2. marts 2014
HEM

Forsvarsministeriet
Att.: Peter Heiberg
Holmens Kanal 42
1060 København K

Høring vedr. Lov om Center for Cybersikkerhed

DI og DI ITEK takker for henvendelsen vedrørende høring af Forslag til Lov om Center for Cybersikkerhed. DI, DI ITEK og TI har i den anledning nedenstående bemærkninger.

Positivt udgangspunkt
DI og DI ITEK er tilfredse med, at der som opfølgning på regeringsbeslutningen i 2011 om at oprette et Center for Cybersikkerhed (CFCS) under Forsvarets Efterretningstjeneste (FE) nu etableres et lovgrundlag for CFCS', herunder GovCERTs, virke (CFCS-loven). Der er tilsvarende tilfredshed med, at der i samme forbindelse etableres et lovgrundlag for MIL-CERTs virke, som tidligere har været ureguleret.

På de overordnede linjer er vi også meget tilfredse med, at væsentlige dele af reguleringen af CFCS' virke tager udgangspunkt i og viderefører en række principper fra den eksisterende "Lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v." (GovCERT-loven), der med det nye forslag til CFCS-loven ophæves.

Endelig er vi tilfredse med, at analysen af de pakkedata, som CFCS' prober opsamler i civile netværk, jf. CFCS-lovens §4, efter CFCS-lovens § 15 kun må "finde sted ved begrundet mistanke om en sikkerhedshændelse og kun i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen", svarende til bestemmelsen i GovCERT-lovens §4, stk. 1. Denne bestemmelse giver en fornuftig begrænsning i forhold til behandling af personoplysninger.

Forholdet til persondataloven
GovCERT-lovens §5 præciserede, at GovCERT-funktionen alene var undtaget persondatalovens §35, mens det nye CFCS med sin placering under FE generelt er undtaget hele persondataloven, jf. CFCS-loven §8, stk. 1 og persondataloven §2, stk. 11.

I lyset af at GovCERT gennem sine prober på nuværende tidspunkt har adgang til betydelige dele af kommunikationen mellem borgerne/virksomheder og staten og på længere sigt får adgang til stadig større dele af kommunikation mellem borger/virksomheder og brede dele af den offentlige sektor m.v. og især i lyset af at ovenstående adgang gives som følge af en proportionalitetsafvejning mellem Grundlovens §72 (indgreb i meddelelseshemmeligheden) og EMRK artikel 8 (retten til privatlivets fred) på den ene side og de samfunds-

Postadresse/Postal address
1787 København V
Danmark
(+45) 3377 3377
itek@di.dk
itek.di.dk

Besøgsadresser/Visiting addresses
Hannemanns Allé 25
København S
Sundkrogskaj 20
København Ø

CVR: 16 07 75 93

mæssige interesser i at håndtere sikkerhedshændelser for offentlige myndigheder på den anden side, og endelig i lyset af den udvidelse af datagrundlaget der lægges op til, herunder særligt mulighederne for at bryde fortrolig krypteret kommunikation (jf. nedenfor), synes det at være en udfordring i forhold til at beskytte borgernes og virksomhedernes retssikkerhed at undtage al denne kommunikation fra den beskyttelse, som persondataloven giver.

I henhold til den evaluering af GovCERTs virke, som Forsvarsministeren skal give Folketinget i henhold til GovCERT-lovens §9, og som foreligger i udkast her i januar 2014, synes der ikke at have været fagligt behov for at udvide undtagelserne fra persondataloven.

