Forsvarsministeriet
fmn@fmn.dk

01-02-2019
EMN-2019-00127
1255493

Høringssvar vedr. forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden)

Danske Regioner har den 7. januar 2019 modtaget "udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden)" i høring.

Høringssvaret fremsendes med forbehold for godkendelse i Danske Regioners bestyrelse den 7. februar 2019.

Cyber- og informationssikkerhed er stor og voksende kerneopgave for regionerne. Danske Regioner er derfor positivt indstillet overfor nationale initiativer, der bidrager til at styrke samfundets – og dermed regionernes – muligheder for at imødegå cyberangreb mod den kritiske infrastruktur og ønsker naturligvis at bidrage til denne udvikling og samarbejdet herom.

Danske Regioner bakker op om formålet med lovforslaget, men har også noteret sig, at lovforslaget giver Center for Cybersikkerhed (CFCS) hjemmel til øgede beføjelser og mandater, der i sidste ende kan føre til indgriben i regionernes selvstændige myndighedsudøvelse, it-drift, patientsikkerheden samt borgernes rettigheder vedr. databeskyttelse.

Det er i lovforslaget ikke klart, hvilke konsekvenser implementeringen af den nye sikkerhedssoftware vil medføre, fx i relation til tilgængelighed, ydeevne, kliniske godkendelser af udstyr. Set fra et regionalt og behandlingsmæssigt perspektiv er det afgørende, at dette præciseres og at rolle- og ansvarsfordelingen fremgår tydeligt. Det er i denne sammenhæng Danske Regioners opfattelse, at CFCS med lovforslaget vil få mulighed for at prioritere handlinger i regionernes it-infrastruktur uden involvering af regionale prioriteringer, kompetencer og indsigt med heraf følgende risici for nedbrud i regionernes kritiske it-infrastruktur og dermed for patientkritiske hændelser. Såfremt CFCS får en sådan bemyndigelse er det således afgørende, at de forskellige hensyn afvejes nøje og at CFCS påtager sig et ansvar for eventuelle følger ved en indgriben i regionernes ansvarsområde.

Danske Regioner savner derudover en præcisering af, hvordan den meget brede adgang til data hos myndighederne, som CFCS får med lovforslaget, håndteres i overensstemmelse med anden lovgivning, som Danske Regioner som offentlig myndighed

DANSKE REGIONER
DAMPFÆRGEVEJ 22
2100 KØBENHAVN Ø
+45 35 29 81 00
REGIONER@REGIONER.DK
REGIONER.DK

er underlagt, særligt databeskyttelseslovgivningen og regionernes forpligtigelser som dataansvarlig, herunder varetagelsen af borgernes rettigheder.

De økonomiske konsekvenser af lovforslaget forventes behandlet efter DUT-reglerne.

Der er vedlagt et bilag med udbydende tekniske og tekstnære bemærkninger til lovforslaget.

Med venlig hilsen

Stephanie Lose

Ulla Astman

Bilag 1. Tekniske og tekstnære bemærkninger

Tekniske bemærkninger

Påbud om tilslutning til netsikkerhedstjenesten

Danske Regioner har noteret, at lovforslaget åbner op for, at CFCS, jf. § 3, kan påbyde virksomheder, regioner og kommuner, der har særligt samfundsvigtig karakter at blive tilsluttet netsikkerhedstjenesten, og, jf. § 4, at CFCS uden retskendelse kan behandle trafikdata, pakkedata og stationære data hidrørende de tilsluttede myndigheder. Der gøres opmærksom på, at dette er en indgriben i regionernes selvstændige myndighedsudøvelse.

Danske Regioner har samtidigt noteret sig, at muligheden for påbud ikke gælder regionernes egne aktive cyberforsvar, de forebyggende sikkerhedstekniske undersøgelser og anvendelse og påvirkning af angrebsmål og angrebsinfrastruktur. Danske Regioner finder det i den sammenhæng vigtigt at understrege, at det bør fastholdes i den videre udformning af loven, at der ikke kan udstedes påbud for disse tjenester.

