FORSVARSMINISTERIET

Januar 2019

U d k a s t

Forslag

til

Lov om ændring af lov om Center for Cybersikkerhed

(Initiativer til styrkelse af cybersikkerheden)

§ 1

I lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed, som ændret ved lov nr. 443 af 8. maj 2018, foretages følgende ændringer:

1. *§§ 2* og *3* affattes således:

»**§ 2.** I denne lov forstås ved:

1) Sikkerhedshændelse: En hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.
2) Pakkedata: Indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester.
3) Trafikdata: Data, som behandles med henblik på at transmittere pakkedata.
4) Stationære data: Data, som opbevares på servere, cloudtjenester, pc'ere, lagerenheder, netværksenheder, mobile enheder og tilsvarende.
5) Malware: Trafikdata, pakkedata og stationære data, hvor der er særligt bestyrket mistanke om, at data er anvendt af en angrebsaktør med det formål at forårsage et brud på informationssikkerheden.
6) Personoplysninger: Enhver form for information om en identificeret eller identificerbar fysisk person.
7) Behandling: Enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for.

§ 3. Center for Cybersikkerheds netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder, jf. stk. 2-4.

Stk. 2. De øverste statsorganer samt statslige myndigheder kan efter anmodning blive tilsluttet netsikkerhedstjenesten.

Stk. 3. Regioner og kommuner samt virksomheder, der har samfundsvigtig karakter, kan efter anmodning blive tilsluttet netsikkerhedstjenesten, såfremt Center for Cybersikkerhed

konkret vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

Stk. 4. Center for Cybersikkerhed kan i særlige tilfælde påbyde virksomheder, regioner og kommuner, der har særligt samfundsvigtig karakter, at blive tilsluttet netsikkerhedstjenesten.

Stk. 5. Forsvarsministeren kan fastsætte nærmere regler om vilkårene for tilslutning efter stk. 2 og 3. Forsvarsministeren kan desuden fastsætte nærmere regler om påbud efter stk. 4, herunder om at myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten på baggrund af et påbud, skal medvirke til netsikkerhedstjenestens opsætning og drift af hardware og software og i den forbindelse skal stille de nødvendige oplysninger om konfiguration og drift af deres digitale infrastruktur til rådighed for netsikkerhedstjenesten.«

2. Overskriften til kapitel 4 affattes således:

»Kapitel 4

Indgreb omfattet af grundlovens § 72«

3. *§§ 4-6* affattes således:

»**§ 4.** Center for Cybersikkerheds netsikkerhedstjeneste kan uden retskendelse behandle trafikdata, pakkedata og stationære data hidrørende fra tilsluttede myndigheder og virksomheder, jf. § 3, stk. 2-4, med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet.

§ 5. Ved begrundet mistanke om en sikkerhedshændelse kan Center for Cybersikkerheds netsikkerhedstjeneste uden retskendelse behandle stationære data fra en myndighed eller virksomhed, der ikke er tilsluttet netsikkerhedstjenesten, når

1) myndigheden eller virksomheden har anmodet Center for Cybersikkerhed om bistand, stillet de stationære data til rådighed for netsikkerhedstjenesten og givet skriftligt samtykke til behandlingen, og
2) behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

§ 6. Efter aftale med en myndighed eller virksomhed, der er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste i medfør af § 3, stk. 2 og 3, kan netsikkerhedstjenesten ved begrundet mistanke om en sikkerhedshændelse uden retskendelse blokere, omdanne eller omdirigere trafikdata og pakkedata hidrørende fra netværk hos myndigheden eller virksomheden med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet.

Stk. 2. Stk. 1 finder tilsvarende anvendelse i forhold til stationære data hos tilsluttede myndigheder og virksomheder. Ved en konstateret sikkerhedshændelse kan netsikkerhedstjenesten endvidere slette de stationære data, der har forårsaget sikkerhedshændelsen.«

4. Efter § 6 indsættes:

»**§ 6 a.** Med henblik på at kunne rådgive myndigheder og virksomheder om forebyggelse af sikkerhedshændelser kan Center for Cybersikkerhed gennemføre forebyggende sikkerhedstekniske undersøgelser, når en myndighed eller virksomhed har anmodet centeret herom.

Stk. 2. Efter anmodning fra myndigheden eller virksomheden kan Center for Cybersikkerhed som led i den forebyggende sikkerhedstekniske undersøgelse

1) uden retskendelse behandle trafikdata, pakkedata og stationære data hos myndigheden eller virksomheden,
2) behandle offentligt tilgængelige data om myndigheden eller virksomheden og dennes medarbejdere, og
3) iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder i myndigheden eller virksomheden.

§ 6 b. Med henblik på at opnå viden om angrebsaktørers metoder og værktøjer kan Center for Cybersikkerhed opsætte fiktive angrebsmål, såfremt opsætningen vurderes at kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at understøtte et højt informationssikkerhedsniveau i samfundet.

Stk. 2. Hvis en angrebsaktør benytter et fiktivt angrebsmål til at deponere data, kan Center for Cybersikkerhed uden retskendelse behandle de deponerede data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller at informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.

§ 6 c. Med henblik på at forhindre, standse eller begrænse en nært forestående eller igangværende sikkerhedshændelse kan Center for Cybersikkerhed gøre brug af domænenavne og tilsvarende it-infrastruktur, som anvendes eller har været anvendt af en angrebsaktør, men som er offentligt tilgængelig.

Stk. 2. Hvis Center for Cybersikkerhed som led i anvendelsen af it-infrastruktur efter stk. 1 modtager data fra tredjemand, kan centeret uden retskendelse behandle de modtagne data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller at informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.«

5. Efter § 6 c indsættes:

»Kapitel 4 a

Edition«

6. *§ 7* affattes således:

»**§ 7.** Med henblik på at afdække sikkerhedshændelser kan der 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.

Stk. 2. Der kan ikke meddeles pålæg efter stk. 1, såfremt der derved vil fremkomme oplysninger om forhold, som den pågældende ville være udelukket fra eller fritaget fra at afgive forklaring om som vidne efter retsplejelovens §§ 169-172.

Stk. 3. Pålæg efter stk. 1 må ikke meddeles, såfremt indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre.«

7. Efter § 7 indsættes i *kapitel 4 a:*

»**§ 7 a.** Afgørelse om pålæg om edition efter § 7 træffes af retten efter Center for Cybersikkerheds begæring.

Stk. 2. Afgørelsen træffes af retten ved kendelse. Retsmøder holdes for lukkede døre. I kendelsen anføres de konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for indgrebet er opfyldt. Kendelsen kan til enhver tid omgøres.

§ 7 b. Inden retten træffer afgørelse efter § 7 a, skal der beskikkes en advokat for den, som indgrebet vedrører, og advokaten skal have lejlighed til at udtale sig. Advokaten beskikkes fra den særlige kreds af advokater, som er nævnt i retsplejelovens § 784, stk. 2.

§ 7 c. En advokat, som er beskikket efter § 7 b, skal underrettes om alle retsmøder i sagen og er berettiget til at overvære disse samt i forbindelse med retsmødet at gøre sig bekendt med det materiale, som Center for Cybersikkerhed har tilvejebragt. Advokaten må ikke give de oplysninger, som denne bliver bekendt med under sagen, videre til andre eller sætte sig i forbindelse med den, over for hvem indgrebet er begæret foretaget. Den beskikkede advokat må ikke give møde ved anden advokat eller ved fuldmægtig.

Stk. 2. Bestemmelserne om beskikkede forsvarere i retsplejelovens kapitel 66 og § 746, stk. 1, finder tilsvarende anvendelse på den beskikkede advokat. Retten kan bestemme, at den beskikkede advokat ikke under en eventuel senere straffesag kan virke som forsvarer for nogen sigtet.

§ 7 d. Inden retten træffer afgørelse om pålæg om edition efter § 7, skal der være givet den, der har rådighed over oplysningerne, adgang til at udtale sig.

Stk. 2. Såfremt hensynet til fremmede magter eller statens sikkerhed taler derfor, kan retten eller Center for Cybersikkerhed pålægge den, der har rådighed over oplysninger, som ønskes forevist eller udleveret efter § 7, tavshedspligt med hensyn til den pågældendes viden om sagen. Når pålæg meddeles en erhvervsvirksomhed, gælder dette også for andre juridiske og fysiske personer, der i kraft af deres tilknytning til virksomheden har fået kendskab til sagen.

Stk. 3. Pålæg efter stk. 2 kan ophæves af Center for Cybersikkerhed eller retten. Center for Cybersikkerheds nægtelse af at ophæve et pålæg skal efter begæring forelægges retten. Den pågældende skal gøres bekendt med adgangen hertil.

§ 7 e. Reglerne i retsplejelovens kapitel 63 om værneting og kapitel 85 om kære til højere ret finder tilsvarende anvendelse.

§ 7 f. Center for Cybersikkerhed foranlediger ved at rette henvendelse til den, der har rådighed over oplysningerne, at en kendelse om edition opfyldes. Rettens kendelse skal på begæring forevises for den pågældende. Afviser den pågældende uden lovlig grund at efterkomme pålægget, finder reglerne i retsplejelovens § 178 tilsvarende anvendelse.«

8. I *§ 8, stk. 1, 2. pkt.*, indsættes efter »forvaltningslovens kapitel 4-6«: », fra § 3, § 5 og § 8, stk. 2, i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter«

9. *§ 8, stk. 2, nr. 1,* affattes således:

»1) centerets behandling af sager om tilslutning til netsikkerhedstjenesten, jf. § 3, stk. 3 og 4,«

10. Efter § 8 indsættes i *kapitel 5:*

»**§ 8 a.** Oplysninger, der er omfattet af denne lov, kan overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen.

Stk. 2. Forsvarsministeren kan fastsætte nærmere regler om Center for Cybersikkerheds behandling af oplysninger, der skal bevares for eftertiden.«

11. *§ 14, stk. 2,* ophæves.

12. *§§ 15-17* affattes således:

»**§ 15.** Center for Cybersikkerhed kan foretage automatiserede analyser af trafikdata, pakkedata og stationære data, der er omfattet af kapitel 4. Manuelle analyser af data, der er omfattet af kapitel 4, 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 afklaring af 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 tests 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 Center for Cybersikkerhed. Øvrige medarbejdere må ikke tilgå oplysninger, der hidrører fra tests. Malware, der ved en tilfældighed opdages som led i en teknisk test, må dog analyseres af øvrige medarbejdere i Center for Cybersikkerhed efter nr. 2.

§ 16. Center for Cybersikkerhed kan 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 Center for Cybersikkerheds opgaver.
3) Danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt til myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger, såfremt der er begrundet mistanke om en sikkerhedshændelse, og hvis det er nødvendigt for udførelsen af Center for Cybersikkerheds opgaver.

Stk. 2. Center for Cybersikkerhed kan 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.

Stk. 3. Center for Cybersikkerhed kan 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 Center for Cybersikkerhed har modtaget de pågældende data i medfør af § 6 b eller § 6 c.

Stk. 4. Center for Cybersikkerhed kan 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 til myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger.

Stk. 5. Stk. 1-4 finder ikke anvendelse på data, der stammer fra tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder. Center for Cybersikkerhed kan alene videregive sådanne data 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 Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger.
2) Trafikdata kan videregives til den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører.

§ 17. Data, der er omfattet af kapitel 4, slettes, når formålet med behandlingen er opfyldt.

Stk. 2. Uanset at formålet med behandlingen ikke er opfyldt, jf. stk. 1, 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, 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 3 år, og
3) øvrige data, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 13 måneder.

Stk. 3. Fristerne i stk. 2 regnes fra tidspunktet for Center for Cybersikkerheds registrering af de pågældende data.

Stk. 4. Center for Cybersikkerhed kan opbevare backup af data i op til 4 måneder efter udløb af fristerne i stk. 1 og 2. Ved indlæsning af data fra backup skal Center for Cybersikkerhed sikre, at data, der tidligere er slettet efter stk. 1 eller 2, straks slettes igen.

Stk. 5. Er data i medfør af § 16 videregivet til andre end den myndighed eller virksomhed, som data hidrører fra, finder stk. 1 og 2 ikke anvendelse på disse data.

Stk. 6. I data, som Center for Cybersikkerhed får adgang til som led i forebyggende sikkerhedstekniske undersøgelser efter § 6 a, skal personoplysninger, der er indeholdt i disse data, endvidere slettes eller anonymiseres, når den sikkerhedstekniske undersøgelse er afsluttet. Såfremt Center for Cybersikkerhed konstaterer, at der i de pågældende data er indeholdt følsomme personoplysninger, skal disse slettes uden unødigt ophold.

Stk. 7. Sletning efter fristerne i stk. 2, nr. 2 og 3, kan i helt særlige tilfælde kortvarigt suspenderes, hvis væsentlige hensyn til varetagelsen af Center for Cybersikkerheds opgaver gør det nødvendigt. Tilsynet med Efterretningstjenesterne skal straks underrettes om suspension efter 1. pkt. og om baggrunden for suspensionen.«

13. Efter § 17 indsættes i *kapitel 7:*

»**§ 17 a.** § 17 finder ikke anvendelse på data, der er deponeret på fiktive angrebsmål efter § 6 b eller modtaget via infrastruktur omfattet af § 6 c, såfremt Center for Cybersikkerhed ikke udtager disse data til nærmere vurdering. Disse data slettes hurtigst muligt. Udtager Center for Cybersikkerhed data til nærmere vurdering, skal sletning ske efter reglerne i § 17.«

14. I *§ 20* indsættes efter »kapitel 4,«: »4 a,«.

15. Efter § 24 indsættes:

»Kapitel 9 a

Straffebestemmelser m.v.

§ 24 a. Med bøde straffes, medmindre strengere straf er forskyldt efter den øvrige lovgivning, den, der undlader at efterkomme et pålæg efter § 7 d, stk. 2.

Stk. 2. I regler, der udfærdiges i medfør af § 3, stk. 5, 2. pkt., kan der fastsættes straf i form af bøde for overtrædelse af bestemmelserne i reglerne.

Stk. 3. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.«

§ 2

Stk. 1. Loven træder i kraft den 1. juli 2019.

Stk. 2. Loven finder ikke anvendelse på data, der er indsamlet før den 1. juli 2019. For sådanne data finder de hidtil gældende regler anvendelse.

§ 3

Loven gælder ikke for Færøerne og Grønland, men kan ved kongelig anordning sættes helt eller delvis i kraft for Færøerne og Grønland med de ændringer, som de færøske og grønlandske forhold tilsiger.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

Cybertruslen er de seneste år øget markant, og der er i dag en meget høj cybertrussel mod Danmark. Både i Danmark og udlandet er der talrige eksempler på alvorlige cyberangreb, som har haft store konsekvenser for myndigheder og virksomheder. Den hastige udvikling i trusselsbilledet betyder, at der er behov for at tilpasse lovgivningen, så Center for Cybersikkerheds muligheder for at imødegå cyberangreb mod den kritiske infrastruktur fremadrettet modsvarer truslerne og den teknologiske udvikling.

Den alvorlige cybertrussel var allerede i 2011 baggrunden for, at opgaver vedrørende it-sikkerhed blev ressortoverført til Forsvarsministeriet, hvorefter en række forskellige myndigheders indsatser blev samlet i Center for Cybersikkerhed som en del af Forsvarets Efterretningstjeneste. Siden 2014 har centerets virke været reguleret i lov om Center for Cybersikkerhed.

I maj 2018 lancerede regeringen en ny national strategi for cyber- og informationssikkerhed. Af strategien fremgår det, at Forsvarsministeriet vil fremsætte et forslag til ændret lovgivning på cyberområdet, som vil medføre en styrkelse af Center for Cybersikkerheds muligheder for at opdage og stoppe cyberangreb samt styrke centerets analytiske arbejde.

Dette lovforslag er et led i udmøntningen af den nationale strategi for cyber- og informationssikkerhed. Forsvarsministeriet har i den forbindelse lagt afgørende vægt på, at lovgivningsinitiativerne udmøntes med den fornødne respekt for retssikkerheden og den personlige frihed. Der er således tale om initiativer, der er målrettede og ikke går videre end formålet tilsiger.

Henset til den hastige udvikling på cybersikkerhedsområdet vil der blive udarbejdet en rapport om erfaringerne med den nye lovgivning, som oversendes til Folketinget tre år efter lovens ikrafttræden.

2. Baggrunden for lovforslaget

2.1. Om Center for Cybersikkerhed

Center for Cybersikkerhed blev oprettet den 18. december 2012 som en del af Forsvarets Efterretningstjeneste.

Center for Cybersikkerheds opgave er først og fremmest at understøtte et højt sikkerhedsniveau i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af.

Denne opgave løses bl.a. gennem Center for Cybersikkerheds netsikkerhedstjeneste, som har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser, herunder avancerede cyberangreb, mod myndigheder og virksomheder, der er beskæftiget med samfundsvigtige funktioner. Det sker i dag primært gennem de pågældende myndigheders og virksomheders tilslutning til netsikkerhedstjenesten. Ved tilslutning opsættes en alarmenhed hos den enkelte myndighed eller virksomhed. Alarmenheden monitorerer ind- og udgående netværkskommunikation, herunder internetkommunikation.

Center for Cybersikkerhed varetager desuden funktionen som Danmarks nationale it-sikkerhedsmyndighed og nationalt kompetencecenter på cybersikkerhedsområdet. Rollen som na-

tional it-sikkerhedsmyndighed indebærer en række opgaver af både forebyggende og afhjælpende karakter. Det gælder bl.a. oplysning, vejledning og rådgivning af danske myndigheder og virksomheder i at styrke cybersikkerheden, så risikoen for cyberangreb mindskes, og så cyberangreb, hvis de lykkes, imødegås på den mest hensigtsmæssige måde. I den forbindelse har centeret en løbende dialog med relevante interessenter.

Derudover er Center for Cybersikkerhed myndighed for informationssikkerhed og beredskab på teleområdet. Det betyder, at centeret bl.a. stiller informationssikkerhedskrav til teleudbydere og fører tilsyn på området, ligesom centeret også rådgiver samfundets beredskabsaktører om teleberedskab. Disse opgaver følger bl.a. af Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), som senest ændret ved Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009.

Center for Cybersikkerhed varetager desuden en række tværgående myndighedsopgaver, herunder funktionen som nationalt centralt kontaktpunkt og beredskabsenhed, der håndterer it-sikkerhedshændelser (CSIRT). Disse opgaver følger af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet).

Med placeringen ved Forsvarets Efterretningstjeneste har Center for Cybersikkerhed adgang til efterretningsmæssige oplysninger, som er afgørende for at kunne levere den optimale beskyttelse mod avancerede cyberangreb. Center for Cybersikkerhed drager nytte af de højt specialiserede kompetencer, som den efterretningsmæssige del af Forsvarets Efterretningstjeneste har på cyberområdet.

Samtidig har Center for Cybersikkerhed en åben og udadvendt profil, og selv om Center for Cybersikkerhed og den efterretningsmæssige del af Forsvarets Efterretningstjeneste tilsammen udgør én myndighed, er de gennem lovgivningen tillagt forskellige opgaver og virkemidler. Mens efterretningsmæssige oplysninger af betydning for cybersikkerheden uden begrænsning kan udveksles fra den efterretningsmæssige del til Center for Cybersikkerhed, gælder det ikke den anden vej. Forsvarsministeren har således i administrative retningslinjer fastsat en række begrænsninger for Center for Cybersikkerheds udveksling af data med den efterretningsmæssige del af Forsvarets Efterretningstjeneste.

2.2. Udviklingen i trusselsbilledet

Danmark er et af verdens mest digitaliserede lande, hvilket gør danske myndigheder og virksomheder særligt sårbare overfor cyberangreb. Cyberangreb mod den digitale infrastruktur vil derfor kunne have store samfundsmæssige konsekvenser, og ved vellykkede angreb mod danske myndigheder vil angriberne potentielt kunne få adgang til meget store mængder følsomme oplysninger, herunder personoplysninger.

Cybertruslen er de seneste år øget markant, og både i Danmark og udlandet er der talrige eksempler på alvorlige cyberangreb, som har haft store konsekvenser for myndigheder og virksomheder. Et særligt omfattende cyberangreb, kendt som NotPetya, spredte sig eksempelvis i 2017 fra Ukraine og ramte især virksomheder i en række lande, herunder Danmark, med meget store omkostninger til følge.

Forsvarets Efterretningstjeneste vurderer, at Danmark står over for en meget høj cybertrussel, særligt fra fremmede stater. Nogle stater forsøger vedholdende at udføre cyberspionage mod danske myndigheder og virksomheder, og de gør det stadigt sværere at opdage deres aktiviteter. Visse stater har desuden vist vilje til også at udføre mere offensive cyberangreb, der f.eks. har til formål at påvirke meningsdannelsen i andre lande. Samtidig bliver avancerede hackerværktøjer også tilgængelige for flere ikke-statslige aktører.

Danske myndigheder og virksomheder er i et vedvarende kapløb med fremmede stater, hackergrupper og individer, der hele tiden udvikler nye måder, hvormed de kan udnytte cyberangreb til at nå deres politiske eller økonomiske mål. Nogle stater udviser samtidig en mere offensiv adfærd, hvor de er villige til at udføre angreb, der har andre formål end cyberspionage, bl.a. hacking og lækage af følsomme oplysninger samt destruktive cyberangreb.

Forsvarets Efterretningstjeneste vurderer, at truslen mod offentlige myndigheder i Danmark fortsat vil gøre sig gældende på langt sigt, og at truslen dermed er blevet et grundvilkår. Sammenlignet med traditionel spionage er cyberspionage en effektiv og relativt risikofri måde for fremmede sikkerheds- og efterretningstjenester at indhente informationer på. Det gælder også i forhold til truslen mod danske virksomheder, hvor fremmede stater kan høste fordele af den viden og teknologi, som andre har brugt ressourcer på at udvikle. Endvidere kan cyberspionage understøtte andre typer cyberangreb og trusler. Cyberspionage kan give en modstander adgang til følsomme oplysninger, der senere kan bruges til afpresning eller lækkes til offentligheden med henblik på at påvirke meningsdannelsen. Endvidere kan cyberspionage anvendes som forudsætning for senere destruktive cyberangreb, herunder hvis cyberspionagen giver adgang til kritiske systemer.

2.3. Lovforslagets formål

Formålet med dette lovforslag er at opdatere lovgrundlaget for Center for Cybersikkerhed, så det tilpasses det aktuelle trusselsbillede og den teknologiske udvikling. Med lovforslaget vil Center for Cybersikkerhed således få bedre muligheder for at løse de opgaver, som centeret er pålagt.

Lovforslaget indebærer for det første bedre muligheder for at udnytte den beskyttelse, der ligger i Center for Cybersikkerheds netsikkerhedstjeneste. I dag er det en udfordring, at relativt få myndigheder og virksomheder er tilsluttet netsikkerhedstjenesten, og at der dermed er mange samfundsvigtige virksomheder, som ikke får monitoreret deres internettrafik for avancerede cybertrusler. En central årsag til den lave tilslutning er, at tilslutningen er dyr, og at der i dag er krav om fuld egenbetaling for tilslutning. Med lovforslaget fjernes gebyret for tilslutning, således at tilslutning fremover vil være gratis for offentlige myndigheder og virksomheder, der har samfundsvigtig karakter, såfremt Center for Cybersikkerhed vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet. Endvidere vil der med lovforslaget blive skabt mulighed for, at der i helt særlige tilfælde vil kunne gives påbud til særligt samfundsvigtige virksomheder eller myndigheder om at blive tilsluttet netsikkerhedstjenesten.

For det andet indebærer lovforslaget, at Center for Cybersikkerheds netsikkerhedstjeneste vil kunne agere mere aktivt i beskyttelsen af samfundsvigtige myndigheder og virksomheder. I dag kan centerets alarmenheder alene anvendes til at registrere den skadelige trafik og derefter varsle myndigheden eller virksomheden om, at den har været udsat for et an-

greb. Med lovforslaget vil der blive skabt mulighed for at anvende alarmenhederne til at stoppe igangværende cyberangreb, f.eks. ved at blokere eller omdirigere skadelig trafik hos de myndigheder og virksomheder, som har ønsket at tilslutte sig en sådan ordning.

For det tredje monitorerer Center for Cybersikkerhed i dag kun datatrafik på de forbindelser, der går ind og ud af de tilsluttede myndigheder og virksomheder. Det giver i stigende grad udfordringer, dels fordi mere og mere datatrafik bliver utilgængeligt på grund af kryptering, hvor det kan passere alarmenhederne uden at udløse en alarm, og dels fordi det ikke er muligt at opdage uregelmæssigheder, som sker på pc'ere og servere hos de tilsluttede myndigheder og virksomheder. Den teknologiske udvikling udhuler således Center for Cybersikkerheds mulighed for effektivt at opdage trusler og hændelser. Lovforslaget indebærer derfor, at der skabes mulighed for at installere sikkerhedssoftware på f.eks. pc'ere og servere hos myndigheder og virksomheder, der er tilsluttet centerets netsikkerhedstjeneste. Det vil udvide centerets muligheder for tidligt at opdage cyberangreb hos de tilsluttede organisationer. Sikkerhedssoftwaren vil kunne opdage unormal aktivitet, såsom kommandoer om at sende store mængder data til en ukendt enhed på internettet. Installation af sikkerhedssoftwaren vil være frivillig, idet dele af funktionaliteten dog i helt særlige tilfælde vil kunne pålægges visse særligt samfundsvigtige myndigheder og virksomheder.

For det fjerde er Center for Cybersikkerhed i dag begrænset i sine muligheder for at støtte myndigheder og virksomheder med at gennemføre effektive forebyggende sikkerhedstekniske undersøgelser. Dermed reduceres Center for Cybersikkerheds muligheder for at udfylde centerets rolle som national it-sikkerhedsmyndighed overfor eksempelvis myndigheder og virksomheder, der efterspørger centerets bistand til at identificere sårbarheder og vurdere robustheden af deres systemer. Derfor indebærer lovforslaget, at der indføres mulighed for, at Center for Cybersikkerhed efter aftale kan gennemføre forebyggende sikkerhedstekniske undersøgelser. Det vil give mulighed for at scanne en organisations netværk og informationssystemer og for at anvende offentligt tilgængelige oplysninger om organisationen og dens medarbejdere til at målrette simulerede angreb for at teste sikkerheden under virkelighedslignende vilkår.

For det femte har Center for Cybersikkerhed i dag kun meget begrænset mulighed for at anvende metoder, hvor centeret for eksempel kan opstille fiktive angrebsmål eller kan søge at påvirke angrebsmål eller angrebsinfrastruktur, så konsekvenserne af et igangværende angreb reduceres. Lovforslaget indebærer derfor, at der gives mulighed for, at Center for Cybersikkerhed kan anvende såkaldte honey pots, som vil kunne bruges som en form for afledningsmanøvre og kilde til viden om aktører bag angreb, og såkaldte sinkholes, som potentielt vil kunne afskære angrebsaktøren fra at styre sin angrebsplatform.

Derudover indebærer lovforslaget, at der skabes mulighed for, at Center for Cybersikkerhed gennem såkaldt edition efter rettens kendelse kan få udleveret oplysninger om brugeren af en e-mailkonto, en ip-adresse eller et domænenavn, hvis det er nødvendigt for at afdække sikkerhedshændelser. Endvidere vil de nuværende meget restriktive rammer for Center for Cybersikkerheds mulighed for at videregive data blive lempet, så det i modsætning til i dag eksempelvis bliver muligt at videregive selve den skadelige kode (malware), der ligger bag et angreb, til relevante aktører. Dertil kommer en forlængelse af slettefristerne, således at Center for Cybersikkerhed eksempelvis får mulighed for at gemme data, der er knyttet til en konkret sikkerhedshændelse, og som stammer fra indgreb i meddelelseshemmeligheden, i fem år mod de tre år, der er tilfældet i dag.

3. Lovforslagets hovedindhold

3.1. Tilslutning til netsikkerhedstjenesten

3.1.1. Gældende ret

Det følger af den gældende § 3, stk. 2, i lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed, som ændret ved lov nr. 443 af 8. maj 2018, at de øverste statsorganer samt statslige myndigheder kan blive tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste efter anmodning. Endvidere kan regioner og kommuner samt virksomheder, der er beskæftiget med samfundsvigtige funktioner, efter anmodning blive tilsluttet, såfremt Center for Cybersikkerhed konkret vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet, jf. § 3, stk. 3.

Det er således frivilligt for myndigheder og virksomheder, om de ønsker at tilslutte sig netsikkerhedstjenesten. Statslige myndigheder vil dog kunne modtage pålæg om at tilslutte sig netsikkerhedstjenesten fra de respektive ressortministre eller gennem regeringsbeslutninger.

Det er i forarbejderne til lov om Center for Cybersikkerhed – jf. Folketingstidende 2013-14, A, L 192 som fremsat, side 18 – forudsat, at regioner, kommuner og virksomheder, der tilsluttes Center for Cybersikkerheds netsikkerhedstjeneste, skal betale et årligt gebyr, som dækker centerets udgifter til tilslutning og drift af den anvendte alarmenhed. Det samme er forudsat for så vidt angår statslige myndigheder, idet hvert ministerområde dog tilbydes én vederlagsfri tilslutning.

Størrelsen af gebyret for tilsluttede regioner, kommuner og virksomheder er for 2019 fastsat i bekendtgørelse nr. 1599 af 14. december 2018 om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste. Gebyret udgør 300.000 kr. excl. moms pr. alarmenhed af typen NSS-1 og 400.000 kr. excl. moms pr. alarmenhed af typen NSS-2. De to typer af alarmenheder adskiller sig alene ved mængden af data, der kan håndteres.

Ultimo oktober 2018 er status på tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste, at godt 60 myndigheder og virksomheder er tilsluttet, heraf kun enkelte myndigheder og virksomheder, der betaler gebyr.

3.1.2. Forsvarsministeriets overvejelser

Forsvarsministeriet finder, at der er behov for at øge antallet af myndigheder og virksomheder, som er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste, med henblik på at understøtte et højt informationssikkerhedsniveau i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af.

