Advokatrådet

ADVOKAT SAMFUNDET

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt til fmn@fmn.dk, tbl@fmn.dk og sbu@fmn.dk

KRONPRINSESSEGADE 28
1306 KØBENHAVN K
TLF. 33 96 97 98

DATO: 4. februar 2019
SAGSNR.: 2019-103
ID NR.: 576561

Høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden) – Forsvarsministeriets sagsnr.: 2018/006599

Ved brev af 7. januar 2019 anmodede Forsvarsministeriet Advokatrådet om eventuelle bemærkninger til ovenstående lovforslag.

Med lovforslaget sker der en stor udvidelse af de data, som Center for Cybersikkerhed får adgang til og indsamler. Center for Cybersikkerhed får endvidere adgang til oplysninger inde i de tilsluttede virksomheder. Der kan være tale om oplysninger, som er fortrolige i forhold til virksomheden. Der kan også være tale om personoplysninger, herunder følsomme personoplysninger om ansatte i virksomhedens private data.

Advokatrådet er bekymret for den store mængde af data, som Center for Cybersikkerhed vil indsamle med de nye værktøjer, som centret får med lovforslaget.

Advokatrådet opfordrer til, at det overvejes, om man ønsker, at en myndighed skal have adgang til så store mængder data. Det bør endvidere overvejes, om det er nødvendigt at indsamle så store mængder data i forhold til formålet hermed – og om det ønskede formål rent faktisk herved opnås. Advokatrådet skal i den anledning gøre opmærksom på, at en sådan mængde af data også giver muligheder for misbrug.

Advokatrådet finder det i den anledning bemærkelsesværdigt, at spørgsmålet om sikkerhed ikke er behandlet i lovforslaget. Hvis en myndighed skal råde over så mange data, bør der nøje redegøres for sikkerheden i forhold til den indsamlede data.

Advokatrådet finder også, at det er vigtigt, at der er tilstrækkelige muligheder for kontrol med de indsamlede data, herunder at Tilsynet med Efterretningstjenesterne har – eller får tilført – de nødvendige ressourcer hertil.

Lovforslaget giver endvidere mulighed for, at der uden retskendelse kan foretages indgreb omfattet af princippet i grundlovens § 72.

Det fremgår af bemærkningerne til lovforslaget, at en række forskellige indgreb ikke er egnet til domstolsprøvelse.

Advokatrådet finder det retssikkerhedsmæssigt betænkeligt, at det udelukkende overlades til Center for Cybersikkerhed at vurdere, hvornår de kan indsamle oplysninger, uden nogen form for domstolskontrol. Advokatrådet skal foreslå, at der som det mindste er en efterfølgende domstolskontrol.

Det fremgår af lovforslagets § 3, stk. 4, at Center for Cybersikkerhed i særlige tilfælde kan påbyde virksomheder, regioner og kommuner, der har særligt samfundsvigtig karakter, at blive tilsluttet netsikkerhedstjenesten.

Det står ikke Advokatrådet klart ud fra bestemmelsens formulering eller bemærkningerne hertil, i hvilke tilfælde det er, at Center for Cybersikkerhed kan påbyde eksempelvis en virksomhed at tilslutte sig netsikkerhedstjenesten.

Af retssikkerhedsmæssige grunde skal Advokatrådet opfordre til, at det i betydelig grad præciseres, i hvilke tilfælde Center for Cybersikkerhed kan anvende dette indgribende værktøj.

Det fremgår endvidere af lovforslaget, at Center for Cybersikkerhed som led i sin overvågning efter aftale med en given myndigheds eller virksomheds ledelse kan "iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder i myndigheden eller virksomheden". Ifølge lovforslagets bemærkninger kan centret i den forbindelse bl.a. gøre brug af andre medarbejderes identiteter og falske e-mails fra en medarbejder til en anden.

Der er således tale om "agent provocateur"-lignende metoder, hvor en medarbejder, som ikke på forhånd er mistænkt for regelbrud, uden dennes viden lokkes af Center for Cybervirksomhed til at bryde virksomhedens eller myndighedens sikkerhedsregler. Resultatet af aktiviteterne kan ifølge lovforslaget i sidste ende få ansættelsesretlige konsekvenser for den enkelte medarbejder.

Henset til konsekvenserne finder Advokatrådet det betænkeligt i forhold til den enkelte ansattes rettigheder, at en offentlig myndighed som Center for Cybersikkerhed vil kunne gøre brug af sådanne metoder.

Det fremgår desuden af bemærkningerne til lovforslaget punkt 3.2.3., at det vil kunne forekomme, at eksempelvis 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.

Det fremgår videre af bemærkningernes punkt 3.3.3.2., at 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.

Ovennævnte tilfælde kan stille en borger i en situation, hvor eksempelvis en kommune ikke er klar over, at borgeren har sendt en e-mail, hvilket kan have betydning for en afgørelse truffet over for den pågældende borger. Det berøres kort i bemærkninger til § 1, nr. 3, at der i visse tilfælde kan gives erstatning.

Advokatrådet skal hertil foreslå, at det nærmere undersøges, hvilke konsekvenser dette kan have for borgerne, og hvordan dette afhjælpes.

Med venlig hilsen

Nicolai Pii

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Akademikernes høringssvar vedrørende lovforslag om ændring af lov om Center for Cybersikkerhed

Den 8. februar 2019
Sagsnr. S-2019-034
Dok.nr. D-2019-5075
ds/bef

AKADEMIKERNE

THE DANISH CONFEDERATION
OF PROFESSIONAL ASSOCIATIONS

Nørre Voldgade 29, 2. sal
DK – 1358
København K.

T +45 3369 4040
E ac@ac.dk
W www.ac.dk

Akademikerne har modtaget høring vedrørende Forsvarsministeriets forslag til lov om ændring af lov om Center for Cybersikkerhed og har følgende bemærkninger:

Helt overordnet vil Akademikerne anbefale, at lovforslaget i den nuværende affatning ikke fremsættes i Folketinget, og at Forsvarsministeriet i stedet udarbejder et helt nyt lovforslag, hvor det reelt er muligt for høringsparterne (i en ny høring) at vurdere, hvilke beføjelser som Center for Cybersikkerhed får, og hvordan disse beføjelser er afgrænset af objektive bestemmelser.

Når staten gør indgreb i borgernes grundlæggende ret til privatliv, er det et krav efter retspraksis fra den Europæiske Menneskerettighedsdomstol, at disse indgreb sker via et retsgrundlag, som er klart og præcist, og at anvendelsen af dette retsgrundlag skal være forudsigeligt for de personer, som er omfattet af dets anvendelsesområde. Det lovudkast, som er sendt i høring, lever ikke op til disse krav, fordi det er totalt umuligt at vurdere rækkevidden af lovforslagets bestemmelser.

Det er også et krav, at indgreb i retten til privatliv skal være egnet til at forfølge et formål af almen interesse, samt være nødvendigt og proportionalt. Et indgreb kan kun anses for at være nødvendigt, hvis der ikke findes mindre indgribende foranstaltninger, som kan opfylde formålet af almen interesse.

I forhold til lovforslagets ansættelsesretlige aspekter skal det oplyses, at Akademikerne ser med meget stor alvor herpå – særligt den del, der vedrører spørgsmålet om målrettede indsamlinger af oplysninger, opsætning af fælder m.v. for konkret udvalgte medarbejdere i virksomheder eller hos myndigheder.

Akademikerne finder det meget bekymrede, at en statslig myndighed skal have mulighed for at optræde under fordækte identiteter, opsætte fælder, målrette angreb mod enkelte medarbejdere/enkeltpersoner, og at anvende kollegerne i den forbindelse m.v.

Der vil være tale om en banebrydende ændring af de retssikkerheds-principper, der gælder på det ansættelsesretlige område.

Det forhold, at Center for Cybersikkerhed gives tilladelse til at anmelde en ansat til den ansattes arbejdsgiver for at have overtrådt interne IT-sikkerhedsforskrifter, indeholder efter Akademikernes opfattelse to helt uacceptable momenter, dels at centret anmelder til en privat juridisk person og ikke til anklagemyndigheden, dels at der anmeldes i forhold til overtrædelse af nogle lokalt udfærdigede IT-forskrifter, som i princippet kan indeholde hvad som helst, som ikke har noget fæste i lovgivningen.

En medarbejder, der i øvrigt umiddelbart intet suspekt foretager sig, kan uforvarende "falde i fælden" – med de konsekvenser dette måtte have for den enkeltes ansættelsesforhold. Lovforslaget anvender decideret udtrykket at "franarre medarbejdere bestemte oplysninger". Det fremgår, at det er for at teste den enkeltes omgang med mistænkelige afsendere, men der er f.eks. i udgangspunktet næppe tale om en mistænkelig afsender, hvis der er tale om en kollega. Det er efter Akademikernes opfattelse at gå alt for vidt.

Dette er yderst problematisk, og er desuden i sit udgangspunkt i strid med de sædvanlige grundlovsfæstede rettigheder, EMK m.v.

Akademikerne vil derfor advare imod indførelse af regler, der på den vis indfører legaliseret mistænkeliggørelse af ansatte, og tilsidesætter deres grundlæggende rettigheder.

Det kan desuden bemærkes, at lovforslagets ansættelsesretlige aspekter ikke er blevet drøftet mellem parterne – hverken på det offentlige eller på det private område.

Det kan samtidig oplyses, at lovforslaget kan underminere de generelle aftaler, som aftaleparterne på det offentlige område har indgået om kontrolforanstaltninger. Formålet med disse aftaler er at skabe størst mulig tryghed for de ansatte i forbindelse med en offentlig arbejdsgivers eventuelle anvendelse af kontrolforanstaltninger.

Kontrolforanstaltninger skal være sagligt begrundede i driftsmæssige årsager og have et fornuftigt formål. Kontrolforanstaltninger skal indrettes således, at der er et rimeligt forhold mellem formål og midler. Kontrolforanstaltningerne må ikke være krænkende over for medarbejderne, og de må ikke forvolde medarbejderne tab eller nævneværdige ulemper. På hjemmearbejdspladser må der ikke indføres kontrolforanstaltninger, der krænker privatlivets fred.

Der er således grænser for, hvilke kontrolforanstaltninger en ledelse må iværksætte over for sine medarbejdere. Der er også en orienteringspligt, som man kun må se bort fra ved konkret mistanke om snyd.

Ingen af de beskyttelser efterleves, hvis Center for Cybersikkerhed får hjemmel til at lave fiktive angreb.

Med venlig hilsen

Dario Silic
D: 21353728
E: ds@ac.dk

Høringsnotat

København, den 6. februar 2019

Høringssvar over udkast til forslag til lov om Center for Cybersikkerhed. (Initiativer til styrkelse af cybersikkerheden).

(Sagsnr. 2018/006599).

Ved mail af 7. januar 2019 har Forsvarsministeriet anmodet om Amnesty Internationals eventuelle bemærkninger til ovennævnte udkast til ændring af lov om Center for Cybersikkerhed.

Generelle bemærkninger

Amnesty International er enig i den grundlæggende betragtning bag udkastet: At det er af afgørende betydning, at det danske samfund sikres en effektiv beskyttelse mod cyberangreb.

Men når man læser udkastet, efterlades man med et indtryk af, at de seneste ti-tolv års diskussioner om forholdet mellem borgernes sikkerhed og borgernes retssikkerhed – og hvordan vi sikrer, at borgernes retssikkerhed ikke kommer unødigt under pres - er gået ubemærket hen i Forsvarsministeriet, FE og Center for Cybersikkerhed.

Diskussionen om sikkerhed og retssikkerhed har fyldt meget – især i 2006-2008 i forbindelse med diskussioner om politiets beføjelser til at iværksætte aflytninger og overvågninger - og den retlige prøvelse af mistankekrav og nødvendighed.

I 2016 afgjorde EU-domstolen i en sag mod Sverige, at logningsdirektivet var i strid med retten til privatliv efter artikel 8 i Den Europæiske Menneskerettighedskonvention – og afgørelsen burde have ført til, at den danske regering havde ophævet den danske logningsbekendtgørelse (som påbyder danske internetudbydere at gemme trafikdata i et år) – hvilket som bekendt ikke skete og endnu ikke er sket.

Disse og mange andre diskussioner om afvejningen mellem sikkerhed på den ene side og retssikkerhed på den anden ses ikke at have sat sig nogen spor i det fremsendte udkast.

Tværtimod indeholder forslaget meget betydelige udvidelser af Center for Cybersikkerheds beføjelser, uden at der på nogen måde søges at indføre nogen former for uafhængig kontrol med Centeret, således at man kunne have talt om en balance mellem de betydeligt udvidede beføjelser og behovet for at beskytte myndighedernes, virksomhedernes og borgernes privatliv.

Det fremgår af bemærkningerne, at formålet med forslaget blandt andet er at få flere myndigheder og virksomheder til at indgå i Centerets netsikkerhedstjeneste. Hidtil har alene et fåtal af myndigheder og virksomheder ønsket at lade sig indrullere i Centerets netsikkerhedstjeneste, hvilket i bemærkningerne henføres til, at det har været for dyrt at deltage. Derfor skal det fremover være gratis at være omfattet af netsikkerhedstjenesten.

Det er dog, som om forslagsstillerne ikke selv tror på, at det er gebyret, som er grunden til, at især virksomheder har afholdt sig fra at slutte sig til netsikkerhedstjenesten. En af de vigtigste nyskabelser i forslaget er, at Centeret for Cybersikkerhed, hvis forslaget vedtages, kan *pålægge* myndigheder og virksomheder at slutte sig til netsikkerhedstjenesten. (Så vidt Amnesty har kunnet forstå på de seneste dages drøftelser i medierne, har kun to private virksomheder sluttet sig til netsikkerhedstjenesten under den hidtidige ordning.)

Det afgørende nye er, at hvor Center for Cybersikkerhed i dag kun monitorerer datatrafik på de forbindelser, der går ind og ud af de tilsluttede myndigheder og virksomheder, skaber lovforslaget mulighed for at installere sikkerhedssoftware på f.eks. pc'ere, servere, tablets, mobiltelefoner m.v. hos de myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten.

Som noget nyt er det meningen, at Centeret skal kunne installere sikkerhedssoftware, ikke bare i den ydre firewall, men også på den indre firewall, herunder servere og stationære pc'er hos den pågældende myndighed eller virksomhed. Efter forslaget skal også tablets og mobiltelefoner kunne tilsluttes.

Man må forstå, at de tilsluttede myndigheder og virksomheder vil blive underrettet, når der installeres sikkerhedssoftware, honey pots, sink holes osv. Men de medarbejdere, som arbejder med de pågældende netværk og pc'er, m.v. nævnes ikke. De skal ikke underrettes om, at deres færden bliver overvåget.

Man savner i det hele taget et overslag over de praktiske konsekvenser, over hvor mange myndigheder, virksomheder, netværk, pc'er eller brugere, der samlet set forventes at blive omfattet eller "ramt" af Center for Cybersikkerheds fremtidige udvidede adgang til transportdata, pakkedata og stationære data.

Som forslaget er formuleret, efterlader det – bevidst eller ikke bevidst – et billede af, at det blot er et hjørne af vores samfund, der undergives en tættere, ureguleret overvågning, hvor man reelt skulle anerkende, at der snarere er tale om, at vores samfund som sådant kan gå fra et niveau af ureguleret overvågning til et andet.

Særligt savnes en reel begrundelse for det gennemgående fravær af domstolskontrol med Centerets tilgang til oplysninger hos myndigheder og virksomheder.

Konkrete bemærkninger

Om indgreb omfattet af grundlovens § 72.

Udkastet indeholder en række bestemmelser – i udkastet til lovs kapitel 4 – indgreb omfattet af grundlovens § 72, hvor der er tale om at foretage indgreb i retten til privatliv – eller indgreb i brevhemmeligheden.

Af udkastet til § 4 fremgår, at Center for Cybersikkerhed skal kunne behandle trafikdata, pakkedata og stationære data hidrørende fra tilsluttede myndigheder *uden retskendelse* med henblik på at understøtte et højt informationssikkerhedsniveau.

Hvor det i dag alene er netværkskommunikation, Centeret kan behandle, vil Centeret fremover kunne behandle enkelte enheder (pc'ere) på lokale netværk, smartphones og tablets.

Det anføres videre i bemærkningerne, side 18, at *"Det bemærkes, at anvendelsen af sikkerhedssoftware – både med passiv og aktiv funktionalitet – 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 (elektroniske data) og brud på meddelelseshemmeligheden (kommunikation gennem email 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."

Det fremgår videre af bemærkningerne, at forslaget betyder, at de data, som kunne udløse en sikkerhedsbegivenhed efter forslaget ikke blot er data, som bevæger sig mellem to forskellige virksomheder, men også kan være "private" data, der befinder sig lagret på en pc hos en medarbejder – som der derfor kan blive tale om at tilgå.

Det konkluderes i bemærkningerne, at en sådan tilgang til disse "private" data vil kunne udgøre et indgreb omfattet af grundlovens § 72, hvorfor der efter ministeriets opfattelse er behov for en udtrykkelig hjemmel.

Forsvarsministeriet har derfor overvejet, om der er behov for en ordning, hvor der sker forudgående indhentelse af retskendelse – men når side 18 frem til, at det vil være for besværligt, og at man derfor ikke bør indføre krav om en retskendelse – hverken forudgående eller efter den eventuelle sikkerhedshændelse:

"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."*** (Vores udhævning).

Denne argumentation for ikke at anvende domstolskontrol er efter Amnestys opfattelse bagvendt. Når en domstol skal tage stilling til, om der er tilstrækkeligt grundlag for at gennemføre en ransagning eller iværksætte en aflytning/overvågning, så sker det vel også ud fra en *samlet vurdering af "trusselsbilledet"*, og ikke ud fra en forventning om kvaliteten af de konkrete data, som forventes at komme frem ved ransagningen.

Forsvarsministeriet leverer ikke en holdbar argumentation for, hvordan det retfærdiggøres, at det, som ministeriet *selv* kalder et indgreb omfattet af grundlovens § 72, ikke i fremtiden skal kræve domstolskontrol.

Endelig skal det bemærkes, at de retlige kriterier for at tilgå disse data er ganske løst formulerede – idet det eneste krav er, at behandlingen sker for at understøtte "*et højt informationssikkerhedsniveau i samfundet."*

Om forslag til ny § 5.

Efter forslaget til § 5 skal Centeret – ved **begrundet mistanke** om en sikkerhedshændelse – kunne behandle stationære data (dvs. data, som er lagret i netværk og pc'er *i virksomheden eller hos myndigheden)* fra en myndighed eller virksomhed, der ikke er tilsluttet netsikkerhedstjenesten – ***uden retskendelse*** – når myndigheden/virksomheden har anmodet Centeret om bistand, stillet de stationære data til rådighed for netsikkerhedstjenesten og givet skriftligt samtykke til behandlingen – **og** behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

Også for § 5 anerkender Forsvarsministeriet, at bestemmelsen isoleret omhandler situationer/indgreb, der er omfattet af grundlovens § 72 – og at der derfor er behov for positiv lovhjemmel til at foretage de pågældende indgreb.

Særligt i en situation hvor der efter ministeriets opfattelse kan være tale om myndigheder eller virksomheder med så mange ansatte, at det reelt ikke er muligt at indhente samtykke fra alle berørte medarbejdere, er det nødvendigt – konkluderer ministeriet - at der tilvejebringes hjemmel til at foretage indgreb omfattet af grundlovens § 72.

Det anføres i bemærkningerne, side 22:

"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."***
(Vores udhævning)

Efter Amnestys opfattelse er Forsvarsministeriets argumentation for ikke at kræve domstolskontrol med indgreb, som åbenbart vil være omfattet af grundlovens § 72 også her nærmest bagvendt.

For det første kan man ikke sammenligne med stikprøvekontroller i fødevareindustrien og andre brancher, hvor stikprøvekontrol skal sikre en forsvarlig kvalitet. De varer, som kontrolleres i fødevareindustrien – og ikke lever op til den krævede standard - er ikke omfattet af retten til privatliv eller brevhemmeligheden. Videre kan man ikke læne sig tilbage og sige, at alt er godt, når blot man har samtykke fra myndighedens eller virksomhedens ledelse. Det ændrer ikke på, at det vil være et indgreb omfattet af grundlovens § 72 over for medarbejderne, når Centeret går ind og undersøger samtlige medarbejderes pc'er, smartphones, tablet etc.

Endelig kortsluttes ræsonnementet i forhold til domstolskontrollens formål, når ministeriet konstaterer, at når det **"således er vanskeligt at opstille et retligt kriterium, som domstolene vil kunne påse overholdelsen af – bør undersøgelsen kunne foretages uden retskendelse."**
(Vores udhævning).

Efter Amnestys opfattelse må svaret være, at hvis man ikke kan opstille et retligt kriterium, som skal være opfyldt, for at Centeret kan gå ind og kontrollere en given myndighed eller virksomhed, (og som kan efterprøves af en domstol) så bør Centeret afholde sig fra - eller ikke have myndighed til at foretage sådanne handlinger.

Også her er kravet om, at behandlingen skal vurderes at bidrage til at understøtte et højt informationssikkerhedsniveau et nærmest tomt kriterium.

Om forslag til § 6

Også i forhold til de beføjelser, som Center for Cybersikkerhed får til at behandle trafikdata, pakkedata og stationære data hidrørende fra de tilsluttede myndigheder og virksomheder – uden retskendelse - må man efterlyse en retlig konstruktion, hvorefter Centeret ville være undergivet uafhængig kontrol – domstolskontrol. Som udkastet er formuleret, vil Centeret kunne tilgå en lang række personlige og rent private data om borgerne, der ikke har saglig relevans for sikkerhedshændelse.

Om forslag til § 17, opbevaringstid

Det fremgår af § 17, stk. 1, at data, der er omfattet af kapitel 4 – om indgreb, der er omfattet af grundlovens § 72 – skal slettes, når formålet med behandlingen er opfyldt, eller efter højst 5 år, uanset om formålet er opfyldt.

Data, som ikke hidrører fra en sikkerhedshændelse, men fra bestemte myndigheder, som særligt beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold – og virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold, må højst opbevares i 3 år. Er data i medfør af § 16 videregivet til andre end den myndighed eller virksomhed, som de pågældende data hidrører fra, finder stk. 1 og 2 ikke anvendelse.

Dét forstår Amnesty International således, at der ikke gælder nogen længste frist for sletning af data, der er videregivet til andre myndigheder eller virksomheder end den, som de pågældende data hidrører fra.

Det er ikke indlysende, hvorfor man skal kunne gemme data, som ikke hidrører fra en sikkerhedshændelse, i 3 år, eller hvorfor slettefristen efter denne lov helt ophæves, hvis data gives videre til andre myndigheder eller virksomheder end dem, som oplysningerne stammer fra.

En generel slettefrist på 5 år forekommer også at være unødigt og uønskeligt lang, når man betænker fraværet af uafhængig retlig kontrol med Center for Cybersikkerhed.

Amnesty International, 6. februar 2019.

Fra: Flemming Dreesen <FLD@da.dk>
Sendt: 5. februar 2019 15:34
Til: FMN-MYN-FORSVARSMINISTERIET
Emne: Korrektion/ DA's høringsvar: Høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed
Vedhæftede filer: Høringsbrev.pdf; Høringsliste.pdf; Lovudkast.pdf

Kategorier: Mille

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

DA skal alene til forslaget til § 6a bemærke, at de beskrevne forebyggelsesaktiviteter, der efter anmodning af centret kan iværksættes på en virksomhed, må antages at være omfattet af de gældende arbejds- ansættelsesretlige principper. DA og LO har således f.eks. indgået en aftale om kontrolforanstaltninger af 27. oktober 2006.

DA skal i øvrigt henvise til høringssvar fra DI og DE.

Forsvarsministeriet bedes se bort fra DA's mail fra 9. januar 2019.

Fra: Forsvarsministeriet <fmn@fmn.dk>
Sendt: 7. januar 2019 16:02
Emne: Høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed

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

Forsvarsministeriet sender hermed udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden) i høring.

Til:
Forsvarsministeriet
Holmens Kanal 9
1060 København K

fmn@fmn.dk

Dok. ansvarlig: PHA / RPR / MOB
Sekretær: SLS
Sagsnr: s2019-060
Doknr: d2019-2047-11.3
04-02-2019

Høringssvar til forslag til lov om ændring af lov nr.713 om Lov om Center for Cybersikkerhed. Journal nr. 2018/006599,

Dansk Energi takker for muligheden for at afgive høringssvar på forslag til lov om ændring af lov om Center for Cybersikkerhed.

Helt overordnet ser Dansk Energi positivt på, at Center for Cybersikkerhed (CFCS) arbejder for at styrke cybersikkerheden i Danmark, og vi samarbejder naturligvis meget gerne herom. Det er væsentligt, at vi sammen kan imødegå sikkerhedshændelser i de samfundsvigtige sektorer, og det vil uden tvivl kræve et tæt og tillidsfuldt samarbejde fra begge parters side.

I den forbindelse vil vi også gerne udtrykke vores forståelse for, at CFCS har behov for et mere detaljeret indblik i trusselsbilledet mod danske virksomheder, der har særlig samfundsvigtig betydning, herunder visse energi- og forsyningsvirksomheder. Som branche ser vi positivt på, at energi- og telesektorerne kan bistå CFCS og bidrage til at skabe et opdateret og repræsentativt trusselsbillede mod Danmark.

Lovforslaget står til at ramme bredt, og den kommende regulering vil således potentielt omfatte både elnetselskaber, elproducenter, balanceansvarlige virksomheder og fibernet-selskaber qua deres rolle som samfundsvigtige aktører i såvel energi- som telesektoren.

Lovforslaget rejser derfor også en række spørgsmål og bekymringer for disse aktører, ligesom vi som branche efterspørger en ramme for det fremtidige samarbejde. Dette er nærmere uddybet nedenfor under følgende hovedafsnit:

- Behov for præcisering af lovens omfang og konsekvens
- Videndeling og ramme om fremtidigt samarbejde
- Økonomi
- Sammenhængen til øvrige internationale initiativer
- Øvrige forhold.

Behov for præcisering af lovens omfang og konsekvens

Dansk Energi ser behov for, at lovforslaget præciseres og uddybes i forhold til følgende tre punkter:

- Omfattede virksomheder – frivilligt eller ved pålæg
- Omfanget af og behandlingen af oplysninger/data, der indsamles
- CFCS' ansvar overfor virksomhederne.

Omfattede virksomheder

I forhold til de virksomheder, som efter forslaget skal være omfattet af loven, er der er et behov for, at dette uddybes i lovforslaget. Det må klart fremgå, hvilke kriterier der kan indgå i CFCS' vurdering af, hvilke virksomheder der ***kan*** tilsluttes netsikkerhedstjenesten, og hvilke der ved eventuelt pålæg ***skal*** tilsluttes. Endvidere bør det uddybes, hvad der nærmere menes med virksomheder af *samfundsvigtig karakter* og virksomheder af ***særlig*** *samfundsvigtig karakter.* Der henvises til lovforslagets § 3 og bemærkningerne hertil.

Det er afgørende for virksomhederne, at denne vurdering foretages på proportionale og gennemskuelige vilkår, ligesom det må kræves, at CFCS' afgørelse herom er begrundet og kan påklages. Dansk Energi efterspørger derfor, at der som minimum indsættes en klar præcisering af lovbemærkninger, så det utvetydigt fremgår, hvilke kriterier der skal indgå i CFCS' afgørelse efter forslagets § 3, stk. 3, og i afgørelse om pålæg efter forslagets § 3, stk. 4. Ligeså bør det fremgå, hvad grundlaget er for udvælgelsen af virksomheder.

Dansk Energi opfordrer endvidere til dialog og forventningsafstemning i forhold til eventuelle kritiske leverandører til virksomheder i energi- og telesektorerne, som forventes at blive omfattet af krav om tilslutning til netsikkerhedstjenesten.

Endelig bemærkes, at lovforslaget lægger op til, at det alene er et fåtal af virksomheder og ikke en hel sektor, som forventes tilsluttet. Trusselsbilledet som CFCS' netsikkerhedstjeneste vil få indblik i fra energi- og telesektorerne vil derfor i sagens natur kun være en delmængde af det samlede trusselsbillede mod energi- og telesektorerne.

Omfanget af og behandlingen af data

Lovforslaget lægger op til, at CFCS kan få kendskab til meget store mængder af data, hvor data kan falde ind under det brede formål om "at understøtte et højt informationssikkerhedsniveau" eller som kan benyttes til at "opdage, analysere eller som kan bidrage til at imødegå sikkerhedshændelser." Disse meget store datamængder hos myndigheder og virksomheder omfatter således også personhenførbare oplysninger som fx elforbrugsdata, telefonsamtaler og internetforbrug, e-mailkorrespondancer, SMS'er, medarbejderes hjemmeside-besøg mv.

Der er derfor efter Dansk Energis opfattelse brug for en nærmere beskrivelse af, hvad der ligger i at "opdage, analysere eller som kan bidrage til at imødegå sikkerhedshændelser" eller "understøtte et højt informationssikkerhedsniveau". Dette er kun meget overfladisk behandlet i lovforslaget, uanset at det er med sådanne brede formål, at der hjemles adgang for CFCS uden retskendelse til at behandle trafikdata, pakkedata og stationære data. Der henvises i den forbindelse til lovforslagets kapitel 4 og 4a, §§ 4-6 samt 6a-6c., og i særdeleshed til bemærkningerne til disse bestemmelser.

Det er i den forbindelse Dansk Energis ønske, at datatilgangen så vidt muligt indskrænkes i forhold til elforbrugsdata, telefonsamtaler og internetforbrug, indhold i e-mailkorrespondancer og SMS'er, medarbejderes hjemmeside-besøg mv. eller anden data, som ikke er relevante for, at CFCS "*kan opdage, analysere eller som kan bidrage til at imødegå sikkerhedshændelser"* eller som er egnet til at "*understøtte et højt informationssikkerhedsniveau*."

Det må være et krav at skulle sådanne irrelevante data alligevel komme til CFCS' kendskab, må de slettes forud for evt. videregivelse. I modsat fald kan det frygtes, at den indsamling af data, som lovforslaget giver CFCS adgang til, får karakter af egentlig overvågning snarere end sikring af vores cybersikkerhed.

Dansk Energi ønsker her at henlede CFCS' opmærksomhed på, at det i sidste ende uvilkårligt bliver den enkelte myndighed og virksomhed, som vil møde både borgere, kunder og medarbejdere, og dermed vil skulle forklare, argumentere og stå på mål for, at CFCS foretager denne overvågning. Derfor er der behov for meget klare rammer for CFCS' overvågning, således at dette kan formidles i et klart og forståeligt sprog til alle.

Af bemærkningerne til nr. 3 fremgår, at adgang uden retskendelse er en videreførelse af gældende ret dog med en udvidelse til også at omfatte stationære data. Det fremgår endvidere, at indgrebet kan foretages, "når behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau".

Det bør efter Dansk Energis opfattelse tilføjes, at adgang til data uden retskendelse fordrer, at CFCS kan godtgøre, at der er en begrundet mistanke om en sikkerhedshændelse og i øvrigt naturligvis, at indgrebet var nødvendigt for ikke at forspilde muligheden for at identificere en sikkerhedshændelse.

Yderligere opfordres til, at forholdet til GDPR uddybes. Der henvises til afsnit 9 i de almindelige bemærkninger, hvor det udtrykkeligt fremgår, at videregivelse af data jf. artikel 6 kan være i overensstemmelse med databeskyttelsesforordningen "i det omfang det er strengt nødvendigt og forholdsmæssigt for at sikre net- og informationssikkerheden". Dansk Energi vil derfor opfordre til, at det præciseres, efter hvilke kriterier CFCS kan finde, at det er "strengt nødvendigt" og "forholdsmæssigt" for at sikre net- og informationssikkerhed.

Dansk Energi finder det uklart, hvorvidt forsyningskritiske IT-systemer (læs: ikke-administrative IT-systemer) står til at blive omfattet af CFCS' monitorering af data, fx IT-systemer som indgår som en del af den operationelle drift af elnettet og elproduktionsanlæg. Såfremt dette er tilfældet, bør det i forbindelse med Lovtekst §1, stk. 3, præciseres, at enheder i forsyningskritiske IT-systemer (fx "produktions- og proces-IT"), der anvendes til fysisk styring af den omtalte kritiske infrastruktur, ligeledes er omfattet af lovforslaget.

Uagtet, at brug af kryptering kan udgøre en overvågningsmæssig udfordring, udgør kryptering også en sikkerhedsforanstaltning for virksomhederne. Ud fra et sikkerhedsmæssigt synspunkt anbefaler Dansk Energi derfor, at det fastholdes, at CFCS ikke kan forlange at få udleveret krypteringsnøgler fra myndigheder, virksomheder eller borgere jf. lovbemærkningerne til nr. 3 (side 56). Dog er vi opmærksomme på, at der alligevel kan være helt særlige hensyn, der kan retfærdiggøre en udlevering i samfundets interesse.

CFCS' ansvar overfor virksomhederne
I lovbemærkninger til §6 (side 58) anføres det, at aktivt cyberforsvar kan indebære en risiko for, at der kan ske fejl, og at det "*… således ikke (kan) 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.*"

Dansk Energi ønsker at udtrykke bekymring overfor muligheden for brugen af aktivt cyberforsvar hos energi- og teleselskaberne – særligt, hvis det aktive cyberforsvar etableres på forsyningskritiske IT-systemer.

Det bør derfor være et krav, at de virksomheder som – frivilligt eller ved pålæg – bliver omfattet af CFCS' aktive monitorering, overvågning, installation af sikkerhedssoftware, etablering af honey pots mv. er velinformerede om de risici og konsekvenser, som et aktivt cyberforsvar kan medføre. CFCS bør derfor ikke kunne pålægge en virksomhed at blive omfattet af aktiv monitorering, overvågning, installation af sikkerhedssoftware, etablering af honey pots mv., hvis virksomheden ikke selv er indstillet på at acceptere de tilbageværende risici, som måtte blive identificeret i dialogen med CFCS forud for tilslutning, og som en forudgående koordinering mellem virksomheden og CFCS har søgt at begrænse til et minimum.

Dansk Energi tolker bemærkningerne således, at CFCS' netværksovervågning kan føre til forretningsmæssige tab for virksomheden, herunder produktionstab, klagesager, GDPR-sager el.lign. Dansk Energi efterspørger derfor en uddybning og redegørelse for det erstatningsansvar, som i sådanne tilfælde påhviler CFCS, herunder om dette vil blive en del af tilslutningsbetingelserne, uanset om tilslutning foregår frivilligt eller efter pålæg. Dansk Energi forventer, at en tilsluttet virksomhed, som evt. måtte lide et tab som følge af CFCS' monitorering og overvågning kompenseres herfor.

Det ønskes samtidig uddybet, i hvilket omfang CFCS yder support (incident respons, responstid mv.), når CFCS går ind og blokerer trafik som led i en aktiv monitorering af data og et aktivt cyberforsvar. Dette ønske for uddybning skal ses i sammenhæng med evt. monitorering af forsyningskritiske IT-systemer, hvor en forsinkelse i datastrømme eller datapakker kan forstyrre driften af elnet eller elproduktionsenheder og i værste fald lede til strømafbrydelser, fysisk skade på elanlæg og potentiel personfare.

Det bør endvidere præciseres, at CFCS jf. den foreslåede § 6a og bemærkningerne hertil alene må foretage forebyggende sikkerhedstekniske undersøgelser, såsom fx aktive scanninger, penetrationstests, social engineering mv. mod tilsluttede virksomheder på frivillig basis og alene på tidspunkter og mod angrebsmål mv., som er aftalt og koordineret med virksomheden på forhånd.

Videndeling og ramme om fremtidigt samarbejde
Som nævnt indledningsvist fordrer en succes på dette område et tæt og tillidsfuldt samarbejde mellem virksomheder og myndigheder. Dansk Energi er derfor positiv over, at CFCS med den foreslåede §16 nu må videregive information om angreb og cybertrusler. Vi ser en sådan videndeling som en nødvendig forudsætning for et robust cyberforsvar og et hurtigt-reagerende beredskab.

Med lovforslaget er CFCS sikret adgang til store mængder af data. Lovforslaget lægger dog op til, at CFCS alene skal fokusere på de mest avancerede angreb, mens virksomhederne selv vil skulle håndtere alle andre sikkerhedshændelser.

Det ønskes derfor uddybet, i hvilket omfang CFCS vil informere tilsluttede virksomheder om (simple) sårbarheder eller trusler, som CFCS måtte få kendskab til, uagtet at lovforslaget lægger op til, at sådanne informationer reelt forventes identificeret og håndteret af de ydelser og services, som kommercielle IT-sikkerhedsfirmaer leverer til virksomhederne i dag.

Dansk Energi vil opfordre til en drøftelse af mulighederne for, at energi- og telesektorernes virksomheder i rimeligt omfang kan modtage trusselsinformation og indikatorer fra CFCS også for sikkerhedsrisici, som umiddelbart falder uden for CFCS fokusområde, men som er kommet til CFCS' kendskab. Tilsvarende kan virksomhederne bidrage med trusselsinformation og indikatorer til CFCS, som ligger inden for CFCS' fokusområde, og som opdages i kraft af virksomhedernes egen drift.

Dansk Energi finder, at det er i delingen af sådanne oplysninger om malware, oplevede og afværgede sikkerhedshændelser mv., at CFCS, virksomhederne og de samfundsvigtige sektorer i fællesskab har mulighed for at skabe et optimalt informationssikkerhedsniveau. I Dansk Energis optik er det derfor både i virksomhedernes og i samfundets interesse, at risici og sårbarheder kommer til de(n) relevante virksomhed(er)s kendskab og håndteres på betryggende vis, ligegyldigt hvem der måtte opnå eller besidde et givent kendskab før andre.

Dansk Energi anbefaler derfor, at CFCS bør videregive information og data til en tilsluttet virksomhed, når der er tale om begrundet mistanke om en alvorlig sikkerhedshændelse mod den pågældende virksomhed, hvor angrebet vurderes som avanceret, eller hvor det vurderes, at der er tale om en sikkerhedshændelse af væsentlig samfundsmæssig betydning.

CFCS' videregivelse af information og data om tilsluttede virksomheder til tredjepart, herunder fx danske myndigheder, andre netsikkerhedstjenester samt myndigheder og virksomheder i øvrigt, bør som hovedregel ske efter forudgående accept fra den tilsluttede virksomhed, som information og data er relateret til. Videregivelse af information til tredjepart bør i videst muligt omfang ske i anonymiseret form, således at en given virksomhed ikke kan identificeres i de data, som videregives.

Dansk Energi ser gerne en tættere dialog med CFCS om, hvordan energi- og telesektorerne sammen med de øvrige samfundsvigtige sektorer kan skabe et fortroligt og tillidsbaseret rum og platform med CFCS med henblik på at sikre bedst mulig tværsektoriel videndeling, i forhold til at alle bidrager til det samlede trusselsbillede mod Danmark.

I forhold til fremtidig videndeling oplever Dansk Energi et presserende behov for at få klarlagt rollefordelingen mellem CFCS (Cybersituationscentret, Netsikkerhedstjenesten og Trusselsvurderingsenheden), de sektoransvarlige myndigheder, herunder de sektorspecifikke DCIS-enheder, tilsynsmyndigheder og sektorernes medarbejdere samt eksisterende og fremtidige sektorCERTer og virksomhederne.

Fra Dansk Energis side finder vi, at den fremtidige rollefordeling har afgørende betydning for et succesfuldt samarbejde mellem myndigheder og virksomhederne både før, under og efter en sikkerhedshændelse.

Økonomi

Lovforslaget omtaler i afsnit 3.1.1. om gældende ret at…"… virksomheder, der tilsluttes Center for Cybersikkerheds netsikkerhedstjeneste, skal betale et årligt gebyr, som dækker centerets udgifter til *tilslutning og drift* af den anvendte alarmenhed." Senere fremgår det, at gebyret har udgjort mellem 300.000 kr. og 400.000 kr. pr. alarmenhed afhængig af den valgte type alarmenhed. Efter forslaget er det imidlertid alene *tilslutningen*, som nu tilbydes uden betaling.

