DANSK ERHVERV
Børsen
1217 København K

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

Forsvarets Efterretningstjeneste,
Center for Cybersikkerhed
Att.: Anette Arnsted
Kastellet 30
2100 København Ø

Sendt til:
fe@fe-mail.dk
fe-4418@fe-ddis.dk

Sagsnr.: 2020/001583.

Den 4. februar 2021

Høring over udkast til bekendtgørelser om sikkerhed i net og tjenester

Nærværende høringssvar drejer sig om *Udkast til bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester*.

Dansk Erhverv sætter pris på at få mulighed for at indgive høringssvar på dette område, som efter vores mening er af stor vigtighed.

Generelle bemærkninger

Sikkerheden i teleinfrastrukturen er af højeste betydning for et velfungerende informationssamfund. Derfor støtter Dansk Erhverv generelt tiltag, som har til formål at styrke teleselskabernes mulighed for at øge sikkerheden i telenet og -tjenester.

Overordnet finder Dansk Erhverv det vigtigt at skabe størst mulig gennemskuelighed og juridisk klarhed for udbydere af net- og kommunikationstjenester. Det vil derfor være hensigtsmæssigt, at Center for Cybersikkerhed (evt. i samspil med andre relevante myndigheder) laver tydelige definitioner og afgrænsninger til denne bekendtgørelse. F.eks. er definitionen af "kritiske netværkskomponenter uhensigtsmæssig bred, ligesom "business support systemer" ikke er et begreb, hvorom der findes en ensartet branchemæssig forståelse.

Dansk Erhverv er endvidere af den holdning, at regulering bør være proportionel ift. den risiko, der adresseres og væres fokuseret på den reelle mulighed for håndhævelse. Dvs. reguleringen bør adressere netop de net- og kommunikationstjenester, hvor en sikkerhedshændelse vil have størst negativ konsekvens, og bør vurderes ud fra, om Center for Cybersikkerhed har en de facto mulighed for at håndhæve reglerne.

For de tjenester, der kendetegnes ved ofte eller altid at have grænseoverskridende karakter, opfordrer Dansk Erhverv til, at danske myndigheder i højere grad arbejder for, at den tilsvarende regulering ligeledes er international, så en udbyder undgår at skulle melde ind til en flerhed af nationale myndigheder, men fx kan melde ind til én EU-myndighed.

Specifikke bemærkninger

§1
En række begreber (fx kritiske netkomponenter) er ikke klart defineret, ligesom der mangler afgræsninger (fx for centrale versus ikke-centrale routere). Dansk Erhverv foreslår, at bekendtgørelsen i højere grad bør gøre brug af klare definitioner og afgræsninger, som bl.a. kan baseres på en konkret risikovurdering el. lign.

§3-6
I overensstemmelse med artikel 40 samt præambel 94-95 i det europæiske kodeks for elektronisk kommunikation (EU direktiv 2018/1972), finder Dansk Erhverv det væsentligt at få sikkerhed for, om forpligtelserne i disse paragraffer i bekendtgørelsen gælder for den bredere gruppe af nummeruafhængige interpersonelle kommunikationstjenester (NUIK-tjenester) og/eller netværksuafhængige nummerbaserede interpersonelle kommunikationstjenester[1].

Dansk Erhverv mener, det vil være uhensigtsmæssigt at omfatte denne type kommunikationstjenester uden en forudgående evidensbaseret vurdering af, hvorvidt disse forpligtelser er nødvendige. Vi beder derfor de danske myndigheder om at bekræfte, om dette er tilfældet.

Samtidig understreges det, at såfremt danske myndigheder ikke vil undtage de ovennævnte typer af kommunikationstjenester, bør nye informationsforpligtelser ikke træde i kraft uden en høring blandt de relevante udbydere, ligesom forpligtelserne bør baseres på evidens og være passende, proportionale og tage hensyn til den kontekst, udbyderne opererer i.

Derudover mener vi, det er vigtigt, at udbydere har klarhed om, hvor hurtigt de kan forvente en reaktion fra Center for Cybersikkerhed, når der foretages en underretning. Dansk Erhverv foreslår derfor, at der i §5 indsættes en frist på max. 20 arbejdsdage dage for, hvornår Center for Cybersikkerhed skal træffe afgørelse om, hvorvidt der er behov for et påbud om indsendelse af endeligt aftaleudkast til centeret.

§7-8
Den skærpede frist for underretning i §7 stk. 3 kan reducere udbyderes mulighed for at analysere en hændelse forud for indberetning, hvilket kan medføre unødvendige indberetninger af hændelser, som ved nærmere eftersyn ikke er væsentlige ud fra de opstillede kriterier.

Dansk Erhverv arbejder med udgangspunkt om, at der skal være fair og lige konkurrence mellem udbydere – herunder de forpligtelser, udbyderne underlægges. Vi finder det ikke klart, hvorfor der i § er gjort forskel på grænseværdier for hhv. NUIK-tjenester og mobilabonnementer. Vi foreslår derfor, at grænseværdierne ensrettes, så de for brugertimer og slutbrugere også er 50.000 for mobilabonnementer.

[1] Et eksempel på netværksuafhængige nummerbaserede interpersonelle kommunikationstjenester er "Skype til telefon"-planer

Vi ønsker, at forpligtelserne for NUIK-tjenester også skal gælde de netværksuafhængige nummerbaserede interpersonelle kommunikationstjenester, som på nuværende tidspunkt ikke falder under nogen af de andre kategorier, da disse minder mest om NUIK-tjenester.

For disse typer tjenester vil det være særdeles uhensigtsmæssigt at bliver underlagt krav om at anmelde hændelser til nationale myndigheder. For disse tjenester vil et nedbrud aldrig eller yderst sjældent skyldes en fejl på en lokal netværkskomponent, og et nedbrud vil med større sandsynlighed være grænseoverskridende og gælde i flere lande og/eller regioner. Disse udbydere bør ikke underlægges krav om at skulle vurdere et enkelt nedbrud på tværs af 27 (EU) eller 31 (EØS) landes forskellige kriterier.

Dansk Erhverv understreger behovet for, at der på sigt bør etableres et (1) sæt af harmoniserede kriterier for hændelsesrapportering indenfor EU, ligesom det i størst mulig grad bør tilstræbes at strømline hændelsesrapporteringsproceduren på tværs af grænser. Hvor det er muligt bør hændelsesrapportering ske til en tværeuropæisk enhed, så virksomhedernes forpligtelser ikke giver unødvendige administrative byrder, samtidig med slutbrugerne ydes tilstrækkelig beskyttelse på tværs af Europa.

Dansk Erhverv opfordrer de danske myndigheder til at være opmærksomme på ENISA-rapporten af 10. januar 2020 *'Security Supervision under the EECC'*, som anerkender, at det eksisterende regime på tværs af Europa bør opdateres, og at der ideelt bør udvikles en fælles grænseværdi og rapporteringsmodel, så et konsistent system for hændelsesrapportering kan implementeres, der samtidig tager højde for de særlige karakteristika ved OTT-kommunikationstjenester.

Vi anmoder de danske myndigheder om at bakke op om etableringen af en sådan fælleseuropæisk løsning, så én hændelse også kun skal anmeldes et sted.

Dansk Erhverv står gerne til rådighed for uddybning af ovenstående.

