HØRINGSNOTAT

Edvard Thomsens Vej 14
2300 København S
Telefon 7221 8800
Fax 7262 6790
info@trafikstyrelsen.dk
www.trafikstyrelsen.dk

Sagsnr.: TS000502-00019
Dato 6. august 2018

I. Høringen

Trafik-, Bygge- og Boligstyrelsen har den 18. juni 2018 sendt udkast til bekendtgørelse om sikkerhed i net- og informationssystemer i transportsektoren i høring hos de i bilag 1 nævnte høringsparter. Udkastet til bekendtgørelsen har også været offentliggjort på Høringsportalen.

Høringsfristen udløb den 13. juli 2018.

Datatilsynet og **Rigsrevisionen** har meddelt, at de ikke har bemærkninger til bekendtgørelsesudkastet.

Trafik-, Bygge- og Boligstyrelsen har herudover modtaget høringssvar fra:

Banedanmark, DSB, Erhvervsflyvningens Sammenslutning, Erhvervsministeriet, Institut for Menneskerettigheder, Københavns Lufthavne, Naviair

I det følgende refereres og kommenteres hovedindholdet i de modtagne høringssvar opdelt efter relevante emner. Trafik-, Bygge- og Boligstyrelsens kommentarer til de enkelte emner følger efter i *kursiv*.

II. Høringssvar

1. Bekendtgørelsens anvendelsesområde

Erhvervsflyvningens Sammenslutning forudsætter, at bekendtgørelsen ikke omfatter Færøerne og Grønland. Erhvervsflyvningens Sammenslutning konstaterer videre, at bekendtgørelsen næppe vil omfatte organisationens medlemmer, da det er styrelsens forventning, at de operatører, der vil kunne komme i betragtning til at blive udpeget, alle vil være karakteriseret ved at være særdeles store operatører, der har en dominerende status på hver deres område.

Trafik-, Bygge- og Boligstyrelsen bekræfter, at bekendtgørelsen ikke gælder for Færøerne og Grønland, og at det er styrelsens forventning, at de operatører, der vil kunne komme i betragtning til at blive udpeget, alle vil være

karakteriseret ved at være særdeles store operatører, der har en dominerende status på hver deres område.

Erhvervsministeriet bemærker, at kriterierne for udpegning af operatører i medfør af bekendtgørelsens § 3 er forholdsvis overordnende. Erhvervsministeriet gør generelt opmærksom på, at sådanne kriterier bør administreres på en måde, som er gennemsigtig, ikke-diskriminerende og proportionel.

Trafik-, Bygge- og Boligstyrelsen bekræfter, at kriterierne vil blive administreret på en måde, som er gennemsigtig, ikke-diskriminerende og proportionel.

2. Halvårlig status for certificeringsprocessen

Naviair anfører, at formålet med løbende halvårlig statusrapportering for certificeringsprocessen i medfør af bekendtgørelsens § 5, stk. 3, forekommer uklar.

Med kravet om akkrediteret certificering senest halvandet år efter udpegningen vil en typisk implementeringsproces vare op til et år – herefter vil det være kutyme, at operatøren afprøver og tilretter systemet i op til et halvt år forud for selve certificeringsprocessen. Der vil derfor typisk ikke være grundlag for at rapportere om selve certificeringsprocessen, før der kontraheres med et akkrediteret certificeringsorgan. Det vil typisk være det akkrediterede certificeringsorgan, der fastlægger certificeringsprocessen. Dette vil med den givne tidsfrist for certificering ske mindre end et halvt år før tidsfristen for certificering. Tilsvarende er det ikke for certificering i henhold til andre væsentlige regler inden for luftfartstjenester kutyme at afgive regelmæssig status under certificeringsprocessen.

Naviair anbefaler, at § 5, stk. 3, fjernes, eller at formålet præciseres, og at der indføres passende tiltag, der understøtter formålet.

Trafik-, Bygge- og Boligstyrelsen præciserer, at den status for certificeringsprocessen, som de udpegede operatører med højest 6 måneders intervaller skal indsende til Trafik-, Bygge- og Boligstyrelsen, skal være overordnet. Der er således ikke tale om en detaljeret gennemgang af tiltag og fremdrift i certificeringsprocessen. Statusrapporten skal tjene som en overordnet orientering til Trafik-, Bygge- og Boligstyrelsen som led i tilsynet med de udpegede operatører.

3. Tidsfrist for certificering

DSB vurderer, at certificering af IT-sikkerhed iht. DS/EN ISO/IEC 27001 eller tilsvarende vil være et redskab til at dokumentere et passende IT-sikker-

hedsniveau. Det er vanskeligt at afgøre, om 18 måneder er en passende periode til at opnå certificeringen, og i lyset af denne usikkerhed vil en 24 måneders periode til opnåelse af certificering være at anbefale.

Københavns Lufthavne (CPH) tilslutter sig fuldt ud ambitionen om at have et højt fælles sikkerhedsniveau for net- og informationssystemer.