Det er derfor uklart, hvorledes omkostningerne til driften håndteres, herunder om driften skal finansieres af virksomhederne, ligesom størrelsen af sådanne omkostninger bør konkretiseres. Dette efterlader en række uafklarede spørgsmål, særligt når henses til, at der af bemærkningerne fremgår, at virksomhederne alene forudsættes at have begrænsede udgifter som led i et samarbejde med CFCS.

CFCS' opgaver og varetagelse heraf er yderligere af national interesse. Dansk Energi efterspørger derfor en nærmere afklaring af, hvordan virksomhedernes omkostninger i forbindelse med CFCS' netsikkerhedstjeneste fordeles. Finansieringen af en sådan national opgave bør ikke være på lokale elforbrugeres regning, men bør i Dansk Energis optik finansieres kollektivt.

Skulle ministeriet være uenig i, at omkostninger til netsikkerhedstjenesten skal finansieres kollektivt, ønsker vi følgende forhold afklaret:

- Hvilke ressourcer/omkostninger skal virksomhederne forvente at skulle afholde/afse ved tilslutning/indkøring?

- Hvilke efterfølgende driftsomkostninger skal virksomheder forvente at skulle afholde/afse ved løbende drift, herunder en løbende dialog med CFCS om verifikation af data mv.?

- Hvilke omkostninger skal virksomheder forvente at skulle afholde/afse i forbindelse med forebyggende sikkerhedsundersøgelser?

- Vil der være situationer, hvor CFCS vil opkræve betaling fra tilsluttede virksomheder? I hvilke situationer?

Endelig anmodes ministeren om at afklare følgende to spørgsmål med Energi-, Forsynings- og Klimaministeren:

- Vil dokumenterede meromkostninger (for elnetselskaberne) komme ind under de samme regler, som gælder ved tilslutning til proaktive/reaktive IT-sikkerhedstjenester jf. BEK425, §25 og §28?

- Og vil sådanne omkostninger være at anse som omfattet af § 26, stk. 3, om tilmelding til IT-sikkerhedstjeneste i bekendtgørelse nr. 969 af 27. juni 2018 om indtægtsrammer for netvirksomheder?

Sammenhængen til øvrige internationale initiativer

Dansk Energi finder det essentielt, at danske initiativer på cyber- og informationssikkerhedsområdet harmoniseres og spiller sammen med relevante internationale krav og initiativer både på EU-niveau og globalt. Eksempelvis findes der allerede i dag både energispecifikke initiativer i regi af Council of European Energy Regulators (CEER) og Agency for the Cooperation of Energy Regulators (ACER) samt mere tværsektorielle initiativer i regi af EU-kommissionen, ENISA og FN[1].

Dette skal ses i lyset af, at cybertruslen er international, og at flere danske energiselskaber har internationale aktiviteter, såvel som at udenlandske energiselskaber har aktiviteter i Danmark. I det omfang der ikke sker en koordinering og harmonisering, vil ressourceforbrug og omkostninger blot blive væsentlig forøget, uden at truslen bliver mindre af den grund; måske snarere tværtimod.

I dén forbindelse finder vi det også relevant at spørge til virksomheders retsstilling, når og hvis CFCS som national, dansk it-sikkerhedsmyndighed og del af Forsvarets Efterretningstjeneste pålægger danske, samfundsvigtige virksomheder med internationale aktiviteter at være tilsluttet CFCS' netsikkerhedstjeneste og dermed give CFCS adgang til at monitorere data og trafik, som er relateret til aktiviteter i andre EU-lande eller i tredjelande.

I en international sammenhæng skal det bemærkes, at der rent formelt kan være begrænsninger i Danmarks muligheder for national lovgivning, i det omfang EU-retten kan siges at have nået et niveau, at det såkaldte pre-emption i EU-retten tilsiger, at Danmark må afvente den igangsatte EU-lovgivning på området. Dansk Energi skal anbefale, at dette forhold undersøges nærmere. Dette nævnes ikke kun for at undgå den uheldige juridiske situation, der ellers kan opstå. Det skal også understreges, at der ellers kan opstå et betydeligt spild af ressourcer, såfremt en dansk implementeret retsstilling efterfølgende må vige for EU-praksis/lovgivning. Pre-emption-aspekter i relation til EU bør således behandles i lovtekst.

Endelig henledes CFCS' opmærksomhed på, at installation af sikkerhedssoftware på interne systemer er en speciel udfordring, når virksomhederne har kontorer i andre lande, der er fuldt integreret i de administrative IT-/tele-løsninger. De juridiske komplikationer (ansvarspådragelse) relateret til dette bør vurderes og reflekteres i lovforslaget.

Øvrige forhold

- Lovbemærkningerne bør i højere grad afspejles direkte i lovtekst, fx i forhold til kriterier, som lægges til grund for tilslutning (og evt. pålæg herom) og CFCS' ansvar overfor virksomhederne.

[1] Såsom udmøntning af EU's Energy Expert Cyber Security Platform (EECSP) anbefalinger til EU Kommissionen og globalt 'The Paris Call of 12 November 2018 for Trust and Security in Cyberspace' underskrevet af 64 lande (inkl. Danmark), 300 virksomheder og flere end 150 NGO-organisationer.

- Det bør præciseres, hvilken sammenhæng lovforslaget vil have til den IT-sikkerhedstjeneste, som virksomheder i el- og naturgassektorerne er underlagt jf. BEK425.

- I lovforslaget har CFCS en række operationelle rettigheder i forbindelse med et evt. cyberangreb. Det ønskes præciseret, hvordan grænsefladen er mellem den aktuelle virksomheds og CFCS' operationelle ansvar og beføjelser, herunder klarlægning af relationer til den i el- og naturgassektorerne operationelle kontrolstruktur med Energinet samt Energistyrelsens beføjelser.

- Det er en udfordring, at virksomhederne underlægges samtidig regulering fra flere ministerier relateret til cybersikkerhed.

- Malware-begrebet inkluderer trafik-, pakke- og stationære data. Dansk Energi efterspørger en præcisering af, om stationære data også kan være en del af andre filer; fx nøgler i en registreringsdatabase.

- Vil sikkerhedssoftware være konstrueret således, at udvalgte IT-administratorer i organisationen vil kunne slå den fra / ændre i den? Og vil IT-sikkerhedsmedarbejdere i en virksomhed få indsigt i de etablerede honey pots, så de ikke karambolerer med andre sikkerhedstjenester i virksomheden?

- Det bør overvejes, at honey pots og især deception-teknologier også indebærer mere risiko. Afhængigt af hvilken honey pot-metode, der vil blive benyttet, kan sårbare systemer blive en del af en virksomheds netværk, og derudover kan virksomheden risikere, at angriberen bliver provokeret til at gennemføre destruktive handlinger.

Såfremt ovenstående giver anledning til spørgsmål, står Dansk Energi naturligvis til rådighed, ligesom vi gerne deltager i et uddybende møde herom.

Med venlig hilsen
Dansk Energi

Regitze Prahl
Chefkonsulent

DANSK ERHVERV
Børsen
DK-1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. +45 3374 6000

Forsvarsministeriet
fmn@fmn.dk
Cc: tbl@kmn.dk og sbu@fmn.dk

4. februar 2019

Høring over lov om Center for Cybersikkerhed, sagsnr. 2018/006599

Generelle bemærkninger

Dansk Erhverv glæder sig over regeringens fornyede og skærpede fokus på informations- og cybersikkerhed, herunder Erhvervspartnerskab for it-sikkerhed, lanceringen af SikkerDigital.dk, Sikkerhedstjekket, samt strategi for cyber- og informationssikkerhed og de sektorspecifikke strategier, hvor Dansk Erhverv deltog i arbejde med teleinfrastruktur.

Dansk Erhverv anerkender behovet for løbende at vurdere om Center for Cybersikkerhed (CFCS) har de nødvendige redskaber og beføjelser. Det aktuelle lovudkast lægger op til at give Forsvarsministeriet en række ganske udvidede beføjelser, som Dansk Erhverv stiller sig kritisk over for.

Dansk Erhverv mener, at lovforslaget går for langt, idet der ikke i lovforslaget i tilstrækkeligt omfang redegøres for, hvordan de foreslåede tiltag er proportionale i forhold til deres indgriben i virksomhedernes private forhold. Desuden har lovforslaget et for ensidigt tilgang til virkemidler.

Dansk Erhverv kan derfor ikke støtte forslaget i sin nuværende form.

Specifikke bemærkninger

Påbud om tilslutning til CFCSs netsikkerhedstjeneste

Lovforslagets §3 giver CFCS mulighed for at pålægge virksomheder at lade sig tilslutte CFCSs sikkerhedstjeneste, herunder at CFCS vil kunne installere aktivt udstyr og software på virksomhedens infrastruktur, som CFCS kontrollerer, samt pålægge virksomheden at indrette sin eksisterende infrastruktur efter det. En sådan bestemmelse vil kunne ramme danske virksomheder negativt, fx hvad angår eksport, samt internationale samarbejde og teknologiudvikling. Lovforslaget siger ikke, hvilke typer (”samfundsvigtige”) virksomheder som CFCF kan kræve tilslutning til, hvilket Dansk Erhverv anser for nødvendigt at præcisere.

Dansk Erhverv kan ikke støtte, at der gives så vide beføjelser i udvælgelsen af, hvilke former for virksomheder, der kan forlanges tilsluttet den forslåede ordning. Desuden savnes en uddybning af, hvilke former for udstyr og software, der skal anvendes. Det er vigtigt for Dansk Erhverv, at

beslutningen om deltagelse overlades til den enkelte virksomheder, og ligeledes er det er virksomhederne, der beslutter, hvilket udstyr og software der er relevant at anvende.

Ubegrænset adgang til data i virksomheder
Lovforslagets §4 giver CFCS meget vidtgående beføjelser til "uden retskendelse [at] behandle trafikdata, pakkedata og stationære data". "Stationære data" defineres som "Data, som opbevares på servere, cloudtjenester, pc'ere, lagerenheder, netværksenheder, mobile enheder og tilsvarende".

Som Dansk Erhverv læser forslaget, indebærer det i praksis, at CFCS får uindskrænket adgang til alle data i de tilsluttede virksomheder, herunder persondata, forretningshemmeligheder, kundedata, private dokumenter m.v. på alt fra virksomhedens servere til den enkelte ansattes telefon eller laptop.

Der er uklart på hvilke præmisser CFCS kan anvende disse tekniske muligheder. Det skaber usikkerhed hos virksomhederne. Det handler ikke kun om, hvad CFCS kan og må foretage sig på en virksomheds it-infrastruktur. Det handler også om, hvad virksomheden kan fortælle sine kunder og samarbejdspartnere, herunder også hvordan CFCS samarbejder med tilsvarende tjenester i andre lande.

Dansk Erhverv mener ikke, at det er proportionelt, at CFCS får en sådan i praksis ubegrænset adgang til alle virksomhedens data. Dansk Erhverv kan derfor ikke støtte denne nye hjemmel.

Offentlige private samarbejder
Dansk Erhverv mener ikke, at man kan slutte, at fordi få virksomheder i dag er tilsluttet CFCS netsikkerhedstjeneste, så er der få virksomheder der foretager monitorering af nettrafik, som er præmissen i lovforslagets bemærkninger (bemærkninger til lovforslaget, side 11-).

Det er ikke korrekt, når lovforslaget slutter, at der i dag ikke foregår monitorering af nettrafik for avancerede angreb. Flere virksomhederne investerer allerede i systemer, der eksempelvis kan detektere mistænkelige mønstre i nettrafik, som kan være tegn på sikkerhedshændelser.

Dansk Erhverv finder, at det er en for unuanceret tilgang, når lovforslaget fokuserer alene på CFCS egne systemer.

Dansk Erhverv opfordrer til at undersøge andre muligheder, fx tættere samspil mellem CFCS og den enkelte virksomhed om allerede etablerede systemer. Det er i det hele taget oplagt at satse på et samarbejde, rammer og evt. krav for de systemer virksomhederne benytter, frem for alene at fokusere på at installere CFCSs egne teknologier som CFCS kontrollerer.

Persondataforordningen og lov om Center for Cybersikkerhed
De virksomheder der omfattes at den forslåede ordning skal overfor de personer, de behandler personoplysninger om være i stand til at oplyse, at de indgår i CFCS overvågning. Oplysninger om personer registret hos de omfattede virksomheder vil efter Dansk Erhvervs vurdering skulle informeres i henhold til GDPR. Derfor opfordrer Dansk Erhverv Forsvarsministeriet til at bistå til

dette ved at udarbejde en standard informationstekst med ministeriet som afsender, som virksomheder kan anvende og lade indgå i deres eksisterende persondatapolitikker

Persondataforordningen stilles skærpede krav om sikkerhed i forhold til behandling af personoplysninger, hvilket betyder at mange virksomheder over de seneste år har investeret betydeligt i at opdaterer deres it-sikkerhed. Det er således helt oplagt at tænke i løsninger, der spiller sammen med allerede implementerede sikkerhedsforanstaltninger.

Andre bemærkninger
Processen med persondataforordningen har medført en ny og anderledes samtale om persondata i samfundet. Fra direktionslokalet til kakkelbordet, og det er grundlæggende sundt. Det aktuelle lovforslag står i kontrast til dette, og ville efterlade tilsluttede virksomheder med et forklaringsproblem over for ansatte, kunder og samarbejdspartnere. Det kan i sidste ende få negative konsekvenser for den enkelte virksomheder, og for Danmark som land for investeringer og teknologiudvikling.

Dansk Erhverv mener den offentlige sektor - som landets ubetinget største dataansvarlige og den dataansvarlige, der behandler flest personfølsomme og fortrolige personoplysninger - bør gå forrest og vise vejen for korrekt og etisk behandling af personoplysninger. Det gælder ikke mindst Center for Cybersikkerhed.

It-kriminalitet er et globalt fænomen, som vi så det med angrebene, der forrige år hærgede lande over hele verden, og som lagde tusindvis af it-systemer ned. Ingen enkeltaktør kan håndtere denne udfordring alene - hverken nogen enkelt virksomhed eller nogen stat. Udfordringen kræver derfor et samarbejde mellem offentlige og private spillere, og det kræver et internationalt samarbejde som i sidste ende globalt. Det var i det lys, at Dansk Erhverv bakkede op om en ”digital genevekonvention” (sommeren 2017), som oprindeligt foreslået af Brad Smith, president and chief legal officer, Microsoft.

Der er behov for en vifte at indsatser, og det er afgørende at der sker som ligebyrdigt samspil mellem offentlige og private spillere, og i et samarbejde hvor viden går begge veje. Der er andre måder at dele viden med CFCS end at give CFCS beføjelser til påbud og vidtrækkende dataadgang med CFCS som den kontrollerende part. Dansk Erhverv mener, at Rådet for Digital Sikkerhed kan spille en vigtig rolle som brobygger her, lige som Dansk Erhverv selvfølgelig selv står til rådighed med vores dialog med erhvervslivet.

Med venlig hilsen

Janus Sandsgaard
Fagchef for it og digitalisering

4. februar 2019
MORV

Forsvarsministeriet
Holmens Kanal 9
1060 København K
Vedr. sagsnummer 2018/006599.

Dansk Industri
Confederation of Danish Industry

Høringssvar fra DI til udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden)

DI takker for muligheden for at afgive høringssvar samt for den hidtidige dialog om lovforslaget i regi af forskellige myndighedsfora samt briefingen for høringsparterne om lovforslaget i Forsvarsministeriet.

Forslag til lov om ændring af lov om Center for Cybersikkerhed har til formål at tilvejebringe de retlige rammer for en styrkelse af Center for Cybersikkerheds muligheder for at opdage og stoppe cyberangreb samt styrke centerets analytiske arbejde. Centerets grundlæggende hjemmel til at udføre sine opgaver er således ikke berørt i lovforslaget.

Særligt i lyset af, at Danmark er et af verdens mest digitaliserede lande, og at Danmark derfor også er særligt sårbart overfor konsekvenserne af succesfulde cyberangreb, støtter DI til fulde regeringens ønsker om at styrke sikkerhedsniveauet i den danske digitale infrastruktur og om at beskytte Danmark mod cyberangreb. DI værdsætter også samarbejdet med myndighederne om sektorstrategier for en styrket cybersikkerhed i samfundskritiske sektorer, hvor særligt virksomhederne i telesektoren er blevet inddraget.

Vigtig balance mellem muligheder og begrænsninger

Det er fortsat forholdsvist nyt, at kriminalitet, chikane, svindel, spionage og sabotage foretages i den digitale verden, og vi er som samfund og i internationale sammenhænge fortsat i en proces, hvor midlerne til at dæmme op for angrebene og til at sikre, at der er konsekvenser, når man vælger at angribe i den digitale verden fremfor den fysiske, ikke er tilstrækkelige .

DI ser det som helt afgørende, at der i denne proces opretholdes den nødvendige balance mellem muligheder og begrænsninger, og at lovforslagets nye initiativer om styrkelse af Center for Cybersikkerheds kompetencer ikke sker på bekostning af retssikkerheden eller forudsigeligheden i myndighedsudøvelsen.

H. C. Andersens Boulevard 18
1787 København V
Danmark

(+45) 3377 3377
di@di.dk
di.dk

CVR: 16 07 75 93

Det er med andre ord vigtigt ikke at tabe retssikkerheden af syne, blot fordi kamppladsen er flyttet fra den fysiske til den digitale verden.

Tre hovedbudskaber fra DI
Der er særligt tre elementer i lovforslaget, der er vigtige for DI at kommentere på.

Det drejer sig om den nye mulighed for at påbyde virksomheder at tilsluttes netsikkerhedstjenesten, udvidelsen af Center for Cybersikkerheds ydelser, der er i direkte konkurrence med det private marked for it-sikkerhed samt sammenhængen med den internationale udvikling.

De tre elementer uddybes i det følgende, men hovedbudskaberne fra DI er:

- DI støtter som udgangspunkt alene en frivillig tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste. Lovforslaget introducerer i § 3, stk. 4 dog muligheden for, at Center for Cybersikkerhed gennem påbud kan tvinge myndigheder og virksomheder af særlig samfundsvigtig karakter til i særlige tilfælde at blive tilsluttet netsikkerhedstjenesten. Grundlæggende ser DI den foreslåede mulighed for at udstede påbud om tilslutning til netsikkerhedstjenesten som problematisk både for retssikkerhed og konkurrenceevne for virksomheder i Danmark samt for Danmarks evne til at tiltrække og fastholde internationale virksomheder.

- Foruden den eksisterende monitorering via netsikkerhedstjenesten vil Center for Cybersikkerhed med lovforslaget få udvidet sine ydelser væsentligt – også til områder der ikke er isoleret til centerets øvrige fokus på de allermest avancerede sikkerhedshændelser. Tilsluttede virksomheder vil få tilbudt nye ydelser i form af et aktivt cyberforsvar og af forebyggende it-sikkerhedsydelser. DI stiller sig uforstående overfor, at der skal anvendes offentlige ressourcer på gratis at tilbyde disse nye forebyggende it-sikkerhedstekniske undersøgelser og ydelser i forbindelse med aktivt cyberforsvar, som i forvejen tilbydes på det private marked. Det er DI's opfattelse, at disse nye gratis ydelser er i konkurrence med det private marked, og dermed er konkurrenceforvridende. DI stiller sig gerne til rådighed for at komme mere balancerede løsninger nærmere, der både tilgodeser høj informationssikkerhed i samfundskritiske funktioner, it-sikkerhedsleverandører og beskyttelse af Center for Cybersikkerheds efterretningsmæssige kilder.

- DI understreger vigtigheden af, at nationale initiativer som dette lovforslag (og tilhørende initiativer, som udmøntes i forlængelse heraf) harmoniseres og spiller sammen med internationale initiativer i regi af EU og i globale sammenhænge. Dette bør afdækkes nærmere, og i lovforslaget understreges som en ledende faktor. Selv mindre divergenser i forhold til internationale regler vil være byrdefulde for mange virksomheder.

Generelle bemærkninger til lovforslaget
Som en generel kommentar til lovforslaget bemærker DI, at der mangler en præcis definition af flere af lovforslagets grundlæggende begreber som "samfundsvigtig", "særlig samfundsvigtig karakter", "opdage, analysere eller som kan bidrage til at imødegå sikkerhedshændelser" og "understøtte et højt informationssikkerheds-niveau"/"

understøtte et højt informationssikkerhedsniveau i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af".

Den manglende definition og afgrænsning af disse grundlæggende begreber gør lovforslaget unødigt upræcist og dets konsekvenser svært at konkretisere i en praktisk virkelighed for virksomhederne. Det betyder også, at de kompetencer, som lovforslaget giver Center for Cybersikkerhed, ligeledes mangler afgrænsninger. Dette skaber grundlag for bekymring på tværs af DI's medlemskreds.

Lovforslaget indeholder omfattende lovbemærkninger, hvilket DI opfatter positivt. For at skabe størst mulig transparens og retssikkerhed, efterspørger DI dog, at lovforslagets lovbemærkninger i højere grad bliver afspejlet direkte i lovteksten.

Lovforslaget giver adgang til data relateret til sikkerhedshændelser. I praksis vil disse data ofte være 'blandet sammen' med andre typer af data, som ikke er indenfor lovens formål. Både af økonomiske som tekniske grunde kan det være uforholdsmæssigt svært eller teknisk begrænset at udskille og afgrænse data, som lovforslagets giver adgang til.

Derved vil Center for Cybersikkerhed have adgang til eller modtage data, som rækker udover lovens lex specialis-karakter. Dette betyder igen, at det ikke er muligt for disse principielt utilsigtede data at opnå en undtagelse i forhold til andre love. Det vil i denne sammenhæng særligt sige i forhold til GDPR. DI efterlyser derfor, at relationen til GDPR som minimum bør uddybes.

I en international sammenhæng skal det bemærkes, at der rent formelt kan være begrænsninger i Danmarks muligheder for national lovgivning, såfremt EU-retten på området kan siges at have nået et niveau, der aktiverer det såkaldte pre-emption-princip i EU-retten. I en sådan situation må Danmark afvente den igangsatte EU-lovgivning på området. Foruden den uheldige juridiske situation, der kan opstå, skal det også understreges, at der kan opstå et betydeligt spild af ressourcer i både myndigheder og virksomheder, såfremt en dansk implementeret retsstilling efterfølgende må vige for EU-praksis/lovgivning. DI efterspørger derfor, at pre-emptionaspekter i relation til EU bør behandles i lovteksten og undersøges nærmere.

Udover en potentiel risiko for, at lovforslagets elementer kan være i konflikt med EU-rettens pre-emptionsprincip, er der også andre grunde til, at DI opfordrer til, forslagets elementer samt ikke mindst de processer og standarder, der udmøntes på bekendtgørelsesniveau afklares i forhold cybertruslens internationale karakter.

Udover at truslen fra internationale aktører er åbenbar, som det også anerkendes i lovforslaget, har mange danske virksomheder udbredte internationale aktiviteter, ligesom udenlandske selskaber opererer i Danmark. Det er derfor essentielt, at danske initiativer på cyber- og informationssikkerhedsområdet harmoniseres og spiller sammen med relevante internationale krav og initiativer både på EU-niveau og globalt. Eksempelvis findes der allerede i dag både sektorspecifikke initiativer (f.eks. på energiområdet) samt mere tværsektorielle initiativer i regi af EU-kommissionen, ENISA og FN.

Nye muligheder for at dele viden om eksempelvis malware
Videndeling er et grundlæggende element, hvis et cyberforsvar skal kunne stå mål med udviklingen i metoder og teknik, der ligger bag de løbende cyberangreb, og hvis cyberangreb skal opdages hurtigt. Derfor bifalder DI, at der i § 16 gives hjemmel til at videregive data om blandt andet malware til relevante modtagere.

Samtidig fjernes den uhensigtsmæssighed i den eksisterende lov, der fratog Center for Cybersikkerhed muligheden for at videregive pakkedata til den myndighed eller virksomhed, som data kommer fra i første omgang for at fastslå, hvorvidt data er ondartet eller ej. Det hilser DI velkommen.

Man kunne dog godt have ønsket sig en mere pædagogisk fremstilling af de mange muligheder for videregivelse af data, som der fremgår af de 38 linjers beskrivelse af de forskellige muligheder i § 16. Eventuelt i form af et skema.

DI bemærker derudover, at det bør præciseres, i hvilket omfang og i hvilke situationer, at Center for Cybersikkerhed må udlevere information og data til andre myndigheder. Dette er særligt vigtigt, idet lovens forældelsesregler ikke videreføres for udleveret information, der i stedet 'blot' skal følge modtagne myndigheds forældelsesregler. Det er endvidere vigtigt, idet der som nævnt indledningsvist kan være data, som er 'blandet sammen' af tekniske/økonomiske grunde, og som derfor er underlagt eksempelvis GDPR-reglerne m.h.t. sletning m.v.

Ny adgang til stationære data
Center for Cybersikkerheds adgang til data hos tilsluttede myndigheder og virksomheder udvides med lovforslaget fra alene at omhandle netværkstrafik i form af trafik- og pakkedata til nu også at omfatte stationære data. Stationære data er f. eks. data, som opbevares på servere, cloudtjenester, pc'ere, lagerenheder, netværksenheder, mobile enheder og tilsvarende.

Det vil sige, at det er svært at forestille sig data, som ikke er indeholdt i enten trafikdata, pakkedata eller stationære data, og at man ved tilslutning til Center for Cybersikkerheds netværkstjeneste dermed giver ubegrænset adgang til alle myndighedens eller virksomhedens data, så længe at adgangen kan siges at understøtte et højt informationssikkerhedsniveau i den danske digitale infrastruktur, hvilket som tidligere nævnt mangler en mere præcis definition og afgræsning.

Denne udvidelse af området, hvor der ikke længere kræves retskendelse, fra særlige begrundede data til nu reelt alle data, virker retssikkerhedsmæssigt bekymrende. DI er af den opfattelse, at adgangen til myndigheder og virksomheders data bør målrettes bedre i lovforslaget, så der er en reel begrænsning i centerets adgang til virksomhedsdata og personlige informationer til alene data, der mere præcist understøtter formålet med Center for Cybersikkerheds virke. Som hjemlen for nuværende er formuleret, er der ikke proportionalitet til stede mellem centerets adgang til alle data uden retskendelse og beskyttelse af personlige informationer og kritiske forretningsoplysninger.

Hvis en tilsvarende hjemmel var blevet indført af en myndighed i et andet land, ville dette have vakt bekymring for de danske virksomheder, der opererede i det pågældende land.

Det er samtidig uklart, hvorledes Center for Cybersikkerhed i praksis vil tilgå stationære data. Det gælder f.eks. i forhold til at tilgå data i cloudtjenester – særligt i situationer, hvor tjenesten er placeret udenfor Danmarks grænser.

Svækkelse af Tilsynet med Efterretningstjenesterne
DI finder det endvidere særligt bekymrende, at der i lovforslaget indføres en mulighed for, at centeret kan vælge ikke at følge en henstilling i en udtalelse fra Tilsynet med efterretningstjenesterne og lade det være op til forsvarsministeren – centerets egen øverste chef – at afgøre sagen. Dette svækker tilsynets mandat og kontrol med Center for Cybersikkerhed og i sidste ende retssikkerheden.[1]

Påbud om tilslutning til netsikkerhedstjenesten
DI støtter alene en frivillig tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste. Lovforslaget introducerer i § 3, stk. 4 dog muligheden for, at Center for Cybersikkerhed gennem påbud kan tvinge myndigheder og virksomheder af særlig samfundsvigtig karakter til i særlige tilfælde at blive tilsluttet netsikkerhedstjenesten. Lovteksten kommer ikke en afgræsning nærmere af, hvilke virksomheder det kunne være eller i hvilke situationer, at påbuddet vil blive anvendt. Lovbemærkningerne giver en række brede og ikke-udtømmende karakteristika. Samlet set er det uklart, hvor bredt virksomheder af særlig samfundsvigtig karakter kan forstås, og principielt er der heller ikke en lovmæssig begrænsning på frekvensen af anvendelsen af påbuddet, og hvad der skal forstås ved "særlige tilfælde".

Denne ikke-transparente risiko for tvangstilslutning til netsikkerhedstjenesten kombineret med den beskrevne udvidede adgang til pakkedata, trafikdata og stationære data uden retskendelse er en tilsidesættelse af Grundlovens § 72, der værner om privatlivets fred og sætter grænserne for, hvilke indgreb offentlige myndigheder kan tillade sig i folks privatliv uden retskendelse, der som udgangspunkt kun er mulig gennem en særegen lovhjemmel.

Videreføres muligheden for at tvinge virksomheder til at tilslutte sig netsikkerhedstjenesten i det endelige lovforslag, er der et stærkt behov for forudsigelighed i de situationer, som kan føre til, at en virksomhed tvinges til at være tilsluttet netsikkerhedstjenesten, som der ikke skabes med det nuværende lovforslag. Det gælder både for forudsigelighed for virksomhederne selv, men i høj grad også for danske virksomheders internationale samarbejdspartnere, hvis data ikke er undtaget Center for Cybersikkerheds adgang, eller hvor Center for Cybersikkerhed får adgang til data relateret til aktiviteter i andre EU-lande eller i tredjelande.

Muligheden for tvangstilslutning sammen med en manglende forudsigelig i den henseende kan have anseelige konsekvenser for særligt virksomheder med internationale

[1] Der kan findes inspiration til begrænsninger i masseovervågning hos andre lande, der opretholder demokratiske hensyn i f.eks. publikationen "*Upping the Ante on Bulk Surveillance - An International Compendium of Good Legal Safeguards and Oversight Innovations*" af Thorsten Wetzling and Kilian Vieth fra november 2018.

aktiviteter. Virksomhedernes bekymringer eller manglende mulighed for at forudsige, hvorvidt de eller deres samarbejdspartnere risikerer at få et påbud om tilslutning til netsikkerhedstjenesten kan føre til overvejelser om at flytte aktiviteterne væk fra Danmark eller fravælge Danmark til placering af datacentre etc.

Grundlæggende ser DI derfor den foreslåede mulighed for at udstede påbud om tilslutning til netsikkerhedstjenesten som problematisk både for danske virksomheders retssikkerhed og konkurrenceevne samt for Danmarks evne til at tiltrække og fastholde internationale virksomheder.

Omkostninger og økonomiske konsekvenser for virksomheder
Det fremgår af lovforslagets bemærkninger, at Center for Cybersikkerheds opgave først og fremmest er at understøtte et højt sikkerhedsniveau i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af. Center for Cybersikkerhed har derfor ikke varetagelse af den enkelte virksomheds informationssikkerhed som sin opgave. Virksomheders tilslutning til netsikkerhedstjenesten handler om at tilgodese et samfundsmæssigt ønske og interesse i, at samfundskritiske funktioner opretholdes uanset den voksende cybertrussel.

Der er derfor kun rimeligt, at omkostningerne til at understøtte denne samfundsinteresse er offentligt finansieret og ikke finansieres af de virksomheder, der enten pålægges eller mere eller mindre frivilligt indgår i arbejdet med at opretholde et højt beskyttelsesniveau af samfundskritiske funktioner ved tilslutning til netsikkerhedstjenesten. En offentlig finansiering af omkostningerne ved at være tilsluttet netsikkerhedstjenesten via finansloven eller forsvarsforliget vil således afspejle, at hele samfundet har en interesse i, at de pågældende funktioner ikke helt eller delvist rammes af nedbrud eller hackes. Samtidig argumenteres der i lovforslagets bemærkninger for, at Center for Cybersikkerheds ydelser ikke kan stå alene, men bygger ovenpå generelle it-sikkerhedsmæssige foranstaltninger i virksomhederne.

Disse forhold ligger til grund for, at det fremgår af lovforslaget, at virksomheder fremover ikke opkræves gebyr for tilslutning til netsikkerhedstjenesten.

Lovforslaget efterlader dog en række økonomiske uklarheder i relation til virksomhedernes omkostninger som følge af lovforslaget.

Som situationen er aktuelt, skal virksomheder, der tilsluttes Center for Cybersikkerheds netsikkerhedstjeneste, betale et årligt gebyr, som dækker centerets udgifter til tilslutning og drift af den anvendte alarmenhed. Af lovforslagets bemærkninger fremgår det, at gebyret har udgjort mellem 300.000 kr. og 400.000 kr. pr. probe afhængig af den valgte alarmenhed. I lovforslaget er det imidlertid alene tilslutningen, som nu tilbydes uden betaling.

Det er derfor uklart, hvorledes omkostningerne til driften håndteres, herunder om driften skal finansieres af virksomhederne, ligesom størrelsen af sådanne omkostninger bør konkretiseres. Dette efterlader en række uafklarede spørgsmål, særligt henset til, at der af bemærkningerne fremgår, at virksomhederne alene forudsættes at få begrænsede udgifter som led i et samarbejde med Center for Cybersikkerhed.

Idet der er tale om samfundsvigtige funktioner, er det er DI's holdning, at samtlige af virksomhedernes omkostninger til samarbejdet med Center for Cybersikkerhed – og ikke alene selve tilslutningen til netsikkerhedstjenesten - bør afholdes for offentlige midler henset til ovenstående argumentation for, at tilslutningen er i samfundets overordnede interesse fremfor den enkelte virksomheds interesse.

Imødekommes dette ikke i det endelige lovforslag, er der et behov for at afklare mere præcist, hvilke ressourcer/omkostninger der kan blive relevante for virksomhederne i forbindelse med løbende drift samt i forbindelse med forebyggende sikkerhedsundersøgelser. DI ønsker i forlængelse heraf ligeledes at få afklaret, om der i relation til andre gældende regler indenfor opretholdelse af et højt informationssikkerhedsniveau i de samfundskritiske sektorer er mulighed for kompensation af dokumenterede meromkostninger som følge af samarbejdet med Center for Cybersikkerhed – f. eks. i medfør af §25 og §28 i bekendtgørelse nr. 425 af 1. maj 2018 og af § 26, stk. 3, i bekendtgørelse nr. 969 af 27. juni 2018.

Forhindringer for udbredt frivillig tilslutning
I forlængelse af de nævnte uklarheder i lovforslaget – særligt i forhold til definitioner på grundlæggende begreber i lovforslaget og til de økonomiske konsekvenser for virksomhederne fremstår der yderligere uklarheder i forhold til samarbejde mellem den enkelte virksomhed og netsikkerhedstjenesten, i forhold til relationen mellem lovforslaget og eksisterende IT-sikkerhedstjenester, som virksomheder i de samfundskritiske sektorer allerede og i stigende omfang er omfattet af, og endelig i forhold til Center for Cybersikkerheds ansvar og erstatningsansvar. DI efterspørger afklaring og præcisering heraf i lovforslaget.

Der er eksempelvis tale om følgende udeståender:

- Virksomheder, der varetager samfundskritiske sektorer kan være underlagt regulering fra flere ministerier. Der mangler en præcisering af en helt klar ansvarsfordeling mellem Center for Cybersikkerhed, virksomhederne og eventuelle tilsynsmyndigheder – særligt i et operationelt henseende i tilfælde af et konkret cyberangreb .

- Anvendelse af honeypots og tilknyttede teknikker kan også indebære en risiko for virksomheden – f.eks. i form af sårbare systemer indenfor virksomhedens perimeter eller provokation af angriberen. Der ønskes en præcisering af et eventuelt erstatningsansvar, der påhviler Center for Cybersikkerhed som følge af en virksomheds eventuelle forretningsmæssige tab i forlængelse af Center for Cybersikkerheds anvendelse af honeypots og deceptionteknologier.

- Samtidig risikerer virksomheden, at Center for Cybersikkerheds aktiviteter kan have konsekvenser for virksomhedens drift. Forsinkelse i datastrømme eller datapakker kan f. eks forstyrre driften i samfundskritiske sektorer og i værste fald lede til eksempelvis strømafbrydelser og skade på elanlæg. Der eksisterer også en risiko for produktionstab, klagesager (herunder GDPR-sager) eller andre forretningsmæssige tab. Ligesom anvendelse af honeypots og tilknyttede teknikker også kan indebære en

risiko for virksomheden – f.eks. i form af sårbare systemer indenfor virksomhedens perimeter eller provokation af angriberen. Der mangler en præcisering af i hvilket omfang Center for Cybersikkerhed yder support i sådanne situationer, samt af hvilket erstatningsansvar, der påhviler Center for Cybersikkerhed.

- Hvordan vil Center for Cybersikkerhed helt konkret samarbejde og dele viden om f.eks. aktiv monitering, blokering eller manipulering af datastrømme, alarmer fra honey-pots med den konkrete virksomhed. Det gælder både i forhold til resultater af handlingerne, men også løbende videndeling, så den konkrete virksomhed i videst muligt omfang er inddraget i centerets aktiviteter hos virksomheden.

Samlet set gør en lang række uklarheder i lovforslaget det svært at gennemskue de praktiske konsekvenser af lovforslaget. DI vurderer, at dette samtidig vil gøre det mindre attraktiv for virksomhederne at tilslutte sig netsikkerhedstjenesten frivilligt.

Lovforslagets uklarheder vil naturligvis være yderligere problematiske, såfremt at virksomheder vil kunne tvinges til at tilslutte sig netsikkerhedstjenesten.

Konkurrenceforvridende nye initiativer
Foruden den eksisterende monitorering via netsikkerhedstjenesten vil Center for Cybersikkerhed med lovforslaget få udvidet sine ydelser væsentligt. Tilsluttede virksomheder vil få tilbudt nye ydelser i form af et aktivt cyberforsvar og af forebyggende it-sikkerhedsydelser. Samtlige af Center for Cybersikkerhedsydelser tilbydes på det private marked.

Der er i lovforslaget taget stilling til konkurrencen mellem Center for Cybersikkerheds ydelser og de ydelser, som tilbydes på det private marked. Lovforslagets argumentation er, at ydelserne i lovforslaget ikke vil påvirke det private marked for it-sikkerhedsydelser negativt, da den sikkerhedsløsning, som centeret stiller til rådighed med netsikkerhedstjenesten, er efterretningsbaseret, og at kommercielle udbydere på markedet ikke kan tilbyde en tilsvarende løsning.

Argumentationen er allerhøjest valid i forhold til monitorering via centerets netsikkerhedstjeneste, som kan have indikatorer fremkommet gennem efterretningsindhentning og/eller efterretningssamarbejde, der kan være – men ikke nødvendigvis er det – ukendte for det private marked.

Monitorering af internettrafik for avancerede trusler, aktivt cyberforsvar som eksempelvis blokering af phishingmail og forebyggende it-sikkerhedstekniske undersøgelser - som eksempelvis simulerede hackerangreb - tilbydes i vidt omfang på det private marked, som der i større grad bør samarbejdes med om aktivt cyberforsvar og forebyggende it-sikkerhedstekniske undersøgelser fremfor at udvide Center for Cybersikkerheds ydelser.

DI stiller sig uforstående overfor, at der skal anvendes offentlige ressourcer på gratis at tilbyde nye forebyggende it-sikkerhedstekniske undersøgelser og ydelser i forbindelse med aktivt cyberforsvar, som i forvejen tilbydes på det private marked.

Det er DI's opfattelse, at disse nye gratis ydelser er i konkurrence med det private marked, og dermed er konkurrenceforvridende.

DI vil i stedet opfordre regeringen til at styrke samarbejdet med det private marked for it-sikkerhedsydelser. Selv hvis regeringen fastholder, at Center for Cybersikkerheds netsikkerhedstjeneste og dens monitorering efter avancerede trusler baseret på efterretningsmateriale skal bestå, kan myndigheder og virksomheder få ydelser indenfor aktivt cyberforsvar og forebyggende it-sikkerhedstekniske undersøgelser leveret af det private marked i samarbejde med Center for Cybersikkerhed uden dermed at miste den efterretningsmæssige viden.