Med venlig hilsen,

Christian von Stamm Jonasson
Erhvervspolitisk konsulent

From: Anne Katrine Boje <AKBO@SUM.DK>
Sent: 3 februar 2021 14:10 (UTC +01)
To: fe@fe-mail.dk <fe@fe-mail.dk>; fe-4418@fe-ddis.dk <fe-4418@fe-ddis.dk>
Subject: H?ingssvar vedr. sagsnr. 2020/001583

Til Center for Cybersikkerhed

Sundhedsministeriet har ingen bemærkninger til høringen vedrørende bekendtgørelse om sikkerhed i net og tjenester. Vi takker for muligheden for at afgive svar til høringen.

Med venlig hilsen

Anne Katrine Boje
Stud. Jur, Sundhedsjura

Sundheds- og Ældreministeriet ● Holbergsgade 6 ●
1057 København K ● Tlf. 7226 9000 ● Fax 7226 9001 ● www.sum.dk

SUNDHEDS- OG ÆLDREMINISTERIET

INSTITUT FOR MENNESKE RETTIGHEDER

Center for Cybersikkerhed
Kastellet 30
2100 København Ø
E-mail: fe@fe-mail.dk og fe-4418@fe-ddis.dk

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
MOBIL 91325719
MIKL@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 21/00354-2

2. FEBRUAR 2021

HØRINGSSVAR OVER UDKAST TIL BEKENDTGØRELSER OM SIKKERHED I NET OG TJENESTER

Center for Cybersikkerhed har den 7. januar 2021 sendt udkast til følgende fire bekendtgørelser i høring:

- Udkast til bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.
- Udkast til bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på området for sikkerhed i net og tjenester.
- Udkast til bekendtgørelse om sikkerhed og beredskab i net og tjenester.
- Udkast til bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester.

Institut for Menneskerettigheder har ingen bemærkninger til de fire udkast.

Instituttet bemærker, at instituttet er blevet opmærksom på høringen på Høringsportalen, og at instituttet ikke ses at have modtaget høringen på mail (info@humanrights.dk) – til trods for, at instituttet fremgår af høringslisten.

Der henvises til sagsnummer 2020/001583.

Med venlig hilsen

Mikkel Lindberg Laursen
SPECIALKONSULENT

From: Torben Stærgaard <TS@KM.DK>
Sent: 1 februar 2021 07:57 (UTC +01)
To: Judith <FE-4418@fe-ddis.dk>; fe@fe-mail.dk <fe@fe-mail.dk>
Cc: Ulla B. Kristiansen <UBK@KM.DK>
Subject: KM: Høringssvar vedr. 2020/001583 (KM F2.: 147333)

Kirkeministeriet har ingen bemærkninger til udkast til bekendtgørelser om sikkerhed i net og tjenester:

- Bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på området for sikkerhed i net og tjenester
- Bekendtgørelse om sikkerhed og beredskab i net og tjenester
- Bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester
- Bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv

Til: Børne-og Undervisningsministeriet (uvm@uvm.dk), Erhvervsministeriet (em@em.dk), Justitsministeriet (jm@jm.dk), KM hovedpostkasse (km@km.dk), Kulturministeriet (kum@kum.dk), Miljø- og Fødevareministeriet (mfvm@mfvm.dk), Skatteministeriet (skm@skm.dk), Social- og Indenrigsministeriet (sim@sim.dk), Sundheds- og ældreministeriet (sum@sum.dk), Transport- og Boligministeriet (trm@trm.dk), Uddannelses- og Forskningsministeriet (ufm@ufm.dk), Udenrigsministeriet (um@um.dk), Udlændige- og Integrationsministeriet (uim@uim.dk), Statsministeriet (stm@stm.dk), Beskæftigelsesministeriet (bm@bm.dk), fm@fm.dk (fm@fm.dk), kefm@kefm.dk (kefm@kefm.dk)
Fra: Judith (FE-4418@fe-ddis.dk)
Titel: Høring over BEK vedr. net- og kommunikationstjenester (it-sikkerhed)
E-mailtitel: Høring
Sendt: 07-01-2021 14:30

Til rette vedkommende

Se venligst vedhæftede høring. Høringsmaterialet er lagt på Høringsportalen i dag.

Med venlig hilsen

Center for Cybersikkerhed

Med venlig hilsen

Torben Stærgaard
Kontorchef

Kirkeministeriet / Folkekirkens It
T: 7020 2535 / D: 7020 2585 / Mail: ts@km.dk
Rådhusstræde 2 / 1466 København K/ www.kirkenettet.dk
CVR nr. 2720 6808 / EAN nr. 5798 000 818 644

From: <19kontor@rigsrevisionen.dk>
Sent: 29 januar 2021 10:11 (UTC +01)
To: fe@fe-mail.dk <fe@fe-mail.dk>; fe-4418@fe-ddis.dk <fe-4418@fe-ddis.dk>
Subject: Høringssvar 2020/001583

Center for Cybersikkerhed har den 7. januar 2021 sendt 4 bekendtgørelser i høring.

Ministeriernes forpligtelse til at høre Rigsrevisionen er fastlagt af rigsrevisorloven, §§ 7 og 10 (Lovbekendtgørelse nr. 101 af 19/01/2012) og angår revisions- og/eller regnskabsforhold, der kan have betydning for Rigsrevisionens opgaver.

Vi har gennemgået bekendtgørelserne og kan konstatere, at de ikke omhandler revisions- eller regnskabsforhold i staten eller andre offentlige virksomheder, der revideres af Rigsrevisionen.

Vi har derfor ikke behandlet henvendelsen yderligere.

Med venlig hilsen

Mette E. Matthiasen
Direktionssekretariatet

Landgreven 4
DK-1301 København K

Tlf. +45 33 92 84 00
Dir. +45 33 92 85 73
mem@rigsrevisionen.dk

www.rigsrevisionen.dk

Fra: Judith <FE-4418@fe-ddis.dk>
Sendt: 7. januar 2021 14:25
Emne: Høring

Til rette vedkommende

Se venligst vedhæftede høring. Høringsmaterialet er lagt på Høringsportalen i dag.

Med venlig hilsen

Center for Cybersikkerhed

Skatteministeriet

Center for Cybersikkerhed
Att.: fe@fe-mail.dk og fe-4418@fe-ddis.dk

25. januar 2021
J.nr. 2020 - 8581

Skatteministeriet
Nicolai Eigtveds Gade 28
DK 1402 – København K

Telefon +45 33 92 33 92
Mail skm@skm.dk

www.skm.dk

Til Center for Cybersikkerhed

Skatteministeriet har modtaget Center for Cybersikkerheds høringsbrev af 7. januar 2021 vedrørende udkast til bekendtgørelser om sikkerhed i net og tjenester (sagsnr.: 2020/001583). Høringen vedrørte følgende:

- Udkast til bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.
- Udkast til bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på området for sikkerhed i net og tjenester.
- Udkast til bekendtgørelse om sikkerhed og beredskab i net og tjenester.
- Udkast til bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester.

Skatteministeriet kan oplyse, at udkastene ikke giver anledning til bemærkninger.

Med venlig hilsen

Kathrine Waage
Fg. kontorchef

From: Mathias Baumann <mathias.baumann@stil.dk>
Sent: 14 januar 2021 21:20 (UTC +01)
To: FE-4418@fe-ddis.dk <FE-4418@fe-ddis.dk>
Subject: SV: Høring over udkast til bekendtgørelser om sikkerhed i net

Kære Judith / Center for Cybersikkerhed

Vi har i Styrelsen for It og Læring modtaget mailen med materiale om høring over udkast til bekendtgørelser om sikkerhed i net og tjenester. Vi har ingen bemærkninger.