Forsvarsministeriet har, for at råde bod på den væsentlige ændring af anvendelsen af persondataloven i GovCERTs virke, dels indarbejdet §§ 9-14 og §18 i CFCS-loven og dels inddraget en række af principperne fra persondataloven i Forsvarsministeriets "Retningslinjer for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste" (Retningslinjer af 13. maj 2013). Således kan der siges at være et betydeligt sammenfald mellem persondataloven, retningslinjerne af 13. maj 2013 og CFCS-loven som følger:

Persondataloven	Retningslinjerne af 13. maj 2013	CFCS-loven
§3 (definitioner)	§2	
§5 (god behandlingsskik)	§10	§9, §13 og §14
§6 (almindelige oplysninger)	§11	§10
§7 (følsomme oplysninger)	§12	§11
§8 (rent private forhold)	§13	§12
§41 (sikkerhed)	§14	§18 (uden krigsreglen)

Retningslinjerne af 13. maj 2013 bliver efter lovens ikrafttræden erstattet af nye retningslinjer, hvis indhold vi ikke kender. Retningslinjerne kan desuden alene anvendes til tjenestelige sager og kan ikke bruges af en domstol.

Det er et positivt skridt, at Forsvarsministeriet lægger op til, at CFCS skal følge persondataloven på så væsentlige punkter. Det er også et naturligt skridt, at visse dele af persondataloven ikke finder anvendelse for CFCS, f.eks. §§ 15-26 om kreditoplysningsbureauer og §§ 43-54 om anmeldelse til Datatilsynet.

Imidlertid synes det bemærkelsesværdigt at:

1. krigsreglen (Retningslinjerne af 13. maj 2013, §14, stk. 3 og persondataloven §41, stk. 4) ikke finder vej til CFCS-loven
2. der ikke lægges op til at spørge eller i det mindste orientere Tilsynet med Efterretningstjenesterne i principielle sager hvor der behandles personoplysninger, jf. f.eks. persondataloven §7, stk. 7
3. der ikke lægges op til at give borgere og virksomheder et lille minimum af rettigheder i henhold til persondatalovens §§ 28-40.

Der opfordres til, at Forsvarsministeren anvender sin mulighed i CFCS-loven §8, stk. 2 og vurderer, om det er muligt at tildele borgere og virksomheder et minimum af rettigheder.

Der opfordres desuden til at bruge Tilsynet som vejledende organ og til at implementere krigsreglen.

Udvidelse af datagrundlaget begrænser konkurrencen
Datagrundlaget for GovCERT var bestemt ved GovCERT-lovens §4, stk. 1, hvor det omfattede: "tilsluttede myndigheders og private virksomheders ind- og udgående pakke- og trafikdata". Med CFCS-loven lægges der op til, at datagrundlaget udvides på fem forskellige måder.

Den første udvidelse af datagrundlaget sker som følge af at mængden af organisationer, som kan tilslutte sig CFCS netsikkerhedstjeneste, bliver udvidet, når man ændrer ordlyden fra "kritisk infrastruktur" (GovCERT-lovens §2) til "samfundsvigtige funktioner" (CFCS-lovens §1).

Med denne udvidelse af datagrundlaget er der en risiko for, at CFCS netsikkerhedstjeneste kommer i konkurrence med private sikkerhedsleverandører. I "bemærkninger til lovforslagets enkelte bestemmelser" præciseres det, at de samfundsvigtige funktioner omfatter: "sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet... medicinalvirksomheder, fødevarevirksomheder, virksomheder, der leverer vigtige komponenter til Forsvaret, og virksomheder, der varetager driften af administrative it-systemer for det offentlige" (p. 35).

Listen viser, at en ganske stor del af det private erhvervsliv kan tilslutte sig CFCS netsikkerhedstjeneste. Dermed kan netsikkerhedstjenesten gå i direkte konkurrence med private udbydere af sammenlignelige services. Der findes på det private marked tjenester, der i et vist omfang er sammenlignelige med CFCS netsikkerhedstjeneste. Flere sikkerhedsvirksomheder har f.eks. et system af prober til at opsamle data og analysere sikkerhedshændelser på det globale internet, svarende til hvad CFCS netsikkerhedstjeneste har på den danske del af internettet. De pågældende virksomheder har selv status af at være CERTer eller CSIRTer og indgår derfor CERT-CC samarbejdet med deres data. At være i konkurrence med sådanne virksomheder synes ikke at være foreneligt med CFCS formål.