Et øget antal af tilsluttede myndigheder og virksomheder vil sætte centeret i stand til at varsle hurtigere og bredere om trusler, ligesom et forbedret datagrundlag vil styrke centerets muligheder for at udarbejde et nationalt situationsbillede og trusselsvurderinger samt styrke centerets rådgivning til myndigheder og virksomheder om risici og passende sikkerhedstiltag.

Den nuværende ordning, hvor myndigheder og virksomheder som udgangspunkt betaler et årligt gebyr for tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste, udgør imidlertid en hindring for en øget tilslutning til netsikkerhedstjenesten. Center for Cybersikkerhed vurderer således, at størrelsen af det årlige gebyr har afholdt en række myndigheder og virksomheder fra at blive tilsluttet netsikkerhedstjenesten.

Der er behov for at sikre, at netsikkerhedstjenestens alarmenheder er udbredt til de myndigheder og private virksomheder, der har størst betydning for den infrastruktur, som samfundsvigtige funktioner er afhængige af. Set ud fra et samfundsmæssigt perspektiv er det således problematisk, at der er myndigheder og virksomheder, som ikke er tilsluttet netsikkerhedstjenesten, når der samtidig er tale om, at cyberangreb, der rammer de pågældende myndigheder og virksomheder, vil kunne have stor samfundsmæssig betydning.

Forsvarsministeriet finder på den baggrund, at der fremover ikke bør opkræves gebyr for tilslutning til netsikkerhedstjenesten. Derudover finder Forsvarsministeriet, at der bør være mulighed for i særlige tilfælde at pålægge regioner og kommuner samt særligt samfundsvigtige virksomheder at blive tilsluttet netsikkerhedstjenesten.

Det vurderes ikke, at en sådan ordning vil påvirke det private marked for it-sikkerhedsydelser negativt. Den sikkerhedsløsning, som Center for Cybersikkerhed stiller til rådighed med netsikkerhedstjenesten, er efterretningsbaseret, og kommercielle udbydere på markedet kan dermed ikke tilbyde en tilsvarende løsning. Centerets netsikkerhedstjeneste vil således aldrig kunne være et alternativ til private løsninger på området.

Netsikkerhedstjenestens ydelser udgør endvidere alene et ekstra lag af sikkerhed, som skal supplere myndighedernes og virksomhedernes øvrige it-sikkerhedsforanstaltninger. Der er således ikke tale om, at centerets løsning kan erstatte behovet for øvrige it-sikkerhedsløsninger.

Det bemærkes desuden, at hvis der i forbindelse med netsikkerhedstjenestens monitorering opstår en begrundet mistanke om en sikkerhedshændelse, vil netsikkerhedstjenestens assistance og rådgivning til den pågældende myndighed eller virksomhed ofte medføre, at der påpeges et konkret behov for at højne informationssikkerhedsniveauet hos myndigheden eller virksomheden – og dermed skabes øget efterspørgsel efter ydelser fra private it-sikkerhedsleverandører.

3.1.3. Den foreslåede ordning

Det foreslås, at der fremover ikke opkræves gebyr for tilslutning til netsikkerhedstjenesten.

Tilslutningen af regioner, kommuner og virksomheder vil – som efter den gældende ordning – ske ud fra et hensyn til statens sikkerhed. Der vil ved vurderingen af, om en myndighed eller virksomhed tilbydes tilslutning, primært blive lagt vægt på, om en tilslutning vil bidrage til at beskytte den kritiske infrastruktur samt om tilslutningen bidrager til at give Center for Cybersikkerheds situationscenter et samlet overblik over den aktuelle angrebsaktivitet mod Danmark. Tilslutning vil således – som efter den gældende ordning – forudsætte, at Center for Cybersikkerhed konkret vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet. For virksomheder forudsætter tilslutning endvidere, at den enkelte virksomhed har samfundsvigtig karakter.

For at sikre en repræsentativ tilslutning til netsikkerhedstjenesten fra de forskellige sektorer og brancher, vil tilslutning i nogle tilfælde alene blive tilbudt til én virksomhed, som i det væsentligste er repræsentativ for andre virksomheder inden for samme branche, idet det som udgangspunkt ikke er nødvendigt for Center for Cybersikkerheds opgavevaretagelse, at alle virksomheder inden for samme branche er tilsluttet. Det bemærkes i den forbindelse, at beslutningen herom altid vil blive truffet på baggrund af saglige kriterier.

Der henvises til den foreslåede § 3, stk. 5, 1. pkt., i lovforslagets § 1, nr. 1, og bemærkningerne hertil.

I forhold til den lille kreds af myndigheder og virksomheder, som er særligt samfundsvigtige, men som ikke selv vil være interesserede i en tilslutning til netsikkerhedstjenesten, heller ikke selv om en sådan tilslutning er gratis, foreslås det, at der skabes mulighed for at pålægge udvalgte virksomheder, regioner og kommuner, herunder regionalt og kommunalt ejede virksomheder, at tilslutte sig netsikkerhedstjenesten. Påbud vil alene kunne meddeles, hvis sådanne myndigheder og virksomheder har en væsentlig betydning for Danmarks kritiske infrastruktur. Et påbud om tilslutning vil kun omfatte netsikkerhedstjenestens monitoreringsaktiviteter og vil således ikke omfatte aktivt cyberforsvar, hvor der kan ske blokering af kommunikation, jf. afsnit 3.2 nedenfor.

Muligheden for at pålægge virksomheder, regioner og kommuner at tilslutte sig netsikkerhedstjenesten skal også ses i sammenhæng med forslaget om at fjerne det årlige gebyr for tilslutning til netsikkerhedstjenesten. Virksomheder, regioner og kommuner, der pålægges at blive tilsluttet netsikkerhedstjenesten, vil således ikke skulle betale gebyr herfor.

Der henvises til den foreslåede § 3, stk. 4, og stk. 5, 2. pkt., i lovforslagets § 1, nr. 1, og bemærkningerne hertil.

3.2. Aktivt cyberforsvar

3.2.1. Gældende ret

Det gældende kapitel 4 i lov om Center for Cybersikkerhed fastsætter netsikkerhedstjenestens muligheder for at foretage indgreb i meddelelseshemmeligheden i forbindelse med behandling af data hidrørende fra bl.a. tilsluttede myndigheder og virksomheder.

Center for Cybersikkerheds netsikkerhedstjeneste monitorerer i dag internettrafikken til og fra de tilsluttede myndigheder og virksomheder ved hjælp af alarmenheder, jf. beskrivelsen i afsnit 2.1 ovenfor. Alarmenhederne er passive i den forstand, at de kopierer internettrafikken, hvorefter trafikken ved hjælp af automatiserede analyseværktøjer undersøges for ondsindet aktivitet. Når den automatiserede analyse udløser en alarm, håndteres denne efterfølgende af medarbejdere i centerets netsikkerhedstjeneste.

Der er ikke i lov om Center for Cybersikkerhed taget stilling til muligheden for også at anvende aktivt cyberforsvar, hvor angreb håndteres i realtid og f.eks. blokeres.

3.2.2. Forsvarsministeriets overvejelser

Center for Cybersikkerheds monitorering af netværkstrafikken hos tilsluttede myndigheder og virksomheder giver ikke i dag de optimale muligheder for at bremse cyberangreb, inden de gør skade.

Det betyder eksempelvis, at Center for Cybersikkerhed i dag i alarmenhederne kan konstatere, at en stor mængde data sendes til en ip-adresse, der er kendt for at indgå i en angrebsaktørs infrastruktur, eller at der sendes e-mails til medarbejdere i de tilsluttede myndigheder og virksomheder, som har til formål at lokke passwords og brugernavne ud af medarbejderne (såkaldte phishing-mails). Men i disse tilfælde vil Center for Cybersikkerheds mulighed for at reagere primært bestå i en efterfølgende underretning af virksomheden eller myndigheden, som så selv skal tage de nødvendige forholdsregler. Denne tidsmæssige forsinkelse betyder, at et antal cyberangreb ikke når at blive bremset i tide.

Beskyttelsen af den samfundsvigtige infrastruktur vil derfor kunne styrkes betydeligt, hvis det passive cyberforsvar suppleres af et aktivt cyberforsvar, der kan håndtere cyberangreb i realtid.

En udvidelse af Center for Cybersikkerheds kompetencer til også at omfatte et aktivt cyberforsvar vurderes ikke at ville påvirke det private marked for it-sikkerhedsydelser negativt. Den sikkerhedsløsning, som centeret stiller til rådighed med netsikkerhedstjenesten, er således efterretningsbaseret, og kommercielle udbydere på markedet kan ikke tilbyde en tilsvarende løsning.

Centerets netsikkerhedstjeneste vil dermed aldrig kunne være et alternativ til private løsninger på området. Netsikkerhedstjenestens ydelser udgør endvidere alene et ekstra lag af sikkerhed, som skal supplere myndighedernes og virksomhedernes øvrige it-sikkerhedsforanstaltninger. Der er således ikke tale om, at centerets løsning kan erstatte behovet for øvrige it-sikkerhedsløsninger.

3.2.3. Den foreslåede ordning

Det foreslås, at der skabes et klart retligt grundlag for, at Center for Cybersikkerhed kan anvende et aktivt cyberforsvar hos de tilsluttede myndigheder og virksomheder.

Det vil indebære, at centeret – ved hjælp af en teknisk løsning – kan blokere, omdanne eller omdirigere ind- eller udgående netværkskommunikation ved konstatering af en kendt signatur på et cyberangreb. En signatur er en form for digitalt fingeraftryk, som eksempelvis kan udvikles på baggrund af en analyse af et tidligere cyberangreb. Reaktionen vil være fuldt automatiseret og foregå i realtid.

Blokering indebærer, at eksempelvis indgående phishing-mails i en konstateret kampagne kan stoppes, inden de når frem til myndigheden eller virksomheden, ligesom udgående trafik, hvor en angrebsaktør henter data fra myndigheden eller virksomheden, potentielt vil kunne bremses. I visse tilfælde vil det endvidere være muligt at uskadeliggøre kommunikationen ved f.eks. at *omdanne* en vedhæftet fil til et format, hvor den ondsindede kode ikke kan eksekveres. Derudover vil kommunikationen kunne *omdirigeres* til en separat server, hvor der kan foretages nærmere undersøgelse og håndtering. Omdirigerede data vil efter

endt undersøgelse og håndtering blive sendt videre til modtageren, såfremt undersøgelsen har vist, at der er tale om uskadelige data.

Det aktive cyberforsvar vil blive opsat til alene at reagere på kendte signaturer og andre kendte indikatorer på et cyberangreb. Dermed vil f.eks. almindelige borgeres eller virksomheders e-mails til den tilsluttede myndighed eller virksomhed som det helt klare udgangspunkt ikke blive berørt. Det vil dog kunne forekomme, at f.eks. en e-mail fra en borger, hvis computer er blevet inficeret med et kendt angrebsværktøj, og som ønsker at kommunikere med en tilsluttet myndighed eller virksomhed, bliver blokeret af systemet. Tilsvarende vil en e-mail kunne blive blokeret, hvis den fejlagtigt identificeres som inficeret.

Endvidere vil det kunne forekomme, at den tilsluttede myndigheds eller virksomheds kommunikation med et bestemt internetdomæne, hvor der er kendte indikatorer på cyberangreb, vil blive blokeret. Det vil f.eks. indebære, at medarbejdere hos den tilsluttede myndighed eller virksomhed ikke kan tilgå domænet, eller at domænet vil få begrænset funktionalitet.

Tilslutning til det aktive cyberforsvar vil altid være frivillig for myndigheder og virksomheder, der således på baggrund af information om systemets funktionalitet og risikoen for fejl vil kunne tage stilling til, om de ønsker at blive tilsluttet.

Center for Cybersikkerhed vil ikke med det aktive cyberforsvar få hjemmel til at foretage indgreb i meddelelseshemmeligheden eller analysere data ud over det, der følger af det nuværende hjemmelsgrundlag.

Der henvises til den foreslåede § 6, stk. 1, i lovforslagets § 1, nr. 3, og bemærkningerne hertil.

3.3. Sikkerhedssoftware på lokale netværk og enheder

3.3.1. Gældende ret

Center for Cybersikkerheds monitorering er i dag reguleret i §§ 4 og 5 i lov om Center for Cybersikkerhed, der forudsætter, at monitoreringen sker i forhold til netværkskommunikation.

Center for Cybersikkerhed har således ikke i dag mulighed for at foretage monitorering af enheder, f.eks. pc'ere, tilhørende en myndighed eller virksomhed, der er tilsluttet centerets netsikkerhedstjeneste.

3.3.2. Forsvarsministeriets overvejelser

Center for Cybersikkerheds netsikkerhedstjeneste monitorerer løbende aktiviteterne på tilsluttede myndigheder og virksomheders forbindelser til digitale netværk, herunder internettet, gennem opsatte alarmenheder, som er indstillet til at reagere på bestemte signaturer og andre kendte indikatorer.

Indholdet af stadig mere internettrafik bliver imidlertid utilgængeligt på grund af kryptering. Det medfører, at krypteret trafik, der er knyttet til et cyberangreb, kan passere alarmenhederne uden at udløse en alarm. Samtidig kan monitoreringen af ind- og udgående internet-

trafik ikke opdage uregelmæssigheder, som alene foregår på enkelte enheder (f.eks. pc'ere) på lokale netværk hos tilsluttede myndigheder eller virksomheder.

Dette er en stigende udfordring for Center for Cybersikkerheds mulighed for effektivt at opdage og imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder.

Forsvarsministeriet finder, at disse udfordringer ved den eksisterende monitorering af tilsluttede myndigheder og virksomheders netværkstrafik bør imødegås ved at give Center for Cybersikkerhed mulighed for også at monitorere aktiviteter på lokale enheder. Det bør ske ved at supplere centerets nuværende alarmenheder med installation af sikkerhedssoftware lokalt på de enkelte enheder, som anvendes af myndigheden eller virksomheden. Disse enheder vil f.eks. kunne være pc'ere, servere, smartphones og tablets.

Ved hjælp af sikkerhedssoftwaren vil skadelig kode, der er indeholdt i krypteret trafik, og som ellers passerer igennem alarmenhederne uden at udløse en alarm, kunne opdages på den enkelte enhed, som modtager eller afsender trafikken, og hvor der er sket afkryptering, eller hvor krypteringen endnu ikke er sket. På samme vis vil angrebsaktørers eventuelle forsøg på at hente data fra den enkelte enhed kunne opdages, også selv om der anvendes en krypteret forbindelse. Endelig vil den lokale placering af softwaren give mulighed for at opdage potentielt skadelig aktivitet på den enkelte enhed, ligesom softwaren kan anvendes til beskyttelse af netværk, der ikke er forbundet til internettet.

Det bemærkes, at anvendelsen af sikkerhedssoftware – både med passiv og aktiv funktionalitet, jf. nedenfor – vil indebære en udvidelse af Center for Cybersikkerheds muligheder for at foretage indgreb, der er omfattet af grundlovens § 72 om bl.a. undersøgelse af breve og andre papirer (elektronisk data) og brud på meddelelseshemmeligheden (kommunikation gennem e-mail og anden internetkommunikation) med henblik på at imødegå sikkerhedshændelser. Efter grundlovens § 72 kan sådanne indgreb, hvor ingen lov hjemler en særegen undtagelse, alene ske efter en retskendelse.

Hvor den nuværende monitorering via alarmenhederne pr. definition altid vil omfatte kommunikation, der sker til eller fra den enkelte myndighed eller virksomhed, og hvor monitoreringen oftest vil have karakter af indgreb i meddelelseshemmeligheden, vil der med dette initiativ også være tale om, at der tilgås data, som opbevares på en lokal enhed. Det vil i den forbindelse også kunne være aktuelt at tilgå (og kopiere) private data, som en medarbejder f.eks. har gemt på en pc, såfremt disse data har udløst en alarm eller på anden måde har givet begrundet mistanke om en sikkerhedshændelse. Disse indgreb vil kunne være omfattet af grundlovens § 72, hvorfor der vurderes at være behov for en udtrykkelig hjemmel.

Forsvarsministeriet har overvejet, om der som led i anvendelsen af sikkerhedssoftware bør etableres en ordning, hvor der sker forudgående indhentelse af retskendelse. Indgrebet vil imidlertid som udgangspunkt ske automatiseret, når sikkerhedssoftwaren løbende scanner – og dermed tilgår – filer for at identificere eventuelle sikkerhedshændelser, og da indgrebet dermed netop sker ved scanning af ukendte data for at fastslå, om der er tale om sikkerhedshændelser, vil en domstolsprøvelse i givet fald ikke kunne basere sig på en vurdering af karakteren af de pågældende data, men alene på en meget overordnet og generel vurdering af, om f.eks. trusselsbilledet i tilstrækkelig grad begrunder, at der anvendes sikkerhedssoftware. Dette område vurderes på den baggrund ikke at være egnet til domstolsprøvelse.

Centerets anvendelse af sikkerhedssoftware vurderes ikke at ville påvirke det private marked for it-sikkerhedsydelser negativt. Sikkerhedssoftwaren kan sammenlignes med kommercielle sikkerhedsprodukter, herunder bl.a. antivirus-software, idet der dog til forskel fra kommercielle produkter vil kunne søges efter de avancerede cyberangreb, som Center for Cybersikkerhed har et særligt efterretningsmæssigt kendskab til. Der findes ikke på det private marked sammenlignelige sikkerhedsydelser. Dermed vil sikkerhedssoftwaren aldrig kunne træde i stedet for de kommercielle produkter, men vil alene kunne udgøre et ekstra lag af sikkerhed.

3.3.3. Den foreslåede ordning

3.3.3.1. Sikkerhedssoftware med passiv funktionalitet

Det foreslås, at det nuværende hjemmelsgrundlag for Center for Cybersikkerhed udvides til også at omfatte monitorering af lokale enheder.

Den sikkerhedssoftware, der anvendes til monitoreringen, vil som udgangspunkt være passiv – i den forstand, at eventuelle cyberangreb ikke bremses undervejs, men blot forsøges opdaget med henblik på efterfølgende at kunne blive håndteret. Softwaren kan i så fald sammenlignes med de eksisterende alarmenheders virkemåde.

Sikkerhedssoftwaren vil løbende foretage scanninger efter kendte signaturer og andre kendte indikatorer på cyberangreb på den enhed, hvor softwaren er installeret, og på den baggrund kunne udløse en alarm. Softwaren vil endvidere kunne søge efter uregelmæssigheder i de processer, der er aktiveret på enheden eller i de netværk, som enheden er tilknyttet, med henblik på at opdage angrebsaktivitet i systemet og udløse en alarm. Begge dele vil foregå automatiseret, mens en efterfølgende behandling på baggrund af en alarm typisk vil indebære en manuel analyse.

Sikkerhedssoftwaren vil kunne videregive generelle, tekniske oplysninger om eksempelvis kørende systemprocesser og services på den enkelte enhed, hvor softwaren er installeret, til Center for Cybersikkerhed. Disse tekniske oplysninger vil ved sammenligning med oplysningerne fra andre enheder kunne bruges til at opdage afvigelser fra normalbilledet, som kan være tegn på uautoriseret aktivitet på systemet. Dermed vil der kunne opdages angreb, som endnu ikke er omfattet af en kendt signatur, og som derfor ikke normalt ville udløse en alarm.

Den foreslåede ordning vil ikke indebære en ændring af betingelserne for, hvornår Center for Cybersikkerheds medarbejdere manuelt må foretage analyse af indhold af filer og kommunikation. Medarbejdere i netsikkerhedstjenesten vil fortsat kun kunne foretage manuel behandling af sådanne data i de tilfælde, hvor der er begrundet mistanke om en sikkerhedshændelse. Forslaget indebærer således ikke, at Center for Cybersikkerhed får en generel, manuel adgang til f.eks. pc'ere hos de tilsluttede myndigheder og virksomheder, og centeret vil dermed ikke kunne tilgå indholdet af medarbejderes data, med mindre disse data har udløst en alarm eller de modtagne oplysninger om systemprocesser viser, at der er en afvigelse fra normalbilledet.

Det foreslås, at installation af sikkerhedssoftwaren vil kunne ske hos de myndigheder og virksomheder, der opfylder lov om Center for Cybersikkerheds betingelser for tilslutning til netsikkerhedstjenesten.

Anvendelse af sikkerhedssoftware vil kun ske efter aftale med den enkelte myndighed eller virksomhed, jf. dog afsnit 3.1 ovenfor om muligheden for i særlige tilfælde at give virksomheder, regioner og kommuner pålæg om installation af softwaren med dennes passive funktionalitet. Det vil fremgå af aftalen om tilslutning til netsikkerhedstjenesten, at det påhviler myndigheder og virksomheder at orientere deres medarbejdere, herunder også nye medarbejdere, om den behandling af data, der finder sted som led i Center for Cybersikkerheds monitorering ved hjælp af sikkerhedssoftware.

Forslaget omfatter kun installation af sikkerhedssoftware på myndighedens eller virksomhedens enheder. Installation af sikkerhedssoftware hos leverandører (herunder databehandlere) vil forudsætte, at der indgås aftale med leverandørerne herom. Der vil endvidere ikke kunne ske installation af sikkerhedssoftware på f.eks. private smartphones eller pc'ere, som medarbejderne anvender til at tilgå arbejdsrelaterede e-mails.

Der henvises til den foreslåede § 4 i lovforslagets § 1, nr. 3.

3.3.3.2. Sikkerhedssoftware med aktiv funktionalitet

Det foreslås endvidere, at sikkerhedssoftwaren kan anvendes i en udgave med aktiv funktionalitet, hvor der fastsættes automatiske reaktioner på bestemte alarmer. Formålet vil være at forebygge, stoppe eller begrænse cyberangreb.

En sådan reaktion vil f.eks. kunne være, at filer med bestemte typer af kendte angrebsværktøjer skal blokeres, slettes, omdirigeres eller omdannes. Sikkerhedssoftwaren vil bl.a. kunne blokere nærmere bestemte systemprocesser, som udfører et cyberangreb. En fil med kendte angrebsværktøjer vil derudover kunne omdannes til et format, hvor skadelig kode ikke kan eksekveres. I de tilfælde, hvor en angrebsaktør forsøger at hente data, vil sikkerhedssoftwaren kunne omdirigere data, således at der ikke sendes data ud af systemet.

Anvendelse af sikkerhedssoftware med aktiv funktionalitet indebærer en risiko for, at der sker fejl. Det kan eksempelvis ikke udelukkes, at blokering af en nærmere bestemt systemproces kan medføre, at dele af den pågældende organisations it-system går ned eller beskadiges. Det kan heller ikke udelukkes, at systemet ved en fejl blokerer en e-mail fra en borger på en lokal pc hos en sagsbehandler, før sagsbehandleren har konstateret, at e-mailen er modtaget.

Anvendelse af sikkerhedssoftwaren med aktiv funktionalitet vil altid være frivillig for myndigheder og virksomheder, der således på baggrund af information om softwarens funktionalitet og risikoen for fejl vil kunne tage stilling til, om anvendelse af den aktive funktionalitet ønskes.

Der henvises til den foreslåede § 6, stk. 2, jf. stk. 1, sammenholdt med den foreslåede § 4 i lovforslagets § 1, nr. 3, og bemærkningerne hertil.

3.4. Forebyggende sikkerhedstekniske undersøgelser

3.4.1. Gældende ret

Det følger af den gældende § 1, stk. 1, i lov om Center for Cybersikkerhed, at centeret har til opgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

Lov om Center for Cybersikkerhed indeholder herudover ikke en nærmere regulering af forebyggende sikkerhedstekniske undersøgelser.

3.4.2. Forsvarsministeriets overvejelser

Center for Cybersikkerhed har med det nuværende hjemmelsgrundlag kun i meget begrænset omfang mulighed for at foretage forebyggende sikkerhedstekniske undersøgelser af systemer og netværk hos myndigheder og virksomheder, som anmoder om centerets bistand hertil.

Som national it-sikkerhedsmyndighed og nationalt kompetencecenter for cybersikkerhed varetager Center for Cybersikkerhed en række opgaver af forebyggende og afhjælpende karakter. Det indebærer bl.a., at centeret rådgiver danske myndigheder og virksomheder vedrørende styrkelse af cybersikkerheden, således at modstandskraften mod cyberangreb øges. Denne forebyggende indsats er et væsentligt element i centerets løsning af sine opgaver.

Center for Cybersikkerhed oplever en stigende efterspørgsel fra myndigheder og virksomheder efter centerets bistand til at vurdere robustheden af deres digitale infrastruktur og identificere sårbarheder i systemer og netværk.

Ved udførelse af forebyggende sikkerhedstekniske undersøgelser kan centeret afdække de områder og sårbarheder, som en ondsindet angrebsaktør ville kunne udnytte til at opnå uautoriseret adgang til systemerne. En del af de sikkerhedstekniske undersøgelser kan udgøre et simuleret angreb på et informationssystem eller netværk, hvor målet er at få adgang til systemets data og funktionalitet, for derigennem at afdække og dokumentere potentielle angrebsvektorer og sårbarheder, der vil kunne udnyttes af angrebsaktører. Centeret kan på baggrund af undersøgelsen rådgive myndigheden eller virksomheden om, hvilke konkrete tiltag der kan gennemføres for at opnå et højere sikkerhedsniveau.

Der vil ofte være tilfælde, hvor det ikke kan udelukkes, at centeret i forbindelse med undersøgelsen får adgang til private data og kommunikation tilhørende brugere. Det nuværende hjemmelsgrundlag tillader imidlertid kun, at centeret foretager sikkerhedstekniske undersøgelser, hvis en adgang ikke vil indebære, at der foretages indgreb omfattet af grundlovens § 72. Det vil kun være muligt, hvor det kan fastslås, at alle data i systemerne ligger inden for myndighedens eller virksomhedens råderet, eller hvor antallet af brugere er så begrænset, at det vil være praktisk muligt at indhente samtykke fra de pågældende.

Det bemærkes i den forbindelse, at det i organisationer med flere tusinde medarbejdere ofte vil være særdeles vanskeligt at indhente samtykke fra samtlige medarbejdere. Det vil også kunne være kontraproduktivt at indhente et samtykke i forbindelse med en sikkerhedstek-

nisk undersøgelse, idet samtlige medarbejdere dermed vil være orienteret om undersøgelsen, hvilket kan føre til, at der ikke opnås et retvisende billede af sikkerhedsniveauet.

Centeret er derfor med det nuværende hjemmelsgrundlag i en række tilfælde nødt til at afslå en anmodning fra en myndighed eller virksomhed, der ønsker centerets bistand til at undersøge, i hvilket omfang deres systemer og netværk er sårbare over for cyberangreb.

Sikkerhedstekniske undersøgelser vil altid ske efter aftale med myndigheden eller virksomheden. Men for at kunne foretage sikkerhedstekniske undersøgelser uden forinden at indhente samtykke fra samtlige berørte medarbejdere, er det nødvendigt, at der tilvejebringes hjemmel til, at centeret i forbindelse med undersøgelserne kan foretage indgreb omfattet af grundlovens § 72.

De sikkerhedstekniske undersøgelser er aktiviteter, der til en vis grad kan sammenlignes med de mange områder, hvor offentlige myndigheder foretager stikprøvekontroller, og hvor det ikke sker efter forudgående retskendelse, idet en domstolsprøvelse ikke vil være meningsfuld, når der er tale om stikprøver. Når der samtidig henses til, at undersøgelsen foretages på baggrund af et samtykke fra myndigheden eller virksomheden selv – og at det således er vanskeligt at opstille et retligt kriterium, som domstolene vil kunne påse overholdelsen af – bør undersøgelsen kunne foretages uden retskendelse.

Medarbejderne hos den pågældende myndighed eller virksomhed bør ikke på forhånd blive orienteret om, at der gennemføres en sikkerhedsteknisk undersøgelse. Dette skyldes – som nævnt ovenfor – at en sådan orientering vil føre til, at der ikke opnås et retvisende billede af sikkerhedsniveauet. Myndigheder og virksomheder vil endvidere ikke mere generelt kunne orientere medarbejderne om, at der kan ske sikkerhedstekniske undersøgelser, da overvejelserne om anvendelse af sådanne undersøgelser typisk først vil ske i umiddelbar tilknytning til, at der indgås aftale med Center for Cybersikkerhed om gennemførelse af undersøgelserne. Det vil imidlertid følge af aftalen med Center for Cybersikkerhed om gennemførelse af undersøgelserne, at myndigheden eller virksomheden efterfølgende orienterer medarbejderne om, at der har været gennemført en sikkerhedsteknisk undersøgelse.

Det bemærkes, at private virksomheder i dag udbyder sikkerhedstekniske undersøgelser. Der er således ikke tale om et nyt sikkerhedsteknisk redskab. Flere offentlige myndigheder, herunder på Forsvarsministeriets område, ønsker imidlertid ikke at benytte private firmaer til at foretage sikkerhedstekniske undersøgelser, fordi myndighederne behandler sensitive oplysninger, herunder klassificerede oplysninger, som den private virksomhed vil kunne komme i besiddelse af som led i en undersøgelse. Der vil således med forslaget ikke ske en negativ påvirkning af det private marked for it-sikkerhedsydelser.

3.4.3. Den foreslåede ordning

Det foreslås, at der skabes hjemmel til, at Center for Cybersikkerhed kan gennemføre forebyggende sikkerhedstekniske undersøgelser.

Sikkerhedstekniske undersøgelser kan opdeles i tre elementer. Hovedelementet består af selve den sikkerhedstekniske undersøgelse, hvor centeret forsøger at skaffe sig adgang til den pågældende myndigheds eller virksomheds systemer og netværk. Dette element foreslås suppleret med to yderligere elementer – henholdsvis profilering og målrettede forebyg-

gelsesaktiviteter rettet mod medarbejdere m.v. – som vil forøge effekten af den sikkerhedstekniske undersøgelse.

Disse i alt tre elementer beskrives nedenfor.