Med venlig hilsen
Mathias Baumann
Specialkonsulent

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR IT OG LÆRING

Børne- og Undervisningsministeriet
Styrelsen for It og Læring
Kontor for Digitalisering
Vester Voldgade 123
1552 København V

Direkte tlf.: +45 35 87 82 40
E-mail: mathias.baumann@stil.dk

Fra: Judith <FE-4418@fe-ddis.dk>
Sendt: 7. januar 2021 14:30
Til: UVM - UVMIPOST <uvm@uvm.dk>; 1-DEP Erhvervsministeriets officielle postkasse <em@em.dk>; Finansministeriets postkasse <fm@fm.dk>; Justitsministeriet <jm@jm.dk>; Ligestillings- og Kirkeministeriet <km@km.dk>; Klima-, Energi- og Forsyningsministeriet <kefm@kefm.dk>; Kulturministeriet <kum@kum.dk>; Miljø- og Fødevareministeriets Departement <mfvm@mfvm.dk>; Skatteministeriet <skm@skm.dk>; Social- og Indenrigsministeriet <sim@sim.dk>; Ministeriet for Sundhed og Forebyggelse <sum@sum.dk>; Transportministeriet <trm@trm.dk>; UFM FP DEP - UFM Departement <ufm@ufm.dk>; Udenrigsministeriet <um@um.dk>; UIM Hovedpostkasse <uim@uim.dk>; Statsministeriet <stm@stm.dk>; BM Postkasse <BM@bm.dk>
Emne: Høring

Til rette vedkommende

Se venligst vedhæftede høring. Høringsmaterialet er lagt på Høringsportalen i dag.

Med venlig hilsen

Center for Cybersikkerhed

From: Ida Helene Høiberg <ihh@ufm.dk>
Sent: 12 januar 2021 10:46 (UTC +01)
To: fe-mail <fe@fe-mail.dk>; fe-4418@fe-ddis.dk <fe-4418@fe-ddis.dk>
Subject: Sv: Høringssvar: 2020/001583 (UFM Id nr.: 200523)

Til: fe-mail (fe@fe-mail.dk), fe-4418@fe-ddis.dk (fe-4418@fe-ddis.dk)
Fra: Ida Helene Høiberg (ihh@ufm.dk)
Titel: Høringssvar: 2020/001583
Sendt: 12-01-2021 10:41

Til Center for Cybersikkerhed

Uddannelses- og Forskningsministeriet har ingen bemærkninger til denne høring.

For

Thomas Voigt Lund
Jura
Uddannelses- og Forskningsministeriet

Venlig hilsen

Ida Helene Høiberg
Student, Jura
Uddannelses- og Forskningsministeriet

Fra: Judith
Sendt: 7. januar 2021 14:30
Til: UVM - UVMIPOST ; 1-DEP Erhvervsministeriets officielle postkasse ; Finansministeriets postkasse ; Justitsministeriet ; Ligestillings- og Kirkeministeriet ; Klima-, Energi- og Forsyningsministeriet ; Kulturministeriet ; Miljø- og Fødevareministeriets Departement ; Skatteministeriet ; Social- og Indenrigsministeriet ; Ministeriet for Sundhed og Forebyggelse ; Transportministeriet ; UFM FP DEP - UFM Departement ; Udenrigsministeriet ; UIM Hovedpostkasse ; Statsministeriet ; BM Postkasse
Emne: Høring

Til rette vedkommende

Se venligst vedhæftede høring. Høringsmaterialet er lagt på Høringsportalen i dag.

Med venlig hilsen

Center for Cybersikkerhed

Københavns Byret

Forsvarets Efterretningstjenesten
Kastellet 30
2100 København Ø

Præsidenten
Domhuset, Nytorv 25
1450 København K.
Tlf. 99 68 70 15
CVR 21 65 95 09
administration.kbh@domstol.dk
J.nr. 9099.2021.1

Den 8. januar 2021

Ved en mail af 7. januar 2021 har Forsvarets Efterretningstjenesten anmodet om eventuelle bemærkninger til høring over udkast til bekendtgørelser om sikkerhed i net og tjenester.

Jeg skal i den anledning på vegne af byretspræsidenterne oplyse, at byretterne ikke ønsker at udtale sig om udkastet.

Der henvises til J.nr. 2020-001583.

Med venlig hilsen

Søren Axelsen

Østre Landsret
Præsidenten

FE Center for Cybersikkerhed

Kastellet 30
2100 København Ø

12. januar 2021

J.nr.: 21/00406-2
Sagsbehandler: CRJ

FE Center for Cybersikkerhed har ved brev af 7. januar 2021 (Sagsnr. 2020/001583) anmodet om eventuelle bemærkninger til høring over udkast til bekendtgørelser om sikkerhed i net og tjenester.

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

Med venlig hilsen

Carsten Kristian Vollmer

Ellen Busck Forsbo

From: Marianne Abildtrup <mab@advokatsamfundet.dk>
Sent: 11 januar 2021 15:28 (UTC +01)
To: Judith <FE-4418@fe-ddis.dk>; fe@fe-mail.dk <fe@fe-mail.dk>
Subject: Sv: Høring (Sagsnr.: 2021 - 3)
Attachments: Høringsliste.pdf, Udkast til bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv..pdf, Udkast til bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester.pdf, Udkast til bekendtgørelse om sikkerhed og beredskab i net og tjenester.pdf, Udkast til bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på området for sikkerhed i net og tjenester.pdf, Høringsbrev.pdf

Sagsnr.: 2020/001583.

Tak for henvendelsen.

Advokatrådet har besluttet ikke at afgive høringssvar.

Med venlig hilsen

Marianne Abildtrup
Direktionssekretær
D +45 33 96 97 79

mab@advokatsamfundet.dk - www.advokatsamfundet.dk

ADVOKATSAMFUNDET
RETSSIKKERHED · UAFHÆNGIGHED · INTEGRITET

Advokatsamfundet, Kronprinsessegade 28, 1306 København K

Til:
Fra: Judith (FE-4418@fe-ddis.dk)
Titel: Høring
Sendt: 07-01-2021 14:24

Til rette vedkommende

Se venligst vedhæftede høring. Høringsmaterialet er lagt på Høringsportalen i dag.

Med venlig hilsen

Center for Cybersikkerhed

Vestre Landsret
Præsidenten

11. januar 2021

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Sendt pr. mail til fe@fe-mail.dk og fe-4418@feddis.dk

J.nr.: 21/00534-2
Sagsbehandler: Lars B Olesen

Forsvarets Efterretningstjeneste, Center for Cybersikkerhed, har ved brev af 7. januar 2021 (sagsnr. 2020/001583) anmodet om eventuelle bemærkninger til høring over udkast til bekendtgørelse om sikkerhed i net og tjenester.

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

Med venlig hilsen

Helle Bertung

TELE INDUSTRIEN
teleselskabernes branchesamarbejde

Center for Cybersikkerhed

Sendt pr. e-mail til
fe@fe-mail.dk
fe-4418@feddis.

Sagsnr.: 2020/001583.

4. februar 2021

Høring over udkast til bekendtgørelser om sikkerhed i net og tjenester

Teleindustrien (TI) har noteret sig, at Center for Cybersikkerhed den 7. januar 2021 har sendt udkast til 4 reviderede bekendtgørelser om sikkerhed i net og tjenester i høring med frist den 4. februar 2021, kl. 12.

