

Til adressaterne på vedlagte høringsliste

Kastellet 30
2100 København Ø
Telefon: 33 32 55 80
cfcs@cfcs.dk
www.cfcs.dk

29. april 2016

Høring over bekendtgørelser om net- og informationssikkerhed

1. Center for Cybersikkerhed sender hermed udkast til fire bekendtgørelser om net- og informationssikkerhed i høring.

Centeret skal anmode om at modtage eventuelle bemærkninger senest **den 18. maj 2016 kl. 12.** Bemærkningerne bedes sendt til jura@cfcs.dk med kopi til stibus@cfcs.dk. Eventuelle spørgsmål til bekendtgørelserne kan sendes til samme e-mail-adresser.

2. De fire bekendtgørelser udstedes med hjemmel i lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed (NIS-loven), der træder i kraft den 1. juli 2016. Der er tale om følgende bekendtgørelser:

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

Bekendtgørelserne vil – for så vidt angår krav til informationssikkerhed og beredskab på teleområdet – erstatte bekendtgørelse nr. 396 af 21. april 2011 om rammerne for informationssikkerhed og beredskab, bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester, bekendtgørelse nr. 597 af 18. juni 2009 om faste kredsløb til beredskabsmæssige formål og bekendtgørelse nr. 598 af 18. juni 2009 om sikring af

offentlige telenet og teletjenester, der alle er udstedt med hjemmel i lov om elektroniske kommunikationsnet og -tjenester (teleloven), jf. lovbekendtgørelse nr. 128 af 7. februar 2014.

3. NIS-loven var et initiativ i den nationale strategi for cyber- og informationssikkerhed, og loven har til formål at styrke informationssikkerheden i telesektoren og dermed beskytte danske borgere, virksomheders og myndigheders oplysninger. Med loven blev den eksisterende regulering af informationssikkerhed og beredskab på teleområdet overført fra teleloven til en selvstændig lov.

Samtidig skete der en skærpelse af kravene til teleudbydernes informationssikkerhed, således at kravene i højere grad tager højde for samfundets afhængighed af telenettet og afspejler det aktuelle trusselsbillede, hvor især cyberangreb og avanceret industrispionage er stærkt stigende.

Bekendtgørelserne udmønter en række hjemmelsbestemmelser i NIS-loven.

4. Med bekendtgørelserne sker der en videreførelse af den eksisterende implementering af dele af Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet) og Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet).

Ved videreførelsen af implementeringen af dele af de to direktiver er der sket en præcisering og sproglig tilpasning af den eksisterende regulering på områder, der har givet anledning til fortolkningstvivl. Der er imidlertid ikke med disse tilpasninger tilsigtet en skærpelse af reguleringen.

Sideløbende med, at implementeringen af direktiverne videreføres, udmønter bekendtgørelserne også en række hjemmelsbestemmelser i NIS-loven, som ud fra et hensyn til den nationale sikkerhed skærper kravene til informationssikkerheden. Disse skærper har således ikke sammenhæng med implementeringen af direktiverne.

5. Der har ved udarbejdelsen af bekendtgørelserne været fokus på at sikre en hensigtsmæssig balance mellem på den ene side de økonomiske og administrative byrder, som reguleringen kan medføre for telebranchen, og på den anden side hensynet til informationssikkerheden. Bekendtgørelserne er således udarbejdet under inddragelse af telebranchen og Erhvervsstyrelsen. I forbindelse med dialogen med telebranchen har det været muligt at imødekomme en række af branchens ønsker til tilpasning af bekendtgørelserne.

Center for Cybersikkerhed har i overensstemmelse med Erhvervs- og Vækstministeriets vejledning om erhvervsøkonomiske konsekvensvurderinger gjort brug af ministeriets særlige skabelon for vurdering af erhvervsøkonomiske konsekvenser i bekendtgørelser. En nærmere beskrivelse af bekendtgørelsernes erhvervsøkonomiske konsekvenser, herunder de administrative konsekvenser, er vedlagt som bilag.

6. Bekendtgørelserne forventes – som NIS-loven – at træde i kraft den 1. juli 2016, idet bekendtgørelsen om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet dog først forventes at træde i kraft den 1. januar 2017, således at der tages højde for ekspeditionstiden for sikkerhedsgodkendelser.