Det er samtidig rimeligt at stille spørgsmålstegn ved, hvorvidt at Center for Cybersikkerhed er i stand til at levere disse nye ydelser på samme eller et højere niveau, end det private marked kan tilbyde. Den hidtidige ydelse har ikke været en succes ad frivillighedens vej. Kun to virksomheder er aktuelt tilsluttet. Det kan både være kvaliteten af ydelsen i forhold til prisen, men også bekymring over Center for Cybersikkerheds adgang til virksomhedens data.

Generelt vil DI opfordre regeringen til at gentænke samarbejdet med det private marked for it-sikkerhedsydelser. Både regeringen og DI har som målsætning, at dansk it-sikkerhed skal styrkes, og at it-sikkerhed skal være et konkurrenceparameter for virksomheder i Danmark. DI opfordrer i forlængelse heraf regeringen til at finde løsninger på, hvordan Center for Cybersikkerheds særlige efterretningsmæssige kompetencer/viden i større grad skal sættes i spil hos it-sikkerhedsleverandører i Danmark, fremfor at Center for Cybersikkerhed bevæger sig ind på det private markeds område. DI stiller sig gerne til rådighed for at komme sådanne løsninger nærmere og finde en balance, der både tilgodeser høj informationssikkerhed i samfundskritiske funktioner, it-sikkerhedsleverandører og beskyttelse af Center for Cybersikkerheds efterretningsmæssige kilder. Man kan også forestille sig, at Center for Cybersikkerhed på nogle områder kan stille minimumskrav til myndigheder og virksomheders it-sikkerhed, som private leverandører kan bidrage til at opfylde, i stedet for at myndighederne og virksomhederne tilsluttes netsikkerhedstjenesten.

DI er endelig også bekymret over, at Centeret for Cybersikkerheds nye ydelser, der tilmed nu er gratis, vil få myndigheder og virksomheder, som vil modtage ydelserne, til at nedprioritere øvrige it-sikkerhedsmæssige foranstaltninger. Dette uanset, at det fremgår af lovforslagets bemærkninger, at centerets ydelser ikke vil kunne træde i stedet for kommercielle produkter, men vil alene kunne udgøre et ekstra lag af sikkerhed.

Der er brug for en langt tydeligere afgrænsning af Center for Cybersikkerheds ydelser som kun et ekstra lag af sikkerhed, der alene baserer sig på efterretningsmæssige kilder og ikke tilbyder nogen former for it-sikkerhed, der kan tilbydes uden efterretningsmæssig viden. Behovet eksisterer både for at afstemme forventningerne til samarbejdet med Center for Cybersikkerhed og for at afgrænse udviklingen af centerets ydelser til ikke at være i konkurrence med det private marked.

Med venlig hilsen

Morten Rosted Vang
Chefkonsulent
DI Digital

Forsvarsministeriet
Holmens Kanal 9
1060 København K
Til fmn@fmn.dk, tbl@fmn.dk og sbu@fmn.dk
Sagsnr.: 2018/006599

Den 1. februar 2019

Høringssvar om forslag til Lov om ændring af lov om Center for Cybersikkerhed

DANSK IT er enig i hensigten med loven; at øge robustheden i Danmark og den generelle beskyttelse. Der er en alvorlig cybertrussel mod Danmark og danske interesser. Det er også nødvendige tilpasninger af gældende lov om Center for Cybersikkerhed på baggrund af de opnåede erfaringer. Det giver f.eks. god mening, at Center for Cybersikkerhed kan monitorere andet end netværkstrafik, da netværkstrafik i stigende grad krypteres, og dermed vil netværkstrafikken skulle dekrypteres for, at man kan se, om der er et match på en angrebssignatur. Det er en naturlig teknologisk udvikling også at kunne opdage angreb på hosts.

Det er også forståeligt, at der skal være mulighed for at blokere, fjerne eller omdirigere skadelig trafik – modsat i dag, hvor skadelig trafik blot detekteres og derefter videresendes til offeret. Endelig er det hensigtsmæssigt, at CFCS har vurderet, at sikkerhedstekniske test (f.eks. såkaldte penetrationstests), som udføres af en offentlig myndighed, vil fordre særskilt hjemmel til at behandle persondata, da disse som led i sikkerhedstesten vil kunne blive behandlet af myndigheden.

Der er dog også i lovforslaget fremsat bekymrende og vidtrækkende ønsker til centerets fremtidige muligheder.

Overordnet er det DANSK IT's holdning, at:

- Indgreb i grundlæggende rettigheder og frihedsrettigheder i loven skal begrænses til det strengt nødvendige.
- Folketinget bør ikke vedtage en lov med så brede og generelle formuleringer, at en myndighed får ret til at gribe ind i grundlæggende rettigheder uden forudgående effektiv kontrol.
- Loven skal opstille de præcise krav til et påbud, herunder udstrækning af påbuddet og hvem påbuddet præcis retter sig til.
- Loven skal – som minimum – give mulighed for efterfølgende domstolsprøvelse af de tvangsindgreb, der foretages, så det er muligt efterfølgende at få en effektiv vurdering af, om betingelserne for indgrebet er/var opfyldt.

Ønsket om at CFCS kan påbyde virksomheder at blive tilsluttet netsikkerhedstjenesten, er i den foreslåede ordning mere vidtgående og vidtrækkende end nødvendigt.

For det første vil et påbud alene være omfattet af almindelig rekursadgang. Det er der altså ministerområdet selv, som vurderer og beslutter, om en virksomhed eller myndighed skal tvangstilsluttes netsikkerhedstjenesten og dermed give indsigt i al kommunikation i virksomheden eller myndigheden. Ved et så vidtgående indgreb bør CFCS' vurdering af behov og nødvendighed suppleres med en vurdering eller som minimum rapportering til en uafhængig part.

CFCS vurderer selv, at domstolsprøvning ikke er egnet til honeypots mv., da CFCS alene vil kunne henvise til en generel trussel. Men i tilfælde af tvangstilslutning til netsikkerhedstjenesten bør CFCS kunne henvise til

en konkret trussel og konkret information, som muliggør domstolsprøvelse fremfor et administrativt påbud. Alternativt - og som absolut minimum – bør CFCS pålægges at udarbejde en rapport om tvangsindgrebet, som forlægges Tilsynet med Efterretningstjenester til godkendelse.

For det andet er der ingen bagkant på tvangsindgrebet. Når CFCS har udsendt et påbud, gælder det i princippet på ubestemt tid. Der er intet krav i loven om, at påbuddet skal genovervejes efter en periode på f.eks. 30 dage. Som loven er formuleret, vil en virksomhed eller myndighed kunne være tvangstilsluttet i årevis uden genovervejelse fra CFCS' side.

For det tredje bør loven forholde sig til, hvorledes en virksomhed skal opfylde et påbud uden at bryde f.eks. aftalte hemmeligholdelsesforpligtelser eller udlevering til oplysning om konfiguration og drift, som virksomheden ikke råder over, da disse i vist omfang tilhører en leverandør.

Når CFCS vil anvende host-agenter, bør det det i loven eller som minimum i en bekendtgørelse tydeliggøres, hvordan f.eks. anvendelse af privatejede enheder håndteres, hvem der installerer, og hvem der afinstallerer sikkerhedssoftware, samt hvilke test CFCS skal foretage, inden sikkerhedssoftware udrulles for på den måde at sikre, at det ikke påvirker virksomhedens drift negativt.

Lovforslaget har i sagens natur fokus på CFCS' ønsker og behov. Det gentages flere steder i lovforslaget, at centeret har en åben og udadvendt profil, men der er ingen steder nævnt en forpligtelse for centeret til at øge informationsdelingen til private sikkerhedsfirmaer, DCIS'er eller lignende som følge af den yderligere information, centeret får adgang til.

Det fremgår flere steder i lovforslaget, at de nye tiltag ikke påvirker det private marked for sikkerhedsydelser negativt med henvisning til, at CFCS' løsninger baserer sig på efterretningsbaseret viden. Det fremgår f.eks. i forbindelse med gebyrfritagelsen ved tilslutning til centeret.

Her må nødvendigvis følge, at netsikkerhedstjenesten alene har fokus på angreb fra andre stater, og at man alene udnytter de tekniske kapaciteter til at opdage og imødegå (med aktivt cyberforsvar) angreb fra andre stater. Hvis de tekniske kapaciteter også forventes anvendt til at stoppe cyberkriminelle og forhindre f.eks. ransomware, må det alt andet lige forventes at påvirke det private marked for it-sikkerhedsydelser negativt.

Det virker utænkeligt, at CFCS (som har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser, herunder avancerede cyberangreb) ved udnyttelse af muligheden for aktivt cyberforsvar bevidst vil undlade - eller afskrive sig muligheden for - at blokere for kendte trusler i form af f.eks. ransomware, hvis én af centerets kunder formodes at være ramt. På den baggrund er det næppe en retvisende fremstilling, når der i bemærkningerne til lovforslaget står, at det ikke negativt påvirker det private marked for sikkerhedsydelser.

Yderligere bemærkninger

DANSK IT har desuden følgende holdninger og anbefalinger til lovforslagets enkelte bestemmelser:

Til den foreslåede § 3 har DANSK IT følgende bemærkninger:

DANSK IT anbefaler, at de helt centrale begreber, der tillader CFCS at påbyde virksomheder, regioner og kommuner at blive tilsluttet, defineres klart, herunder at det tydeliggøres i loven, præcis hvilke dele af de pågældende virksomheders eller regioner/kommuners aktiviteter, der må anses for at være af "samfundsvigtig" og "særlig samfundsvigtig karakter". Dette er ikke mindst vigtigt i lyset af, at

forsvarsministeren til Politiken i maj 2018 udtalte, at et cyberangreb på en kommune er "ikke noget, der vil lamme samfundet."

Der kan således efter DANSK IT's opfattelse være behov for i lovteksten at få præciseret, hvor grænserne går for, at noget kan anses for at være af samfundsvigtig og særlig samfundsvigtig karakter. Dette skal ses i lyset af, at formålet med et eventuelt påbud er at understøtte et højt informationssikkerhedsniveau i samfundet generelt. Det bemærkes herunder, at der af lovens bemærkninger side 15 fremgår, at der er tale om en lille kreds af virksomheder og myndigheder, der er særligt samfundsvigtige, og at der på side 51 står, at "begrebet samfundsvigtig karakter vil imidlertid også omfatte virksomheder, som ikke i sig selv er samfundsvigtige".

Med den uklarhed, der er omkring begrebet samfundsvigtig i lovforslaget, vil eksempelvis en medievirksomhed kunne påbydes tilslutning. Det virker ikke proportionalt eller hensigtsmæssigt.

Loven bør udtrykkeligt og meget præcis forholde sig til, hvornår en tilsluttet virksomhed kan få oplyst, at den pågældende har været udsat for et persondatasikkerhedsbrud, så virksomheden kan håndtere de forpligtigelser, den har til anmeldelse til Datatilsynet og orientering af de registrerede.

Loven bør således klart angive, at hvis en virksomhed af CFCS er anmodet om at afvente med at anmelde et sikkerhedsbrud/orientere de registrerede, så skal det altid af Datatilsynet anses for en rimelig begrundelse for, at fristen på 72 timer ikke er overholdt. Ligeledes skal det anses som en lovlig forsinkelse, fsva. databehandlere, der af CFCS er blevet anmodet om at afvente med at orientere den dataansvarlige.

DANSK IT anbefaler også, at loven indeholder nogle klare retningslinjer for, hvordan CFCS skal vægte hensyn til opretholdelse af et højt informationssikkerhedsniveau over hensynet til den registreredes rettigheder, så det bliver tydeliggjort, hvornår CFCS kan anmode en virksomhed om ikke at anmelde et persondatasikkerhedsbrud, samt at afvente med at foretage foranstaltninger for at håndtere bruddet på persondatasikkerheden, således at retsusikkerhed undgås.

<u>Til den foreslåede § 5 har DANSK IT følgende bemærkninger:</u>
Uanset at der er tale om en videreførelse af gældende ret, så mener DANSK IT, at der er behov for at tydeliggøre reglerne, og henviser i øvrigt til forholdet til databeskyttelsesforordningen og reglerne om videregivelse og behandling til andre formål end de oprindelige.

<u>Til den foreslåede § 6, stk. 2, har DANSK IT følgende bemærkninger:</u>
Det bør efter DANSK IT's opfattelse i den foreslåede § 6, stk. 2, sidste punktum, præciseres i selve lovteksten, at sletningen sker efter aftale med myndigheden/virksomheden. Det bør endvidere anføres, at sletningen af personoplysninger, som er inficeret, kun bør ske, hvis det er strengt nødvendigt for at opretholde et højt sikkerhedsniveau. Sletning af personoplysning kan udgøre et persondatasikkerhedsbrud, særligt hvis der er tale om en permanent sletning af personoplysninger, der ikke findes andre steder/umiddelbart lader sig genskabe.

Også her anbefaler DANSK IT, at lovgiver forholder sig til reguleringen i databeskyttelsesforordningen, særligt reguleringen af forhold til anmeldelsespligten, underretningen af den registrerede, og hvem der eventuelt skal bære udgifterne til genskabelse af personoplysninger.

<u>Til den foreslåede § 6 a har DANSK IT følgende bemærkninger:</u>
Det fremgår af bemærkningernes side 23 nederst - side 24 øverst, at CFCS ikke vil kunne opbevare følsomme personoplysninger. Dette bør præciseres i loven, da CFCS i medfør af lovens § 11 har hjemmel til

at indsamle og behandle følsomme oplysninger, der er blevet offentliggjort af den pågældende, eller såfremt behandlingen er omfattet af kapital 4, hvor § 6, a er foreslået placeret.

Til den foreslåede § 6 c har DANSK IT følgende bemærkninger:
DANSK IT anbefaler, at begrebet "offentlige tilgængelige" i § 6 c, stk. 2, ændres til "forudsat de er ledige" da dette efter DANSK IT's opfattelse er en mere retvisende betegnelse for, at et domæne, IP-adresse eller e-mail ikke er ejet af nogen, men kan erhverves og anvendes af CFCS.

DANSK IT anbefaler også, at lovforslagets bemærkninger (side 64) gøres til en del af lovteksten, således at CFCS får pligt til at rette henvendelse til ejeren af de pågældende data, hvis det er umiddelbart muligt, og uden yderligere indsats, at identificere ejeren. DANSK IT forudsætter, at loven som anført andetsteds indeholder en regulering af, hvorledes ejeren så skal forholde sig til anmeldelse af det brud på persondatasikkerheden, der så må være tale om.

Til den foreslåede § 7 har DANSK IT følgende bemærkninger:
DANSK IT anbefaler, at der i § 7 c gives mulighed for, at forsvarsadvokaten kan give møde sammen med en kyndig i it, da det ellers vil være meget vanskeligt for forsvarsadvokaten at udtale sig om den af CFCS foretagne proportionalitetsvurdering. DANSK IT bemærker i den forbindelse, at det kunne være hensigtsmæssigt, hvis det i § 7, stk. 3, blev præciseret, at ulempen skal vurderes i forhold til både indehaveren og brugeren af IP-adressen.

Til den foreslåede 8, stk. 2 nr. 1. har DANSK IT følgende bemærkninger:
DANSK IT anbefaler, jf. det tidligere anførte, at der direkte i lovteksten tages stilling til, hvordan forholdene til databeskyttelsesforordningen skal reguleres, særligt i forhold til opfyldelse af et påbud.

Yderligere information:
DANSK IT - Bredgade 25 A - 1260 København K
Tlf: 33 11 15 60 - Email: ks@dit.dk - web: www.dit.dk

02. februar 2019

Til Forsvarsministeriet

Sendt pr. mail til fmn@fmn.dk
med kopi til tbl@fmn.dk og sbu@fmn.dk

Dansk Journalistforbund
Medier & kommunikation

The Danish Union of Journalists

Gammel Strand 46
1202 København K
Danmark

+45 3342 8000
dj@journalistforbundet.dk
journalistforbundet.dk

Dansk Journalistforbunds høringssvar vedrørende udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden), sagsnummer 2018/006599

Dansk Journalistforbund, DJ, skal hermed fremkomme med sit høringssvar vedrørende ovennævnte udkast til forslag til lov.

DJ manglede på høringslisten:
Indledningsvist skal DJ bemærke sin kritik af, at hverken Dansk Journalistforbund eller eksempelvis brancheorganisationen Danske Medier, DR eller TV2 optræder på Forsvarsministeriets høringsliste vedrørende et udkast til et lovforslag, som potentielt kan have en overordentligt indgribende betydning for journalisters og mediers arbejdsforhold.

Generelt om cybersikkerhed:
Fra DJ's side har vi forståelse for forsvarsministerens og andre politikeres ønske om og behovet for en betydeligt øget indsats for at øge cybersikkerheden.

Der er ingen tvivl om, at de ting, der – tilsyneladende, i hvert fald – skete omkring valgene i blandt andet USA, Frankrig, Tyskland og Sverige har været en øjenåbner.

Nej, vi må ikke være naive. Men der er på den anden side også nogle meget væsentlige, demokratiske principper, som vi ikke må give fuldkommen køb på.

Allerede på det generelle plan er det DJ's opfattelse, at det foreliggende lovudkast går alt for vidt i sit indgreb.
DJ mener, at inden politikerne griber til en så detaljeret overvågning af al trafik i og omkring en lang række myndigheder og virksomheder, som lovudkastet giver mulighed for, så bør man grundigt overveje en række øvrige midler til at understøtte forsvaret af de væsentligste samfundsinstitutioner mod cyberangreb.

Eksempelvis bør man prioritere at oplære befolkningen i at kunne kende forskel på fakta og fake på de sociale medier. Det teknologiske forsvar skal styrkes. Men det er mindst lige så vigtigt, at befolkningens generelle evner til at kunne vurdere, om man er i gang med at blive spundet en løgn på ærmet, bliver styrket.

Konkret om medierne:
Lovudkastet er heller ikke acceptabelt, når vi vurderer de konkrete dele af lovudkastet, som vedrører medierne.

Medier og kommunikation nævnes direkte som et område for netsikkerhedstjenestens virke. Lovudkastet giver potentielt mulighed for, at efterretningstjenesten kan overvåge al kommunikation til og fra og i en medievirksomhed. Om nødvendigt med tvang.

Det er helt uacceptabelt. For dermed er man i lovudkastet langt inde og berøre nogle af de væsentligste forudsætninger for at kunne bedrive den uafhængige journalistik og medievirksomhed, som er definerende for et demokratisk samfund. Man antaster mediernes uafhængighed i almindelighed og i særdeleshed muligheden for, at medierne og den enkelte journalist skal kunne beskytte sine kilder.

Det er i den forbindelse kritisabelt, at man i bemærkningerne til lovudkastet ikke i det mindste gør sig nogle overvejelser om disse principielle forhold.

Samtidigt argumenterer man med, at der ikke bliver en tvangsmæssig overvågning, hvis virksomhederne, herunder medievirksomhederne, frivilligt går med til det.
Jo, men det er vel stadigvæk overvågning, selv om det er frivillig overvågning.

Konkret om mediernes muligheder for kildebeskyttelse:
Hvis der fra Forsvarsministeriets side ikke er forståelse for de ovennævnte principielle betragtninger om mediernes uafhængighed og muligheden for at kunne beskytte sine kilders identitet, så vil vi fra DJ's side understrege følgende:

DJ opfordrer til, at mediernes og journalisternes mulighed for at kunne beskytte sine kilders identitet eksplicit sikres i forbindelse med en justering af det foreliggende udkast til lovforslag

Det kan eksempelvis ske ved, at der indsættes en direkte henvisning til retsplejelovens § 172 om kildebeskyttelse.

Hvis dette høringssvar giver anledning til yderligere spørgsmål eller kommentarer, står DJ gerne til rådighed, mail DJ@journalistforbundet.dk.

Venlig hilsen

Hans Jørgen Dybro
politisk konsulent
dybjournalistforbundet.dk

Lægeforeningen

Høringssvar

Formanden

30. januar 2019
Sagsnr: 2019 - 513/1675891

Domus Medica
Kristianiagade 12
2100 København Ø

Tlf.: 35448500
Tlf.: 35448141 (direkte)
E-post: dadl@dadl.dk
E-post: llg@DADL.DK
www.laeger.dk

Høring over udkast til Lov om ændring af lov om Center for Cybersikkerhed

Lægeforeningen ser risiko for

- **at fortroligheden mellem læge og patient bliver kompromitteret, når en større personkreds får adgang til personfølsomme helbredsdata, og**
- **at nogle patienters behandling som minimum bliver besværliggjort, pga. risikoen for at personfølsomme journaloplysninger slettes**

Endvidere mener Lægeforeningen, at lovforslaget i højere grad skal sikre, at personfølsomme helbredsoplysninger ikke deles blandt personer, der ikke har patienterne i aktuel behandling.

Lægeforeningen er blevet opmærksom på høring om ændring af lov om Center for Cybersikkerhed. Lægeforeningen er ikke høringspart, men afgiver hermed høringssvar.

Det skyldes ifølge lovudkastet, at kommuner, regioner og virksomheder der har "samfundsvigtig karakter" kan blive anmodet om at blive tilsluttet netsikkerhedstjenesten – og at man også kan få påbud om at blive tilsluttet.

Da sundhedssektoren er udpeget som en samfundskritisk sektor[1] forventer Lægeforeningen, at loven kan komme til at berøre medlemmer af Lægeforeningen direkte eller indirekte.

Lægeforeningen deler lovforslagets overordnede målsætning om at styrke cybersikkerheden i vores samfund. Men vi har følgende punkter, der har betydning for medlemmerne:

1) *Udvidelse af personkredsen, der får adgang til journaldata*
   Lovudkastet vedrører indhentning og opbevaring af stationære data. I sundhedsvæsenet er en stor del af de stationære data personfølsomme. Det er sundhedsloven, der bl.a. regulerer, hvem der i dag har adgang til patientfølsomme helbredsoplysninger til andre formål end behandling. Lægeforeningen mener, at lovændringen medfører en væsentlig udvidelse af personkredsen, der kan få adgang til journaldata. Det medfører en risiko for, at tilliden og fortrolighedsforholdet mellem læge og patient kompromitteres. Vi mener derfor, at lovforslaget i højere grad skal sikre, at personfølsomme helbredsoplysninger ikke deles blandt personer, der ikke har patienterne i aktuel behandling.

[1] Strategi 2019- 2022: En styrket, fælles indsats for cyber- og informationssikkerhed, Politisk Cyberforum for sundhedssektoren.

2) *Sletning af stationære data*
Lovudkastet indeholder i §6 en mulighed for, at Center for Cybersikkerhed, kan slette stationære data. Lægeforeningen pointerer, at sletning af journaldata vil være meget ødelæggende for patientbehandlingen og foreslår, at det fremgår af loven, at sletning kun bør forekomme i yderste nødstilfælde.
Lægeforeningen er opmærksom på lovbemærkningerne side 17 om, at det er frivilligt at tilslutte sig det aktive cyberforsvar.
Lægeforeningen mener endvidere, at der er risiko for, at sundhedsvæsenets aktører ikke vil tilslutte sig det aktive cyberforsvar, hvis deres indtryk er, at der er høj risiko for, at journaldata slettes.

3) *Meromkostninger for læger i almen praksis og speciallægepraksis*
I det omfang de virksomheder, der leverer lægesystemer, som praktiserende læger og praktiserende speciallæger anvender, bliver anmodet eller pålagt at blive tilsluttet netsikkerhedstjenesten, gør vi opmærksom på, at det, hvis det påfører leverandørerne et øget tidsforbrug eller lignende, kan medføre meromkostninger for almen praktiserende læger og praktiserende speciallæger gennem højere priser til leverandørerne.

Med venlig hilsen

Andreas Rudkjøbing

Forsvarsministeriet
Holmens Kanal 42
1060 København K
Danmark
E-mail: fmn@fmn.dk. Kopi til tbl@fmn.dk og sbu@fmn.dk

Dansk Magisterforening

4. februar 2019
Sag 19-01326

Dansk Magisterforenings høringssvar til Lov om ændring af lov om Center for Cybersikkerhed

Dansk Magisterforening (DM) afgiver hermed høringssvar til ændring af Lov om Center for Cybersikkerhed (CFCS).

DM deler lovforslagets overordnede målsætning om at styrke indsatsen for større cybersikkerhed i samfundet. Men vi er meget bekymrede over, at lovforslaget lægger op til at give CFCS adgang til at iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejdere uden en retskendelse.

I forhold til det konkrete forslag har DM valgt at fokusere på den del af udkastet, der omhandler forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder.

Vedr. forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder

Af lovforslaget fremgår det, at CFCS i forbindelse med en sikkerhedsteknisk undersøgelse, kan anvende social engineering i form af f.eks. spear-phishing, hvor der målrettes et simuleret angreb mod udvalgte medarbejdere.

DM finder det dybt problematisk, at CFCS, efter aftale med virksomhedens ledelse, får adgang til at lægge fælder ud for udvalgte medarbejdere, uden en retskendelse eller en konkret mistanke om en sikkerhedshændelse.

Det fremgår ligeledes af lovforslaget, at medarbejderne først orienteres efter den sikkerhedstekniske undersøgelse er afsluttet. Det er i det hele bekymrende, at en myndighed får mulighed for at narre bestemte medarbejdere til uforvarende at bryde virksomhedens eller myndighedens retningslinjer.

DM finder ikke, at der er proportionalitet mellem forslagets formål og de konsekvenser, herunder ansættelsesretlige konsekvenser for medarbejderen, som dette kan få. DM mener derfor, at:

- Det skal præciseres og afgrænses præcist hvornår og med hvilke midler CFCS har adgang til at iværksætte yderligere forebyggelsesaktiviteter rettet mod medarbejdere.
- Virksomheder og myndigheder skal pålægges en orienteringspligt om, at der iværksættes kontrolforanstaltninger, som der kun må ses bort fra, hvis CFCS har en konkret og begrundet mistanke.

Såfremt der måtte være spørgsmål eller kommentarer til vores bemærkninger ovenfor, er I velkommen til at kontakte undertegnede.

Venlig hilsen

Camilla Gregersen
Formand
cg@dm.dk

DANSKE MEDIER

Pressens Hus
Skindergade 7
DK-1159 København K

Telefon 3397 4000

info@danskemedier.dk
www.danskemedier.dk

Forsvarsministeriet
Holmens Kanal 9
1060 København K

30. januar 2019

Høringssvar vedr. udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed – sagsnummer 2018/006599

Danske Medier ønsker hermed at fremkomme med bemærkninger til Forsvarsministeriets høring over det ovenfor nævnte lovudkast.

Indledningsvist bemærkes, at Danske Medier som præmis for lovudkastet anerkender, at der er en høj cybertrussel mod Danmark, og at trusselsbilledet til stadighed forandres. Derfor har foreningen heller ikke bemærkninger til det overordnede behov for at justere lovgrundlaget for Center for Cybersikkerhed (CFCS) under Forsvarets Efterretningstjeneste.

Danske Medier finder imidlertid anledning til at kommentere enkelte elementer i forslaget, herunder navnlig udformningen af den nye § 3 om CFCS' netsikkerhedstjeneste.

Ad § 3

Det er magtpåliggende for Danske Medier, at private medievirksomheder i Danmark ikke under nogen omstændigheder kan tvinges til at underlægge sig et system under en efterretningstjeneste, hvorved man – uden retskendelse – kan behandle virksomhedernes data, herunder indholdet af den kommunikation, der transmitteres.

En sådan ordning vil bringe mediernes muligheder for at producere fri og uafhængig journalistik i fare og være ødelæggende for omverdenens tillid til, at medierne er i stand til at beskytte deres kilder. Dette vil samtidig være i strid med artikel 10 i Den Europæiske Menneskerettighedskonvention. Der henvises i øvrigt til Europarådets Parlamentariske Forsamlings rekommandation 1950 (2011) om beskyttelsen af journalisters kilder, der i punkt 12 direkte adresserer offentlige myndigheders indgreb i journalisters korrespondance m.v. Derfor er foreningen selvsagt meget optaget af, hvilke virksomheder, der efter lovudkastet kan blive tilsluttet CFCS' netsikkerhedstjeneste og under hvilke betingelser.

Danske Medier konstaterer, at lovudkastets § 3, stk. 3, muliggør, at virksomheder, der har "samfundsvigtig karakter" – ligesom efter den gældende CFCS-lov – efter anmodning kan blive tilsluttet netsikkerhedstjenesten. Foreningen har ikke indvendinger mod denne mulighed for virksomheder, selvom den ifølge bemærkningerne til lovforslagets enkelte bestemmelser omfatter medier. Det fremgår således, at der ved samfundsvigtige funktioner

forstås ”funktioner, som er særligt vigtige for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed”, herunder blandt andet medier.

Danske Medier noterer, at der i tillæg til muligheden for virksomheder for frivillig tilslutning til netsikkerhedstjenesten i § 3, stk. 3, endvidere ønskes indført en mulighed for, at CFCS kan påbyde virksomheder, der har ”særligt samfundsvigtig karakter”, at blive tilsluttet netsikkerhedstjenesten, jf. § 3, stk. 4. Foreningen finder det meget vidtgående og principielt stærkt betænkeligt, at der ved lov indføres en mulighed for tvangsovervågning af private virksomheder. Danske Medier konstaterer i øvrigt, at de i lovbemærkningerne nævnte kriterier for, hvornår en virksomhed kan anses for at have særligt samfundsvigtig karakter, ikke umiddelbart omfatter virksomheder, der udgiver massemedier. Foreninger finder imidlertid, at det bør fremhæves explicit i bemærkningerne, at bestemmelsen ikke kan anvendes på virksomheder, hvis hovedformål er at udgive massemedier omfattet af medieansvarslovens § 1.

Ad kapitel 4

Danske Medier mener, at der i tillæg til den oven for foreslåede udelukkelse af at anvende § 3, stk. 4, på medievirksomheder bør indsættes en reference i kapitel 4 til retsplejelovens §§ 169-172 om vidnefritagelse m.v. Det bør således tydeliggøres, at CFCS ikke kan behandle data fra virksomheder, der er tilsluttet netsikkerhedstjenesten, hvis der derved vil fremkomme oplysninger om forhold, som ikke kan gøres til genstand for vidneforklaring i retten.

Det bemærkes, at lovudkastets forslag til kapitel 4 a om edition i § 7, stk. 2, netop indeholder en reference til retsplejelovens §§ 169-172.

Danske Medier står naturligvis til rådighed, såfremt ovenstående bemærkninger ønskes uddybet. Henvendelser herom kan rettes til chefjurist Holger Rosendal på telefon 3397 4000 eller email hrd@danskemedier.dk.

Med venlig hilsen
Danske Medier

Morten Langager
Adm. direktør

DanskeRederier

Forsvarsministeriet
Att.: Chefkonsulent Stine Østergren
Holmens Kanal 9
1060 København K
(Sendt via e-mail)

Høringssvar vedr. udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed

4. februar 2019

Sagsnummer:
EMN-2016-00289

Der henvises til høringsbrev af 7. januar 2019 vedr. udkast til forslag om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden), sagsnummer: 2018/006599.

Vi noterer os, at der med lovforslaget foreslås, at bl.a. virksomheder, der har samfundsvigtig karakter, kan anmode om at blive tilsluttet netsikkerhedstjenesten hos Center for Cybersikkerhed (CFCS), jf. § 3, stk. 3. I den forbindelse finder vi det positivt, at der fremover ikke vil blive opkrævet et tilslutningsgebyr. Vi er af den opfattelse, at afskaffelsen af tilslutningsgebyret vil kunne være med til at øge antallet af virksomheder, som ønsker at blive tilsluttet CFCS's netsikkerhedstjeneste. Det skal dog bemærkes, at der fortsat kan være væsentlige omkostninger forbundet ved at tilslutte sig netsikkerhedstjenesten.

Vi finder, at det er meget væsentligt, at virksomhedernes evt. tilslutning til netsikkerhedstjenesten sker ad frivillighedens vej, og i en åben dialog mellem virksomheden og CFCS. En tilslutning til netsikkerhedstjenesten skal være til fælles gavn for virksomhedens cyberbeskyttelse og CFCS's opgavevaretagelse. Derfor finder vi det stærkt bekymrende, at der med lovforslagets § 3, stk. 4 gives hjemmel til CFCS at kunne påbyde virksomheder, at blive tilsluttet netsikkerhedstjenesten, såfremt en virksomhed ikke selv ønsker at blive tilsluttet netsikkerhedstjenesten. Denne mulighed finder vi både ubegrundet og uproportional. Efter vores opfattelse, er muligheden for et påbud meget problematisk, da det vil tvinge private virksomheder til at dele kundefølsomme data og informationer med CFCS. Det er vores bekymring, at dette kan medføre,

at kunderne finder andre tjenesteudbydere, hvor kunderne fuldt ud kan sikre sig, at deres data og indsigt i deres processer holdes fortrolige og ikke deles med tredjepart. Det er umiddelbart vores vurdering, at fjernelsen af tilslutningsgebyret i sig selv vil være tilstrækkeligt til i nødvendigt omfang at sikre tilslutning til CFCS' netsikkerhedstjeneste – og derfor er muligheden for et påbud ikke nødvendigt og bør ikke indgå i den reviderede lov om Center for Cybersikkerhed.

Såfremt den rapport om erfaringer med den nye lovgivning, som skal oversendes til Folketinget tre år efter lovens ikrafttræden, jf. side 9 i udkastet konkret efterfølgende måtte begrunde et sådant behov, vil det på dette tidspunkt kunne overvejes gennemført ved en senere lovændring.

Skulle der med lovforslag forsat blive givet CFCS mulighed for at komme med påbud om tilslutning til netsikkerhedstjenesten, er det vores opfattelse at dette skal begrænses til offentlige myndigheder.

Det er yderligere vores vurdering, at enhver form for tilslutning til netsikkerhedstjenesten kan have en finansiel indvirkning i forbindelse med opsætningen og driften af hardware og software. I forslaget hedder det, at de nærmere regler kan fastsættes af ministeriet (jf. § 3, stk. 5). Særlig ved et evt. påbud bør der være mulighed for en kollektiv/national finansiering i stedet for at kunne pålægge virksomhederne disse afledte ekstraomkostninger, som der lægges op til, jf. bemærkningerne i forslaget nedrest side 43.

Såfremt den nye lovgivning kommer til at indeholde en påbudsmulighed, har vi noteret os, at der i lovforslaget gøres opmærksom på, at påbuddet om tilslutning til netsikkerhedstjenesten udelukkende vil kunne meddeles virksomheder, som har særlig samfundsvigtig karakter og væsentlig betydning for Danmarks kritiske infrastruktur. I den forbindelse henvises der til 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), jf. nederst side 53. Definitionen af hvad der forstås ved kritisk infrastruktur, finder vi ikke er nærmere defineret i lovforslaget. Med henvisning til den

DanskeRederier

sektorspecifikke implementering af NIS-direktivet i Danmark, finder vi det derfor væsentligt, at der er overensstemmelse mellem de virksomheder den sektoransvarlige myndighed har udpeget, og dem som CFCS evt. ønsker at påbyde tilslutning til netsikkerhedstjenesten. Ved de sektorspecifikke implementeringer af NIS-direktivet er der generelt opstillet klart fastlagte kriterier og processer for udvælgelse.

Med venlig hilsen

Morten Glamsø
Chefkonsulent

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.

Forsvarsministeriet
Holmens Kanal 9
1060 København K

ATT.: fmn@fmn.dk, cc: tbl@fmn.dk og sbu@fmn.dk
Sagsnummer 2018/006599

DATO: 1. februar 2019
PROJEKTNR.: 3012
pm/sv/CEL

Høringssvar - ændring af lov om Center for Cybersikkerhed

Dansk Vand- og Spildevandsforening (DANVA) mener principielt, at Center for Cybersikkerhed (CFCS) og Forsvarets Efterretningstjeneste(FE) bør have de rammer og den adgang til data, informationer og viden, der er nødvendige for, at CFCS og FE kan være med til at sikre og understøtte samfundet - bl.a. selskabernes IT, driften af forsyningerne mv.

DANVA mener, at det er vigtigt, at lov om Center for Cybersikkerhed løbende, efter behov, justeres til gavn for cybersikkerheds- og efterretningsarbejdet. DANVA vil gerne fremover sættes på høringslisten, så vi ikke en anden gang skal agere med afsæt i pressens omtale af en høring.

DANVA vil gerne bidrage til at sikre forsyningsselskabernes informationssystemer, der er afgørende for forsyningssikkerheden samt de produkter og services, som vandselskaberne leverer til kunderne. Kritiske digitale systemer og data skal beskyttes effektivt, og CFCS vil på mange måder kunne bidrage til at forbedre cybersikkerheden i forsyningsselskaber.

Udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed finder vi er med til at forbedre rammerne for cybersikkerheds- og efterretningsarbejdet, og vi værdsætter, at der i bemærkningerne lægges vægt på, at der arbejdes frem mod at etablere et frugtbart og effektivt samarbejde med forsyningsselskaberne.

Vi vil gerne kvittere for, at det fremgår af lovbemærkningerne, at drikkevandsforsyning og –distribution indgår som en særlig samfundsvæsentlig sektor. Vi forventer, at samarbejdet mellem CFCS og vandsektoren udbygges i de kommende år til fælles fordel for CFCS og vandsektoren.

Udover at loven løbende bør forbedres, anser vi det også for vigtigt, at der løbende tages yderligere initiativer udenfor CFCS regi, der skaber gode vilkår for at forbedre cybersikkerheden. Fx initiativer der kan forbedre videndeling, krav til leverandører, best-practices, standarder mv.

Vi bemærker, at en del væsentlige forhold er beskrevet i bemærkningerne. Forhold, der er afgørende for at få en god implementering og for CFCS's virke. Væsentlige forhold er understreget nedenfor i 5 kortfattede afsnit sammen med få forslag til forbedringer af udkastet. Vi har i vores høringssvar primært fokus på forhold, der er afgørende for et velfungerende cybersikkerhedssamarbejde mellem CFCS og vandsektorens forsyningsselskaber, da vi finder, at det er her, DANVA fremadrettet har en central rolle.

Velfungerende cybersikkerhedsarbejde, frugtbart og klart samarbejde mellem CFCS og selskaberne

Det er vigtigt, at der etableres et frugtbart og velfungerende, dialogbaseret samarbejde mellem CFCS og de selskaber, der, enten frivilligt eller via påbud, er med i netsikkerhedstjenesten. Dette indebærer, at det er synligt og klart, hvilke midler og mål samarbejdet er baseret på. Derfor værdsætter vi, at der i bemærkningerne lægges vægt på, at samarbejdet om netsikkerhedstjenesten tager højde for selskabernes behov, og at aftaler er dialogbaserede.

Omfattede virksomheder
I forhold til de virksomheder, som efter forslaget skal være omfattet af loven, er der behov for, at det uddybes, hvilke kriterier der kan indgå i CFCS's vurdering af, hvilke virksomheder der *kan* tilsluttes netsikkerhedstjenesten, og hvilke der ved eventuelt pålæg *skal* tilsluttes, herunder hvad der nærmere menes med virksomheder af *samfundsvigtig karakter* og virksomheder af *særlig samfundsvigtig karakter.*

Det er afgørende for virksomhederne, at påbudsafgørelser foretages på proportionale og gennemskuelige vilkår, ligesom det må kræves, at CFCS's afgørelse herom er begrundet og kan påklages.

Påbud og aftaler - tidsbegrænsede og velbegrundede
CFCS og det enkelte selskab bør regelfast være i dialog om samarbejdet og justere påbud, tilslutningsaftaler og øvrige samarbejdsaftaler. Vores betragtning er baseret på, at dette sikrer, at påbud og aftaler regelmæssigt genovervejes og tilrettes, og samarbejdet justeres for at undgå, at der opstår uhensigtsmæssigheder, unødig administration og arbejde.

Det er DANVAs opfattelse, at det bør tilføjes, at adgang til data uden retskendelse fordrer, at CFCS kan godtgøre, at der er en begrundet mistanke og i øvrigt naturligvis, at indgrebet var nødvendigt for at undgå, at formålet forspildes. Hertil skal lægges et almindeligt krav om ret til domstolsprøvelse. Det forekommer retssikkerhedsmæssigt betænkeligt, at en myndighed på så løst et grundlag som en vurdering af "et højt informationssikkerhedsniveau" kan knægte en grundlovssikret ret om privatlivets fred.