En velfungerende og sikker teleinfrastruktur er afgørende for det danske samfund, teleselskabernes kunder og naturligvis også branchen selv. Med det afsæt har branchen over de seneste 10 år investeret 70 mia. kr. i at udbygge den digitale infrastruktur i Danmark med fokus på både kapacitet og sikkerhed. Udbygningen er sket i tæt dialog med danske myndigheder, herunder særligt Center for Cybersikkerhed.

TI har forståelse for, at bekendtgørelserne opdateres som følge af de ændringer, der er gennemført ved lov nr. 1831 af 8. december 2020 om ændring af lov om net- og informationssikkerhed, med henblik på implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation (Koden) herunder, at anvendelsesområdet udstrækkes til at omfatte udbydere af nummeruafhængig interpersonelle kommunikationstjenester (NUIK-tjenester).

TI har dog også noteret sig, at nogle af bekendtgørelserne indeholder yderligere skærpende ændringer, end der er nødvendige i forhold at sikre en EU-konform implementering af Koden. CFCS har ikke begrundet, hvorfor disse ændringer er nødvendige, og TI finder ikke, at der er tilstrækkeligt grundlag for at foretage sådanne skærpelser over for teleselskaberne. TI skal i den forbindelse henvise til, at Forsvarsministeren den 12. november 2020 i en besvarelse til Folketingets Forsvarsudvalg udtalte følgende:

> *"I forhold til de traditionelle teleudbydere vil lovforslaget som udgangspunkt kun indebære, at der foretages mindre justeringer af de eksisterende rammer i lov om net- og informations-*

sikkerhed. Lov om net- og informationssikkerhed er en rammelov, som i dag er udmøntet i fire bekendtgørelser.

Lovforslaget ændrer ikke ved lovens grundlæggende struktur. Strukturen, hvor den detaljerede regulering sker i bekendtgørelser, er valgt for at give mulighed for, at reglerne løbende kan tilpasses den hastige udvikling i teknologi, best practices og trusselsbilledet. Samtidig giver strukturen den bedste mulighed for at tage højde for anbefalinger fra EU's Agentur for Cybersikkerhed (ENISA), der bl.a. har til opgave at fremme medlemsstaternes samordning på området."

TI skal derfor anmode CFCS om nærmere at redegøre for, hvorfor de skærpede regler anses for at være nødvendige, henset til ministerens udtalelse.

På den baggrund har TI i det følgende kommenteret på ændringerne i bekendtgørelserne.

Generelt skal TI opfordre CFCS til at udarbejde **vejledninger** til de enkelte bekendtgørelser, så det bliver lettere for udbyderne at efterleve reglerne, herunder få en bedre forståelse af CFCS' praksis og fortolkning af de enkelte regler. Fx vil det være nyttigt at få en nærmere forståelse af, hvilke typer af tjenester der omfattes af definitionen "NUIK-tjenester".

Ud over ovennævnte bemærkninger har TI ikke yderligere bemærkninger til **bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv**.

Til **bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet for sikkerhed i net og tjenester** har TI følgende bemærkninger:

TI foreslår, at det tydeliggøres, hvilke medarbejdere som skal sikkerhedsgodkendes, om godkendelsen skal ske til PET-HEM eller FE-HEM, samt hvilket udstyr der er omfattet af følgende "adgang til udstyr eller systemer, som benyttes i forbindelse med indgreb i meddelelseshemmeligheden". Efter TI's opfattelse bør de pågældende systemer afgrænses til de særlige systemer, hvor det kan identificeres, at der foretages et konkret indgreb.

Til **bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og Informationssikkerhed i net og tjenester** har TI følgende bemærkninger:

§1: Definition af, hvad der er "Kritiske netkomponenter", er ikke ændret. TI har dog tidligere i forbindelse med vedtagelsen af første udgave af bekendtgørelsen og i forbindelse med høringen over lovforslag til lov om leverandørsikkerhed peget på, at definitionen i prak-

sis er meget bred og også rammer systemer og komponenter, der ud fra en sikkerhedsfaglig vurdering ikke er kritiske.

De anvendte begreber som fx ”operations support systemer” og ”business support systemer” udgør ikke nogen entydig branchemæssig forståelse, hvorved stort set alle IT-systemer, der anvendes i en teleudbyders forretning, herunder tjenesteudbydere, der ikke har eget netværk, men anvender egne support-systemer, bliver omfattet. Det er også uklart, hvad der forstås ved ”centrale routere og servere i backbonenettet”. Der er ingen afgrænsning af, hvad der er ”centrale” og ”ikke-centrale” routere. Udbyderne er således overladt til Center for Cybersikkerheds uforudsigelige vurdering af, om et netværkselement er omfattet.

Det er tilsvarende uklart, hvad der menes med ”hardware […], der anvendes i core-net”. Det er uklart, om det også betyder, at fx passive dele som fiberkablerne i et core-net omfattes, selvom et fiberkabel vanskeligt kan indeholde aflytningsudstyr eller kan kompromitteres af leverandøren.

TI skal opfodre til, at definitionen tilrettes, så de dele af udbydernes infrastruktur, der omfattes, afgrænses til kun at gælde det absolut mest nødvendige og fremstår entydig for den enkelte udbyder. Det kunne fx ske ved, at ”Kritiske netkomponenter” defineres ud fra den sikkerhedsmæssige vurdering, udbyderen har foretaget af sit netværk, eller som CFCS ved en gennemgang af udbyderens netværk har identificeret som kritiske. Dermed undgår udbyderne fx at skulle anmelde aftaler og forhandlinger om systemkomponenter, som i praksis ikke udgør en sikkerhedsmæssig risiko.

§3 og §5: Udbyderens pligt til at underrette CFCS om aftaleforhandlinger og CFCS’s mulighed for at udstede påbud om, at en endelig aftale skal indsendes til CFCS, er ikke nye. Der er dog ikke efter de gældende bestemmelser fastsat nogen frist for, hvornår Center for Cybersikkerhed skal give et påbud om at få det færdigt udkast til aftale indsendt. Erfaringerne har vist, at teleudbyderne har oplevet, at centeret ikke har reageret eller forholdt sig passiv i lang tid. Udbyderne kan dermed have indrette sine forhandlinger på, at aftalen kan indgås uden anmærkninger fra Center for Cybersikkerhed. Med de kommende regler om leverandørsikkerhed skærpes behovet for, at udbyderne hurtigt får klarhed, om der udstedes et påbud. TI skal derfor foreslå, at der i § 5 indsættes en frist således, at Center for Cybersikkerhed senest 20 arbejdsdage efter, underretning er foretaget, skal afgøre, om der er behov for at udstede et påbud om at indsende det endelige udkast til aftale til CFCS.

Der henvises i øvrigt herom til TI’s høringssvar af 4. januar 2021 vedrørende lov om leverandørsikkerhed.[1]

[1] http://www.teleindu.dk/wp-content/uploads/2021/01/4-januar-2021-h%C3%B8ringssvar-vedr-leverand%C3%B8rsikkerhed.pdf

§ 7, stk. 2 og § 9: Ud over grænseværdien for, hvornår en hændelse skal indberettes efter § 7, stk. 2, er lavere, jf. § 9, end ved hændelser efter § 7, stk. 1, jf. § 8, så er det uklart, hvilke hændelser der er omfattet af § 7, stk. 2. TI skal derfor anmode CFCS om nærmere at redegøre for begrundelsen for den skærpede indberetningspligt efter § 7, stk. 2, herunder hvad der forstås ved "en begivenhed, der faktisk har haft væsentlig negativ indvirkning på net og tjenesters evne til at modstå handlinger, der er til skade for fortroligheden, integriteten eller autenticiteten…"

Der ønskes i øvrigt en særlig præcisering af, hvad der i bestemmelsen forstås ved "handlinger der er til skade for.. autenticiteten".

