Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt på e-mail: fmn@fmn.dk
Kopi til: sbu@fmn.dk; tbl@fmn.dk

Dok. ansvarlig: RPR
Sekretær:
Sagsnr: s2019-421
Doknr: d2019-9978-7.0
28-05-2019

Høringssvar til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste – FMN sags nr. sagsnummer 2019/002526.

Dansk Energi har modtaget udkast til ovennævnte bekendtgørelse i høring, og takker for muligheden for at komme med bemærkninger hertil.

Dansk Energi er positiv over for muligheden for at virksomheder i energisektoren kan vælge at lade sig tilslutte netsikkerhedstjenesten, og Dansk Energi indgår også gerne i en konstruktiv dialog med Center for Cybersikkerhed og Energistyrelsen om, hvilke virksomheder i energisektoren, som skal/bør omfattes af netsikkerhedstjenesten.

I forhold til det foreliggende udkast til bekendtgørelse efterspørges konkret en afklaring af:

- Hvilke forhold og kriterier der lægges til grund for at en virksomhed udpeges til at blive tilsluttes netsikkerhedstjenesten.
- Hvad virksomhederne forpligter sig til, når de lader sig tilslutte netsikkerhedstjenesten.
- Hvilke omkostninger, som virksomheder pålægges/påtager sig og skal forvente at dække (ved opsætning/indkøring og efterfølgende drift).
- Hvad de tilsluttede virksomheder reelt (hvordan, hvornår mv.) får retur fra CFCS/netsikkerhedstjenesten af viden om sikkerhedshændelser i egne IT-systemer.
- Hvad der nærmere må forstås ved at CFCS vil deklassificere information, så information fra netsikkerhedstjenesten kan tilgå flere/alle og ikke alene den virksomhed, som informationen stammer fra.

I lov om Center for Cybersikkerhed er det omtalt, at også underleverandører til de samfundsvigtige sektorer kan blive omfattet af netsikkerhedstjenesten. Disse synes imidlertid ikke umiddelbart at være omfattet af bekendtgørelsen. I den forbindelse skal vi høre om det er forventningen, at underleverandører også kan blive omfattet?

I forhold til reglerne om klage skal vi bemærke, at forvaltningslovens § 25 om klagevejledning finder anvendelse – ikke kun principperne i denne bestemmelse.

Endelig skal vi venligst anmode om

- **at** klagemulighed og klageinstans fremgår af bekendtgørelsen, og
- **at** Forsvarsministeren benytter sin adgang i lovens § 8, stk. 2 til at bestemme, at forvaltningslovens kapitel 4-6 helt eller delvis finder anvendelse for Center for Cybersikkerhed vedrørende beslutninger efter denne bekendtgørelse.

Såfremt ovennævnte giver anledning til spørgsmål, eller der er et behov for en uddybning, står Dansk Energi naturligvis til rådighed.

Med venlig hilsen

Regitze Prahl

Dansk Energi

DANSK ERHVERV
Børsen
DK-1217 København K

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

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

Sagsnummer 2019/002526.

3. juni 2019

Høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste / sagsnummer 2019/002526.

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, og Dansk Erhverv har tidligere afgivet høringssvar til lovudkast om Center for Cybersikkerhed (sagsnr. 2018/006599, 4. februar 2019). Dansk Erhverv noterede sig med tilfredshed, at der i den efterfølgende proces blev indgået politisk aftale om at skrive de allermest vidtgående beføjelser ud af det oprindelige lovudkast.

Hvad angår det aktuelle udkast til bekendtgørelse stiller Dansk Erhverv sig stadig kritisk over for muligheden for at pålægge virksomheder tilslutning til CFCS netsikkerhedstjeneste.

En tvungen tilslutning til CFCSs sikkerhedstjeneste kan påføre virksomheden flere direkte udgifter, og efterlade virksomheden med et forklaringsproblem over for kunder og samarbejdspartnere. Det kan i sidste ende få negative konsekvenser for den enkelte virksomheder, og for Danmark som land for investeringer og teknologiudvikling

Derfor er det helt afgørende, at et påbud om tilslutning til netsikkerhedstjenesten sker som den absolut sidste og eneste løsning på et problem der ikke kan løses med andre midler. Der bør altid være tæt dialog, så virksomheden har indflydelse på valg af teknologi og procedurer, og med stor opmærksomhed på eventuelle negative konsekvenser, samt stor fokus på kommunikation af bagvedliggende rationaler og praksis for en tilslutning.

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.

Specifikke bemærkninger

§2 Definition af omfattede virksomheder

Dansk Erhverv savner en klar definition af hvilke virksomheder som kan omfattes af påbud om tilslutning til netsikkerhedstjenesten. Udkastet til bekendtgørelsen beskriver potentielt omfattede som virksomheder af "særligt samfundsvigtig karakter" og "af væsentlig betydning for Danmarks kritiske infrastruktur". Dansk Erhverv ser behov for en klarede definition af hvilke virksomheder CFCS overvejer at påbyde tilslutning.

§2, stk. 7 Krav til myndighederne ved afgørelse om påbud

Dansk Erhverv noterer sig, at §2, stk. 7 definerer, at en afgørelse om påbud bl.a. skal ledsages af en vejledning om klageadgang, samt en beskrivelse af CFCSs behandling af personoplysninger, som virksomheden kan anvende til at informere organisationens medarbejdere.

Dansk Erhverv opfordrer til, at beskrivelsen udformes på en måde så den også er egnet til at informere virksomhedernes kunder og samarbejdspartnere, herunder at materialet også er tilgængeligt på engelsk.

Dansk Erhverv noterer sig, at §2 stk. 7 taler om en "*standard*beskrivelse af Centre for Cybersikkerheds behandling af personoplysninger". Dansk Erhverv opfordrer til at myndighederne forpligtes til at sikre at man i beskrivelsen til virksomhedens medarbejdere, samarbejdspartnere og kunder også redegør specifikt for CFCS behandling af personoplysninger for den specifikke virksomheds medarbejdere, samarbejdspartnere og kunder. En generisk beskrivelse af CFCS behandling af persondata vil næppe besvare de spørgsmål, der vil opstå som følge af pålæg om tilslutning.

§3 – byrder for medvirken til netsikkerhedstjenesten opsætning og drift

Udkastet til bekendtgørelsen definerer, at en virksomhed "loyalt (skal) medvirke til netsikkerhedstjenestens opsætning og drift af en eller flere alarmenheder", og at virksomheden skal "stille den nødvendige fysiske, tekniske og netværksmæssige understøttelse til rådighed". Udkastet til bekendtgørelse definerer en række punkter, man som virksomhed skal leve op til ift. den interne drift af it, tekniske oplysninger, procedurer leverandører, adgangsforhold m.v.

Dansk Erhverv vurderer, at §3 kan blive ganske byrde- og omkostningsfuldt for de tilsluttede virksomheder i etablering såvel som i drift. Dansk Erhverv finder det derfor mest rigtigt, at den ansvarlige myndighed finder en løsning for kompensation for de tekniske og organisatoriske foranstaltninger, som et påbud om tilslutning indebærer for virksomheden.

Med venlig hilsen

Janus Sandsgaard
Fagchef, digitalisering

DanskeRederier

Forsvarsministeriet
Holmens Kanal 9
1060 København K
Sendt elektronisk til fmn@fmn.dk

Høringssvar vedr. udkast til bekendtgørelse om tilslutning til CFCS netsikkerhedstjeneste

3. juni 2019

Sagsnummer:
EMN-2016-00289

Danske Rederier vil gerne kvittere for modtagelse af høringsbrev af 3. maj 2019 vedr. høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds (CFCS) netsikkerhedstjeneste, sagsnummer 2019/002526.

I forbindelse med udkast til bekendtgørelse vil finder vi det positivt, at i forbindelse med et evt. påbud, kan dette kun ske i samarbejde med tilsynsmyndigheden i den relevante sektor, jvf. §2, stk. 5.

Der er dog i forbindelse med udkastet, et par områder, som med fordel kunne afklares:

- Hvad er definitionen af ”væsentlig betydning” jf. §2 stk. 1.
- Hvordan vurderes virksomheder påvirkning af Danmarks forhold til andre stater og internationale organisationer og økonomisk stabilitet og handlefrihed, jvf. §2 stk. 3.
- Hvordan defineres ”det, der er nødvendigt” jvf. §2 stk. 4.
- Hvordan defineres ”loyalt” jvf. §3 stk. 1.
- Hvordan kompenseres virksomheden for de omkostninger der kan påføres ved evt. påbud jvf. §3 Stk. 3.

