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