3.4.3.1. Den sikkerhedstekniske undersøgelse

Selve den sikkerhedstekniske undersøgelse vil som udgangspunkt blive udført i et trindelt forløb. Undersøgelsen påbegyndes med, at der indsamles offentligt tilgængelige oplysninger om eksempelvis myndighedens eller virksomhedens opbygning, it-infrastruktur m.v. Disse oplysninger kan f.eks. bruges til at planlægge et simuleret angreb.

Der foretages herefter scanninger på ydersiden af myndighedens eller virksomhedens netværk i søgen efter åbne netværksadgange, tjenester og sårbare applikationer, herunder styresystemer, der ikke er opdateret. Selv om der ikke på dette tidspunkt foretages indtrængen i systemerne, indebærer den aktive kommunikation med netværkene en mulighed for, at myndigheden eller virksomheden nu kan opdage og bremse aktiviteterne. Det er således også et led i undersøgelsen, at myndigheden eller virksomheden kan øve sig i at opdage og imødegå indtrængen i systemerne.

Hvis der konstateres sårbarheder i myndighedens eller virksomhedens netværk eller informationssystemer, udnyttes disse til at skaffe sig adgang til systemerne. Det undersøges herefter, i hvilket omfang myndighedens eller virksomhedens data kan tilgås og hentes ud. Det undersøges endvidere, om sårbarheder kan udnyttes til at skaffe sig særlige rettigheder i systemerne, herunder administratorrettigheder, med henblik på at sikre fortsat adgang til systemerne.

Undersøgelsen afsluttes med, at de etablerede adgange og rettigheder m.v. lukkes ned. Myndigheden eller virksomheden modtager efterfølgende en tilbagemelding fra Center for Cybersikkerhed om erfaringerne fra undersøgelsen samt råd og vejledning om, hvordan informationssikkerheden kan styrkes.

Undersøgelsen er som nævnt frivillig for myndigheden eller virksomheden, og den foretages på baggrund af en aftale med disse. Der vil i den forbindelse blive fastsat en nærmere afgrænsning af formål og mål, herunder hvilke dele af forløbet, undersøgelsen skal omfatte, og hvilke områder, der eventuelt ikke må gøres til genstand for undersøgelse.

3.4.3.2. Anvendelse af offentligt tilgængelige oplysninger

Det foreslås, at den sikkerhedstekniske undersøgelse vil kunne suppleres med anvendelse af offentligt tilgængelige oplysninger til en form for social engineering. Som led i dette element søger Center for Cybersikkerhed at opnå viden om medarbejdere i myndigheden eller virksomheden gennem åbne kilder med henblik på at kunne målrette det simulerede angreb yderligere.

Det vil i praksis kunne foregå ved, at centeret – som led i den indledende del af undersøgelsen – indsamler offentligt tilgængelige oplysninger, f.eks. fra avisartikler eller åbne profiler på sociale medier, om medarbejdere. Der kan i den forbindelse kun indsamles oplysninger om medarbejderne, som er umiddelbart tilgængelige. Centeret vil desuden ikke kunne opbe-

vare følsomme oplysninger om medarbejderne, herunder oplysninger om politisk overbevisning, seksuelle forhold m.v.

Oplysningerne vil kunne anvendes af centeret til at skabe eller lette adgangen til myndighedens eller virksomhedens systemer, eksempelvis ved, at det bliver muligt at gætte medarbejdernes passwords. Det vil således kunne være relevant at indsamle oplysninger om navnet på medarbejderens ægtefælle, børn, husdyr eller fødeby, fordi disse navne erfaringsmæssigt ofte vil indgå i medarbejderens password. Oplysningerne vil endvidere kunne benyttes til at foretage målrettede forebyggelsesaktiviteter, jf. afsnit 3.4.3.3 nedenfor.

Det vil være frivilligt for myndigheden eller virksomheden, om dette element skal indgå i den konkrete sikkerhedstekniske undersøgelse.

3.4.3.3. Forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder

Det foreslås endvidere, at den sikkerhedstekniske undersøgelse vil kunne suppleres med et yderligere element af social engineering, der har til formål at skabe eller eskalere adgangen til systemerne.

Dette element vil navnlig bestå af såkaldt spear-phishing, hvor Center for Cybersikkerhed søger at målrette et simuleret angreb mod udvalgte medarbejdere.

Det vil f.eks. kunne foregå ved, at centeret – typisk på baggrund af undersøgelser af offentligt tilgængelige oplysninger – sender en e-mail til en bestemt medarbejder, hvor centeret udgiver sig for at være en kollega på den pågældende arbejdsplads. E-mailen vil være udformet på en sådan måde, at den skal få medarbejderen til at sende oplysninger til centeret, som centeret kan benytte til at skaffe sig adgang til myndighedens eller virksomhedens netværk eller opnå særlige rettigheder i systemerne, f.eks. administratorrettigheder. Det vil være kendetegnende for spear-phishing-mails, at centeret udgiver sig for at være en anden for at franarre medarbejdere bestemte oplysninger. Centeret vil dog kun udgive sig for at være medarbejdere i den myndighed eller virksomhed, der er genstand for undersøgelsen.

Dette element vil endvidere kunne indebære, at der placeres usb-nøgler eller andre eksterne medier på myndighedens eller virksomhedens område, som potentielt giver fjernadgang til systemerne, såfremt en medarbejder indsætter mediet i sin pc.

Det vil være frivilligt for myndigheden eller virksomheden, om også dette element skal indgå i den konkrete sikkerhedstekniske undersøgelse.

Det vil følge af aftalen med Center for Cybersikkerhed om gennemførelse af den sikkerhedstekniske undersøgelse, at myndigheden og virksomheden efter den sikkerhedstekniske undersøgelse er afsluttet orienterer deres medarbejdere om undersøgelsen.

Der henvises i det hele til den foreslåede § 6 a i lovforslagets § 1, nr. 4, og bemærkningerne hertil.

3.5. Anvendelse og påvirkning af angrebsmål og angrebsinfrastruktur

3.5.1. Gældende ret

Lov om Center for Cybersikkerhed regulerer ikke muligheden for, at Center for Cybersikkerhed kan anvende fiktive angrebsmål og påvirke angrebsinfrastruktur.

3.5.2. Forsvarsministeriets overvejelser

Center for Cybersikkerheds netsikkerhedstjeneste har med de nuværende alarmenheder mulighed for at opdage cyberangreb, som anvender metoder, der i forvejen er kendt af netsikkerhedstjenesten.

Centeret har imidlertid kun i meget begrænset omfang mulighed for at anvende mere offensive metoder, hvor centeret enten opstiller fiktive angrebsmål, som giver mulighed for at lære om angrebsaktørernes metoder, eller hvor centeret søger at påvirke angrebsinfrastruktur, så konsekvenserne af et igangværende cyberangreb reduceres.

Center for Cybersikkerheds evne til at beskytte den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af, vil kunne øges ved at anvende teknikker til at tilegne sig større viden om udviklingen af nye angrebsmetoder og -værktøjer, samt ved at anvende teknikker, der aktivt kan bremse eller hæmme igangværende cyberangreb.

Ved anvendelse af sådanne teknikker kan det imidlertid ikke udelukkes, at Center for Cybersikkerhed kommer i besiddelse af data, som stammer fra et cyberangreb – og hvor der dermed kan blive tale om, at centeret dels skal foretage indgreb omfattet af grundlovens § 72, dels skal behandle personoplysninger.

Forsvarsministeriet har overvejet, om der bør etableres en ordning, hvor der sker forudgående indhentelse af retskendelse. I de meget få tilfælde, hvor der som led i anvendelse og påvirkning af angrebsmål og angrebsinfrastruktur måtte opstå behov for, at Center for Cybersikkerhed tilgår data, vil det imidlertid ikke på forhånd være muligt at afdække, om centeret ved at tilgå sådanne data foretager et indgreb i meddelelseshemmeligheden og hvem indgrebet i givet fald foretages overfor. Dette vil således først kunne afdækkes, når data analyseres og det f.eks. konstateres, at der blandt store mængder tekniske oplysninger også indgår en meddelelse. En domstolsprøvelse vil således ikke kunne baseres på en vurdering af karakteren af data, men alene på en meget overordnet vurdering af, om f.eks. trusselsbilledet i tilstrækkelig grad begrunder anvendelse af fiktive angrebsmål og påvirkning af angrebsinfrastruktur, hvilket på tidspunktet for domstolsprøvelsen alene vil kunne beskrives generelt og teoretisk. Dette område vurderes på den baggrund ikke at være egnet til domstolsprøvelse.

Anvendelse af sådanne teknikker vurderes ikke at kunne påvirke det private it-sikkerhedsmarked negativt.

3.5.3. Den foreslåede ordning

Det foreslås, at Center for Cybersikkerhed gives mulighed for at anvende fiktive angrebsmål og påvirke angrebsinfrastruktur.

Lovhjemlen vil give Center for Cybersikkerhed mulighed for at gøre brug af to teknikker. For det første opsætning af fiktive angrebsmål, som er udstyret med potentielle sårbarheder, med det formål at tiltrække angrebsaktører, herunder hjemmel til at foretage indgreb omfattet af grundlovens § 72 i denne forbindelse, jf. beskrivelsen af de såkaldte honey pots i afsnit 3.5.3.1 nedenfor. For det andet overtagelse af en del af en ondsindet aktørs angrebsinfrastruktur med henblik på at standse eller begrænse et angreb, herunder hjemmel til at foretage indgreb omfattet af grundlovens § 72 i denne forbindelse, jf. beskrivelsen af de såkaldte sinkholes i afsnit 3.5.3.2 nedenfor.

Den teknologiske udvikling gør, at de konkrete tekniske metoder løbende vil skulle tilpasses angrebsaktørernes fremgangsmåder.

3.5.3.1. Anvendelse af honey pots

En honey pot er typisk et computersystem eller en server, der indeholder sårbarheder og er placeret på netværket hos et interessant angrebsmål med det formål at tiltrække sig opmærksomhed fra en angrebsaktør, der søger efter mål på netværket. En honey pot vil således kun blive opdaget af angrebsaktører, der bevidst søger efter de pågældende sårbarheder.

Dermed lokkes angrebsaktøren til at bruge sine ressourcer på at angribe et system, der er indrettet til formålet, i stedet for reelle mål på netværket. Ved at lade systemet udsætte for kompromittering kan Center for Cybersikkerhed endvidere indsamle oplysninger om angrebsaktørens færden og brug af kommandoer i systemet, herunder tilegne sig de angrebsværktøjer, som aktøren søger at placere på det sårbare system.

En honey pot fungerer dermed både som afledningsmanøvre i forsvaret af relevante netværk og som redskab til at opnå større viden om angrebsaktørens værktøjer og fokusområder. Den særlige mulighed for på en honey pot at følge med i et cyberangrebs fulde udstrækning vil kunne give Center for Cybersikkerhed en dybere indsigt i de anvendte angrebsmetoder og dermed et bedre grundlag for at styrke beskyttelsen mod cyberangreb. Tilegnelsen af konkrete angrebsværktøjer og den efterfølgende analyse af angrebsaktørens metoder m.v. kan således føre til udviklingen af nye signaturer på cyberangreb og opdatering af alarmenhederne hos tilsluttede myndigheder og virksomheder, således at lignende angrebsforsøg kan opdages.

Honey pots vil efter omstændighederne kunne opsættes på myndigheders og virksomheders egne netværk og eget udstyr, hvilket dog vil forudsætte samtykke fra de pågældende myndigheder eller virksomheder.

Der henvises til den foreslåede § 6 b i lovforslagets § 1, nr. 4, og bemærkningerne hertil.

3.5.3.2. Anvendelse af sinkholes

Ved anvendelse af et sinkhole vil Center for Cybersikkerhed registrere rettighederne til eksempelvis et domænenavn, der indgår i angrebsaktørens infrastruktur, og som ikke i forvejen er registreret, hvorefter den trafik, der ellers ville være tilgået angrebsaktøren gennem det pågældende domæne, i stedet modtages af Center for Cybersikkerhed som operatør af sinkholet.

Desuden vil centeret på tilsvarende vis kunne købe adgang til ip-adresser, der anvendes i et cyberangreb. Dermed kan centeret f.eks. modtage data, som angrebsaktøren har hentet fra en inficeret enhed, eller kommandoer, som angrebsaktøren – via domænenavnet eller ip-adressen – sender til inficerede enheder.

Centeret vil tillige kunne registrere eksempelvis en e-mailadresse eller en konto på en kommunikationsplatform, når e-mailadressen eller kontoen ikke i forvejen er registreret, hvorefter den kommunikation, der ellers ville være tilgået angrebsaktøren, i stedet modtages af Center for Cybersikkerhed. Dermed kan centeret f.eks. modtage meddelelser og andre data, som angrebsaktøren ellers skulle have modtaget fra en kompromitteret bruger eller inficeret enhed.

Centeret vil således med et sinkhole potentielt kunne afskære angrebsaktøren fra at styre dennes angrebsplatform – og dermed standse et igangværende angreb.

Eftersom teknikken potentielt vil kunne bruges til at bremse omfattende cyberangreb, vil den kunne komme en bred kreds af internetbrugere til gode. Det var f.eks. tilfældet med det meget omtalte WannaCry-angreb, der fandt sted i 2017. WannaCry var en ondsindet kode rettet mod en kendt sårbarhed i en række styresystemer fra Microsoft. Den ondsindede kode indeholdt en komponent, der krypterede udvalgte filtyper og slettede originalerne, hvorefter offeret automatisk blev opkrævet en løsesum for at få dekrypteret filerne. Den ondsindede kode havde således karakter af ransomware. Angrebet blev bremset af en privat it-sikkerhedsforsker, der identificerede et domænenavn, som blev anvendt i angrebet, men som dog ikke var blevet registreret af angrebsaktøren. Ved at registrere domænenavnet kunne it-sikkerhedsforskeren dirigere trafikken over til en server, der dermed fungerede som et såkaldt sinkhole. Det bremsede i det konkrete tilfælde angrebets spredning, og tillod samtidig forskeren at dele information om, hvem der var ramt, med relevante parter.

Der er altså tale om en sædvanlig og almindeligt anvendt procedure for f.eks. opkøb af domænenavne. Proceduren vil typisk kunne anvendes i tilfælde, hvor domænenavnet er ledigt, fordi angrebsaktøren har undladt at registrere retten til domænenavnet eller har undladt at forlænge en registrering, eller hvor angrebsaktøren har undladt at registrere en e-mailadresse eller en konto på en kommunikationsplatform. Det er derimod ikke hensigten, at Center for Cybersikkerhed skal skaffe sig uberettiget adgang til et domænenavn eller en konto på en kommunikationsplatform, f.eks. gennem hacking, eller at der skal kunne gives påbud om, at et domænenavn eller en konto overdrages til centeret.

Der henvises til den foreslåede § 6 c i lovforslagets § 1, nr. 4, og bemærkningerne hertil.

3.6. Påbud om udlevering af oplysninger på baggrund af forudgående kendelse

3.6.1. Gældende ret

De sikkerhedshændelser, som Center for Cybersikkerhed beskæftiger sig med, vil i en række tilfælde kunne være udslag af en strafbar handling (eller forsøg herpå). Der er derfor etableret et tæt samarbejde mellem centeret og politiet, herunder Politiets Efterretningstjeneste, som indebærer, at centeret videregiver oplysninger til politiet, når der er indikationer på en strafbar handling, ligesom politiet underretter centeret om sager, der kan have betydning for centerets funktion.

Efter politiets begæring kan retten efter retsplejelovens § 804 som led i efterforskningen af en strafbar lovovertrædelse pålægge en person, der ikke er mistænkt, at forevise eller udlevere en genstand, som den pågældende har rådighed over, hvis genstanden eksempelvis kan tjene som bevis i en straffesag (edition).

Bestemmelsen om edition kan bl.a. anvendes til at få oplysninger om, hvem der på et givet tidspunkt har været bruger af en specifik ip-adresse eller e-mailkonto. Hvis efterforskningen f.eks. vedrører et hackerangreb, kan sådanne oplysninger samtidig være afgørende for Center for Cybersikkerheds mulighed for at undersøge en sikkerhedshændelse. I disse situationer vil politiet ofte videregive oplysningerne til centeret. Derudover indhenter politiet også i dag editionskendelser i medfør af retsplejelovens § 804 efter anmodning fra Center for Cybersikkerhed, forudsat at sikkerhedshændelsen gøres til genstand for efterforskning hos politiet.

Center for Cybersikkerhed undersøger imidlertid sikkerhedshændelser, uanset om hændelserne er genstand for efterforskning hos politiet eller ej. Centerets formål med undersøgelserne vil være at søge at imødegå eller begrænse effekten af sikkerhedshændelserne.

Center for Cybersikkerhed har ikke i dag mulighed for at anmode retten om at pålægge personer og virksomheder at udlevere oplysninger om brugeren af en e-mailkonto, ip-adresse eller et domænenavn, selvom det måtte være nødvendigt for at afdække forhold vedrørende en sikkerhedshændelse, herunder for at kunne underrette offeret for et cyberangreb om en kompromittering af vedkommendes it-system.

3.6.2. Forsvarsministeriets overvejelser

Center for Cybersikkerhed får som udgangspunkt mistanke om en sikkerhedshændelse ved alarmer, der udløses i alarmenhederne, eller ved modtagelse af varslinger fra Forsvarets Efterretningstjeneste eller samarbejdspartnere. Centeret vil imidlertid ikke nødvendigvis have et tilstrækkeligt grundlag for at henføre aktiviteten til en bestemt angrebsaktør eller at identificere målet for et muligt angreb.

For at kunne afdække sådanne forhold har centeret typisk behov for oplysninger om brugerne af e-mailkonti, ip-adresser eller domænenavne, der knytter sig til hændelsen. Disse oplysninger vil ofte foreligge hos et teleselskab eller en webhostingvirksomhed.

Oplysninger om brugeren af en bestemt e-mailkonto, ip-adresse eller et domænenavn er ofte afgørende for at kunne vurdere karakteren og alvorligheden af en mistænkelig aktivitet. Brugeroplysningerne vil kunne anvendes til at iværksætte eventuelle relevante modforanstaltninger ved at identificere dels den infrastruktur, som angrebet udgår fra, dels målet for angrebet. Denne viden vil centeret bl.a. kunne benytte til at orientere eventuelle ofre for et cyberangreb.

Da Center for Cybersikkerhed har behov for oplysningerne med henblik på at kunne varetage centerets opgaver med at afdække og imødegå cyberangreb, finder Forsvarsministeriet, at der bør skabes en ny hjemmel til at centeret efter rettens kendelse kan få udleveret oplysninger om brugeren af en e-mailkonto, ip-adresse eller et domænenavn med henblik på at afdække sikkerhedshændelser.

Det bemærkes i øvrigt, at udlevering af oplysninger om brugeren af en e-mailkonto, ip-adresse eller et domænenavn ikke vurderes at udgøre et indgreb i meddelelseshemmeligheden.

Forslaget vurderes ikke at påvirke det private it-sikkerhedsmarked negativt.

3.6.3. Den foreslåede ordning

Det foreslås, at der skabes hjemmel til, at retten efter begæring fra Center for Cybersikkerhed ved kendelse kan pålægge personer og virksomheder, typisk teleudbydere og webhostingvirksomheder, at udlevere oplysninger om brugeren af en e-mailkonto, ip-adresse eller et domænenavn til centeret, hvis det er nødvendigt for at afdække forhold vedrørende en sikkerhedshændelse.

Forslaget omfatter ikke udlevering af øvrige oplysninger, der kan bidrage til at afdække forhold vedrørende en eventuel sikkerhedshændelse, herunder eksempelvis udlevering af logfiler eller krypteringsnøgler fra myndigheder, virksomheder eller borgere.

Den foreslåede ordning følger i det væsentligste bestemmelserne om edition i retsplejelovens kapitel 74. Den foreslåede ordning adskiller sig imidlertid ved, at der ikke skal være et krav om mistanke om en strafbar lovovertrædelse, men derimod alene krav om, at oplysningerne skal kunne medvirke til at afdække sikkerhedshændelser.

Ligesom efter retsplejelovens regler om edition vil der ikke ske underretning af den pågældende bruger af e-mailkontoen, ip-adressen eller domænenavnet, medmindre vedkommende efterfølgende sigtes af politiet. Det bemærkes dog, at de oplysninger, som Center for Cybersikkerhed vil få udleveret som led i edition, ofte vil være oplysninger om offeret for et cyberangreb. I disse situationer vil en væsentlig del af formålet med at få udleveret oplysningerne kunne være at informere den pågældende om angrebet.

Som en yderligere retssikkerhedsmæssig garanti foreslås det, at der – i modsætning til efter retsplejelovens editionsregler – beskikkes en advokat for den, som indgrebet vedrører. Advokaten vil dermed kunne varetage interessen for den bruger af eksempelvis et domænenavn, som Center for Cybersikkerhed ønsker oplysninger om.

Det bemærkes, at forslaget ikke ændrer ved den grundlæggende ansvarsfordeling mellem Center for Cybersikkerhed og politiet, herunder Politiets Efterretningstjeneste. Det vil således fortsat være politiets opgave at forebygge og efterforske strafbare forhold samt forsøg herpå, herunder i relation til cyberangreb, og centeret vil fortsat videregive oplysninger – herunder oplysninger, der er udleveret på baggrund af editionskendelse – til politiet, når der er indikationer på en formodet strafbar handling (eller et forsøg herpå). Dette indebærer, at der fortsat vil være behov for en tæt dialog mellem Center for Cybersikkerhed og politiet i forbindelse med udførelsen af deres respektive forebyggende og efterforskningsmæssige opgaver.

Der henvises til de foreslåede §§ 7 - 7 f i lovforslagets § 1, nr. 6, og bemærkningerne hertil.

3.7. Videregivelse og analyse af data

3.7.1. Gældende ret

Lov om Center for Cybersikkerhed skelner i dag mellem trafikdata og pakkedata. Pakkedata er indholdet af kommunikation (f.eks. indholdet i en e-mail, en vedhæftet fil eller data, der sendes fra et program, som er downloadet på en computer), mens trafikdata er metadata om kommunikation (f.eks. oplysninger om, hvilken ip-adresse e-mailen stammer fra eller som programmet sender data til).

Der er i loven knyttet langt strengere betingelser til behandling af pakkedata end til behandling af trafikdata. Center for Cybersikkerhed kan f.eks. efter den gældende § 16 videregive trafikdata til en række myndigheder og virksomheder, mens pakkedata som udgangspunkt kun kan videregives til én modtager, nemlig politiet.

3.7.2. Forsvarsministeriets overvejelser

De restriktive betingelser for at videregive pakkedata udgør en betydelig udfordring for Center for Cybersikkerheds muligheder for at understøtte et højt informationssikkerhedsniveau i den samfundsvigtige infrastruktur.

De nuværende videregivelsesregler for data tilvejebragt gennem indgreb i meddelelseshemmeligheden er således til hinder for, at Center for Cybersikkerhed i forbindelse med håndteringen af sikkerhedshændelser kan videregive malware indeholdt i pakkedata samt phishing-mails til andre end politiet.

De gældende regler tager dermed ikke højde for, at malware oftest vil foreligge som en del af indholdet af en kommunikation, f.eks. som en vedhæftet fil i en e-mail, ligesom links til inficerede domæner og filer i phishing-mails også er en del af indholdet. Det betyder, at behandlingen af malware og phishing-mails er omfattet af de restriktive videregivelsesregler, og at centeret derfor er forhindret i at videregive malware og phishing-mails til relevante myndigheder og virksomheder, herunder eksempelvis teleudbydere og andre netsikkerhedstjenester, der f.eks. ville kunne anvende disse data til at styrke deres eget cyberforsvar ved at stoppe tilsvarende angreb mod dem selv.

De gældende regler giver endvidere ikke mulighed for, at centeret kan videregive pakkedata til den tilsluttede myndighed eller virksomhed, som de pågældende data stammer fra, med henblik på at få bistand til at fastslå, om data reelt er ondartet. Det kan eksempelvis være relevant i tilfælde, hvor det konstateres, at myndighedens eller virksomhedens systemer reagerer på kommandoer, der potentielt kan være udtryk for angrebsaktivitet.

Derudover giver reglerne ikke mulighed for, at centeret i forbindelse med test og konfiguration af alarmenhederne kan videregive trafikdata, uden at der er begrundet mistanke om en sikkerhedshændelse, til den tilsluttede myndighed eller virksomhed med henblik på, at de kan fastslå og oplyse karakteren af de pågældende data. En sådan videregivelsesmulighed ville betyde, at centeret kunne etablere et normalbillede af netværkstrafikken til og fra de enkelte myndigheder og virksomheder, således at det ville kunne fastslås, hvornår specifikke datamønstre er en del af den rutinemæssige trafik i netværket, og hvornår der er tale om afvigelser, der kan være tegn på sikkerhedshændelser.

Endelig tager reglerne ikke højde for videregivelse af data, der stammer fra forebyggende sikkerhedstekniske undersøgelser.

3.7.3. Den foreslåede ordning

Det foreslås for det første, at de nuværende rammer for videregivelse af pakkedata fra Center for Cybersikkerhed udvides, således at centeret for det første får mulighed for at videregive den meget lille delmængde af pakkedata, som vurderes at være ondartet data i form af malware, til andre end blot politiet.

Ved malware forstås i denne sammenhæng data, hvor der er særligt bestyrket mistanke om, at data er anvendt af en angrebsaktør med det formål at forårsage et brud på informationssikkerheden. Det kan eksempelvis være selve den skadelige kode, phishing-mails eller kommandoer, der kan være udtryk for angrebsaktivitet.

Kredsen af myndigheder og virksomheder – udover politiet – som centeret vil kunne videregive data til, foreslås afgrænset på samme måde som i den gældende § 16, nr. 2, i lov om Center for Cybersikkerhed. Der vil dermed være tale om bl.a. virksomheder, der er tilsluttet netsikkerhedstjenesten, danske myndigheder og teleudbydere samt andre netsikkerhedstjenester, herunder tilsvarende netsikkerhedstjenester i Danmark og udlandet, f.eks. CERT'er, CSIRT'er, ikt-sikkerhedsmyndigheder og efterretningstjenester. Disse modtagere vil selvstændigt kunne anvende de pågældende data til at styrke cybersikkerheden, f.eks. ved at beskytte deres egne og deres kunders infrastruktur mod angreb af samme type. Desuden vil de på baggrund af de modtagne data kunne give Center for Cybersikkerhed supplerende oplysninger, herunder om f.eks. tilsvarende eller relaterede angreb, som de er bekendt med.

Der henvises til den foreslåede § 16, stk. 4, nr. 2 og 3, i lovforslagets § 1, nr. 12, og bemærkningerne hertil.

Det foreslås for det andet, at pakkedata generelt skal kunne videregives til den tilsluttede myndighed eller virksomhed, som dataene stammer fra, hvis der er begrundet mistanke om en sikkerhedshændelse.

Center for Cybersikkerheds videregivelse af data vil skulle ske i overensstemmelse med tavshedspligtsreglerne i straffelovens § 152 og §§ 152 c-152 f og forvaltningslovens § 27. Centerets videregivelse af oplysninger til en anden forvaltningsmyndighed vil desuden skulle ske i overensstemmelse med forvaltningslovens § 28.

Det bemærkes, at danske modtageres behandling – herunder videregivelse – af de pågældende data vil være underlagt de databeskyttelsesretlige regler. Offentlige myndigheder vil desuden være underlagt bl.a. de nævnte regler i forvaltningsloven om videregivelse samt forvaltningslovens og straffelovens regler om tavshedspligt.

Der henvises til den foreslåede § 16, stk. 2, nr. 2, i lovforslagets § 1, nr. 12, og bemærkningerne hertil.

Det foreslås for det tredje, at trafikdata, der stammer fra tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder, skal kunne videregives til den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører.

Der henvises til den foreslåede § 16, stk. 5, nr. 2, i lovforslagets § 1, nr. 12, og bemærkningerne hertil.

For det fjerde foreslås det, at malware, der opdages ved en tilfældighed i forbindelse med behandling af data som led i tekniske test og konfiguration af alarmenhederne, kan videregives til samme kreds af myndigheder og virksomheder, som det foreslås, at malware generelt kan videregives til.

Der henvises til den foreslåede § 16, stk. 5, nr. 1, i lovforslagets § 1, nr. 12, og bemærkningerne hertil.

For det femte foreslås det, at Center for Cybersikkerhed får adgang til at foretage manuelle analyser som led i tekniske tests og konfiguration af netsikkerhedstjenestens alarmenheder. Analysen vil kunne omfatte trafikdata og pakkedata i det omfang, det er nødvendigt for at gennemføre testen.

Der kan i forbindelse med den løbende udvikling og drift af alarmenhederne være behov for kortvarigt at tilgå trafikdata og pakkedata. For det første er der behov for, at relevante medarbejdere kan tilgå og anvende data i forbindelse med udvikling af ny funktionalitet i alarmenhederne. Som led i udviklingsarbejdet er der således behov for at teste, om en given funktionalitet reagerer efter hensigten, når den udsættes for faktiske datastrømme. For det andet er der i forbindelse med opsætning og konfiguration af alarmenhederne på tilsvarende vis behov for at sikre sig, at enhederne fungerer korrekt. Ved at kunne tilgå data vil centeret kunne konstatere, om enheden kan håndtere mængden, hastigheden og variationen af de unikke datastrømme, der hidrører fra den tilsluttede myndighed eller virksomhed.

Der henvises til den foreslåede § 15, nr. 5, i lovforslagets § 1, nr. 12, og bemærkningerne hertil.

Det bemærkes, at der endvidere foreslås tilpasninger af reglerne om Center for Cybersikkerheds hjemmel til analyse og videregivelse af data som en konsekvens af de foreslåede ordninger vedrørende sikkerhedssoftware, jf. afsnit 3.3, forebyggende sikkerhedstekniske undersøgelser, jf. afsnit 3.4, og anvendelse og påvirkning af angrebsmål og angrebsinfrastruktur, jf. afsnit 3.5.