Endelig finder vi, at det er problematisk, at §3 stk. 3 pkt. 2 påvirker virksomhedens frie beslutningsevne, da man ikke kan lave ændringer uden, de er aftalt med CFCS. Herved forlænger man virksomhedens beslutningsproces og øger eventuel time-to-market, som kan være vital i en konkurrencesituation.

Med venlig hilsen

Morten Glamsø
Chefkonsulent

DATATILSYNET

Forsvarsministeriet
Holmens Kanal 42
1060 København K

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

29. maj 2019

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

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

J.nr. 2019-12-0489
Dok.nr. 101582
Sagsbehandler
Camilla Andersen

Høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste – sagsnummer 2019/002526

Ved e-mail af 3. maj 2019 har Forsvarsministeriet anmodet om Datatilsynets bemærkninger til ovennævnte udkast til bekendtgørelse.

Datatilsynet har følgende bemærkninger:

1. I udkastet foreslås indsat en bestemmelse med følgende ordlyd i bekendtgørelsens § 4:

> "**§ 4**. Den eller de alarmenheder, som opsættes i medfør af tilslutningsaftalen, jf. § 1, stk. 2, nr. 1, eller i medfør af § 2, stk. 6, er Center for Cybersikkerheds ejendom, og centeret er at betragte som dataansvarlig for data, der indsamles og i øvrigt behandles i forbindelse med driften af alarmenheden.
>
> Stk. 2. Ved installation og drift af sikkerhedssoftware på lokale enheder, jf. § 1, stk. 2, nr. 2, er Center for Cybersikkerhed at betragte som dataansvarlig for den behandling, der foretages ved hjælp af sikkerhedssoftwaren.
>
> Stk. 3. Ved løbende overførsel af oplysninger fra eget sikkerhedssystem til Center for Cybersikkerhed, jf. § 1, stk. 2, nr. 3, er Center for Cybersikkerhed at betragte som dataansvarlig for data, når data er videregivet til centeret, herunder til eventuelt installeret udstyr tilhørende centeret."

Datatilsynet har i den forbindelse noteret sig, at det endvidere følger af punkt 4.1. i de almindelige bemærkninger til lovforslag L125 fremsat den 27. marts 2019, at Center for Cybersikkerhed, i relation til de tilsluttede myndigheder og virksomheder, er selvstændig dataansvarlig for den behandling af personoplysninger, som centeret udfører. Disse behandlinger foretages eksempelvis i forbindelse med netværksmonitorering, monitorering med sikkerhedssoftware, aktivt cyberforsvar og som led i sikkerhedstekniske undersøgelser. Centerets behandlinger sker her til centerets egne formål og med egne hjælpemidler.

Det følger endvidere af bemærkningerne, at myndigheder og virksomheder, der er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste, eller som anmoder centeret om bistand, fortsat vil være selvstændige dataansvarlige for deres egne behandlinger af personoplysningerne, herunder indsamling og opbevaring.

Når Center for Cybersikkerhed får adgang til data hos myndigheder og virksomheder, er der dermed tale om en videregivelse mellem to selvstændige dataansvarlige.

2. Datatilsynet henviser i øvrigt til tilsynets høringssvar af 30. januar 2019[1]. Der henvises særligt til høringssvarets punkt 3.3, da det fortsat ikke står Datatilsynet klart, med hvilken hjemmel de tilsluttede virksomheder og myndigheder videregiver følsomme personoplysninger til Center for Cybersikkerhed.

Datatilsynet har imidlertid noteret sig, at Forsvarsministeriet har foretaget en vurdering i henhold til den tjekliste om udarbejdelse af nye nationale særregler for behandling af følsomme personoplysninger, som fremgår af betænkning nr. 1565 om databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning[2].

Med venlig hilsen

Camilla Andersen

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

[2] Se pkt. 4.2. i de almindelige bemærkninger til lovforslag L125 fremsat den 27. marts 2019

Digital

Til
Forsvarsministeriet fmn@fmn.dk
Kopi: tbl@fmn.dk og sbu@fmn.

4. juni 2019
Sagsnummer: 2019/002526

Høringssvar vedr. bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste

1. Baggrund

DI Digital takker for høring over forslag til bekendtgørelse til Center for Cybersikkerheds netsikkerhedstjeneste. Vi skal samtidig henvise til vores høringssvar af 4. februar 2019 om forslag til lov om ændring af lov om Center for Cybersikkerhed.

2. Generelle bemærkninger

DI støtter alene en frivillig ordning.

DI støtter som udgangspunkt alene en frivillig tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste, som nævnt i ovenstående høringssvar. 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.

DI foreslår generelt et øget samarbejde mellem CFCS og it-sikkerhedsbranchen om at forbedre sikkerheden for det generelle erhvervsliv, se forslag nedenfor.

DI er positive over for, at man i bekendgørelsen har forsøgt at præcisere flere af de punkter, som DI tidligere har kommenteret på. DI har alligevel en række konkrete bemærkninger jf. nedenfor.

3. Konkrete bemærkninger

Der bør tages hensyn til ikke at forstyrre driften.

Bekendtgørelsens § 2 indfører bestemmelsen om et påbud. Her bør der indsættes et princip om, at CFCS i videst muligt omfang forsøget at installere deres udstyr under hensyn til virksomhedernes økonomiske forhold, herunder navnlig under hensyn til at forstyrre driften mindst muligt. Der skal være proportionalitet mellem hensynet til at udstede påbuddet og

hensynet til virksomhedens drift og omkostninger ved påbuddet.

DI støtter præcisering af samfundsvigtige interesser.

§ 2, stk.3 definerer samfundsvigtige interesser og hermed hvilke virksomheder, der er omfattet at loven og bekendtgørelsen. Generelt er det positivt, at man har forsøgt at præcisere dette og generelt men det kan diskuteres, om definitionen, fx henvisningen til befolkningens grundlæggende velfærd, er blevet lidt vel bred. Vi foreslår, at man ser til udlandet for en mere præcis definition.

Præcisering af klageadgang

DI noterer sig, at et påbud skal ledsages af en klar klageadgang. Dette punkt er dog så centralt at det bør præciseres nærmere i bekendtgørelsen, fx at der skal være tale om en anden instans.

Der bør indføres et princip om bedre deling af viden med den konkrete virksomhed.

§ 2 stk. 4 til 8 præciserer grænserne for påbuddet hvilket er positivt. § 2 stk. 7 litra 1 bør indeholde, at man i påbuddet angiver hvilke data eller oplysninger man konkret eftersøger – i det mindste typen af oplysninger. Den pågældende virksomhed vil ofte kunne kvalificere og gøre opsætningen af udstyret mest effektivt, hvis det oplyses, hvilken type af data, der eftersøges eller hvor data kommer fra. Generelt bør deling af viden med virksomhederne være et princip i bekendtgørelsen – alene for at kunne sikre et mere ligeværdigt samarbejde og udbytte om at forbedre sikkerheden.

Der bør ikke indføres unødige begrænsninger for omfattede virksomheders mulighed for at ændre i opsætning

§ 3 stk. 2 litra 2 indeholder en bestemmelse om, at den konkrete virksomhed ikke må ændre i sin tekniske opsætning, hvis det kan påvirke de opsatte alarmenheder, medmindre det er aftalt. Her bør ordet "aftalt" ændres til "meddelt" idet en virksomhed ikke unødigt bør begrænses i sin ret til at ændre sin opsætning. Den frie ret til at planlægge sin drift skal ikke aftales med CFCS – det skal højst meddeles.

Forholdet til underleverandører bør præciseres.

§ 3 stk. 6 omfatter forholdet til underleverandører. Her påhviler det de omfattede virksomheder, at sikre at underleverandører samarbejder i nødvendigt omfang. Det forekommer unødigt at dette ansvar skal påhvile den omfattede virksomhed. I praksis vil det betyde at den omfattede virksomhed i sin kontrakt med leverandører specificerer dette. Men det kan være uklart hvordan denne forpligtelse skal udformes og samtidigt tilføre et ekstra forhandlingspunkt til i forvejen komplicerede forhandlinger. I stedet bør bekendtgørelsens påbud omfatte virksomheder og deres eventuelle underleverandører. Her skal DI gentage den ovenstående bemærkning om at tage hensyn til de økonomiske omkostninger for omfattede virksomheder. Det er samtidig vigtigt at kun virksomheder i Danmark under dansk jurisdiktion omfattes af et evt. påbud. Det er et særligt problem når behandling af data foretages i centre i andre lande. Bekendtgørelsen bør ikke umuliggøre udveksling af data på tværs

af lande, da det vil gøre det problematisk for at bibeholde Danmark som et attraktivt land at placere datacentre i.