Tilgængelighed

Danske Regioner skal indskærpe vigtigheden af, at netsikkerhedstjenesten skal designes således, at hverken sikkerhedssoftwaren eller CFCS' handlinger har en negativ indvirkning på regionernes drift, ydeevne og behov for tilgængelighed til applikationer. Regionernes har et stort behov for stabil drift, da det blandt andet har betydning for den enkelte klinikers arbejdsbetingelser og for patientsikkerheden. Dertil kommer, at Danske Regioner også har et sektoransvar, der indebærer et ansvar for at opretholde sikkerheden omkring borgerens behandling og sundhedsdata, således at *fortrolighed, integritet og tilgængelighed* bevares, jf. "Strategi for cyber- og informationssikkerhed i sundhedssektoren 2019-2022".

Præcisering af "begrundet mistanke om en sikkerhedshændelse"

Danske Regioner har noteret, at udkast til lovforslaget indebærer en række beføjelser for CFCS i det tilfælde, at der er tale om en begrundet mistanke om en sikkerhedshændelse. Eksempelvis kan CFCS, jf. § 6, ved begrundet mistanke om en sikkerhedshændelse uden retskendelse blokere, omdanne eller omdirigere trafikdata og pakkedata hos myndigheden. Blokering af regionens trafikdata og pakkedata kan føre til, at tilgængeligheden af data i kliniske sammenhænge forstyrres, og at det dermed i yderste konsekvens kan få konsekvenser for patientsikkerheden. Der er i den sammenhæng behov for, at det konkretiseres nærmere, hvornår der er tale om en begrundet mistanke om en sikkerhedshændelse. På sit nuværende grundlag er formuleringen for åben for fortolkning af CFCS.

Danske Regioner skal generelt henstille til, at berørte myndigheder orienteres så tidlig som mulig – i bedste fald inden den intervenerende handling foretages – om handlinger fra CFCS på baggrund af begrundet mistanke. I forhold til den løbende monitorering er det også væsentligt, at CFCS orienterer om de handlinger, der foretages.

Danske Regioner anbefaler – som minimum – at såfremt tilslutningen til netsikkerhedstjenesten sker på grund af påbud, skal CFCS pålægges at redegøre for bevæggrundene for at udstede påbuddet.

Databeskyttelsesretlige bemærkninger
CFCS får med lovforslaget en meget bred adgang til både trafikdata, pakkedata og stationære data hos myndighederne, herunder også personfølsomme og fortrolige data. Dertil kommer, at det på foreliggende grundlag ikke er muligt at afgøre, hvilke data CFCS opsamler, da der i princippet er adgang til alle typer data. Danske Regioner finder det bekymrende, at denne brede adgang til data indebærer adgang til fortrolige oplysninger og følsomme personoplysninger. Regioner er ligeledes bekymret for om den brede adgang til data om både regionens medarbejdere og borgere, i tilstrækkelig grad adresserer den registreredes rettigheder (jf. EU's persondataforordning og Databeskyttelseslovgivningen).

Bekymringerne gælder særlig henset til, at der kan sås tvivl om, hvorvidt borgernes og patienternes rettigheder bliver tilstrækkeligt varetaget i lovforslaget, når CFCS undtages fra retssikkerhedslovens § 3, som blandt andet fastslår, at forvaltningslovens regler om partsaktindsigt finder anvendelse ved beslutninger om at iværksætte tvangsindgreb. Denne bekymring gælder også, hvis CFCS's virksomhed udtages fra retssikkerhedslovens § 5, som stiller krav om underretning af parten i forbindelse med iværksættelse af et tvangsindgreb, samt fra retssikkerhedslovens § 8, stk. 2, som bl.a. stiller krav om, at der på begæring skal udleveres en rapport om udførelsen af tvangsindgreb. Det vil indebære en indskrænkning af borgernes rettigheder.

Danske Regioner savner en præcisering af, hvordan lovforslaget er i overensstemmelse med anden lovgivning, som Danske Regioner som offentlig myndighed er underlagt, særligt databeskyttelseslovgivningen og Danske Regioners forpligtigelser som dataansvarlig, herunder varetagelsen af de registreredes rettigheder. Hvilket samtidigt skal ses i lyset af, af det i lovforslagets bemærkninger, jf. pkt. 1, hedder:

"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."

Med henblik på at beskytte borgernes og patienternes rettigheder anbefales det, som minimum, 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, finder anvendelse for CFCS vedrørende centrets behandling af sager om tilslutning til netsikkerhedstjenesten og ligeledes i de sager, hvor tilslutningen sker på baggrund af et påbud. Danske Regioner efterspørger en klar stillingtagen til ansvars-konstruktionen for data, såfremt der skal ske tilslutning til netsikkerhedstjenesten, eksempelvis om CFCS kan/skal betragtes som en databehandler for regionerne, selvstændig dataansvarlig eller fælles dataansvarlig.