Der henvises til de foreslåede §§ 15 og 16 i lovforslagets § 1, nr. 12, og bemærkningerne hertil.

Der vil ikke med de foreslåede ændringer af videregivelsesreglerne ske en udvidelse af Center for Cybersikkerheds mulighed for at foretage indgreb, der er omfattet af grundlovens § 72.

3.8. Frister for sletning af data

3.8.1. Gældende ret

Der gælder i medfør af § 14 i lov om Center for Cybersikkerhed en generel sletteregel for personoplysninger svarende til bestemmelsen i § 5, stk. 5, i den tidligere gældende persondatalov. Reglen indebærer, at personoplysninger skal slettes, når det ikke længere er nød-

vendigt at opbevare dem. Det følger dog af § 14, stk. 2, i lov om Center for Cybersikkerhed, at personoplysninger kan overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen.

Herudover gælder der i medfør af lovens § 17 særlige sletteregler for data, der er tilvejebragt på baggrund af indgreb i meddelelseshemmeligheden, herunder bl.a. gennem den netværksmonitorering, som centeret foretager hos myndigheder og virksomheder, der er tilsluttet centerets netsikkerhedstjeneste.

Det følger således af lovens § 17, stk. 1 og 2, at data, der er omfattet af kapitel 4 (om indgreb i meddelelseshemmeligheden), skal slettes, når formålet med behandlingen er opfyldt. Uanset, at formålet med behandlingen ikke er opfyldt, må data, der knytter sig til en sikkerhedshændelse, højst opbevares i tre år, mens data, der ikke knytter sig til en sikkerhedshændelse, højst må opbevares i 13 måneder. Den tre-årige slettefrist for data knyttet til en sikkerhedshændelse løber dog på ny, hvis data inden for den tre-årige periode igen konstateres anvendt i forbindelse med en sikkerhedshændelse.

3.8.2. Forsvarsministeriets overvejelser

De nuværende sletteregler for data, der er tilvejebragt på baggrund af indgreb i meddelelseshemmeligheden, tillader ikke i tilstrækkelig grad, at Center for Cybersikkerhed kan opbevare oplysninger, som kan bidrage til at opdage og imødegå sikkerhedshændelser.

Data, der er knyttet til en sikkerhedshændelse, f.eks. oplysninger vedrørende et forsøgt eller succesfuldt cyberangreb, anvendes efterfølgende til at udvikle signaturer (indikatorer) til alarmenhederne, således at nye angreb, der kommer fra samme kilde eller anvender samme værktøjer, kan opdages. Centeret anvender desuden sin viden om angrebsaktører og angrebsmetoder, der er tilvejebragt på baggrund af indgreb i meddelelseshemmeligheden, til at forsøge at være på forkant med nye angrebsmetoder.

Selv om angrebsmetoderne løbende udvikler sig, ses det jævnligt, at tidligere afprøvede teknikker forsøges anvendt på ny. Det ses endvidere ofte, at tidligere anvendte metoder eller delelementer heraf videreudvikles, så de genopstår i nye variationer.

Hvis en angrebsmetode ikke har været anvendt de seneste tre år, skal centeret imidlertid slette oplysningerne om metoden. Det indebærer, at centerets muligheder for at opdage, at metoden genanvendes, vanskeliggøres betydeligt. Dertil kommer, at sletning af oplysningerne vanskeliggør opdagelse af nye variationer af tidligere afprøvede metoder.

De restriktive betingelser for at opbevare data knyttet til en sikkerhedshændelse har således i en række konkrete tilfælde vist sig at udgøre en betydelig hindring for centerets effektive beskyttelse af samfundsvigtig infrastruktur.

På tilsvarende vis er den nuværende pligt til inden 13 måneder at slette data, der ikke er knyttet til en sikkerhedshændelse, uhensigtsmæssig i de tilfælde, hvor eksempelvis danske myndigheder er genstand for længerevarende angrebskampagner.

Særligt når det gælder opdagelse af avancerede cyberangreb fra statsstøttede aktører har det i forbindelse med alvorlige angreb vist sig at være af meget stor betydning for Center for Cybersikkerhed, at der skabes mulighed for, at centeret kan tilgå ældre data med henblik på at afdække angrebets iværksættelse og varighed, herunder eventuelt identificere andre ofre

for samme type angreb. Der vil her være tale om data, som ikke på det foreliggende tidspunkt er identificeret som knyttet til en sikkerhedshændelse.

Herudover tager formuleringen af den nuværende bestemmelse i lovens § 14, stk. 2, vedrørende overførsel af personoplysninger til arkiv efter reglerne i arkivlovgivningen, ikke i tilstrækkelig grad højde for, at der kan være oplysninger, som ikke (også) er personoplysninger, men som det kan være relevant at bevare for eftertiden. Det følger af arkivloven, at data kan overføres til arkiv, men i overensstemmelse med ordningen i databeskyttelsesloven bør forholdet til arkivlovgivningen tydeliggøres.

Endelig vurderes der at være behov for at kunne fastsætte nærmere regler om Center for Cybersikkerheds behandling af oplysninger, der skal bevares for eftertiden, men som af praktiske eller sikkerhedsmæssige årsager ikke kan overføres til Rigsarkivet.

3.8.3. Den foreslåede ordning

Det foreslås at udvide Center for Cybersikkerheds muligheder for at opbevare data, der stammer fra indgreb i meddelelseshemmeligheden, hvilket beskrives nærmere nedenfor.

3.8.3.1. Data, der er knyttet til en sikkerhedshændelse

For så vidt angår data, der er knyttet til en sikkerhedshændelse, foreslås det, at slettefristen udvides til fem år. Det skyldes et hensyn til at bevare Center for Cybersikkerheds viden om tidligere anvendte angrebsmetoder.

Ved fastsættelse af den foreslåede tidsgrænse er der endvidere lagt vægt på karakteren af de opbevarede data. Der er således tale om data, hvor det specifikt er konstateret, at de knytter sig til en sikkerhedshændelse.

Der henvises til den foreslåede § 17, stk. 2, nr. 1, i lovforslagets § 1, nr. 12, med tilhørende bemærkninger.

3.8.3.2. Data, der ikke er knyttet til en sikkerhedshændelse

For så vidt angår data, der ikke er knyttet til en sikkerhedshændelse, foreslås det, at slettefristen udvides til tre år for data, der stammer fra myndigheder, som i særlig grad beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold samt virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold.

Den nuværende slettefrist på 13 måneder fastholdes for data, der stammer fra øvrige myndigheder og virksomheder.

Det bemærkes i øvrigt, at data – uanset de absolutte slettefrister – fortsat vil skulle slettes i medfør af lovens § 17, stk. 1, når formålet med behandlingen efter en konkret vurdering er udtømt.

Der henvises til den foreslåede § 17, stk. 2, nr. 2, i lovforslagets § 1, nr. 12, med tilhørende bemærkninger.

3.8.3.3. Suspension af slettefristen

Som supplement til den foreslåede forlængelse af de absolutte slettefrister foreslås det endvidere, at der indføres mulighed for i helt særlige tilfælde at suspendere slettefristerne kortvarigt. Det vil indebære, at sletning kan undlades, hvis væsentlige hensyn til varetagelsen af Center for Cybersikkerheds opgaver gør det nødvendigt.

Det kan f.eks. være i tilfælde, hvor der er konstateret en sikkerhedshændelse, og hvor der er fare for, at relevant data, der endnu ikke er analyseret, ellers skal slettes i medfør af de absolutte slettefrister, før sikkerhedshændelsens fulde omfang kan afdækkes.

Det følger af ordningen, at oplysningerne skal slettes, så snart begrundelsen for at undlade sletning ikke længere er til stede.

Der henvises til den foreslåede § 17, stk. 7, i lovforslagets § 1, nr. 12, og bemærkningerne hertil.

3.8.3.4. Særlige sletteregler for visse data

Som en konsekvens af de foreslåede § 6 b og § 6 c, der skaber hjemmel til, at Center for Cybersikkerhed kan opsætte fiktive angrebsmål samt gøre brug af domænenavne og tilsvarende it-infrastruktur, som har været anvendt af en angrebsaktør, foreslås der særlige sletteregler for de data, som Center for Cybersikkerhed får adgang til ved anvendelsen af fiktive angrebsmål og overtaget angrebsinfrastruktur.

Disse data vil herefter ikke være omfattet af de almindelige sletteregler i § 17, såfremt Center for Cybersikkerhed ikke udtager data til nærmere vurdering.

Der henvises til den foreslåede § 17 a i lovforslagets § 1, nr. 12, og bemærkningerne hertil.

3.8.3.5. Forholdet til arkivlovgivningen

Det foreslås endvidere at flytte den nuværende bestemmelse om forholdet til arkivlovgivningen til kapitel 5, der omhandler forholdet til anden lovgivning. Derudover foreslås det at tydeliggøre, at bestemmelsen omfatter alle oplysninger omfattet af lov om Center for Cybersikkerhed, og ikke kun personoplysninger.

Endelig foreslås det, at der skabes hjemmel til, at der i en bekendtgørelse kan fastsættes nærmere regler om centerets behandling af oplysninger, der skal bevares for eftertiden, men som ikke kan overføres til Rigsarkivet af praktiske eller sikkerhedsmæssige årsager.

Der henvises til den foreslåede § 8 a i lovforslagets § 1, nr. 10, og bemærkningerne hertil.

3.9. Delvis undtagelse fra retssikkerhedsloven

3.9.1. Gældende ret

Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, og det følger af den gældende § 8, stk. 1, i lov om Center for Cybersikkerhed, at centerets virksomhed som udgangspunkt er undtaget fra lov om offentlighed i forvaltningen bortset fra lovens § 13. Cen-

ter for Cybersikkerheds virksomhed er endvidere undtaget fra forvaltningslovens kapitel 4-6 og fra databeskyttelsesloven og Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, jf. § 3, stk. 2, i databeskyttelsesloven, og fra lov om retshåndhævende myndigheders behandling af personoplysninger, jf. § 1, stk. 2, i lov om retshåndhævende myndigheders behandling af personoplysninger.

Med lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter (retssikkerhedsloven) er der gennemført en samlet regulering af en række spørgsmål, der vedrører tilfælde, hvor en forvaltningsmyndighed har mulighed for uden for strafferetsplejen at foretage tvangsindgreb.

Det følger af retssikkerhedslovens § 1, stk. 1, at lovens kapitel 2 og 3 finder anvendelse ved tvangsindgreb, som foretages af den offentlige forvaltning uden for strafferetsplejen, og som består i husundersøgelse eller undersøgelse eller beslaglæggelse af breve og andre papirer. Endvidere følger det af § 1, stk. 2, at lovens kapitel 3 finder anvendelse ved tvangsindgreb, som foretages af den offentlige forvaltning uden for strafferetsplejen, og som består i undersøgelse af andre lokaliteter, undersøgelse eller beslaglæggelse af andre genstande, brud på meddelelseshemmeligheden eller eftersyn eller anden undersøgelse af personer.

Center for Cybersikkerheds netsikkerhedstjeneste har efter gældende ret hjemmel til at foretage indgreb i meddelelseshemmeligheden og er derfor omfattet af reglerne i retssikkerhedslovens kapitel 3.

I retssikkerhedslovens kapitel 2 følger det af § 2, at tvangsindgreb kun må anvendes, hvis mindre indgribende foranstaltninger ikke er tilstrækkelige, og hvis indgrebet står i rimeligt forhold til formålet med indgrebet. Efter § 3 finder forvaltningslovens §§ 3-9 a, 10-18 og 22-26 (om inhabilitet, vejledning, repræsentation, partsaktindsigt, begrundelse og klagevejledning m.v.) anvendelse ved beslutninger om iværksættelse af tvangsindgreb. Efter § 4 skal en myndighed i sager om iværksættelse af tvangsindgreb, når den mundtligt eller på anden måde bliver bekendt med oplysninger om en sags faktiske grundlag eller eksterne faglige vurderinger, der er af betydning for beslutningen om iværksættelse af tvangsindgreb, snarest muligt gøre notat om indholdet af oplysningerne eller vurderingerne. Det gælder dog ikke, hvis oplysningerne eller vurderingerne i øvrigt fremgår af sagens dokumenter. En myndighed skal i sager om iværksættelse af tvangsindgreb endvidere snarest muligt tage notat om væsentlige sagsekspeditionsskridt, der ikke i øvrigt fremgår af sagens dokumenter.

Herudover følger det af § 5, at parten forud for gennemførelsen af en beslutning om iværksættelse af et tvangsindgreb skal underrettes om beslutningen. Bestemmelsen fastsætter en række krav til underretningen, herunder at underretningen skal ske skriftligt senest 14 dage, inden tvangsindgrebet gennemføres. Kravet om forudgående underretning kan fraviges helt eller delvis, bl.a. hvis forudgående underretning viser sig umulig eller er uforholdsmæssig vanskelig. Hvis en beslutning om iværksættelse af tvangsindgreb gennemføres uden forudgående underretning, skal beslutningen samtidig med gennemførelsen af indgrebet meddeles parten skriftligt.

Efter § 6 må tvangsindgreb, der foretages uden for myndighedernes embedssteder, som udgangspunkt kun foretages mod forevisning af legitimation. Efter § 7 skal tvangsindgrebet foretages så skånsomt, som omstændighederne tillader det.

Efter § 8 skal myndigheden udfærdige rapport om udførelsen af indgrebet, hvis myndigheden under gennemførelsen af et tvangsindgreb finder, at den, som indgrebet er rettet imod, har tilsidesat regler i lovgivningen m.v. Rapporten skal snarest muligt udleveres til vedkommende. Hvis myndigheden ikke finder, at den, som indgrebet er rettet imod, har tilsidesat regler i lovgivningen m.v., skal myndigheden efter stk. 2 udfærdige og udlevere en rapport om udførelsen af indgrebet, hvis en part fremsætter begæring om det.

I retssikkerhedslovens kapitel 3 følger det af § 9 bl.a., at hvis en enkeltperson eller juridisk person med rimelig grund mistænkes for at have begået en strafbar lovovertrædelse, kan tvangsindgreb over for den mistænkte med henblik på at tilvejebringe oplysninger om det eller de forhold, som mistanken omfatter, alene gennemføres efter reglerne i retsplejeloven om strafferetsplejen. Denne regel gælder dog ikke, hvis tvangsindgrebet gennemføres med henblik på at tilvejebringe oplysninger til brug for behandlingen af andre spørgsmål end fastsættelse af straf.

3.9.2. Forsvarsministeriets overvejelser

Den monitorering, som Center for Cybersikkerheds netsikkerhedstjeneste foretager efter gældende ret, er omfattet af retssikkerhedslovens kapitel 3. De indgreb i meddelelseshemmeligheden, som Center for Cybersikkerheds netsikkerhedstjeneste foretager, sker primært, når centerets alarmenheder tilgår elektronisk kommunikation for at fastslå, om kommunikationen er led i et cyberangreb.

Med lovforslaget vil Center for Cybersikkerhed også få mulighed for at foretage indgreb omfattet af grundlovens § 72, når der anvendes sikkerhedssoftware til løbende at scanne lokale enheder for tegn på cyberangreb, jf. afsnit 3.3, når der foretages forebyggende sikkerhedsundersøgelser, jf. afsnit 3.4, og når der tilgås data, som en angrebsaktør har deponeret i forbindelse med centerets anvendelse af honey pots eller sinkholes, jf. afsnit 3.5. Disse indgreb vil efter omstændighederne kunne være omfattet af retssikkerhedslovens § 1, stk. 1, hvorved både lovens kapitel 2 og 3 finder anvendelse. Særligt i forhold til centerets adgang til data, der er deponeret på honey pots eller sinkholes, vil det imidlertid være tvivlsomt, om adgang til disse data vil udgøre en husundersøgelse eller undersøgelse eller beslaglæggelse af breve og andre papirer, jf. retssikkerhedslovens § 1, stk. 1.

Kapitel 2 i retssikkerhedsloven stiller en række krav til gennemførelsen af tvangsindgreb. Forsvarsministeriet finder det naturligt at fastholde udgangspunktet om, at retssikkerhedsloven finder anvendelse på Center for Cybersikkerheds virksomhed. Det gælder ikke mindst i forhold til retssikkerhedslovens § 2 om proportionalitetsprincippet og § 7, som bl.a. fastslår, at tvangsindgrebet skal foretages så skånsomt som muligt.

Forsvarsministeriet vurderer imidlertid, at enkelte af de øvrige bestemmelser i kapitel 2 har en sådan karakter, at det ikke vil være hensigtsmæssigt, at de finder anvendelse på Center for Cybersikkerheds virksomhed. Det skyldes, at de indgreb, som foretages af Center for Cybersikkerhed, adskiller sig væsentligt fra de tvangsindgreb, der anvendes af forvaltningen ved kontrolbesøg m.v. Centerets indgreb sker som altovervejende hovedregel som led i en automatiseret (maskinel) proces, og de sker mange tusinde gange i timen. Indgrebene er endvidere karakteriserede ved, at de ikke er rettet mod konkrete borgere eller virksomheder og ikke sker som led i kontrol- eller tilsynsvirksomhed, men derimod har til formål at fremfinde tekniske oplysninger i form af angrebsværktøjer eller resultaterne af cyberangreb – med henblik på at forebygge og stoppe sådanne angreb. At fremfinde disse oplysninger for-

udsætter imidlertid, at Center for Cybersikkerhed foretager indgreb, der er omfattet af grundlovens § 72 og af retssikkerhedsloven.

De tvangsindgreb, der gennemføres af Center for Cybersikkerhed, sker ikke på baggrund af konkrete beslutninger i de enkelte tilfælde, men – for så vidt angår anvendelse af sikkerhedssoftware og sikkerhedstekniske undersøgelser – primært på baggrund af generelle aftaler med myndigheder eller virksomheder. Forsvarsministeriet finder derfor, at retssikkerhedslovens § 3 om, at forvaltningslovens §§ 3-9 a, 10-18 og 22-26 finder anvendelse ved beslutninger om iværksættelse af tvangsindgreb, ikke bør finde anvendelse for Center for Cybersikkerhed. Det bemærkes i den forbindelse, at forvaltningslovens §§ 3-6 om inhabilitet uanset dette vil finde anvendelse på de aftaler om anvendelse af sikkerhedssoftware eller udførelse af forebyggende sikkerhedstekniske undersøgelser, som indgås mellem Center for Cybersikkerhed og en myndighed eller virksomhed.

Retssikkerhedslovens § 5 fastsætter en række krav til underretning af parten i forbindelse med gennemførelse af tvangsindgreb. Derudover stiller retssikkerhedslovens § 8, stk. 2, bl.a. krav om, at der på begæring af den, som indgrebet har rettet sig imod, skal udleveres en rapport om udførelsen af indgrebet.

Når borgere og virksomheder kommunikerer med tilsluttede myndigheder og virksomheder, indgår deres data i de løbende indgreb, som foretages af Center for Cybersikkerhed. Identiteten på de borgere og virksomheder, hvis data måtte indgå i de løbende indgreb, kendes som altovervejende hovedregel ikke af Center for Cybersikkerhed, hverken før, under eller efter indgrebet. Det skal ses i lyset af, at formålet med indgrebene ikke er at tilvejebringe oplysninger om borgere eller virksomheder, ligesom formålet ikke er at indlede en sag, der involverer borgere eller virksomheder. Center for Cybersikkerheds netsikkerhedstjeneste opretter således ikke sager vedrørende borgere eller virksomheder, der kommunikerer med tilsluttede myndigheder eller virksomheder, hvorfor de ikke bliver parter i sager, ligesom netsikkerhedstjenesten ikke har til opgave at iværksætte sanktioner mod borgere eller virksomheder. I det omfang der måtte være tale om indgreb over for medarbejdere, som er ansat hos de tilsluttede myndigheder og virksomheder, henvises til beskrivelsen af kompenserende foranstaltninger nedenfor. Hertil kommer, at en stor del af de omhandlede tvangsindgreb sker på baggrund af en automatiseret proces og rent teknisk på en sådan måde, at det ikke i praksis vil være muligt forud for indgrebets gennemførelse at underrette den, som indgrebet er rettet imod, om Center for Cybersikkerheds beslutning om at gennemføre indgrebet.

Det vurderes derfor, at Center for Cybersikkerheds virksomhed bør undtages fra kravene i § 5 om underretning i forbindelse med de løbende indgreb som foretages af centerets netsikkerhedstjeneste. Det vurderes endvidere, at centerets virksomhed bør undtages fra kravet i § 8, stk. 2, hvorefter der på begæring skal udarbejdes og udleveres en rapport om det enkelte indgreb.

Det bemærkes i den forbindelse, at de hensyn, der ligger bag retssikkerhedslovens § 5, i stort omfang opfyldes på anden vis.

I forhold til anvendelsen af sikkerhedssoftware vil det således indgå som en del af tilslutningsaftalen mellem Center for Cybersikkerhed og myndigheden eller virksomheden, at der skal ske orientering af medarbejderne om monitoreringen. Medarbejderne vil således fra deres arbejdsgiver modtage forudgående information om indgrebet. I forhold til de forebyg-

gende sikkerhedstekniske undersøgelser vil det indgå som en del af aftalen med myndigheden eller virksomheden, at medarbejdere orienteres om undersøgelsen, efter at den har fundet sted. Ved centerets adgang til data, der er deponeret på honey pots eller sinkholes, er det som nævnt tvivlsomt, om adgang til disse data kan anses for omfattet af retssikkerhedslovens kapitel 2. Centerets analyse af disse data vil derudover ofte have til formål at udfinde og orientere ofrene for et cyberangreb, hvorved den pågældende myndighed, virksomhed eller borger, som data hidrører fra, i disse tilfælde vil blive orienteret om, at centeret har haft adgang til data.

3.9.3. Den foreslåede ordning

Det foreslås, at retssikkerhedslovens § 3, § 5 og § 8, stk. 2, ikke skal gælde for Center for Cybersikkerheds virksomhed.

Det foreslås i øvrigt, at orientering af de enkelte medarbejdere om indgrebene i forbindelse med anvendelse af sikkerhedssoftware og udførelse af forebyggende sikkerhedstekniske undersøgelser vil blive fastsat som led i de aftaler, der indgås mellem Center for Cybersikkerhed og virksomheden eller myndigheden. I forhold til anvendelsen af sikkerhedssoftware vil det således fremgå af tilslutningsaftalen mellem Center for Cybersikkerhed og myndigheden eller virksomheden, at det påhviler myndigheden eller virksomheden at orientere medarbejderne, herunder nytiltrådte medarbejdere, om monitoreringen. I forhold til de forebyggende sikkerhedstekniske undersøgelser vil det indgå som en del af aftalen med myndigheden eller virksomheden, at medarbejdere orienteres om undersøgelsen, efter at den har fundet sted.

Der henvises til det foreslåede § 8, stk. 1, 2. pkt., i lovforslagets § 1, nr. 8, og bemærkningerne hertil.

4. Forholdet til Den Europæiske Menneskerettighedskonvention

Efter Den Europæiske Menneskerettighedskonventions (EMRK) artikel 8, stk. 1, har enhver ret til respekt for bl.a. sit privatliv og familieliv. Det følger endvidere af artikel 8, stk. 2, at ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder.

Beskyttelsen efter artikel 8, stk. 1, omfatter både indgreb i meddelelseshemmeligheden, f.eks. monitorering af e-mailkorrespondance og internetkommunikation, samt ransagning, og offentlige myndigheders indsamling, opbevaring og anvendelse m.v. af personoplysninger generelt.

Lovforslaget indebærer, at Center for Cybersikkerhed fremadrettet vil få mulighed for i større omfang end i dag at foretage indgreb omfattet af EMRK artikel 8, stk. 1. Disse indgreb omfatter monitorering af lokale enheder ved hjælp af sikkerhedssoftware, jf. afsnit 3.3, behandling af oplysninger om medarbejdere i forbindelse med forebyggende sikkerhedstekniske undersøgelser, jf. afsnit 3.4, behandling af deponerede data i forbindelse med anvendelse af fiktive angrebsmål og påvirkning af angrebsinfrastruktur, jf. afsnit 3.5, behandling af oplysninger på baggrund af en editionskendelse, jf. afsnit 3.6, samt monitorering på baggrund af påbud om tilslutning til centerets netsikkerhedstjeneste, jf. afsnit 3.1. Derudover

indebærer lovforslaget, at der sker en vis tilpasning af de nuværende analyse-, slette- og videregivelsesregler, jf. afsnit 3.7 og 3.8.

De foreslåede tiltag skal være i overensstemmelse med EMRK artikel 8, stk. 2, hvilket indebærer, at de skal være foreskrevet ved lov, at de skal varetage et eller flere anerkendelsesværdige formål, og at de skal være nødvendige i et demokratisk samfund for at opnå det eller de omhandlede formål.

De foreslåede tiltag skal vurderes i lyset af den samlede ramme for Center for Cybersikkerheds virksomhed, således at der foretages en samlet vurdering af, om de foreslåede tiltag samt de nugældende regler for centerets virksomhed, der foreslås videreført, samlet set er i overensstemmelse med EMRK artikel 8.

Der findes en righoldig praksis fra Den Europæiske Menneskerettighedsdomstol (EMD) vedrørende indgreb i meddelelseshemmeligheden og forholdet til EMRK artikel 8. Sagerne spænder fra politiets målrettede indgreb i meddelelseshemmeligheden til efterretningstjenesternes såkaldte bulkindhentning. Det karakteristiske for den foreliggende praksis synes imidlertid at være, at den vedrører indhentning, hvor formålet er at overvåge eller udfinde nærmere bestemte målpersoner, enten ud fra et strafferetligt efterforskningshensyn eller ud fra et hensyn til statens sikkerhed.

I modsætning til ved egentlig efterretningsvirksomhed og politiets efterforskning foretager Center for Cybersikkerhed imidlertid ikke en decideret registrering af de personoplysninger, som centeret behandler, ligesom der ikke opereres med sager om enkeltpersoner. Centeret søger via netsikkerhedstjenesten primært at indsamle tekniske oplysninger, som gør det muligt at undersøge og forebygge cyberangreb. Som led i denne indsamling vil Center for Cybersikkerhed dog uundgåeligt behandle personoplysninger, fordi personoplysningerne er indeholdt i de data, som indsamles med henblik på at lokalisere de relevante tekniske oplysninger om sikkerhedshændelser. De indgreb i meddelelseshemmeligheden, som uundgåeligt foretages af centeret i forbindelse med eksempelvis monitoreringen af en myndigheds eller virksomheds netværk eller enheder, vurderes på den baggrund at indebære et mindre intensivt indgreb i privatlivet end de indgreb, der foretages med henblik på at udfinde målpersoner.

Det vurderes herefter, at de krav til lovgivning om indgreb i meddelelseshemmeligheden, som kan udledes af EMD's praksis, ikke uden videre kan overføres til lovgivning, der vedrører indgreb i meddelelseshemmeligheden som led i opretholdelsen af et højt informationssikkerhedsniveau. Som eksempel herpå kan nævnes de minimumskrav til lovgivning vedrørende indgreb i meddelelseshemmeligheden, som EMD bl.a. opstiller i præmis 231 i Roman Zakharov v. Russia af 4. december 2015. Her stilles således bl.a. krav om, at det skal fremgå af lovgivningen, hvilke kategorier af personer, som kan blive udsat for et indgreb, hvorimod Center for Cybersikkerhed, som nævnt, ikke har til formål at overvåge eller udfinde personer og dermed selvsagt ikke vil kunne angive sådanne kategorier.

I det følgende vurderes den foreslåede ordning i relation til kravene i EMRK artikel 8, stk. 2, om, at ordningen skal være foreskrevet ved lov, at ordningen skal varetage et eller flere anerkendelsesværdige formål, og at ordningen skal være nødvendig i et demokratisk samfund for at opnå det eller de omhandlede formål.

4.1. Foreskrevet ved lov

Kravet om, at indgreb skal være foreskrevet ved lov, indebærer bl.a., at loven skal være tilgængelig, og effekten heraf skal være forudsigelig for borgerne, jf. bl.a. EMD's dom Rotaru v. Romania af 4. maj 2000 (præmis 52). Domstolen har endvidere fastslået, at i relation til love vedrørende indgreb i meddelelseshemmeligheden omfatter kravet om forudsigelighed, at loven skal være klar nok til at give borgerne en tilstrækkelig indikation af de omstændigheder og betingelser, der kan medføre, at offentlige myndigheder må foretage indgreb i retten til privatliv, jf. EMD's dom Roman Zakharov v. Russia af 4. december 2015 (præmis 229).

Det vurderes, at den foreslåede ordning er forudsigelig for borgerne. De foreslåede kapitler 4 og 4 a fastslår således tydeligt, under hvilke omstændigheder Center for Cybersikkerhed må foretage indgreb omfattet af beskyttelsen af privatlivet i EMRK's artikel 8. Derudover fastsætter kapitel 6 en række krav til Center for Cybersikkerheds behandling af personoplysninger, ligesom kapitel 7 fastsætter detaljerede regler for Center for Cybersikkerheds analyse, videregivelse og sletning af data. Det vurderes således samlet, at den foreslåede ordning opfylder kravet om at være foreskrevet ved lov.

4.2. Anerkendelsesværdige formål

Ved vurderingen af, om ordningen varetager anerkendelsesværdige formål, har Forsvarsministeriet lagt vægt på, at lovforslaget bunder i et hensyn til den nationale sikkerhed, herunder sikring af et højt informationssikkerhedsniveau i den samfundsvigtige infrastruktur, og den offentlige tryghed.

Lovforslaget har således til formål at give Center for Cybersikkerhed de nødvendige muligheder for at kunne løse centerets opgaver med at opdage, analysere og bidrage til at imødegå sikkerhedshændelser, og dermed bidrage til en mere effektiv beskyttelse af den samfundsvigtige infrastruktur mod cyberangreb.

4.3. Nødvendigt i et demokratisk samfund

Det er endvidere et krav, at ordningen må anses for nødvendig i et demokratisk samfund for at forfølge de ovenfor angivne hensyn. Heri ligger, at ordningen skal opfylde proportionalitetsprincippet.