DI, DI ITEK og TI mener derfor, at det bør præcises i lovens bemærkninger, at CFCS's aktiviteter bør tilrettelægges således, at netsikkerhedstjenesten mindst muligt konkurrer med private udbydere af sammenlignelige services.

Der er omvendt begrænsninger på, hvem der kan tilslutte sig CFCS' netsikkerhedstjeneste, og disse begrænsninger fastlås det i loven, at CFCS selv skal være herre over. I "bemærkninger til lovforslagets enkelte bestemmelser" uddybes kriterier for at en virksomhed kan tilsluttes: "[virksomhederne skal] kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet" og at "netsikkerhedstjenesten samlet set opnår en samfundsmæssigt repræsentativ dækning" (p. 36). Det betyder, at den første medicinalvirksomhed, som tilmelder sig tjenesten godt kan blive optaget, men den næste medicinalvirksomhed, kan ikke blive tilsluttet. Skulle det ske, at CFCS opdager en sikkerhedshændelse indenfor medicinalindustrien, kan den første virksomhed altså blive bedre stillet end de øvrige.

CFCS bør i loven pålægges, at i det omfang, de opdager sikkerhedshændelser, der er målrettet enkelte virksomheder eller sektorer, har CFCS en forpligtelse til at orientere den enkelte virksomhed eller sektorens brancheorganisation med relevante informationer om angrebet uanset om virksomheden eller sektoren er tilsluttet CFCS eller ej.

Den anden udvidelse af datagrundlaget sker, når man udvider netsikkerhedstjenesten til foruden af omfatte data fra GovCERT også omfatter data fra MILCERT. DI, DI ITEK og TI har ingen bemærkninger til denne udvidelse af datagrundlaget.

Den tredje udvidelse af datagrundlaget sker, når man åbner op for, at virksomheder og myndigheder midlertidigt kan tilsluttes netsikkerhedstjenesten i henhold til CFCS-lovens §6. Den fjerde udvidelse af datagrundlaget sker, når der er behov for at analysere data fra et informationssystem i henhold til CFCS-lovens §7. Hvad angår håndtering af sådanne pludseligt opståede sikkerhedshændelser, findes der en lang række af private aktører, som allerede påtager sig at levere sådanne services på markedsvilkår. At være i konkurrence med sådanne virksomheder synes ikke at være foreneligt med CFCS formål. Vi anbefaler derfor, at CFCS henviser til private leverandører, når der skal foretages arbejde afledt af midlertidig tilslutning efter §6, og når der skal analyseres informationssystemer efter §7.

Iøvrigt fremgår det ikke klart af loven, om den midlertidige tilslutning og analyse af data fra et informationssystem er noget, som er frivilligt for den som er ramt af en sikkerhedshændelse, eller om CFCS har myndighed til at pålægge en juridisk person, som CFCS mener har været udsat for en sikkerhedshændelse, at blive tilsluttet eller få analyseret sit informationssystem. Det bør præciseres i bemærkningerne, at samtykket i CFCS-loven §6, nr. 1 og §7, nr. 1 betyder at både midlertidig tilslutning og analyse af data fra et informationssystem er frivilligt, og ikke kan pålægges af CFCS.

Den femte udvidelse af datagrundlaget sker i og med at GovCERT ikke havde hjemmel til at bryde kryptering, men at CFCS får denne hjemmel (bemærkninger til lovforslagets enkelte bestemmelser, p. 37). DI, DI ITEK og TI anerkender, at kriminelle ofte anvender kryptering for at skjule deres handlinger. Det forhold bør dog afvejes imod at borgere og virksomheder ofte også bruger kryptering til at særligt fortrolige data, og at CFCS derfor ved at bryde krypteringen må forvente at få adgang til data, som er endnu mere følsomme end hidtil. Det er vigtigt, at man fra politisk hold er opmærksom på denne afvejning.