Vi håber, at deltagelse i netsikkerhedstjenesten giver 'value for money', så flere selskaber vil indgå i netsikkerhedstjenesten.

Indvirkning på selskabernes økonomi og kompensation
Det er ikke velbeskrevet, hvilke omkostninger – direkte som indirekte – loven vil afstedkomme for selskaberne. Selskaber, der som følge af den nye lov må afsætte ressourcer og økonomi hertil, bør kompenseres, så samfundsvæsentlige selskaber ikke straffes økonomisk og ressourcemæssigt: Fx hvis et selskab efter kriterier (der pt. er uklare) påbydes deltagelse i netsikkerhedstjenesten og dermed pålægges omkostninger og må anvende ressourcer på samarbejdet. Det synes at give mening, at sammenhængen med den økonomiske regulering for vandsektoren overvejes, således at selskaberne sikres omkostningsdækning.

Erstatningsansvar ved sikkerhedsbrud forårsaget af CFCS
Fejl og sikkerhedsbrud kan opstå i forbindelse med CFCS's og selskabernes samarbejde både i forbindelse med databehandling og datakommunikation. Disse sikkerhedsbrud vil i værste tilfælde kunne medføre store omkostninger for selskaberne eller på anden måde have en negativ effekt på selskaberne. CFCS's ansvar og erstatningsansvar i forbindelse med sikkerhedsbrud, forårsaget af CFCS, bør beskrives i bemærkningerne om erstatningsansvar side 58-59. Det skal sikres, at sandsynligheden for sikkerhedsbrud minimeres, og at der er en ansvarsfordeling og organisering, der tager hånd om sikkerhedsbrud, så der ikke opstår tvister mv.

Sikring af selskabernes data, kundedata og databeskyttelsesloven
Beskyttelse af kunde- og selskabsdata er meget vigtig og bør prioriteres højt. Der bør være saglige, faste og velbeskrevne regler for CFCS's databehandling og sletning af data, i det omfang det er muligt. CFCS bør kun behandle og analysere data efter klare regler og bør ikke opbevare overflødige data. Selskaber bør underrettes regelfast, hvis data, herunder kundedata, blokeres eller slettes, og kommunikation forsinkes, så selskaberne er bekendt hermed og kan tage højde for dette. Det er afgørende, at persondata beskyttes, at meddelelseshemmeligheden håndhæves, og at CFCS's arbejde tager højde for databeskyttelsesloven.

Videndeling og udsendelse af advarsler og operationel information
De indsamlede data, information og viden skal deles til gavn for forsyningsselskaber m. fl. I bemærkningerne kommer det også frem, at selskaberne får afrapportering af overvågningen og logs. Det er meget positivt, at der afrapporteres, og vi ser frem til, at det sker på en operationel måde. Selskaber bør også videregive data, information og viden om cybersikkerhed, herunder trusler, som selskaberne mener vil kunne bidrage til CFCS's arbejde.
CFCS bør generelt bestræbe sig på at publicere information og viden om cybersikkerhed til gavn for forsyningskritiske selskaber fx via nyhedstjenester, databaser eller lign., hvor der publiceres advarsler, Indicators of compromise, IOC, guidelines mv.

CFCS er en del af Danmarks efterretningstjeneste. Det indebærer, at en stor del af centrets aktiviteter er fortrolige. Det medfører samtidig, at selskaber, øvrige myndigheder og borgere må have tillid til centrets arbejde og aktiviteter. I forhold til samfundskritiske forsyningsselskaber anbefaler DANVA, at der er fortrolighed og en så stor åbenhed som muligt mellem centret og selskaberne. Dette vil kunne danne et godt udgangspunkt for at parterne - samlet – kan arbejde effektivt med at forbedre cybersikkerheden.

DANVA står naturligvis til rådighed for en uddybning eller yderligere diskussion af indholdet.

Med venlig hilsen

Carl-Emil Larsen
DANVA

DATATILSYNET

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt til: fmn@fmn.dk
Cc: tbl@fmn.dk, sbu@fmn.dk og jm@jm.dk

30-01-2019

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200

E-mail dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2019-11-0188
Dok.nr. 61302
Sagsbehandler
Camilla Andersen

Høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden) – sagsnummer 2018/006599

Ved e-mail af 7. januar 2019 har Forsvarsministeriet anmodet om Datatilsynets bemærkninger til ovennævnte udkast til lovforslag.

1. Indledning

Databeskyttelsesforordningen[1] og databeskyttelsesloven[2] finder ikke anvendelse på den behandling af personoplysninger, som udføres for eller af politiets eller forsvarets efterretningstjenester, jf. databeskyttelseslovens § 3, stk. 2.

Center for Cybersikkerhed (herefter CFCS) er en del af Forsvarets Efterretningstjeneste, og databeskyttelsesforordningen og databeskyttelsesloven finder derfor ikke anvendelse på de behandlinger af personoplysninger, CFCS som dataansvarlig foretager.

Reglerne i databeskyttelsesforordningen og databeskyttelsesloven finder derimod anvendelse på behandlinger af personoplysninger foretaget af myndigheder og private virksomheder, som er tilsluttet CFCS' netsikkerhedstjeneste eller på anden måde anmoder om bistand fra centeret og i den forbindelse bl.a. videregiver personoplysninger til CFCS.

På den baggrund – og idet udkastet efter Datatilsynets opfattelse åbner op for en bred behandling af personoplysninger, som hører under databeskyttelsesforordningens og databeskyttelseslovens anvendelsesområde – finder Datatilsynet anledning til at fremkomme med følgende bemærkninger:

---

[1] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF.

[2] Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

2. Generelle bemærkninger

2.1. I bemærkningerne til lovforslaget henvises der flere steder til persondataloven og de centrale principper heri. Der henvises bl.a. hertil i de særlige bemærkninger til § 1, nr. 4:

> "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."

Datatilsynet skal henstille til, at alle henvisninger til persondataloven ændres, så der i stedet alene henvises til de gældende databeskyttelsesretlige regler.

2.2. Det fremgår af pkt. 1 i de almindelige bemærkninger, at der – henset til den hastige udvikling på cybersikkerhedsområdet – vil blive udarbejdet en rapport om erfaringerne med den nye lovgivning, som oversendes til Folketinget tre år efter lovens ikrafttræden.

Datatilsynet finder, at netop den hastige udvikling på området, men også det forhold, at der som tidligere nævnt efter tilsynets opfattelse med udkastet ses at blive åbnet op for en bred behandling af personoplysninger, taler for, at rapporten om erfaringerne med den nye lovgivning oversendes til Folketinget allerede ét år efter lovens ikrafttræden.

2.3. Det er endvidere Datatilsynets vurdering, at udkastet på følgende punkter giver anledning til væsentlige uklarheder om de databeskyttelsesretlige regler:

- Definitionerne (udkastets § 1, nr. 1).
- Fordelingen af dataansvaret i forbindelse med behandling af personoplysninger, herunder særligt indsamling og videregivelse til de tilsluttede myndigheder og virksomheder.
- Behandlingsgrundlag i henhold til databeskyttelsesforordningens artikel 6 og 9 samt databeskyttelseslovens § 8 for de tilsluttede myndigheder og virksomheder.
- Behandlingssikkerheden og forpligtelserne der følger af databeskyttelsesforordningens artikel 32-34.

Ovenstående punkter behandles nærmere nedenfor.

3. Konkrete bemærkninger

3.1. I udkastets § 1, nr. 1, foreslås § 2 i lov om Center for Cybersikkerhed affattet 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."

3.1.1. Af de særlige bemærkninger til udkastets § 1, nr. 1, fremgår følgende:

> "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."

Begrebet behandling defineres i databeskyttelsesforordningens artikel 4, nr. 2, imidlertid som enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for.

Datatilsynet skal henstille til, at udtrykkene "operationer" og "elektronisk" i lovteksten og bemærkningerne hertil ændres, således at indeholdet af bestemmelsen kommer til at svare til de gældende databeskyttelsesretlige regler.

3.1.2. I den foreslåede § 2, stk. 1, nr. 1, defineres en sikkerhedshændelse som en hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.

Datatilsynet skal i den forbindelse oplyse, at der efter databeskyttelsesforordningens artikel 33 gælder en generel forpligtelse for alle dataansvarlige til som udgangspunkt at anmelde brud på persondatasikkerheden til Datatilsynet.

Et brud på persondatasikkerheden defineres i forordningens artikel 4, nr. 12, som et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger der er transmitteret, opbevaret eller på anden måde behandlet.

En sikkerhedshændelse som defineret i den foreslåede § 2, stk. 1, nr. 1, ses dermed også at kunne være et brud på persondatasikkerheden. Det er imidlertid alene de sikkerhedshændelser, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personop-

lysninger, der også udgør et brud på persondatasikkerheden. En sikkerhedshændelse vil således ikke altid være et brud på persondatasikkerheden.

Datatilsynet finder, at det er vigtigt, at ovenstående præciseres og direkte fremgår af bemærkningerne til udkastet.

3.1.3. I den foreslåede § 2, stk. 1, nr. 2-5, defineres begreberne pakkedata, trafikdata, stationære data og malware.

Det er Datatilsynets opfattelse, at disse fire begreber også indeholder personoplysninger, som defineret i databeskyttelsesforordningen og i den foreslåede § 2, stk. 1, nr. 6. Dette ses dog ikke at fremgå af hverken de foreslåede definitioner i § 2, stk. 1, nr. 2-5, eller bemærkningerne hertil. På nuværende tidspunkt sondres der således skarpt imellem om oplysningerne hører under enten et af begreberne "pakkedata, trafikdata, stationære data, malware" eller begrebet "personoplysninger", selv om der meget ofte vil være et betydeligt sammenfald.

Det er efter Datatilsynets opfattelse vigtigt, at dette præciseres og direkte fremgår af bemærkningerne til udkastet.

Der henvises endelig til det ovenfor under pkt. 2.1. anførte om henvisninger i udkastets bemærkninger til "persondataloven".

3.2. Af udkastet fremgår det, at CFCS skal kunne tilbyde passivt og aktivt cyberforsvar til de tilsluttede myndigheder og virksomheder. Endvidere vil CFCS, efter aftale med den tilsluttede myndighed eller virksomhed, kunne foretage forebyggende sikkerhedstekniske undersøgelser.

Det er Datatilsynets forståelse, at der kan ske behandling af personoplysninger både i forbindelse med et passivt og aktivt cyberforsvar og i forbindelse med forebyggende sikkerhedstekniske undersøgelser. Det er imidlertid ikke klart, hvem der anses for dataansvarlig i forbindelse med disse behandlinger af personoplysninger.

Udkastet fastslår således på nuværende tidspunkt ikke, hvem der er dataansvarlig for den eventuelle behandling af personoplysninger, der vil ske som følge af monitorering af lokale enheder i forbindelse med det passive cyberforsvar[3], eller når CFCS efter aftale med den tilsluttede myndighed eller virksomhed foretager sikkerhedstekniske undersøgelser og i den forbindelse bl.a. indsamler oplysninger om de ansatte via offentlige tilgængelige kilder.

Datatilsynet kan i den forbindelse oplyse, at en dataansvarlig i databeskyttelsesforordningens artikel 4, nr. 7, defineres som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

---

[3] Se de almindelige bemærkninger pkt. 3.3.3.1.

En databehandler defineres i forordningens artikel 4, nr. 8, som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne.

Datatilsynet har endvidere noteret sig, at det følger af bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste[4] § 2, at den eller de alarmenheder, som opsættes i medfør af tilslutningsaftalen, jf. § 1, er Center for Cybersikkerheds ejendom, og at centeret er dataansvarlig for data, der indsamles og i øvrigt behandles i forbindelse med driften af alarmenheden.

Datatilsynet skal derfor henstille, at Forsvarsministeriet nærmere overvejer – og i forlængelse heraf i udkastet præciserer – hvem der er dataansvarlig for de behandlinger af personoplysninger, der sker som følge af det aktive og passive cyberforsvar og i forbindelse med forebyggende sikkerhedstekniske undersøgelser, herunder om den ovennævnte bestemmelse i bekendtgørelsen om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste bør fremgå af udkastet eller bemærkningerne hertil, hvis CFCS må anses som dataansvarlig.

Datatilsynet skal i forlængelse heraf understrege vigtigheden af, at det er klart, hvem der er dataansvarlig for de enkelte behandlinger af personoplysninger, særligt for de registrerede, som efter de databeskyttelsesretlige regler har en række rettigheder over for de dataansvarlige, men også for de tilsluttede myndigheder og virksomheder i forhold til deres forpligtelser efter de databeskyttelsesretlige regler, herunder overholdelse af de registreredes rettigheder.

3.3. Af pkt. 9 i udkastets almindelige bemærkninger om forholdet til EU-retten fremgår følgende:

> ”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.

[4] Bekendtgørelse nr. 1599 af 14. december 2018

> 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."

Datatilsynet skal om behandling af almindelige personoplysninger henlede opmærksomheden på databeskyttelsesforordningens artikel 6, hvorefter der alene kan ske behandling af almindelige personoplysninger, i det omfang mindst ét af følgende forhold gør sig gældende:

a) Den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.
b) Behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.
c) Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.
d) Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser.
e) Behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.
f) Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

Det følger endvidere af artikel 6, stk. 1, litra f, 2. afsnit, at litra f, første afsnit, ikke gælder for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.

En offentlig myndighed vil dermed som udgangspunkt ikke kunne behandle personoplysninger, herunder videregive personoplysninger til CFCS, på baggrund af legtime interesser i medfør af artikel 6, stk. 1, litra f.

Om behandling af oplysninger om strafbare forhold kan Datatilsynet endvidere oplyse, at behandling af disse oplysninger er reguleret i databeskyttelseslovens § 8.

På den baggrund finder Datatilsynet, at Forsvarsministeriet skal overveje, hvorvidt de tilsluttede myndigheder og virksomheders behandling af personoplysninger i forbindelse med udkastet kan ske inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

Forsvarsministeriet skal i den forbindelse særligt overveje, om de tilsluttede myndigheder har hjemmel i forordningens artikel 6, stk. 1, litra a-e til behandling af almindelige personoplysninger, om de tilsluttede myndigheder og virksomheder har hjemmel i databeskyttelseslovens § 8 til behandling af oplysninger om strafbare forhold og endelig om reglerne i udkastet kan udgøre en national særregel i medfør af databeskyttelsesforordningens artikel 9, stk. 2, litra g. Forsvarsministeriet skal i den forbindelse foretage en vurdering i henhold til "tjeklisten" om udarbejdelse af nye nationale særregler for behandling af følsomme personoplysninger, som fremgår af side 229f i betænkning nr. 1565 om databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning.

3.4. Af de særlige bemærkninger til udkastets § 1, nr. 3, fremgår følgende om den foreslåede § 6:

> "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.
>
> […]
>
> 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.
> […]
>
> 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.

> […]
>
> 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.
>
> […]
>
> 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."

Datatilsynet skal i den forbindelse henlede opmærksomheden på reglerne i databeskyttelsesforordningen om behandlingssikkerhed og brud på persondatasikkerheden.

Det følger af forordningens artikel 32, at den dataansvarlige og databehandleren under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

Af forordningens artikel 32, stk. 2, følger det endvidere, at der ved vurderingen af, hvilket sikkerhedsniveau der er passende, navnlig skal tages hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Et brud på persondatasikkerheden defineres – som tidligere nævnt – i forordningens artikel 4, nr. 12, som et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Den tilsluttede myndighed eller virksomhed bør derfor – eventuelt i samarbejde med CFCS – nærmere overveje, hvordan denne risiko for fejl fra CFCS' side i forbindelse med det aktive cyberforsvar håndteres i forhold til den dataansvarliges forpligtelser i databeskyttelsesforordningens artikel 32, 33 og 34.

3.5. Som følge af det foreslåede passive cyberforsvar – men især det aktive cyberforsvar og de forebyggende sikkerhedstekniske undersøgelser er det

endvidere Datatilsynets forståelse, at CFCS vil kunne få kendskab til brud på persondatasikkerheden, som den tilsluttede myndighed eller virksomhed ikke nødvendigvis selv er bekendt med.
Datatilsynet skal i den forbindelse igen henlede opmærksomheden på de forpligtelser den tilsluttede myndighed eller virksomhed har efter databeskyttelsesforordningens artikel 33 til at anmelde et brud på persondatasikkerheden uden unødig forsinkelse og om muligt senest 72 timer efter, at denne er blevet bekendt med bruddet. Der kan endvidere henvises til artikel 32 om den dataansvarliges forpligtelse til at sikre persondatasikkerheden.

På den baggrund forekommer det efter Datatilsynets opfattelse uhensigtsmæssigt, at CFCS kan blive bekendt med et brud på persondatasikkerheden hos en tilsluttet myndighed eller virksomhed, uden at CFCS ses at være forpligtet til at oplyse den tilsluttede myndighed eller virksomhed herom.

Kopi af dette brev sendes til Justitsministeriets Lovafdeling til orientering.

Med venlig hilsen

Camilla Andersen

Dansk Internet Forum

Forsvarsministeriet
E-mail: fmn@fmn.dk

Høringssvar

30-01-2019

DIFO om ændring af lov om Center for Cybersikkerhed

Dansk Internet Forum (DIFO) skal indledningsvis takke for muligheden for at komme med bemærkninger til Forsvarsministeriets udkast til forslag om ændring af lov om Center for Cybersikkerhed, der blev sendt i høring den 8. januar 2019.

DIFO som administrator af .dk-domænenavne

DIFO, herunder dennes driftsselskab, DK Hostmaster, er af Erhvervsministeriet udpeget til at stå for registreringen af .dk-domænenavne med hjemmel i lov nr. 164 af 26. februar 2014 om internetdomæner (domæneloven) og dertil hørende bekendtgørelser. Der er pt. registreret cirka 730.000 brugere (registranter) af samlet set 1.300.000 .dk-domænenavne.

DIFO er som administrator af .dk-domænenavne samtidig operatør af en væsentlig tjeneste på domæneområdet og underlagt særregler om informationssikkerhed. Det følger af lov nr. 436 af 8. maj om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester. Loven er udstedt som led i implementeringen af EU's NIS-direktiv og er udmøntet i bekendtgørelse nr. 453 af 8. maj 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige tjenester på domæneområdet.

Bemærkninger til udkast til lovforslag

Som det fremgår af lovforslaget lægges der op til, at Center for Cybersikkerhed skal have udvidet sine beføjelser, herunder i forhold til virksomheder og myndigheder, der er tilsluttet netsikkerhedstjenestens monitorering. Formålet er at understøtte et højt informationssikkerhedsniveau i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af. Dette formål bakker DIFO op om i erkendelse af, at den cybertrussel, som Forsvarsministeriet beskriver, er reel og skal håndteres.

DIFO er imidlertid bekymret for, at lovforslagets beføjelser til Center for Cybersikkerhed kan få uhensigtsmæssige konsekvenser for de virksomheder, der på forskellig vis sikrer Danmark et robust internet, og at det dermed kan modarbejde et højt informationssikkerhedsniveau i det danske samfund.

DIFO har følgende bemærkninger til Forsvarsministeriets udkast til forslag om ændring af lov om Center for Cybersikkerhed:

1. Risiko forbundet med Center for Cybersikkerheds hardware og software

Proportionalitet

DIFO har noteret sig, at lovforslaget lægger op til, at Center for Cybersikkerhed skal kunne tilgå tilsluttede virksomheders og myndigheders data i bl.a. systemer, enheder og cloudservices ud over data i intern og ekstern kommunikation, som det er tilfældet i dag. Ligeledes vil Center for Cybersikkehed som noget nyt i særlige tilfælde kunne give påbud om tilslutning til bl.a. virksomheder, der har "særlig samfundsvigtig karakter", og dermed tvinge dem til at lade centeret få systemteknisk adgang til sine data. På den baggrund kan det konkluderes, at tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste vil få en markant mere indgribende karakter, og at der bliver mulighed for, at Center for Cybersikkerhed får adgang til alle oplysninger – også følsomme personoplysninger, medarbejderoplysninger, forretningshemmeligheder og fortrolige oplysninger i øvrigt.

Af den grund savner DIFO en præcisering i lovforslaget af, hvordan Center for Cybersikkerhed sikrer proportionalitet. Det anbefales, at centeret i samarbejde med en virksomhed, der skal tilsluttes, sørger for at der ikke sker unødig monitorering og kopiering af data, hvor risikoen for en sikkerhedshændelse er lav eller kan håndteres af virksomheden selv. Virksomheder, som beskæftiger sig med samfundsvigtig infrastruktur, er i dag typisk omfattet af lovkrav om sikring af informationssikkerhed, således fx både DIFO og de større udbydere af DNS-tjenester. DNS står for "Domain Name System" og omfatter virksomheder, der udbyder navneservere, hvilket er nødvendigt for, at et domænenavn virker.

Risiko ved fravalg af danske udbydere

Det skal dertil nævnes, at kunder "de facto" kan fravælge de ydelser, som udbydes af henholdsvis domæneadministrator, DNS-tjenesteudbydere og for den sags skyld også webhostingudbydere (der vedrører lagring af kunders hjemmesider på servere). Danske brugere kan således komme uden om Center for Cybersikkerheds monitorering mv. ved at vælge udenlandske udbydere. Det vil fx medføre, at brugere fravalgte .dk-domænenavne og i stedet gik over til et domænenavn med en anden landekode eller .com, .bank, .org mv.

Risiko for virksomhedens sikkerhed

Det skal endvidere bemærkes, at uanset opkrævning af et tilslutningsgebyr, kan der alligevel være legitime grunde til, at en virksomhed ikke anmoder om tilslutning. Eksempelvis er det sådan for DIFO's vedkommende, at der er reel risiko forbundet med at have ukendt hardware og software i vores netværk, som vi ikke styrer selv. DIFO er underlagt lovkrav om at være ISO27001-cerfiticeret; det indebærer bl.a., at DIFO skal have kontrol med, hvem der kan få adgang til data, som er lagret i vores systemer og enheder. En sådan kontrol vil blive udfordret ved, at Center for Cybersikkerhed med sin overvågning tager kopi af data løbende, herunder videregiver data til andre uden om DIFO.

Der kan også være legitime grunde til, at en virksomhed ikke kan indvillige i at være omfattet af det såkaldte aktive cyberforsvar, herunder lade Center for Cybersikkerhed installere hardware eller software i sine systemer og enheder til håndtering af en sikkerhedshændelse. Det vil være forbundet med risiko for fejl, der kan føre til, at it-systemer går ned eller beskadiges. DIFO er underlagt lovgivningskrav om at have en oppetid på minimum 99 procent på administrative systemer og 100 procent på domænenavneservertjenesten. Vi er således som virksomhed og som udbyder af domæneadministration meget sårbare over for systemnedbrud.

Samlet set anbefales, at der i lovforslaget skabes en reel mulighed for at fravælge tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste. Alternativt bør det

tydeliggøres i selve lovforslaget, hvilke kriterier der vil blive lagt til grund for en vurdering af, at en virksomhed er af *særlig* samfundsvigtig karakter og dermed kan blive påbudt tilslutning. Det bør være Folketinget, der sætter barren for denne form for tvang.

Det anbefales desuden, at det medtages i lovforslaget, at de tilslutningsvilkår, som en virksomhed ved evt. påbud eller efter tilslutningsaftale kan blive pålagt, ikke må medføre en reel forringelse af virksomhedens informationssikkerhedsniveau. En sådan forringelse vil jo i lyset af virksomhedens samfundsvigtige karakter være en risiko for informationssikkerheden i samfundet.

2. Center for Cybersikkerheds brug af domænenavne

DIFO har noteret sig, at Center for Cybersikkerhed vil kunne registrere domænenavne som led i at etablere såkaldte sinkholes. Dertil skal til Forsvarsministeriets orientering bemærkes, at DIFO's driftsselskab, DK Hostmaster, med hjemmel i domænelovens § 14, stk. 1 fastsætter forretningsbetingelser og vilkår for alle registranter af .dk-domænenavne. Disse vilkår forpligter alle, der registrerer et .dk-domænenavn, også Center for Cybersikkerhed. Det omfatter blandt andet krav om, at registranter registreres i DK Hostmasters WHOIS-database med navn, adresse og andre kontaktoplysninger, og at registranter skal gennemføre en identitetskontrol ved NemID, før et domænenavn kan bruges. DK Hostmaster har gennem det seneste år udført en indsats med skærpet identitetskontrol af alle registranter af .dk-domænenavne, hvilket har haft som konsekvens, at mere end 3.000 formodede online fupbutikker er blevet fjernet fra .dk-zonen. Det har i øvrigt haft den effekt, at politiet ikke længere har det samme behov for at få beslaglagt domænenavne i .dk-zonen.

DK Hostmasters vilkår indeholder ikke krav om brugspligt eller krav om, hvad domænenavne må bruges til. Der er dog krav om, at man ikke må bruge .dk-domænenavne uretmæssigt. Dette kan være i form af såkaldt typosquatting, åbenbar risiko for økonomisk kriminalitet, kompromittering af it-udstyr såsom phishing og malware-distribution mv., samt hvis et domænenavn anvendes i forbindelse med ulovlige handlinger eller undladelser, der krænker væsentlige sikkerhedsmæssige eller samfundsmæssige hensyn. DK Hostmaster kan i forbindelse med klage over sådan uretmæssig brug suspendere et .dk-domænenavn med henblik på sletning.

DIFO skal således anbefale, at Center for Cybersikkerhed er opmærksom på, at centeret som registrant er underlagt DK Hostmasters vilkår, men også at disse vilkår giver centeret en klageadgang ved en anden registrants uretmæssige brug af et domænenavn. Det bør sikres ved lov om nødvendigt, at Center for Cybersikkerhed kan rette en klage til DK Hostmaster og redegøre for, at et givent domænenavn bruges uretmæssigt på en af de ovenfor beskrevne måder. DIFO forventer, at det – i og med centeret har stor ekspertise inden for identifikation af sikkerhedshændelser, herunder cyberangreb – vil være en effektiv og betryggende måde at få belyst, hvordan et domænenavn anvendes i en konkret sikkerhedshændelse. På den baggerund kan DK Hostmaster suspendere domænenavnet og få inddæmmet sikkerhedshændelsen.

3. Edition af oplysninger om brugere af domænenavne

Lovforslaget introducerer en adgang for Center for Cybersikkerhed til edition, altså ved retskendelse at få udleveret oplysninger om brugere af bl.a. domænenavne. Det beskrevne setup kan ses som en formalisering af de muligheder, Center for Cybersikkerhed allerede i dag kan benytte sig af for at få udleveret oplysninger om registrerede .dk-domænenavne og dertil knyttede e-mailkonti hos DIFO.

I lyset af retssikkerhedsmæssige betragtninger er det imidlertid betryggende, at der sikres Center for Cybersikkerhed et generelt grundlag for at få udleveret oplysninger, som vil

kunne accepteres af alle udbydere af funktionalitet til internettet. Det skal i den forbindelse nævnes, at det under alle omstændigheder er en forudsætning, at Center for Cybersikkerhed sikrer, at en retskendelse retter sig mod en udbyder, der faktisk ligger inde med de ønskede oplysninger, og at det er muligt at afgrænse de oplysninger, der er brug for (proportionalitet).

Det anbefales, at lovforslaget bliver mere præcist i forhold til, hvilke udbydere der vil være underlagt editionsforpligtelsen. I det foreliggende lovforslag er der nævnt "teleudbyder", hvilket er uklart, al den stund at teleudbydere står for udbud af teletjenester, f.eks. telefoni; hvorimod en internetudbyder (også kaldet ISP'er) udbyder internet. Det kan også være relevant at nævne domæneadministratorer og deres forhandlere (registratorer), som jo typisk er dem, der ligger inde med brugeroplysninger om domæner. Webhostingvirksomheder er nævnt i lovforslaget, hvilket gør det usikkert, hvorvidt DNS-hostingudbydere (en anden betegnelse for udbydere af DNS-tjenester) er omfattet. Internettet understøttes af mange aktører og forskellige former for udbud af tjenesteydelser; og der er brug for i lovforslaget, at det fremstår mere præcist, hvem der er omfattet.

4. Videregivelse af data

Lovforslaget lægger op til en afgrænsning af, hvem Center for Cybersikkerhed kan få lov til at videregive trafikdata, pakkedata, stationære data og malware, som er indsamlet hos de tilsluttede virksomheder og myndigheder, til. En sådan afgrænsning er afgørende, og deling af data bør begrænses til det absolut nødvendige. Til gengæld mener DIFO, at loven i højere grad bør forpligte Center for Cybersikkerhed til at dele data med den konkrete virksomhed eller myndighed.

Lovforslaget indeholder således ikke nogen pligt for Center for Cybersikkerhed til at bistå de tilsluttede virksomheder og myndigheder med den viden, der konkret kommer ud af at lave dataanalyse på virksomhedens og myndighedens data. Center for Cybersikkerhed bør efter DIFO´s opfattelse være forpligtet til at dele viden fra dataanalysen med de tilsluttede virksomheder og myndigheder, som data stammer fra. Der er tale om data, som knytter sig til en sikkerhedshændelse eller sårbarhed hos disse virksomheder og myndigheder, og hvor der bør være en ret til, at netsikkerhedstjenestens analyse af data fra en virksomhed kommer virksomheden selv til gavn og direkte kan omsættes til risikominimerende tiltag. En hurtig tilbagemelding fra Center for Cybersikkerhed vil være af stor værdi. En sådan gensidighed i forpligtelsen til datadeling vil derudover lægge et fundament for opbygning af tillid til Center for Cybersikkerhed og en fælles opfattelse af, at et højt informationssikkerhedsniveau i det danske samfund er noget vi står sammen om.

DIFO og DK Hostmaster er af den opfattelse, at et sikkert og trygt internet er en forudsætning for digital vækst og velfærd. Derfor er informations- og cybersikkerhed også blandt vores højeste prioriteter, og vi står som administrator af .dk-domænet til enhver tid rådighed for dialog om at skabe et højt informationssikkerhedsniveau på Internettet.

Med venlig hilsen

Henrik Udsen
Bestyrelsesformand for DIFO og DK Hostmaster

Jakob Bring Truelsen
Direktør for DIFO og DK Hostmaster

Fra: Mikael Sjöberg <MikaelSjoeberg@OestreLandsret.dk>
Sendt: 6. februar 2019 09:03
Til: FMN-MYN-FORSVARSMINISTERIET; FMN-TBL Larsen, Tina Kathrine Berg; FMN-SBU Østergren, Stine Busch
Cc: Carina Marie Gjede Hansen; Ellen Busck Porsbo
Emne: høringssvar til Forsvarsministeriet (2018/0006599)

Kategorier: Tino

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

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Ved en mail af 7. januar 2019 har Forsvarsministeriet anmodet om eventuelle bemærkninger til høring over udkast til forslag om ændring af lov om Center for Cybersikkerhed (initiativer til styrkelse af Cybersikkerheden)(2018/006599).

Det fremgår af lovbemærkningerne , at lovforslaget er et led i udmøntningen af den nationale strategi for cyber- og informationssikkerhed, og at Forsvarsministeriet i den forbindelse har lagt afgørende vægt på, at lovgivningsinitiativerne udmøntes med den fornødne respekt for retssikkerheden og den personlige frihed. Initiativerne er målrettede og går efter udkastet ikke videre, end formålet tilsiger.

Udkastet til lovændring har været drøftet på et bestyrelsesmøde i Dommerforeningen.

En række af de indgreb, der kan foretages efter lovudkastet, vil – som det også fremgår i lovudkastets alm. del, pkt. 3.3.2 – utvivlsomt være omfattet Grundlovens § 72. Af samme grund indeholder udkastet udtrykkelig lovhjemmel til indgrebene for at imødekomme Grundlovens krav om, at indgreb kun kan ske efter retskendelse, medmindre lovgivningen "hjemler særegen undtagelse".

Den meget væsentlige afgrænsning mellem på den ene side § 72-indgreb, der foretages som følge af mistanke om et strafbart forhold, og som er omfattet af strafferetsplejen og dermed reguleret af retsplejelovens bestemmelser om forudgående – eller undtagelsesvis efterfølgende – dommerkendelse, og på den anden side andre indgreb, der ligeledes er omfattet af § 72, og som kan foretages uden retskendelse, hvis der er skabt lovhjemmel, beror på en konkret vurdering og kan i praksis være vanskelig at drage. Den endelige afgørelse af tvister herom henhører under domstolene. Grundlovens krav om forudgående dommerkendelse – medmindre særegen hjemmel findes i lovgivningen – må også ses i lyset af denne afgrænsningsproblematik, ligesom kravet om forudgående dommerkendelse helt grundlæggende tjener som et værn mod personforfølgelse og andre former for magtfordrejning.

Dommerforeningen forudsætter i den forbindelse, at måtte man via de af lovforslaget omfattede indgreb, som uden retskendelse giver adgang til trafikdata, pakkedata og nu tillige stationære data hidrørende fra pc'ere, smartphones, tablets og servere hos myndigheder og virksomheder, der er tilsluttet (herunder påtvunget tilsluttede), jf. lovudkastets forslag til § 4, komme i besiddelse af oplysninger, som rejser mistanke om et strafbart forhold, vil sådanne oplysninger ikke kunne anvendes, medmindre der forholdes i overensstemmelse med retsplejelovens straffeprocessuelle regler.

Dommerforeningen er bekendt med høringssvaret fra Københavns Byret, der er afgivet på byretspræsidenternes vegne. Dommerforeningen kan tilslutte sig bemærkningerne om, at bistand af en indgrebsadvokat i de situationer, der er omtalt i lovudkastets § 7, jf. § 7a er ufornøden.

Med venlig hilsen

Mikael Sjöberg
landsdommer/Formand for Den Danske Dommerforening
Direkte: + 45 99 68 65 01/ + 45 21 66 18 49

DR

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt pr. e-mail til fmn@fmn.dk
med kopi til tbl@fmn.dk og sbu@fmn.dk

DR Jura, Indkøb og
Rettigheder
Emil Holms Kanal 20
DK-0999 København C
T +45 3520 3040
www.dr.dk

Charlotte Gundersen
D +45 2854 3664
E cgun@dr.dk
Sagsnr.: 19/00207

1. februar 2019

Høringssvar vedr. udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed – ministeriets sagsnummer 2018/006599

DR er blevet bekendt med ovennævnte lovforslag og ønsker hermed at fremkomme med bemærkninger hertil, jf. Forsvarsministeriets høring af 7. januar 2019.

DR anerkender, at cybertruslen er øget markant igennem de seneste år, og at der i dag er en meget høj cybertrussel mod Danmark. DR er derfor også enig i behovet for at styrke mulighederne for at imødegå cyberangreb.

Der er imidlertid bestemmelser i lovforslaget, som er yderst problematiske for DR. Det er særligt lovforslagets § 3, stk. 4, hvorefter Center for Cybersikkerhed (CFCS) i særlige tilfælde kan påbyde virksomheder, regioner og kommuner, der har særligt samfundsvigtig karakter at blive tilsluttet netsikkerhedstjenesten.

Hverken selve lovbestemmelsen eller bemærkningerne til lovforslaget giver et klart svar på, hvem der kan blive udsat for et sådant påbud, ligesom udstrækningen heraf er uklar.

Det forhold, at hverken DR eller andre medier er medtaget på Forsvarets høringsliste, indikerer, at medievirksomheder ikke er omfattet. I bemærkningerne til lovforslagets enkelte bestemmelser nævnes imidlertid på side 51 medier og kommunikation som samfundsvigtige funktioner.

Det er magtpåliggende for DR, at CFCS ikke tillægges en mulighed for at kunne påbyde DR at skulle tilslutte sig netsikkerhedstjenesten, som er en del af Forsvarets Efterretningstjeneste. Det er derfor afgørende, at det klargøres, hvem et sådant påbud kan rettes mod, og at det tydeligt fremgår, at CFCS på intet tidspunkt kan påbyde DR og andre medievirksomheder, hvis hovedformål er at udgive massemedier omfattet af medieansvarslovens § 1, at blive tilsluttet netsikkerhedstjenesten.

Det skal i den forbindelse bemærkes, at det efter DR's opfattelse er problematisk, at Forsvarsministeriet i § 3, stk. 5, bemyndiges til at kunne fastsætte nærmere regler om disse påbud, og at denne mulighed i hvert fald ikke bør kunne anvendes til at fastsætte regler om, hvilke virksomheder og myndigheder, der anses at have en særligt samfundsvigtig karakter. Det bør være lovgiver, der beslutter, hvem der kan blive omfattet af en så indgribende foranstaltning.

Som bekendt indtager DR som Public Service station en særstilling i det danske samfund og har en afgørende rolle som offentlighedens kontrol- og informationsorgan. DR agerer som offentlighedens vagthund ved at afdække kritisable forhold i samfundet. Det er derfor helt afgørende, at DR er uafhængig af myndighederne og på ingen måde kan blive opfattet som politiets forlængede arm.

Det er derfor DR's vurdering, at det vil være særdeles problematisk for pressefriheden og kildebeskyttelsen, hvis CFCS efter lovændringen kan påbyde DR at tilslutte sig Netssikkerhedstjenesten.

Det vil medføre en risiko for, at DR's kilder udtørrer, idet færre kilder vil være villige til at samarbejde med og udtale sig til DR, hvis de frygter, at deres identitet efterfølgende risikerer at blive afsløret til myndighederne.

I sidste ende vil det endvidere kunne medføre, at DR ser sig nødsaget til ikke at videregive information til offentligheden på grund af risikoen for overvågning fra myndighederne. Dette vil således alvorligt knægte DR's ytringsfrihed og borgernes informationsfrihed, hvilket efter DR's opfattelse vil være i strid med artikel 10 i Den Europæiske Menneskerettighedskonvention.

I tillæg til ovennævnte vil DR endvidere bemærke, at der i lovudkastets kapitel 4 bør indsættes en reference til retsplejelovens §§ 169-172 om vidnefritagelse m.v. Det bør - ligesom det er tilfældet i kapitel 4 a om edition – tydeliggøres, at CFCS ikke kan behandle data fra virksomheder og myndigheder, hvis der derved vil fremkomme oplysninger om forhold, som ikke kan gøres til genstand for vidneforklaring i retten.

DR står naturligvis til rådighed, såfremt ovenstående giver anledning til spørgsmål eller der er behov for uddybning. I så fald kan der rettes henvendelse til Juridisk chefkonsulent Charlotte Gundersen på telefon 28543664 eller på e-mail cgun@dr.dk.

Med venlig hilsen

Maria Rørbye Rønn
Generaldirektør

ENERGINET
Myndighedsenheden

Energinet
Tonne Kjærsvej 65
DK-7000 Fredericia

+45 70 10 22 44
info@energinet.dk
CVR-nr. 28 98 06 71

Dato:
4. februar 2019

Forfatter:
MVF/SGL

NOTAT

HØRINGSSVAR TIL UDKAST TIL FORSLAG TIL LOV OM ÆNDRING AF LOV OM CENTER FOR CYBERSIKKERHED (INITIATIVER TIL STYRKELSE AF CYBERSIKKERHEDEN)

1. Indledning

Energinet takker for muligheden for at give bemærkninger til forslag til lov om ændring af lov om center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden), idet vi samtidig bemærker, at Energinet ikke fremgår af høringslisten som direkte høringspart.

Energinet har gennemgået forslag til *'lov om ændring af lov om center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden)'* med fokus på de emner, der har særlig betydning for Energinet, og har målrettet kommenteringen til disse.

Energinet anerkender, at det aldrig har været vigtigere at fortage vidensdeling indenfor området; herunder både erfaringsudveksling fra nationalt og international hændelser - samt udveksling af operationel viden (de såkaldte 'Indicators Of Compromise – IOC'er) på tværs af sektorerne, som har kritisk infrastruktur.

Det ses som et meget positivt tiltag at Center for Cybersikkerhed, nu også vil benytte sikkerhedsteknologier, såsom de nævnte Honeypots (3.5.3.1) og sink-hole (3.5.3.2) teknologier.