EMD anerkender, at de enkelte stater har en vis skønsmargin i relation til indretningen af ordninger, hvor der foretages indgreb i meddelelseshemmeligheden ud fra hensynet til statens sikkerhed.

Lovforslaget har som nævnt ovenfor til formål at sikre et højt informationssikkerhedsniveau i den samfundsvigtige infrastruktur ved at give Center for Cybersikkerhed de nødvendige muligheder for at kunne opdage, analysere og bidrage til at imødegå cyberangreb. Den foreslåede ordning vurderes i den forbindelse at være begrænset til det, der er nødvendigt set i lyset af den teknologiske udvikling og den meget alvorlige cybertrussel.

Domstolen fastslår, at ordninger, hvor der foretages indgreb i meddelelseshemmeligheden ud fra hensynet til statens sikkerhed, skal være underlagt tilstrækkelige og effektive sikkerhedsforanstaltninger mod eventuelt misbrug. Sådanne sikkerhedsforanstaltninger omfatter

bl.a. tilsyn, underretningsmekanismer og retsmidler. Der henvises til dommen Roman Zakharov v. Russia af 4. december 2015 (præmis 232).

Som nævnt ovenfor vurderes det, at Center for Cybersikkerheds monitorering af en myndigheds eller virksomheds netværk eller enheder indebærer et mindre intensivt indgreb omfattet af EMRK artikel 8 end de indgreb, der foretages med henblik på at udfinde målpersoner.

Den foreslåede ordning indebærer desuden, at der fortsat stilles klare krav til, hvornår Center for Cybersikkerhed må analysere og videregive data. Derudover indebærer ordningen, at der fortsat fastsættes absolutte slettefrister for Center for Cybersikkerheds opbevaring af data, der stammer fra indgreb i meddelelseshemmeligheden. Det bemærkes i den forbindelse, at de foreslåede ændringer af videregivelses- og slettereglerne samlet set ikke vurderes at have en sådan karakter, at der ved centerets behandling af personoplysninger ændres nævneværdigt på den hidtidige balance mellem på den ene side hensynet til retssikkerheden og borgernes ret til privatliv og på den anden side hensynet til at give Center for Cybersikkerhed de nødvendige muligheder for at imødegå den alvorlige cybertrussel mod Danmark.

Endelig videreføres de gældende regler om Tilsynet med Efterretningstjenesternes varetagelse af opgaven med at føre tilsyn med Center for Cybersikkerheds overholdelse af lovens regler om behandling af personoplysninger. Tilsynet med Efterretningstjenesterne er et særligt uafhængigt kontrolorgan, der agerer efter klage eller af egen drift. Tilsynet kan i forbindelse med sin tilsynsvirksomhed kræve enhver oplysning og alt materiale, der er af betydning herfor, og tilsynet har til enhver tid adgang til Center for Cybersikkerheds lokaler. Tilsynet kan endvidere afkræve centeret skriftlige udtalelser om faktiske og retlige forhold af betydning for tilsynets virksomhed. Tilsynet kan desuden afgive udtalelser overfor centeret, hvori tilsynet bl.a. kan tilkendegive sin opfattelse af, om centeret overholder reglerne om behandling af personoplysninger. Hvis centeret undtagelsesvist beslutter ikke at følge en henstilling i en udtalelse fra tilsynet, skal centeret underrette tilsynet herom og straks forelægge sagen for forsvarsministeren til afgørelse. Tilsynet vil desuden i forbindelse med behandling af klagesager vedrørende Center for Cybersikkerhed i sine afgørelser kunne give oplysninger om, at centeret har sagsbehandlet oplysninger om en klager og om indholdet af en sådan sagsbehandling.

På den baggrund vurderes det, at den foreslåede ordning opfylder proportionalitetsprincippet, og at ordningen samlet set er i overensstemmelse med EMRK artikel 8.

5. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Lovforslaget indebærer en styrkelse af Center for Cybersikkerheds netsikkerhedstjeneste samt visse følgeudgifter, bl.a. udgifter til indgrebsadvokater i forbindelse med edition. Dette er finansieret indenfor rammerne af forsvarsforlig 2018-2023, og denne del af lovforslaget har således ikke yderligere økonomiske konsekvenser for staten.

Øvrige statslige myndigheder vil som led i lovforslaget kunne få tilbudt installation af sikkerhedssoftware på lokale enheder og gennemførelse af forebyggende sikkerhedstekniske undersøgelser, hvilket vil kunne give begrænsede udgifter til myndighedernes samarbejde med Center for Cybersikkerhed i forbindelse med installation og drift af softwaren og gennemførelse af undersøgelserne. Der vil typisk være tale om udnyttelse af eksisterende personaleressourcer, og udgifterne kan således ikke kvantificeres yderligere.

Regioner, kommuner og tilhørende institutioner, der allerede er tilsluttet netsikkerhedstjenesten, vil opnå en besparelse på grund af forslaget om, at det løbende gebyr for tilslutning bortfalder. Vælger yderligere regioner, kommuner og tilhørende institutioner at blive tilsluttet netsikkerhedstjenesten, vil der for disse være begrænsede merudgifter i forhold til udgifter til samarbejde med Center for Cybersikkerhed vedrørende medvirken til netsikkerhedstjenestens opsætning og drift af hardware og software samt efterfølgende samarbejde i forbindelse med håndtering af konkrete sikkerhedshændelser.

Regioner og kommuner vil endvidere som led i lovforslaget kunne få tilbudt installation af sikkerhedssoftware på lokale enheder og gennemførelse af forebyggende sikkerhedstekniske undersøgelser, hvilket vil kunne give begrænsede udgifter til virksomhedernes samarbejde med Center for Cybersikkerhed i forbindelse med installation, drift og gennemførelse. Der vil typisk være tale om udnyttelse af eksisterende personaleressourcer, og udgifterne kan således ikke kvantificeres yderligere.

Med lovændringen får Center for Cybersikkerhed desuden mulighed for i visse tilfælde at pålægge bl.a. regioner og kommuner at blive tilsluttet netsikkerhedstjenesten. Fjernelsen af gebyret for tilslutning forventes at øge incitamentet til at tilslutte sig netsikkerhedstjenesten – og dermed mindske behovet for at give påbud om tilslutning. I det omfang der alligevel måtte blive behov for at give påbud, vil de økonomiske og administrative konsekvenser for kommunerne og regionerne vedrøre medvirken til netsikkerhedstjenestens opsætning og drift af hardware og software samt efterfølgende samarbejde i forbindelse med håndtering af konkrete sikkerhedshændelser. Det forventes, at muligheden for at give påbud til regioner, kommuner og regionalt eller kommunalt ejede selskaber maksimalt vil blive anvendt et etcifret antal gange om året. De administrative konsekvenser af loven forhandles med de kommunale og regionale parter.

6. Økonomiske og administrative konsekvenser for erhvervslivet m.v.

Erhvervsvirksomheder, der allerede er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste, vil opnå en besparelse på grund af forslaget om, at det løbende gebyr for tilslutning bortfalder. Vælger yderligere erhvervsvirksomheder at blive tilsluttet netsikkerhedstjenesten, vil der for disse være begrænsede merudgifter i forhold til udgifter til samarbejde med Center for Cybersikkerhed i forbindelse med installation, drift og gennemførelse.

Erhvervsvirksomheder vil endvidere som led i lovforslaget kunne få tilbudt installation af sikkerhedssoftware på lokale enheder og gennemførelse af forebyggende sikkerhedstekniske undersøgelser, hvilket vil kunne give begrænsede udgifter til virksomhedernes samarbejde med Center for Cybersikkerhed i forbindelse med installation, drift og gennemførelse. Der vil typisk være tale om udnyttelse af eksisterende personaleressourcer, og udgifterne kan således ikke kvantificeres yderligere.

Med lovændringen får Center for Cybersikkerhed desuden mulighed for i visse tilfælde at pålægge erhvervsvirksomheder at blive tilsluttet netsikkerhedstjenesten. Fjernelsen af gebyret for tilslutning til netsikkerhedstjenesten forventes at øge incitamentet til at tilslutte sig netsikkerhedstjenesten – og dermed mindske behovet for at give påbud om tilslutning. I det omfang der alligevel måtte blive behov for at give påbud, vil de økonomiske og administrative konsekvenser for erhvervslivet vedrøre medvirken til netsikkerhedstjenestens opsætning og drift af hardware og software samt efterfølgende samarbejde i forbindelse med håndte-

ring af konkrete sikkerhedshændelser. Det forventes, at muligheden for at give påbud til virksomheder maksimalt vil blive anvendt et et-cifret antal gange om året.

Det bemærkes i øvrigt, at lovforslaget ikke vurderes at påvirke erhvervsvirksomheders mulighed for at teste, udvikle og anvende nye digitale teknologier og forretningsmodeller. Forsvarsministeriet vurderer på den baggrund, at principperne for agil erhvervsrettet regulering ikke er relevante for nærværende lovforslag.

7. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

8. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

9. Forholdet til EU-retten

Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) finder ikke anvendelse for Center for Cybersikkerhed, idet forordningen ikke gælder for behandling af personoplysninger under udøvelse af aktiviteter, der falder udenfor EU-retten, jf. forordningens artikel 2, stk. 2, litra a.

Databeskyttelsesforordningen vil imidlertid finde anvendelse for de myndigheder og virksomheder, som er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste, eller som på anden vis anmoder om centerets bistand, eksempelvis i forbindelse med cyberangreb eller som led i forebyggende sikkerhedstekniske undersøgelser.

De tilsluttede myndigheder og virksomheder videregiver som led i samarbejdet med netsikkerhedstjenesten data, herunder personoplysninger, til Center for Cybersikkerhed. Denne videregivelse vil kunne ske indenfor rammerne af databeskyttelsesforordningen. I relation til almindelige personoplysninger henvises til databeskyttelsesforordningens artikel 6 og til forordningens præambelbetragtning 49, hvoraf det fremgår, at behandling af personoplysninger – i det omfang, det er strengt nødvendigt og forholdsmæssigt for at sikre net- og informationssikkerheden – der foretages af eksempelvis Computer Emergency Response Teams (CSIRT'er), udgør en legitim interesse for den berørte dataansvarlige.

Samme hensyn vurderes at gøre sig gældende for personoplysninger vedrørende straffedomme og lovovertrædelser omfattet af databeskyttelsesforordningens artikel 10.

I relation til behandling af særlige kategorier af personoplysninger omfattet af databeskyttelsesforordningens artikel 9, henvises til bestemmelsens stk. 2, litra g, hvorefter forbuddet mod behandling af sådanne personoplysninger ikke finder anvendelse, når behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i et rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser. Henvisningen til EU-retten eller medlemsstaternes nationale ret i artikel 9, stk. 2, litra g,

forudsætter, at behandlingen er forankret i f.eks. national ret, for at udgangspunktet i artikel 9, stk. 1, om forbud mod behandling kan fraviges. Forordningens artikel 9, stk. 2, litra g, stiller således krav om udfyldning i national ret og kan ikke uden videre anvendes som behandlingshjemmel. Der stilles imidlertid ikke krav om, at den nationale ret skal indeholde en udtrykkelig hjemmel til behandling af sådanne personoplysninger. Det vurderes på den baggrund at være tilstrækkeligt, at myndigheders og virksomheders videregivelse af personoplysninger er forudsat i lov om Center for Cybersikkerhed.

10. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslaget har i perioden fra den 7. januar 2019 til den 4. februar 2019 været sendt i høring hos følgende myndigheder og organisationer m.v.:

Advokatrådet, Akademikernes Centralorganisation (AC), Amnesty International, Brancheorganisation for Den Danske Vejgodstransport (ITD), Danske Rederier, Dansk Arbejdsgiverforening (DA), Dansk Energi, Dansk Erhverv, Dansk Internet Forum (DIFO), DANSK IT, Danske Advokater, Danske Regioner, Datatilsynet, Dansk Industri (DI), Den Danske Dommerforening, DI ITEK, DKCERT, Finans Danmark, Finanssektorens Arbejdsgiverforening, Foreningen Danske Olieberedskabslagre, Foreningen af Vandværker i Danmark, Funktionærernes og Tjenestemændenes Fællesråd (FTF), Institut for Menneskerettigheder, ISP Sikkerhedsforum, IT-Branchen, IT-Politisk Forening, Justitia, KL, Landbrug & Fødevarer, Landsorganisationen i Danmark (LO), Ledernes Hovedorganisation, Lægemiddelindustriforeningen (LIF), Procesindustriens Brancheforening, PROSA, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Rigsombudsmanden i Grønland, Rigsombudsmanden på Færøerne, Rådet for Digital Sikkerhed, samtlige byretspræsidenter, Statens IT-projektråd, Teleindustrien (TI) og Tilsynet med Efterretningstjenesterne.

11. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/Hvis nej, anfør »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/Hvis nej, anfør »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner	Regioner, kommuner og tilhørende institutioner, der allerede er tilsluttet netsikkerhedstjenesten, vil opnå en besparelse på grund af forslaget om, at det løbende gebyr for tilslutning bortfalder.	Styrkelsen af Center for Cybersikkerheds netsikkerhedstjeneste er finansieret indenfor rammerne af forsvarsforlig 2018-2023. Øvrige statslige myndigheder samt regioner, kommuner og tilhørende institutioner vil kunne få begrænsede udgifter til myndighedernes samarbejde med Center for Cybersikkerhed.

Implementeringskonsekvenser for stat, kommuner og regioner	Ingen.	For stat, kommuner og regioner vil der være begrænsede administrative konsekvenser knyttet til disse myndigheders samarbejde med Center for Cybersikkerhed.
Økonomiske konsekvenser for erhvervslivet	Erhvervsvirksomheder, der allerede er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste, vil opnå en besparelse på grund af forslaget om, at det løbende gebyr for tilslutning bortfalder.	Erhvervsvirksomheder vil kunne få begrænsede udgifter til virksomhedernes samarbejde med Center for Cybersikkerhed.
Administrative konsekvenser for erhvervslivet	Ingen.	For erhvervsvirksomheder vil der være begrænsede administrative konsekvenser knyttet til virksomhedernes samarbejde med Center for Cybersikkerhed.
Administrative konsekvenser for borgerne	Ingen.	Ingen.
Miljømæssige konsekvenser	Ingen.	Ingen.
Forholdet til EU-retten	Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) finder ikke anvendelse for Center for Cybersikkerhed, idet forordningen ikke gælder for behandling af personoplysninger under udøvelse af aktiviteter, der falder udenfor EU-retten, jf. forordningens artikel 2, stk. 2, litra a. Databeskyttelsesforordningen vil imidlertid finde anvendelse for de myndigheder og virksomheder, som er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste, eller som på anden vis anmoder om centerets bistand eksempelvis i forbindelse med cyberangreb eller som led i forebyggende sikkerhedstekniske undersøgelser. De tilsluttede myndigheder og virksomheder videregiver som led i samarbejdet med netsikkerhedstjenesten data, herunder personoplysninger, til Center for Cybersikkerhed. Denne videregivelse vil kunne ske indenfor rammerne af databeskyttelsesforordningen.	

Er i strid med de fem principper for implementering af erhvervs-rettet EU-regulering/Går videre end minimumskrav i EU-regulering (sæt X)	JA	NEJ X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Til nr. 1

Den gældende *§ 2* definerer fem centrale begreber i lov om Center for Cybersikkerhed. Det foreslås, at disse begreber videreføres uændret, men at der tilføjes yderligere to definitioner.

Nr. 1 viderefører definitionen af begrebet sikkerhedshændelse, der således fortsat defineres som en hændelse med en negativ påvirkning af tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester. Begrebet sikkerhedshændelse omfatter hændelser, der vurderes at ville kunne have den beskrevne påvirkning. Definitionen indebærer, at enhver unormal situation, der potentielt kan kompromittere informationssystemer, digitale netværk, digitale tjenester eller andre elektroniske systemer eller data, der lagres, processeres eller transmitteres af disse systemer, vil være at betragte som en sikkerhedshændelse.

Begrebet omfatter data, informationssystemer, digitale netværk og digitale tjenester. Også hændelser, som rammer netværk, der ikke er forbundet til internettet, kan have karakter af sikkerhedshændelser.

Et eksempel på en sikkerhedshændelse, der negativt påvirker tilgængeligheden af en digital tjeneste, er et overbelastningsangreb (denial-of-service angreb), hvor f.eks. en hjemmeside rammes af et stort antal forespørgsler, så brugere ikke kan få adgang til hjemmesiden. En sikkerhedshændelse, der negativt påvirker integriteten af såvel data som et informationssystem, kan eksempelvis være indtrængen i en database, hvor oplysninger ændres uden databaseejerens vidende. En sikkerhedshændelse, der negativt påvirker fortroligheden af et informationssystem, kan være en såkaldt »trojansk hest«, hvor der installeres et program på en myndigheds informationssystem, som muliggør uautoriseret kopiering af data fra myndigheden.

Definitionen af begrebet sikkerhedshændelse omfatter alene sikkerhedshændelser på it-området og vil således f.eks. ikke omfatte andre strafbare handlinger, der ikke er knyttet til it-området (eksempelvis hærværk, tyveri eller terror).

Definitionen af begrebet pakkedata i *nr. 2* er ligeledes en uændret videreførelse. Pakkedata er således indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester. Begrebet er ikke begrænset til internetbaseret kommunikation. Det semantiske indhold af kommunikation, der transmitteres gennem digitale netværk eller tjenester, vil dermed være omfattet af begrebet pakkedata. Det kan f.eks. være indholdet af en e-mailkorrespondance eller indholdet af tilgåede hjemmesider. Derudover er det tekniske indhold af kommunikationen, f.eks. HTML- eller XML-koder, omfattet af begrebet pakkedata.

Bestanddelene af en internetkommunikation betegnes teknisk som »pakker«. Denne tekniske betegnelse er ikke identisk med betegnelsen pakkedata efter den foreslåede § 2, nr. 2. En »pakke« i teknisk forstand vil således bestå af såvel pakke- som trafikdata i lovforslagets forstand.

Det foreslåede *nr. 3* viderefører definitionen af begrebet trafikdata. Ved trafikdata forstås data, som behandles med henblik på overførsel af pakkedata. Det vil sige data, som beskriver oprindelse, destination og rutestyringsinformation, herunder oprindelsesdomænet eller den oprindelige elektroniske adresse samt anden tilsvarende information.

Trafikdata kan eksempelvis være header-informationen i digitale kommunikationsprotokoller, men vil også omfatte protokoller, der udelukkende anvendes til rute- og kommunikationsstyring, f.eks. DNS og SIP. Konkrete eksempler på trafikdata er oplysninger om ip-adresser, e-mailadresser, hjemmesideadresser, browserversioner, kommunikationens varighed og tidspunktet for kommunikationen.

Den foreslåede definition af begrebet stationære data i *nr. 4* er ny. Mens pakke- og trafikdata, jf. de foreslåede nr. 2 og 3, er knyttet til kommunikation, der sker i et netværk, er stationære data defineret som data, der opbevares på servere, cloudtjenester, pc'ere, lagerenheder, netværksenheder, mobile enheder og tilsvarende.

Eksempler på stationære data er et dokument eller et billede, som findes på en medarbejders (tjenestelige) pc, eller en database, der findes på en server hos en myndighed. Det karakteristiske for stationære data er, at de er lagret eller i øvrigt tilgængelige på en enhed – herunder »i skyen« – og ikke er et egentligt led i en igangværende kommunikation. Stationære data vil dog kunne være resultatet af en kommunikation, f.eks. hvis e-mails opbevares på en mailserver eller er blevet lagret eller fremvises på en medarbejders tjenestelige pc, ligesom stationære data teknisk set kortvarigt kan være led i en igangværende kommunikation, f.eks. det korte øjeblik, der går fra en bruger vælger at afsende en e-mail, til den forlader enhedens fysiske netværkslag. Så længe data er tilgængelig på enheden og tilgås på denne, vil de have karakter af stationære data.

Den foreslåede definition af begrebet malware i *nr. 5* er ligeledes ny. Begrebet defineres som trafikdata, pakkedata og stationære data, hvor der er særligt bestyrket mistanke om, at data er anvendt af en angrebsaktør med det formål at forårsage et brud på informationssikkerheden.

Mens trafikdata, pakkedata og stationære data omfatter data, der for langt størstedelens vedkommende er godartede data, så er der med malware tale om en meget lille delmængde af trafikdata, pakkedata og stationære data, hvor Center for Cybersikkerhed efter en konkret analyse har konkluderet, at der er særligt bestyrket mistanke om, at data er ondartet. Det vil typisk dreje sig om selve den kode, der anvendes til et angreb mod en myndighed eller virksomhed, men også den tilknyttede kommunikation, f.eks. den konkrete e-mail, der er anvendt til at fremsende den ondartede kode, eller som er anvendt til at fremsende et link til en skadelig hjemmeside.

At data skal være anvendt af en angrebsaktør indebærer ikke, at Center for Cybersikkerhed skal kunne udpege en bestemt angrebsaktør som ophavsmand til de pågældende data. Men begrebet malware vil ikke omfatte data, der utilsigtet forårsager et brud på informationssikkerheden, f.eks. på grund af en fejl i en softwareopdatering fra en leverandør, idet der i så fald ikke er tale om, at data er anvendt af en angrebsaktør.

Ved brud på informationssikkerheden forstås brud på integritet, fortrolighed eller tilgængelighed af data, informationssystemer, digitale netværk eller digitale tjenester.

Definitionen af begrebet personoplysninger i *nr. 6* er en uændret videreførelse af den gældende § 1, nr. 4. Definitionen er identisk med den definition, der tidligere var gældende efter persondatalovens § 3, nr. 1, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Definitionen af begrebet behandling i *nr. 7* er en uændret videreførelse af den gældende § 1, nr. 5. Definitionen er identisk med den definition, der tidligere var gældende efter persondatalovens § 3, nr. 2, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Der henvises i øvrigt til afsnit 3.3 og 3.4 i de almindelige bemærkninger.

Den foreslåede *§ 3* er en delvis videreførelse af den gældende § 3, og bestemmelsen vil fortsat fastsætte de overordnede rammer for Center for Cybersikkerheds netsikkerhedstjeneste.

Det foreslåede *stk. 1* beskriver, at netsikkerhedstjenestens opgave er at opdage, analysere og bidrage til at imødegå sikkerhedshændelser. Dette er indholdsmæssigt en uændret videreførelse af den gældende bestemmelse.

Netsikkerhedstjenesten er betegnelsen for Center for Cybersikkerheds samlede aktiviteter i forbindelse med at opdage, analysere og bidrage til at imødegå sikkerhedshændelser. Netsikkerhedstjenesten omfatter således alle de kapaciteter ved Center for Cybersikkerhed, der på forskellig vis bidrager til monitoreringens gennemførelse, herunder CERT-aktiviteterne på det civile og militære område, sikkerhedstekniske aktiviteter (f.eks. forebyggende sikkerhedstekniske undersøgelser, analyse af malware og forensicundersøgelser) samt støttefunktioner.

Ved tilslutning til netsikkerhedstjenesten vil der som hidtil blive indgået en tilslutningsaftale, der nærmere regulerer specifikke forhold i relationen mellem netsikkerhedstjenesten og den enkelte tilsluttede myndighed eller virksomhed. En tilslutningsaftale kan være tidsbegrænset, og der er ikke nogen nedre grænse for aftalens varighed. Tilslutningen anses for at være sket, når tilslutningsaftalen er indgået.

På Forsvarsministeriets område er det den militære it-sikkerhedsmyndighed, som pålægger myndigheder at blive tilsluttet netsikkerhedstjenesten, og på dette område indgås ikke tilslutningsaftaler. Der indgås endvidere ikke tilslutningsaftale, hvis tilslutningen sker på grundlag af et påbud efter den foreslåede § 3, stk. 4. En myndighed eller virksomhed, der er tilsluttet på grundlag af et påbud, vil dog til enhver tid kunne vælge i stedet at indgå en tilslutningsaftale, der herefter regulerer de specifikke forhold i relationen mellem netsikkerhedstjenesten og den pågældende myndighed eller virksomhed.

En myndighed eller virksomhed, der tilsluttes netsikkerhedstjenesten, vil modtage en sikkerhedsydelse, der aftales nærmere mellem netsikkerhedstjenesten og myndigheden eller virksomheden, og som er tilpasset den enkelte myndigheds eller virksomheds behov. Der vil eksempelvis kunne ske en monitorering af myndighedens eller virksomhedens forbindelse til internettet, således at netsikkerhedstjenesten ved hjælp af en lokalt placeret alarmenhed kan opdage og analysere sikkerhedshændelser, og der vil kunne installeres sikkerhedssoftware på lokale enheder. På den baggrund – og på baggrund af tilsvarende analyser hos de øvrige tilsluttede myndigheder og virksomheder – kan netsikkerhedstjenesten dels alarmere myndigheden eller virksomheden, når der konstateres konkrete sikkerhedshændelser, dels

udsende mere generelle varslinger. Sikkerhedsydelsen vil også kunne omfatte aktivt cyberforsvar, hvor netsikkerhedstjenesten blokerer, omdanner eller omdirigerer potentielt skadelige data, jf. den foreslåede § 6.

Som en særlig variant af tilslutning til netsikkerhedstjenesten kan det forekomme, at der ikke hos myndigheden eller virksomheden opsættes lokalt placerede alarmenheder eller installeres sikkerhedssoftware, men i stedet sker en løbende overførsel af logoplysninger og oplysninger om konstaterede og mulige sikkerhedshændelser fra myndighedens eller virksomhedens eget sikkerhedssystem. De data, der i så fald overføres fra myndigheden eller virksomheden til Center for Cybersikkerhed, vil have karakter af stationære data, jf. definitionen i den foreslåede § 2, nr. 4. Såfremt der er tale om en sådan løbende overførsel, anses myndigheden eller virksomheden for at være tilsluttet netsikkerhedstjenesten, og der indgås en tilslutningsaftale.

Stk. 2 er ligeledes en uændret videreførelse af den gældende bestemmelse. Efter bestemmelsen kan de øverste statsorganer samt statslige myndigheder efter anmodning blive tilsluttet netsikkerhedstjenesten.

Netsikkerhedstjenestens ydelser stilles som udgangspunkt til rådighed for statens institutioner. Som hidtil vil alle de øverste statsorganer – det vil sige Folketinget med tilhørende institutioner, regenten og domstolene – også kunne tilsluttes netsikkerhedstjenesten.

Efter det foreslåede *stk. 3* kan regioner og kommuner samt virksomheder, der har samfundsvigtig karakter, efter anmodning blive tilsluttet netsikkerhedstjenesten, såfremt Center for Cybersikkerhed konkret vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet. Den gældende bestemmelse er i det væsentligste videreført.

Kredsen af virksomheder, der kan tilsluttes, vil efter den foreslåede bestemmelse omfatte virksomheder, der har samfundsvigtig karakter. Begrebet omfatter først og fremmest de virksomheder, som efter den gældende bestemmelse kan tilsluttes netsikkerhedstjenesten, fordi de er beskæftiget med samfundsvigtige funktioner.

Ved samfundsvigtige funktioner forstås i denne sammenhæng funktioner, som er særligt vigtige for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed, herunder funktioner inden for sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet. Som eksempler på virksomheder, der har mulighed for at blive tilsluttet netsikkerhedstjenesten, kan nævnes forsyningsselskaber, teleudbydere, internetudbydere, medicinalvirksomheder, fødevarevirksomheder, virksomheder, der leverer vigtige komponenter til Forsvaret, og virksomheder, der varetager driften af administrative it-systemer for det offentlige eller for andre samfundsvigtige virksomheder.

Begrebet samfundsvigtig karakter vil imidlertid også omfatte virksomheder, som ikke i sig selv er samfundsvigtige, men som kan være vigtige ud fra et sikkerhedsperspektiv, eksempelvis fordi deres servere er blevet inficeret gennem et cyberangreb og nu anvendes som en del af en angrebsaktørs infrastruktur. Det forudsættes, at disse virksomheder, som ikke i sig selv er beskæftiget med samfundsvigtige funktioner, alene tilsluttes netsikkerhedstjenesten, så længe omstændighederne gør, at de har samfundsvigtig karakter.

Den foreslåede ændring skal ses i lyset af, at der med lovforslaget lægges op til at gå bort fra den hidtidige ordning med forskellige kriterier for tilslutning til netsikkerhedstjenesten alt efter, om der er tale om en midlertidig eller permanent tilslutning til netsikkerhedstjenesten, jf. bemærkningerne til den foreslåede § 4. Der vil således efter den foreslåede ordning både kunne ske længerevarende og midlertidig tilslutning af virksomheder, som har samfundsvigtig karakter.

Bestemmelsen omfatter alle juridiske personer, der har samfundsvigtig karakter.

I forhold til internetudbyderne og andre serviceudbydere, der har samfundsvigtig karakter, vil tilslutningen alene omfatte udbyderens egen internetadgang, eget netværk, egne pc'ere og tilsvarende. Derimod vil tilslutningen ikke omfatte trafik, der udveksles fra kunde til kunde som led i den udbudte service (medmindre der er indgået en tilslutningsaftale med den enkelte kunde). At en internetudbyder tilsluttes netsikkerhedstjenesten, indebærer således ikke, at netsikkerhedstjenesten f.eks. kan monitorere udbyderens ADSL-kunders eller hostingkunders internetkommunikation.

Da netsikkerhedstjenestens kapacitet er begrænset, foreslås det, at Center for Cybersikkerhed fortsat får hjemmel til at foretage en konkret vurdering af, om en anmodning fra en region, kommune eller virksomhed, der ønsker at blive tilsluttet netsikkerhedstjenesten, kan imødekommes. Centerets afgørelse vil blive truffet ud fra en overordnet vurdering af, om den pågældende myndigheds eller virksomheds tilslutning vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

Ved denne vurdering vil der som hidtil blive lagt vægt på netsikkerhedstjenestens aktuelle kapacitet. Der vil endvidere blive lagt vægt på, om den pågældende myndighed eller virksomhed har en it-infrastruktur, der kan udnytte fordelene ved den monitoreringsydelse, som leveres. Det forudsætter, at it-infrastrukturen er hensigtsmæssigt indrettet, at den pågældende myndighed eller virksomhed har et tilfredsstillende informationssikkerhedsniveau, og at it-driftsorganisationen har et beredskab, der kan håndtere alarmer fra netsikkerhedstjenesten.