CPH har igangsat arbejdet med at udvælge en rådgiver, der skal bistå med implementeringen af ISO 27001 standarden, og bemærker, at flere af rådgiverne har oplyst, at i en virksomhed med en størrelse og en kompleksitet som CPH's vil en optimal proces for implementering af ISO 27001 forventeligt have en varighed på to år. Akkrediteret certificering senest halvandet år efter udpegningen vurderes ikke urealistisk, men det vil medføre en forceret proces, som kan få negativ indflydelse på implementeringsresultatet. CPH opfordrer derfor til, at fristen i bekendtgørelsesudkastets § 5, stk. 1, ændres til to år. Alternativt er det CPH's forhåbning, at Trafik-, Bygge- og Boligstyrelsen vil være indstillet på at benytte bekendtgørelsens dispensationsadgang og indrømme udvalgte operatører en længere frist for derved at sikre et optimalt implementeringsresultat.

Trafik-, Bygge- og Boligstyrelsen imødekommer bemærkningerne og ændrer fristen for akkrediteret certificering til to år fra udpegningen for derved at sikre et optimalt implementeringsresultat.

4. Udformningen af certificeringscertifikatet

Naviair bemærker, at i medfør af bekendtgørelsens § 6, stk. 2, skal det fremgå af certifikatet, hvilke net- og informationssystemer der er omfattet af certificeringen.

Naviair anfører, at det er kendetegnet for den certificering, der skal gennemføres, at den omfatter et sikkerhedsledelsessystem. Et sikkerhedsledelsessystem omfatter informationssikkerhed, personsikkerhed, fysisk sikkerhed og beredskab med tilhørende processer og procedurer og ikke blot de pågældende systemer, der understøtter tjenesten. Certifikatet for et sikkerhedsledelsessystem er rettet mod operatørens samlede tjeneste og ikke blot de enkelte net- og informationssystemer.

Det vil i sig selv af hensyn til sikkerheden for net- og informationssystemer være kompromitterende for tjenesten og et sikkerhedsledelsessystem, såfremt it-arkitektur og sikkerhedsarkitektur bliver publiceret sammen med certifikatet i form af en samlet systemoversigt. IT-arkitekturen og sikkerhedsarkitekturen må anses som fortrolig information og bero hos operatøren under dennes sikkerhed.

Naviair anbefaler, at sidste linje i § 6, stk. 2, slettes.

Trafik-, Bygge- og Boligstyrelsen imødekommer bemærkningerne og fjerner bestemmelsen om, at det af certifikatet eller et bilag hertil skal fremgå, hvilke net- og informationssystemer der er omfattet af certificeringen.

Styrelsen bemærker i forlængelse heraf, at det i forhold til afgrænsningen af certificeringen fortsat gælder i medfør af bekendtgørelsens § 5, stk. 5, at den akkrediterede certificering skal omfatte den del af operatørens net- og informationssystemer, som operatøren er afhængig af for at levere den væsentlige transporttjeneste, og hvor en hændelse vil få væsentlig forstyrrende virkning for leveringen af den pågældende transporttjeneste.

Styrelsen bemærker endvidere, at det certificeringscertifikat, som certificeringsorganet udsteder, er dokumentation for, at en operatøren opfylder kravene i bekendtgørelsen og i en internationalt anerkendt standard for styring af sikkerheden i net- og informationssystemer, jf. bekendtgørelsens § 6, stk. 2.

5. Leverandørydelser til operatører

Banedanmark bemærker, at det er meget sandsynligt, at Banedanmark vil blive udpeget som operatør af væsentlige transporttjenester i medfør af bekendtgørelsen.

Banedanmarks IT-sikkerhedsstrategi på programniveau er bygget op omkring principperne i ISO 27001 og overholder således eksisterende lovkrav, som Banedanmark er underlagt, om at efterleve principperne i ISO 27001. I overensstemmelse hermed har Banedanmark stillet krav om, at leverandørkontrakter, i det omfang det er relevant, ligeledes efterlever principperne i ISO 27001.

Det er Banedanmarks opfattelse, at ISO 27001 ikke stiller krav om en akkrediteret certificering hos leverandørerne. Et krav om akkrediteret certificering hos Banedanmarks leverandører vil have omfattende økonomiske konsekvenser for Banedanmark, herunder for Signalprogrammet, da Banedanmarks leverandører er globale virksomheder med flere hundredetusinde ansatte.

Naviair anfører, at det er afgørende, at de tjenester uden for transportsektoren, som de udpegede operatører af væsentlige transporttjenester benytter sig af, tillige udpeges og omfattes af tilsvarende krav for at opnå et samlet ensartet sikkerhedsniveau. Dette omfatter bl.a. relevante teleselskaber. Det er uklart for Naviair, om sådanne tjenester tillige vil blive omfattet, og hvorledes det sikres, at alle relevante tjenester til stadighed vil være omfattet.

Trafik-, Bygge- og Boligstyrelsen bemærker, at ved akkrediteret certificering i henhold til ISO 27001 er det alene operatøren af den væsentlige transporttjeneste, der er underlagt krav om akkrediteret certificering, og ikke desuden eventuelle leverandører. I henhold til standarden skal operatøren imidlertid

sikre sig, at leverandørens ydelser opfylder kravene i medfør af standarden. Det kan eksempelvis foregå ved overvågning og gennemgang af leverancerne.