Der ønskes endelig en nærmere begrundelse for, hvorfor grænseværdien for indberetning efter 7, skt. 2, er sat til 1000 slutbrugere, jf. § 9, hvilket TI anser for at være en væsentlig skærpelse i forhold til den gældende indberetningspligt.

§7, stk 3: Fristen for underretning af sikkerhedshændelser er efter de gældende regler 14 dage (jf. den gældende § 10). Med den ændrede tekst i § 7, stk. 3, ændres underretningspligten til "uden unødigt ophold". Dette er en alvorlig skærpelse. Man vil ofte skulle undersøge en hændelse grundig, inden man i praksis vil kunne underrette om, hvad der rent faktisk er sket, hvor mange slutbrugere der er berørt og lign. Ændringen vil potentielt medføre indberetning af hændelser, før de er analyseret. Det vil potentielt betyde indberetning af hændelser, som ved nærmere analyse ikke er væsentlige eller løbende vil ændre sig efterhånden, som fejlundersøgelse pågår.

TI finder denne skærpelse ubegrundet og finder, at det vil være rimeligt med en frist på ikke mindre end 72 timer efter, udbyderen bliver bekendt med, at sikkerhedshændelsen har haft væsentlig indvirkning på driften.

En frist på mindst 72 timer vil sikre;

- at udbyderen kan holde fokus på kritisk udbedring og mitigering af den samfundsmæssige risiko
- en mere præcis og korrekt indrapportering til de offentlige myndigheder
- adgang til de nødvendige kompetencer og bemyndigede personer, hvis sikkerhedshændelsen sker uden for normal arbejdstid, f.eks. i weekenden eller påsken
- at indberetningspligten vil svare til den, der også gælder efter GDPR ved brud på persondatasikkerheden. Det vil således være ske en ensrettet håndtering ved indberetning af sikkerhedshændelser.

§8: De gældende grænseværdier for vurdering af, hvornår en hændelse anses for at have væsentlig indvirkning på driften af net og tjenester, er i det væsentlige opretholdt, dog er der indført en ny kate-

gori for NUIK-tjenester, og der er i § 8, stk. 4, indføjede nye kategorier.

TI ønsker en afklaring af, hvorfor der er forskel i grænseværdierne, herunder hvilke overvejelser har CFCS gjort i forbindelse med fastlæggelsen af grænseværdierne. TI finder det uklart, hvordan værdierne er opgjort og henstiller derfor til, at der foretages en ensretning af grænseværdierne. Dette vil skabe transparens, og TI kan ikke se, hvorfor der skal være forskel på mobilabonnementer og NUIK-tjenester. TI ønsker en ensretning af f.eks. de 35.000 brugertimer for mobilabonnementer og 50.000 brugertimer for NUIK-tjenester – dette bør ensrettes til 50.000 brugertimer.

Det er uklart, hvad kategorien ”øvrige tjenester” dækker over, og som ikke allerede er dækket af de andre nævnte tjenester, herunder hvorfor grænsen for ”øvrige tjenester” er sat væsentlig lavere end de andre anførte tjenester, som må anses at være de væsentligste tjenester på telemarkedet.

TI savner en nærmere begrundelse for indførsel af de nye kategorier, som er anført i stk. 4. Udbyderne har ikke systemer til at identificere præcist

- om mere end 200 slutbrugere indenfor forsvar, politi eller beredskab er berørt. Udbyderne har ikke nødvendigvis viden om, hvor slutbrugerne er ansat, eller hvilket formål kommunikationstjenesten anvendes til.
- hvilke tjenester beredskabsmyndighederne vælger at anvende til beredskabssituationer, eller hvad der i øvrigt forstås ved ”ekstraordinære situationer”.
- hvilke dele af udbyderens kapacitet, der dækker ikke-brofaste øer.

TI skal anbefale, at der indledes en dialog med branchen, inden der fastsættes nye kategorier, således at der findes kan underrettes på forhold, som udbyderne er i stand til at monitorere.

§13: Der indføres en ny skærpende informationspligt, hvorefter udbydere skal informere deres potentielt berørte brugere om mulige beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som brugerne kan træffe, når udbyderne bliver bekendt med en særlig og betydelig trussel om en sikkerhedshændelse i deres net eller tjenester.

Den foreslåede bestemmelse pålægger udbyderne et stort ansvar samt en ressourcemæssig byrde.

Der er tale om en helt ny og detaljeret forpligtelse, som det ikke indenfor høringsfristen er muligt fuldt ud at afklare virkninger af, herunder om det er muligt i praksis at efterleve forpligtelsen.

TI mener derfor, at § 13 skal udgå og indtænkes i sektorens cyberstrategi som generel awareness overfor brugerne.

Bestemmelsen indeholder en række uklarheder i forhold til fx, hvordan og hvad der konkret skal informeres om. I værste fald kan udbyderne blive forpligtet til at "overinformere", hvorved kundernes opmærksomhed på de alvorlige trusler helt udebliver.

Det er i øvrigt uklart, om det er udbyderen af et net eller udbyderen af en tjeneste, der har forpligtelsen til at informere. Denne afklaring er særlig relevant, når netejer og tjenesteudbyder ikke er samme selskab.

TI finder betegnelsen 'potentielt berørte brugere' for vidtgående. 'Potentielt berørte brugere' indebærer, at der ikke længere er noget råderum for udbyderne til at vurdere, hvorvidt det er nødvendigt at involvere og underrette kunderne. Der er således ikke mulighed for at vurdere underretningen af de potentielle berørte brugere ift. den risiko, der reelt har eksisteret. TI skal derfor anbefale, at betegnelsen kvalificeres til alene at omfatte 'berørte brugere'.

TI forstår i øvrigt, at hændelserne som udgangspunkt kan kommunikeres til brugerne via generel driftsinformation, f.eks. på udbyderens hjemmeside.

I forhold til de i bestemmelsen anførte trusler (§ 13, stk. 1, nr. 1-7) har TI følgende bemærkninger:

Nr.1 og 2: Det er ikke sikkert, at udbyderne præcist har alle oplysninger om, hvem der fx benytter en DNS-løsning. Det samme gælder i forbindelse med BGP hijack, hvor alle slutbrugere anvender det pågældende IP-net. Sådanne trusler egner sig således bedst til information via fx udbyderes hjemmeside.

Nr. 2: Visse udbydere har det, man kalder rekursive DNS servere, hvor kompromittering kan kun identificeres to måder. Enten ved at en bruger henvender sig, eller ved at miljøet er ustabilt. Udbyderne foretager typisk ikke selv opdateringer, idet disse arves fra overliggende nationale servere – fx når www.dr.dk skifter IP-adresse, så kommer informationen automatisk til udbyderne fra de overliggende nationale servere. Informationspligten bør således ikke ligge på udbyderne, men på udbyderne af de nationale servere.

Nr. 3: Kompromittering af en brugers konto kan ofte være, at brugeren selv der har givet kontooplysninger videre på uheldig vis, dvs. noget, som udbyderne ikke er herre over. Sådanne situationer bør udbyderne ikke være forpligtet til at informere den enkelte slutbruger om.