Der vil endvidere blive lagt vægt på, at netsikkerhedstjenesten samlet set opnår en samfundsmæssigt repræsentativ dækning, således at netsikkerhedstjenesten dækker så mange forskellige sektorer, brancher, virksomhedstyper og it-teknologier som muligt, hvorved netsikkerhedstjenesten får optimale muligheder for at forebygge cyberangreb.

Såfremt Center for Cybersikkerhed ikke imødekommer en anmodning om tilslutning, vil der være tale om en afgørelse, der vil kunne påklages til Forsvarsministeriet som led i den almindelige rekursadgang, ligesom afgørelsen vil kunne indbringes for domstolene. Det bemærkes i den forbindelse, at Center for Cybersikkerheds virksomhed er undtaget fra forvaltningslovens kapitel 4-6, jf. den gældende § 8, stk. 1, men at centeret i videst muligt omfang efterlever principperne i forvaltningslovens kapitel 4-6.

Center for Cybersikkerhed vil regelmæssigt offentliggøre, hvor mange myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten efter stk. 2 og 3, samt fordelingen på sektorer.

Efter det foreslåede *stk. 4* vil Center for Cybersikkerhed i særlige tilfælde kunne påbyde virksomheder, kommuner og regioner, der har særlig samfundsvigtig karakter, at blive tilsluttet netsikkerhedstjenesten.

Den foreslåede ordning omfatter påbud om tilslutning til netsikkerhedstjenesten i form af monitorering af myndighedens eller virksomhedens netværkskommunikation samt installation af sikkerhedssoftware med passiv funktionalitet. Hvis en virksomhed eller myndighed pålægges at blive tilsluttet netsikkerhedstjenesten, vil det derimod ikke omfatte aktivt cyberforsvar, hvor der efter den foreslåede § 6 kan ske blokering, omdannelse eller omdirigering af kommunikation.

Det vil kun være aktuelt at anvende muligheden for at pålægge virksomheder og myndigheder at blive tilsluttet netsikkerhedstjenesten, hvis det ikke har været muligt på frivillig basis at indgå en tilslutningsaftale. Påbud kan således kun gives, hvis mindre indgribende tiltag ikke har været tilstrækkelige.

Center for Cybersikkerheds påbud om tilslutning til netsikkerhedstjenesten vil kunne påklages til Forsvarsministeriet som led i den almindelige rekursadgang, ligesom afgørelsen vil kunne indbringes for domstolene. Det bemærkes i den forbindelse, at Center for Cybersikkerheds virksomhed er undtaget fra forvaltningslovens kapitel 4-6, jf. den gældende § 8, stk. 1, men at centeret i videst muligt omfang efterlever principperne i forvaltningslovens kapitel 4-6.

Der henvises i øvrigt til bemærkningerne til det foreslåede stk. 5, 2. pkt., nedenfor.

Det foreslås med *stk. 5*, at forsvarsministeren kan fastsætte nærmere regler om vilkårene for tilslutning efter stk. 2 og 3. Forsvarsministeren kan desuden fastsætte nærmere regler om påbud efter stk. 4, herunder om at myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten på baggrund af et påbud, skal medvirke til netsikkerhedstjenestens opsætning og drift af hardware og software og i den forbindelse skal stille de nødvendige oplysninger om konfiguration og drift af deres digitale infrastruktur til rådighed for netsikkerhedstjenesten.

Med den foreslåede bestemmelse ændres kompetencen til fastsættelse af nærmere regler, således at de nærmere regler om vilkår for tilslutning vil skulle udstedes af forsvarsministeren og ikke som hidtil af Center for Cybersikkerhed.

Stk. 5, 1. pkt., er en delvis videreførelse af gældende ret, hvorefter forsvarsministeren kan fastsætte regler om vilkårene for tilslutning, idet der dog ikke længere vil ske opkrævning af gebyr for tilslutning. Reglerne vil bl.a. kunne regulere ejerskab til og håndtering af monitoreringsudstyr.

Efter stk. 5, 2. pkt., hvorefter forsvarsministeren kan fastsætte nærmere regler om påbud om tilslutning efter stk. 4, vil der i de regler, som udstedes i medfør af bestemmelsen, kunne fastsættes nærmere kriterier for, hvornår et påbud kan udstedes. Kun myndigheder eller virksomheder, der har en særligt samfundsvigtig karakter, vil være omfattet af ordningen.

Et væsentligt kriterium for, hvornår en myndighed eller virksomhed anses for at have særligt samfundsvigtig karakter, vil være den sektor, som myndigheden eller virksomheden indgår i. De sektorer, som er omfattet af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af

6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet), anses således for særligt samfundsvigtige. Det drejer sig om sektorerne energi, transport, bankvæsen, finansielle markedsinfrastrukturer, sundhed, drikkevandsforsyning og -distribution samt digital infrastruktur. Øvrige dele af samfundet, der ikke er omfattet af NIS-direktivet, kan dog også være særligt samfundsvigtige, herunder navnlig telesektoren, forsvarsindustrien, forskningsinstitutioner og virksomheder, der behandler beskyttelsesværdig information. Herudover vil der blive lagt vægt på kriterier som antallet af brugere, andre sektorers afhængighed af myndigheden eller virksomheden, geografisk udbredelse og de konsekvenser, som cyberangreb vil kunne have på økonomiske og samfundsmæssige aktiviteter. Myndigheder og virksomheder, som vil kunne meddeles påbud, vil eksempelvis være teleudbydere og energiselskaber, der leverer ydelser til et stort antal kunder. Det forudsættes, at påbud alene vil kunne meddeles til de myndigheder og virksomheder, der har en væsentlig betydning for Danmarks kritiske infrastruktur.

Det vil også i reglerne kunne fastsættes, at myndigheden eller virksomheden skal orientere dennes medarbejdere om, at der vil ske monitorering.

Som ved øvrige tilslutninger vil en tilslutning efter påbud alene omfatte virksomhedens eller myndighedens egen internetadgang, eget netværk, egne pc'ere og tilsvarende. Derimod vil tilslutningen ikke omfatte trafik, der udveksles fra kunde til kunde som led i services, som virksomheden eller myndigheden udbyder. Hvis f.eks. en internetudbyder får påbud om at blive tilsluttet netsikkerhedstjenesten, vil det ikke indebære, at netsikkerhedstjenesten får adgang til udbyderens ADSL-kunders eller hostingkunders internetkommunikation.

Der vil endvidere kunne fastsættes regler om, at de virksomheder og myndigheder, som får påbud om tilslutning, skal stille nødvendige oplysninger om konfiguration og drift af deres digitale infrastruktur til rådighed for Center for Cybersikkerhed. Disse oplysninger vil være en forudsætning for, at centeret kan vurdere, hvor i organisationens infrastruktur monitoreringen skal ske for at have optimal effekt. Desuden vil det kunne fastsættes, at de pågældende myndigheder og virksomheder loyalt vil skulle medvirke til gennemførelse af monitoreringen.

Det bemærkes, at Center for Cybersikkerhed ikke i medfør af bestemmelsen vil kunne få adgang til f.eks. en virksomheds lokaler uden dommerkendelse. Retsvirkningen af, at en virksomhed eller myndighed ikke efterlever et påbud om tilslutning eller ikke medvirker loyalt ved tilslutningen, vil i reglerne kunne fastsættes til bøde, jf. den foreslåede § 24 a.

Det bemærkes endvidere, at det følger af retsplejelovens § 997, stk. 3, at der i domme, hvorved nogen tilholdes at opfylde en forpligtelse mod det offentlige, som tvangsmiddel kan fastsættes en fortløbende bøde, der tilfalder statskassen. Denne mulighed for at fastsætte fortløbende bøder vil være aktuel at anvende i sager, hvor en myndighed eller virksomhed afviser at medvirke til netsikkerhedstjenestens opsætning og drift af hardware og software eller afviser at stille de nødvendige oplysninger til rådighed for netsikkerhedstjenesten.

Der henvises i øvrigt til afsnit 3.1 i de almindelige bemærkninger.

Til nr. 2

Med bestemmelsen foreslås det, at overskriften til *kapitel 4* ændres fra »Indgreb i meddelelseshemmeligheden« til »Indgreb omfattet af grundlovens § 72«.

Med ændringen tages der højde for, at der ved anvendelse af aktivt cyberforsvar, jf. den foreslåede § 6, og sikkerhedstekniske undersøgelser, jf. den foreslåede § 6 a, udover indgreb i meddelelseshemmeligheden vil kunne være tale om andre former for indgreb, der er omfattet af grundlovens § 72.

Til nr. 3

Den gældende *§ 4* giver Center for Cybersikkerheds netsikkerhedstjeneste hjemmel til at foretage indgreb i meddelelseshemmeligheden i forbindelse med behandling af pakke- og trafikdata hidrørende fra netværk hos tilsluttede myndigheder og virksomheder. Den gældende § 5 giver en tilsvarende hjemmel vedrørende pakke- og trafikdata hidrørende fra netværk hos myndigheder på Forsvarsministeriets område.

Den foreslåede nyaffattelse af § 4 indebærer, at de gældende §§ 4 og 5 samles i én bestemmelse, således at der ikke længere i bestemmelsen skelnes mellem data, der hidrører fra myndigheder på Forsvarsministeriets område, og data, der hidrører fra andre myndigheder og virksomheder. Samtidig foreslås det, at bestemmelsen udvides, så den udover pakke- og trafikdata også omfatter stationære data, ligesom bestemmelsen vil omfatte både monitorering af netværkstrafik og monitorering via lokal sikkerhedssoftware.

Efter den foreslåede bestemmelse vil Center for Cybersikkerheds netsikkerhedstjeneste uden retskendelse kunne behandle trafikdata, pakkedata og stationære data hidrørende fra tilsluttede myndigheder og virksomheder, jf. § 3, stk. 2-4, med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet.

Netsikkerhedstjenesten har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder. Netsikkerhedstjenesten varetager opgaver i forhold til tilsluttede myndigheder og virksomheder på det civile område samt myndigheder og institutioner på Forsvarsministeriets myndighedsområde. For myndigheder på Forsvarsministeriets områdes vedkommende vil opgavevaretagelsen – herunder monitorering af netværkstrafik og monitorering via lokal sikkerhedssoftware – udover i Danmark ske i udlandet forbindelse med internationale stabiliseringsindsatser og operationer.

Bestemmelsen er teknologineutral, og behandlingen vil således kunne ske med de teknologier, der aktuelt giver de bedste resultater. I dag sker der behandling af trafikdata og pakkedata i et netværk af særlige alarmenheder, der monitorerer internettrafikken ved tilsluttede myndigheder og virksomheder. Alarmenhederne kopierer internettrafikken, hvorefter trafikken ved hjælp af automatiserede analyseværktøjer undersøges for ondsartet aktivitet. Når den automatiserede analyse udløser en alarm, håndteres denne efterfølgende af medarbejdere i Center for Cybersikkerheds netsikkerhedstjeneste.

Med bestemmelsens udvidelse til også at omfatte stationære data, jf. definitionen i den foreslåede § 2, nr. 4, vil den eksisterende monitorering kunne suppleres med installation af sikkerhedssoftware lokalt på de enkelte enheder, som anvendes af myndigheden eller virksom-

heden. Disse enheder vil f.eks. kunne være pc'ere, servere, smartphones og tablets. Sikkerhedssoftwaren vil ikke i medfør af den foreslåede bestemmelse kunne anvendes til at bremse cyberangreb undervejs, men vil alene kunne anvendes til at opdage cyberangreb med henblik på, at de efterfølgende kan håndteres. Sikkerhedssoftwaren vil dog også kunne have en aktiv funktionalitet, jf. den foreslåede § 6.

Sikkerhedssoftwaren vil løbende foretage scanninger på den enhed, hvor softwaren er installeret, efter kendte signaturer eller andre indikatorer på angrebsaktivitet, hvilket i givet fald vil udløse en alarm. Softwaren vil endvidere kunne søge efter uregelmæssigheder i de processer, der er aktiveret på enheden eller i de netværk, som enheden er tilknyttet, med henblik på at opdage angrebsaktivitet i systemet og udløse en alarm. Begge dele vil foregå automatiseret, mens en efterfølgende behandling på baggrund af en alarm typisk vil indebære en manuel analyse.

Sikkerhedssoftwaren kan herudover videregive generelle, tekniske oplysninger om eksempelvis kørende systemprocesser og services på den enkelte enhed, hvor softwaren er installeret, til Center for Cybersikkerhed. Disse tekniske oplysninger vil ved sammenligning med oplysningerne fra andre enheder i samme netværk kunne bruges til at opdage afvigelser fra normalbilledet, som kan være tegn på uautoriseret aktivitet på systemet. Dermed vil der kunne opdages angreb, som endnu ikke er omfattet af en kendt signatur, og som derfor ikke udløser en alarm.

Sikkerhedssoftware vil alene kunne anvendes på myndighedens eller virksomhedens enheder. Installation af sikkerhedssoftware hos leverandører (herunder databehandlere) vil forudsætte, at der indgås aftale med leverandørerne herom, og der vil ikke ske installation af sikkerhedssoftware på f.eks. private smartphones eller pc'ere, som medarbejderne anvender til at tilgå arbejdsrelaterede e-mails.

Tilsluttede myndigheder og virksomheder vil endvidere kunne vælge at udlevere krypteringsnøgler og certifikater til netsikkerhedstjenesten med henblik på dekryptering af data i alarmenhederne. Center for Cybersikkerhed vil dog ikke kunne forlange krypteringsnøgler udleveret fra myndigheder, virksomheder eller borgere.

Endelig indebærer bestemmelsen, at Center for Cybersikkerhed hos tilsluttede myndigheder og virksomheder kan foretage indgreb, der er omfattet af grundlovens § 72, i stationære data, som myndigheden eller virksomheden stiller til rådighed for centeret. Tilsluttede myndigheder og virksomheder kan i medfør af bestemmelsen udlevere eksempelvis logfiler fra myndighedens eller virksomhedens eget sikkerhedsudstyr, herunder hardware og software. Dette kan eventuelt ske automatiseret ved løbende videregivelse af logfiler eller data fra sikkerhedshændelser til centeret.

En myndighed eller virksomhed kan eksempelvis også stille stationære data til rådighed for centeret, hvis myndigheden eller virksomheden har mistanke om, at en server, pc, smartphone eller lignende har været udsat for et cyberangreb og har behov for bistand til en nærmere undersøgelse af, om det er tilfældet. Det vil være en forudsætning, at myndigheden eller virksomheden anmoder Center for Cybersikkerhed om bistand. Der er tale om en delvis videreførelse af den ordning, der følger af den gældende § 7.

Der henvises til afsnit 3.3, herunder navnlig 3.3.3.1, i de almindelige bemærkninger om sikkerhedssoftware med passiv funktionalitet.

Efter den gældende § 7 kan Center for Cybersikkerheds netsikkerhedstjeneste ved begrundet mistanke om en sikkerhedshændelse uden retskendelse behandle data, som er indeholdt i eller hidrører fra et informationssystem, der anvendes af en myndighed eller virksomhed, når myndigheden eller virksomheden har anmodet Center for Cybersikkerhed om bistand, stillet informationssystemet eller dataene herfra til rådighed for netsikkerhedstjenesten og givet skriftligt samtykke til, at netsikkerhedstjenesten behandler dataene. Det er endvidere en forudsætning, at behandlingen vurderes at kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner er afhængige af.

Det foreslås, at bestemmelsen videreføres som ny *§ 5*. Bestemmelsen tilpasses dog, således at den i stedet for det hidtidige begreb, "data, som er indeholdt i eller hidrører fra et informationssystem", omfatter det nye begreb "stationære data", jf. definitionen i den foreslåede § 2, nr. 4.

Endvidere foreslås det, at bestemmelsen fremover kun omfatter behandlingen af stationære data fra myndigheder og virksomheder, der ikke er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste. For tilsluttede myndigheder og virksomheder reguleres adgangen til stationære data i den foreslåede § 4, jf. bemærkningerne ovenfor til denne bestemmelse.

Bestemmelsen omfatter også såkaldt incident response (bistand til håndtering af konkrete sikkerhedshændelser). Som led heri kan centeret bl.a. anvende software til analyse af de stationære data, der er stillet til rådighed for centeret af myndigheden eller virksomheden. Såfremt der herudover er behov for egentlig monitorering ved hjælp af alarmenheder eller sikkerhedssoftware, vil der skulle ske tilslutning til netsikkerhedstjenesten efter den foreslåede § 3.

Herudover foreslås en tilpasning af kriteriet i nr. 2, således at stationære data kan behandles, når behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet. Efter gældende ret er det tilsvarende kriterium, at behandlingen skal kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner er afhængige af. Med forslaget vil der gælde samme kriterium som for tilslutning til netsikkerhedstjenesten efter det foreslåede § 3, stk. 3.

Bortset herfra er der tale om en videreførelse af gældende ret.

Anvendelse af bestemmelsen forudsætter fortsat, at der er begrundet mistanke om en sikkerhedshændelse. Der vil således skulle foreligge konkrete indikationer, der peger i retning af, at en sikkerhedshændelse har fundet eller vil finde sted.

Det er efter det foreslåede *nr. 1* et krav, at myndigheden eller virksomheden har anmodet Center for Cybersikkerhed om bistand, stillet de stationære data til rådighed for netsikkerhedstjenesten og givet skriftligt samtykke til behandlingen.

Efter det foreslåede *nr. 2* er det et krav, at netsikkerhedstjenesten forud for behandlingen af data konkret skal have vurderet, at behandlingen kan bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet. I forhold til virksomheder er det således ikke et krav, at en virksomhed selv beskæftiger sig med samfundsvigtige funktioner.

Den foreslåede *§ 6* er ny og indebærer, at Center for Cybersikkerheds netsikkerhedstjeneste efter aftale med en myndighed eller virksomhed, der er tilsluttet i medfør af § 3, stk. 2 og 3, ved begrundet mistanke om en sikkerhedshændelse uden retskendelse vil kunne blokere, omdanne eller omdirigere trafikdata og pakkedata hidrørende fra netværk hos myndigheden eller virksomheden med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet.

Med bestemmelsen skabes hjemmel til, at Center for Cybersikkerhed kan anvende aktivt cyberforsvar, hvor der reageres på cyberangreb i realtid. Det skal ses i modsætning til den monitoreringsydelse, der kan tilbydes efter gældende ret og efter den foreslåede § 4, og hvor monitoreringen er passiv i den forstand, at internettrafik alene undersøges for ondartet aktivitet. Hvis der konstateres en sådan ondartet aktivitet, håndteres denne efterfølgende af medarbejdere i centerets netsikkerhedstjeneste.

Aktivt cyberforsvar efter den foreslåede bestemmelse indebærer, at centeret ved hjælp af en teknisk løsning kan blokere, omdanne eller omdirigere netværkskommunikation ved konstatering af en kendt signatur (indikator) på et cyberangreb. Reaktionen vil være fuldt automatiseret og foregå i realtid.

Blokering indebærer eksempelvis, at indgående phishing-mails i en konstateret kampagne kan stoppes, inden de når frem til myndigheden eller virksomheden, ligesom udgående trafik med data, som en angrebsaktør henter fra myndigheden eller virksomheden, potentielt vil kunne bremses. I visse tilfælde vil det endvidere være muligt at uskadeliggøre kommunikationen ved f.eks. at omdanne en vedhæftet fil til et format, hvor skadelig kode ikke kan eksekveres. En omdannelse vil imidlertid ikke indebære, at det semantiske indhold af kommunikationen ændres, uden at dette vil fremgå tydeligt, f.eks. ved en angivelse af, at et skadeligt link er slettet fra en e-mail. Derudover vil kommunikationen i visse tilfælde kunne omdirigeres til en separat server, hvor der (bl.a. manuelt) kan foretages nærmere undersøgelse og håndtering. I modsætning til blokerede data vil omdirigerede data efter endt undersøgelse og håndtering blive sendt videre til modtageren, såfremt undersøgelsen har vist, at der er tale om uskadelige data.

Ved en aktiv reaktion vil den tilsluttede myndighed eller virksomhed kunne modtage en automatisk genereret log over kommunikation, der er blevet blokeret, omdannet eller omdirigeret. Videregivelse til den tilsluttede myndighed eller virksomhed af logfiler vil, såfremt de indeholder data omfattet af kapitel 4, være reguleret af den foreslåede § 16.

Aktivt cyberforsvar vil – i modsætning til det passive cyberforsvar – indebære risiko for, at der sker fejl. På samme vis som med eksisterende kommercielle sikkerhedsløsninger kan det således ikke udelukkes, at systemet ved en fejl programmeres eller installeres på en måde, hvor ikke-skadelig netværkstrafik fejlagtigt bliver påvirket, og hvor dette påfører tredjemand eller den tilsluttede myndighed eller virksomhed et økonomisk tab. Et eventuelt erstatningsansvar for Center for Cybersikkerhed vil skulle vurderes efter de almindelige regler for offentlige myndigheders erstatningsansvar.

Det kan endvidere ikke udelukkes, at systemet ved en fejl udelukker en borger fra f.eks. at sende e-mails til de tilsluttede myndigheder. En sådan blokering vil eksempelvis kunne betyde, at en borger ikke får behandlet en ansøgningssag, eller at der bliver truffet en mangelfuld afgørelse, idet borgerens oplysninger ikke når frem til den pågældende sagsbehandler.

En e-mail, der fejlagtigt blokeres, vil imidlertid blive anset for at være kommet frem til den pågældende myndighed, hvis den er kommet frem til myndighedens netværk, men derefter er blevet blokeret af det aktive cyberforsvar – også selv om e-mailen dermed ikke er registreret som modtaget af myndigheden. Dermed vil det for myndigheden kunne udgøre en sagsbehandlingsfejl, hvis der som følge af blokeringen træffes en forvaltningsretlig afgørelse på et mangelfuldt faktuelt grundlag. En sådan sagsbehandlingsfejl vil efter omstændighederne kunne medføre afgørelsens ugyldighed og – såfremt erstatningsbetingelserne i øvrigt er opfyldt – erstatningsansvar for myndigheden. Det bemærkes for god ordens skyld, at hvis systemet blokerer en borgers e-mail, som er inficeret med malware, vil dette – uanset om den pågældende borger var uvidende om infektionen – ikke anses for at være en fejl.

Det vil være naturligt, at de tilsluttede myndigheder på deres hjemmesider i relevant omfang orienterer om, at det kan forekomme, at kommunikation blokeres af sikkerhedsmæssige årsager. Konkret vil det f.eks. kunne ske i form af en kort informationstekst, der bringes tydeligt på myndighedens kontaktside. Det bemærkes i den forbindelse, at aktivt cyberforsvar normalt ikke vil indebære, at der sker blokering af henvendelser via de kontakt- og ansøgningsformularer på myndigheders hjemmesider, hvor der alene er mulighed for at indtaste tekstbaserede oplysninger.

Tilslutning til det aktive cyberforsvar vil altid være frivillig for myndigheder og virksomheder, der således på baggrund af information om systemets funktionalitet og risikoen for fejl vil kunne tage stilling til, om de ønsker at blive tilsluttet.

Der henvises til afsnit 3.2 i de almindelige bemærkninger om et aktivt cyberforsvar.

Det foreslås med *stk. 2*, at stk. 1 finder tilsvarende anvendelse i forhold til stationære data hos tilsluttede myndigheder og virksomheder, samt at netsikkerhedstjenesten ved en konstateret sikkerhedshændelse endvidere kan slette de stationære data, der har forårsaget sikkerhedshændelsen.

I den aktive udgave vil der i sikkerhedssoftwaren kunne fastsættes automatiske reaktioner på bestemte alarmer. Formålet vil være at forebygge, stoppe eller begrænse cyberangreb.

Det kan eksempelvis være, at filer med bestemte typer af kendt angrebsaktivitet skal blokeres, slettes, omdirigeres eller omdannes. Sikkerhedssoftwaren vil bl.a. kunne blokere nærmere bestemte systemprocesser, som udfører et cyberangreb. En fil med kendte indikatorer på angrebsaktivitet vil derudover kunne omdannes til et format, hvor den skadelige kode ikke kan eksekveres. En omdannelse vil imidlertid ikke indebære, at det semantiske indhold af filen ændres, uden at dette vil fremgå tydeligt, f.eks. ved en angivelse af, at et skadeligt link er slettet fra en e-mail. I de tilfælde, hvor en angrebsaktør forsøger at hente data, vil sikkerhedssoftwaren kunne omdirigere data, således at der ikke sendes data ud af systemet. Det følger af bestemmelsen, at Center for Cybersikkerhed endvidere ved en konstateret sikkerhedshændelse kan slette de stationære data, der har forårsaget sikkerhedshændelsen.

Sikkerhedssoftwaren vil blive indrettet således, at der automatisk genereres en log over aktive reaktioner, som kan sendes til den tilsluttede myndighed eller virksomhed.

Anvendelse af sikkerhedssoftwaren i en aktiv udgave vil altid være frivillig for myndigheder og virksomheder, der således på baggrund af information om softwarens funktionalitet og risikoen for fejl vil kunne tage stilling til, om anvendelsen ønskes.

Der henvises i øvrigt til afsnit 3.3 i de almindelige bemærkninger, herunder navnlig 3.3.3.2 om sikkerhedssoftware med aktiv funktionalitet.

Til nr. 4

Den foreslåede *§ 6 a* er ny, og med bestemmelsen vil Center for Cybersikkerhed med henblik på at kunne rådgive myndigheder og virksomheder om forebyggelse af sikkerhedshændelser kunne gennemføre forebyggende sikkerhedstekniske undersøgelser, når en myndighed eller virksomhed har anmodet centeret herom.

Efter anmodning fra myndigheden eller virksomheden vil Center for Cybersikkerhed som led i den sikkerhedstekniske undersøgelse uden retskendelse kunne behandle trafikdata, pakkedata og stationære data hos myndigheden eller virksomheden samt behandle offentligt tilgængelige data om myndigheden eller virksomheden og dennes medarbejdere. Desuden vil centeret kunne iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder i myndigheden eller virksomheden.

Bestemmelsen vil give Center for Cybersikkerhed mulighed for at foretage forebyggende sikkerhedstekniske undersøgelser, hvor centeret kan afdække de områder og sårbarheder, som en angrebsaktør vil kunne udnytte til at opnå uautoriseret adgang til myndigheders og virksomheders systemer med risiko for driftsforstyrrelser og tyveri eller manipulation af data til følge. De sikkerhedstekniske undersøgelser vil altid ske efter nærmere aftale med myndigheden eller virksomheden, og de vil typisk udgøre et simuleret angreb på et informationssystem eller netværk, hvor målet er at få adgang til systemets data og funktionalitet, for derigennem at afdække og dokumentere potentielle angrebsvektorer og sårbarheder, der vil kunne udnyttes af angrebsaktører. Centeret kan på baggrund af undersøgelsen rådgive myndigheden eller virksomheden om, hvilke konkrete tiltag der kan gennemføres for at opnå et højere sikkerhedsniveau.

Den sikkerhedstekniske undersøgelse udføres som udgangspunkt i et trindelt forløb. Undersøgelsen påbegyndes med, at der indsamles eller modtages offentligt tilgængelige oplysninger om eksempelvis myndighedens eller virksomhedens opbygning, domæner m.v. Disse oplysninger kan f.eks. bruges til at planlægge et simuleret angreb.

Der foretages herefter scanninger på ydersiden af myndighedens eller virksomhedens netværk i søgen efter åbne netværksadgange, tjenester og sårbare applikationer, herunder styresystemer, der ikke er opdaterede.

Hvis der konstateres sårbarheder i organisationens netværk eller informationssystemer, udnyttes disse til at skaffe sig adgang til systemerne. Centeret vil som led heri kunne få adgang til data om eller fra myndigheden eller virksomheden og dennes medarbejdere, og det foreslås med *stk. 2, nr. 1*, at centeret efter anmodning fra myndigheden eller virksomheden uden retskendelse kan behandle trafikdata, pakkedata og stationære data hos myndigheden eller virksomheden.

Behandlingen omfatter også den efterfølgende undersøgelse af, i hvilket omfang myndighedens eller virksomhedens data kan tilgås og udtrækkes. Det undersøges endvidere, om sårbarheder kan udnyttes til at skaffe sig særlige rettigheder i systemerne, herunder administratorrettigheder, med henblik på at sikre fortsat adgang til systemerne.

Undersøgelsen afsluttes med, at de etablerede adgange og rettigheder m.v. lukkes ned. Myndigheden eller virksomheden modtager efterfølgende en tilbagemelding fra Center for Cybersikkerhed om erfaringerne fra undersøgelsen samt råd og vejledning om, hvordan informationssikkerheden kan styrkes.

Undersøgelsen er altid frivillig for myndigheden og virksomheden, og den foretages på baggrund af en aftale med denne. Der vil i den forbindelse blive fastsat en nærmere afgrænsning af formål og mål, herunder hvilke dele af forløbet, undersøgelsen skal omfatte, og hvilke områder, f.eks. specifikke databaser, der eventuelt ikke må gøres til genstand for undersøgelse. Det kan i den forbindelse aftales, at centeret gives forudgående adgang til systemerne gennem f.eks. et legitimt brugernavn og password, og dermed ikke skal forsøge at trænge ind i disse udefra, men blot undersøge, i hvilket omfang adgangen kan udnyttes til at opnå særlige rettigheder og udtrække data. Aftalen vil blive indgået med myndigheden eller virksomheden, og der vil derfor ikke blive indgået aftaler med de enkelte medarbejdere.