2. Energinets bemærkninger til lovforslag

2.1 Placering af udstyr

Energinet bemærker, at der hverken i lovforslaget (eller de tilhørende noter) tydeligt beskrives, hvor Center for Cybersikkerhed's udstyr/software bliver placeret hos myndigheden/virksomheden.

Rent teknisk kan udstyr placeres på tre former for netværk modeller:

1. Udstyr/software kan placeres på netværket imellem myndigheden/virksomheden og Internettet (et såkaldt DMZ netværk)

2. Udstyr/software kan placeres på det/de interne kontornetværk, ejet af myndigheden/virksomheden (de såkaldte IT netværk)

3. Udstyr/software kan placeres på det/de interne industri-/produktionsnetværk, ejet af myndigheden/virksomheden (de såkaldte Industrielle netværk)

Energinet er bekymrede, såfremt Center for Cybersikkerhed påtænker at kunne placere udstyr/software på det industrielle netværk. På dette netværk findes typisk industrielle enheder/system såsom f.eks. ICS (Industrial control systems, SCADA (Supervisory Control And Data Acquisition) PLC (Programmable Logic Controller) enheder – I Energisektoren styrer dette form for udstyr f.eks. den danske forsyning af El –og Gas.

2.2 Industrielle enheder er ikke som almindelige IT-enheder

Ovenstående industrielle enheder er opbygget på en særlig måde – og har en helt særlig profil, idet de som helhed styrer en række kritiske processer. Denne form for enheder er markant anderledes end traditionelle IT-systemer.

Det ses som problematisk, at det beskrives 3.9.2 at "*..løbende at scanne lokale enheder for tegn på cyberangreb*..", idet en sådan scanning af industrielt udstyr – på netværk, CPU eller RAM niveau - potentielt kan påvirke det industrielle udstyr negativt med efterfølgende risiko for, at udstyret ikke længere vil fungere efter hensigten.

2.3 Konfigurationsmetode- og ressourcebehov

Særligt problematisk, ses beskrivelsen af 3.3.3.1. Sikkerhedssoftwaren. I lovforslaget beskrives det, at denne kan benyttes i to former for konfiguration (hhv. passivt –og aktiv).

Uanset valg af konfigurationsmetode, er det Energinet's faglige vurdering, baseret på konkret produktviden – og erfaringsudveksling med samarbejdspartnere indenfor området, at der er en markant risiko for, – særligt i industrielle miljøer – at softwaren ikke har tilstrækkelig indsigt og forståelse af det normalt accepterede driftsmønster i et sådan produktionsmiljø – dette gælder både ved de typiske industrielle enheder (PLC/RTU m.v) samt de tilhørende servere og PC-arbejdsstationer, som understøtter det samlet produktions miljø.

Denne manglende indsigt vil derfor kunne påvirke f.eks. industrielle tidskritiske autonome drift processer – hvorved at den nævnte sikkerhed software kan negativt påvirke forsyningselementer – og derved potentielt i værste tilfælde kunne påvirke forsyningsevnen.

Selv ved implementering af den passive konfiguration, kræver det et meget stort forarbejde af et hold af specialister der besidder både IT-sikkerhed, Industriel sikkerhed samt Industriel proces baggrund at sikre en pålidelig implementering af et sådan sikkerheds software – Vi kan ikke læse i lovforslaget, hvordan dette er indtænkt – og hvorvidt at Center for Cybersikkerhed stiller mandskab og/eller afholder udgifterne til denne omfattende aktivitet, - dette er særligt relevant, såfremt myndigheden/virksomheden er blevet pålagt en sådan implementering for at blive tilsluttet netsikkerhedstjenesten.

2.4 Ingen internetforbindelse – 'By design'

Et typisk industrielt netværk, vil aldrig have en åben direkte forbindelse til Internettet. For at Center for Cybersikkerhed kan få nytte af udstyret –og de tilhørende log & event indsamlinger, vil det betyde at der rent netværksteknisk skal åbnes for en ekstraordinær adgang, fra netværket ud til Center for Cybersikkerhed, hvilket vil kunne reducere modstandsdygtigheden – og dermed cybersikkerheden for det nævnte netværk.

Vi forventer naturligvis ikke, at det er den tiltænkte effekt at reducerer cybersikkerheden hos myndigheden/virksomheden, men desværre kan vi ikke læse i materialet om hvordan Center for Cybersikkerhed konkret vil løse denne tekniske problemstilling.

2.5 Øget fokus på tilsyn

Som et led i indførslen af lovgivningen, så bliver det endnu vigtigere at sikre, et sikkert tilsynskoncept med CFCS. Der er en række anbefalinger i sidste tilsyn, hvor det bør sikres, at CFCS afhjælper disse anbefalinger samt at dette gøres indenfor en acceptabel deadline samt der sikres opfølgning herpå. Der bør ligeledes stilles krav (i lighed med Mikaels kommentar nedenfor) om periodisk sikkerhedstest af de ydelser, som CFCS leverer – herunder både hardware, software og ydelser.

2.6 Anbefalinger

Baseret på ovenstående bekymringer, vil Energinet anbefale, at det i lovforslaget ændres/tydeliggøres, at en virksomhed/myndighed ikke kan pålægges at skulle opstille Center for Cybersikkerhed's udstyr på netværk, såfremt der står industrielle enheder – alternativt at virksomhed/myndigheden kan fritages for pålæg, såfremt det via dialog sandsynliggøres, at en sådan implementering vil kunne påvirke samfundsvigtige funktioner, herunder forsyningsevnen hos myndigheden/virksomheden.

Vi vil anbefale, at det indføres i lovforslaget, at en virksomhed/myndighed, som frivilligt ønsker at deltage – for egen regning - må have lov til at sikkerhedsteste udstyret, før det går i produktion. Dette skal koordineres med Center for Cybersikkerhed og de tekniske resultater, samt eventuelle sårbarheder fra testen skal derefter deles med Center for Cybersikkerhed, såfremt Center for Cybersikkerhed ønsker dette. Et sådan tiltag ligger i tråd med almindelig praksis.

FAGBEVÆGELSENS HOVEDORGANISATION

Islands Brygge 32D
2300 København S

Tlf. 3524 6000
Mail: FH@fho.dk

Forsvarsministeriet

fmn@fmn.dk
cc:
tbl@fmn.dk og sbu@fmn.dk

Sagsnr. 19-0588
Vores ref. AGV/M
Deres ref. 2018/006599

Den 4. februar 2019

Høringssvar – sagsnr. 2018/006599 - Høring over udkast til lovforslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden)

FH har modtaget Forsvarsministeriets høring over udkast til lovforslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden).

Af høringen fremgår, at lovforslaget er et led i udmøntningen af den nationale strategi for cyber- og informationssikkerhed.

I lovforslaget foreslås det, at der efter § 6 i den gældende lov om Center for Cybersikkerhed indsættes følgende:

"**§ 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 offentlig tilgængelige data om myndigheden eller virksomheden og dennes medarbejdere, og

3) iværksætte forebyggelsesaktiviteter rettet imod udvalgte medarbejdere eller enheder i myndigheden eller virksomheden."

Af bemærkningerne til lovforslaget fremgår det, at Center for Cybersikkerhed efter det foreslåede § 6a, stk. 2, nr. 3 efter anmodning fra myndigheden eller virksomheden vil kunne iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejder eller enheder i myndigheden eller virksomheden. De i bemærkningerne nærmere beskrevne forebyggelsesaktiviteter i form af fx såkaldt spear phishing, er omfattet af aftalerne om

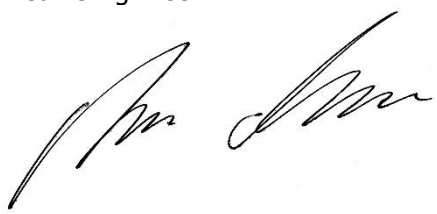
kontrolforanstaltninger på det statslige, regionale og kommunale område (Cirkulære om aftale om kontrolforanstaltninger, CIR nr. 9588 af 01/11/2010, Aftale om kontrolforanstaltninger indgået mellem RLTN og Forhandlingsfællesskabet, samt Aftale om kontrolforanstaltninger indgået mellem KL og Forhandlingsfællesskabet).

FH retter opmærksomheden på § 4, stk. 1, som er enslydende i cirkulæret/aftalerne, om information til de ansatte 6 uger forud for iværksættelse af nye kontrolforanstaltninger samt cirkulæret/aftalernes § 4, stk. 3, ligeledes enslydende i cirkulæret/aftalerne, hvoraf det fremgår:

"Hvis formålet med kontrolforanstaltningen vil forspildes ved en forudgående information, eller tvingende driftsmæssige grunde er til hinder herfor, skal kommunen informere de ansatte snarest muligt efter iværksættelsen af kontrolforanstaltningen samt redegøre for årsagen til, at der ikke kunne ske en forudgående information."

En tilsvarende aftale om kontrolforanstaltninger indeholdende informationspligt er gældende på det private område, jf. den af DA og LO indgåede aftale om kontrolforanstaltninger af 27. oktober 2006.

Med venlig hilsen



Arne Grevsen

Forsvarsministeriet
fmn@fmn.dk
tbl@fmn.dk
sbu@fmn.dk

Henvisning til sagsnummer 2018/006599.

FINANS DANMARK

Styrkelse af Center for Cybersikkerheds mulighed for at forsvare Danmark samtidig med, at virksomhedernes retssikkerhed sikres

Høringssvar

4. februar 2019

Dok. nr. FIDA-151247800-646019-v1
Kontakt Mette Stürup

Resumé

Danmark er et af verdens mest digitaliserede lande. Det gør os så mere sårbare over for digitale angreb. Det er væsentligt at sikre, at der er adgang til samfundskritiske tjenester som strøm, internet og finansielle tjenester. Finans Danmark mener, at der er behov for at styrke Danmarks cybersikkerhed. Der er en reel risiko for cyberangreb og for at blive hacket.

Et led i dette er, at Center for Cybersikkerhed har de rette værktøjer til at bekæmpe det stigende antal cyberangreb med. Vi støtter derfor lovforslagets intentioner. Men vi finder de brede og uprøcise hjemmeler betænkelige. Herunder giver det især anledning til bekymring, at er mulighed for at der skal gives adgang til alle virksomheders trafik uden retskendelse. Når dette så kombineres med muligheden for at pålægge en virksomhed at tilslutte sig centerets sensornetværk, kan det blive problematisk. Vi foreslår, at tilslutning sker ad frivillighedens vej og i fælles dialog.

Endelig finder vi det væsentligt, at der sker en øget videndeling, og vi opfordrer til, at der sker en endnu tættere dialog på operativ dialog med især de samfundskritiske sektorer. Vi ser gerne denne videndelingsforpligtigelse stærkere understreget i lovforslaget.

Finans Danmarks bemærkninger til lovforslag om ændring af Lov om Center for Cybersikkerhed

Høringssvar

4. februar 2019
Dok. nr. FIDA-151247800-646019-v1

Generelle bemærkninger

Danmark er et af verdens mest digitaliserede lande. Det gør os så mere sårbare over for digitale angreb. Det er væsentligt at sikre, at der er adgang til samfundskritiske tjenester som strøm, internet og finansielle tjenester. Finans Danmark mener, at der er behov for at styrke Danmarks cybersikkerhed. Der er en reel risiko for cyberangreb og for at blive hacket.

Et led i dette er, at Center for Cybersikkerhed har et tilstrækkeligt overblik i forhold til aktuelle trusler og de rette værktøjer til at bekæmpe det stigende antal cyberangreb med. Vi støtter derfor generelt set lovforslagets intentioner. Imidlertid finder vi det betænkeligt, at der påtænkes udstukket vide rammer i forhold til at kunne kræve bestemte sikkerhedskomponenter installeret hos bestemte myndigheder/virksomheder.

Finans Danmark og Cybersikkerhed

Finans Danmarks og vores medlemmer er særdeles optaget af cyber- og informationssikkerhed. Det er en topprioritet for sektoren, og vi har i de seneste år taget en lang række initiativer for at forbedre cyber- og informationssikkerheden i sektoren, blandt andet med etablering af NFCERT (Nordic Financial CERT) og FSOR (Finansielt Sektorforum for Operationel Robusthed). I sidstnævnte gennemfører sektoren bl.a. en meget omfattende red team test i de kommende år baseret på TIBER-DK rammeværket.

Derudover deltager Finans Danmark og Finans Danmarks medlemmer i en række offentlige aktiviteter og samarbejder om netop cybersikkerhed. Det drejer sig om fx Det Strategiske Samarbejdsforum i regi af Center for Cybersikkerhed og regeringens advisory board for den Nationale Cyber- og informationssikkerhedsstrategi. Vi deltager også i følgende samarbejder i regi af Erhvervsministeriet: Virksomhedsrådet for IT-sikkerhed og Erhvervspartnerskabet for øget it-sikkerhed i dansk erhvervsliv.

Finans Danmark har bidraget til og er positive over for de nye sektorstrategier for styrkelse af cyberrobustheden i energi-, tele-, søfart-, finans-, transport- og sundhedssektoren, der alle blev præsenteret primo januar 2019. Vi forventer, at disse strategier vil bidrage til at skabe et robust fundament for et øget og nødvendigt

samarbejde mellem offentlige og private parter, så vi i fællesskab kan styrke cyberrobustheden i Danmark i de kommende år. Det er vigtigt, at Center for Cybersikkerhed har de fornødne beføjelser for derved at kunne løfte sit ansvar i denne forbindelse.

Specifikke kommentarer til lovforslaget:

Pålæg om tilslutning til sensornetværket

Finans Danmark finder det betænkeligt, at der påtænkes udstukket vide rammer i forhold til at kunne kræve bestemte sikkerhedskomponenter installeret hos udvalgte myndigheder/virksomheder. Dette kan i sig selv udgøre en ny sikkerhedsmæssig risiko.

Herunder kan der være grund til at bekymre sig over den brede hjemmel, der giver adgang til virksomhedernes data uden retskendelse. Når dette så kombineres med muligheden for at pålægge en virksomhed at tilslutte sig centerets sensornetværk, kan det blive problematisk. Vi foreslår, at tilslutning sker ad frivillighedens vej og i fælles dialog.

Det er ikke helt klart, hvem denne bestemmelse i loven retter sig imod, da den ikke indeholder en nærmere definition af, hvem som kan blive pålagt et påbud om tilslutning.

Lovforslaget forholder sig ikke til de komplikationer, der kan opstå, såfremt sensornetværk påvirker eksempelvis den tilsluttede virksomheds it-driftsstabilitet. Leverer Center for Cybersikkerhed 24x7x365 support, hvis problemer opstår? Hvis er skylden, hvis virksomheden pga. sensornetværket får en forhøjet nedetid af virksomhedens it-systemer?

Endvidere skal det bemærkes, at der i disse år finder en hård konkurrence sted i forhold til, hvor nye tech-virksomheder etablerer sig. Dette gælder også inden for finansiel teknologi, hvor Danmark har oplevet en positiv og markant vækst inden for fintechvirksomheder. Der er en risiko for, at lovforslagets mulighed for at pålægge virksomheder at implementere sensornettet kan få en negativ indvirkning på Danmarks muligheder for fortsat at tiltrække investorer og virksomheder.

Karakteren og placeringen af sensorerne kan også have stor betydning for virksomhederne, og derfor bør installation være med passive elementer og udelukkende ske på ydersiden hos virksomhederne. Hvis tilslutningen skal have værdi for virksomheden. Er det er væsentligt, at der altid sker notificering hos dem, der er

tilsluttet sensornetværket, når Center for Cybersikkerhed identificerer en kritisk hændelse.

Virksomhederne bør derfor selv have læseadgang og adgang til at oprette regler. Virksomhederne bør også have adgang til de logs, som dannes på Center for Cybersikkerhed's enheder. Center for Cybersikkerhed må gerne begrænse adgang til specifikke regler på sensorerne, hvis denne visen ikke kan deles af hensyn til samarbejde med andre efterretningstjenester.

Selve tilslutningen til sensornetværket gøres fremadrettet gratis, men lovforslaget forholder sig ikke til, at en tilslutning kan medføre omkostninger vedr. fx dekryptering af data, væsentlig kompleks systemarkitektur etc. Dette kan også medføre udgifter for de tilsluttede virksomheder, hvis der ikke direkte kan gives adgang til ukrypteret netværkstrafik

Samlet set mener Finans Danmark derfor, at påbud ikke bør være en del af lovforslaget.

Aktivt Cyberforsvar

Indgriben/behandling ved begrundet mistanke bør altid foretages proportionalt med risikoen, herunder skal den indgribende handling vurderes i forhold til virksomhedens samlede aktiviteter og samfundsmæssige funktion. Vi henstiller til agtpågivenhed og særligt at oplyse om alle handlinger med evt. indgriben, der indebærer eks. nedlukning af systemer/services, blokeringer af datastrømme eller sletning af data.

Vi kan ikke acceptere ændringer, der kan have en negativ forretningsmæssig konsekvens i forhold til vores services uden at have mulighed for indsigelse eller selv foretage en risikovurdering forud for sådanne handlinger. Derudover kommer, at der er en risiko for "falske positiver".

Vi finder, at berørte virksomheder har et krav på at modtage rettidig information om alvorligheden og det potentielle omfang af en vurderet sikkerhedshændelse, herunder eventuel behandling af netværket. Dels for at kunne etablere egne forsvarsforanstaltninger på det præventive, opdagende og korrigerende plan, dels for at være oplyst om eventuelle direkte og afledte forretningsmæssige risici, som virksomheden skal tage højde for i den fortsatte daglige drift.

Ved konstaterede sikkerhedshændelser, hvor netsikkerhedstjenesten beslutter at forhindre levering af disse data til virksomheden, skal sådanne beslutninger ligele-

des ske under hensyntagen/overvejelser af konsekvenser for virksomhedens fortsatte drift. Vi mener, at netsikkerhedstjenesten kan have disse beføjelser i de situationer, hvor den nationale sikkerhed er truet eller er påvirket særlig negativt, men henstiller til, at det skal foregå under ordnede forhold og i høj kvalitet i udførelsen, hvor hensynet til konsekvensen for de berørte virksomheder er i højsædet.

Behov for øget videndeling mellem offentlige myndigheder og private virksomheder

I forbindelse med lovforslaget finder vi det væsentligt, at der er fokus på en øget videndeling, og vi opfordrer til, at der sker en endnu tættere dialog på et operationelt niveau mellem de samfundskritiske sektorer, herunder mellem de kommende sektor-"CERT'er". I forbindelse med lovforslaget finder vi det væsentligt, at der er fokus på øget videndeling, og vi opfordrer til, at der sker en endnu tættere dialog på et operationelt niveau mellem de samfundskritiske sektorer, herunder mellem de kommende sektor-CERT'er. Vi ser gerne denne videndelingsforpligtigelse stærkere understreget i lovforslaget.

Pakkedata

Bestemmelsen i forhold til Center for Cybersikkerheds adgang til at videregive data, jf. § 16, stk. 2, synes at være meget bred. Det bør præciseres under hvilke forhold og til hvem?

Forholdet til lov om finansiel virksomhed

Bankerne er underlagt regler om bankhemmelighed både i Danmark men også i udlandet. Der savnes en nærmere redegørelse for, hvordan disse regler spiller sammen med, at Forsvarets Efterretningstjeneste ønsker adgang til al kommunikation i finanssektoren. Der savnes en beskrivelse (eller en lempelse) af forholdet til særlovgivningens (FIL's) fortroligheds- eller tavshedspligtsbestemmelser.

En række finansielle institutter og virksomheder behandler også data for ikke-danske kunder. Her skal man også overholde udenlandske regler og kan være underlagt udenlandske tilsynsmyndigheder. Vi efterlyser, at lovforslaget forholder sig til denne problemstillling, der formentlig også gælder for andre sektorer.

Tilslutning til Center for Cybersikkerhed kan ske ved, at man tilslutter sig ordningen, og det kan ske ved, at Center for Cybersikkerhed påbyder en virksomhed at tilslutte sig. Hvis tilslutningen sker som følge af et påbud, kan det hævdes, at enhver efterfølgende videregivelse af oplysninger fra banken til Center for Cybersikkerhed er berettiget, da den følger af lov, jfr. FIL § 117. Hvis tilslutningen sker frivilligt, kan videregivelse af oplysninger næppe ske med henvisning til FIL § 117

(berettiget videregivelse), og det kunne være ønskværdigt, at lovforslaget forholder sig FIL § 117 og muligheden for at videregive oplysninger.

De finansielle outsourcingregler

Ad § 15: Hvilke kontroller er der etableret i forhold til at sikre Center for Cybersikkerhed's adgang til virksomhedens kommunikation og data, som centret opnår gennem sensornetværket ? Kan de tilsluttede virksomheder opnå en tilstrækkelig indsigt i Forsvarets Efterretningstjeneste's kontroller, fx gennem tilsynet med Center for Cybersikkerhed? Dette er et formelt krav i Outsourcingbekendtgørelsen, som gælder for finansielle institutioner i forhold til anvendte (kritiske) underleverandører.

Forholdet til de fire essentielle europæiske garantier i forhold til GPDR

De almindelige bemærkninger indeholder en analyse af forholdet til den Europæiske Menneskerettighedskonvention (EMRK), men ikke en specifik analyse af forholdet til de fire essentielle europæiske garantier.

Fra Finans Danmarks side ser vi gerne, at lovforslaget udbygges med en analyse af forholdet til de fire essentielle europæiske garantier, som de europæiske datatilsyn har beskrevet i *"Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (WP 237)"*.

De fire essentielle europæiske garantier har følgende indhold:

1. Myndigheder i tredjelandes adgang til og brug af personoplysninger hidrørende fra EU skal ske på grundlag af klare, præcise og tilgængelige regler.
2. Myndigheder i tredjelandes adgang til og brug af personoplysninger hidrørende fra EU skal være nødvendig og proportional, der skal være balance mellem formålet (national sikkerhed) og indgrebet i de registreredes ret til beskyttelse af deres privatliv.
3. Der skal være en uafhængig og effektiv tilsynsmyndighed i tredjelandet.
4. Der skal være tilgængelige og effektive retsmidler for de registrerede i tredjelandet.

I dag påkalder de fire essentielle europæiske garantier sig især opmærksomhed, når personoplysninger om europæiske registrerede overføres fra EU til tredjelande uden for EU.

På længere sigt har EU-kommissionen imidlertid bebudet, at man vil kigge nærmere på, hvorvidt EU's medlemslande også selv overholder de fire essentielle garantier, og hvordan – i det omfang dette ikke er tilfældet – det sikres, at garantierne overholdes inden for EU's grænser.

Lovforslaget indebærer, at Center for Cybersikkerhed fremadrettet vil få mulighed for i større omfang end hidtil at indsamle personoplysninger af hensyn til national sikkerhed. I dét lys henstiller Finans Danmark til, at lovgiver forholder sig til, om forslaget i sin nuværende udformning sikrer tilstrækkelige garantier for de registrerede, når deres personoplysninger overføres til Danmark.

Specifikke bemærkninger

Er § 8 a omfattet af offentlig aktindsigt?

Med venlig hilsen

Mette Stürup

Direkte: +4527152020
Mail: ms@fida.dk

FA FINANSSEKTORENS ARBEJDSGIVERFORENING

Forsvarsministeriet
Att. Chefkonsulent Stine Østergren

Sendt pr. e-mail til fmn@fmn.dk
Sendt cc til tbl@fmn.dk og sbu@fmn.dk

Den 6. februar 2019

DOK. NR.:
FAID-
873754581-
64921

Forsvarsministeriets forslag til lov om ændring af lov om Center for Cybersikkerhed – sagsnr. 2018/006599
(initiativer til styrkelse af cybersikkerheden)

FA takker for høringen om Forsvarsministeriets forslag til lov om ændring af lov om Center for Cybersikkerhed (initiativer til styrkelse af cybersikkerheden), og for den givne fristforlængelse for vores høringssvar.

FA deler opfattelsen af, at det er nødvendigt at sikre og styrke cybersikkerheden i Danmark, og FA støtter også lovforslagets intentioner. Virksomhederne i finanssektoren bruger allerede i dag mange ressourcer på cybersikkerhed og beskyttelse af borgernes personoplysninger. Lovforslaget giver dog FA anledning til at udtrykke bekymring for rækkevidden af dele af forslaget, idet de fremstår meget bredt og upræcist formuleret.

Indgreb i meddelelseshemmeligheden er grundlæggende betænkeligt og bør kun finde sted i meget begrænset omfang, når det er proportionalt og nødvendigt af hensyn til tungtvejende hensyn. FA er også bekymret for, om der med forslaget gives adgang til overvågning af virksomheders datatrafik i sager, der ikke berører cybersikkerheden. Der bør tilsikres større beskyttelse af medarbejdernes retssikkerhed, og centeret bør pålægges at overveje, om målet med indgreb kan nås med mindre indgribende foranstaltninger.

Det er også vigtigt at sikre, at de tiltag, centeret gennemfører i virksomhederne, ikke skader virksomhedernes egne foranstaltninger til sikring af datasikkerheden.

Forslagets formulering af § 5 indebærer en vidtgående adgang til data uden retskendelse, kombineret med, at virksomheder kan blive pålagt at deltage i Center for Cybersikkerheds sensornetværk. Formuleringen af denne bestemmelse er upræcis i forhold til, hvilke situationer der er omfattet, hvilke data der gives adgang til, samt hvilket formål der konkret skal opnås.

Det forekommer meget bredt, at centeret bemyndiges til disse indgreb på grundlag af en vurdering af, at behandlingen "kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet". Bestemmelsen giver adgang til data uden retskendelse, hvis en virksomhed, der ikke er med i sensornetværket, beder om det. Er der behov for at give hjemmel i loven til

denne adgang til data uden retskendelse, når virksomheden selv har bedt centeret om bistand?

FA er særligt bekymret for rækkevidden af forslagets § 6a, der, for at gøre det muligt at rådgive om forebyggelse, giver centeret ret til at iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejdere i virksomheden, dog på virksomhedens anmodning. Bestemmelsen kan indebære, at udvalgte medarbejdere bringes til at overtræde virksomhedens sikkerhedsforanstaltninger, hvilket kan få ansættelsesretlige konsekvenser. Dermed kan bestemmelsen også forårsage uro på arbejdspladsen, til skade for virksomheden og medarbejderne. FA savner en nærmere persondataretlig analyse af, at medarbejdernes personoplysninger behandles, uden at der er indhentet samtykke fra medarbejderne. Hvilket behandlingsgrundlag i de persondataretlige regler støttes behandlingen på?

I forhold til forslagets bestemmelser om videregivelse af oplysninger fra virksomheder til centeret, foreslår FA at Finanstilsynet høres specifikt om, hvorvidt en videregivelse af oplysninger fra finansielle virksomheder er berettiget efter den finansielle lovgivning, både i situationer, hvor virksomheden selv anmoder om centerets bistand, og hvor centeret påbyder det.

FA savner herudover en nærmere analyse af, om forslaget åbner for videregivelse af oplysninger til tredjelande, og FA gør i den forbindelse opmærksom på de europæiske garantier for grundlæggende rettigheder i forhold til persondatasikkerhed, jf. det europæiske datatilsyns WP 237, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and dataprotection through surveillance measures when transferring personal data.

FA henholder sig i øvrigt til høringssvarene fra Forsikring & Pension og fra Finans Danmark. FA har ikke yderligere bemærkninger til forslaget.

Med venlig hilsen

Merete Preisler
Underdirektør, advokat (H)
mep@fanet.dk

Telefon: +45 3391 4700
Direkte: +45 3338 1613

Forsvarsministeriet

Sendt e-mail til fmn@fmn.dk
c.c. tbl@fmn.dk og sbu@fmn.dk

Forsikring & Pension

Lov om ændring af lov om Center for Cybersikkerhed - høringssvar - deres sagsnummer 2018/006599

30.01.2019

Forsikring & Pension
Philip Heymans Allé 1
2900 Hellerup
Tlf.: 41 91 91 91
Fax: 41 91 91 92
fp@forsikringogpension.dk
www.forsikringogpension.dk

Henriette Günther Sørensen
Chefkonsulent
Dir. 41 91 91 74
hgs@forsikringogpension.dk

Sagsnr. GES-2019-00024
DokID 376113

Forsikring & Pension (F&P) værdsætter muligheden for at komme med bemærkninger til lovforslaget om ændring af lov om Center for Cybersikkerhed.

Der er stor opbakning fra F&P til en mere fokuseret indsats, der bidrager til at understøtte et højt informationssikkerhedsniveau i samfundet og til de overordnede tanker om, at Center for Cybersikkerhed (CFCS) får et bedre datagrundlag til forebyggelse og bekæmpelse af cyberangreb i Danmark. Særligt forslaget om mulighed for at kunne foretage forebyggende sikkerhedstekniske undersøgelser og at kunne foretage anvendelse og påvirkning af angrebsmål og angrebsinfrastruktur vil få stor betydning i det forebyggende arbejde. Det arbejde deltager forsikrings- og pensionsbranchen gerne i og støtter den ambitiøse nationale dagsorden om at beskytte samfundsvigtige funktioner og kritisk digital infrastruktur.

Forsikrings- og pensionsbranchen bruger i dag mange ressourcer på at følge cyber-risikobilledet og beskytte borgernes personoplysninger. Derfor hilser branchen det også velkomment, at det offentlige styrker Danmarks samlede robusthed i forhold til cybersikkerhed gennem aktivt og frivilligt samarbejde mellem offentlige virksomheder og private samfundsvigtige virksomheder. Det vil styrke Danmarks samlede robusthed.

F&P finder dog, at lovforslaget i sin nuværende form er alt for vidtgående. Lovforslaget giver meget vidtgående rammer for CFCS' adgang til virksomheders data uden retskendelse. Samtidig med at der åbnes for adgang til, at CFCS kan påbyde virksomheder at blive tilsluttet CFCS - hvis det har samfundsvigtig karakter – uden at der foreligger en nærmere definition af samfundsvigtig. Videre skal det bemærkes, at branchen finder det problematisk, at CFCS vil have mulighed for at tilgå ikke alene danske data uden en retskendelse men også udenlandske data. I de tilfælde, det er en finansiel koncern, vil CFCS derved få en videre adgang end tiltænkt i lovforslaget. Det er problematisk, at der ikke er taget stilling til denne udfordring, herunder om der vil være en udfordring i relation til persondataforordningen, at CFCS vil kunne tilgå andre EU borgeres persondata.

Forslaget er bekymrende i forhold til borgernes grundlæggende rettigheder og frihedsrettigheder. Indgreb i borgernes grundlovsikrede rettigheder bør kun forekomme, hvis der er en væsentlig trussel, og det sker under iagttagelse af proportionalitetsprincippet. Det er F&P's vurdering, at lovforslaget i sin nuværende form ikke imødekommer ovenstående.

Sektorstrategierne

Der er allerede med de seks sektorstrategier taget hul på at igangsætte initiativer, der sikrer, understøtter og ruster samfundet mod cyberangreb. Initiativerne i sektorstrategierne igangsætter målrettede indsatser for de enkelte sektorer, ligesom CFCS har en central rolle i forhold til at sikre de rette tværgående indsatser for de seks kritiske sektorer. I delstrategien for den finansielle sektor lægges der op til, at Finansielt Sektorforum for Operationel Robusthed (FSOR) fortsat bliver et vigtig fora til at skabe overblik over operationelle risici på tværs af sektoren, sikre gennemførelse af fælles tiltag ift., at skabe robusthed overfor cyberangreb og endelig skabe rammer for samarbejde og vidensdeling. Der er også lagt op til at udvide samarbejdet med den Nordiske finansielle CERT (NFCERT), så alle større finansielle virksomheder, herunder forsikrings- og pensionsselskaber bliver en del af disse fora. Det er derfor vigtigt, at disse eksisterende og velfungerende fora ikke undermineres af den nye lovgivning, men i stedet indtænkes. CFCS deltager på lige fod med de finansielle virksomheder allerede i disse fora.

Det er F&P's anbefaling, at Forsvarsministeriet bør afvente og vurdere effekten af de initiativer, der netop er igangsat, førend der gribes til en grundlæggende og vidtrækkende ændring af lovgivningen, der giver CFCS ubegrænset adgang til data fra regioner, kommuner og virksomheder, hvis dette tilbydes eller påbydes.

En indsats i den finansielle sektorstrategi går på, at viden skal udnyttes til at bekæmpe it-sikkerhedstrusler effektivt. Her vil man styrke indberetning af hændelser for at forbedre vidensgrundlaget. Det kan være en anden måde at dele data med CFCS og herigennem se på, hvordan der kan ske en hurtigere, bedre og om muligt realtime deling af data om cyberhændelser.

Retssikkerhed og proportionalitetsprincippet

Det er et grundlæggende princip i et retssamfund som Danmark, at indgreb i grundlovssikrede rettigheder – her meddelelseshemmeligheden – både er 1; nødvendigt, 2; at der er særligt tungtvejende hensyn til fx statens sikkerhed, som kan begrunde indgrebet, og 3; at der er proportionalitet mellem mål og middel (proportionalitetsprincippet).

En anden konsekvens af lovforslaget er, at indgrebet i meddelelseshemmeligheden medfører videregivelse og behandling af store mængder personoplysninger. Her bør der også foretages en afvejning af, om målet kan nås med mindre indgribende metoder end totalovervågning af alle en virksomheds data.

Der lægges op til, at CFCS kan behandle en virksomheds data uden retskendelse men efter frivillig "aftale". I særlige tilfælde kan en virksomhed også blive pålagt tilslutning, hvorefter CFCS kan få adgang til alle virksomhedens data uden retskendelse.

Det grundlæggende kriterium om, at indgrebet skal kunne bruges til at understøtte "et højt informationssikkerhedsniveau" i samfundet er for upræcist defineret i lovforslagets bemærkninger og efterlader et meget vidt skøn hos CFCS. Det bør defineres fuldstændigt klart og præcist i lovforslaget, hvad der skal til for at udløse CFCS' beføjelser.

Det er særligt vigtigt, at man overholder de grundlæggende retsprincipper i de situationer, hvor centeret har beføjelse til i *§ 3, stk. 4*, at udpege virksomheder af særlig samfundsvigtig karakter, der skal tilsluttes netsikkerhedstjenesten. F&P opfordrer til, at det præciseres i bemærkningerne, hvad definitionen "samfundsvigtig" indebærer, og at det tydeliggøres, at proportionalitetsprincippet skal indgå i vurderingen af, hvornår det er nødvendigt at udstede påbud om tilslutning.

Lovforslaget indeholder heller ikke nogen nærmere ramme for indgrebets omfang, som sikrer, at CFCS anvender mindre indgribende midler end en totalovervågning af virksomhedens data. F&P opfordrer derfor til, at der i lovforslaget pålægges CFCS en forpligtelse til at undersøge, om målet kan nås på en mindre indgribende måde end ved at overvåge alle virksomhedens data.

F&P finder endvidere, at de rammer, der opsættes i den foreslåede § 15 for behandling af data erhvervet ved indgreb i meddelelseshemmeligheden, er alt for vide og upræcist definerede. P.t. står der blot, at manuel analyse kan foretages, når det vurderes at være "nødvendigt". Det bør klart beskrives i bemærkningerne, hvornår det er nødvendigt at foretage manuelle analyser af data.

Retsikkerheden og behandling af personoplysninger

Selvom det primære formål er overvågning af datatrafikken og ikke overvågning af enkeltpersoner, finder F&P det særdeles vidtgående, at der som led i overvågningen vil ske behandling af store mængder personoplysninger uden forudgående retskendelse og uden, at de almindelige retssikkerhedsmæssige garantier i fx retssikkerhedsloven overholdes.

Forsikrings- og pensionsbranchen er i sagens natur en branche, der lever af at behandle personoplysninger herunder mange følsomme oplysninger. En generel overvågning, som inkluderer alle data om en forsikringsvirksomheds kunder, er derfor meget vidtgående. For eksempel kan det nævnes, at et selskab som PFA har 1,2 mio. kunder.

F&P mener derfor, at CFCS ikke bør få mulighed for at kunne påbyde forsikrings- og pensionsselskaber at blive tilsluttet netsikkerhedstjenesten.

Specifikke bemærkninger

Nedenfor listes en række særlige opmærksomhedspunkter og specifikke bemærkninger.

1. Frivillighed

Al anvendelse i den private sektor af netsikkerhedstjenesten bør i øvrigt ske frivilligt og med fuld gennemsigtighed for de deltagende virksomheder. Således bør den enkelte virksomhed have underretning og rapportering i alle tilfælde, hvor der foreligger mistanke om, eller er sket fuldbyrdet cyberangreb, mod virksomheden. Virksomheden skal ligeledes have mulighed for at tilkoble netsikkerhedstjenesten til sit eget SIEM-system, for bl.a. selv at kunne kontrollere, hvilke data

der oversendes til netsikkerhedstjenesten. Endelig skal den enkelte virksomhed kunne frakoble netsikkerhedstjenesten umiddelbart, hvis den finder tjenesten uhensigtsmæssig.

2. Formål

Det bør være et ultimativt krav, at hverken Forsvarets Efterretningstjeneste eller Politiets Efterretningstjeneste skal kunne gøre brug af netsikkerhedstjenesten i deres efterretningsmæssige virke således forstået, at ingen af de to tjenester kan benytte netsikkerhedstjenesten til at overvåge eller på anden vis indhente oplysninger om en af dem i anden sammenhæng mistænkt virksomhed.

3. De finansielle videregivelsesregler

Hvor der sker videregivelse af data fra finansielle virksomheder, vil disse endvidere være underlagt Lov om Finansiel virksomhed kap. 9.

F&P opfordrer Forsvarsministeriet til at indhente en udtalelse fra Finanstilsynet om, hvorvidt tilsynet anser en videregivelse af oplysninger fra forsikrings- og pensionsselskaber for berettiget – både i situationen, hvor tilslutning til netsikkerhedstjenesten sker på frivillig basis og i situationen, hvor tilslutning sker efter konkret påbud.

4. Reguleringen bør præciseres – i særdeleshed på nedenstående punkter:

4.1. Jf. § 3 stk. 5 kan Forsvarsministeren fastsætte reglerne om påbud, uden at disse er nærmere defineret

4.2 Jf. § 5 kan netsikkerhedstjenesten uden retskendelse behandle data fra en virksomhed, som ikke er tilsluttet (hvis det vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet), uden at dette er nærmere præciseret

5. Tilsyn

Den tilhørende kontrolmyndighed bør føre periodiske tilsyn med, at sikkerhedsniveauet hos Center for Cybersikkerhed, og herunder netsikkerhedstjenesten, er på et absolut højt niveau. Et brud på sikkerheden hos Center for Cybersikkerhed vil kunne få katastrofale følger for hele samfundet, såfremt bruddet medførte uvedkommendes adgang til netsikkerhedstjenestens funktionalitet og de indhentede data.

6. Opfølgning

Ifølge kommentarerne til lovændringen skal Center for Cybersikkerhed efter tre år udarbejde en rapport om erfaringerne med den nye lovgivning til Folketinget. Henset til den alvorlige og hastige ændring i cybertruslerne, bør denne rapportering ske allerede efter første år og følges op med rapportering efter andet og tredje år. Rapporten bør være offentlig tilgængelig.

7. Det tekniske setup og performance

Der udtrykkes bekymring vedrørende CFCS' anvendte tekniske løsninger i forhold til opretholdelse eller ændring af virksomhedens sikkerhedsniveau og eventuelle påvirkning af systemernes og infrastrukturs ydeevne.

Afslutningsvist bemærkes, at F&P ikke har været på Forsvarsministeriets høringsliste. Fremadrettet bedes I være opmærksomme på dette og sørge for, at F&P er på høringslisten og modtager orienteringerne. I bedes sende til Forsikring & Pension på fp@forsikringogpension.dk.