Teknik og proces
Danske Regioner bemærker, at der i forhold til en eventuel udvidelse af den eksisterende netsikkerhedstjeneste, fx ved påbud, er behov for at få præciseret indholdet og omfanget af de tiltag og opgaver, som regionerne kan blive pålagt. Der er blandt andet behov for en præcisering af pkt. 3.1 og 3.3.3.1. i bemærkningerne til lovforslaget, hvor af det fremgår, at myndigheder kan blive pålagt at installere sikkerhedssoftware med passiv funktionalitet på sine enheder. Den tekniske løsning er ikke umiddelbart beskrevet tilstrækkeligt til, at der kan foretages endelig vurdering af, hvilke komplikationer det vil have i relation til regionernes drift og forretning. Der er flere aspekter, som er uklare eksempelvis, hvordan sikkerhedssoftwaren ses vedligeholdt i forhold til skiftende windows/citrix miljøer, og hvorvidt CFCS kan installere og opdatere uden om regioners s change managementproces – hvilket i sig selv potentielt kan udgøre en sikkerhedsrisiko. Dertil kommer, at den konkrete løsningsarkitektur ikke er beskrevet i forslaget, men det virker umiddelbart som meget vidtrækkende, at tilslutning til netsikkerhedstjenesten fordrer installering af software på den enkelte organisations enheder f.eks. pc'ere, servere og smart phones – hvilket i sig selv er omfattende.

Danske Regioner vil gerne påpege, at det på det nuværende grundlag er uklart, i hvilket omfang en installation af CFCS' sikkerhedssoftware vil påvirke driften af regionernes servere. Men der vil være en udfordring forbundet med tilslutningen til netsikkerhedstjenesten, hvis dette påvirker performance på regionernes netværk. Og i den henseende er det afgørende for Danske Regioner, at installationer af sikkerhedssoftwaren ikke besværliggør eller fordyrer opgradering, patchning eller udvikling af infrastrukturen og designes således, at hverken sikkerhedssoftwaren eller CFCS' handlinger har en negativ indvirkning på regionernes drift eller tilgængelighed til applikationer.

Endvidere forudses det, at implementeringen af softwaren på klinisk godkendt udstyr kan være en udfordring og udgør en risiko for, at implementering af sikkerhedssoftwaren på klinisk godkendt udstyr medfører en uacceptabel situation, hvor den kliniske godkendelse helt eller delvis bortfalder. Danske Regioner foreslår, at hvis sikkerhedssoftwaren skal implementeres på klinisk godkendt udstyr, skal der som minimum gennemføres en gennemgribende test, der viser, at sikkerhedssoftwaren *ikke* påvirker udstyrets funktionalitet og bringer patientbehandlingen i fare.

Center for cybersikkerhed håndtering og vidensdeling
De foreslåede udvidede beføjelser og deraf forventede øgede antal tilslutninger til netsikkerhedstjenesten vil øge den centraliserede datamængde hos CFCS. Dette, er faktorer, der i endnu højere grad udsætter CFCS for en risiko i forhold til at lamme kritiske dele af it-infrastrukturen i Danmark. Lovforslaget beskriver ikke, hvordan denne øgede risiko imødegås eller hvordan eventuelle konsekvenser håndteres.

Danske Regioner savner en angivelse af CFCS's muligheder/forpligtelser til at give regionernes adgang til indsamlede data, således at regionerne selv er i stand til at anvende disse (til rapporter, statistik, hændelser, anbefalinger, rådgivning mv.) til at løfte det generelle sikkerhedsniveau i regionerne.

Endeligt er der behov for en afdækning af, hvad tilslutning til netværkstjenesten løser ift. til de opgaver og ansvar, myndighederne har ift. egen cyber- og informationssikkerhed.

Økonomiske og administrative konsekvenser
Danske Regioner er positivt indstillet overfor, at tilslutningen til netsikkerhedstjenesten bliver gebyrfri. I og med at ingen af regionerne på nuværende tidspunkt er tilsluttet CFCS's netværkstjeneste, vil regionerne derfor ikke opnå en besparelse på grund af forslaget om, at det løbende gebyr for tilslutning af netværkstjenesten bortfalder.