Særlig opmærksomhed omkring data fra netsikkerhedstjenesten

Der bør indføres et princip om, at data indsamlet gennem netsikkerhedstjenesten bør være omfattet af et "særligt opmærksomt" tilsyn fra TET – som har det generelle tilsyn med efterretningstjenesterne.

Ansvar for overholdelse af GDPR bør være klart

Det er positivt at bekendtgørelsen forholder sig til GDPR. Det kan præciseres, at omfattede virksomheder ikke har et ansvar i medfør af GDPR for de omfattede data.

Ingen krav om hemmeligholdelse af påbud.

Endelig bør det være en ret for omfattede virksomheder at kunne kommunikere frit om hvorvidt de er omfattet af et påbud. Det ville være relevant for kunderne til de pågældende virksomheder.

Med venlig hilsen

Morten Kristiansen, Chefkonsulent, DI Digital

Fra: Claus Ryde <clr@fanet.dk>
Sendt: 22. juli 2019 10:36
Til: FMN-MYN-FORSVARSMINISTERIET
Cc: FMN-TBL Larsen, Tina Kathrine Berg; FMN-SBU Østergren, Stine Busch
Emne: Vedr. : Supplerende høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste (2019/003498)

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

FA takker for Forsvarsministeriets supplerende høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste, Forsvarsministeriets sagsnummer 2019/003498.

FA har ikke bemærkninger til udkastet, og henviser til høringssvar fra Finansdanmark og Forsikring & Pension.

Med venlig hilsen
Claus Ryde
Seniorkonsulent, DPO
clr@fanet.dk

Telefon: +45 3391 4700
Direkte: +45 3338 1614

Finanssektorens Arbejdsgiverforening
Amaliegade 7
1256 København K

Besøg os på www.fanet.dk og abonnér på vores nyhedsmail

Fra: Aase Asmussen <asm@fanet.dk>
Sendt: 29. maj 2019 09:15
Til: FMN-MYN-FORSVARSMINISTERIET; FMN-TBL Larsen, Tina Kathrine Berg
Emne: Høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste
Vedhæftede filer: CFCS-bekendtgørelse.pdf; Høringsbrev .pdf; Høringsliste.pdf; signaturbevis.txt

Kategorier: Tino

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

FA takker for høringen. FA har ingen bemærkninger, men henviser til svar fra brancheorganisationerne.

Med venlig hilsen
Aase Asmussen
Advokatsekretær
asm@fanet.dk

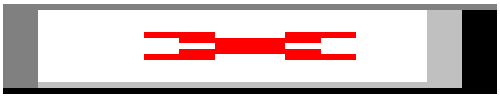
Telefon: +45 3391 4700
Direkte: +45 3338 1620

Finanssektorens Arbejdsgiverforening
Amaliegade 7
1256 København K

Besøg os på www.fanet.dk og abonnér på vores nyhedsmail

Fra: Forsvarsministeriet <fmn@fmn.dk>
Sendt: 3. maj 2019 14:08
Til: samfund@advokatsamfundet.dk; ac@ac.dk; amnesty@amnesty.dk; itd@itd.dk; info@danishshipping.dk; dalo@da.dk; mail@danskeadvokater.dk; de@danskenergi.dk; info@danskerhverv.dk; di@di.dk; registry@difo.dk; info@danskemedier.dk; dit@dit.dk; regioner@regioner.dk; dt@datatilsynet.dk; dommerforeningen@gmail.com; cert@cert.dk; info@energinet.dk; mail@finansdanmark.dk; Finanssektorens Arbejdsgiverforening <fa@fanet.dk>; fdo@fdo.dk; fvd@fvd.dk; fp@forsikringogpension.dk; ida@ida.dk; info@humanrights.dk; henrikfriis@globalconnect.dk; fh@fho.dk; itb@itb.dk; bestyrelsen@itpol.dk; info@justitia-int.org; kl@kl.dk; info@lf.dk; lo@lo.dk; lederne@lederne.dk; dadl@dadl.dk; info@lif.dk; doi@di.dk; prosa@prosa.dk; post@oestrelandsret.dk; post@vestrelandsret.dk; formand@retspolitik.dk; ro@gl.stm.dk; ro@fo.stm.dk; info@digitalsikkerhed.dk; kobenhavn@domstol.dk; esbjerg@domstol.dk; glostrup@domstol.dk; helsingor@domstol.dk; herning@domstol.dk; hillerod@domstol.dk; hjorring@domstol.dk; holbaek@domstol.dk; holstebro@domstol.dk; horsens@domstol.dk; kolding@domstol.dk; lyngby@domstol.dk; nykobing@domstol.dk; naestved@domstol.dk; odense@domstol.dk; randers@domstol.dk; roskilde@domstol.dk; svendborg@domstol.dk; sonderborg@domstol.dk; viborg@domstol.dk; aalborg@domstol.dk; aarhus@domstol.dk; bornholm@domstol.dk; frederiksberg@domstol.dk; digst@digst.dk; jw@teleindu.dk; info@tet.dk
Cc: bm@bm.dk; efkm@efkm.dk; em@em.dk; fm@fm.dk; jm@jm.dk; km@km.dk; kum@kum.dk; mfvm@mfvm.dk; skm@skm.dk; sm@sm.dk; sum@sum.dk; trm@trm.dk; ufm@ufm.dk; um@um.dk;

uim@uim.dk; uvm@uvm.dk; oim@oim.dk; stm@stm.dk
Emne: Høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste



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

Se venligst vedhæftede dokumenter.

Forsvarsministeriet

FINANS DANMARK

Høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste

29. maj 2019
FIDA-151247800-647742

Tak for muligheden for at afgive høringssvar.

Beslutning om påbud

Finans Danmark er positive overfor at påbud ikke kan besluttes af CFCS alene, og at tilsynsmyndigheden i den relevante sektor inddrages (§ 2, stk. 5).

Change Management

Hvordan tænkes den nødvendige Change Management koordineret omkring de "tekniske og netværksmæssige ændringer, som kan påvirke driften af alarmenhederne" (§3 stk. 3 punkt 2). Det vil være en udfordring hvis, adgangen til at foretage fysiske, tekniske og netværksmæssige ændringer i virksomhedens net begrænses af udstyret fra CFCS (§3 stk.2).

Adgangsstyring

Det bør præciseres, hvad der er passende sikkerhedsforanstaltninger for adgang til net sikkerhedstjenestens alarmenheder og tilhørende udstyr (§3 stk. 3).

Databehandleraftaler

Der ønskes belyst, hvorvidt der kræves databehandleraftale mellem CFCS og de enkelte virksomheder ved udveksling af personhenførbare oplysninger i forbindelse med logning.

Ansvarsforhold

Finans Danmark finder at afsnittet om ansvarsforhold ikke tilstrækkeligt behandler ansvarsforholdet for begge parter. Den form for udstyr der ønskes anvendt kan afstedkomme IT-nedbrud for de, der er tilsluttet. Center for Cybersikkerhed bliver således en outsourcing leverandør og skal indgå i virksomhedens, som en sådan med henblik på at sikre en professionel IT-drift af de relevante systemer. Udstyret vil derfor være en del af risikostyringen. Ikke alene kan disse systemer forsage

nedbrud, de vil også I nogle tilfælde være en del af "incident resolution processes" for at identificere om de er kilden til en given problematik eller ej.

Vi foreslår derfor at bestemmelsen om ansvarsforhold præciseres på følgende måde:
§4 stk 4.
Enhver form for driftsforstyrrelse på IT-stabilitet, der er afstedkommet af det installerede udstyr og de etablerede dataforbindelser I forbindelse med tilslutningsaftalen for en given virksomhed, region eller kommune påhviler ansvarsmæssigt Center for Cybersikkerhed. Center for Cybersikkerhed vil holde enhver virksomhed, region eller kommune skadesfri for sådanne hændelser.

29. maj 2019
FIDA-151247800-647742

Med venlig hilsen

Mette Stürup

Direkte: [+45 27152020]
Mail: [ms@fida.dkil]

Forsvarsministeriet

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

Sagsnummerhenvisning: 2019/002526

Forsikring & Pension

Forsikring & Pensions høringssvar til udkast til "Bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste"

03.06.2019

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

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

Sagsnr. GES-2019-00208
DokID 383339

Forsikring & Pension (F&P) værdsætter muligheden for at komme med et høringssvar til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

Der er generelt 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. Det arbejde deltager forsikrings- og pensionsbranchen gerne i og støtter den ambitiøse nationale dagsorden om at beskytte samfundsvigtige funktioner og kritisk digital infrastruktur.
s
Forsikrings- og pensionsbranchen bruger i dag mange ressourcer på at forebygge cyberhændelser, værne om borgernes personoplysninger og klæde medarbejderne godt på. Cybersikkerhed er af høj prioritet i branchen.