Med venlig hilsen

Henriette Günther Sørensen

Fra: Nella Festirstein <nellaf@tinganes.fo>
Sendt: 14. januar 2019 18:38
Til: FMN-MYN-FORSVARSMINISTERIET; FMN-TBL Larsen, Tina Kathrine Berg; FMN-SBU Østergren, Stine Busch
Cc: 'ro@fo.stm.dk'; VMR-Journal
Emne: Høringssvar fra Færøernes landsstyre over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (RIGS-FO Sagsnr.: 2017 - 647)
Vedhæftede filer: Høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed.pdf; Høringsbrev.pdf; Høringsliste.pdf; Lovudkast.pdf; smime.p7s

Kategorier: Christina

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

Til Forsvarsministeriet

Færøernes Landsstyre har fra Rigsombudsmanden på Færøerne fået tilsendt i høring *"Forslag til Lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden)".*

Ifølge lovudkastets § 3 skal loven ikke gælde direkte for Færøerne, men loven kan senere ved kongelig anordning helt eller delvist sættes i kraft for Færøerne, såfremt færøske myndigheder anmoder herom.

Færøernes Landsstyre tager dette til efterretning og har på nuværende tidspunkt ikke andre bemærkninger til lovforslaget.

Venlig hilsen

Nella Festirstein
Afdelingschef

Beskrivelse:...

Lagmandens Kontor
Lovafdelingen
Tlf. +298 30 60 00
Direkte tlf. +298 55 80 76

Fra: Rigsombuddet <ro@fo.stm.dk>
Sendt: 9. januar 2019 08:22
Til: Nella Festirstein <nellaf@tinganes.fo>; Journalin hjá LMS <journalin@tinganes.fo>
Emne: Høring hos færøske myndigheder over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (RIGS-FO Sagsnr.: 2017 - 647)

Til Løgmansskrivstovuna

På vegne af Forsvarsministeriet fremsendes i høring udkast til forslag til lov om ændring av lov om Center for Cybersikkerhed.

Forsvarsministeriet har sat høringsfristen til at være **senest 4. februar kl. 11.**

Bemærkninger bedes sendt til fmn@fmn.dk, tbl@fmn.dk, sbu@fmn.dk med kopi til Rigsombuddet på ro@fo.stm.dk

Med venlig hilsen

John Johannessen
Administrativ kontorleder
Postboks 12
FO-110 Tórshavn
Tlf.: +298 731203
E-mail: jjo@fo.stm.dk
www.rigsombudsmanden.fo

Til:
Fra: Forsvarsministeriet (fmn@fmn.dk)
Titel: Høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed
Sendt: 07-01-2019 16:01:50

Den vedhæftede e-mail er blevet behandlet af Sikker E-mail Postkasse.

Modtaget af Sikker E-mail Postkasse: 07-01-2019 16:02:08,940 CET

Sikkerhedskontrollen af e-mailen gav følgende resultat:

Fortrolig (krypteret): Nej
Digital signatur: Gyldig
signatur verificeret: 07-01-2019 16:02:08,957 CET

Virksomhedscertifikat
Navn : Forsvarsministeriet Departementet - Forsvarsministeriet
CVR : CVR:25775635

Bemærkning:

Øvrige oplysninger:

Krypteringstilstand:
transport nøgle krypteret med: Ingen kryptering
data krypteret med: Ingen kryptering

Ingeniørforeningen, IDA
Kalvebod Brygge 31-33
DK-1780 København V
Tlf. +45 33 18 48 48

Viden der styrker
ida.dk

Forsvarsministeriet
Holmens Kanal 9
1060 København K

fmn@fmn.dk

tbl@fmn.dk, sbu@fmn.dk

4. februar 2019

Svar på Høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden)

Ingeniørforeningen, IDA vil gerne takke for muligheden for at komme med svar på Høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden).

Indledningsvist vil vi gerne understrege opbakning til en styrkelse af indsatsen for en øget cybersikkerhedsindsats i Danmark. Det gælder både en aktiv indsats under Forsvarsministeriets institutioner, men også myndighedernes generelle indsats for at højne niveauet for både viden, kompetencer til at håndtere udfordringerne og den rådgivningsindsats, der er sat i værk fra forskellige myndigheder. Det er IDAs opfattelse, at der er brug for en bredspektret indsats overfor både offentlige institutioner, virksomheder samt borgerne som privatpersoner. IDA bidrager generelt meget gerne – og aktivt – til denne indsats.

I forhold til fremlagte lovforslag har IDA dog følgende betænkeligheder:

Manglende ajourføring af kapitel 6 til GDPR
Center for Cybersikkerhed har i forbindelse med det aktuelle lovforslag ikke revideret det såkaldte kapitel 6 i den eksisterende lov. Kapitel 6 omfatter Center for Cybersikkerheds håndtering af personoplysninger, og følger den nu tidligere persondatalov. Center for Cybersikkerhed har således valgt ikke at opdatere kapitel 6 til GDPR (EU's databeskyttelsesforordningen/loven), hvilket betyder, at Center for Cybersikkerhed lægger op til at være undtaget fra GDPR.

IDA har bedt sit it-politiske panel[1] forholde sig til, at Center for Cybersikkerhed lægger op til at undtage sig selv fra at følge GDPR, og mere end hver anden mener, at Center for Cybersikkerhed burde leve op til GDPR.

[1] IDAs it-politiske panel består af it-professionelle medlemmer af IDA.

På denne baggrund anbefaler IDA, at lovforslaget justeres, sådan at kapitel 6 opdateres til at følge formålet med GDPR.

Jf. §3 og kapitel 4 om øgede muligheder for Center for Cybersikkerheds netsikkerhedstjeneste.

Påbud

Center for Cybersikkerheds netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder. Med forslaget i §3, stk. 4 kan Center for Cybersikkerhed i "særlige tilfælde påbyde virksomheder, regioner og kommuner, der har særlig samfundsvigtig karakter at blive tilsluttet netsikkerhedstjenesten".

IDA har forståelse for at dele af den kritiske danske infrastruktur (til trods for vi i Danmark endnu ikke har en klar definition heraf) med fordel kunne falde ind under et behov for øget overvågning. Det gælder ikke mindst de dele af den kritiske infrastruktur, der er ejet eller driftes af udenlandske virksomheder. Dog er det afgørende nødvendigt, at det defineres klart, hvad der menes med kritisk infrastruktur, herunder eventuelt dele af organisationer eller institutioner, og at der skelnes klart i forhold til om denne infrastruktur involverer personfølsomme eller udelukkende ikke-personfølsomme data.

IDA har bedt sit it-politiske panel forholde sig til dette påbud (jf. desuden tabel 1):

- 63 pct. svarer, at Center for Cybersikkerhed skal have lov til at påbyde virksomheder/myndigheder at være med i sensornetværket - forudsat det alene sker i særlige og lovdefinerede tilfælde.
- 24 pct. mener, at Center for Cybersikkerhed slet ikke skal have lov til at påbyde virksomheder/myndigheder at være med i sensornetværket.

Tabel 1. Hvad tænker du om det?

	Procent
CFCS skal have lov til at påbyde virksomheder/myndigheder at være med i sensornetværket	11 %
CFCS skal have lov til at påbyde virksomheder/myndigheder at være med i sensornetværket - forudsat det alene sker i særlige og lovdefinerede tilfælde	63 %
CFCS skal ikke have lov til at påbyde virksomheder/myndigheder at være med i sensornetværket	24 %
Ved ikke	2 %
Ønsker ikke at svare	0 %
I alt	100 %

Kilde: IDA Analyse (2019): Ny lov for CFCS – en analyse blandt IDAs it-politiske panel.
Note: IDAs it-politiske panel består af it-professionelle medlemmer af IDA.

IDA må på denne baggrund påpege, at det som følge af de øgede beføjelser i §3, er afgørende nødvendigt med en specifik beskrivelse af, hvilke virksomheder og hvilke funktioner i regioner og kommuner, der vil kunne høre under denne definition – og dermed blive ramt af påbud.

Udvidelse af sensornetværkets funktionalitet

Med lovforslaget ønsker Center for Cybersikkerhed at udvide funktionaliteten i sensornetværket. Det betyder, at man ønsker at lave dataindsamlingen in-line for at kunne gøre sensorerne aktive. Derved får Center for Cybersikkerhed mulighed for at manipulere med datatrafikken. Fx standse datahøst eller manipulere det svar til en hacker, som myndigheden/virksomheden måtte levere ved hack.

IDA har bedt sit it-politiske panel forholde sig dette element i lovforslaget, og de tilkender blandt andet følgende (jf. desuden tabel 1):

- 64 pct. er **uenig eller helt uenig** i, at Center for Cybersikkerhed i alle tilfælde skal have lov til at udvide funktionaliteten, herunder også i forbindelse med påbud
- 46 pct. er **enig eller helt enig** i, at Center for Cybersikkerhed skal have lov til at udvide funktionaliteten, men kun de i tilfælde hvor en virksomhed/myndighed **frivilligt** ønsker det – dvs. at man fortsat kan blive på den gamle ordning, hvis man ønsker det.

Tabel 2. Hvad tænker du om forslaget om at udvide sensornetværkets funktion?

	Helt uenig	Uenig	Hverken eller	Enig	Helt enig	Ved ikke	I alt
CFCS skal i alle tilfælde have lov til at udvide funktionaliteten, herunder også i forbindelse med påbud	24 %	40 %	12 %	8 %	9 %	7 %	100 %
CFCS skal have lov til at udvide funktionaliteten, men kun de i tilfælde hvor en virksomhed/myndighed frivilligt ønsker det. Dvs. at man fortsat kan blive på den gamle ordning, hvis man ønsker det	12 %	21 %	16 %	27 %	19 %	5 %	100 %

Kilde: IDA Analyse (2019): Ny lov for CFCS – en analyse blandt IDAs it-politiske panel.
Note: IDAs it-politiske panel består af it-professionelle medlemmer af IDA.

IDA anbefaler derfor, at Center for Cybersikkerhed skriver ind i loven, hvornår og i hvilket omfang en udvidet funktionalitet af sensornetværket skal kunne bruges. Det skal være klart for virksomheder og myndigheder, om de kan påbydes, at Center for Cybersikkerhed indsamler data in-line eller om de kan forblive på/nøjes med den gamle ordning. IDA anbefaler i den forbindelse, at Center for Cybersikkerhed gør det frivilligt for virksomheder og myndigheder selv at vælge, om de vil

være med i netværket på ny eller gammel ordning.

Jf. §§ 4 - 6
IDA er betænkelig ved §§ 4 – 6, der er omfattet af Grundlovens § 72. §§ 4- 6 giver mulighed for at Center for Cybersikkerheds netsikkerhedstjeneste "uden retskendelse kan behandle trafikdata, pakkedata og stationære data hidrørende fra tilsluttede myndigheder og virksomheder". Formålet med Grundlovens § 72 er at sikre, at myndighederne ikke krænker privatlivets fred. Under helt særlige omstændigheder kan der undviges fra Grundloven efter afvejning af proportionalitetsprincippet. Ved at tillade en efterretningstjeneste adgang til at behandle trafikdata, pakkedata og stationære data fra f.eks. sundhedsmyndigheder eller visse typer virksomheder, vil tjenesten herved få adgang til personfølsomme oplysninger om borgere og kunder, herunder social- og sundhedsoplysninger, data vedr. genetik og biometri, samt oplysninger om bl.a. religiøse, politiske og seksuelle tilhørsforhold, som ikke vedrører andre end borgeren selv og en evt. behandler.

IDA finder det problematisk, at det ikke er præcist formuleret, i) hvordan og i hvilket omfang efterretningstjenesten vil få adgang til sådanne oplysninger og ii) hvordan man vil håndtere disse oplysninger, f.eks. jf. regler i GDPR, der har til formål at beskytte og sikre borgerens ret til egne data.
For det andet finder IDA ikke, at der er proportionalitet mellem den fuldstændige adgang til hele spektret af personfølsomme oplysninger og det formål, der er udgangspunktet for lovforslaget.

Sammenfatning i forhold til §§ 3-6
IDA kan derfor ikke støtte ændringsforslagene i §§ 3-6 med de nuværende formuleringer, mangel på præciseringer og afgrænsninger og vi anbefaler derfor, at der afsøges alternative muligheder til at overvåge eventuelle hændelser i de omtalte institutioner og virksomheder.

Jf. § 16
IDA har forståelse for det fornuftige i at kunne videresende information om data eller malware til de aktører, der måtte være negativt berørt af en sikkerhedshændelse. IDA er derfor positive overfor denne ændring.

Jf. §17
IDA anerkender, at Center for Cybersikkerhed har identificeret et behov for at arkivere data i forbindelse med sikkerhedshændelser i en længere periode end hidtil antaget, herunder når formålet er at kunne genbruge erfaringer til at modvirke eller forebygge nye hændelser. IDA vil dog gerne i den forbindelse bemærke to ting:

1. Så længe Center for Cybersikkerhed er fuldt og helt underlagt Forsvarets Efterretningstjeneste, og herunder undtaget GDPR, offentlighedslov og forvaltningslov kan vi ikke bakke op om en udvidelse af slettefristen. Dette primært fordi, at det øger tidsrummet, hvori Center for Cybersikkerhed kan dele informationer med andre. Hverken de distribuerede informationer eller disse andre, som data deles med, kan der føres demokratisk kontrol med, fordi Center for Cybersikkerhed er organisatorisk placeret, som det er. Og det finder IDA problematisk. Vil centeret derfor øge slettefristerne, må der tilsvarende åbenhed og demokratisk kontrol med ind i lovforslaget.

2. Slettefristen på de (foreslåede) fem år gælder alene for Center for Cybersikkerhed. Er data delt med andre, gælder slettefristen ikke for dem. Det finder IDA problematisk, og mener, at det bør skrives ind i loven, at slettefristen er en absolut størrelse, som også gælder for dem, som data er blevet delt med. Vi ser derfor ingen grund til at videregivelse af data eller informationer om hændelser skulle annullere sletningsfristen. Derimod bør Center for Cybersikkerhed gøre modtagerne af informationerne opmærksom på, at data skal slettes. Udgangspunktet for denne holdning er, at data helt generelt kun bør opbevares i så lang tid, som det er nødvendigt for at udføre en given opgave.

Med venlig hilsen

Grit Munk
Chefkonsulent
Politik, Analyse og Presse
Ingeniørforeningen, IDA

Helena Juul Jensen
Chefkonsulent
Politik, Analyse og Presse
Ingeniørforeningen, IDA

IT-Branchens svar på høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed

IT-Branchen hilser Regeringens store fokus på cybersikkerhed velkommen. Cybersikkerhed er en afgørende forudsætning for vores gennemdigitaliserede samfund, og derfor er det glædeligt, at regeringen, med den nationale strategi for cyber og informationssikkerhed og de mange sektorstrategier, har forstået at løfte indsatsen på området markant.

Center for Cybersikkerhed (CfCS) spiller en central rolle i regeringens indsats på cybersikkerhedsområdet, og får med det nuværende lovforslag en endnu mere central rolle. CfCS har de seneste år i høj grad vist sin berettigelse, og har været med til at øge awareness og hjælpe danske myndigheder og virksomheder med at forebygge, imødegå og beskytte sig mod cyberangreb.

IT-Branchen har dog en række bekymringer omkring den rolle, som CfCS vil få som følge af Regeringens lovforslag.

1. **Påbud om tilslutning til sensornetværket er problematisk**

Det er højest problematisk, at lovforslaget lægger op til, at CfCS kan påbyde private virksomheder at blive tilsluttet Netsikkerhedstjenesten.

For mange virksomheder kan det kan være kritisk at blive tvunget til tilslutning, uden at kunne redegøre overfor kunder og ejerkreds, hvad data bliver brugt til og hvor de havner.

Vi har en lang tradition i Danmark for tillid og åbenhed, og Danmark har en international styrkeposition, fordi der er tillid til dansk digitalisering, og fordi Danmark internationalt er kendt for, at have et åbent statsapparat.

Tvangstilslutning til overvågningstjenesten risikerer derfor både at ramme danske virksomheders eksport samt internationale investeringer i forskning og produktudvikling i Danmark.

2. **Der mangler klarhed om hvem der kan blive påbudt tilslutning**

Det er meget bekymrende at der ingen steder i lovforslaget er nærmere defineret, hvilke typer af virksomheder der kan påbydes at blive tilsluttet Netsikkerhedstjenesten. Begrebet ”samfundsvigtige virksomheder” er et meget uklart og kan tolkes meget bredt.

Det overlades hermed til centeret selv og Forsvarsministeren egenhændigt at beslutte, hvilke virksomheder der skal påbydes at blive tilsluttet. Det vil skabe en stor usikkerhed hos mange virksomheder. IT-Branchen anbefaler derfor at man fastholder at anvende begrebet samfundskritisk infrastruktur (jf. NIS-direktivet), samt definerer hvad begrebet dækker i Danmark og lader det være scope for loven.

3. **Mangel på effektivt demokratisk tilsyn**

Med udvidelsen af CfCS’s beføjelser er der en stigende nødvendighed for at sikre at centrets beføjelser ikke misbruges.

Lovforslaget lægger op til at skabe en myndighed, som får øgede beføjelser over for civilsamfundet uden at være underlagt domstolsprøvelse eller offentlig kontrol – bortset fra Folketingets kontroludvalg. Ud over mulighed for at påbyde tilslutning til sensornetværket får centeret blandt andet også mulighed for jf. kapitel 4 at tilgå data hos private virksomheder uden retskendelse.

I en tid hvor den frie vestlige verden generelt går mod større åbenhed og kontrol med efterretningsvæsenet, går Danmark den stik modsatte vej med dette lovforslag.

IT-Branchen vil på det kraftigste opfordre til at CfCS, underlægges almindelig parlamentarisk kontrol, ligesom deres afgørelser bør kunne prøves ved civile domstole.

4. Gør tilslutning frivillig

IT-Branchen anbefaler derfor på det kraftigste, at tilslutning til Netsikkerhedstjenesten gøres frivillig. Den enkelte virksomhed eller myndighed bør selv træffe beslutning om hvilke sikkerhedsforanstaltninger de anvender. Hvis CfCS alligevel finder det afgørende at påbyde tilslutning til Netsikkerhedstjenesten bør tilslutning i disse tilfælde kunne ske gennem virksomhedernes eget valg af teknologi og udstyr. Udveksling af data vil med et sådan setup kunne ske på den tilsluttede virksomheds præmisser, krypteret og i et standardiseret format.

5. Centerets aktiviteter vil konkurrere på ulige vilkår med kommercielle it-sikkerhedsleverandører

Flere elementer i lovforslaget vil gøre CfCS i stand til at tilbyde og påbyde ydelser gratis, som i dag tilbydes af kommercielle aktører. Det er yderst problematisk for det danske marked for it-sikkerheds produkter og services.

I bemærkningerne til lovforslaget fremhæves flere steder, at CfCS kan noget private leverandører ikke kan, da centerets løsning er efterretningsbaseret. Vi er ikke i tvivl om, at CfCS har adgang til efterretningsviden, som it-leverandørerne ikke har, og at det kan give centret nogle muligheder, som branchen ikke har. Men det kan kun være relevant for en lille delmængde af de aktiviteter centeret har. Mange af centerets informationer kommer fra de kommercielle aktører og langt de fleste aktiviteter vil kunne løses mindst ligeså godt af private aktører.

Med det nuværende lovforslag som udvider centerets aktiviteter markant, vil en stadigt større del af centerets aktiviteter være i direkte og ulige konkurrence med private aktører. Som eksempler på foreslåede aktiviteter, der vil konkurrere med private leverandører, kan nævnes muligheden for at tilbyde et aktivt cyberforsvar (3.2), installation af sikkerhedssoftware på lokale netværk og enheder (3.3) og forebyggende sikkerhedstekniske undersøgelser (3.4).

Hvis CfCS ligger inde med efterretningsmæssig information der kan forbedre den sikkerhedssoftware, der allerede findes på markedet anbefaler IT-Branchen i øvrigt, at centeret stiller disse til rådighed for de relevante private aktører så de kan indlejres i deres sikkerhedssoftware.

6. Brug markedet aktivt som medspiller

I stedet for at tilbyde aktiviteter i konkurrence med markedet, vil IT-Branchen anbefale at CfCS i langt højere grad gør brug af de kommercielle aktører. Danmark har ifølge Erhvervsstyrelsen over 260 it-sikkerhedsleverandører med omkring 3.000 ansatte. Hertil kan lægges de ansatte, som internationale leverandører kan trække på i udlandet.

Den ekspertise som hele erhvervslivet besidder inden for IT sikkerhed kan bringes langt bedre i spil, ved at CfCS alene forestår det efterretningsbaserede analysearbejde, mens fx den konkrete dataindsamling og det aktive cyberforsvar kan overlades til den tilsluttede organisation selv eller private aktører efter udbud. En model der kunne overvejes er fx stille minimumskrav til sikkerheden i virksomheder der varetager kritisk infrastruktur, eller ved at indgå en rammeaftale med flere

leverandører, således at alle kan tilsluttede organisationer kan vælge mellem en række godkendte løsninger.

Herved kan CfCS bruge deres kompetencer og ressourcer mere effektivt, ligesom ressourcerne i den danske it-sikkerhedsbranche ligeledes kan bringes bedre i spil. Samlet set vil indsatsen kunne nå ud til langt flere.

Vi stiller gerne op
IT-Branchen ser frem til den fortsatte dialog, og vi står naturligvis til rådighed for en uddybning af ovenstående.

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt per email til **fmn@fmn.dk**
med kopi til **tbl@fmn.dk** og **sbu@fmn.dk**

IT-Politisk Forening
c/o Jesper Lund
Carl Bernhards Vej 15, 2.tv
1817 Frederiksberg C

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 4. februar 2019

Høringssvar vedr. udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Sagsnr. 2018/006599)

Lovforslaget indeholder en række meget brede beføjelser til Center for Cybersikkerhed, som er formuleret på en særdeles uklar måde, hvor de kan betyde næsten hvad som helst.

Konstruktionen omkring Center for Cybersikkerhed indebærer allerede i dag meget omfattende indgreb i borgernes grundlæggende rettigheder til privatliv og beskyttelse af personlige oplysninger. Lovudkastet medfører en betydelig udvidelse af disse allerede meget omfattende indgreb, men det er umuligt at vurdere rækkevidden af de nye udvidede indgreb på grund af lovtekstens meget brede og upræcise formuleringer.

Udvidelsen af Center for Cybersikkerheds beføjelser gælder både i forhold til antallet af tilsluttede virksomheder og offentlige institutioner og mængden af personoplysninger som Center for Cybersikkerhed kan få adgang til. Hvor der tidligere alene var adgang til nettrafik, er der med lovforslaget adgang til alle data via det nye begreb ”stationære data”. Alle afgrænsninger af disse meget vidtgående beføjelser er alene overladt til Center for Cybersikkerheds egne vurderinger uden nogen uafhængig kontrolfunktion.

IT-Politisk Forening vil anbefale, at lovforslaget i den nuværende affatning ikke fremsættes i Folketinget, og at Forsvarsministeriet i stedet udarbejder

et helt nyt lovforslag, hvor det reelt er muligt for høringsparterne (i en ny høring) at vurdere hvilke beføjelser som Center for Cybersikkerhed får og hvordan disse beføjelser er afgrænset af objektive bestemmelser. En ”collect it all” beføjelse, som derefter alene begrænses af Center for Cybersikkerheds egne vurderinger, er ikke acceptabelt i et demokratisk samfund.

Indgreb i grundlæggende rettigheder og EMRK

Når staten gør indgreb i borgernes grundlæggende ret til privatliv, er det et krav efter retspraksis fra den Europæiske Menneskerettighedsdomstol (EMD), at disse indgreb sker via et retsgrundlag, som er klart og præcist, og at anvendelsen af dette retsgrundlag skal være forudsigeligt for de personer, som er omfattet af dets anvendelsesområde. Det lovudkast, som er sendt i høring, lever ikke op til disse krav, fordi det er totalt umuligt at vurdere rækkevidden af lovforslagets bestemmelser.

Det er også et krav, at indgreb i retten til privatliv skal være egnet til at forfølge et formål af almen interesse, samt være nødvendigt og proportionalt. Et indgreb kan kun anses for at være nødvendigt, såfremt der ikke findes mindre indgribende foranstaltninger, som kan opfylde formålet af almen interesse.

IT-Politisk Forening anser samfundets cybersikkerhed for at være et formål af almen interesse, som kan begrunde visse indgreb i retten til privatliv, men vi vil stille os stærkt tvivlende over for, om den potentielt meget omfattende bulkindhentning overhovedet er egnet til at opfylde formålet. Derudover er der i lovforslaget absolut ingen overvejelser om, hvorvidt andre, mindre indgribende foranstaltninger kan opfylde formålet. I afsnittet om nødvendighed henviser lovforslagets bemærkninger pkt. 4.3 alene meget overordnet til den skønsmargin, som EMD anerkender at stater har. Det ændrer imidlertid ikke ved, at Forsvarsministeriet skal overveje, om der er andre, mindre indgribende foranstaltninger, som kan opfylde det almene formål vedr. cybersikkerhed.

I forhold til kravet om proportionalitet henviser Forsvarsministeriet til, at Tilsynet med Efterretningstjenesterne (TET) fører tilsyn med Center for

Cybersikkerheds behandling af personoplysninger. Dette tilsyn er imidlertid alene en legalitetskontrol med de indhentede personoplysninger. Der er ingen uafhængige kontrolforanstaltninger vedrørende omfanget af selve indhentningen, som sker uden retskendelse og alene efter vurderinger foretaget af Center for Cybersikkerhed. Sammenholdt med de meget generelle beføjelser kan det på ingen måde sikres, at kravene om proportionalitet overholdes.

Det nævnes i lovforslagets pkt. 3.3.2, at overvågning (bulkindhentning) på interne netværk og enheder ikke vurderes til at være ”egnet til domstolsprøvelse”. På den baggrund er den uafhængige forhåndskontrol fravalgt. Den begrundelse er helt og aldeles uacceptabel i et demokratisk samfund. Hvis de nuværende uafhængige kontrolfunktioner som domstolene ikke er egnede til at udføre kontrolopgaven med bulkindhentningen hensigtsmæssigt, bør der oprettes nye uafhængige kontrolfunktioner for denne aktivitet. Her kunne man givetvis med fordel søge inspiration hos europæiske lande, som har mere veludviklede systemer for uafhængig kontrol og tilsyn med efterretningstjenesterne end Danmark.

Det fremhæves i lovforslaget, at Center for Cybersikkerheds indgreb i retten til privatliv modsat den almindelige bulkindhentning hos efterretningstjenester (som Forsvarets Efterretningstjeneste) ikke foretages med henblik på at udfinde målpersoner, og at indgrebet i retten til privatliv derfor skulle være ”mindre intensivt”. Det er imidlertid temmelig misvisende, idet Center for Cybersikkerhed har specifikke beføjelser til at videregive oplysninger om udfundne målpersoner til politiet ved begrundet mistanke om en sikkerhedshændelse, og med det nye lovforslag får Center for Cybersikkerhed sågar hjemmel til at indhente yderligere oplysninger til identifikation af udfundne målpersoner med editionskendelser (lovforslagets kapitel 4 a).

Af de ovennævnte grunde, altså de meget uklare men omfattende beføjelser til Center for Cybersikkerhed og en helt utilstrækkelig og mangelfuld vurdering af om lovforslaget er foreneligt med Den Europæiske Menneskerettighedskonvention (EMRK), har IT-Politisk Forening ikke fundet det formålstjenstligt at komme med mere detaljerede kommentarer til lovforslagets

bestemmelser på nuværende tidspunkt.

Tvangsmæssig tilslutning til uønsket tjeneste

Som en overordnet kommentar vil IT-Politisk Forening dog påpege, at Center for Cybersikkerhed trods meget store bevillinger ikke har været i stand til at tilbyde en netsikkerhedstjeneste, som danske virksomheder ønsker at gøre brug af. Hverken Forsvarsministeriet eller Center for Cybersikkerhed har udvist nogen interesse for at afdække årsagerne til dette. Den manglende tilslutning fra private virksomheder kunne i høj grad indikere, at der er behov for grundlæggende reformer af den måde, som Center for Cybersikkerhed er organiseret på og samarbejder med det øvrige samfund (offentlige institutioner, private virksomheder og organisationer, samt borgere). Det er næppe udgiften på 400.000 kr. om året, som får store private virksomheder af ”samfundsvigtig karakter” til at gå uden om Center for Cybersikkerhed.

I den forbindelse vil det være oplagt at vurdere, om det er hensigtsmæssigt at placere opgaver som næsten udelukkende er civile og som indebærer behandling af omfattende mængder personoplysninger hos Forsvarets Efterretningstjeneste, en offentlig myndighed som er undtaget fra væsentlige retsgarantier for beskyttelse af borgerne som databeskyttelsesforordningen (GDPR) og betydelige dele af offentlighedsloven og forvaltningsloven. Med lovforslaget tilføjes i øvrigt en undtagelse fra retssikkerhedsloven, som åbenbart blev glemt på listen med undtagelser i 2014.

I stedet for disse helt nødvendige og essentielle overvejelser om hvorfor det nuværende setup ikke skaber værdi for samfundet, vælger Forsvarsministeriet med lovforslaget at indføre mulighed for tvangsmæssig tilslutning for de virksomheder og offentlige myndigheder, som Center for Cybersikkerhed finder tilpas interessante for tjenestens opgavevaretagelse. Det sker samtidig med at overvågningsbeføjelsen udvides fra indgående og udgående nettrafik til at omfatte samtlige data, som behandles i IT-systemer (”stationære data”).

Det anføres i lovforslagets bemærkninger, at den tvungne tilslutning kun forventes at ske i sjældne tilfælde (under 10

gange om året). Men det er langtfra sikkert (der er ikke en juridisk bindende kvote for antallet af tvungne tilslutninger), og fremadrettet kan det i øvrigt blive særdeles vanskeligt at vurdere, hvor mange tilslutninger der reelt er tvungne. Udsigten til at kunne modtage et pålæg om tilslutning kan meget vel få flere private virksomheder til at vælge en ”frivillig” tilslutning til Center for Cybersikkerhed. Disse bemærkninger gælder også for den nye overvågning på interne netværk og enheder (adgang til ”stationære data”), som er frivillig for de tilsluttede organisationer, undtagen når den i særlige tilfælde er tvungen. Hvad det betyder er selvsagt meget uklart.

For de borgere, som får deres personoplysninger videregivet til Center for Cybersikkerhed, er der principielt ingen forskel på om tilslutningen er frivillig eller tvungen. Men den nye mulighed for tvungen tilslutning vil uundgåeligt medføre, at der videregives langt flere personoplysninger til Center for Cybersikkerhed, også via de formelt frivillige (men i praksis måske reelt tvungne) tilslutninger.

Transparens om tilsluttede organisationer fjernes

Transparensen omkring de tilsluttede virksomheder og offentlige myndigheder fjernes fuldstændigt, uden at Forsvarsministeriet på nogen måde redegør for motivationen til dette. I bemærkningerne til den nuværende § 3 i lov om Center for Cybersikkerhed står der:

> *Center for Cybersikkerhed vil regelmæssigt offentliggøre, hvilke myndigheder og virksomheder der er tilsluttet netsikkerhedstjenesten efter § 3, stk. 2 og 3.*

Uden nogen kommentarer eller begrundelser er denne transparensbestemmelse (der i øvrigt ikke var med i det lovudkast, som blev sendt i høring i 2014) erstattet med:

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

Det er helt uacceptabelt, at borgerne på den måde bliver frataget muligheden for at få information om hvornår de kan blive overvåget af Center for Cybersikkerhed. Det udelukker blandt andet, at borgerne selv kan træffe passende foranstaltninger mod denne overvågning ved eksempelvis at undgå de danske virksomheder, som er under overvågning af Center for Cybersikkerhed, enten frivilligt eller via tvangsmæssig foranstaltninger (påbud).

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sags-ID: Sagsbehandler: MRC Deres ref.: 2018/006599 Dato: 04.02.2019

Lyren 1
DK-6330 Padborg
Danmark

T: +45 7467 1233
F: +45 7467 4317

itd@itd.dk
itd.dk

CVR: 40990917

Høring vedrørende forslag til lov om ændring af lov om Center for Cybersikkerhed

ITD kvitterer for den fremsendte høring og muligheden for at komme med bemærkninger til lovforslaget.

Indledningsvist bemærkes, at spørgsmålet om cybersikkerhed er højt prioriteret i ITD grundet den stadig stigende betydning for transporterhvervet. Behovet for IT-sikkerhed bliver væsentligt større, når flere processer og systemer er digitaliseret og afhænger af hinanden. Det gælder blandt andet persondatabeskyttelse, håndtering af fortrolige oplysninger og beskyttelse mod misbrug af data generelt.

Vejgodstransporten og -logistikken står over for en gennemgribende digitalisering i de kommende årtier. Ændringerne har potentiale til at ændre verdenshandelen og åbne for helt nye forretningsmodeller. Samtidig forventes fremtidens transportteknologier i tiltagende grad at omfatte selvkørende og på sigt førerløse køretøjer, hvilket vil kræve større systemer til overvågning og styring. Dermed øges også potentialet for cybertrusler.

ITD hilser derfor lovforslaget velkomment og tilslutter sig ambitionen om en styrkelse af Center for Cybersikkerhed.

På baggrund af ovenstående skal ITD dog understrege behovet for også at have fokus på den digitale transportinfrastruktur i forbindelse med vurderingen af mulige cybertrusler.

Endvidere skal ITD understrege behovet for fortrolighed omkring forretningskritiske data. ITD anerkender behovet for øgede beføjelser til Center for Cybersikkerhed, men det er helt afgørende, at oplysninger om virksomhedernes forretningsforhold af konkurrencemæssige årsager beskyttes, og at der ligger helt klare retningslinjer for, hvor langt Center for Cybersikkerhed kan gå uden tilsagn eller dommerkendelse.

ITD har ikke bemærkninger til lovforslagets enkelte bestemmelser.

Med venlig hilsen

ITD

Mads Røddik Christensen
Chefkonsulent

INSTITUT FOR
MENNESKE
RETTIGHEDER

Forsvarsministeriet
Holmens Kanal 42
1060 København K
Danmark
E-mail: fmn@fmn.dk med kopi til tbl@fmn.dk og sbu@fmn.dk

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
MOBIL 9132 5761
MAAK@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 19/00103-2

4. FEBRUAR 2019

HØRING OVER UDKAST TIL FORSLAG TIL LOV OM ÆNDRING AF LOV OM CENTER FOR CYBERSIKKERHED (INITIATIVER TIL STYRKELSE AF CYBERSIKKERHEDEN)

Forsvarsministeriet har ved e-mail af 7. januar 2019 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til et udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (initiativer til styrkelse af cybersikkerheden).

Instituttet har valgt at fokusere på følgende dele af udkastet: 1) påbud om tilslutning til netsikkerhedstjenesten, 2) udvidet adgang til indgreb i meddelelseshemmeligheden, og 3) ændrede frister for sletning af data.

SAMMENFATNING

Instituttet bemærker indledningsvist, at udkastet varetager det væsentlige og anerkendelsesværdige formål at sikre Danmark mod cybertrusler i form af blandt andet cyberspionage, cyberkriminalitet og infrastrukturangreb og at sikre, at Danmark har et højt cybersikkerhedsniveau.

Udkastet lægger op til betydelige kompetenceudvidelser for Center for Cybersikkerhed på en række områder med den konsekvens, at centret kommer i besiddelse af en betydelig mængde personoplysninger, herunder følsomme personoplysninger.

Dette sker blandt andet ved en tvunget tilslutning til centrets såkaldte netsikkerhedstjeneste, hvorfra centret kan monitorere al digital korrespondance til og fra virksomheden eller myndigheden samt såkaldt stationær data, som for eksempel private data på en medarbejders pc.

Centret har i øvrigt også adgang til sådanne private data hos virksomheder og myndigheder, der ikke er tilsluttet netsikkerhedstjenesten – og uden et krav om retskendelse.

For samtlige de indhentede data er centret i øvrigt ikke forpligtet til at slette disse før efter 5 år, hvis oplysningerne knytter sig til en sikkerhedshændelse og 3 år, hvis oplysningerne ikke knytter sig til en sikkerhedshændelse. En sikkerhedshændelse er blandt andet en hændelse, der negativt påvirker tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.

Efter gældende ret er fristerne henholdsvis 3 år og 13 måneder.

Alt i alt kommer Center for Cybersikkerhed til at være i besiddelse af en betydelig mængde data – og for en længere periode – end centret hidtil har haft beføjelse til at indsamle og behandle.

Udvidelserne kan hver for sig og samlet føre til indgreb i retten til respekt for privatliv, beskyttet i Den Europæiske Menneskerettighedskonvention artikel 8, ligesom enkelte af udvidelserne udgør et indgreb i meddelelseshemmeligheden, beskyttet i grundlovens § 72.

- Instituttet anbefaler blandt andet, at ministeriet overvejer at indsætte et krav om efterfølgende retskendelse ved Center for Cybersikkerheds indhentelse af oplysninger, som udgør indgreb i meddelelseshemmeligheden.

Instituttet vurderer endvidere, at der er risiko for uproportionale indgreb ved en slettefrist på 3 år i stedet for 13 måneder for oplysninger, som ikke vedrører sikkerhedshændelser.

- Instituttet anbefaler, at ministeriet i lovbemærkningerne nøje redegør for, hvorledes det vil sikres, at en udvidelse af slettefristen fra 13 måneder til 3 år ikke vil føre til uproportionale indgreb i retten til respekt for privatliv.

Mere generelt har instituttet principielle betænkeligheder ved centrets placering under Forsvarets Efterretningstjeneste (FE), som instituttet også har rejst tidligere.

Instituttet bemærker i den forbindelse, at det eneste retsgrundlag, som adskiller deling af oplysning fra Center for Cybersikkerhed til FE's efterretningsfunktioner er en vejledning fra Forsvarsministeriet.

Disse principielle bekymringer får fornyet aktualitet ved en udvidelse af centrets beføjelser – navnlig i fraværet af effektive retsgarantier som for eksempel krav om retskendelse og skærpede slettefrister.

- Instituttet anbefaler, at der i udkastet indføres en bestemmelse om betingelserne for videregivelse af data fra centret til resten af Forsvarets Efterretningstjeneste, således at forholdet reguleres på lovniveau.

UDKASTETS INDHOLD

PÅBUD OM TILSLUTNING TIL CENTER FOR CYBERSIKKERHEDS NETSIKKERHEDSTJENESTE

Med udkastet vil der blive skabt mulighed for, at Center for Cybersikkerhed i særlige tilfælde kan påbyde særligt samfundsvigtige virksomheder eller myndigheder at blive tilsluttet centrets netsikkerhedstjeneste (udkastets § 3, stk. 4).

Netsikkerhedstjenesten er en samlebetegnelse for Center for Cybersikkerheds aktiviteter i forbindelse med at opdage, analysere og bidrage til at imødegå sikkerhedshændelser (sikkerhedshændelser er i udkastets § 2 defineret som hændelser, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester). Netsikkerhedstjenesten omfatter alle de kapaciteter ved Center for Cybersikkerhed, der på forskellig vis bidrager til monitorering, herunder CERT (Computer Emergency Response Team), aktiviteter på det civile og militære område, sikkerhedstekniske aktiviteter samt støttefunktioner (jf. de særlige bemærkninger til § 1, nr. 1).

Virksomheder og myndigheder, der varetager samfundsvigtige funktioner, er ifølge udkastet navnlig 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, 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

Imidlertid omfatter begrebet også virksomheder, som ikke i sig selv er samfundsvigtige, men som kan være vigtige ud fra et sikkerhedsperspektiv, for eksempel fordi deres servere er blevet inficeret gennem et cyberangreb og nu anvendes som en del af en angrebsaktørs infrastruktur (jf. de særlige bemærkninger til § 1, nr. 1).

En tilslutning til netsikkerhedstjenesten indebærer, at Center for Cybersikkerhed kan monitorere en række kategorier af data, herunder pakkedata (indholdet af digital kommunikation) og stationær data (se nærmere nedenfor).

Center for Cybersikkerheds påbud om tilslutning til netsikkerhedstjenesten kan påklages administrativt til Forsvarsministeriet og kan indbringes for domstolene.

