaring af de data, der hidrører fra tilsluttede myndigheder.

Efter CFCS-lovens § 17, stk. 1, skal data, der er omfattet af kapitel 4, slettes, når formålet med behandlingen er opfyldt. Endvidere følger en række slettefrister af § 17, stk. 2, nr. 1-3, hvor det fastsættes, at uanset om formålet med behandlingen ikke er opfyldt, må

1) data, der knytter sig til en sikkerhedshændelse, højst opbevares i 5 år,
2) data, der ikke knytter sig til en sikkerhedshændelse, men som stammer fra myndigheder, der 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 3 år,
3) øvrige data, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 13 måneder.

[...]

I praksis er lagringskapaciteten i den pågældende alarmenhed også en afgørende faktor for, hvor længe selve pakkedata på alarmenhederne fra de hidrørende myndigheder opbevares. Når lagringskapaciteten er opbrugt, bliver der løbende overskrevet data på alarmenheden, hvor det ældste data overskrives først. Lagringskapaciteten på de enkelte alarmenheder er således, udover den lovgivningsmæssige slettefrist, en begrænsende faktor, som fører til automatisk overskrivning.

Beskrivelse af sensor-data (metadata, pakkedata, krypteret data, klartekst data)
CFCS-lovens § 2 definerer syv centrale begreber i loven, herunder begreberne pakkedata, trafikdata og stationære data, der er nærmere beskrevet nedenfor. Den data, som CFCS monitorerer gennem opsatte alarmenheder, kan omfatte trafik- og pakkedata.

Pakkedata
Indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester (indholdsdata), jf. CFCS-lovens § 2, nr. 2. Det kan eksempelvis være indholdet af en e-mailkorrespondance eller indholdet af tilgåede hjemmesider. Herudover er det tekniske indhold af kommunikationen omfattet af begrebet (f.eks. HTML- eller XML-koder).[1]

Trafikdata
Data, der behandles med henblik på at transmittere pakkedata, jf. CFCS-lovens § 2, nr. 3. Det er f.eks. oplysninger om IP-adresser, emailadresser, hjemmesideadresser, kommunikationens varighed og tidspunktet for kommunikationen.[2]

Stationære data
Data, der opbevares på servere, cloudtjenester, computere, lagerenheder, netværksenheder, mobile enheder og tilsvarende, jf. CFCS-lovens § 2, nr. 4. Data er karakteriseret ved at være lagret eller i øvrigt tilgængeligt på en enhed, herunder i "skyen", og ikke et egentligt led i en igangværende kommunikation. Det vil eksempelvis

[1] 1 Lovforslag nr. L 215 af 27. marts 2019 om ændring af lov om Center for Cybersikkerhed, de specielle bemærkninger til den foreslåede § 2
[2] Lovforslag nr. L 215 af 27. marts 2019 om ændring af lov om Center for Cybersikkerhed, de specielle bemærkninger til den foreslåede § 2

være et dokument eller et billede, der er lagret på en pc eller i en database, eller en e-mail, der opbevares på en mailserver.[3]

Overvågning af STM og JM netværk
Statsministeriets og Justitsministeriets interne og eksterne trafik er omfattet af CFCS' monitorering. CFCS' monitorering ser automatisk på data som eksempelvis IP-adresser og portnumre, der kører ind og ud af de to ministeriers netværk via internettet. Systemet scanner efter filer eller forbindelser, der indeholder skadelig software, og kigger efter mønstre, der med høj sandsynlighed indikerer ondsindet trafik.

Kan netværksdata indeholde SMS'er fra minksagen
CFCS' monitorering 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 granskningskommissonen.