F&P finder dog, at bekendtgørelsen i sin nuværende form er for uklar i forhold til, hvem og hvornår et påbud kan forventes at skulle iværksættes. Endvidere mener F&P ikke, at omkostningerne forbundet med tilslutning til netsikkerhedstjenesten bør bæres af virksomhederne.

Konkrete bemærkninger til bekendtgørelsen vedr. §1

F&P ønsker, at lovforslaget udvides til at give virksomheder indsigt i, hvilke data/logs der indsamles fra infrastrukturen om medarbejdere og kunder, som videregives til Center for Cybersikkerhed.

Konkrete bemærkninger til bekendtgørelsen vedr. §2

F&P mener, at der bør være en yderligere præcisering af, hvilke (typer af) selskaber der forventes at være omfattet af definitionen – gerne gennem konkrete eksempler, jf. § 2 stk. 3, nr. 4 og 5.

§ 2 og §3. Det er uklart, hvilke tidsfrister, infrastrukturpåvirkninger og ressourcekrav som det er rimeligt at stille til virksomheden. Det virker ikke rimeligt, at virksomhederne selv skal afholde udgifter og uden begrænsning stille ressourcer til rådighed for at imødekomme CFCS' anmodninger.

I stk. 4 skrives, at påbud kun kan meddeles, såfremt mindre indgribende midler ikke er tilstrækkelige, men der er ikke forklaring på, hvad et mindre indgribende middel kan være. Det savner F&P for at kunne forstå, hvornår påbud reelt vil være aktuelle.

Når CFCS giver et påbud om tilslutning, bør de beskrive, hvad der udgør det særlige tilfælde, og på hvilken baggrund påbuddet baseres.

Formålet med påbuddet bør også beskrives (herunder hvilke data, logs og systemer, der skal overvåges), så virksomheden har mulighed for at afgrænse infrastrukturpåvirkninger og beskytte virksomheds- og kundedata, som ikke har en væsentlig betydning for Danmarks kritiske infrastruktur, og/eller som ikke er nødvendigt af hensyn til formålet med påbuddet (jf. §2. *Stk. 4.*). Ydermere bør det også præciseres, at det kun gælder danske data og ikke udenlandske, da flere af F&P's medlemmer også er udenlandske.

Sådanne beskrivelser er også vigtige for, at virksomheden kan vurdere CFCS' overholdelse af §2. *stk. 4.*, fx til det formål at kunne vurdere behovet for en klage jf. §2. *stk. 7.* 2).

I bekendtgørelsen angives, at et påbud kan defineres, så det kun omfatter dele af en virksomhed. Det er en teoretisk indsnævring, som i praksis ikke vil være mulig at implementere. Branchen har ikke designet sine processer, datastrømme og systemer efter, hvorvidt der bliver udført opgaver der har væsentlig betydning for Danmarks kritiske infrastruktur. Det betyder, at Center for Cybersikkerhed vil få adgang til data om mere, end der er behov for, og det er problematisk.

§2. *stk. 7, nr.* 3)
Hvis de ikke er omfattet af slettereglerne i § 17, stk. 2, nr. 2, i lov om Center for Cybersikkerhed, hvad er de så omfattet af? Det er mere hensigtsmæssigt at beskrive slettereglerne for de specifikke data herunder de data, der indsamles under §3. *stk. 2.*

§2. *stk. 7, nr.* 4)
Det bør tilføjes, at beskrivelsen af behandlingen af personoplysninger (herunder sletning, mulighed for indsigelse osv.) skal være tilstrækkelig til, at virksomheden kan opfylde sine forpligtigelser under GDPR.

Derudover bør det præciseres, hvorledes borgere og kunder skal underrettes om, at CFCS har adgang til deres personoplysninger i den pågældende virksomhed?

Konkrete bemærkninger til bekendtgørelsen vedr. §3

I §3 er angivet krav til virksomheder, som underlægges et påbud om at medvirke til opsætning og drift af alarmenheder, at stille nødvendig fysisk, teknisk og netværksmæssig understøttelse til rådighed og ikke mindst at sikre, at der er etableret passende sikkerhedsforanstaltninger for adgang til deres alarmenheder. F&P bemærker, at der kan være en væsentlig økonomiske omkostninger forbundet

med det arbejde, både til arbejdstid, men også til tekniske implementeringer og undersøgelser. Herunder også de underleverandører som bliver involveret, og som fakturerer deres tid overfor virksomheden. Der er ingen angivelse af kompensation herfor til virksomheden, hvilket vi mener der bør være.

§3. *stk. 3.* nr. 2.
Det kan have impact på vores forretning og dermed på vores regulerede aktiviteter, hvis en hændelse gør, at man ikke kan agere, som man finder bedst for enten at forhindre, stoppe eller recover for et angreb eller for en produktionsfejl.

§3, stk. 6
Krav om at underleverandører skal medvirke til opsætning og drift vil have impact på vores kontrakt og leverandørforhold, hvilket dels vil kræve kontraktuelle forhandlinger up front og potentiel have økonomisk impact.

Med venlig hilsen

Herietter Günther Sørensen

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@mmn.dk, sbu@fmn.dk

Vedr. sagsnummer 2019/002526

Svar på Høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste

3. juni 2019

Ingeniørforeningen, IDA, vil gerne takke for muligheden for at komme med svar på Høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

I lighed med tidligere høringssvar vedr. høring over udkast til ændring af lov for Center for Cybersikkerhed 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 høje niveauet for både i) viden, ii) kompetencer til at håndtere udfordringerne og iii) den rådgivningsindsats, der er sat i værk i 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 udkast til bekendtgørelse har IDA følgende bemærkninger:

§1 stk. 2
I tidligere høringssvar vedr. høring over udkast til ændring af lov for Center for Cybersikkerhed bemærkede IDA, at der blev lagt op til at udvide sensornetværkets funktionalitet. IDA anbefalede dengang derfor, at Center for Cybersikkerhed skrev 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 anbefalede 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.

Som vi læser bekendtgørelsen, vil de påbudte virksomheder og myndigheder komme på den gamle ordning (jf. §2). Men som vi læser §1 stk. 2 vil det kun være muligt for virksomheder og myndigheder, der melder sig frivilligt, at komme på den nye og udvidede ordning. Det er IDA fortsat imod, og anbefaler i lighed med tidligere høringssvar, 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. Såfremt IDA har læst § 1 stk. 2 forkert, bør bekendtgørelsen præciseres/tydeliggøres, sådan at det er klart, at man som virksomhed/myndighed har et valg i forhold til ikke at ville lade Center for Cybersikkerhed lave dataindsamlingen in-line.

Endvidere ifølge §1 stk. 2 kan tilslutningsaftalen med Center for Cybersikkerhed omfatte blandt andet "*løbende overførsel af logoplysninger*". Det er IDAs optik en meget bred formulering, og det bør præciseres, hvad der menes med logoplysninger.

§2

I IDAs høringssvar til udkast over ændring af lov for Center for Cybersikkerhed stillede IDA sig kritisk overfor den påbudsmulighed, som loven lagde op til. IDA har forståelse for at dele af den danske kritiske 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.

Vi gav dog udtryk for, at det er 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.

Vi læser nærværende udkast som et forsøg på at skærpe de situationer, funktioner, virksomheder og myndigheder, hvor et påbud om tilslutning til netsikkerhedstjenesten kan blive aktuelt.

Vi ser os dog nødsaget til at anmode om, at beskrivelsen af de situationer, hvor et påbud kan blive aktuelt, skærpes yderligere. De oplistede hensyn og situationer under **§2 stk. 3** er i IDAs optik simpelthen for altfavnende og på ingen måde afgrænsende. Særligt formuleringer som "befolkningens grundlæggende sikkerhed og velfærd" giver anledning til alskens fortolkningsmuligheder, og derfor på ingen måde konkret og definerede nok. Derudover bør man skrive ind i bekendtgørelsen, at man i forbindelse med påbud også tager højde for virksomhedens/myndighedens dokumenterede evne til at beskytte sig selv. Det bør alt andet lige være mere aktuelt og relevant at påbyde virksomheder/myndigheder netsikkerhedstjenesten, hvis det kan dokumenteres, at de ikke selv er i stand til at beskytte sig selv.