Efter det foreslåede *stk. 2, nr. 2*, kan Center for Cybersikkerhed endvidere efter anmodning fra myndigheden eller virksomheden behandle offentligt tilgængelige data om myndigheden eller virksomheden og dennes medarbejdere. Dermed vil det være muligt at supplere den sikkerhedstekniske undersøgelse med anvendelse af offentligt tilgængelige oplysninger til en form for social engineering. Som led i dette element søger Center for Cybersikkerhed gennem offentligt tilgængelige oplysninger at opnå viden om medarbejdere i myndigheden eller virksomheden med henblik på at kunne målrette det simulerede angreb yderligere.

Det vil i praksis kunne foregå ved, at centeret – som led i den indledende del af undersøgelsen – indsamler offentligt tilgængelige oplysninger, f.eks. fra avisartikler eller åbne profiler på sociale medier, om medarbejdere. Der kan i den forbindelse kun indsamles oplysninger, som er umiddelbart tilgængelige om medarbejderne. Derimod kan der ikke tages kontakt til medarbejderne med henblik på at opnå yderligere oplysninger, ligesom der ikke kan sendes såkaldte venne-anmodninger med henblik på at opnå et større indblik i medarbejderens profiler på sociale medier. Der kan heller ikke indsamles oplysninger om medarbejderne gennem tredjeparter eller tredjeparters profiler på sociale medier.

De indsamlede oplysninger kan anvendes af centeret til at skabe eller lette adgangen til organisationens systemer, eksempelvis ved at det bliver muligt at gætte medarbejdernes passwords. Det vil således kunne være relevant at indsamle oplysninger om navnet på en medarbejders ægtefælle, børn, husdyr eller fødeby, fordi disse navne erfaringsmæssigt ofte vil indgå i medarbejderens password.

Det vil være frivilligt for myndigheden eller virksomheden, om undersøgelser af offentligt tilgængelige oplysninger skal indgå i den konkrete sikkerhedstekniske undersøgelse.

Efter det foreslåede *stk. 2, nr. 3,* vil Center for Cybersikkerhed efter anmodning fra myndigheden eller virksomheden kunne iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder i myndigheden eller virksomheden. Dermed vil det være muligt at supplere den sikkerhedstekniske undersøgelse med et yderligere element af social engineering, der har til formål at skabe eller eskalere adgangen til systemerne. Dette element vil navnlig bestå af såkaldt spear-phishing, hvor Center for Cybersikkerhed søger at målrette et simuleret angreb mod udvalgte medarbejdere eller enheder.

Det vil f.eks. kunne foregå ved, at centeret – eventuelt på baggrund af undersøgelser af offentligt tilgængelige oplysninger efter stk. 2, nr. 2 – sender en e-mail til en bestemt medarbejder, hvor centeret udgiver sig for at være en kollega på den pågældende arbejdsplads. E-mailen vil være udformet på en sådan måde, at den skal få medarbejderen til at sende oplysninger til centeret, som centeret kan benytte til at skaffe sig adgang til myndighedens eller virksomhedens netværk eller opnå særlige rettigheder i systemerne, f.eks. administratorrettigheder. Det vil være kendetegnende for spear-phishing-mails, at centeret udgiver sig for at være en anden for at franarre medarbejdere bestemte oplysninger. Centeret vil dog kun udgive sig for at være medarbejdere i den myndighed eller virksomhed, der er genstand for undersøgelsen. Hvis centeret udgiver sig for at være en "ægte" medarbejder i den pågældende myndighed eller virksomhed, skal der være tale om en medarbejder, som er bekendt med den sikkerhedstekniske undersøgelse og omfanget heraf, og som derfor kan reagere hensigtsmæssigt på eventuelle henvendelser fra kollegaer om de modtagne spear-phishing-mails.

Dette element vil f.eks. også kunne indebære, at der placeres usb-nøgler eller andre eksterne medier på myndighedens eller virksomhedens område, som potentielt giver fjernadgang til systemerne, såfremt en medarbejder indsætter usb-nøglen eller mediet i sin computer.

Det vil være frivilligt for myndigheden eller virksomheden, om dette element af social engineering skal indgå i den konkrete sikkerhedstekniske undersøgelse.

Center for Cybersikkerhed vil i forbindelse med sikkerhedstekniske undersøgelser kunne blive opmærksom på, at en myndigheds eller virksomheds medarbejdere foretager en handling, der udgør en overtrædelse af arbejdspladsens it-sikkerhedsregler. Når sådanne oplysninger videregives til myndigheden eller virksomheden, vil det i særlige tilfælde kunne få ansættelsesretlige konsekvenser for medarbejderen. Det bemærkes, at eventuelle ansættelsesretlige konsekvenser vil være reguleret af almindelige retsgrundsætninger, herunder krav om saglighed og proportionalitet.

Der henvises i øvrigt til afsnit 3.4 i de almindelige bemærkninger.

Den foreslåede *§ 6 b* er ligeledes ny. Med bestemmelsen vil Center for Cybersikkerhed med henblik på at opnå viden om angrebsaktørers metoder og værktøjer kunne opsætte fiktive angrebsmål, såfremt opsætningen vurderes at kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at understøtte et højt informationssikkerhedsniveau i samfundet.

Bestemmelsen vil indebære, at Center for Cybersikkerhed får mulighed for at opsætte såkaldte honey pots. En honey pot er typisk et computersystem eller en server, der indeholder sårbarheder og er placeret på netværket hos interessante angrebsmål med det formål at tiltrække sig opmærksomhed fra en angrebsaktør, der søger efter mål på netværket. En honey pot vil således kun blive opdaget af angrebsaktører, der bevidst søger efter de pågældende sårbarheder.

Dermed lokkes angrebsaktøren til at bruge sine ressourcer på at angribe et system, der er indrettet til formålet, i stedet for reelle mål på netværket. Ved at lade systemet udsætte for kompromittering kan Center for Cybersikkerhed endvidere indsamle oplysninger om angrebsaktørens færden og brug af kommandoer i systemet, herunder tilegne sig de angrebsværktøjer, som angrebsaktøren søger at placere på det sårbare system.

Honey pots vil efter omstændighederne kunne opsættes på tilsluttede myndigheder og virksomheders egne netværk og eget udstyr, hvilket dog vil forudsætte samtykke fra de pågældende myndigheder eller virksomheder.

Med *stk. 2* foreslås det, at hvis en angrebsaktør benytter et fiktivt angrebsmål til at deponere data, vil Center for Cybersikkerhed uden retskendelse kunne behandle de deponerede data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller at informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.

Som udgangspunkt vil trafikken på en honey pot bestå af angrebsaktørens afsøgning af systemet, og ved Center for Cybersikkerheds tilgang til denne trafik vil der ikke i sig selv ske indgreb omfattet af grundlovens § 72. Det kan imidlertid ikke udelukkes, at en angrebsaktør i særlige tilfælde vil anvende en honey pot til at deponere data, der er hentet som led i et angreb mod tredjemand. Centeret vil i givet fald ved at tilgå data i en honey pot kunne foretage indgreb omfattet af grundlovens § 72, f.eks. for at forsøge at identificere offeret for det pågældende angreb.

I det omfang, det vil være muligt umiddelbart at identificere ejeren af de pågældende data, vil Center for Cybersikkerhed rette henvendelse til vedkommende og orientere om forholdet, ligesom centeret vil kunne rette henvendelse til relevante myndigheder, f.eks. netsikkerhedstjenester i det land, hvor angrebet har fundet sted. Såfremt det ikke umiddelbart er klart, hvem de pågældende data stammer fra, herunder om data måtte stamme fra flere forskellige kilder, vil data hurtigst muligt blive slettet, medmindre Center for Cybersikkerhed udtager data til nærmere analyse. Der henvises i den forbindelse til den foreslåede § 17 a og bemærkningerne hertil.

Behandling af data, der indeholder personoplysninger, vil ske i overensstemmelse med de generelle regler for Center for Cybersikkerheds behandling af data, hvor en række af persondatalovens centrale principper er indarbejdet i lov om Center for Cybersikkerhed, herunder krav til behandlingsgrundlag samt krav om proportionalitet og dataminimering.

Der henvises i øvrigt til afsnit 3.5 i de almindelige bemærkninger.

Den foreslåede *§ 6 c* er også ny. Efter bestemmelsen vil Center for Cybersikkerhed med henblik på at forhindre, standse eller begrænse en nært forestående eller igangværende sikkerhedshændelse kunne gøre brug af domænenavne og tilsvarende it-infrastruktur, som anvendes eller har været anvendt af en angrebsaktør, men som er offentligt tilgængelig.

Bestemmelsen vil indebære, at Center for Cybersikkerhed får mulighed for at anvende såkaldte sinkholes. Center for Cybersikkerhed vil f.eks. kunne registrere rettighederne til et domæne, der indgår i angrebsaktørens infrastruktur, og som ikke i forvejen er registreret, eller få allokeret en ip-adresse. Derefter vil den trafik, der ellers ville være tilgået angrebsaktøren gennem det pågældende domæne eller den pågældende ip-adresse, i stedet modtages af Center for Cybersikkerhed som operatør af sinkholet. Det kan f.eks. dreje sig om data, som angrebsaktøren har hentet fra en inficeret enhed, eller om kommandoer, som angrebsaktøren – via domænet – sender til inficerede enheder. Centeret vil tillige kunne registrere eksempelvis en e-mailadresse eller en konto på en kommunikationsplatform, når e-mailadressen eller kontoen ikke i forvejen er registreret, hvorefter den kommunikation, der

ellers ville være tilgået angrebsaktøren, i stedet modtages af Center for Cybersikkerhed. Dermed kan centeret f.eks. modtage meddelelser og andre data, som angrebsaktøren skulle have modtaget fra en kompromitteret bruger eller inficeret enhed. Det vil også i disse tilfælde være en forudsætning, at e-mailadressen eller kontoen anvendes eller har været anvendt af en angrebsaktør.

Centeret vil således med et sinkhole potentielt kunne afskære angrebsaktøren fra at styre dennes angrebsplatform og dermed standse et igangværende angreb.

Proceduren vil særligt kunne anvendes i tilfælde, hvor et domæne er ledigt, fordi angrebsaktøren har undladt at registrere retten til domænet eller har undladt at forlænge en registrering, eller hvor angrebsaktøren har undladt at registrere en e-mailadresse eller en konto på en kommunikationsplatform. Center for Cybersikkerhed vil ikke kunne skaffe sig uberettiget adgang til et domæne eller en konto på en kommunikationsplatform, f.eks. gennem hacking, ligesom der ikke vil kunne gives påbud om, at et domæne eller en konto overdrages til centeret. Den foreslåede bestemmelse påvirker dog ikke Center for Cybersikkerheds muligheder for at samarbejde med andre myndigheder i situationer, hvor disse myndigheder i medfør af anden lovgivning har fået råderet over domænenavne eller anden tilsvarende it-infrastruktur, herunder ved at den pågældende myndighed har fået overdraget et beslaglagt domænenavn eller en konto på en kommunikationsplatform.

Med *stk. 2* foreslås det, at hvis Center for Cybersikkerhed som led i anvendelsen af it-infrastruktur efter stk. 1 modtager data fra tredjemand, kan centeret uden retskendelse behandle de modtagne data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller at informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.

Ved anvendelse af teknikken kan det således ikke udelukkes, at Center for Cybersikkerhed kommer i besiddelse af data, som stammer fra et angreb – og hvor der dermed kan blive tale om, at centeret dels skal foretage indgreb omfattet af grundlovens § 72, dels skal behandle personoplysninger, f.eks. fordi der sendes data, som stammer fra et cyberangreb, til et sinkhole.

I det omfang, det vil være muligt umiddelbart at identificere ejeren af de pågældende data, vil Center for Cybersikkerhed rette henvendelse til vedkommende og orientere om forholdet, ligesom det vil kunne være hensigtsmæssigt for centeret at rette henvendelse til relevante myndigheder, f.eks. netsikkerhedstjenester i det land, hvor angrebet har fundet sted. Såfremt det ikke umiddelbart er klart, hvem de pågældende data stammer fra, herunder om data måtte stamme fra flere forskellige kilder, vil data i stedet blive slettet. Der henvises i den forbindelse til den foreslåede § 17 a og bemærkningerne hertil.

Behandling af data, der indeholder personoplysninger, vil ske i overensstemmelse med de generelle regler for Center for Cybersikkerheds behandling af data, hvor en række af persondatalovens centrale principper er indarbejdet i lov om Center for Cybersikkerhed, herunder krav til behandlingsgrundlag samt krav om proportionalitet og dataminimering.

Der henvises i øvrigt til afsnit 3.5 i de almindelige bemærkninger.

Til nr. 5

Det foreslås med bestemmelsen, at der indsættes et nyt *kapitel 4 a* med overskriften »Edition«.

Det foreslåede kapitel indebærer, at Center for Cybersikkerhed med henblik på at afdække sikkerhedshændelser som noget nyt vil kunne anmode retten om at pålægge en juridisk eller fysisk person at forevise eller udlevere oplysninger om brugeren af en e-mailkonto, en ip-adresse eller et domænenavn, såfremt oplysningerne er undergivet den pågældendes rådighed.

Den foreslåede ordning følger i det væsentligste bestemmelserne om edition i retsplejelovens kapitel 74. Den foreslåede § 7 adskiller sig imidlertid ved, at der ikke vil være et krav om mistanke om en strafbar lovovertrædelse, men derimod alene krav om, at oplysningerne skal kunne medvirke til at afdække sikkerhedshændelser.

Ligesom efter retsplejelovens regler om edition vil der ikke ske underretning af den pågældende bruger af e-mailkontoen, ip-adressen eller domænenavnet, medmindre vedkommende efterfølgende sigtes af politiet.

Som en yderligere retssikkerhedsmæssig garanti foreslås det med § 7 b, at der – i modsætning til efter retsplejelovens editionsregler – beskikkes en advokat for den, som indgrebet vedrører. Advokaten vil dermed kunne varetage interessen for den bruger af eksempelvis et domænenavn, som Center for Cybersikkerhed ønsker oplysninger om.

Til nr. 6

Den foreslåede *§ 7* er ny. Efter bestemmelsen kan der med henblik på at afdække sikkerhedshændelser meddeles en juridisk eller fysisk person pålæg om at forevise eller udlevere oplysninger om brugeren af en e-mailkonto, en ip-adresse eller et domænenavn, såfremt oplysningerne er undergivet den pågældendes rådighed.

Pålæg kan således alene gives, såfremt oplysningerne er undergivet den pågældendes rådighed. Bestemmelsen indebærer dermed ikke, at personer og virksomheder pålægges at opbevare oplysninger, som de ikke ellers ville opbevare. Der er alene tale om en pligt til – efter rettens kendelse – at udlevere foreliggende oplysninger til Center for Cybersikkerhed.

Det foreslåede *stk. 2* indebærer, at der ikke kan meddeles pålæg om edition, såfremt der derved vil fremkomme oplysninger om forhold, som den pågældende ville være udelukket fra eller fritaget fra at afgive forklaring om som vidne efter retsplejelovens §§ 169-172. Retsplejelovens §§ 169-172 omhandler de særlige vidnefritagelses- og vidneudelukkelsesgrunde. Det følger således bl.a. af retsplejelovens § 171, at en part ikke har pligt til at afgive forklaring som vidne, såfremt forklaringen må antages at udsætte vidnet selv for straf eller tab af velfærd.

Med *stk. 3* foreslås det, at pålæg om edition ikke må meddeles, såfremt indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre. Bestemmelsen indebærer, at der skal foretages en proportionalitetsvurdering forud for meddelelsen af et pålæg.

Til nr. 7

Efter den foreslåede *§ 7 a, stk. 1,* træffes afgørelse om pålæg om edition af retten efter Center for Cybersikkerheds begæring.

Det foreslåede *stk. 2* indebærer endvidere, at afgørelsen træffes af retten ved kendelse. Derudover følger det af den foreslåede bestemmelse, at retsmøder holdes for lukkede døre, at der i kendelsen anføres de konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for indgrebet er opfyldt, og at kendelsen til enhver tid kan omgøres.

Det foreslås med *§ 7 b*, at der, inden retten træffer afgørelse om edition, skal beskikkes en advokat for den, som indgrebet vedrører, og advokaten skal have lejlighed til at udtale sig. Advokaten beskikkes fra den særlige kreds af advokater, som er nævnt i retsplejelovens § 784, stk. 2.

Bestemmelsen indebærer, at der i forbindelse med, at Center for Cybersikkerhed anmoder retten om en kendelse, skal beskikkes en advokat fra den særlige kreds af advokater, der i medfør af retsplejelovens § 784, stk. 2, af justitsministeren er antaget til beskikkelse i sager, hvor efterforskningen angår overtrædelse af straffelovens kapitel 12 (landsforræderi og andre forbrydelser mod statens selvstændighed og sikkerhed) eller kapitel 13 (om forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme m.v.). Dette svarer således til den kreds af advokater, som beskikkes i sager, hvor FE og PET anmoder om kendelser.

Med *§ 7 c* foreslås det, at en advokat, som er beskikket efter den foreslåede § 7 b, skal underrettes om alle retsmøder i sagen og er berettiget til at overvære disse samt i forbindelse med retsmødet at gøre sig bekendt med det materiale, som Center for Cybersikkerhed har tilvejebragt. Advokaten må ikke give de oplysninger, som denne bliver bekendt med under sagen, videre til andre eller sætte sig i forbindelse med den, over for hvem indgrebet er begæret foretaget. Den beskikkede advokat må desuden ikke give møde ved anden advokat eller ved fuldmægtig.

Bestemmelsen fastsætter regler om den beskikkede advokats rettigheder og pligter i forbindelse med sagen. Den beskikkede advokat er efter bestemmelsen alene berettiget til i forbindelse med retsmødet at gøre sig bekendt med det materiale, som Center for Cybersikkerhed har tilvejebragt, men kan derimod ikke få udleveret en genpart af det materiale, som centeret har tilvejebragt. Advokaten vil få den fornødne tid til at læse materialet, inden retsmødet begynder, men har ikke en adgang til at tage materialet med sig efter retsmødets afslutning. Baggrunden herfor er de særlige fortrolighedshensyn, der gør sig gældende for dette materiale. Sådanne fortrolighedshensyn kan eksempelvis være hensynet til fremmede magter eller beskyttelse af oplysninger om Center for Cybersikkerheds metoder til at opdage eller imødegå cyberangreb.

Det foreslåede s*tk. 2* indebærer, at bestemmelserne om beskikkede forsvarere i retsplejelovens kapitel 66 (om sigtede og hans forsvarer) og § 746, stk. 1, finder tilsvarende anvendelse på den beskikkede advokat. Retten kan bestemme, at den beskikkede advokat ikke under en eventuel senere straffesag kan virke som forsvarer for nogen sigtet.

Med *§ 7 d* foreslås det, at der, inden retten træffer afgørelse om pålæg om edition, skal være givet den, der har rådighed over oplysningen, adgang til at udtale sig.

Den, der har rådighed over oplysningen, vil typisk være en teleudbyder eller en webhostingvirksomhed. Det forudsættes, at denne adgang til at udtale sig udøves på skrift. Udtalelsen vil kunne ske på baggrund af oplysninger fra Center for Cybersikkerhed om, hvilke nærmere oplysninger, der ønskes udleveret, samt en generel oplysning om at oplysningerne ønskes udleveret med henblik på afdækning af forhold vedrørende en sikkerhedshændelse.

Det foreslås med *stk. 2*, at retten eller Center for Cybersikkerhed, såfremt hensynet til fremmede magter eller statens sikkerhed taler derfor, kan pålægge den, der har rådighed over oplysningen, som ønskes forevist eller udleveret efter stk. 1, tavshedspligt med hensyn til den pågældendes viden om sagen. Når pålæg om tavshedspligt meddeles en erhvervsvirksomhed, gælder dette også for andre, der i kraft af deres tilknytning til virksomheden har fået kendskab til sagen, f.eks. medarbejdere eller samarbejdspartnere.

Med *stk. 3* foreslås det, at pålæg om tavshedspligt kan ophæves af Center for Cybersikkerhed eller retten. Det foreslås endvidere, at såfremt Center for Cybersikkerhed nægter at ophæve pålægget, skal spørgsmålet herom forelægges retten efter begæring. Den pågældende skal gøres bekendt med adgangen til at indbringe spørgsmålet for retten.

Den foreslåede *§ 7 e* indebærer, at reglerne i retsplejelovens kapitel 63 om værneting og kapitel 85 om kære til højere ret finder tilsvarende anvendelse.

Det foreslås med *§ 7 f*, at Center for Cybersikkerhed foranlediger, at en kendelse om edition opfyldes ved at rette henvendelse til den, der har rådighed over oplysningen. Rettens kendelse skal på begæring forevises for den pågældende.

Afviser den pågældende uden lovlig grund at efterkomme pålægget, finder reglerne i retsplejelovens § 178 tilsvarende anvendelse. Dette indebærer bl.a., at der kan pålægges den, der har rådighed over oplysningen, en bøde eller efter omstændighederne løbende bøder, hvis den pågældende uden lovlig grund afviser at efterkomme pålægget.

Der henvises i øvrigt til afsnit 3.6 i de almindelige bemærkninger.

Til nr. 8

Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, og det følger af den gældende *§ 8, stk. 1*, i lov om Center for Cybersikkerhed, at centerets virksomhed som udgangspunkt er undtaget fra lov om offentlighed i forvaltningen bortset fra lovens § 13. Center for Cybersikkerheds virksomhed er endvidere undtaget fra forvaltningslovens kapitel 4-6 og fra databeskyttelsesloven og Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, jf. § 3, stk. 2, i databeskyttelsesloven, og fra lov om retshåndhævende myndigheders behandling af personoplysninger, jf. § 1, stk. 2, i lov om retshåndhævende myndigheders behandling af personoplysninger.

Det foreslås, at Center for Cybersikkerheds virksomhed undtages fra § 3, § 5 og § 8, stk. 2, i lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter (retssikkerhedsloven).

De pågældende bestemmelser finder ikke i dag anvendelse på centerets virksomhed, som bl.a. indebærer, at der løbende foretages indgreb i meddelelseshemmeligheden i forbindelse med centerets monitorering af ind- og udgående kommunikation hos tilsluttede myndighed og virksomheder.

Forslagene om, at Center for Cybersikkerhed kan anvende sikkerhedssoftware til monitorering og at centeret i forbindelse med udførelse af forebyggende sikkerhedstekniske undersøgelser kan foretage indgreb omfattet af grundlovens § 72, medfører imidlertid at disse indgreb kan blive omfattet af de pågældende bestemmelser, jf. retssikkerhedslovens § 1, stk. 1, nr. 2.

Den foreslåede bestemmelse indebærer, at Center for Cybersikkerheds virksomhed undtages fra retssikkerhedslovens § 3, som bl.a. fastslår, at forvaltningslovens regler om partsaktindsigt finder anvendelse ved beslutninger om at iværksætte tvangsindgreb. Derudover vil centerets virksomhed blive undtaget fra retssikkerhedslovens § 5, som stiller krav om underretning af parten i forbindelse med iværksættelse af et tvangsindgreb. Endelig vil centerets virksomhed blive undtaget fra retssikkerhedslovens § 8, stk. 2, som bl.a. stiller krav om, at der på begæring skal udleveres en rapport om udførelsen af tvangsindgreb.

Baggrunden for undtagelsen er særligt, at de indgreb, som foretages af Center for Cybersikkerhed, adskiller sig væsentligt fra de tvangsindgreb, der anvendes af forvaltningen ved kontrolbesøg m.v. som led i forvaltningens kontrol- og tilsynsvirksomhed. Centerets indgreb sker som altovervejende hovedregel som led i en automatiseret proces, og de sker mange tusinde gange i timen. Indgrebene er endvidere karakteriserede ved, at de ikke er rettet mod konkrete borgere eller virksomheder, men derimod har til formål at fremfinde tekniske oplysninger i form af angrebsværktøjer eller resultaterne af cyberangreb – med henblik på at forebygge og stoppe sådanne angreb.

Der henvises i øvrigt til afsnit 3.9 i de almindelige bemærkninger.

Til nr. 9

Efter den gældende *§ 8, stk. 2. nr. 1*, kan forsvarsministeren bestemme, at databeskyttelsesloven, Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, lov om offentlighed i forvaltningen og forvaltningslovens kapitel 4-6 helt eller delvis finder anvendelse for Center for Cybersikkerhed vedrørende centerets behandling af sager om tilslutning til netsikkerhedstjenesten, jf. § 3, stk. 3.

Det foreslås, at forsvarsministeren ligeledes får hjemmel til at bestemme, at de nævnte regler skal finde helt eller delvis anvendelse for Center for Cybersikkerhed vedrørende centerets behandling af sager om tilslutning til netsikkerhedstjenesten efter den foreslåede § 3, stk. 4, d.v.s. sager, hvor der sker tilslutning på baggrund af et påbud.

Til nr. 10

Efter den gældende § 14, stk. 2, kan personoplysninger overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen.

Det foreslås, at der i kapitel 5 vedrørende forholdet til anden lovgivning indsættes en ny *§ 8 a*, hvorefter oplysninger omfattet af loven kan overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen.

Den foreslåede bestemmelse indebærer, at Center for Cybersikkerhed vil kunne overføre oplysninger til opbevaring i arkiv i det omfang, Rigsarkivaren har fastsat bevarings- og kassationsbestemmelser for de pågældende oplysninger. Der er således blot tale om en tydeliggørelse af, hvad der allerede følger af arkivlovgivningen. Den foreslåede ændring skyldes, at det ikke kan udelukkes, at der af Rigsarkivaren udstedes bevarings- og kassationsbestemmelser vedrørende oplysninger, som ikke er personoplysninger. Da bestemmelsen ikke som hidtil kun vedrører personoplysninger, foreslås bestemmelsen flyttet fra kapitel 6 vedrørende behandlingen af personoplysninger til kapitel 5 vedrørende forholdet til anden lovgivning.

Det bemærkes i øvrigt, at i det omfang Center for Cybersikkerheds oplysninger opbevares i systemer, der er fælles for hele Forsvarets Efterretningstjeneste, overføres oplysningerne til opbevaring i arkiv efter de bevarings- og kassationsbestemmelser, der af Rigsarkivet er fastsat for Forsvarets Efterretningstjeneste. Der er ikke på nuværende tidspunkt fastsat bevarings- og kassationsbestemmelser for oplysninger, der særskilt behandles af Center for Cybersikkerhed.

Som noget nyt foreslås det med *stk. 2*, at forsvarsministeren kan fastsætte nærmere regler om Center for Cybersikkerheds behandling af oplysninger, der skal bevares for eftertiden.

Rigsarkivaren kan fastsætte bevarings- og kassationsbestemmelser for centeret, der indebærer, at centeret skal bevare oplysninger af historisk interesse.

Selv om oplysningerne skal slettes i medfør af slettebestemmelserne i lov om Center for Cybersikkerhed, skal oplysninger af historisk interesse således overføres til Rigsarkivet i medfør af bestemmelser om bevaring og kassation udstedt af Rigsarkivet, og disse oplysninger må derfor ikke destrueres eller slettes.

I visse tilfælde vil disse bevaringsværdige oplysninger af praktiske eller sikkerhedsmæssige årsager ikke kunne overføres til Rigsarkivet. Det forudsættes derfor, at der bl.a. fastsættes nærmere regler om, at Center for Cybersikkerhed skal behandle sådanne oplysninger adskilt fra centerets øvrige oplysninger, indtil overførsel kan ske. Det forudsættes endvidere, at der fastsættes særlige adgangsbegrænsninger for sådanne oplysninger.

Bemyndigelsen forventes anvendt, såfremt der af Rigsarkivaren udstedes bevarings- og kassationsbestemmelser for oplysninger, der særskilt behandles af Center for Cybersikkerhed.

Der henvises i øvrigt til afsnit 3.8.3.5 i de almindelige bemærkninger.

Til nr. 11

Det foreslås, at den gældende *§ 14, stk. 2*, ophæves. Ophævelsen er en konsekvens af den foreslåede § 8 a, jf. lovforslagets § 1, nr. 9.

Til nr. 12

Efter den gældende *§ 15* må analyse af pakkedata, der er omfattet af de gældende §§ 4, 6 og 7, kun finde sted ved begrundet mistanke om en sikkerhedshændelse og kun i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen. Den gældende bestemmelse omfatter manuelle analyser, d.v.s. analyser, der foretages af Center for Cybersikkerheds sikkerhedsanalytikere.

Det foreslås, at denne bestemmelse videreføres, men tilpasses som konsekvens af bl.a. de nye former for data, der vil være behov for at analysere som følge af bl.a. muligheden for at anvende sikkerhedssoftware, jf. den foreslåede § 4.

Det foreslås, at Center for Cybersikkerhed kan foretage automatiserede analyser af trafikdata, pakkedata og stationære data, der er omfattet af kapitel 4. Dette er for så vidt angår trafikdata og pakkedata en uændret videreførelse af gældende ret, hvilket dog hidtil kun er fremgået forudsætningsvist af bestemmelsen og af bemærkningerne til denne, jf. Folketingstidende 2013-14, A, L 192 som fremsat. Stationære data er tilføjet som konsekvens af indførelsen af denne nye kategori af data, jf. den foreslåede § 2, nr. 4.

De automatiserede analyser af data sker løbende i centerets alarmenheder, hvor data, der transmitteres til og fra tilsluttede myndigheder og virksomheder, bl.a. sammenholdes med signaturer og scannes for andre indikatorer på kendte angrebsformer. Tilsvarende automatiserede analyser af stationære data vil finde sted i den kommende sikkerhedssoftware, jf. den foreslåede § 4. Som resultat af denne form for automatiserede analyser vil centerets medarbejdere kunne få præsenteret analytiske resultater, f.eks. en oversigt over de tekniske systemprocesser, der aktuelt anvendes på de pc'ere, som monitoreres. Hvis medarbejderne på den baggrund har behov for at tilgå de bagvedliggende data, vil der være tale om en manuel analyse.

Efter det foreslåede *nr. 1* må manuelle analyser af trafikdata finde sted for at opdage, analysere og bidrage til at imødegå sikkerhedshændelser. Analysen kan ske i det omfang, det er nødvendigt. Der er tale om en ny bestemmelse, da rammerne for manuelle analyser af trafikdata ikke hidtil har været udtrykkeligt reguleret i loven.