Har CFCS undersøgt om netværksdata måtte indeholde SMS'er fra STM og JM CFCS ikke er blevet anmodet om at undersøge dette, og CFCS har i øvrigt ikke hjemmel til at se efter indholdsdata, som måtte ligge i CFCS' sensornetværk, for at undersøge, om der i sensornetværket eventuelt er oplysninger af relevans for granskningskommissionens opgave. CFCS må, jf. ovenfor, alene tilgå og foretage manuelle analyser af pakkedata, når der foreligger en begrundet mistanke om en sikkerhedshændelse, og det er nødvendigt for at afklare forhold vedrørende hændelsen.

Har FE eksperter, der er i stand til at genskabe mobiltelefoner
[Spørgsmålet kan ikke besvares IKL].

Evt. samarbejde om forensic samt hjemmel hertil
Andre myndigheder kan anmode CFCS om bistand til at løse en opgave, som den respektive myndighed har hjemmel til at udføre. CFCS vil kunne yde bistand til andre myndigheder, hvis den ønskede bistand har en naturlig tilknytning til CFCS' opgave som national it-sikkerhedsmyndighed og særlige sagkundskab. Det er den anmodende myndigheds opgave at sikre, at de materielle betingelser i henhold til den pågældende myndigheds lovgrundlag for gennemførelse af bistanden er opfyldt.

I forarbejderne til FE-loven er det forudsat, at FE yder støtte til PET, og denne bistand ydes i praksis i visse tilfælde af CFCS.

Kan FE bryde iMessage-kryptering
[Spørgsmålet kan ikke besvares IKL].

Med venlig hilsen Forsvarets Efterretningstjeneste

Dok. nr.	Titel	Brevdato
321035	VS: Varsel: GRA alm. del - samrådsspørgsmål C til forsvarsministeren og justitsministeren (vedr. slettede SMS'er)	29-11-2021

Til info er FM-godkendelse af bidrag til REU-svar sat på pause grundet indkaldelse til samråd i sagen – se vedhæftede.

[3] Lovforslag nr. L 215 af 27. marts 2019 om ændring af lov om Center for Cybersikkerhed, de specielle bemærkninger til den foreslåede § 2

Dok. nr.	Titel	Brevdato
321042	HASTER: Anmodning om FE bidrag til samråd [RELEASABLE TO INTERNET TRANSMISSION]	01-12-2021

Granskningsudvalget har stillet samrådsspørgsmål C til justitsministeren og forsvarsministeren vedr. slettede SMS'er. Samrådet forventes berammet allerede **tirsdag den 7. december** efter ønske fra ministrene.

Dok. nr.	Titel	Brevdato
322679	Bilag 4: 20211213_Besvarelse_af_GRA_spørgsmål	13-12-2021

Til: Forsvarsministeriet
Center for Cyber og Digitalisering,
Christine E. Christensen, Niels Poul Petersen og Lea Møberg Kristensen
Kopi til: Center for Cybersikkerhed og Operationer, Peter Kim Laustsen og Kristoffer Breindal

Bidrag til besvarelse af GRA spørgsmål nr. 9, 10 og 11 (alm. del)
Forsvarsministeriet har den 9. december 2021 anmodet Forsvarets Efterretningstjeneste (FE) om bidrag til besvarelse af spørgsmål nr. 9, 10 og 11 (alm. del) fra Granskningsudvalget.

Spørgsmål 9:
Forsvarsministeren bedes i forlængelse af besvarelsen af samrådsspørgsmål C redegøre nærmere for, hvordan censornetværket fungerer og oplyse, hvilke typer af data, der opfanges af det nævnte censornetværk og som der derfor er muligt at få adgang til?

Spørgsmål 10:
I forlængelse af besvarelsen af samrådsspørgsmål A-C bedes forsvarsministeren oplyse om, om det forholder sig således, at alle i-messages monitoreres, både dem, der er sendt via wi-fi-netværk og via telefonens mobile bredbånd.

Spørgsmål 11:
I forlængelse heraf bedes forsvarsministeren endvidere oplyse, om der er en særlig ordning for kryptering af sådanne beskeder i regeringen, eller om der er tale om en kryptering, som er standard for også almindelige brugere uden en særlig opsætning af kryptering?