Derudover anerkender IDA, at udkast til bekendtgørelse følger IDAs anbefalinger i forhold til, at påbudte virksomheder og myndigheder ikke skal overvåges på interne netværk, men at de alene bliver overvåget på ydersiden af virksomhedens/myndighedens netværk.

§3
Det er pt. klart, at omkostninger i forbindelse med opsætning mv. påhviler den påbudte virksomhed/myndighed. Men det er imidlertid uklart, hvilke omkostninger der tales om. Af samme årsag bør bekendtgørelsen gøre mere ud af at belyse, hvilke omkostninger der er i spil – herunder fx mandetimer, performancetab og udgifter til dokumentation mv.

Endvidere bør paragraffen gennemskrives, idet den pt. er alt for bred i sine formuleringer. Det giver i IDAs optik Center for Cybersikkerhed alt for vide beføjelser til at bestemme over omfanget af implementeringen af påbuddet, og det kan i værste fald give meget store omkostninger for den påbudte virksomhed/myndighed.

Generelt mener IDA, at der skal være så meget klarhed som overhovedet muligt vedr. de her få mulige påbud. Herunder både potentielle omkostninger, omfang af implementering samt hvilke myndigheder/virksomheder, der kan blive påbudt netsikkerhedstjenesten. Center for Cybersikkerhed opfordres derfor på det kraftigste til at blive betragteligt mere konkrete, sådan at virksomheder/myndigheder kan have en fair chance for at vide, hvad der rammer dem i forbindelse med eventuelle påbud.

§3 stk. 4
I IDAs optik er denne formulering til gengæld *for* specifik. Man kunne med fordel erstatte med ”at den påbudte virksomhed/myndighed har pligt til straks at stille videre til en relevant person.

Med venlig hilsen

Grit Munk og Helena Juul Jensen
Chefkonsulenter, Politik, Analyse og Presse
IDA, Ingeniørforeningen

INSTITUT FOR
MENNESKE
RETTIGHEDER

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
MOBIL 91325761
MAAK@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 19/01285-2

11. JUNI 2019

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

HØRING OM UDKAST TIL BEKENDTGØRELSE OM TILSLUTNING TIL CENTER FOR CYBERSIKKERHEDS NETSIKKERHEDSTJENESTE

Forsvarsministeriet har ved e-mail af 3. maj 2019 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

Med udkastet gør ministeriet brug af bemyndigelsesbestemmelsen i § 3, stk. 5 i lov om Center for Cybersikkerhed, som senest blev ændret ved L 215 i foråret 2019.

Af lovens § 3, stk. 5 følger, at ministeren blandt andet kan fastsætte regler om centrets adgang til at påbyde virksomheder mv., der har "særligt samfundsvigtig karakter", at blive tilsluttet centrets netsikkerhedstjeneste med henblik på monitorering af netværkskommunikation. Centrets påbud omfatter de dele af virksomheden, der "har en væsentlig betydning for Danmarks kritiske infrastruktur".

I loven er der ikke fastsat objektive kriterier for, hvilke virksomheder der kan anses for at have en så væsentlig betydning for Danmarks kritiske infrastruktur, at de kan blive meddelt et påbud om tilslutning. Det følger dog af bemærkningerne til lovens § 3 stk. 5, at der skal være tale om myndigheder eller virksomheder, der leverer ydelser, som er så vigtige, at en sikkerhedshændelse hos den pågældende virksomhed eller myndighed vil kunne indebære en væsentlig indvirkning på samfundet, herunder i relation til f.eks. sikkerhed, forsyning, økonomi eller sundhed.

Ligeledes følger det af bemærkningerne, at samfundsvigtig karakter ikke kan defineres og i øvrigt kan omfatte virksomheder, som ikke i sig

selv er samfundsvigtige, men som kan være vigtige ud fra et sikkerhedsperspektiv.

I nærværende udkast er det i § 2, stk. 2 fastsat, at centret ved vurderingen af, om der skal meddeles påbud om tilslutning til netsikkerhedstjenesten skal vurdere, om en sikkerhedshændelse ville kunne medføre konsekvenser for "nationale sikkerhedsinteresser". Dette begreb er defineret i udkastets § 2 stk. 3 med i alt 5 kategorier af interesser.

Fordi de objektive kriterier for, hvornår virksomhederne bliver omfattet af påbuddet fremgår af udkastet til bekendtgørelse i stedet for loven, er kriterierne ikke udbygget med lovbemærkninger. Instituttet bemærker, at dette kan indebære en vis retssikkerhedsmæssig udfordring i brugen af kriterierne.

Herudover bemærker instituttet, at enkelte af kategorierne af beskyttede interesser, som for eksempel nr. 3 "forholdet til andre stater og internationale organisationer" og 5. "befolkningens grundlæggende sikkerhed og velfærd" er ganske vide i deres ordlyd.

- Instituttet anbefaler, at Forsvarsministeriet ændrer udkastets § 2, stk. 3, således at de beskyttede interesser opregnet i nr. 1 – 5 indsnævres og præciseres i deres ordlyd.

Med venlig hilsen

Marya Akhtar
SPECIALKONSULENT

IT-Branchens svar på høring over Bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste

IT-Branchen har modtaget Forsvarsministeriets høring af den vedrørende bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste. IT-Branchen har følgende bemærkninger til bekendtgørelsen.

IT-Branchen vurderer fortsat, at det er højest problematisk, at Center for Cybersikkerhed (CFCS) med de seneste ændringer af lov om Center for Cybersikkerhed, kan påbyde private virksomheder at blive tilsluttet netsikkerhedstjenesten. Vi mener således, at udmøntningen af loven risikerer at skade den danske digitale førerposition, ligesom krav om tilslutning kan have betydelige skadevirkninger for danske virksomheder.

Vi har en lang tradition i Danmark for tillid og åbenhed, og Danmark er internationalt kendt for at have et statsapparat med en høj grad af transparens. Danmark har en international styrkeposition, fordi der er tillid til dansk digitalisering, og fordi digitaliseringen er sket i tæt samspil mellem det offentlige og erhvervslivet.

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

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

Henset til de potentielle skadevirkninger bør bemyndigelsen til CFCS derfor afgrænses så snævert som muligt og så klart som overhovedet muligt.

Det er således afgørende for IT-Branchen, at bekendtgørelsen om tilslutning til CFCS netsikkerhedstjeneste sikrer, at CFCS kun har mulighed for at påbyde tilslutning for de allermest samfundskritiske virksomheder, samt at påbud kun anvendes hvis CFCS ikke på anden, mindre indgribende vis kan indsamle de relevante oplysninger. Endelig er det afgørende, at påbudte virksomheder ikke pålægges for omfattende krav, som vil være dyre eller problematiske at overholde.

1. Der mangler klarhed om hvem der kan blive påbudt tilslutning

Af bekendtgørelsen fremgår det, at CFCS i sin vurdering af, om en virksomhed kan påbydes tilslutning til netsikkerhedstjenesten skal lægge vægt på, om en sikkerhedshændelse vil kunne medføre konsekvenser for *nationale sikkerhedsinteresser*.

IT-Branchen er særligt bekymret for den meget brede definition i §2 stk. 3 af hvad nationale sikkerhedsinteresser omfatter. IT-Branchen vurderer særligt at punkt 5 ”interesser knyttet til befolkningens grundlæggende sikkerhed og velfærd” er formuleret så bredt, at stort set alle større virksomheder vil kunne falde ind under kategorien.

Det overlades hermed til CFCS selv og tilsynsmyndigheden i den relevante sektor 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 fjerner §2 stk. 3, punkt 5, og at beskrivelsen af hvilke virksomheder der kan påbydes tilslutning udbygges, således at der sker en afgrænsning.

2. Proportionalitet

IT-Branchen hæfter sig særligt ved, at det i §2 stk. 4 fremgår, at påbud kun kan meddeles, såfremt mindre indgribende midler ikke er tilstrækkelige.

IT-Branchen vurderer, at det til en hver tid vil være muligt at opnå formålet med påbuddet med mindre indgribende midler, fx gennem tilbud om tilslutning med virksomhedernes eget valg af teknologi og udstyr, hvor virksomheden selv ejer og kontrollerer udstyret. Udveksling af data vil med et sådan setup kunne ske på den tilsluttede virksomheds præmisser, krypteret og i et standardiseret format.

IT-Branchen foreslår, at CFCS pålægges altid at tilbyde denne mindre indgribende løsning inden der udsteds påbud om placering af CFCS's eget udstyr hos virksomheden.