Nr. 6: Efter TI's opfattelse er beskrivelsen af "ondsindet SS7-trafik" ikke realistisk, da der i praksis ses meget 'signalerings støj' fra fejlkonfigureret netværkselementer i fremmed netværk, og desuden ses der løbende sårbarhedsscanninger (pen-tests) fra mange forskellige

udenlandske aktører, som jævnligt scanner (pen-tester) med byger af forskellig SS7 angrebsmønstrer rettet mod tilfældige SIM/IMSI mhp. profilering af nettes sårbarhedsprofil og som forberedelse til evt. kommende spydspidsangreb.

I denne henseende kan støjen på SS7 nettet ses som analog til støjen på Internet, hvor der også er et konstant støjloft og vedvarende scanninger. Forskellen med SS7 støjen er, at der indgår et IMSI (en kunde) ifm. de alle støjende SS7 beskeder.

En stor andel af denne type støj vil subjektivt kunne tolkes eller fejltolkes som ondsindet forsøg på positionsindhentning, idet der i forskellige angrebsmønstre er SS7 MAP kommandoer, der kan relateres til position.

TI skal derfor anbefale, at nr. 6 præcises og ændres til:

> *"Identificeret vellykket ondsindet SS7-angreb målrettet en eller flere kunder, hvor det er lykkes at kompromittere kunden, og hvor det skønnes at have almenhedens interesse. Dette kan f.eks. være opsnapning af SMS/2-faktor autentifikationskoder, indhentning af positionsoplysninger eller omdirigering af talesamtaler."*

Til **Bekendtgørelse om sikkerhed og beredskab i net og tjenester** har TI følgende bemærkninger:

§ 2: TI skal anmode om, at begreberne defineres, herunder begrebet "autenticitet".

§3, §5 og § 6: I de gældende bestemmelser stod der, at udbyderne skulle styre informationssikkerheden, udarbejde en informationssikkerhedspolitik og foretage risikostyring "med udgangspunkt i en international standard", fx ISO27001. Med den foreslåede ændring fremgår det nu, at disse skal udarbejdes "efter en international standard". Det er uklart, om der med den pågældende ændring er tiltænkt en indholdsmæssig ændring.

Hvis det betyder, at man skal følge en bestemt international standard slavisk, vil det ikke medføre nogen sikkerhedsmæssig styrkelse af infrastrukturerne. For de fleste operatører er der en klar værdi i at selektere og inddrage brugbare vejledninger, modeller o.l. fra andre anerkendte standarder end ISO/IEC 27001; f.eks. NIST's Cybersecurity Framework og ISF's "Standard of Good Practice".

Der fremgår i øvrigt af lovbemærkningerne til § 3 i lov om sikkerhed i net og tjenester[2], at:

> *"Der kan således administrativt stilles krav om, at processerne skal fastlægges og gennemføres med udgangspunkt i en rele-*

[2] https://www.retsinformation.dk/eli/ft/201512L00010

vant og anerkendt international standard eller tilsvarende." (TI's understregning)

For at undgå fortolkningstvivl, skal TI opfodre til, at bestemmelserne ikke ændres, og at der fastholdes en tekstnær formulering svarende til rammerne i hjemmelsbestemmelsen.

§§11-15: TI finder det ubegrundet, at der er forskel på, hvordan NU-IK-tjenester og elektroniske kommunikationstjenester skal håndteres.

§ 26 og 27: Med de foreslåede bestemmelser gives CFCS som noget nyt mulighed for at påbyde udbyderne at foretage en risikovurdering under særlige ikke-afgrænsede omstændigheder.

TI mener, at bestemmelsen er for vidtgående og giver CFCS bred bemyndigelse til at indføre indgribende foranstaltninger på udbyderne. Bestemmelsen synes ikke at tage højde for, at der er nødt til at være proportionalitet i de iværksatte foranstaltninger, som kan pålægges i forhold til truslen. Myndighederne kan reelt pålægge ret omfattende foranstaltninger uden at tage højde for omkostningerne forbundet hermed, og der synes at mangle en form for afvejning af truslen og de pågældende foranstaltninger.

CFCS kan benytte bemyndigelsen, når der foreligger en "betydelig trussel", men det er ikke defineret nærmere og er et meget løst begreb. Der savnes også en sondring af, hvordan begreberne "betydelig trussel" i §§ 26 og 27 og "væsentlig samfundsmæssig betydning" i § 28 skal forstås. I den forbindelse skal TI anmode om, at der nærmere redegøres for, hvorfor foranstaltningerne efter § 28 ikke anses for at være tilstrækkelige.

TI finder det også uklart, hvordan processen vil være, hvis CFCS udsteder et påbud, herunder hvilken information CFCS er forpligtet til at forsyne udbyderen med, herunder om udbyderne skal udlevere risikovurderingen til CFCS, og hvordan skal der følges op på disse risikovurderinger.

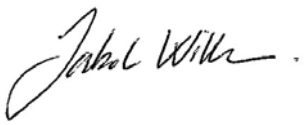
De udvidede beføjelser kan medføre krav om yderligere foranstaltninger, hvilket vil medføre omkostninger for udbyderne. Særligt nedenstående bestemmelsens (§ 27, nr. 3-5) sætter store krav til udbyderne, hvis de umiddelbart skal kunne implementeres:

> *3) Sikring af sporbarhed eller logning af fysisk eller logisk adgang til nærmere angivne og særligt kritiske netkomponenter, systemer og værktøjer, herunder krav om analyse af logfiler.*
>
> *4) Iværksættelse af kryptering efter internationale anerkendte standarder eller best practice på kritiske netkomponenter, systemer og værktøjer.*
>
> *5) Sikring af, at leverancer af hardware, firmware eller software, der kan udgøre en sårbarhed i den pågældende udbyders net og tjenester, undersøges for sårbarheder.*

Eksempelvis er det udefineret, hvad § 27, nr. 5, indebærer og kan i praksis være meget omfattende. I praksis kan det måske være helt umuligt at gennemføre fx en sourcekode review.

TI skal derfor henstille til, at §§ 26, 27 og 28 ændres, således at ansvaret for at definere, hvilke præcise passende foranstaltninger, der skal implementeres ved en betydelig trussel, ligger hos udbyderne. TI mener udbyderne kender deres virksomhederne bedst og således bedst kan vurdere, hvad der er passende foranstaltninger.

Med venlig hilsen



Jakob Willer
Direktør

HØRINGSSVAR

28-01-2021
EMN-2020-00132
1417272
Maria Möger

Høringssvar til *Høring over udkast til bekendtgørelser om sikkerhed i net og tjenester*

Center for Cybersikkerhed har d. 7. januar 2021 anmodet Danske Regioner om bemærkninger til udkast til bekendtgørelser om sikkerhed i net og tjenester. Danske Regioner fremsender høringssvar på vegne af de fem regioner.

Regionerne mener ikke, at de kan karakteriseres som værende erhvervsmæssig udbyder, som anført i definitionerne i bekendtgørelserne. Det er derfor uklart i hvilket omfang regionerne vil blive omfattet af den nye lovgivning på både kort og langt sigt.

Region Syddanmark bemærker følgende:

Supplerende kan det oplyses, at i og med at Region Syddanmark ikke anses for at være en væsentlig erhvervsmæssig netudbyder, finder Region Syddanmark ikke, at CFCS har mulighed for at opsætte prober til logopsamling på det generelle netværk. Trafikken på nettet er endvidere dedikeret til sundhedsbehandling og diagnosticering, hvilket betyder, at der skal udføres størst mulig fortrolighed for beskyttelse af patienter og borgeres privatliv og sundhedsoplysninger.