Videregivelse af data til teleselskaberne
Med CFCS-lovens §16 lægges der op til at udvide videregivelse af forskellige data til forskellige parter. Videregivelse af trafikdata kan i henhold til stk. 2 bl.a. ske til "udbydere af offentlige elektroniske kommunikationsnet og –tjenester". I "bemærkninger til lovforslagets enkelte bestemmelser" p. 44 hedder det, at "især teleselskaber kan forbedre deres sikkerhedssystemer, således at den ikt-infrastruktur, som samfundsvigtige funktioner i overvejende grad er afhængige af, kan sikres yderligere". Formuleringen rejser spørgsmålet om, hvem der har ansvaret for brugen af informationerne. Konkret vil CFCS formodentlig levere en række IP-adresser, som indeholder skadelige services - f.eks. command and controlservere eller dropservere i BOT-nets - til teleselskaberne og ved samme lejlighed fremsætte et ønske om, at de pågældende IP-adresser blokeres. Loven placerer imidlertid ikke et ansvar for blokeringen, og det betyder, at hvis teleselskaberne efterkommer CFCS

ønske, så kan teleselskaberne risikere at hænge på regningen og dårlig omtale ved at bedrive censur af tjenester på internettet og lege politimand på CFCS' vegne. Når §16, stk. 2 så ses i sammenhæng med §17, stk. 4, hvor det fremgår, at CFCS ikke pålægger en sletteplig ved videregivelse af data i medfør af §16, stk. 2, står teleselskaberne i en situation, hvor de ikke ved, hvornår blokeringen af de omtalte IP-adresser skal ophøre, og altså risikerer at holde tjenester på nettet blokeret længere end nødvendigt.

DI, DI ITEK og TI mener, at det er ganske udmærket, at loven ikke forhindrer, at CFCS netsikkerhedstjeneste kan videregive trafikdata til teleselskaberne. Men skal man få succes med dette tiltag og gøre en reel forskel for at beskytte samfundsvigtige funktioner gennem blokering, er det vigtigt, at loven præciserer, at ansvaret for blokeringen ligger hos CFCS, og at CFCS har en forpligtelse til at angive, i hvilket tidsrum blokeringen skal opretholdes. Det bør desuden overvejes at kompensere teleselskaberne for den økonomiske byrde, det vil være at implementere og fjerne blokeringen.

Videregivelse af data fra GovCERT til MILCERT og FE
I GovCERT-loven §6, stk. 2 hed det: "Pakkedata, der knytter sig til en sikkerhedshændelse, kan videregives til Forsvarets Efterretningstjenestes militære CERT, hvor IT- og Telestyrelsen skønner det nødvendigt for at beskytte nationale digitale infrastrukturer mod sikkerhedsmæssige trusler". CFCS har gentagne gange understreget, at netop opretholdelsen af dette forhold er det, som sikrer borgernes retssikkerhed.

Med CFCS-loven fjernes denne beskyttelse: "En sådan intern udveksling af data har efter oprettelsen af Center for Cybersikkerhed ikke længere karakter af en videregivelse, og den interne udveksling af data i Forsvarets Efterretningstjeneste er… ikke længere reguleret i lovforslaget" (almindelige bemærkninger, p. 26). I udgangspunktet betyder det, at FE i bred forstand får adgang til GovCERTs data (også pakkedata), og FE kan derfor i udgangspunktet bruge disse data, indenfor de rammer der er bestemt i FE-loven. Det synes at være en ganske vid udvidelse i anvendelsen af data, ikke mindst fordi det som tidlige anført handler om al kommunikation mellem borgere/virksomheder og den offentlige sektor m.v.