3. Store krav til påbudte virksomheder

Endvidere frygter IT-Branchen, at der med bekendtgørelsen om tilslutning til CFCS netsikkerhedstjeneste stilles mange dyre og omfattende krav til de tilsluttede virksomheder.

I §3 stk. 1 fremgår det at virksomheder der er påbudt tilslutning, loyalt skal medvirke til netsikkerhedstjenestens opsætning og drift af en eller flere alarmenheder, og i stk. 3 punkt 1-3 pålægges virksomheder at blandt andet at stille den nødvendige fysiske, tekniske og netværksmæssige understøttelse til rådighed samt at etablere passende sikkerhedsforanstaltninger for adgang til netsikkerhedstjenestens alarmenheder.

Dette er meget upræcist formulerede krav, der lukker op for en bred fortolkning. Hvad er fx "passende sikkerhedsforanstaltninger". Disse krav kan nemt løbe op i en stor regning for de påbudte virksomheder. IT-Branchen foreslår, at påbudte virksomheder kompenseres for disse udgifter.

4. Problematiske krav ift. driftsleverandører

Enkelte krav i bekendtgørelsen kan være særligt problematiske at efterleve for en virksomhed.

Af §3 stk. 6 fremgår det, at en virksomhed der er meddelt et påbud, skal sikre, at eventuelle driftsleverandører i nødvendigt omfang medvirker til opsætning og drift af alarmenhederne.

Det må forventes at mange af de virksomheder der kan risikere et påbud om tilslutning til netsikkerhedstjenesten vil have en lang række driftsleverandører, herunder flere cloud-leverandører bl.a. med servere placeret i udlandet. Hvordan forestiller Forsvarsministeriet sig, at dette krav skal kunne håndteres, fx i en situation hvor en dansk virksomhed får driftet en løsning i EU eller i et tredje land? Og hvordan skal en virksomhed håndtere det, hvis driftsleverandøren ikke ønsker at medvirke til opsætning og drift af alarmenhederne?

IT-Branchen vurderer, at dette krav i realiteten vil være umuligt at overholde for en virksomhed, der får driftet et eller flere systemer i skyen. Dette krav, kan derfor reelt ende med at umuliggøre anvendelse af cloud-løsninger for en meget lang række danske virksomheder.

5. Øvrige bemærkninger

I § 4 stk. 2 fastslås det, at CFCS er dataansvarlig for det indsamlede data. Det fremgår dog ikke, om det kan sluttes heraf, om den oprindelige dataansvarlige er friholdt fra GDPRs krav om at informere datasubjekterne, når data overlades/overføres til en anden dataansvarlig. Dette bør fremgå af bekendtgørelsen.

Der er ingen beskrivelse af eventuelle krav om hemmeligholdelse. Det bør gøres klart, om det står parterne frit at kommunikere offentlig om, at de har givet/fået påbud, og om der er et timelimit på evt. hemmeligholdelse.

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

Til Forsvarsministeriet (Sag 2019/002526)

KL-svar på høring af forslag til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste

Dato: 29. maj 2019

Sags ID: SAG-2019-03120
Dok. ID: 2766608

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Bekendtgørelsen er en udfyldelse af lov om Center for Cybersikkerhed og i KLs høringssvar til denne blev der udtrykt bekymring vedr. overvejelser om erstatningsansvar, såfremt det skulle ske, at nettjenesten er årsag til kompromittering af borgerdata. Herunder sammenhængen med Datatilsynets udmeldinger om evt. overtrædelser af meddelelseshemmeligheden, krænkelser af medarbejderes private data mv. Det udestår forsat i udkastet til tilslutning om netsikkerhedstjenesten, at disse problemstillinger adresseres.

Det udestår, hvad definitionen af "stationære data", omfatter, som også som omtales forskellige steder i L215 og dermed også har betydning for forståelsen af høringsudkast til bekendtgørelsen.

Frivillig tilslutning
Af bekendtgørelsen fremgår det, ikke hvad Center for Cybersikkerheds (CFCS) betingelser for frivillig tilslutning omfatter, og om den myndighed der tilsluttes har mulighed for tilpasning af aftalen ift. egne behov. Skal frivillig tilslutning forstås således, at den enkelte myndighed selv beslutter eller har krav på, om de vil tilsluttes?

Indhold af standardbeskrivelse
Det fremgår af bekendtgørelsesudkastet, at der ved påbud medsendes en standardbeskrivelse af CFCSs behandling af personoplysninger, som kommunen kan bruge til at informere medarbejdere. Det fremgår ikke, hvad indholdet af denne standardskrivelse er.
KL anbefaler, at standardbeskrivelsen adresserer hvilke oplysninger, der kan indsamles om ansatte, borgere, virksomheder samt kommunalbestyrelses- og regionsrådsmedlemmers varetagelse af deres hverv jf. loven om Center for cybersikkerhed.

Bekendtgørelsesudkast § 2, henviser til at der vil kunne gives påbud om overvågning af en myndigheds net. Det udestår, hvordan man teknisk skal håndtere dette, hvis netsikkerhedstjenesten ikke skal have adgang til hele kommunens infrastruktur.

Det fremgår, at kommunen ved et påbud om adgang, skal stille den nødvendige fysiske, tekniske og netværksmæssige understøttelse til rådighed. Der er brug for klarhed over, hvordan CFCSs eventuelle ansvar og erstatningsspørgsmål fastlægges, såfremt det påbydes kommunen at installere software, hardware eller andet, samt hvordan ansvaret placeres ift. evt. erstatningsspørgsmål, såfremt kommunens egne medarbejdere har medvirket til installationen.

Det fremgår også, at kommunen skal sikre, at eventuelle driftsleverandører i nødvendigt omfang medvirker til opsætning og drift af alarmenhederne. Dette krav fremgår ikke i de eksisterende kontrakter med driftsleverandører. Det udestår, om et sådant påbud fra CFCS også gælder ift. det tilfælde, hvor en driftsleverandør ikke ønsker at efterleve CFCSs påbud til kommunen.

Økonomiske og administrative konsekvenser
Gennemførelse af de tiltag af et evt. påbud, der er lagt op til i bekendtgørelsen vil medføre merudgifter for kommunerne, hvorfor det forventes at kommunerne vil blive kompenseret for dette.

Endelig skal nævnes, at KL gerne indgår i videre dialog om bekendtgørelsens indhold og særligt ift. konsekvenser for de lokale myndigheder.

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

Høringssvar

LÆGEFORENINGEN

Høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste

3. juni 2019
Sagsnr: 2019-513
Aktnr: 1932075

Lægeforeningen finder det vigtigt, at Center for Cybersikkerheds adgang til patientfølsomme helbredsoplysninger i sundhedsvæsenet følger sundhedslovens bestemmelser.
Endvidere vil Lægeforeningen påpege, at patientbehandlingen vil blive besværliggjort, hvis journaldata slettes.

Lægeforeningen har modtaget bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste i høring.

Lægeforeningen har tidligere afgivet høringssvar, da lovforslaget var i høring (høringssvaret er vedlagt).

Lægeforeningen deler lovens overordnede målsætning om at styrke cybersikkerheden i vores samfund.

Lægeforeningen finder, at der er følgende opmærksomhedspunkter i forbindelse med bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste

1) Lægeforeningen hilser velkommen, at der skal foreligge en beskrivelse af Center for Cybersikkerheds behandling af personoplysninger (jf § 2 stk. 7 pkt. 4).

   Lægeforeningen finder det vigtigt, at denne beskrivelse følger sundhedslovens bestemmelser om adgang til patientfølsomme helbredsoplysninger, når det er den type oplysninger, som centeret behandler.

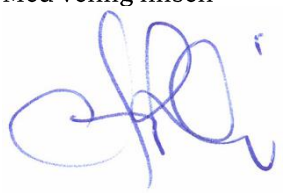
2) Der vil besværliggøre patientbehandlingen, hvis stationære data (dvs. journaldata slettes).

   Derfor mener Lægeforeningen at det er godt, at der skal foreligge oplysning, om man er omfattet af slettereglerne (jf § 2 stk. 7 pkt. 3), da det betyder, at ikke alle, der tilsluttes Center for Cybersikkerheds netsikkerhedstjeneste er i risiko for at få slettet data.

3) Lægeforeningen pointerede i forbindelse med lovforslaget, at der kan blive meromkostninger for de læger i almen praksis og i speciallægepraksis, der er meddelt påbud.

Det er fortsat et punkt, som Lægeforeningen vil gøre opmærksom på, idet det er nævnt i §3 stk. 3 pkt. 1) – 3), at virksomhed, region eller kommune skal stille forskellige systemer til rådighed for Center for Cybersikkerhed, hvilket Lægeforeningen vurderer kan pålægge vores medlemmer merudgifter.