Region Nordjylland bemærker følgende:

I Region Nordjylland er adgang til data samt en sikker og stabil drift af den digitale infrastruktur en forudsætning for, at regionen kan leve op til sit mål om at give patienter og borgere en tryg og sikker behandling. Digitale løsninger spiller i dag en stadig større rolle i sundhedssektoren, der som samfundskritisk sektor således er særligt sårbar overfor cyberangreb. Samtidig har regionen ansvaret for mange følsomme oplysninger og sundhedsdata, som patienter og borgere fortsat skal kunne have tillid til, at regionen passer godt på og behandler i overensstemmelse med lovgivningen.
Det er derfor Region Nordjyllands klare målsætning at oppebære et højt niveau for cyber- og informationssikkerhed. Et niveau der naturligvis lever op til den ambitiøse nationale strategi for cyber- og informationssikkerhed. Derfor arbejder Regionen med at gøre den risikobaseret, i erkendelse af at 100% sikkerhed ikke eksisterer. En

risikobaseret tilgang gør nemlig regionen i stand til at sikre såvel sikkerheden som effektiviteten af området, ved rettidigt at kunne dirigere ressourcerne hen til de mest kritiske systemer med henblik på at undgå driftsstop, datalæk, cyberangreb mv. Region Nordjylland hilser enhver tilpasning af lovgivningen velkommen i det omfang det er nødvendigt. Det er Regionens opfattelse at de udbedte høringssvar, ikke mindst udkast til bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester, giver omfattende udvidelse af beføjelser til Center for Cybersikkerhed (CFCS). Da det er Region Nordjyllands opfattelse at regionen som udgangspunkt ikke udbyder NUIK-tjenester eller offentligt tilgængelige elektroniske kommunikationsnet på nuværende tidspunkt, er det dog uklart i hvilket omfang regionen vil blive omfattet af denne nye lovgivning på både kort og lang sigt.

Det er dog udenfor enhver tvivl, at sådanne omfattende krav, ikke mindst som de er beskrevet i udkast til bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed i net og tjenester, vil kunne få betydelige økonomiske implikationer for Regionen, i fald man vælger at udbyde NUIK-tjenester eller offentligt tilgængelige elektroniske kommunikationsnet.

Dertil kommer at de beføjelser CFCS får med blandt andet Bekendtgørelse om sikkerhed og beredskab i net og tjenester, potentielt vil kunne medføre ikke ubetydelige udgifter for regionerne i fald disse udbyder NUIK eller offentligt tilgængelige elektroniske kommunikationsnet. Heraf følger, at Region Nordjylland er skeptisk overfor vurderingen i DUT høringens "sammenfattende skema" over forventede omkostninger. Konsekvensen af ovenstående vil være, at regionen - med baggrund i de eksisterende økonomiaftaler - må kunne forventes at revidere hvilke borgerrettede services, regionen vælger at tilbyde.

Venlig hilsen

Maria Möger, Danske Regioner

From: Mette Sloth Hedegaard (EM-DEP) <meshed@em.dk>
Sent: 4 februar 2021 14:03 (UTC +01)
To: fe-4418@fe-ddis.dk <fe-4418@fe-ddis.dk>; fe-myn@fe-ddis.dk <fe-myn@fe-ddis.dk>
Subject: EMs' høringssvar: Høring sagsnr.: 2020/001583

Erhvervsministeriet har følgende bemærkninger til den fremsendte høring:

Erhvervsstyrelsens Område for Bedre Regulering (OBR) har modtaget bekendtgørelsesudkastene i høring.

OBR's vurdering af udkastenes administrative konsekvenser for erhvervslivet samt bemærkninger til Center for Cybersikkerheds vurdering af principperne for agil erhvervsrettet regulering fremgår individuelt for hvert bekendtgørelsesudkast nedenfor.

Bekendtgørelse nr. 564 af 1. juni 2016 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv. Bekendtgørelsen ændrer ikke titel.

Administrative konsekvenser
OBR har følgende bemærkninger om de administrative konsekvenser for erhvervslivet.

OBR vurderer, at bekendtgørelsesudkastet ikke medfører administrative konsekvenser for erhvervslivet og har dermed ikke yderligere kommentarer.

Principper for agil erhvervsrettet regulering

Center for Cybersikkerhed har i forbindelse med prøhøringen af bekendtgørelsesudkastet vurderet, at principperne for agil erhvervsrettet regulering ikke er relevante for de konkrete ændringer i bekendtgørelsesudkastet. OBR har yderligere ingen bemærkninger hertil.

Bekendtgørelse nr. 565 af 1. juni 2016 om sikkerhedsgodkendelse af medarbejdere på informationssikkerhedsområdet. Bekendtgørelsen ændrer titel til: "Bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på området for sikkerhed i net og tjenester".

Administrative konsekvenser
OBR har følgende bemærkninger om de administrative konsekvenser for erhvervslivet.

OBR vurderer, at bekendtgørelsesudkastet ikke medfører administrative konsekvenser for erhvervslivet og har dermed ikke yderligere kommentarer.

Principper for agil erhvervsrettet regulering

Center for Cybersikkerhed har i forbindelse med prøhøringen af bekendtgørelsesudkastet vurderet, at principperne for agil erhvervsrettet regulering ikke er relevante for de konkrete ændringer i bekendtgørelsesudkastet. OBR har yderligere ingen bemærkninger hertil.

Bekendtgørelse nr. 567 af 1. juni 2016 om informationssikkerhed og beredskab i net og tjenester. Bekendtgørelsen ændrer titel til: "Bekendtgørelse om sikkerhed og beredskab i net og tjenester".

Administrative konsekvenser

OBR har følgende bemærkninger om de administrative konsekvenser for erhvervslivet.

OBR vurderer, at bekendtgørelsesudkastet medfører administrative konsekvenser for erhvervslivet. Disse konsekvenser vurderes at være under 4 mio. kr., hvorfor de ikke kvantificeres nærmere.

Principper for agil erhvervsrettet regulering
OBR har i forbindelse med prøhøringen af bekendtgørelsesudkastet afgivet bemærkninger til Center for Cybersikkerheds vurdering af, at et eller flere af principperne for agil erhvervsrettet regulering er relevante for de konkrete ændringer i bekendtgørelsesudkastet. OBR har ingen yderligere bemærkninger hertil.
Bekendtgørelse nr. 1256 af 27. november 2019 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed. Bekendtgørelsen ændrer titel til: "Bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester".

Administrative konsekvenser
OBR har følgende bemærkninger om de administrative konsekvenser for erhvervslivet.

OBR vurderer, at bekendtgørelsesudkastet medfører administrative konsekvenser for erhvervslivet. Disse konsekvenser vurderes at være under 4 mio. kr., hvorfor de ikke kvantificeres nærmere.

Principper for agil erhvervsrettet regulering
OBR har i forbindelse med prøhøringen af bekendtgørelsesudkastet afgivet bemærkninger til Center for Cybersikkerheds vurdering af, at et eller flere af principperne for agil erhvervsrettet regulering er relevante for de konkrete ændringer i bekendtgørelsesudkastet. OBR har ingen yderligere bemærkninger hertil.

Kontaktperson vedrørende ovenstående bemærkninger:

Lotte Dalgaard
Specialkonsulent
Tlf. direkte 3529 1660
E-post LotDal@erst.dk

ERHVERVSMINISTERIET

METTE SLOTH HEDEGAARD (EM-DEP)
Direktionssekretær

Slotsholmsgade 10-12
1216 København K
meshed@em.dk
Tlf. 33 92 33 50
Mobil 91 33 70 46
EAN 5798000026001

Erhvervsministeriet er ansvarlig for behandlingen af de personoplysninger, vi modtager om dig. Du kan læse mere om, hvordan vi behandler dine personoplysninger på vores hjemmeside https://em.dk/privatlivspolit k.