For så vidt angår teleselskabernes sikkerhedsniveau bemærker Trafik-, Bygge- og Boligstyrelsen, at NIS-direktivet i Danmark er implementeret sektorvist, og at Trafik- Bygge- og Boligstyrelsen alene har kompetence til at udpege operatører inden for Transport-, Bygnings- og Boligministeriets ressortområde. Trafik-, Bygge- og Boligstyrelsen vil videreformidle Naviairs høringssvar vedrørende teleselskabernes sikkerhedsniveau til andre relevante myndigheder.

De nævnte bemærkninger giver herefter ikke Trafik-, Bygge- og Boligstyrelsen anledning til at ændre i bekendtgørelsesudkastet.

6. Underretning om hændelser

Københavns Lufthavne (CPH) anser det for yderst positivt, at bekendtgørelsen indeholder en eksemplificering af de kriterier, der navnlig skal lægges vægt på, når operatører skal vurdere, om en given hændelse er omfattet af underretningsforpligtelsen.

CPH anfører, at sondringen mellem, hvornår en hændelse skal indrapporteres henholdsvis ikke indrapporteres, er af stor vigtighed for de udpegede operatører, idet manglende indrapportering er omfattet af strafbestemmelsen i udkastets § 10. De udpegede operatører inden for de forskellige dele af transportsektoren kan derfor meget vel have behov for yderligere vejledning i, hvornår styrelsen vil anse en hændelse for omfattet af underretningsforpligtelsen. Det er CPH's forhåbning, at styrelsen efter bekendtgørelsens udstedelse vil stille sig til rådighed for en nærmere dialog herom.

Trafik-, Bygge- og Boligstyrelsen bekræfter, at der er behov for yderligere vejledning. Styrelsen vil indgå i dialog med de udpegede virksomheder om, hvilke hændelser der er omfattet af underretningspligten, og bekendtgørelsen vil blive fulgt op af vejledning til de udpegede operatører.

7. Center for Cybersikkerheds rolle som national "CSIRT"

Institut for Menneskerettigheder har ingen bemærkninger til bekendtgørelsesudkastet, idet instituttet blot henviser til sine principielle betragtninger om Center for Cybersikkerheds rolle som national "CSIRT" (Computer Security Incident Response Team) i instituttets høringssvar[1] af 4. januar 2018

[1] Instituttet anfører i høringssvar af 4. januar 2018, at det er problematisk, at Center for Cybersikkerhed varetager rollen som CSIRT og dermed modtager underretninger om

over udkast til forslag til lov om sikkerhed i net- og informationssystemer i transportsektoren (gennemførelse af NIS-direktivet) under Transport-, Bygnings- og Boligministeriet.

Trafik-, Bygge- og Boligstyrelsen henviser til Forsvarsministerens besvarelse af Transport-, Bygnings- og Boligudvalgets spørgsmål nr. 5 til L 135 (Forslag til lov om sikkerhed i net- og informationssystemer i transportsektoren, fremsat den 7. februar 2018 af transport-, bygnings- og boligministeren).

De nævnte bemærkninger giver herefter ikke Trafik-, Bygge- og Boligstyrelsen anledning til at ændre i bekendtgørelsesudkastet.

8. Økonomiske konsekvenser

DSB vurderer, at det vil være forbundet med markante omkostninger og tid at gennemføre en certificering iht. DS/EN ISO/IEC 27001 eller tilsvarende, og omkostningerne for DSB vurderes også at være væsentligt højere end de 200.000 kr., der er anslået i høringsbrevet.

Trafik-, Bygge- og Boligstyrelsen bemærker, at estimatet over de direkte omkostninger til certificering er baseret på den forventning, at de operatører, der vil kunne komme i betragtning til at blive udpeget, alle vil være karakteriseret ved at være særdeles store operatører.

9. Øvrige ændringer

Trafik-, Bygge- og Boligstyrelsen har ud over ovennævnte ændringer foretaget enkelte præciserende ændringer i bekendtgørelsen i forhold til det udkast, der har været i høring.

Det er i § 6, stk. 1, præciseret, at certificeringsorganerne, der certificerer operatører af væsentlige transporttjenester, skal være akkrediteret til at certificere operatører i henhold til bekendtgørelsen, og at certificeringsorganet skal være akkrediteret efter den relevante standard i EN ISO/IEC 170xx-serien.

---

hændelser, da Forsvarets Efterretningstjeneste som udgangspunkt er undtaget fra offentlighedslovens anvendelsesområde og fra centrale dele af forvaltningsloven. Forsvarets Efterretningstjeneste er endvidere generelt undtaget fra den gældende persondatalov og forslaget til en ny databeskyttelseslov (L 68). Med den forventede etablering af CSIRT som en del af Forsvarets Efterretningstjeneste vil CSIRT derfor være generelt undtaget fra den EU-retlige ramme for databeskyttelse, som NIS-direktivets artikel 2 kræver overholdelse af.