UDVIDET ADGANG TIL INDGREB I GRUNDLOVENS § 72

En af de beføjelser, som udvides med udkastet, er Center for Cybersikkerheds adgang til indgreb i meddelelseshemmeligheden uden krav om retskendelse.

Meddelelseshemmeligheden er beskyttet i grundlovens § 72 og er tillige omfattet af retten til respekt for privatliv, som beskyttet i Den Europæiske Menneskerettighedskonventions (EMRK) artikel 8.

Det følger af udkastet, at Center for Cybersikkerhed fremadrettet blandt andet skal kunne tilgå data, som opbevares på en lokal enhed (såkaldt stationær data, som er data, der opbevares på servere, cloudtjenester, pc'er, lagerenheder, netværksenheder, mobile enheder og tilsvarende jf. udkastets § 2, nr. 4).

For så vidt angår virksomheder og myndigheder, som er tilknyttet netsikkerhedstjenesten kan centret tilgå disse data uden retskendelse og uden mistanke om en sikkerhedshændelse, forudsat det understøtter et højt informationssikkerhedsniveau i samfundet (forslagets § 4).

For så vidt angår virksomheder og myndigheder, som ikke er tilknyttet, har Center for Cybersikkerhed adgang til lokale enheder (stationær data) uden retskendelse, hvis der er begrundet mistanke om en sikkerhedshændelse og den pågældende virksomhed eller myndighed enten har givet samtykke eller hvis behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet (§ 5).

Af udkastet fremgår nærmere, at stationær data kan være private data, som en medarbejder f.eks. har gemt på en pc, en arbejdsmobil eller lignende.

Forsvarsministeriet fastslår i udkastet, at indgrebet ikke er egnet til domstolsprøvelse, da indgrebet oftest vil ske automatiseret og ved scanning af ukendt data for at fastslå, om der overhovedet er tale om en sikkerhedshændelse i lovens forstand. En eventuel domstolsprøvelse vil derfor ifølge ministeriets vurdering 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 indgrebet (de almindelige bemærkninger, afsnit 3.3.2)

Den foreslåede ordning vil ikke indebære en ændring af betingelserne for, hvornår Center for Cybersikkerhed manuelt må foretage analyse af indhold af filer og kommunikation, men derimod en udvidelse af, hvilke filer og kommunikation, centret kan tilgå.

ÆNDREDE SLETTEFRISTER

Med udkastet ændres Center for Cybersikkerheds forpligtelser til at slette oplysninger markant.

Efter gældende ret skal data slettes, når formålet med behandlingen er opfyldt. Endvidere følger det af gældende ret, 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.

Fremadrettet vil centret i medfør af udkastet have en slettefrist på 5 år ved konstaterede sikkerhedshændelser og 3 år for data, der ikke knytter sig til en sikkerhedshændelse.

Data omfattet af den nye 3 års frist (som altså ikke er knyttet til en sikkerhedshændelse) vil ifølge udkastet stamme 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 (jf. de almindelige bemærkninger, afsnit 3.8.3.2).

FORSVARSMINISTERIETS VURDERING AF UDKASTET EFTER DEN EUROPÆISKE MENNESKERETTIGHEDSKONVENTION

I udkastet vurderer ministeriet, at de foreslåede ændringer er forenelige med artikel 8 om respekt for privatlivet i Den Europæiske Menneskerettighedskonvention (EMRK).

Ministeriet vurderer i den forbindelse, at den praksis, som Den Europæiske Menneskerettighedsdomstol (EMD) har udviklet vedrørende indgreb i meddelelseshemmeligheden, ikke kan finde anvendelse på centrets behandling af personoplysninger.

Ministeriet anfører i de almindelige bemærkninger, afsnit 4:

> ”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. […] De indgreb i meddelelseshemmeligheden, som uundgåeligt foretages af centeret […], vurderes på den baggrund at indebære et mindre intensivt indgreb i privatlivet end de indgreb, der foretages med henblik på at udfinde målpersoner.”

INSTITUTTETS BEMÆRKNINGER

UDVIDET ADGANG TIL PERSONOPLYSNINGER MV.

Instituttet bemærker indledningsvist, at udkastet varetager det væsentlige og anerkendelsesværdige formål at sikre Danmark mod cybertrusler i form af blandt andet cyberspionage, cyberkriminalitet og infrastrukturangreb og at sikre, at Danmark har et højt cybersikkerhedsniveau.

Udkastet lægger op til betydelige kompetenceudvidelser for Center for Cybersikkerhed på en række områder, blandt andet: 1. adgang til at meddele påbud om tilslutning til netsikkerhedstjenesten med den følge, at centret har adgang til en stor mængde data i form af trafikdata, pakkedata og stationær data, 2. adgang til stationær data hos virksomheder og myndigheder, der ikke er tilsluttet netsikkerhedstjenesten, og 3. lempeligere slettefrister.

Hertil kommer en adgang til oplysninger, som retten kan pålægge virksomheder at udlevere om brugeren af en e-mailkonto, ip-adresse eller et domænenavn til centret (edition). I straffeprocessuel sammenhæng kræver edition mistanke om en strafbar lovovertrædelse. I de foreslåede regler vil der derimod alene være krav om, at oplysningerne skal kunne medvirke til at afdække sikkerhedshændelser.

Disse udvidelser kan hver for sig og samlet føre til indgreb i retten til respekt for privatliv, beskyttet i EMRK artikel 8.

Alt i alt kommer Center for Cybersikkerhed til at være i besiddelse af en betydelig mængde data, blandt andet personoplysninger (herunder følsomme personoplysninger), end centret hidtil har haft beføjelse til at indsamle og behandle.

Center for Cybersikkerheds adgang til at påbyde tilslutning til netsikkerhedstjenesten er betinget af, at en virksomhed eller en myndighed af centret anses for at varetage samfundsvigtige funktioner.

Samfundsvigtige virksomheder og myndigheder som defineret i udkastet er en ganske vid kategori, uden nærmere kvalificerede kendetegn. Påbudskompetencen kan således få et bredt anvendelsesområde på tværs af sektorer.

En tilknytning til netsikkerhedstjenesten indebærer, at centret har adgang til langt mere data om virksomheder og myndigheder og disses medarbejdere, end hvad der har været adgang til efter gældende ret (i form af trafikdata, pakkedata og stationær data). Denne adgang er ikke betinget af retskendelse eller noget mistankekrav om en sikkerhedshændelse men skal alene understøtte et højt informationssikkerhedsniveau i samfundet (§ 4).

For så vidt angår virksomheder og myndigheder, der ikke er tilknyttede, har centret ligeledes en vid adgang til oplysninger – uden retskendelse – hvis der er en begrundet mistanke om en sikkerhedshændelse. I disse tilfælde skal centret (i fraværet af samtykke) blot vurdere, at behandlingen understøtter et højt informationssikkerhedsniveau i samfundet (§ 5, nr. 2).

Instituttet bemærker, at kravet om, at behandlingen af oplysninger understøtter et højt informationsniveau i samfundet ikke kan anses for en selvstændigt kvalificeret juridisk vurdering, men derimod blot er sammenfaldende med selve formålet med Center for Cybersikkerhed, jf. således lovens formålsbestemmelse, § 1.

Instituttet bemærker, at der i tilfælde, hvor virksomheden eller myndigheden ikke er tilsluttet netsikkerhedstjenesten, eller er tilsluttet efter påbud, er tale om et særligt intensiveret indgreb vis-a-vis virksomheden/myndigheden, som efter EMRK artikel 8, stk. 2, er underlagt en tilsvarende skærpet proportionalitetsvurdering.

I øvrigt bemærker instituttet, at det er tvivlsomt, om et samtykke fra virksomheden eller myndigheden, eller frivillig tilslutning til tjenesten, vil ændre på proportionalitetsvurderingen i forhold til centrets adgang til følsomme personoplysninger om medarbejdere.

Ministeriet anfører, at indgrebet efter §§ 4 og 5 ikke er egnet til domstolsprøvelse, da indgrebet skal fastslå, om der overhovedet er tale om en sikkerhedshændelse i lovens forstand.

Instituttet bemærker, at denne usikkerhed vedrørende indholdet af den identificerede data ikke nødvendigvis adskiller sig fra andre indgreb i meddelelseshemmeligheden, hvorfor der netop stilles mere eller mindre kvalificerede mistankekrav i de straffeprocessuelle regler, og hvorfor disse netop er underlagt domstolsprøvelse.

Den betydelige udvidelse af kompetencer, som udkastet vil indebære, stiller tilsvarende krav til fornødne retsgarantier. Ellers risikerer indgrebene at være i strid med retten til respekt for privatliv, som blandt andet beskyttet i EMRK artikel 8.

Efter instituttets vurdering gør det ikke i sig selv indgrebet uegnet til domstolsprøvelse, at det er forbundet med usikkerhed, om der er en sikkerhedshændelse.

Instituttet bemærker i øvrigt, at ministeriet ikke har taget stilling til, om et krav om efterfølgende retskendelse ville være muligt henset til, at indgrebet i første omgang sker automatisk.

- Instituttet anbefaler, at ministeriet i lovbemærkningerne redegør for, hvordan usikkerheden ved en sikkerhedshændelse adskiller sig fra usikkerheder, når der i øvrigt foretages indgreb i

meddelelseshemmeligheden samt overvejer at indsætte et krav om efterfølgende retskendelse
- Uanset om ministeriet indarbejder anbefalingen om efterfølgende retskendelse, anbefaler instituttet, at kravet om adgang til stationær data fra myndigheder og virksomheder, der ikke er tilsluttet netsikkerhedstjenesten eller som er tilsluttet ved et påbud, skærpet betydeligt og ikke blot betinges af et krav, der har samme ordlyd, som centrets formålsbestemmelse i § 1.

LEMPELIGERE SLETTEFRISTER

Adgangen til data skal tillige ses i lyset af slettefristerne, som yder en retsgaranti i tilfælde, hvor en myndighed har videregående beføjelser til personoplysninger.

Instituttet anerkender, at det er væsentligt, at Center for Cybersikkerhed er i besiddelse af de fornødne oplysninger for effektivt at beskytte mod cyberangreb.

Imidlertid skal centrets vide – og længerevarige – adgang til oplysninger være proportionalt med formålet hermed.

Navnlig for så vidt angår adgangen til fremadrettet at opbevare oplysninger, som ikke vedrører en sikkerhedshændelse i 3 år i stedet for 13 måneder kan dette efter instituttets vurdering føre til et uproportionalt indgreb.

Instituttet bemærker i den forbindelse, at der allerede ved en lovændring af 11. juni 2014 (L 192), skete en betydelig udvidelse fra den dagældende slettefrist på 14 dage til 13 måneder.[1]

- Instituttet anbefaler, at ministeriet i lovbemærkningerne nøje redegør for, hvorledes det vil sikres, at en udvidelse af slettefristen fra 13 måneder til 3 år ikke vil føre til uproportionale indgreb i retten til respekt for privatliv.

CENTER FOR CYBERSIKKERHEDS ORGANISERING

Center for Cybersikkerhed er organiseret under Forsvarets Efterretningstjeneste (FE).

Instituttet skal i den forbindelse på ny fremhæve de principielle bekymringer, som instituttet tidligere har rejst i forhold til Center for

[1] Se instituttets høringssvar til den dagældende ændring her: https://menneskeret.dk/sites/menneskeret.dk/files/media/researchpublications/hoeringssvar/hoeringssvar_afgivet_i_2014/marts%202014/marts_2014_tilgaengeligt/24_b_center_for_cybersikkerhed.pdf

Cybersikkerheds placering under FE, når centret varetager centrale, civile samfundsstrukturer.[2]

Det eneste retsgrundlag, som adskiller deling af oplysning fra Center for Cybersikkerhed til FE's efterretningsfunktioner er en vejledning fra Forsvarsministeriet.

Instituttet har tidligere fremhævet det betænkelige ved, at der ikke på lovniveau er sikret en retssikkerhedsmæssig garanti imod videregivelse af oplysninger fra centret til FE til brug for efterretningstjenestens øvrige arbejde inden for det militære område.

Disse principielle bekymringer får fornyet aktualitet ved en udvidelse af centrets beføjelser – navnlig i fraværet af effektive retsgarantier (som domstolsprøvelse og skærpede slettefrister).

- Instituttet anbefaler, at der i udkastet indføres en bestemmelse om betingelserne for videregivelse af data fra centret til resten af Forsvarets Efterretningstjeneste, således at forholdet reguleres på lovniveau.

Netop på grund af centrets placering under FE skal instituttet i øvrigt bemærke, at centerets indsamling og håndtering af personoplysninger skal vurderes i lyset af den retspraksis fra EMD, som vedrør efterretningstjenesters adgang til og behandling af personoplysninger. Instituttet er således ikke enig i, at centerets adgang til personoplysninger er et mindre intensivt indgreb, end indgreb foretaget i øvrigt af politiet og efterretningstjenesterne.

Instituttets bemærker i den forbindelse, at EMD's praksis og betingelserne etableret heri, naturligvis skal anvendes tilpasset til det formål og de opgaver, som Center for Cybersikkerhed varetager.

- På grund af Center for Cybersikkerheds organisatoriske placering under Forsvarets Efterretningstjeneste anbefaler instituttet, at ministeriet i lovbemærkningerne redegør for centrets adgang til personoplysninger i lyset af den relevante praksis fra Den Europæiske Menneskerettighedsdomstol om efterretningstjenesterne.

Der henvises til ministeriets sagsnummer 2018/006599.

Med venlig hilsen

Marya Akhtar
SPECIALKONSULENT

[2] Ibid.

Til Forsvarsministeriet (Sag 2018/006599)

KL-svar på høring af forslag til lov om ændring af lov om Center for Cybersikkerhed

Dato: 5. februar 2019

Sags ID: SAG-2019-00318
Dok. ID: 2710582

E-mail: BETR@kl.dk
Direkte: 3370 3064

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Overordnet mener KL, at lovforslaget og den tilhørende tekst indeholder gode intensioner ift. at give de kommunale myndigheder bedre muligheder i arbejdet med cybersikkerhed.

Dog skal nævnes en bekymring, idet lovforslaget lægger op til, at Center for Cybersikkerheds netsikkerhedstjeneste uden retskendelse kan behandle trafikdata, pakkedata og stationære data hidrørende fra tilsluttede myndigheder og virksomheder med begrundelse om at understøtte et højt informationssikkerhedsniveau. KL er naturligvis ikke bekendt med de trusler, der måtte være, men finder det afgørende, at borgere er trygge ved offentlige myndigheders håndtering af følsomme personoplysninger, hvilket bl.a. også har været bærende for samarbejdet med Sundhedsministeriet om cyberstrategi for sundhedsområdet. Det er KL's opfattelse, at især ønsket om adgang til stationære data kan være med til at svække borgernes tillid til, at følsomme oplysninger, som de har afgivet i f.eks. et behandlingsforløb, vil kunne tilgås af Center for Cybersikkerhed (CFCS) uden hverken medarbejdere eller borgeres viden og uden retskendelse.

Samarbejde på tværs af sektorerne
Forsvarsministeriet lægger op til at øge antallet af myndigheder og virksomheder, der tilsluttes netsikkerhedstjenesten, for at understøtte et højt informationssikkerhedsniveau i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af. På baggrund af høringsmaterialet er det uklart, i hvilket omfang kommunerne vil blive omfattet, og /eller om det er noget, kommunerne evt. vil skulle anmode om. Det ser ud til, at man også kan blive afvist. Der synes således at være tvivl om kommunernes status ift. det tværgående samarbejde om cybersikkerhed.

I forbindelse med arbejdet med høringen er der opstået tvivl om en række af de juridiske og tekniske forhold omkring det at være tilsluttet netsikkerhedstjenesten. Det er tvivl ift. kommunernes mulighed for risikovurdering af egen it-portefølje, sammenhængen mellem databeskyttelsesloven og evt. udlevering af personoplysninger til CFCS, hvor der er krav, der skal overholdes. Overvejelser om erstatningsansvar, såfremt det er nettjenesten, der er årsag til kompromittering af borgerdata og sammenhængen med Datatilsynets udmeldinger om evt. overtrædelser af meddelelseshemmeligheden, krænkelser af medarbejderes private data mv.

Endelig synes der at være tvivl omkring underretning af bl.a. medarbejdere. Det fremgår både, at medarbejderne hos en myndighed ikke på forhånd bør blive orienteret om, at der gennemføres en sikkerhedsteknisk undersøgelse, end ikke generelt. Der kan orienteres efterfølgende efter aftale med CFCS , men samtidig fremgår det som en del af tilslutningsaftalen mellem CFCS og myndigheden, at der skal ske orientering af medarbejderne om monitoreringen.

Ovenstående synes også umiddelbart at stå i modsætning til Datatilsynets praksis, hvorefter det er den absolutte hovedregel, at de registrerede på forhånd er orienterede om logning og mulig brug heraf. Det er desuden generelt beskrevet som god databehandlingsskik.

KL indgår gerne i dialog om ovenstående. Det har ikke været muligt at behandle lovforslaget politisk, hvorfor der tages forbehold for politisk behandling i KL.

Med venlig hilsen

Pia Færch
Kontorchef
Digitalisering og Teknologi

E-mail: BETR@kl.dk
Direkte: 3370 3064

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Københavns Byret

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Præsidenten
Domhuset, Nytorv 25
1450 København K.
Tlf. 99 68 70 15
CVR 21 65 95 09
administration.kbh@domstol.dk
J.nr. 9099.2019.7

Den 1. februar 2019

Ved en mail af 7. januar 2019 har Forsvarsministeriet anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af Cybersikkerheden).

Jeg skal i den anledning på byretspræsidenternes vegne oplyse, at byretterne har følgende bemærkninger:

Ved afgørelse om edition efter lovudkastets § 7, jf. § 7 a, vil retten kunne meddele pålæg om edition med hensyn til tre præcist afgrænsede oplysninger: oplysning om brugeren af en e-mailkonto, brugeren af en ip-adresse eller brugeren af et domænenavn. Det fremgår af bemærkningerne til lovudkastet p. 29 blandt andet, " at udlevering af oplysninger om brugen af en e-mailkonto, ip-adresse eller et domænenavn ikke vurderes at udgøre et indgreb i meddelelseshemmeligheden". Dette er i overensstemmelse med retspraksis, jf. UFR 2005. 777 V, og UFR 2007.22Ø. Retten skal efter lovudkastet påse, om editionen skal tjene til at afdække en sikkerhedshændelse.

Efter retsplejelovens editionsregler kan anklagemyndigheden indhente samme type – men også en lang række andre – oplysninger, hvis der er grund til at antage, at oplysningerne kan tjene som bevis, bør konfiskeres eller ved lovovertrædelse er fravendt nogen, som kan kræve dem tilbage.

Behandling af editionsbegæringer efter retsplejeloven foregår uden medvirken af indgrebsadvokat.

Henset til den meget nøje afgrænsning af karakteren af oplysninger i lovudkastets § 7, stk. 1, sammenholdt med, at oplysningerne skal tjene til at afdække en sikkerhedshændelse, ses der ikke at være grundlag for at fravige det udgangspunkt, som er fastlagt i retsplejeloven, hvorefter der ved behandlingen af sådanne pålæg ikke medvirker indgrebsadvokat.

Det tilføjes, at editionspålægget hviler på en forudsætning om, at man ikke har kendskab til, hvem der er bruger af den pågældende e-mailkonto, ip-adresse eller domænenavn. Bestemmelsen i forslaget § 7, stk. 2, forekommer derfor ikke relevant.

Der henvises til Deres j.nr. 2018/006599.

Med venlig hilsen

Søren Axelsen

Forsvarsministeriet
Holmens Kanal 9
1060 København K

fmn@fmn.dk, tbl@fmn.dk, sbu@fmn.dk

Sagsnummer 2018/006599

København
den 4. februar 2019

Ledernes høringssvar på høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed

Ledernes Hovedorganisation har den 7. januar 2019 modtaget høring om udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden).

Ledernes Hovedorganisation anerkender og støtter fuldt ud formålet med lovforslaget og hensynet bag.

Det er dog vores vurdering, at lovforslaget har for vidtrækkende konsekvenser for privat- og offentligt ansatte, som i værste fald risikerer deres ansættelse som følge af en lovligt sat fælde. Dertil kommer, at ledelser i danske virksomheder, regioner og kommuner kan pålægges at medvirke til at bringe deres medarbejdere i denne situation. Ledernes Hovedorganisation foreslår på den baggrund, at lovforslaget justeres på disse punkter.

Lederne Hovedorganisation har følgende konkrete bemærkninger til lovforslaget

Især er lovforslagets bestemmelse om såkaldt "spear-phishing", jf. lovforslagets § 6a, stk. 2, betænkelig, idet bestemmelsen giver Center for Cybersikkerhed adgang til at lægge en individualiseret, personaliseret og målrettet fælde for udvalgte medarbejdere for at kunne afdække sikkerhedsbrister i virksomheden, med henblik på at kunne lukke sådanne brister og højne sikkerheden. Spear-phishing foregår ifølge bemærkningerne ved, at centret udgiver sig for at være en af medarbejderne kendt person/kollega, som beder pågældende om at foretage en handling, som er i strid med cybersikkerheden. Ifølge lovforslagets bemærkninger skal spear-phishingen bevidst foregå med den intention og det mål at få modtageren til at hoppe i fælden og bryde cybersikkerheden.

Formålet med spear-phishing anerkendes af Ledernes Hovedorganisation, men metoden anses for særdeles betænkelig, idet intetanende medarbejdere – uden forudgående orientering eller samtykke og uden, at der i øvrigt foreligger mistanke om sikkerhedsrisiko hos pågældende – på den beskrevne vis, narres til at afsløre sig selv som en sikkerhedsbrist. Som konsekvens heraf risikerer den pågældende medarbejder sit ansættelsesforhold, såfremt ledelsen på virksomheden vurderer, at sikkerhedsbristen er af en karakter som kan begrunde en opsigelse eller bortvisning, hvilket fremgår udtrykkeligt af bemærkningerne til lovforslaget.

Ledernes
Hovedorganisation

Vermlandsgade 65
2300 København S
Telefon 3283 3283

www.lederne.dk

I forhold til ledelsen på de berørte virksomheder finder Ledernes Hovedorganisation det tillige betænkeligt, at disse skal medvirke til at narre deres medarbejdere og potentielt bringe disse i en situation, hvor de kan miste deres arbejde. En ledelseskultur, hvor ledelsen aktivt bidrager til at få deres medarbejdere til at falde i en fælde med alvorlige konsekvenser, er ikke ønskelig på det danske arbejdsmarked, hvor forholdet mellem ledelse og medarbejdere i høj grad er præget af og båret af tillid.

Evt. spørgsmål kan rettes til teamchef og advokat Rikke Agervig Helles.

Med venlig hilsen

Berit Toft Fihl
Politisk sekretariatschef

PROSA
Forbundet af It-professionelle

Association of IT Professionals
Vester Farimagsgade 37A
1606 København V

Søren Frichs Vej 38K
8230 Åbyhøj

Overgade 54
5000 Odense

prosa.dk
+45 33 36 4141

Forsvarsministeriet
Holmens Kanal 9
1060 København K
fmn@fmn.dk
Cc: tbl@fmn.dk, sbu@fmn.dk

København, 4. februar 2019

Høringssvar om *Initiativer til styrkelse af cybersikkerheden (2018/006599)*

Forsvarsministeriet har udsendt udkast til ændring af lov om Center for Cybersikkerhed (CfCS). PROSA – Forbundet af It-professionelle er blevet inviteret til at udtale sig om udkastet.

Test af sikkerhed

Lovforslaget lægger op til at teste de tilsluttede organisationers sikkerhed.

Ligesom det er en god idé at tjekke, at fødevarereglerne overholdes, så er det også en god idé at teste, at organisationerne lever op til de IT-forskrifter, som de har forpligtet sig til.

Det skal naturligvis ske på en ansvarlig måde: Det giver ikke mening at lave en penetrationstest på en organisation, hvor ledelsen ikke har prioriteret at leve op til forskrifterne. Ledelsen bør jævnligt afholde beredskabsøvelser, hvor sikkerheden testes, og CfCS kunne være med til at afholde disse.

Vi betragter grundlæggende IT-sikkerhed på linje med GDPR som et ledelsesansvar, hvorfor vi som udgangspunkt mener, at evt. sanktioner i forbindelse med test af IT-sikkerhed skal lægges på ledelsen. En undtagelse kan være, hvis en medarbejder handler i ond tro, hvilket vi mener, eksisterende lovgivning dækker fint.

I øvrigt finder PROSA det bekymrende, at en statslig myndighed skal have mulighed for at optræde under fordækte identiteter, anspore ansatte til ulovligheder, få dén medarbejder, hvis identitet de har overtaget, til at "reagere hensigtsmæssigt", hvis den berørte medarbejder henvender sig, og dermed er med til at kompromittere en kollega og i det hele taget, at det skal være nødvendigt med dén slags beføjelser for at sikre et fornuftigt sikkerhedsniveau i danske virksomheder og institutioner.

Stor udvidelse af beføjelser

Lovforslaget lægger op til en drastisk udvidelse af CfCS' beføjelser. Således vil CfCS installere sikkerhedssoftware på såvel servere som klienter. Dette er for at kunne monitorere data, der sendes krypteret. Sikkerhedssoftware vil også kunne tilgå harddiskene på disse maskiner.

Det betyder i princippet, at CfCS vil kunne læse:

- Alle data, der flyder ind og ud af organisationen
- Alle data, der ligger på alle harddiskene

Oven i dette vil CfCS kunne tvinge organisationer til at tilslutte sig.

Dette er væsentligt udvidede beføjelser til CfCS virke. Forventeligt vil CfCS ikke misbruge disse beføjelser og vil næppe heller kræve udrulning af sikkerhedssoftwaren på alle maskiner hos alle tilsluttede, men loven giver disse beføjelser, hvilket i sig selv er problematisk.

Alle æg i én kurv

Der findes ikke 100 % sikkerhed. Det tilbyder CfCS da heller ikke. Derfor bør man overveje, hvad der vil ske, hvis CfCS bliver kompromitteret – det kan f.eks. ske via et digitalt angreb eller via medarbejdere, som bliver afpresset.

Et velkendt eksempel er Stuxnet, som var en virus, der blev udviklet til at angribe iranske uranberigelsescentrifuger, og som det lykkedes at få ind i berigelsesanlægget på trods af de skrappe sikkerhedsforanstaltninger, der helt sikkert har været. Et succesfuldt angreb er derfor ingenlunde et utænkeligt scenarie. Med de muligheder, som sikkerhedssoftwaren giver, vil muligheden for at kunne få adgang til at fjernstyre sikkerhedssoftwaren være et meget værdifuldt mål, som man sagtens kunne forestille sig, at organisationer med budget som nationalstater ville prioritere. PROSA er bekymret for, at ved at putte alle æg i én kurv, så udsætter man sig for en unødig risiko.

En bedre løsning vil være at gøre, som vi gør med bankerne: Her er der ikke én enkelt organisation, der har adgang til alle bankers data. Derimod er der skarpt opdelte organisationer, så hvis én bank bliver kompromitteret, så vil det ikke betyde, at alle andre banker samtidigt er kompromitterede.

CfCS's rolle kunne da være at hjælpe med at sikre de forskellige organisationer, uden at CfCS selv ville få adgang til udstyret.

Mangel på transparens

CfCS ligger under Forsvarets Efterretningstjeneste (FE). Det er helt naturligt, at der nødvendigvis må være et center under FE, som kan udveksle hemmeligt stemplede informationer med udenlandske efterretningstjenester. Det er fuldt forståeligt, at befolkningen ikke kan få adgang til visse informationer, som efterretningstjenesterne indhenter.

Men centerets virke bør være begrænset til de elementer, som *kun* kan varetages af en efterretningstjeneste – de elementer, der kan varetages af et ikke-militært center, bør ligge i en civil del, der ikke er underlagt samme begrænsninger i indsigt.

Rollen som Danmarks nationale IT-sikkerhedsmyndighed og nationalt kompetencecenter mener PROSA bedre ville kunne varetages uden for efterretningstjenesterne (f.eks. som et center under Indenrigsministeriet). Derved kan borgerne få indsigt i omfanget af centerets virke – en indsigt som borgerne er frataget ved at lægge centeret under FE.

PROSA foreslår derfor, at man, i stedet for at give CfCS meget vidtgående beføjelser, opdeler CfCS i et civilt CfCS (f.eks. under Indenrigsministeriet) og i et militært CfCS (som forbliver under FE). Det civile center vil da kunne blive det nationale kompetencecenter, der hjælper myndigheder og virksomheder med at sikre deres IT-infrastruktur. En udveksling af viden mellem de to centre vil selvfølgelig være en naturlig del, men vi ser ingen grund til, at de dele, der er uproblematiske at give befolkningen indsigt i, tilbageholdes med henvisning til, at centeret hører under FE.

Opsummering

Det er PROSAs opfattelse, at frem for at udstyre CfCS med så omfattende beføjelser i en organisation uden nævneværdig demokratisk kontrol bør centerets opgave være at opstille sikkerhedskriterier og niveauer for de virksomheder og institutioner, som arbejder med samfundskritiske opgaver. Herudover kunne der være en opgave med at kontrollere, at de pågældende sikkerhedsforskrifter overholdes, evt. gennem et samarbejde med virksomheder, som udbyder digitale sikkerhedsløsninger. Herved undgås, at der sker en centralisering af data med en øget sårbarhed til følge, og det giver de enkelte virksomheder og institutioner mulighed for selv at vælge, hvilke sikkerhedssystemer der passer til deres forretning.

Venlig hilsen

Niels Bertelsen

Formand

R E T S P O L I T I S K F O R E N I N G

HØRINGSSVAR

Til: Forsvarsministeriet.

Høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed

Høringsbrev fra 7. januar 2019 - med svarfrist 4. februar 2019

Svar til: fmn@fmn.dk og tbl@fmn.dk og sbu@fmn.dk - Att: Sagsnr. 2018/006599

Retspolitisk Forening kan uden videre erkende, at den moderne IT-baserede kommunikation skaber voldsomme udfordringer for både virksomheder, private og offentlige myndigheder. Samtidig ophobes et uendeligt antal informationer af følsom karakter om borgerne. Det er derfor indlysende, at der er behov for beskyttelse og overvågning af såvel ind- som udgående datamængder for at forhindre, at uvedkommende kan tilegne sig disse oplysninger. Der imidlertid væsentlige retssikkerhedsmæssige interesser knyttet til den måde, hvorpå overvågning, opbevaring, videregivelse og sletning sker.

Foreningen har tidligere den 3. marts 2014 i et høringssvar over forslaget til lov om Center for Cybersikkerhed udtalt sig kritisk om placeringen af styrkelsen af cybersikkerheden under Forsvarets Efterretningstjeneste. Denne kritik står foreningen fortsat ved, men finder ikke anledning til her at gentage argumentationen. Lovudkastet er tydeligvis en opfølgning af CFCS' bidrag af 12. juni 2017 til evaluering af lov om cybersikkerhed. Vi finder det imidlertid nødvendigt at påpege, at det ved forslagets udformning hverken ses eller synes overvejet, hvilke konsekvenser det ville eller kunne have for en virksomhed at blive inddraget under nyordningen, hvis virksomheden eksporterer sine produkter og/eller samarbejder med virksomheder i udlandet. I lyset af den udvikling, som er i gang i flere lande, herunder også i Danmark, omkring det kinesiske it- og kommunikationsselskab Huawei og dets mulige relationer til kinesiske efterretningstjenester hverken kan eller bør dette aspekt imidlertid efter foreningens opfattelse ignoreres.

Herefter har Retspolitisk Forening følgende bemærkninger til det fremsendte lovudkast:

Ad nr. 1 § 3.
Foreningen har ikke bemærkninger til denne bestemmelses stk'erne 1-3, der er baseret på et frivillighedsprincip. Der er således ikke noget behov for rettens medvirken uanset, at aftalen er et brud på meddelelseshemmeligheden. Myndigheder, virksomheder og andre er formentlig opmærksomme på de gældende regler om beskyttelse af personlige oplysninger.

Bestemmelsens stk. 4, hvorefter Center for Cybersikkerhed i særlige tilfælde skal kunne påbyde virksomheder, kommuner og regioner, der har særlig samfundsvigtig karakter at blive tilsluttet netsikkerhedstjenesten. Det fremgår ikke af lovudkastets almindelige bemærkninger eller af bemærkningerne til bestemmelsen (s. 53), hvilke særlige tilfælde, der er tænkt på udover, at en aftale ikke kan opnås.

Foreningen skal anbefale, at det tydeliggøres, i hvilke situationer bestemmelsen er tænkt anvendt samt, at der indføjes et krav om indhentning af rettens kendelse om tilslutning efter påbud. Det forekommer retssikkerhedsmæssigt utilstrækkeligt at pege på administrativ rekurs til Forsvarsministeriet med efterfølgende mulighed for domstolsprøvelse. Dette ønske understreges af det forhold, at centrets virksomhed ikke er omfattet af forvaltningslovens begrundelseskrav. Man kan således forestille sig, at et hospital uden begrundelse må acceptere et påbud om tilslutning.

Ad nr. 3 § 4.
Det anføres i bestemmelsen, at Center for Cybersikkerheds netsikkerhedstjeneste uden retskendelse kan 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. (Retspolitisk Forenings kursivering). Det fremgår ikke af lovudkastets bemærkninger, hvad der menes med "et højt informationsniveau i samfundet". Det anføres (s. 55), at:

> "Netsikkerhedstjenesten har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser os 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".

Dette forekommer ikke som en tydeliggørelse af, hvad der skal forstås ved et højt informationsniveau i samfundet.

Tilsvarende gælder, når dette kriterium anføres som grundlag for indgreb efter § 5 stk. 1 nr. 2 og § 6 stk. 1 selvom der her gælder et skriftligt samtykkekrav og efter § 6 et krav om forudgående tilslutning.

Ad nr. 6-11.
Foreningen har ingen bemærkninger.

Ad nr. 12 § 16 stk. 3 nr. 3.
Foreningen har ingen bemærkninger til videregivelse til fremmede netsikkerhedstjenester, såfremt det sikres, at der ikke videregives personoplysninger, der er modtaget i medfør af §§ 6 b og 6 c.

Ad § 17, stk. 2, nr. 1-2.
Foreningen anbefaler, at personoplysningerne indeholdt i data, der hidrører fra sikkerhedshændelser, anonymiseres efter 1 år. De i stk. 2, nr. 1 angivne frister bør nedsættes til 3 år.

Foreningen har ikke yderligere bemærkninger til lovudkastet.

København, den 4. februar 2019

Bjørn Elmquist	Leif Hermann
Formand	bestyrelsesmedlem

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Rådet for Digital Sikkerheds høringssvar til Lov om ændring af Lov om Center for Cybersikkerhed

Rådet for Digital Sikkerhed (herefter Rådet) takker for muligheden for at afgive bemærkninger til udkastet til Lov om ændring af Lov om Center for Cybersikkerhed, som er sendt i offentlig høring d. 8. januar d.å.

Rådet har først og fremmest noteret sig, at regeringen har god fokus på informations- og cybersikkerhed. Der er gennem det seneste år iværksat mange gode tiltag. Finansministeriets strategi for cyber- og informationssikkerhed, Digitaliseringsstyrelsens portal Sikker Digital, Erhvervsstyrelsen og Rådets Sikkerhedstjekket, Erhvervsstyrelsens Privacy-kompas, som er ved at blive moderniseret, Justitsministeriets revision af Lov om TV-overvågning, Sektorstrategierne for sikkerhed og senest men ikke mindst nu revisionen af Lov om Center for Cybersikkerhed. Rådet er meget tilfredse med regeringens fokus. Det er afgørende for, at borgerne kan have tillid til digitalisering af samfundet, at der er god fokus på informationssikkerhed i både den offentlige og private sektor. Alle regeringens tiltag bidrager på forskellig vis hertil.

Rådets skal med dette brev komme med sine bemærkninger til ovennævnte lov.

Bemærkninger til Lov om ændring af Lov om Center for Cybersikkerhed

Rådet har overordnet noteret sig, at Center for Cybersikkerhed (herefter CFCS) har et ønske om at udvide sine muligheder for at gribe ind forskellige steder i den digitale infrastruktur med det formål at understøtte et højt informationssikkerhedsniveau ved at opdage, analysere og bidrage til at imødegå sikkerhedshændelser. Rådet mener, at de udfordringer CFCS søger at løse er af kritisk betydning for rigets sikkerhed og stabilitet, hvorfor vi støtter op om behovet for at øge sikkerheden på den kritiske infrastruktur, hvor dette lovforslag er en ud af flere potentielle løsninger. Rådet mener samtidig, at det er vigtigt løbende at vurdere, om CFCS har de rette midler for at beskytte danske interesser i lyset af den teknologiske udvikling tillige med udviklingen i trusselsbilledet. Det er ved en sådan vurdering helt centralt, at midlerne er proportionale henset til borgernes fundamentale rettigheder i et demokratisk samfund og private virksomheders

interesser og behov for at holde deres data fortrolige. En række af de midler, som fremgår af lovforslaget, kan i Rådets optik ikke anses for at leve op til et sådant proportionalitetsprincip.

Rådet bemærker dog, at hvor lovforslaget har en række fundamentale problemer, så er den underliggende problemstilling, der søges adresseret af en sådan vigtighed, at det er afgørende, at der findes holdbare løsninger hertil. Hvor det er Rådets opfattelse, at lovforslaget som det foreligger ved høringen ikke er denne løsning, kan elementer heraf alligevel danne inspiration for løsninger. Eksempelvis kunne man overordnet opnå den underliggende målsætning ved at 1) Sætte minimumskrav til sikkerhed og beredskab for de organisationer, der indgår i den kritiske infrastruktur; 2) Opsætte CFCS services til krypteret modtagelse af relevante anonymiserede sikkerhedshændelser og/eller logninger; 3) Opsætte en statslig pulje af økonomiske midler til finansiering af de nødvendige tiltag og værktøjer ude i de enkelte organisationer. På denne vis opnås det ønskede formål, samtidig med at virksomheder og privates rettigheder respekteres, og tilgang til reel data stadig kan betinges af en dommerkendelse.

Med en sådan alternativ tilgang i tankerne findes nedenfor Rådets øvrige bemærkninger til lovforslaget, som det foreligger ved høringen.

Sikkerhedssoftware og adgang til stationære data
Forslagets § 3, stk. 1 indebærer jf. bemærkningerne p. 50, at CFCS fremadrettet skal kunne monitorere de tilsluttedes forbindelse til internettet, skal kunne installere sikkerhedssoftware på lokale enheder hos de tilsluttede og overføre oplysninger fra den tilsluttedes egne sikkerhedssystemer til CFCS. Videre fremgår det af § 4, at der lægges op til, at CFCS får adgang til stationære data – foruden de trafik- og pakkedata, som CFCS allerede har adgang til. I § 15 lægges der videre op til, at CFCS kan foretage automatiserede analyser af trafikdata, pakkedata og stationære data. Disse kan suppleres af manuelle analyser.

Rådet noterer sig, at det er en betydelig udvidelse af de beføjelser, som CFCS har i dag. I dag kan CFCS alene opsamle trafik- og pakkedata på ydersiden af den tilsluttedes firewall. I fremtiden er det med forslaget tanken, at CFCS kommer dybt ind i den tilsluttedes infrastruktur og kan tilgå alle data. CFCS vil dermed få adgang til forretningshemmeligheder, alle oplysninger om ansatte, kunder og borgere, de ansattes private filer m.v. Rådet har noteret sig, at CFCS ikke får adgang til internetudbydernes kunders kommunikation og dermed som udgangspunkt ikke borgernes private kommunikation med hinanden.