Erhvervsministeriet gør opmærksom på, at denne e-mail og eventuelle vedhæftede filer er fortrolige. Hvis du ikke er den tilsigtede modtager, bedes du straks underrette afsenderen ved at besvare denne e-mail og derefter slette e-mailen. Hvis du har modtaget denne e-mail ved en fejl, skal vi gøre klart, at enhver form for kopiering, offentliggørelse eller distribution af denne e-mail kan være ulovlig.

From: Daniel Mathias Bager <damab@kefm.dk>
Sent: 4 februar 2021 11:56 (UTC +01)
To: fe@fe-mail.dk <fe@fe-mail.dk>; fe-4418@fe-ddis.dk <fe-4418@fe-ddis.dk>
Subject: Sv: Høring (KEMIN Id nr.: 1156091)

Vedr. sagsnr. 2020/001583

Til rette vedkommende i Center for Cybersikkerhed,

På vegne af Klima-, Energi- og Forsyningsministeriet kan jeg oplyse om, at ministeriet ikke har nogle bemærkninger til de 4 høringer.

Vi har i departementet hørt underliggende styrelser, der ikke havde nogle bemærkninger heller. Dog har Energistyrelsen (ENS) ikke meldt tilbage inden for tidsfristen, hvorfor nærværende høringssvar skal tages med forbehold for, at ENS muligvis sender et individuelt høringssvar afsted til jer.

Med venlig hilsen

Daniel Mathias Bager
Studentermedhjælper
Team Jura
+ 45 2934 9008
damab@kefm.dk

Klima-, Energi- og Forsyningministeriet
Holmens Kanal 20
DK-1060 København K.
www.kefm.dk

Til: Hovedpostkassen (kefm@kefm.dk), Beskæftigelsesministeriet (bm@bm.dk), Finansministeriet (fm@fm.dk), Justitsministeriet (jm@jm.dk), Kirkeministeriet (km@km.dk), Skatteministeriet (skm@skm.dk), Statsministeriet (stm@stm.dk), Transportministeriet (trm@trm.dk), Udenrigsministeriet (um@um.dk), Undervisningsministeriet (uvm@uvm.dk), Kulturministeriet (kum@kum.dk), D-DEP - enhedspostkasse (ufm@ufm.dk), Miljø- og Fødevareministeriets Departement (mfvm@mfvm.dk), sim@sim.dk (sim@sim.dk), UIM Hovedpostkasse (uim@uim.dk), em@em.dk (em@em.dk), DEP Ministeriet for Sundhed og Forebyggelse (sum@sum.dk)
Fra: Judith (FE-4418@fe-ddis.dk)
Titel: Høring
Sendt: 07-01-2021 14:30

Til rette vedkommende

Se venligst vedhæftede høring. Høringsmaterialet er lagt på Høringsportalen i dag.

Med venlig hilsen

Center for Cybersikkerhed

RIGSPOLITIET

POLITI

Center for Cybersikkerhed

Sendt pr. e-mail til fe@fe-mail.dk og fe-4418@fe-ddis.dk

Dato: 04-02-2021
J. nr.: 2021-060038
Dok.nr.: 1232278

Center for Databeskyttelse

–
Rigspolitiet
Polititorvet 14
1780 København V

Tlf.: 33 14 88 88
Email: politi@politi.dk

Høringssvar til udkast til bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på området for sikkerhed i net og tjenester

1. Center for Cybersikkerhed har ved brev af 7. januar 2021 sendt bl.a. udkast til bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på området for sikkerhed i net og tjenester i høring.

Bekendtgørelsen vil erstatte bekendtgørelse nr. 565 af 1. juni 2016 om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet.

2. Det følger af § 1, stk. 2 i både den gældende bekendtgørelse og udkastet til den kommende, at bestemmelsen i stk. 1 ikke omfatter medarbejdere eller repræsentanter for udbyderne, der forestår kontakten til politiet i forbindelse med indgreb i meddelelseshemmeligheden og dermed er omfattet af bekendtgørelse nr. 1144 af 20. november 2006 om telenet- og teletjenesteudbyderes praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden (sikkerhedsgodkendelse af personale i telebranchen).

Det bemærkes i den forbindelse, at Rigspolitiets Center for Databeskyttelse i efteråret 2019 gennemførte et tilsyn med en række teleudbyderes efterlevelse af reglerne i bekendtgørelse nr. 1144 af 20. november 2006.

Center for Databeskyttelse kunne herved konstatere, at der kunne være behov for en mere tydelig afgrænsning mellem bekendtgørelse nr. 1144 af 20. november 2006 og bekendtgørelse nr. 565 af 1. juni 2016.

3. For at adressere dette behov skal Center for Databeskyttelse derfor foreslå, at der i den kommende bekendtgørelse på området for sikkerhed i net og tjenester foretages ændringer i bekendtgørelsens § 1, stk. 2, således at der i denne del af bestemmelsen angives en klassifikationsgrad svarende til § 1, stk. 1.

Dette ændringsforslag er begrundet i, at bekendtgørelse nr. 1144 af 20. november 2006 alene foreskriver, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal sikre, at medarbejdere eller repræsentanter for udbyderen,

der forestår kontakten til politiet i forbindelse med indgreb i meddelelseshemmeligheden, sikkerhedsgodkendes af Rigspolitiet til at håndtere klassificerede oplysninger, uden angivelse af en specifik klassifikationsgrad.

En medarbejder, der forestår kontakten til politiet, vil derfor i princippet kunne klassificeres til en lavere grad end HEMMELIGT, og samtidig opfylde kravene i bekendtgørelse nr. 1144 af 20. november 2006, desuagtet at samme medarbejder – udover at forestå kontakten - tillige måtte have adgang til udstyr eller systemer, som benyttes i forbindelse med indgreb i meddelelseshemmeligheden.

Sendt til fe@fe-mail.dk og fe-4418@feddis.dk

Vedr. sagsnr. 2020/001583

Dok. ansvarlig: MOB
Sekretær: EDR
Sagsnr: s2021-105
Doknr: d2021-1940-5.0
4. februar 2021

Høring over udkast til bekendtgørelser om sikkerhed i net og tjenester

Center for Cybersikkerhed har den 7. januar 2021 sendt udkast til fire bekendtgørelser med hjemmel i lov nr. 1831 af 8. december 2020 om ændring af lov om net- og informationssikkerhed i høring.

Dansk Energi noterer sig med tilfredshed, at udbydere af NUIK-tjenester, i overensstemmelse med lov om ændring af lov om net- og informationssikkerhed og med forventet virkning fra 15. februar 2021, vil blive sidestillet med udbydere af offentligt tilgængelige elektroniske kommunikationsnet og tjenester på de områder, som de nye bekendtgørelser regulerer vedrørende oplysnings- og underretningspligter samt sikkerhed og beredskab i net og tjenester. Dansk Energi har på nuværende tidspunkt ikke yderligere bemærkninger til bekendtgørelserne.

Med venlig hilsen
Dansk Energi

Morten Baadsgaard Trolle

DANSK ENERGI
Vodroffsvej 59 | DK-1900 Frederiksberg C | T: +45 35 300 400 | info@danskenergi.dk | www.danskenergi.dk