FE kan til brug for besvarelsen af spørgsmål nr. 9 og 10 oplyse følgende:

"Center for Cybersikkerheds (CFCS) netsikkerhedstjeneste driver et sensornetværk. Sensornetværket er et alarmsystem bestående af hardwareenheder, såkaldte sensorer, der via en automatisk proces monitorerer ind- og udgående internettrafik hos myndigheder og virksomheder, der efter aftale er tilsluttet sensornetværket.

Sensorerne er programmeret med informationer om ondartet trafik, som hardwareenheden leder efter i internettrafikken. Hvis sensoren identificerer mistænkelig trafik, udløser det en alarm, hvorefter de relevante data bliver analyseret af en analytiker i CFCS.

Den data, som CFCS monitorerer gennem sensornetværket i henhold til CFCS-loven, kan omfatte både trafik- og pakkedata. Disse begreber er nærmere defineret i CFCS-lovens kapitel 2. CFCS-lovens kapitel 7 fastsætter de nærmere rammer for analyse, videregivelse og sletning af data fra sensornetværket. I den forbindelse bemærkes det, at CFCS kun i helt særlige tilfælde har hjemmel til at tilgå oplysningerne i sensornetværket.

CFCS' monitorering omfatter ikke mobiloperatørernes mobilnetværk og dermed heller ikke disse netværks fremføring af sms'er eller iMessages mv. Beskeder, der ved anvendelse af

et wifi-netværk sendes via en internetforbindelse (f.eks. via applikationen iMessage), som CFCS monitorerer, vil imidlertid potentielt kunne blive opfanget af CFCS' sensorer.

[...].

FE kan i øvrigt henvise til FE's bidrag til Forsvarsministeriets besvarelse af spørgsmål nr. 307 fra Folketingets Retsudvalg den 6. december 2021.

For så vidt angår besvarelsen af spørgsmål nr. 11 kan FE ikke inden for rammerne af et folketingsspørgsmål oplyse, om der i centraladministrationen er implementeret sikkerhedsmæssige tiltag for kryptering af beskeder. FE kan desuden oplyse, at iMessage er en beskedtjeneste, der drives af den amerikanske virksomhed Apple Inc. FE kan derfor ikke redegøre nærmere for, hvilke specifikke krypteringsløsninger, der stilles til rådighed af virksomheden i forbindelse med driften heraf, herunder om der tilbydes forskellige løsninger til brugerne.

Med venlig hilsen

Forsvarets Efterretningstjeneste

Dok. nr.	Titel	Brevdato
520982	SV: Telefondata 1	03-12-2021

Der har konkret været anvendt 5 forskellige kriminaltekniske it-værktøjer til at forsøge at genskabe de slettede SMS'er.

Alle 5 værktøjer anvendes internationalt af politimyndigheder, efterretningstjenester og it-sikkerhedsfirmaer.

Og alle undersøgte mobile enheder samt cloud-konti er undersøgt med de samme værktøjer og processer.

Det er ikke usædvanligt at anvende 2 til 3 forskellige værktøjer til efterforskning af mobile enheder. Det skyldes, at værktøjerne har forskellige styrker og begrænsninger i forhold til udlæsning, processering, analyse samt visualisering af data.

De samme værktøjer er efterfølgende anvendt til at samle alle data i en såkaldt beskyttet evidensfil, som også anvendes af politiet i forbindelse med kriminaltekniske it-undersøgelser.

Herefter er data processeret, hvilket vil sige, at al data er lagt på 'rette hylde' i de kriminaltekniske it-værktøjer i forhold til datatyper. Det handler om at sortere SMS'er, iMessages, billeder, kontaktpersoner osv. for sig.

It-efterforskerne har brugt værktøjerne til at finde eventuelle SMS'er og iMessages fra perioden 1. april 2020 til 31. december 2020.