Med venlig hilsen



Andreas Rudkjøbing
Formand for Lægeforeningen

Domus Medica
Kristianiagade 12
DK-2100 København Ø

Tlf.: +45 3544 8500
Tlf.: +45 3544 8141 (direkte)
E-post: dadl@dadl.dk
E-post: llg@DADL.DK
www.laeger.dk

regionernes
sundheds-it

Forsvarsministeriet
fmn@fmn.dk

03. 06.2019
2019/002526

Fællesregionalt høringssvar over udkast til bekendtgørelse om tilslutning til CFCS' netsikkerhedstjeneste

Cyber- og Informationssikkerhed har en stor opmærksomhed hos regionerne, og har igennem mange år været en central opgave. Set i lyset af den voksende cybertrussel er opgaven påkrævet, herunder at der forefindes og implementeres nationale initiativer, som kan adressere cyberangreb og medvirke ved håndtering.
Regionerne er dermed positive over for lovforslagets formål.

Regionerne vil dog gøre opmærksom på, at der er flere uklarheder i lovforslaget, som potentielt kan have store konsekvenser for it-drift, myndighedsudøvelse og borgernes rettigheder i de enkelte regioner.

Det er ikke tydeligt beskrevet, hvordan man vil håndtere eventuelle konsekvenser på området. Center for Cybersikkerheds hjemmel til øgede beføjelser og mandater er på den ene side plausible i forhold til formålet, men på den anden side er de meget bekymrende i forhold til de store konsekvenser for it-drift og myndighedsudøvelsen i de enkelte regioner - ligesom tilslutningsaftalen ligeledes indbefatter handlinger, der berører principielle rettigheder som patientsikkerhed og borgerrettigheder.

Det er særligt Center for Cybersikkerheds mulighed for installation og drift af sikkerhedssoftware på lokale enheder, som vækker bekymring.
Der er stadig usikkerhed om, hvordan netsikkerhedstjenesten er udformet, og hvordan den tilsluttes.
Det fremgår af § 3, at opsætning, konfigurering, drift og nedtagning af alarmenheder foretages af netsikkerhedstjenesten. Det er uklart, hvilke potentielle konsekvenser tilslutningen vil have i forhold til regionernes it-setup og dermed i sidste ende patientsikkerheden.
Det er desuden ikke angivet, hvem der er ansvarlig ved eventuelle nedbrud i regionernes kritiske infrastrukturer, som følge af implementeringen af sikkerhedssoftwaren.
Regionerne anbefaler, at det positivt fremgår af bekendtgørelsen, at tilslutningen ikke må have negativ påvirkning af de systemlandskaber, hvor tilslutningen foretages.

Endvidere er det uklart, hvem der bærer udgifterne forbundet med tilslutning til netsikkerhedstjenesten. Det fremgår af § 3, at den organisation som meddeles påbud, skal medvirke loyalt til netsikkerhedstjenestens opsætning og drift af en eller flere alarmenheder, ligesom det fremgår, at det er organisationen, der skal sikre, at eventuelle driftsleverandører, i nødvendigt omfang, medvirker til opsætning og drift af alarmenhederne.
I denne henseende vil regionerne anbefale, at det positivt fremgår af bekendtgørelsen, at interne omkostninger samt afledte udgifter i forbindelse med påbud om tilslutning til netsikkerhedstjenesten afholdes af Center for Cybersikkerhed.

Der er stor usikkerhed i forhold til påbuddet i § 2 efter § 3, stk. 4 i lov om Center for Cybersikkerhed, hvor regionerne kan blive påbudt at tilslutte sig netsikkerhedstjenesten.
Forslagets § 2 stk. 5 indeholder hjemmel til at udstede påbud, som forudsætter enighed mellem Center for Cybersikkerhed og tilsynsmyndigheden – i modsætning til ordlyden af Lov om Center for Cybersikkerhed § 3 stk. 4, som alene angiver Center for Cybersikkerhed, som udsteder af påbud. Her er det er vanskeligt at afgøre, hvorvidt Center for Cybersikkerhed kan påbyde en myndighed denne tjeneste, eller om påbuddet sker under forudsætning af en gensidig enighed.
Den løbende vurdering af et meddelt påbud, i henhold til § 2 stk. 8, skal dog (uanset) foretages uden involvering af tilsynsmyndigheden, som også forudsat i lovens § 3 stk. 4.
Denne usikkerhed søges afklaret.
Det er endvidere uklart, hvem der er tilsynsmyndighed for regionerne i denne henseende.

Slutteligt påpeger regionerne, at implementering af netsikkerhedstjenesten afføder et behov for at tydeliggøre, hvilke data der kan, må eller skal ske overførsel af.
Regionerne anbefaler, at der i bekendtgørelsen tilføjes information om, hvilke data bekendtgørelsen dækker, ligesom det bør anføres, hvorvidt eventuelle data ikke er omfattet.

Regionerne står til rådighed, hvis der måtte være afklarende spørgsmål.

Med venlig hilsen

På regionernes vegne, den tværregionale styregruppe for informationssikkerhed

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Rådet for Digital Sikkerheds høringssvar om bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

Rådet for Digital Sikkerhed (herefter Rådet) takker for muligheden for at afgive bemærkninger til høringssvar om bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste, som Rådet modtog 16. juli med frist for bemærkninger senest den 26. juli 2019 kl. 12. Rådet beklager at have overskredet svarfristen. Grundet den korte tidsfrist, der i øvrigt lå i sommerferien, har det ikke været muligt at afgive svar før. Det vil være ønskeligt fremover at modtage høringer med længere frist og udenfor ferieperioden.

Rådet støtter, at der som udgangspunkt er tale om en frivillig tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste. Rådet er af den opfattelse, at påbud om tilslutning er problematisk for konkurrenceevne for virksomheder både i sikkerhedsbranchen og samfundskritiske virksomheder i Danmark og ikke mindst er det problematisk for retssikkerheden. I stedet bør et samarbejdet mellem CFCS og it-sikkerhedsbranchen fremme sikkerheden for erhvervslivet. Generelt bør deling af viden med virksomhederne være et princip i bekendtgørelsen. I tilfælde af et påbud bør der være en tydelig og let tilgængelig klageadgang gerne hos anden instans.

Herunder følger mere konkrete bemærkninger fra Rådet.

Med bekendtgørelsens § 2 indfører bestemmelsen et påbud. Rådet er uenig i dette og mener, der bør være tale om en frivillig ordning, hvor CFCS ved installation af udstyr tager hensyn til organisationens økonomiske forhold samt mindst mulig forstyrrelse af organisationens daglige drift.

§ 2, stk.3 definerer samfundsvigtige interesser og hermed organisationer omfattet af loven og bekendtgørelsen. Rådet støtter en præcisering og anbefaler yderligere, at der i forhold til afgrænsning trækkes på internationale erfaringer.

§ 2 stk. 7 litra 1 bør inkludere en beskrivelse af, hvilke data eller oplysninger man i påbuddet konkret eftersøger. Den pågældende organisation vil ofte kunne kvalificere og gøre opsætningen af udstyret mest effektivt, hvis det oplyses, hvilken type af data der eftersøges, eller hvor data kommer fra.

§ 3 stk. 2 litra 2 indeholder en bestemmelse om, at den konkrete virksomhed ikke må ændre i sin tekniske opsætning, hvis det kan påvirke de opsatte alarmenheder, medmindre det er aftalt på forhånd. Her bør ordet ”aftalt” ændres til ”meddelt” idet en virksomhed ikke unødigt bør begrænses i sin ret til at ændre sin opsætning. Den frie ret til at planlægge sin drift skal ikke aftales med CFCS – det skal højst meddeles.

Rådet står naturligvis til rådighed for en uddybelse af ovenstående synspunkter.

På bestyrelsens vegne

Henning Mortensen
Formand, Rådet for Digital Sikkerhed

Forsvarsministeriet

Til: fmn@fmn.dk

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

3. juni 2019

Høringssvar vedrørende udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds (CFCS) netsikkerhedstjeneste 2019/002526.

Forsvarsministeriet har udsendt udkast til bekendtgørelse om tilslutning til CFCSs netsikkerhedstjeneste i høring.

Teleindustrien (TI) skal hermed fremkomme med sine bemærkninger til enkelte bestemmelser i udkastet.