I forslaget præciseres det ikke, hvilken sikkerhedssoftware CFCS har i tankerne at installere i de tilsluttede myndigheder og virksomheders infrastruktur. Der gives dog flere steder indikationer af softwarens funktionalitet[1], der bl.a. omfatter:

[1] "unormal aktivitet" (p. 12), "blokere, omdanne eller omdirigere" (p. 16), "reagere på kendte signaturer" (p.17), "opdage uregelmæssigheder… på enkelte enheder (f.eks. pc'er)" (p. 18) og "servere, smartphones og tablets" (p. 18), "beskyttelse af netværk, der ikke er forbundet til internettet" (p. 18), "tilgå data, som opbevares på en lokal enhed" (p. 18), sammenligning med "antivirus-software" (p. 19), "uregelmæssigheder i de processer, der er aktiveret på enheden eller i de netværk, som enheden er tilknyttet" (p. 19), "opdage afvigelser fra normalbilledet" (p. 19), "forebyggende sikkerhedstekniske undersøgelser… [der]… afdække[r] områder og sårbarheder (p. 21), "simuleret

Logopsamling fra systemer og end-points og opsamling af flowdata på indersiden af firewallen, således at der kan reageres på baggrund af på forhånd definerede genkendelse af trafikmønstre og angrebsvektorer. Der er formodentlig desuden tale om forskellige produkter til overvågning af end-points, hvor der søges efter malware, kontakt til skadelige sider og analyseres afvigende brugeradfærd (logon på mærkelige tidspunkter, kopiering af større mængder filer, osv.). Der er videre formodentlig tale om analyse af netværkstrafik og for så vidt angår den aktive software, mulighed for at reagere på cyberangreb i realtid. På netværk og endpoints kan der søges efter bestemte signaturer. Der tales videre om at gennemføre skanninger på ydersiden af firewallen med henblik på at identificere og udnytte sårbarheder. Der tales om at overvåge systemprocesser og services. Videre nævnes der nogle få sikkerhedsteknologier eller begreber: spearphishing mails, spredning af skadelige usb-nøgler, anvendelsen af honeypots og sinkholes samt social engineering. Der er med andre ord tale om en bred vifte af teknologier med funktionalitet, som allerede udbydes af det private marked, og allerede mange steder er installeret af myndigheder og virksomheder.

Rådet finder, at anvendelsen af disse teknologier er rigtig fornuftige sikkerhedstiltag. Anvendelsen af dem bør baseres på en risikovurdering, og hvor risici tilsiger det, kan de med fordel implementeres som korrigerende foranstaltninger.

CFCS vil med disse softwareteknologier kunne få adgang til alle de tilsluttede myndigheder og virksomheders data – herunder forretningskritiske data, strategiske data, intellectual property rights, personoplysninger i form af sundhedsoplysninger, biometriske data, genetiske data, sagsbehandling relateret til etnisk tilhørsforhold, oplysninger om seksuelt, politisk, religiøst og filosofisk tilhørsforhold om ansatte hos de tilsluttede (følsomme personoplysninger) (se f.eks. bemærkningerne p. 18, 24, 61 og 62) (endda med mulige ansættelsesretlige konsekvenser), sagsbehandling om landets mest udsatte borgere (se f.eks. beskrivelsen p. 59), CPR-numre, personalefiler for de ansatte hos tilsluttede (fortrolige personoplysninger) og en lang række andre oplysninger – f.eks. fra de ansatte eller data om kunder, som er lagret (almindelige personoplysninger). Teknologierne kan således i vid udstrækning anvendes til at krænke privatlivets fred, som adresseret i Grundlovens § 72. I lovforslaget bemærkes det da også, at installation af software og undersøgelse af data på lokale enheder kræver særskilt lovgivning for ikke at være i modstrid med Grundlovens § 72. Udgangspunktet for § 72 er, at myndighederne ikke må krænke privatlivets fred. Helt undtagelsesvist kan der laves lovgivning, som under særligt vigtige omstændigheder kan tilsidesætte borgerens ret efter Grundloven – f.eks. hvis politiet jager en forbryder i et hus, og ikke kan nå at indhente dommerkendelse. Der skal således foretages en proportionalitetsvurdering mellem to hensyn. Rådet bemærker, at de grænser, der i lovforslagets bemærkninger pp. 55-60 søges opstillet for CFCS adgang til de tilsluttedes data, er uklare. Rådet er således usikker på, i hvilket omfang CFCS foruden søgning med software faktisk vil have adgang til

angreb" (p. 21), "dokumentere potentielle angrebsvektorer og sårbarheder" (p. 21), "skanninger på ydersiden… i søgen efter åbne netværksadgange, tjenester og sårbare applikationer" (p. 23 og p. 60), "social engineering" (p. 23 og p. 61), "spear-phishing" mails (p. 24 og p. 61), usb-nøgler, "honeypots og sinkholes" (p. 26 og p. 62), "monitorering af netværkstrafik og monitorering via lokal sikkerhedssoftware" (p. 55), "kørende systemprocesser og services" (p. 55), "logfiler" (p. 55), "reagere på cyberangreb i realtid" (p. 58).

med andre - herunder manuelle midler - at tilgå de tilsluttedes data. Rådet bemærker videre, at denne præcisering bør fremgå af loven og ikke alene af bemærkningerne.

Foruden privacy problemet vil det for internationale virksomheder være problematisk at lagre data om udviklingsprojekter i et land, hvor efterretningstjenesten systematisk tilgår data. Tilsvarende vil det være problematisk at iværksætte udviklingsprojekter i sådanne lande. Endelig er der en risiko for, at danske virksomheder ikke kan indgå som partner i sådanne udviklingsprojekter. Der er derfor en risiko for, at internationale virksomheder vil gå uden om Danmark, når der skal besluttes, hvor udviklingsprojekter kan foregå.

Rådet mener, at de foreslåede adgange for en myndighed i en efterretningstjeneste ikke lever op til et gængs proportionalitetsprincip for et demokratisk samfund, givet mængden af kritiske data og personoplysninger der søges tilgået uden dommerkendelse. Rådet anbefaler, at det præciseres og afgrænses præcist i hvilket omfang og med hvilke midler, CFCS kan tilgå de tilsluttedes data. Videre er det en udfordring for danske virksomheder, at CFCS kigger med i fortrolige internationale projekter.

Påbud
I henhold til forslagets § 3, stk. 4 er det hensigten, at CFCS kan påbyde, virksomheder, regioner og kommuner, der har særligt samfundsvigtig karakter at blive tilsluttet netsikkerhedstjenesten. Videre følger det af § 3, stk. 4 at de parter, der har modtaget påbud skal medvirke til netsikkerhedstjenestens opsætning og drift af hardware og software.

Rådet noterer sig, at det foreslåede påbud gælder tilslutning til CFCS. Rådet skal igen bemærke, at man kunne forestille sig alternative veje til at arbejde med påbud. F.eks. kunne man give myndigheder og virksomheder indenfor kritisk infrastruktur påbud om at udarbejde risikovurderinger og/eller påbud om at installere konkrete tekniske sikkerhedsforanstaltninger, som de selv administrerer, uden at CFCS skal have adgang til data eller kun begrænset anonymiseret adgang. Det er vigtigt at overveje, hvordan man kan gøre påbud så lidet indgribende overfor data, som muligt. Slutteligt kunne man igen gøre disse tiltag statsfinansieret igennem en pulje, hvorfra virksomhederne kan søge omkostningsdækning for tilslutningsomkostninger. Dette vil bidrage til en tættere tilslutning og derved øget sikkerhed i den kritiske infrastruktur.

Rådet mener, at det bør være op den enkelte myndighed eller virksomhed, hvilke sikkerhedsforanstaltninger de ønsker at tage – herunder om de ønsker tilslutning til CFCS. Rådet anbefaler, at hvis man vil påbyde myndigheder og virksomheder sikkerhedsforanstaltninger, at dette så gøres på så lidet en indgribende måde som muligt, og hvor omkostninger hertil afholdes af staten.

Aktiv versus passiv sikkerhedssoftware
Forslagets § 6, stk. 1 lægger op til, at den software, som installeres hos myndigheder og virksomheder, kan være aktiv og blokere, omdanne eller omdirigere trafik- og pakkedata. I § 6, stk. 2 fastslås det, at tilsvarende finder anvendelse for stationære data – tillige med sletning.

Endelig lægges der i §§ 6a-c op til, at CFCS kan gennemføre sikkerhedstekniske undersøgelser, installere sikkerhedssoftware, tilgå offentlige informationer andre steder og rette forebyggelsesaktiviteter mod enkelte medarbejdere, tillige med muligheden for at gøre brug af honeypots og sinkholes.

Rådet bemærker igen, at vi ikke finder det proportionalt at gennemføre de skitserede tiltag og anbefaler i stedet alternative tilgange med samme målsætning.

Sletning ved videregivelse
I § 17 lægges der op til en forlængelse af slettefristerne.

Henset til den tid, der som gennemsnit går før en sikkerhedshændelse opdages, og i tilknytning hertil, hvor længe det tager at efterforske en sag – særligt APT-angreb, som må antage at være CFCS fokus-område – har Rådet ikke overordnet bemærkninger til de forlængede slettefrister.

I henhold til § 17, stk. 5 lægges der op til, at hvis data er videregivet, skal slettefristerne angivet i § 16 ikke gælde. Herefter gælder der jf. forslagets § 17, stk. 6, at personoplysninger skal slettes, når de sikkerhedstekniske undersøgelser er afsluttet. Det præciseres videre p. 34, at data i medfør af § 17, stk. 1 skal slettes, når formålet med behandlingen efter konkret vurdering er udtømt. Det forekommer på den baggrund uklart, i hvilket omfang videregivne data skal slettes.

Rådet mener ikke, at videregivelse kan fravige sletningskrav for data, hvis formål er opfyldt. Rådet skal derfor henstille til 1) at det fastslås at alle data – inkl. videregivne data – slettes når formålet er opfyldt og 2) at der ligesom på det persondataretlige område fastlægges et krav om underretning ved sletning, således at de aktører, til hvem data er videregivet, underrettes om at CFCS har foretaget sletning, og at modtagere derfor skal overveje, om de forsat skal lagre data.

Andre forhold
Med forslaget lægges der i § 7 samt §§ 7a-f op til at vedtage editionsbestemmelser og i § 8 op til at undtage CFCS fra Lov om retssikkerhed.

Rådet har ikke bemærkninger til disse undtagelser.

Konkurrence
I tal kan man af CFCS' årsberetning for 2017 se, at der var 39 tilslutningsaftaler fordelt på 25 civile myndigheder, 12 militære myndigheder og 2 private virksomheder[2]. I høringsmaterialets side 11 fastslås det, 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". Det lægges således til grund af Forsvarsministeriet, at fordi der er så relativt få tilslutninger, så sker der ikke en monitorering af internettrafik for avancerede cybertrusler. For at løse dette problem lægges der p. 14 op til at gøre tjenesten gratis.

[2] https://fe-ddis.dk/cfcs/publikationer/Documents/CFCS_Beretning_2017.pdf, p. 4.

Rådet vil gerne rejse tvivl om, hvorvidt mange samfundsvigtige myndigheder ikke får monitoreret deres internettrafik for avancerede trusler. Rådet er af den opfattelse, at der på det private marked findes mange sikkerhedsteknologier, der monitorerer internettrafik for avancerede cybertrusler. Rådet finder, at det er uheldigt signal, at Forsvarsministeriet ikke tillægger nogen videre vægt til den betydelige effekt disse private leverandører har på sikkerheden i Danmark. Det bemærkes, at den lavere tilslutning til CFCS ligeledes kunne skyldes, at det udbudte produkt står konkurrencemæssigt svagere på funktionalitet og/eller pris ift. det private marked, eller at CFCS' formål som efterretningstjeneste opfattes som i uoverensstemmelse med de kommercielle virksomheders interesser. Det er meget tænkeligt, at CFCS' produkt ikke foretrækkes af virksomheder og myndigheder, i forhold til alternativer fra det private marked.

Forsvarsministeriet hævder flere steder i høringsmaterialet at både de eksisterende tiltag med monitorering af trafik via sensorer såvel som de fremtidige tiltag, hvor der skal installeres software, der kan reagere aktivt og tilgå stationære data, ikke påvirker det private marked for IT-sikkerhedsprodukter og -services - f.eks. pp. 14, 16, 19, 22, 25 og 29. Argumentet som gives af Forsvarsministeriet er bl.a., at den tjeneste, som CFCS stiller til rådighed, er efterretningsbaseret, hvilket de private tjenester ikke er. Da de nødvendige tekniske tiltag for at opnå CFCS' ønskede formål er tilgængelige på det private marked, finder Rådet ikke dette argument overbevisende.

Rådet er af den opfattelse, at lovforslaget vil have en meget betydelig konkurrenceforvridende effekt. Rådet skal derfor anbefale, at CFCS i stedet for at tilbyde software, tilbyder efterretningsmæssig information og lader denne indgå i den software, der allerede findes på markedet. Konkret foreslås det, at CFCS stiller f.eks. efterretningsbaseret information om skadelige IP-adresser, signaturer af malware m.v. til rådighed for de tilsluttede myndigheder og virksomheder til indlejring i deres sikkerhedssoftware.

Rådet noterer sig videre, at det p. 15 nævnes, at CFCS i visse tilfælde alene vil tilbyde sin gratis service til én virksomhed i en given branche. Rådet skal bemærke, at i henhold til GDPR pålægges myndigheder og virksomheder at implementere betydelige organisatoriske og tekniske sikkerhedsforanstaltninger. Dette har betydelige omkostninger for virksomhederne. Med forslaget p. 15 er der altså én virksomhed i hver branche, som potentielt kan spare millioner af kroner på at foretage investering i sikkerhedsprodukter ved blot at anvende CFCS i stedet. Dette vil også medvirke til at skabe konkurrenceforvridning i disse brancher.

Rådet er af den opfattelse, at forslaget ikke alene vil skabe konkurrenceforvridning på IT-sikkerhedsmarkedet, men også potentielt på de markeder, der er omfattet af kritisk infrastruktur.

Rådet står naturligvis til rådighed for en uddybelse af ovenstående synspunkter.

På bestyrelsens vegne

Henning Mortensen
Formand, Rådet for Digital Sikkerhed

Forsvarsministeriet

fmn@fmn.dk

tbl@fmn.dk

sbu@fmn.dk

4. februar 2019

Høring vedrørende udkast til *"Forslag til Lov om ændring af lov om Center for Cybersikkerhed"* (sagsnummer 2018/006599)

Teleindustrien (*"TI"*) har nu haft mulighed for at gennemgå Forsvarsministeriets udkast til *"Forslag til Lov om ændring af lov om Center for Cybersikkerhed".*

TI anerkender Forsvarsministeriets sikkerhedsdagsorden, der afspejler det eksisterende trusselsbillede mod den digitale infrastruktur. Som følge heraf forstår TI behovet for via lovgivning at give relevante myndigheder de nødvendige redskaber til at understøtte et tilstrækkeligt sikkerhedsniveau.

TI er dog samtidig af den opfattelse, at der med lovforslaget er tale om en meget indgribende regulering, og at forslagene på nogle punkter synes at gå længere, end hvad der kan retfærdiggøres og forsvares som proportionalt. Endvidere er det TIs opfattelse, at lovforslaget på nogle punkter ikke er tilstrækkeligt præcist til at kunne sikre den nødvendige forudsigelighed og klarhed i reguleringen.

Det er på den baggrund TIs opfattelse, at lovforslaget bør justeres med henblik på at sikre, at myndighedernes redskaber og muligheder for indgriben i virksomheders og enkeltpersoners rettigheder sker inden for på forhånd specificerede rammer og ved iagttagelse af proportionalitet.

I det følgende skal TI fremkomme med sine konkrete bemærkninger til *"Forslag til Lov om ændring af lov om Center for Cybersikkerhed".*

Definitioner

I forslaget til ny § 2, nr. 3 fremgår, at *"Trafikdata"* defineres som *"Data, som behandles med henblik på at transmittere pakkedata".* TI finder anvendelsen af begrebet *"Trafikdata"* uhensigtsmæssig, da samme begreb i forvejen anvendes - med en anden definition - i *"bekendtgørelse om udbud af elektroniske kommunikationsnet og -tjenester*" (§ 2, nr.2).

Det bør desuden præciseres i lovteksten, og ikke kun i bemærkningerne til den foreslåede § 3, stk. 4, at Center for Cybersikkerhed (*"CFCS"*) ikke har adgang til observation af teletrafik mellem virksomheders kunder.

Endelig fremgår det af forslag til ny § 2, nr. 5, at *"Malware"* udgør *"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."*

Det er TI's vurdering, at en definition af begrebet *"Malware"* udelukkende bør indeholde en objektiv, teknisk beskrivelse af, hvad der betragtes som malware og ikke en kvalificering af, at en *"særligt bestyrket mistanke"* kan medføre subsumption af data under begrebet. Sidstnævnte vil medføre uforudsigelighed, da begrebets definition hermed vil afhænge af CFCS' subjektive vurdering af den pågældende data.

Præcisering af begrebet "tilslutning"

Forslaget til den nye lovgivning indeholder efter TI's vurdering ikke en tilstrækkelig præcisering af, hvad en *"tilslutning"* til netsikkerhedstjenesten indebærer. Dette gælder både for så vidt angår frivillige tilslutninger efter aftale (§ 3, stk. 3) samt tilfælde, hvor CFCS efter forslaget skal kunne pålægge påbud om tilslutning (§ 3, stk. 4).

Det har stor betydning for tilsluttede virksomheder, hvor stort et antal punkter i nettet, som en tilslutning indebærer installationer i, samt hvor det pågældende udstyr placeres.

I det tilfælde, at den nye lovgivning kommer til at indeholde mulighed for CFCS til at udstede påbud om tilslutning, bør de deraf følgende installationer hos virksomheder udelukkende kunne påbydes installeret under iagttagelse af proportionalitet, jf. nærmere nedenfor.

Derudover bør det gøres klart, på hvilke øvrige vilkår der forventes indgået aftale mellem CFCS og virksomheder om tilslutning til netsikkerhedstjenesten. Herunder bør forhold vedrørende kommunikation, rapportering, fejlretning, kompetencer, ansvarsfordeling, m.v. indgå. En aftaleskabelon kan eventuelt vedlægges som bilag til lovforslaget.

Påbud om tilslutning

Med lovforslaget foreslås det, at CFCS gives hjemmel til at påbyde tilslutning til CFCS' netsikkerhedstjeneste. Samtidig foreslås det, at gebyret for tilslutning til tjenesten bortfalder.

TI finder det som udgangspunkt positivt, at gebyret forslås fjernet, men TI finder samtidig den nævnte mulighed for påbud om tilslutning både ubegrundet og uproportional, jf. nedenfor.

Det er TI's vurdering, at fjernelsen af tilslutningsgebyret i sig selv vil være tilstrækkeligt til i nødvendigt omfang at sikre tilslutning til CFCS' netsikkerhedstjeneste. Af denne årsag er det TI's vurdering, at det ikke er nødvendigt at indføre muligheden for at meddele myndigheder og virksomheder et påbud om tilslutning.

TI skal desuden bemærke, at det faktum, at en virksomhed – også en virksomhed, der råder over samfundskritisk infrastruktur – ikke er tilknyttet netsikkerhedstjenesten, ikke er ensbetydende med, at der ikke i tilstrækkeligt omfang sker monitorering af virksomhedens infrastruktur. Virksomhederne har en egen interesse i at sikre sig mod angreb udefra, hvorfor det er TI's formodning, at langt de fleste virksomheder, der råder over kritisk infrastruktur, i forvejen er tilstrækkeligt beskyttet, hvorfor der ikke synes at eksistere et selvstændigt behov for at kunne tvinge virksomheder til at blive tilsluttet netsikkerhedstjenesten.

Det er på den baggrund TI's forslag, at den reviderede lov om Center for Cybersikkerhed ikke skal indeholde ovenstående påbudsmulighed. Såfremt den rapport om erfaringer med den nye lovgivning, som oversendes til Folketinget tre år efter lovens ikrafttræden, jf. side 9 i udkast til *"Forslag til Lov om ændring af lov om Center for Cybersikkerhed"* konkret måtte begrunde et sådant behov, vil dette kunne overvejes gennemført ved en senere lovændring.

Såfremt den nye lovgivning mod TI's anbefaling kommer til at indeholde en påbudsmulighed, er det TI's vurdering, at loven ikke indeholder tilstrækkelige kriterier for, hvem et påbud kan rettes mod. Det fremgår af forslag til § 3, stk. 4, at:

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

Det synes dog ikke at være specificeret, hvad der udgør en virksomhed, region eller kommune med *"særlig samfundsvigtig karakter".* Særligt bemærkningerne til lovforslagets enkelte bestemmelser synes at ophæve forudsigeligheden af hvilke enheder, der kan betragtes som havende *"særligt samfundsvigtig karakter".* Her fremgår det, at (side 51):

> *"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 infi-*

ceret 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."

En specificering af begrebet *"særligt samfundsvigtig karakter "* kunne eventuelt formuleres med inspiration fra definitionen af *"væsentlige erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester"* som defineret i *"Bekendtgørelse om informationssikkerhed og beredskab i net og tjenester"* (§ 1, nr. 5). En præcisering bør fremgå direkte af lovteksten.

Det skal understreges, at TI ikke er uenige i ovenstående betragtning om, at en i sig selv ikke-samfundsvigtig virksomhed efter omstændighederne via tilslutning til CFCS's netsikkerhedstjeneste vil kunne bidrage til højere digital sikkerhed. Sammenholdes det ovenfor citerede imidlertid med forslag til ny § 3, stk. 4 (CFCS' mulighed for at udstede påbud om tilslutning), synes CFCS' mulighed for at kræve virksomheder, regioner og kommuner tilsluttet netsikkerhedstjenesten at være stort set uindskrænket, hvilket retssikkerhedsmæssigt er problematisk.

Proportionalitet

Det er væsentligt at sikre overholdelse af grundlæggende frihedsprincipper og privatlivets fred, også i situationer, hvor der er trusler mod sikkerheden. Indgreb i meddelelseshemmeligheden skal begrænses til det mindst mulige under hensyntagen til opretholdelse af samfundskritisk infrastruktur. Det er afgørende, at der er klare og afgrænsede rammer for hvor og hvordan, indgrebene kan finde sted. Bemærkningerne til forslaget bør udbygges til at beskrive den proportionalitetsvurdering, som CFCS skal foretage, forud for en beslutning om udstedelse af påbud, således at det sikres, at formålet med påbuddet ikke kan opnås ad andre veje.

Det er TI's forståelse, at forslaget til ny lovgivning skal medføre hjemmel til, at CFCS kan udstede påbud om tilslutning med installation af passivt udstyr på såvel 'ydersiden' som 'indersiden' hos virksomhederne. Dette fremgår efter TI's vurdering ikke klart af forslaget til ny lovtekst.

Enhver installation på 'indersiden' hos en virksomhed vil indebære tilstedeværelse af en fremmed IT-enhed i virksomhedens infrastruktur, hvilket i sig selv forøger risikoen for fejl i virksomhedens infrastruktur, ligesom den fremmede IT-enhed potentielt kan medføre en forringelse af virksomhedens samlede IT-sikkerhed. Som eksempel kan nævnes risikoen for interferens mellem CFCS' installerede 'agenter' og virksomhedens egne 'agenter'.

Monitorering på 'indersiden' skal også ses i forhold til indgreb i meddelelseshemmeligheden, hvor bemærkningerne til lovforslaget (s. 18) oplyser, at installation af agenter på virksomhedens enheder kan give adgang til ansattes private oplysninger. Installationen vil dermed være langt mere indgribende over for den enkelte ansatte end overvågning af trafikken ind og ud af virksomheden.

Derudover vil CFCS' udstyr samlet kunne medføre en centralisering af kritiske oplysninger, der dermed vil udgøre et særligt attraktivt mål for cyberangreb. Sammenholdes dette med, at Tilsynet med Efterretningstjenesterne de seneste år har udtrykt kritik over fejl i Forsvarets Efterretningstjeneste og Center for Cybersikkerhed (https://politiken.dk/udland/art6960996/Forsvarets-Efterretningstjeneste-har-stadig-ikke-styr-p%C3%A5-it-sikkerheden, https://fe-ddis.dk/Nyheder/nyhedsarkiv/2018/Pages/TET17.aspx), er det TI's vurdering, at CFCS' installationer kan udgøre en ikke ubetydeligt risiko for tilsluttede virksomheder.

Ovenstående gør sig naturligvis i højeste grad gældende, når der er tale om 'aktivt' udstyr på 'indersiden' af en virksomheds IT-infrastruktur, jf. også afsnit 3.3.3.2 (side 20) i udkast til *"Forslag til Lov om ændring af lov om Center for Cybersikkerhed"*, hvoraf fremgår:

> *"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."*

Da karakteren og placeringen af de med en tilslutning medfølgende installationer har stor betydning for virksomhederne, deres kunder, samarbejdspartnere og ansatte, jf. ovenfor, er det TI's klare holdning, at såfremt CFCS med den endelige lovtekst får mulighed for udstedelse af påbud om tilslutning, skal denne kun kunne medføre installation af 'passive' elementer, og udelukkende på 'ydersiden' hos virksomhederne. I modsat fald bør det præciseres, at påbud om installation af udstyr på 'indersiden' hos en virksomhed udelukkende kan ske i særlige og udtømmende specificerede tilfælde.

Herudover bør det være et krav, at virksomhederne informeres fyldestgørende og vedvarende om installation og funktion af udstyr på 'indersiden', herunder særligt 'aktivt' udstyr på 'indersiden', da enhver blokering, omdannelse eller omdirigering af data dels kan medføre fejl, der påvirker virksomhedernes kundeforhold. Ligeledes vil manglende viden om en blokering betyde, at virksomhederne vil opleve den manglende datatrafik (som følge af blokeringen) som en fejl og dermed bruge unødige ressourcer på fejlretning i egne systemer.

Derudover bør lovteksten indeholde en utvetydig kvalificering af, hvorledes det sikres, at CFCS' indgreb er proportionale, samt at også proportionaliteten efterprøves, eksempelvis af Tilsynet med Efterretningstjenesterne.

Forslaget lægger op til en evaluering efter tre år, men for at give størst mulig transparens om omfanget og effekten af indgrebene, bør der årligt, eksempelvis i CFCS' beretning, gøres rede for udviklingen i forhold til netsikkerhedstjenesten, herunder antallet af påbud, resultatet af overvågningen, omfanget af blokering, m.v.

Yderligere skal det understreges, at installation af udstyr på 'indersiden' hos virksomheder vil kunne medføre en væsentlig forøgelse af virksomhedens ressourceforbrug i

forhold til det påkrævede ressourceforbrug, der udspringer af installationer på 'ydersiden' hos virksomheden.

Selvom gebyret for tilslutning bortfalder, vil der fortsat påhvile en virksomhed, der bliver påbudt at tilslutte sig netsikkerhedstjenesten, en potentielt betragtelig omkostning i forhold til implementering, udrulning og sikring af udstyrets kompatibilitet med eksisterende udstyr i virksomhedernes digitale infrastruktur. Det forekommer således generelt misvisende, at der ikke er taget hensyn hertil i forbindelse med den i lovforslaget foretagne vurdering af økonomiske konsekvenser for erhvervslivet.

Endelig skal TI bemærke, at der i lovforslaget ikke synes at være taget stilling til, hvordan eventuelle netnedbrud og skader som følge af CFCS' installationer skal håndteres både i forhold til fejlsøgning, genopretninger, erstatninger m.m. Det samme gælder i forhold til CFCS' mulighed for at omdanne og blokere indhold, hvorved eksempelvis forretningskritisk information kan risikere at gå tabt. Regulering af ansvaret for sådanne følger af CFCS' aktivitet og en eventuel erstatning for tab i medfør heraf, er der ikke taget stilling til i lovteksten, hvilket TI finder yderst problematisk. Disse forhold bør afklares, før lovforslaget fremsættes endeligt.

Edition

CFCS gives med forslaget til den nye lovgivning hjemmel til ved pålæg at indhente oplysninger om brugeren af en e-mailkonto, IP-adresse eller et domænenavn (forslag til ny § 7, stk. 1). Efter TI's vurdering mangler bestemmelsen en definition af, hvad der menes med at *"afdække sikkerhedshændelser"* samt med hvilket nærmere afgrænset formål, der må indhentes oplysninger. Særligt, når forslag til ny § 7, stk. 1 sammenholdes med de sædvanlige editionskrav, må det konstateres, at der mangler et krav om, at der skal foreligge konkret mistanke.

CFCS har på informationsmøde om forslaget oplyst, at hensigten med forslaget er at kunne identificere ofre for cyberangreb og at informere disse om angrebet. I de indledende bemærkninger til forslaget (s. 28) nævnes der dog både identifikation af angrebsaktører og mål for angreb, og gruppen af brugere, der kan kræves oplysninger om, er ikke nærmere beskrevet i lovteksten eller de specifikke bemærkninger til den foreslåede bestemmelse. Det bør præciseres i lovteksten og uddybes i bemærkningerne, hvilke parter identifikationen sigter mod, herunder hvilket formål der kan varetages gennem edition.

TI har noteret sig, at adgangen til edition ikke kun er rettet mod tilsluttede virksomheder, men derimod omfatter alle udbydere, der tildeler burgere e-mailadresser, domænenavne og IP-numre. En udvidelse af editionsadgangen vil uden tvivl medføre yderligere administrative byrder og omkostninger for udbyderne. Anvendelsen af edition bør derfor i videst muligt omfang forsøges minimeret af CFCS, og udbyderne bør kompenseres for omkostningerne ved at yde CFCS bistand svarende til den omkostningsdækning, udbyderne har ret til ved bistand til politiets indgreb i meddelelseshemmeligheden efter telelovens 10 (se lovbemærkningerne til § 10, stk. 2).

Det bør ligeledes præciseres, at muligheden for at indhente oplysninger i henhold til forslag til ny § 7, stk. 1 om en bruger eller medarbejder hos en tilsluttet virksomhed udelukkende kan ske, såfremt oplysningen ikke kan skaffes via den tilsluttede virksomhed. Ud over at sidstnævnte vil begrænse byrderne hos udbyderne, vil det være naturligt, at den tilsluttede virksomhed inddrages, når CFCS vil kontakte medarbejdere og brugere hos den tilsluttede virksomhed.

I forhold til ovenstående pålæg om udlevering af oplysninger om brugeren bag en IP-adresse skal TI gøre opmærksom på, at udbydere af internetadgang i væsentligt omfang anvender den såkaldte NAT-teknologi, hvor mange brugere tildeles det samme IP-nummer. Der vil derfor kunne være flere tusinde brugeroplysninger tilknyttet hvert IP-nummer, og en udlevering af en sådan mængde oplysninger vil dels udgøre et uproportionalt indgreb, og dels være forbundet med et uproportionalt stort ressourceforbrug for de tilsluttede virksomheder. En IP-adressen består af både et IP-nummer og et portnummer, hvorfor det vil være nødvendigt at oplyse begge dele, for at kunne identificere en bestemt bruger bag en IP-adresse. Det bør derfor præciseres, at udlevering af oplysninger om brugeren bag en IP-adresse udelukkende kan ske, såfremt kendelsen både indeholder oplysning om det relevante IP-nummer og portnummer.

Videregivelse af oplysninger

TI kan konstatere, at kredsen, som CFCS kan videregive oplysninger til med lovforslaget foreslås udvidet betragteligt. Det er TI's vurdering, at CFCS' videregivelse af oplysninger kan medføre en forøget sikkerhedsrisiko. Det bør i lovforslaget sikres, at oplysninger om en specifik virksomhed ikke deles med samarbejdspartnere, som den pågældende virksomhed ikke ønsker at dele oplysninger med. Det bør generelt sikres, at der ikke sker videregivelse af data, der indeholder virksomhedsspecifikke oplysninger, der hermed indikerer, hvor den pågældende data stammer fra. Dette vil eksempelvis kunne være tilfældet for kode på malware.

Det bør desuden af lovteksten fremgå, at CFCS' samarbejdspartnere skal have et tilstrækkeligt højt sikkerhedsniveau. Det er i denne sammenhæng TI's opfattelse, at samarbejdspartnerne som minimum bør have et sikkerhedsniveau som tilsvarer kravene til teleoperatørerne, jf. lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester.

Sletning af videregivet data

Det fremgår af forslag til ny § 17, stk. 4, at:

> *"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."*

Det forekommer uhensigtsmæssigt at anvende et 'slettebegreb', som giver mulighed for at indlæse slettet data fra en backup. Det er TI's vurdering, at slettet data definitivt og i sagens natur ikke bør kunne (gen)indlæses.

Derudover fremgår det af forslag til ny § 17, stk. 5, at:

> *"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."*

Der bør efter TI's vurdering ikke gælde udvidede opbevaringsfrister for videregivet data. Det bør derfor i den endelige lovtekst sikres, at videregivet data bliver slettet rettidigt.

Påvirkning af det private marked

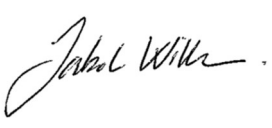
På en række områder foreslås det, at CFCS kan foretage visse forebyggende sikkerhedsforanstaltninger, hvor det ikke kan afvises, at aktiviteterne helt eller delvist vil være i konkurrence med private udbydere af sikkerhedsydelser. For at sikre, at CFCS's aktiviteter ikke unødigt skader udbuddet på det private marked, skal TI derfor opfordre til, at CFCS i videst muligt omfang udbyder opgaverne til private sikkerhedsfirmaer således, at de kan forestå de forebyggende sikkerhedsforanstaltninger for CFCS. TI ser også gerne, at CFCS vælger flere alternative udbydere således, at de tilsluttede virksomheder kan vælge blandt de valgte udbydere, da der kan være udbydere, som af forretningsmæssige grunde ikke kan arbejde internt hos den tilsluttede virksomhed.

Beskikkelse af advokat for den, et indgreb vedrører

Slutteligt skal TI bemærke, at foreningen kan støtte det hensyn, der med forslag til ny § 7b m.fl. er taget til den, som indgreb vedrører. Det er væsentligt at sikre domstolsprøvelse af indgreb i meddelelseshemmeligheden og privatlivets fred, herunder at sikre varetagelsen af hensynet til den, udleveringen af oplysninger vedrører. Derfor er forslaget om beskikkelse af advokat efter TI's vurdering et særdeles hensigtsmæssigt tiltag, som værner positivt om et indgrebssubjekts retssikkerhed.

Med venlig hilsen

Jakob Willer, direktør, Teleindustrien



Tilsynet med Efterretningstjenesterne

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Dato: 4. februar 2019
Sagsnr.: 2018-152-60
Dok.: 18962

Vedrørende høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden)

Ved brev af 7. januar 2019 har Forsvarsministeriet anmodet Tilsynet med Efterretningstjenesterne om bemærkninger vedrørende udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden).

I den anledning skal tilsynet bemærke følgende:

Ved brev af 25. april 2017 besvarede tilsynet Forsvarsministeriets anmodning om bidrag til en rapport om erfaringer med lov om Center for Cybersikkerhed (CFCS-loven). I brevet bemærkede tilsynet vedrørende tilsynets kontrol af CFCS' behandling af oplysningerne om fysiske personer, at det i mange tilfælde er vanskeligt eller slet ikke muligt at fastslå, hvorvidt data indeholder oplysninger om fysiske personer og dermed er omfattet af tilsynet kontrol.

Tilsynet noterer sig, at udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed ikke forholder sig til ovennævnte problemstilling.

Med venlig hilsen
Tilsynet med Efterretningstjenesterne

v/Michael Kistrup
Formand

Borgergade 28, 1.
DK-1300 København K
t 25 50 10 34
www.tet.dk

FMN-TBL Larsen, Tina Kathrine Berg

Fra:	Mikkel Hippe Brun <mhb@tradeshift.com>
Sendt:	4. februar 2019 11:59
Til:	FMN-MYN-FORSVARSMINISTERIET
Cc:	FMN-TBL Larsen, Tina Kathrine Berg; FMN-SBU Østergren, Stine Busch
Emne:	2018/006599 - Høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed

Til rette vedkommende,

På vegne af Tradeshift ApS (CVR 35391282) fremsendes respons på ovenstående høring.

Det er glædeligt at se, at Center for Cybersikkerhed tager yderligere initiativ til at sikre Danmarks informations- og cybersikkerhed.

Vores perspektiv er at vi er en multinational virksomhed med hovedkvarter i San Francisco, USA. Vi har kontorer i 15 lande og har udviklingsteams i så forskellige lande som USA, Danmark, Belgien, Rumænien, Rusland og Kina. Vi har mere end 500 multinationale kunder på vores cloud-baserede platform og ca. 1,5 millioner virksomheder på platformen. I Danmark har vi et stort kontor i København med 160 medarbejdere, som vi forventer at udvide til 300 medarbejdere. Vi har også netop åbnet kontor i Århus. Vi er en af de danske 'Unicorns' med en værdi på over 1,2 milliarder USD.

Vores kunder er multinationale selskaber og offentlige myndigheder over hele verden. Vores cloud-løsning indeholder handelsdata (kataloger, ordrer, logistikdokumenter, fakturaer og betalingsinformation) for vores kunder. Disse data er naturligvis ekstremt følsomme, og vores kunder er meget sensitive overfor hvem, der har adgang til disse data. Vi benytter cloud-tjenester til opbevaring af data rundt omkring i verden (AWS, Google, etc).

Samtidig med at vi sætter pris på at Center for Cybersikkerhed øger beredskabet og skærper de værktøjer, der står til centerets rådighed, så er vi også bekymrede over rækkevidden og den udvidede ret til at anvende disse værktøjer uden retskendelse.

Helt konkret har vi følgende indvendinger:

§3
CFCS kan påbyde virksomheder som Tradeshift at blive tilsluttet, og det er alene Forsvarsministeren, der kan fastsætte de nærmere regler om vilkårene for tilslutning. Denne ændring er for vidtgående. I princippet betyder forslaget, at CFCS vil kunne få adgang til alle de data, som Tradeshift behandler. Det omfatter f.eks. fremmed offentlige myndigheders data herunder handelsdata indenfor forsvarsindustrien og sundhedsvæsenet.

Udlevering af data bør altid ske på en konkret vurdering og med retskendelse. Der bør i særdeleshed tages hensyn til at udlevering af data og integration med netsikkerhedstjenesten ikke kompromitterer fremmede myndigheders data eller data indenfor særligt sensitive industrier.

§4
At CFCS netsikkerhedstjeneste kan behandle data uden retskendelse kan i yderste konsekvens betyde, at en virksomhed som Tradeshift ikke længere kan drives i Danmark. Der skal være en konkret vurdering og en retskendelse.

§5
Tradeshift ligger inde med terabytes af stationære data. Som nævnt er disse data stærkt følsomme og indbefatter data fra udenlandske virksomheder og offentlige myndigheder. En tilgængeliggørelse af disse data til CFCS vil ganske givet kompromitere den lovgivning som vi er omfattet af i andre lande. Anmodning bør altid ske med retskendelse.

Venlig hilsen
--
Mikkel Hippe Brun
Co-founder & SVP of APAC

Email: mhb@tradeshift.com
WhatsApp / Cell: +45 3118.9102
Executive Assistant: Isabela Justo - isj@tradeshift.com
Wechat: hippebrun
Twitter: @hippebrun @tradeshift

TRADESHIFT
All your suppliers. All in one place.
tradeshift.com | tradeshift blog

Vestre Landsret
Præsidenten

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt pr. mail til fmn@fmn.dk, tbl@fmn.dk og sbu@fmn.dk

J.nr. 40A-VL-7-19
Den 10/01-2019

Forsvarsministeriet har ved brev af 7. januar 2019 (sagsnr. 2018/006599) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden).

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Helle Bertung

Østre Landsret
Præsidenten

Den 06/02-2019
J.nr. 40A-ØL-4-19
Init: RSL

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt pr. e-mail til: fmn@fmn.dk, tbl@fmn.dk og sbu@fmn.dk

Forsvarsministeriet har ved brev af 7. januar 2019 (Sagsnr. 2018-006599) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerheden (Initiativer til styrkelse af cybersikkerheden).

I den anledning skal jeg meddele, at landsretten er bekendt med Dommerforeningens udtalelse af 6. februar 2019 om anførte lovudkast, og at landsretten i det hele kan henholde sig til denne udtalelse.

Med venlig hilsen

Bent Carlsen

Ellen Basse Porsbo