I bemærkningerne, p. 9, hedder det også om Retningslinjerne af 13. maj 2013, at: "Retningslinjerne fastsætter derudover en række bestemmelser om den interne udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste". Retningslinjerne erstattes af nye retningslinjer efter CFCS-lovens vedtagelse. Hvis det kan lægges til grund at indholdet af retningslinjerne vil blive videreført, således som de almindelige bemærkninger (p. 26) indikerer: "Forsvarsministeriet vil imidlertid med lov om Center for Cybersikkerheds ikrafttræden udstede administrative retningslinjer, der sikrer, at den interne udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste også fremadrettet sker med respekt for retssikkerheden og den personlige frihed", så gælder det jf. §6, stk. 2, at "Vurderingen af, om en videregivelse af trafikdata til FE's efterretningsmæssige virksomhed er nødvendig i henhold til varslingstjenestens formål og aktiviteter, jf. GovCERT-lovens §6, nr. 3, foretages af chefen for CFCS eller en af denne udpeget person"..

DI, DI ITEK og TI mener, at det er uklart, i hvilket omfang GovCERTs data kan bruges af FE. Vi mener også, at det er en uheldig konsekvens af CFCS placering i FE, at der er risiko for at der bliver en så vid adgang til GovCERTs data. Vi anbefaler, at:

- at det i de kommende retningslinjer fortsat fastslås, at der fra gang til gang skal tages stilling til, om pakkedata kan videregives fra CFCS til FE
- at adgang for FE kun må gives, når det er nødvendigt i henhold til CFCS's formål og aktiviteter eller der foreligger et andre nærmere kvalificerede beskyttelsesværdige formål,
- at det overordnet sikres, at der ikke sker et automatisk og generelt flow af alle trafikdata fra GovCERT til FE

Videregivelse af data til udlandet

I CFCS-lovens §16, nr. 2 hedder det, at: "trafikdata videregives til… andre netsikkerhedstjenester". Dette uddybes i de almindelige bemærkninger (p. 25) med, at det er en forudsætning for CFCS succes, at trafikdata kan videregives til andre landes CERTer og iktsikkerhedsmyndigheder.

Vi noterer os med tilfredshed, at pakkedata alene må videregives til politiet jf. §16, nr. 1. Vi finder det samtidig absolut nødvendigt med et samarbejde mellem myndighederne på tværs af grænser, idet langt størsteparten af den it-kriminalitet der foregår, er grænseoverskridende. Da §16, nr. 2 henviser til data der er omfattet af §§ 4, 6 og 7 synes der ikke at være nogen begrænsning på omfanget af trafikdata, som kan videregives til udlandet. Basalt set ville alle indsamlede trafikdata kunne overføres til samarbejdspartnere i fremmede lande. I lyset af den udvidelse af datagrundlaget, der med lovforslaget finder sted, synes det rimeligt, at sikre en vis begrænsning i mulighederne for at overføre data eller i det mindste at underlægge omfanget demokratisk kontrol. DI, DI ITEK og TI anbefaler konkret, at der kun må overføres trafikdata til udlandet, som er tilknyttet en sikkerhedshændelse som defineret i §2, nr. 1. Alle trafikdata, som ikke er tilknyttet en sikkerhedshændelse, må dermed ikke overføres.

Slettefrister

Med CFCS-loven ændres der betydeligt i slettefristerne. Trafik- og pakkedata behandles nu ens. Det betyder, at pakkedata, hvortil der ikke er knyttet en sikkerhedshændelse, nu kan gemmes i 13 måneder (CFCS-loven, §17, stk. 2) i modsætning til tidligere i 14 dage (GovCERT-loven, §4, stk. 3, nr. 2). Trafikdata, hvortil der ikke er sket en sikkerhedshændelse, kan gemmes i 13 måneder mod tidligere 12 måneder.

Yderligere slås det i CFCS-loven, §4, stk. 4 fast, at der ikke stilles krav om sletning for data, som videregives.

Sammenholdes bestemmelserne om videregivelse til udlandet og slettefristerne står der basalt set i loven, at alle trafikdata kan videregives til udlandet og aldrig behøver at blive slettet.

