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