Nationale sikkerhedsinteresser

Det er positivt, at CFCS har skærpet tonen i forhold til, at påbud ikke kan gives med mindre de er nødvendige og proportionale bl.a. ved at inkludere en definition af, hvad der kan anses for nationale sikkerhedsinteresser, hvis beskyttelse kan føre til påbud, og som sætter barren relativt højt (§ 2, stk. 3).

TI finder, at det bør præciseres, hvor omfattende dokumentation og hvilke informationer selskaber evt. skal udlevere eller stille til rådighed til brug for vurderingen af, om et selskab evt. kan være omfattet af et påbud om tilslutning til netsikkerhedstjenesten, jf. §2 stk. 2.

Beslutning om påbud

Det er positivt, at påbud ikke kan besluttes af CFCS alene, men at der foreslås indført en regel om, at det kræver enighed med tilsynsmyndigheden i den relevante sektor (jf. § 2, stk. 5).

For telesektorens aktører har dette dog ingen reel betydning, idet CFCS også er tilsynsmyndighed for telesektoren. For at sikre lige retssikkerhed for alle selskaber foreslår TI, at der her etableres en tilsvarende to-faktor myndighedsudøvelse for telesektoren med inddragelse af en anden myndighed (departement eller styrelse).

Installation af software

Det er positivt, at det er sikret i formuleringen af bekendtgørelsen, at der kun er tale om monitorering på ydersiden af virksomhederne eller myndighederne og ikke installation af software osv. (§ 2, stk. 6), hvilket afspejler den justering af de oprindelige udkast til lovforslag, der skete på baggrund af høringen, hvor bl.a. TI foreslog en begrænsning af den foreslåede lovhjemmel.

TI efterspørger en nærmere beskrivelse af, hvilken slags alarmenheder der skal forbindes til netværkene og hvilken information, der skal opsamles.

Endvidere efterlyses en nærmere beskrivelse af de praktiske opgaver, der skal udføres i forbindelse med tilslutning til netsikkerhedstjenesten, herunder en nærmere beskrivelse af, om CFCS opsætter, installerer software og forestår driften, og om det er operatørerne selv, der stiller den nødvendige fysiske, tekniske og netværksmæssige understøttelse til rådighed, eller om CFCS også håndterer dette.

Løbende vurdering af påbud

Af § 2, stk. 8, fremgår, at CFCS løbende skal vurdere, om forudsætningerne for et meddelt påbud fortsat er tilstede.

TI støtter, at der skal foretages en løbende vurdering af forudsætningerne for et påbud. TI foreslår endvidere, at såfremt CFCS ikke inden for fristen på et halvt år foretager en vurdering af, om et meddelt påbud skal opretholdes, da bortfalder påbuddet automatisk.

Oplysninger om den digitale infrastruktur

Af § 3, stk. 2, fremgår, at en virksomhed, region eller kommune, der er meddelt et påbud, efter anmodning fra CFCS skal stille de nødvendige oplysninger om konfiguration og drift af deres digitale infrastruktur til rådighed for netsikkerhedstjenesten til brug for opsætning og drift af alarmenheder, herunder:

1) Oversigt over netarkitektur og segmentering.
2) Liste over netværkssystemer og infrastrukturkomponenter, herunder type og funktion.
3) Liste over ip-adresser, der håndterer netværksbaserede tjenester, og allokering af disse.
4) Angivelse af, hvilke dele af driften af den digitale infrastruktur, der varetages af eventuelle driftsleverandører.

Det skal bemærkes, at forpligtelsen til at stille oplysninger til rådighed ikke indebærer en forpligtelse til udlevering af oplysninger, da sådanne oplysninger kan være fortrolige.

Change Management

Det fremgår af udkastets §3, stk. 3, at det påhviler virksomheden at sikre, at der ikke foretages fysiske, tekniske og netværksmæssige ændringer, som kan påvirke driften af alarmenhederne, med mindre dette på forhånd er aftalt med net-sikkerhedstjenesten.

TI finder det meget problematisk, at det foreslås, at selskaber ikke må foretage ændringer i deres eget net uden aftale med CFCS. CFCS har ikke hjemmel til at lave en sådan begrænsning og forhindre ændringer og lignende i udbydernes net.

Det rejser også et konkret spørgsmål om, hvordan den nødvendige Change Management i givet fald tænkes koordineret omkring de "tekniske og netværksmæssige ændringer, som kan påvirke driften af alarmenhederne" (§3 stk. 3 punkt 2)?

Adgangsstyring

Det bør præcises, hvad der er passende sikkerhedsforanstaltninger for adgang til net-sikkerhedstjenestens alarmenheder og tilhørende udstyr (§3 stk. 3, nr. 3).

Databehandleraftaler

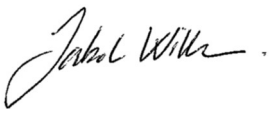
Det ønskes belyst, hvorvidt der kræves databehandleraftale mellem CFCS og de enkelte operatører ved udveksling af personhenførbare oplysninger i forbindelse med logning.

Klageadgang

TI opfordrer til, at det præciseres, hvorledes der er sikret klageadgang vedr. afgørelser truffet efter bekendtgørelsen.

Med venlig hilsen

Jakob Willer, direktør, Teleindustrien



Tilsynet med Efterretningstjenesterne

Forsvarsministeriet
Holmens kanal 9
1060 København K

Dato: 3. juni 2019
Sagsnr.: 2019-152-67
Dok.: 20461

Høring over udkast til Bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste

Ved brev af 3. maj 2019 har Forsvarsministeriet anmodet Tilsynet med Efterretningstjenesterne om bemærkninger til udkast til Bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

I den anledning skal tilsynet oplyse, at udkastet ikke giver anledning til bemærkninger.

Der henvises til Forsvarsministeriets sagsnummer 2019/002526.

Med venlig hilsen
Tilsynet med Efterretningstjenesterne

v/Emil Bock Greve
Sekretariatschef

Borgergade 28, 1.
DK-1300 København K
t 25 50 10 34
www.tet.dk

Fra: Kristian Henningsen <krhge@vestas.com>
Sendt: 3. juni 2019 15:50
Til: FMN-MYN-FORSVARSMINISTERIET
Cc: FMN-TBL Larsen, Tina Kathrine Berg; FMN-SBU Østergren, Stine Busch
Emne: 2019/002526 - Høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste

Kategorier: Christina

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

Vestas skal hermed beklage, at vi ikke har sendt et hørringsvar inden kl. 12:00 dagsdato. Vestas håber, at Center for Cybersikkerhed alligevel vil tage nedenstående betragtning med i ift. bekendtgørelsen om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

Vestas betragtninger til høringen kan findes i DI's høringssvar. Vestas vil dog godt selvstændig bemærke, at vi som virksomhed i lovforslaget savner en forståelse af forretningsmæssige hensyn ift. kunder i bestemte regioner, hvor det må forventes, at disse lande ikke vil se mildt på, at data fra vindparker flyder tilbage til Vestas og videre til Center for Cybersikkerhed.

Venlig hilsen / Yours sincerely

Kristian Henningsen
Head of Public Affairs Denmark
Group Marketing, Communications & Public Affairs

Vestas Wind Systems A/S
M: +4540610505
krhge@vestas.com
http://www.vestas.com

Company reg. name: Vestas Wind Systems A/S
This e-mail is subject to our e-mail disclaimer statement.
Please refer to www.vestas.com/legal/notice
If you have received this e-mail in error please contact the sender.

Classification: Restricted

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-43-19
Den 19/07-2019

Forsvarsministeriet har ved brev af 16. juli 2019 (sagsnr. 2019/003498) anmodet om eventuelle bemærkninger til høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Helle Bertung

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-39-19
Den 20/05-2019

Forsvarsministeriet har ved brev af 3. maj 2019 (sagsnr. 2019/002526) anmodet om eventuelle bemærkninger til høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Helle Bertung

Østre Landsret
Præsidenten

Den 05/08-2019
J.nr. 40A-ØL-35-19
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 16. juli 2019 (Sagsnr. 2019/003498) anmodet om eventuelle supplerende bemærkninger til høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

I den anledning skal jeg meddele, at landsretten kan henholde sig til vores brev af 20. maj 2019, om ikke at udtale sig om udkastet.

Med venlig hilsen

Bent Carlsen

Ellen Basse Porsbo

Østre Landsret
Præsidenten

Den 20/05-2019
J.nr. 40A-ØL-35-19
Init: rsl

Forsvarsministeriet
Holmens Kanal 9
1060 København K

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

Forsvarsministeriet har ved brev af 3. maj 2019 (Sagsnr. 2019/002526) anmodet om eventuelle bemærkninger til høring over udkast til bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Bent Carlsen

Ellen Basse Borsbo