DI, DI ITEK og TI finder det ikke proportionalt, at pakkedata kan gemmes i 13 måneder og foreslår, at tidshorisonten sænkes til én måned. Desuden synes det ikke rimeligt, at der ikke stilles krav om sletning, når data videregives. Dette gælder både videregivelse af trafikdata til teleudbyderne (jf. bemærkningerne ovenfor) og ved videregivelse til myndighe-

der i udlandet. Derfor anbefaler vi, at der når data videregives, fastsættes krav om sletning.

Tilsynet
I lyset af placeringen af CFCS i FE er det naturligt at nedlægge Tilsynet med GovCERT og overlade opgaven til Tilsynet med Efterretningstjenesterne.

Tilsynet med GovCERT skulle i henhold til GovCERT-loven §7, stk. 2 kunne præstere juridisk, it-revisionsmæssig og sikkerhedsmæssig sagkundskab. Tilsynet med CFCS bliver i henhold til CFCS-loven, kapitel 9, Tilsynet med Efterretningstjenesterne. Men i PET-lovens kapitel 9 findes der ikke tilsvarende krav til sagkundskaben hos dem, der udpeges til Tilsynet. Der er derfor en risiko for, at man vil mangle kompetencer i det nye tilsyn.

Det bør sikres, at Tilsynet med Efterretningstjenesterne har adgang til den fornødne sagkundskab og ikke alene repræsenterer juridiske kompetencer.

Andre bemærkninger
I CFCS-loven §17, stk. 3 omtales registrering af data. Registrering defineres ikke noget sted i loven. I den konkrete situation er der dermed en risiko for, at CFCS kan have data liggende, som ikke er registrerede, og dermed ikke er omfattet af slettefristerne. I et bredere perspektiv kunne der også være en risiko for, at sådanne data slet ikke er omfattet af loven. Det bør i bemærkningerne præciseres, at en registrering i overensstemmelse med det persondataretlige begreb er en behandling jf. CFCS-lovens § 2, nr. 5.

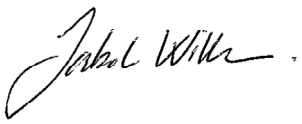
I både "Evaluering af GovCERT-loven" og lovforslagets almindelige bemærkninger 3.2.2 fremhæves vigtigheden af adgang til pakkedata. Imidlertid vil det være nyttigt, dersom der mere generelt bliver fremlagt vurdering af CFCS effektivitet med hensyn til at efterleve formålet i CFCS-lovens §1. Vi opfordrer til, at CFCS offentligt demonstrerer, at de faktisk har en effekt på cybersikkerheden i Danmark.

For at sikre, at formålet med CFCS kan opfyldes er det nødvendigt, at CFCS får informationer fra de tilsluttede virksomheder enten i form af CFCS anmoder om oplysningerne eller virksomheden af egen drift informere CFCS om forhold der er kan understøtte et højt informationssikkerhedsniveau i samfundet eller virksomheden har en mistanke om en sikkerhedshændelsen. Loven synes imidlertid alene at vedrører den behandling af oplysninger Center for Cybersikkerhed kan foretage. Selve udleveringen af personoplysning herunder trafik- og pakkedata der sker på initiativ af en privat virksomhed er derimod ikke behandlet i loven. Da en sådan udlevering af oplysninger ikke nødvendigvis er lovlig efter hhv. persondataloven eller teleloven, bør det præciseres i CFCS-loven, at udleveringen af personoplysning herunder trafik- og pakkedata til CFCS lovlig kan foretages af en tilsluttet virksomhed uden at der foreligger en konkret anmodning fra CFCS.

Vi står naturligvis til rådighed med en uddybelse af ovenstående synspunkter.

Med venlig hilsen

Henning Mortensen
Chefkonsulent
DI ITEK



Jakob Willer
Direktør
Teleindustrien