Det er uklart, hvor mange lokale ressourcer en eventuel tilslutning til netværkstjenesten vil forudsætte i regionerne. Her tænkes blandt andet på medvirkning til netsikkerhedstjenestens opsætning og driften af tilhørende hardware og software. Da der ikke foreligger en tilstrækkelig beskrivelse af kravene til den tekniske løsning, herunder hvilke forudsætninger der skal være opfyldt, er det vanskeligt at be- eller afkræfte de fremførte antagelser vedr. de økonomiske konsekvenser. Da regionernes systemlandskaber er store og komplekse, må det dog forventes, at det ikke er en lille opgave at foretage implementeringen og driften, hvorfor der må forventes et betydeligt ressourceforbrug til opgaven med evt. tilslutning til netsikkerhedstjenesten.

Danske Regioner vil opfordre til, at der foretages en analyse af de tekniske og økonomiske konsekvenser forud for DUT-behandlingen.

Tekstnære bemærkninger
Ad forslagets §1
Det er værd at bemærke, at det i bemærkninger til lovforslagets enkelte bestemmelser vedr. § 1 anføres, at tilslutning til netsikkerhedstjenesten som en særlig variant kan forekomme ved, at logoplysninger fra fx en myndigheds eget sikkerhedssystem overføres til CFCS. Denne mulighed er væsentlig at opretholde, idet denne tilgang muliggør, at den enkelte myndighed har klarhed over hvilke data, der tilgår CFCS, samt muligheden for at få indblik i, hvilke informationer CFCS evt. videreformidler.

Ad forslagets § 3, stk. 1-4:
Det følger af lovforslagets § 3, stk. 1-4, at:

"Center for Cybersikkerheds netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder.

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."

Den sikkerhedsløsning, som CFCS imidlertid stiller til rådighed med netsikkerhedstjenesten, er efterretningsbaseret, hvilket formentlig besværliggør Danske Regioner s mulighed for at få fornuftigt og brugbart feedback til eget brug. Der er tilsyneladende ikke noget i lovforslaget, som pålægger CFCS at samarbejde, dele og kvalificere feedback. Der er alene tale om tilbagelevering af rådata-grundlaget (trafikdata, pakkedata og stationære data) for CFCS analyser og databrug.

Ad forslagets § 7, stk. 1-3;
Det foreslåede kapitel indebærer, at CFCS 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. Der vil i denne forbindelse heller ikke ske underretning af den pågældende bruger.

Det er retssikkerhedsmæssigt betænkeligt, at der i forbindelse med ovenstående alene er krav om, at oplysningerne skal kunne medvirke til at afdække sikkerhedshændelser og ikke en konkret mistanke om strafbar lovovertrædelse.

Ad forslagets § 8a, stk. 1:
Det bør tydeliggøres i bemærkningerne, hvilke oplysninger som er arkiveringspligtige. Ydermere bør det begrundes, hvorfor arkiveringen skal omfatte alle oplysninger omfattet af CFCS og ikke kun personoplysninger.

Ad forslagets § 17, stk. 2, pkt. 3:
Det følger af lovforslagets § 17, stk. 2, pkt. 3, at øvrige data, der ikke knytter sig til en sikkerhedshændelse, højest opbevares i 13 måneder. Umiddelbart savnes der en uddybning af, hvad behovet er for, at disse data kan opbevares i 13 måneder. Det fremstår ikke tydeligt, hvorfor det er nødvendigt, at data opbevares i længere tid, end hvad der er relevant i forhold til formålet, jf. hovedreglen i § 17, stk. 1.

Ad forsalgets §18:
Det bemærkes, at CFCS med lovforslaget får en bredere adgang til både pakke data og stationære data ift. gældende ret. CFCS opfordres til at genoverveje sine foranstaltninger ift. §18 i den gældende lov om Center for Cybersikkerhed. CFCS bør pålægges at logge i de tilfælde, at man tilgår pakke data og stationære data hos en myndighed.

Ad nr. 9 under almindelige bemærkninger til lovforslaget
Det bemærkes, at:

"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, dvs. sager, hvor der sker tilslutning på baggrund af et påbud."

Med henblik på at beskytte borgernes og patienternes rettigheder anbefales det, som minimum, 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, finder anvendelse for CFCS vedrørende centrets behandling af sager om tilslutning til netsikkerhedstjenesten og ligeledes i de sager, hvor tilslutningen sker på baggrund af et påbud.