Efter det foreslåede *nr. 2* må manuelle analyser af pakkedata og stationære data finde sted ved begrundet mistanke om en sikkerhedshændelse i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen. Manuelle analyser af trafikdata under tilsvarende omstændigheder vil være omfattet af det foreslåede nr. 1. Bestemmelsen er ny for så vidt angår stationære data, hvilket er en konsekvens af de foreslåede ordninger om sikkerhedssoftware på lokale netværk og enheder, jf. den foreslåede § 6, forebyggende sikkerhedstekniske undersøgelser, jf. den foreslåede § 6 a, samt anvendelse og påvirkning af angrebsmål og angrebsinfrastruktur, jf. de foreslåede §§ 6 b og 6 c.

Efter det foreslåede *nr. 3* må manuelle analyser af trafikdata, pakkedata og stationære data endvidere finde sted som led i forebyggende sikkerhedstekniske undersøgelser efter den foreslåede § 6 a i det omfang, det er nødvendigt for at gennemføre undersøgelserne. Bestemmelsen er ny og er en konsekvens af den foreslåede ordning om forebyggende sikkerhedstekniske undersøgelser, jf. den foreslåede § 6 a.

Med *nr. 4* foreslås det, at manuelle analyser af trafikdata og pakkedata, der hidrører fra myndigheder på Forsvarsministeriets område, desuden må ske som led i det løbende arbejde med at understøtte et højt informationssikkerhedsniveau på Forsvarsministeriets område, herunder ved kontrol af, om kommunikation indeholder klassificeret materiale.

Rammerne for analyse af pakkedata, der hidrører fra myndigheder på Forsvarsministeriets område, har ikke hidtil været reguleret i lov om Center for Cybersikkerhed, men den foreslåede bestemmelse viderefører gældende ret. Således følger det af § 4 i Forsvarsministeriets retningslinjer vedrørende behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste, at analyse af pakkedata hidrørende fra netværk hos myndigheder på Forsvarsministeriets område kun må finde sted ved begrundet mistanke om en sikkerhedshændelse og som led i det løbende arbejde med at understøtte et højt informationssikkerhedsniveau på Forsvarsministeriets område, herunder ved kontrol af, om kommunikation indeholder klassificeret materiale. Endvidere følger det af retningslinjernes § 4, stk. 2, at analyse kun må ske i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen eller nødvendigt for at understøtte et højt informationssikkerhedsniveau på Forsvarsministeriets område.

Den særlige ordning vedrørende myndigheder på Forsvarsministeriets område skyldes, at disse myndigheder behandler store mængder klassificeret materiale. Der er derfor behov for, at Center for Cybersikkerhed kan foretage analyser, der ikke kun vedrører sikkerhedshændelser, men også skal afdække, om der forsætligt eller uagtsomt sendes klassificeret materiale fra myndighedernes netværk.

Efter det foreslåede *nr. 5* kan analyse endvidere ske som led i tekniske tests og konfiguration af netsikkerhedstjenestens alarmenheder. Analysen må omfatte trafikdata og pakkedata 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 Center for Cybersikkerhed. Øvrige medarbejdere må ikke tilgå oplysninger, der hidrører fra tests. Malware, der ved en tilfældighed opdages som led i en teknisk test, må dog analyseres af øvrige medarbejdere i Center for Cybersikkerhed efter det foreslåede nr. 2. Bestemmelsen er ny og er begrundet i behovet for kortvarigt at tilgå trafikdata og pakkedata.

Der kan i forbindelse med den løbende udvikling og drift af alarmenhederne være behov for kortvarigt at tilgå trafikdata og pakkedata. For det første er der behov for, at relevante medarbejdere kan tilgå og anvende data i forbindelse med udvikling af ny funktionalitet i alarmenhederne. Som led i udviklingsarbejdet er der således behov for at teste, om en given funktionalitet reagerer efter hensigten, når den udsættes for faktiske datastrømme. For det andet er der i forbindelse med opsætning og konfiguration af alarmenhederne på tilsvarende vis behov for at sikre, at enhederne fungerer korrekt. Ved at kunne tilgå data vil centeret kunne konstatere, om enheden kan håndtere mængden, hastigheden og variationen af de unikke datastrømme, der hidrører fra den tilsluttede myndighed eller virksomhed.

Data, der anvendes som led i tekniske tests, vil fortsat være omfattet af de absolutte slettefrister for data efter § 17.

Der henvises i øvrigt til afsnit 3.7.3 i de almindelige bemærkninger (det femte forslag).

Efter den gældende *§ 16* kan data, der er omfattet af de gældende §§ 4, 6 og 7, videregives til politiet ved begrundet mistanke om en sikkerhedshændelse. Ved begrundet mistanke om en sikkerhedshændelse og hvis det er nødvendigt for udførelsen af netsikkerhedstjenestens opgaver, kan trafikdata desuden videregives til danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester, andre netsikkerhedstjenester, virksomheder, der er omfattet af de gældende §§ 4, 6 og 7, samt til myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger.

Videregivelse af trafikdata sker således bl.a. i forbindelse med, at Center for Cybersikkerhed udsender sikkerhedsvarslinger, hvor centeret eksempelvis gør myndigheder og virksomheder opmærksomme på, at en bestemt ip-adresse anvendes til cyberangreb. Sådanne varslinger giver myndigheder og virksomheder mulighed for at tage deres forholdsregler, f.eks. ved at blokere den pågældende ip-adresse i en lokal firewall, og undersøge (f.eks. ved at gennemgå logfiler), om de selv har været udsat for cyberangreb.

Ved begrundet mistanke om en sikkerhedshændelse og med henblik på nærmere undersøgelse af hændelsen, kan der endvidere ske videregivelse af trafikdata til f.eks. andre netsikkerhedstjenester, herunder tilsvarende netsikkerhedstjenester i Danmark og udlandet, f.eks. CERT'er, CSIRT'er, ikt-sikkerhedsmyndigheder og efterretningstjenester.

Det er ikke hensigten med bestemmelsen at begrænse Center for Cybersikkerheds mulighed for at anvende gængse søgefunktioner på internettet til at indsamle oplysninger om mulige sikkerhedshændelser. Når der opstår mistanke om en mulig sikkerhedshændelse, kan det således være relevant at undersøge, om der foreligger offentligt tilgængelige oplysninger om, at eksempelvis den anvendte ip-adresse i andre sammenhænge har været anvendt som led i et cyberangreb. Sådanne oplysninger kan foreligge i form af offentlige undersøgelsesrapporter, artikler, blogopslag og lignende. Almindelig søgning efter sådanne offentligt tilgængelige oplysninger anses for at have en materielt anderledes beskaffenhed end den videregivelse, der er omfattet af bestemmelsen, uanset at sådanne søgninger i visse tilfælde vil blive logget og dermed i princippet kan siges at have karakter af en videregivelse.

Hvis der er tale om personoplysninger, vil principperne om relevans og proportionalitet, jf. den gældende § 9, stk. 2, tillige skulle iagttages. Der vil dermed alene kunne videregives personoplysninger, som er relevante og tilstrækkelige for at opnå formålet med den konkrete videregivelse.

Det bemærkes, at Center for Cybersikkerheds videregivelse af personoplysninger fortsat vil være underlagt tilsyn af Tilsynet med Efterretningstjenesterne, jf. de gældende §§ 19-24.

Det foreslås, at bestemmelsen videreføres, men således at mulighederne for videregivelse øges.

Det foreslås med *stk. 1*, *nr. 1,* at Center for Cybersikkerhed kan videregive trafikdata, der er omfattet af kapitel 4, til politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse. Der er tale om en videreførelse af gældende ret, og Center for Cybersikkerhed vil dermed fortsat kunne videregive trafikdata, der stammer fra indgreb i meddelelseshemmeligheden, til dansk politi (og anklagemyndigheden). Dermed sikres, at centeret kan videregive alle relevante oplysninger til politiet i de tilfælde, hvor det kan være relevant for politiet at indlede en strafferetlig efterforskning.

Kravet om, at der skal være tale om en begrundet mistanke om en sikkerhedshændelse, indebærer, at Center for Cybersikkerhed alene kan videregive de pågældende data, hvis der foreligger konkrete indikationer, der peger i retning af, at en sikkerhedshændelse har fundet eller vil finde sted.

Det foreslås med *stk. 1, nr. 2*, at Center for Cybersikkerhed endvidere kan videregive trafikdata, der er omfattet af kapitel 4, til 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 Center for Cybersikkerheds opgaver.

Kravet om, at der skal være tale om en begrundet mistanke om en sikkerhedshændelse, indebærer, at Center for Cybersikkerhed alene kan videregive de pågældende data, hvis der foreligger konkrete indikationer, der peger i retning af, at en sikkerhedshændelse har fundet eller vil finde sted.

Der er indholdsmæssigt tale om en videreførelse af gældende ret.

Endvidere foreslås det med *stk. 1, nr. 3,* at Center for Cybersikkerhed kan videregive trafikdata til danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt til myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger, såfremt der er begrundet mistanke om en sikkerhedshændelse, og hvis det er nødvendigt for udførelsen af netsikkerhedstjenestens opgaver.

Kravet om, at der skal være tale om en begrundet mistanke om en sikkerhedshændelse, indebærer, at Center for Cybersikkerhed alene kan videregive de pågældende data, hvis der foreligger konkrete indikationer, der peger i retning af, at en sikkerhedshændelse har fundet eller vil finde sted.

Der er tale om en videreførelse af gældende ret.

Det foreslås med *stk. 2, nr. 1,* at Center for Cybersikkerhed kan videregive pakkedata, der er omfattet af kapitel 4, til politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse. Der er tale om en videreførelse af gældende ret, og Center for Cybersikkerhed vil dermed fortsat kunne videregive pakkedata, der stammer fra indgreb i meddelelseshemmeligheden, til dansk politi (og anklagemyndigheden). Dermed sikres, at centeret kan videregive alle relevante oplysninger til politiet i de tilfælde, hvor det kan være relevant for politiet at indlede en strafferetlig efterforskning.

Kravet om, at der skal være tale om en begrundet mistanke om en sikkerhedshændelse, indebærer, at Center for Cybersikkerhed alene kan videregive de pågældende data, hvis der foreligger konkrete indikationer, der peger i retning af, at en sikkerhedshændelse har fundet eller vil finde sted.

Det foreslås med *stk. 2, nr. 2,* at Center for Cybersikkerhed endvidere kan videregive pakkedata, der er omfattet af kapitel 4, til den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse.

Bestemmelsen er ny og indebærer, at videregivelse af pakkedata til den tilsluttede myndighed eller virksomhed for det første vil kunne ske, når der er mistanke om en sikkerhedshændelse, og videregivelsen er nødvendig for at kunne få myndighedens eller virksomhedens bistand til at fastslå, om der rent faktisk er tale om en sikkerhedshændelse. Videregivelse vil for det andet kunne ske, hvis der er konstateret en sikkerhedshændelse, og videregivelsen er nødvendig for, at den tilsluttede myndighed eller virksomhed kan tage de fornødne forholdsregler.

Om baggrunden for bestemmelsen henvises til lovforslagets almindelige bemærkninger, afsnit 3.7.3 (det andet forslag).

Det foreslåede *stk. 3* er nyt og regulerer Center for Cybersikkerheds mulighed for at videregive stationære data, som er en ny kategori af data, der defineres i den foreslåede § 2, nr. 4. Stationære data er data, som opbevares på servere, cloudtjenester, pc'ere, lagerenheder, netværksenheder, mobile enheder og tilsvarende. Bestemmelsen er en konsekvens af de foreslåede ordninger om sikkerhedssoftware på lokale netværk og enheder, jf. den foreslåede § 6, forebyggende sikkerhedstekniske undersøgelser, jf. den foreslåede § 6 a, samt anvendelse af angrebsmål og påvirkning af angrebsinfrastruktur, jf. de foreslåede §§ 6 b og 6 c.

Det foreslås med *stk. 3, nr. 1*, at Center for Cybersikkerhed kan videregive stationære data, der er omfattet af kapitel 4, til politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse. Der er tale om samme rammer for videregivelse, som gælder for trafikdata og pakkedata. Center for Cybersikkerhed vil dermed kunne videregive stationære data, der stammer fra indgreb i meddelelseshemmeligheden, til dansk politi (og anklagemyndigheden). Dermed sikres, at centeret kan videregive alle relevante oplysninger til politiet i de tilfælde, hvor det kan være relevant for politiet at indlede en strafferetlig efterforskning.

Endvidere foreslås det med *stk. 3, nr. 2,* at Center for Cybersikkerhed kan videregive stationære data, der er omfattet af kapitel 4, til den myndighed, virksomhed eller borger, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse. Der er tale om samme rammer for videregivelsen, som gælder for pakkedata.

Med bestemmelsen vil Center for Cybersikkerhed få mulighed for at få fastslået, om data rent faktisk er ondartet. Center for Cybersikkerhed vil endvidere få mulighed for at tilbagelevere data, der er blevet stjålet fra en myndighed, virksomhed eller borger, og som Center for Cybersikkerhed efterfølgende f.eks. får adgang til i forbindelse med opsætning af honey pots eller sinkholes efter de foreslåede §§ 6 b og 6 c.

Efter *stk. 3, nr. 3*, vil der endvidere kunne ske videregivelse til andre netsikkerhedstjenester, såfremt Center for Cybersikkerhed har modtaget de pågældende data i medfør af de foreslåede § 6 b eller § 6 c.

Det foreslåede *stk. 4* er nyt og regulerer Center for Cybersikkerheds mulighed for at videregive malware, der er en ny kategori af data, som defineres i den foreslåede § 2, nr. 5. Malware er trafikdata, pakkedata og stationære data, hvor der er særlig bestyrket mistanke om, at data er anvendt af en angrebsaktør med det formål at forårsage et brud på informationssikkerheden.

Efter bestemmelsens *nr. 1* vil malware, der er omfattet af kapitel 4, kunne videregives til politiet, efter *nr. 2* til den myndighed eller virksomhed, hvorfra de pågældende data hidrører, og efter *nr. 3* til danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt til myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger.

Efter gældende ret kan pakkedata – herunder malware – alene videregives til politiet. Det foreslås, at muligheden for at videregive malware udvides for at give en bredere kreds af modtagere mulighed for selvstændigt at anvende de pågældende data til at styrke cybersikkerheden, f.eks. ved at beskytte deres egne og deres kunders infrastruktur mod angreb af samme type, jf. nr. 3. Desuden vil de på baggrund af de modtagne data kunne give Center for Cybersikkerhed supplerende oplysninger om f.eks. tilsvarende angreb, som de er bekendt med. Der henvises til lovforslagets almindelige bemærkninger, afsnit 3.7.3 (det første forslag).

Det foreslås herudover, at muligheden for at videregive malware udvides til at omfatte den myndighed eller virksomhed, hvorfra de pågældende data hidrører, jf. nr. 2. Herved gives den tilsluttede myndighed mulighed for at bidrage med viden om det fundne malware og kunne erhverve viden om fremtidige hændelser.

Det bemærkes, at danske modtageres behandling – herunder videregivelse – af de pågældende data vil være underlagt databeskyttelsesreguleringen. Offentlige myndigheder vil desuden være underlagt forvaltningslovens regler om videregivelse samt forvaltningslovens og straffelovens regler om tavshedspligt.

Det foreslås med *stk. 5*, at videregivelsesbestemmelserne i stk. 1-4 ikke finder anvendelse på data, der stammer fra tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder, og at Center for Cybersikkerhed alene vil kunne videregive sådanne data i de tilfælde, der beskrives i bestemmelsens nr. 1 og 2.

Efter *stk. 5, nr. 1*, kan malware, der er opdaget ved en tilfældighed, videregives til politiet, den myndighed eller virksomhed, hvorfra de pågældende data hidrører, til danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt til myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger.

Med bestemmelsen sikres det således, at malware, der opdages tilfældigt som led i tekniske tests, kan behandles på samme vis som øvrig malware, jf. den foreslåede *stk. 4*. Endvidere vil der i forhold til de myndigheder og virksomheder, hvorfra data stammer, efter det foreslåede *stk. 5, nr. 2*, være mulighed for videregivelse af trafikdata.

Begge bestemmelser i stk. 5 er nye. Om baggrunden herfor henvises til lovforslagets almindelige bemærkninger, afsnit 3.7.3 (det tredje og fjerde forslag).

Den gældende *§ 17* fastsætter de tidsmæssige rammer for Center for Cybersikkerheds opbevaring af de data, der behandles i medfør af kapitel 4 og dermed behandles på baggrund af indgreb i meddelelseshemmeligheden.

Efter den gældende § 17, stk. 1, skal data, der er omfattet af det gældende kapitel 4, slettes, når formålet med behandlingen er opfyldt. Endvidere følger det af bestemmelsens stk.

2, at uanset at formålet med behandlingen ikke er opfyldt, må data, der knytter sig til en sikkerhedshændelse, højst opbevares i tre år, mens data, der ikke knytter sig til en sikkerhedshændelse, højst må opbevares i 13 måneder. Efter stk. 3 regnes fristerne fra tidspunktet for Center for Cybersikkerheds registrering af de pågældende data. Efter stk. 4 finder reglerne i stk. 1 og 2 ikke anvendelse på data, der er videregivet i medfør af den gældende § 16.

Bestemmelsen skal ses i sammenhæng med den gældende § 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 alene anvendelse på de data, der er omfattet af kapitel 4.

Såfremt en virksomhed eller myndighed opsiger en tilslutningsaftale med netsikkerhedstjenesten, vil en sådan opsigelse indebære, at Center for Cybersikkerhed snarest muligt sletter pakke- og trafikdata og stationære data, der stammer fra myndigheden eller virksomheden. Sletningen vil omfatte alle data, som centeret har behandlet på baggrund af tilslutningsaftalen med den pågældende myndighed eller virksomhed – dog ikke data, der konkret knytter sig til en sikkerhedshændelse, da disse data fortsat i relevant omfang vil blive anvendt til at beskytte de øvrige tilsluttede myndigheder og virksomheder mod cyberangreb, ligesom de potentielt vil kunne indgå i politiets efterforskning af strafbare forhold.

Det foreslås med *stk. 1*, at data, der er omfattet af kapitel 4, skal slettes, når formålet med behandlingen er opfyldt. Der er tale om en videreførelse af gældende ret.

Bestemmelsen indebærer, at der fortsat vil 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 omfatter alle data, der behandles på baggrund af indgreb omfattet af grundlovens § 72.

Det foreslåede *stk. 2* fastsætter øvre grænser for, hvor længe data, der ikke er slettet efter stk. 1, kan opbevares. 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.

Det foreslåede *stk. 2, nr. 1*, vedrører data, der er knyttet til en sikkerhedshændelse. Det kan f.eks. være en ip-adresse, som har været anvendt ved et cyberangreb mod en dansk myndighed, eller en e-mail-adresse, som har været anvendt til at sende phishing-mails til danske myndigheder. Sådanne data vil især blive anvendt i netsikkerhedstjenestens monitoreringsudstyr for at give mulighed for, at nye angreb, som kommer fra samme kilde, eller som anvender samme angrebsmetode og -værktøjer, straks kan opdages.

Efter bestemmelsen må data, der knytter sig til en sikkerhedshændelse, højst opbevares i fem år, hvorefter de skal slettes. Det er en udvidelse i forhold til gældende ret, hvor den maksimale opbevaringsperiode er tre år. Såfremt data inden for den fem-årige periode igen

konstateres anvendt i forbindelse med en sikkerhedshændelse, vil en ny fem-årig periode starte.

Det foreslåede *stk. 2, nr. 2,* vedrører data, der ikke er knyttet til en sikkerhedshændelse, men som stammer fra myndigheder, som i særlig grad beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold, samt virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold. Det foreslås, at sådanne data kan opbevares i højst tre år.

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. Såfremt en myndighed eller virksomhed, der ikke tidligere har været omfattet af bestemmelsen, ved varetagelse af nye opgaver eller indgåelse af nye aftaler kommer til i særlig grad at beskæftige sig med eller have betydning for udenrigs-, sikkerheds- og forsvarspolitiske forhold, vil der blive udarbejdet et tillæg til tilslutningsaftalen eller truffet afgørelse herom.

Hvis en tilsluttet myndighed eller virksomhed under tilslutningen vurderes at have ændret status, således at den omfattes af det foreslåede stk. 2, nr. 2, vil bestemmelsen alene finde anvendelse på data, der indsamles efter det tidspunkt, hvor tilslutningsaftalen er ændret. Tidligere indsamlede data vil således fortsat være omfattet af den almindelige slettefrist efter den foreslåede stk. 2, nr. 3. Hvis en tilsluttet virksomhed hidtil har været omfattet af stk. 2, nr. 2, men ændrer status og omfattes af stk. 2, nr. 3, vil dette ligeledes kun gælde for data indsamlet efter det tidspunkt, hvor tilslutningsaftalen er ændret.

Det foreslåede *stk. 2, nr. 3*, vedrører øvrige data, der ikke er knyttet til en sikkerhedshændelse. Det foreslås, at sådanne data må opbevares i højst 13 måneder. Dette er en videreførelse af gældende ret.

Med *stk. 3* foreslås det, at de frister for sletning, som følger af stk. 2, regnes fra det tidspunkt, hvor Center for Cybersikkerhed har registreret de pågældende data, hvilket svarer til tidspunktet for centerets lagring af data. Dette er en videreførelse af gældende ret.

Ved behandling af stationære data, regnes fristen fra det tidspunkt, hvor data er modtaget hos eller stillet til rådighed for Center for Cybersikkerhed.

Med *stk. 4* foreslås det, at Center for Cybersikkerhed kan opbevare backup af data i op til fire måneder efter udløb af fristerne i stk. 2. Ved indlæsning af data fra backup skal Center for Cybersikkerhed sikre, at data, der tidligere er slettet efter stk. 1 eller 2, straks slettes igen.

Der er tale om en ny bestemmelse.

Med *stk. 5* foreslås det, at stk. 1 og 2 ikke finder anvendelse på data, der i medfør af § 16 er videregivet til andre end den myndighed eller virksomhed, som data hidrører fra.

Når data er videregivet, har Center for Cybersikkerhed i sagens natur ikke mulighed for at sikre, at der efterfølgende sker en sletning hos modtageren, ligesom centeret selv vil være forpligtet til at registrere de udsendte varslinger m.v. Bestemmelsen indebærer, at data, der er videregivet, hverken hos Center for Cybersikkerhed eller hos modtagerne af varslingerne vil skulle slettes efter stk. 1 og 2. Der er tale om en videreførelse af gældende ret, idet undtagelsen fra sletteregleme dog ikke vil omfatte situationer, hvor videregivelsen alene er sket til den myndighed eller virksomhed, som data hidrører fra. I de tilfælde vil Center for Cybersikkerhed fortsat skulle slette data efter stk. 1 og 2.

Den myndighed eller virksomhed, som data er videregivet til, vil fortsat skulle slette data efter de for myndigheden eller virksomheden relevante regler, og ikke efter lov om Center for Cybersikkerheds sletteregler.

Uanset at sletteregleme i stk. 1 og 2 ikke finder anvendelse, vil personoplysninger indeholdt i data fortsat skulle behandles i overensstemmelse med den gældende § 14, hvorefter indsamlede personoplysninger 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.

Det foreslåede s*tk. 6* er nyt. Bestemmelsen er en konsekvens af den foreslåede § 6 a, der skaber hjemmel til, at Center for Cybersikkerhed kan gennemføre forebyggende sikkerhedstekniske undersøgelser, når en myndighed eller virksomhed har anmodet centeret herom.

Bestemmelsen fastsætter supplerende sletteregler for de data, som Center for Cybersikkerhed får adgang til ved gennemførelsen af sikkerhedstekniske undersøgelser. Personoplysninger, der er indeholdt i sådanne data, vil skulle slettes eller anonymiseres, når den sikkerhedstekniske undersøgelse er afsluttet, hvilket sker i forbindelse med afgivelse af en afsluttende rapport til den pågældende myndighed eller virksomhed. Såfremt Center for Cybersikkerhed konstaterer, at der i data, som Center for Cybersikkerhed får adgang til som led i forebyggende sikkerhedstekniske undersøgelser efter § 6 a, er indeholdt følsomme personoplysninger, slettes disse uden unødigt ophold.

Med *stk. 7* foreslås det, at sletning efter fristerne i stk. 2, nr. 2 og 3, i helt særlige tilfælde kortvarigt kan suspenderes, hvis væsentlige hensyn til varetagelsen af Center for Cybersikkerheds opgaver gør det nødvendigt. Tilsynet med Efterretningstjenesterne skal straks underrettes om suspension efter 1. pkt. og om baggrunden for suspensionen.

Der er tale om en ny bestemmelse.

Bestemmelsen vil kunne anvendes i helt særlige tilfælde, hvor der er mistanke om en sikkerhedshændelse, og hvor der er fare for, at relevant data, der endnu ikke er analyseret, ellers skal slettes i medfør af de absolutte slettefrister, før sikkerhedshændelsens eventuelle omfang kan afdækkes. Suspensionens varighed vil afhænge af den pågældende sikkerhedshændelses kompleksitet og af omfanget af de data, der skal analyseres. Det forudsættes, at der kun i særligt komplekse og omfattende tilfælde kan ske suspension i mere end tre måneder.

Data vil skulle slettes, så snart begrundelsen for at undlade sletning ikke længere er til stede.

Det forudsættes, at underretningen af Tilsynet med Efterretningstjenesterne alene skal ske, hvis der er tale om data, der er omfattet af tilsynets kompetence efter kapitel 9, d.v.s. Center for Cybersikkerheds behandling af personoplysninger. Såfremt der undtagelsesvist måtte være tale om, at en suspension af slettefristen udelukkende vedrører data, der ikke indeholder personoplysninger, vil Tilsynet med Efterretningstjenesterne således ikke skulle underrettes.

Der henvises i øvrigt til afsnit 3.8 i de almindelige bemærkninger.

Til nr. 13

Den foreslåede *§ 17 a* er ny. Bestemmelsen er en konsekvens af de foreslåede § 6 b og § 6 c, der skaber hjemmel til, at Center for Cybersikkerhed kan opsætte fiktive angrebsmål samt gøre brug af domænenavne og tilsvarende it-infrastruktur, som har været anvendt af en angrebsaktør.

Bestemmelsen fastsætter særlige sletteregler for de data, som Center for Cybersikkerhed får adgang til ved anvendelsen af fiktive angrebsmål og overtagelse af angrebsinfrastruktur. Data, der er deponeret på fiktive angrebsmål efter den foreslåede § 6 b eller modtaget via infrastruktur omfattet af den foreslåede § 6 c, skal slettes hurtigst muligt, såfremt Center for Cybersikkerhed ikke udtager data til nærmere vurdering. I disse tilfælde vil data derfor ikke være omfattet af sletteregelerne i § 17, idet der sker en hurtigere sletning end den, der følger af den foreslåede § 17, stk. 1 og 2.

Udtager Center for Cybersikkerhed derimod data til nærmere vurdering, skal sletning ske efter de almindelige regler i den foreslåede § 17.

De angrebsværktøjer og lignende, som en angrebsaktør selv anvender i forbindelse med brugen af et fiktivt angrebsmål, anses ikke for deponerede data og er ikke omfattet af de særlige sletteregler i bestemmelsen.

Der henvises i øvrigt til afsnit 3.5 og afsnit 3.8.3.4 i de almindelige bemærkninger.

Til nr. 14

Efter den gældende *§ 20* påser Tilsynet med Efterretningstjenesterne efter klage eller af egen drift Center for Cybersikkerheds overholdelse af de gældende regler i kapitel 4, 6 og 7 vedrørende behandling af personoplysninger.

Som konsekvens af det foreslåede kapital 4 a, hvorefter der vil ske behandling af personoplysninger i forbindelse med edition, foreslås Tilsynet med Efterretningstjenesternes kompetence udvidet til også at omfatte dette kapitel.

Til nr. 15

Det foreslås, at der indsættes et nyt *kapitel 9* med overskriften »Straffebestemmelser m.v.«.

Den foreslåede *§ 24 a* er ligeledes ny.

Det foreslås med *stk. 1,* at undladelse af at efterkomme Center for Cybersikkerheds pålæg om tavshedspligt efter den foreslåede § 7 d, stk. 2, kan straffes med bøde, medmindre strengere straf er forskyldt efter den øvrige lovgivning.

Med *stk. 2* bemyndiges forsvarsministeren til at fastsætte straf i form af bøde for overtrædelse af bestemmelser i regler, som udfærdiges i medfør af det foreslåede § 3, stk. 5, 2. pkt. Efter § 3, stk. 5, 2. pkt., vil der kunne fastsættes regler om, at de myndigheder og virksomheder, som får påbud om tilslutning, skal medvirke til netsikkerhedstjenestens opsætning og drift af hardware og software og i den forbindelse skal stille de nødvendige oplysninger om konfiguration og drift af deres digitale infrastruktur til rådighed for netsikkerhedstjenesten. Det vil således være manglende efterlevelse heraf, som vil kunne gøres strafbart i medfør af de fastsatte regler.

Efter det foreslåede *stk. 3* kan der pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel. Bestemmelsen indebærer, at der også i regler, som udfærdiges i medfør af loven, kan fastsættes regler om, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Til § 2

Det foreslås med *stk. 1*, at loven træder i kraft den 1. juli 2019. Med *stk. 2* foreslås det, at loven ikke finder anvendelse på data, der er indsamlet før den 1. juli 2019. For sådanne data finder de hidtil gældende regler anvendelse.

Til § 3

Lov om Center for Cybersikkerhed gælder ikke for Færøerne og Grønland, men kan ved kongelig anordning sættes helt eller delvis i kraft for Færøerne og Grønland med de ændringer, som de færøske og grønlandske forhold tilsiger. Det foreslås, at en tilsvarende ordning skal gælde for denne lov.