Center for Cybersikkerhed vil i resten af 2016 have fokus på en dialog med de teleudbydere, der er omfattet af bekendtgørelserne, om den praktiske implementering af de nye krav, der følger af bekendtgørelserne. Centeret forventer således først i 2017 at iværksætte et egentligt tilsynskoncept til sikring af, at bekendtgørelsernes krav efterleves.

7. En fortegnelse over de myndigheder, virksomheder og organisationer, der høres over udkastene til bekendtgørelser, vedlægges.

Med venlig hilsen

Thomas Lund-Sørensen
Chef for Center for Cybersikkerhed

Bilag: Vurdering af erhvervsøkonomiske konsekvenser

Der er med udgangspunkt i Erhvervs- og Vækstministeriets vejledning om erhvervsøkonomiske konsekvensvurderinger foretaget konsekvensvurderinger i forhold til de bekendtgørelsesudkast, der skal udmønte lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed:

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

Administrative konsekvenser for erhvervslivet

Erhvervsstyrelsens Team Effektiv Regulering har i overensstemmelse med Erhvervs- og Vækstministeriets vejledning foretaget en vurdering af bekendtgørelsesudkastenes administrative konsekvenser for erhvervslivet.

Erhvervsstyrelsen har i et præhøringssvar af 12. april 2016 oplyst, at styrelsen vurderer, at bekendtgørelsesudkastene medfører administrative konsekvenser på under 4 mio. kr. årligt.

Øvrige efterlevelsesomkostninger

Center for Cybersikkerhed har endvidere foretaget en vurdering af bekendtgørelsesudkastenes øvrige efterlevelsesomkostninger. De øvrige efterlevelsesomkostninger er beregnet ved anvendelse af den metode, der er beskrevet i Erhvervs- og Vækstministeriets vejledning.

Med henblik på at fastslå de faktiske meromkostninger for erhvervslivet har Center for Cybersikkerhed indledningsvis foretaget en kortlægning af, hvilke bestemmelser i bekendtgørelsesudkastene, der indebærer skærpede krav, og hvilke bestemmelser, der alene er en videreførelse af gældende ret. Centeret har herefter gennemgået de bestemmelser, der indfører skærpede krav, enkeltvist med henblik på at vurdere bestemmelsernes direkte udgifter eller produktionsbegrænsninger.

Ved vurderingen er der – ligeledes i overensstemmelse med Erhvervs- og Vækstministeriets vejledning – taget højde for de såkaldte "business as usual"-omkostninger, som er udtryk for de aktiviteter, som teleudbyderne foretager, uanset om der stilles krav herom i reguleringen eller ej. Særligt i forhold til udkastet til bekendtgørelse om informationssikkerhed og beredskab i net og tjenester bemærkes det, at kravene til teleudbydernes risikostyring og størstedelen af kravene til gene-

relle informationssikkerhedsforanstaltninger er fastsat med udgangspunkt i DS/ISO/IEC27001, som er en anerkendt international standard, der i forvejen anvendes af en række teleudbydere.

Fastlæggelse af omkostninger og omstillingskonsekvenser er herefter som nævnt sket for hver enkel bestemmelse. Udover en vurdering af "business as usual"-omkostninger er der foretaget en vurdering af, hvor mange teleudbydere, som vil være omfattet af de enkelte bestemmelser, og en vurdering af deres omkostninger ved efterlevelse af kravene. Vurderingen er foretaget af Center for Cybersikkerheds telefaglige eksperter med udgangspunkt i det kendskab til telebranchens eksisterende informationssikkerhedsarbejde, som Center for Cybersikkerhed har opnået i forbindelse med de seneste tre års tilsynsvirksomhed.

Det vurderes på den baggrund, at bekendtgørelsesudkastene medfører øvrige efterlevelseseomkostninger på under 10 mio. kr. årligt.

Kvantificeringsskema for erhvervsøkonomiske konsekvenser

| | Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang) | Negative konsekvenser/merudgifter (hvis ja, angiv omfang) |
|---|---|--|
| Økonomiske konsekvenser for erhvervslivet | | Under 10 mio. kr. |
| Administrative konsekvenser for erhvervslivet | | Under 4 mio. kr. |