BEK nr 259 af 22/02/2021 (Gældende)

Bekendtgørelse om sikkerhed og beredskab i net og tjenester

Ministerium: Forsvarsministeriet

Journalnummer: Forsvarsmin.,
Center for Cybersikkerhed, j.nr. 2020/001583

Bekendtgørelse om sikkerhed og beredskab i net og tjenester[1)]

I medfør af § 3, stk. 1, 3 og 4, § 5, stk. 1 og 2, og § 14, stk. 2, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, fastsættes:

Kapitel 1

Definitioner

§ 1. I denne bekendtgørelse forstås ved:

1) Beredskabsaktører: Myndigheder, institutioner og virksomheder, som skal bidrage til opretholdelse af samfundets funktioner i beredskabssituationer og i andre ekstraordinære situationer.
2) Beredskabssituationer og andre ekstraordinære situationer: Større ulykker, katastrofer eller hændelser, hvor det kan være nødvendigt at indføre særlige foranstaltninger vedrørende net og tjenester med henblik på at kunne opretholde samfundets funktioner.
3) Kritiske netkomponenter, systemer og værktøjer: Operations support systemer, network management systemer og business support systemer, der kan benyttes til at aflæse, ændre indhold af eller dirigere data, som relaterer sig til slutbrugere, samt hardware, firmware og software, der anvendes i eller i forbindelse med core-net i mobilnet, fastnet og internet, eller i centrale routere og servere i backbonenettene eller i kontrolenheder, som anvendes til styring i mobilnettenes radionet.
4) Slutbruger: En bruger af net og tjenester, som ikke på kommercielt grundlag stiller de pågældende net og tjenester til rådighed for andre.
5) Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester:
   a) Udbydere af net, hvor disse net anvendes af mere end 50.000 slutbrugere. Ved opgørelsen medregnes de slutbrugere, der har aftaleforhold med udbyderens kunder. Radio- og tv-stationer, der er udbydere af net, er kun omfattet, såfremt de har landsdækkende public service-forpligtelser.
   b) Udbydere, der gennem aftaler med statslige myndigheder og institutioner betjener mere end 500 slutbrugere. Ved opgørelsen medregnes de statslige myndigheder og institutioners egne slutbrugere.
6) Erhvervsmæssige udbydere af NUIK-tjenester: Udbydere, der med kommercielt formål udbyder NUIK-tjenester som sine hovedydelser eller som en ikke accessorisk del af virksomheden.
7) Væsentlige erhvervsmæssige udbydere af NUIK-tjenester:
   a) Udbydere af NUIK-tjenester, hvor disse tjenester anvendes af mere end 50.000 slutbrugere. Ved opgørelsen medregnes de slutbrugere, der har aftaleforhold med udbyderens kunder.
   b) Udbydere af NUIK-tjenester, der gennem aftaler med statslige myndigheder og institutioner betjener mere end 500 slutbrugere. Ved opgørelsen medregnes de statslige myndigheder og institutioners egne slutbrugere.

Kapitel 2

Risikostyring mv.

Udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

§ 2. Udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal gennemføre en risikovurdering, der skal tage stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i de net og tjenester, der udbydes.

Stk. 2. Såfremt udbydernes net og tjenester helt eller delvist drives af en tredjepart, skal eventuelle risici forbundet hermed medtages i risikovurderingen efter stk. 1.

Stk. 3. På baggrund af risikovurderingen efter stk. 1 og 2 skal udbyderne implementere passende foranstaltninger til sikring af tilgængelighed, autenticitet, integritet og fortrolighed i net og tjenester samt sikre, at tredjepart opretholder en tilsvarende sikkerhed i forhold til driftsleverancer til udbyderne efter stk. 2.

Stk. 4. Risikovurderinger efter stk. 1 og 2 samt foranstaltninger efter stk. 3 skal løbende tilpasses, herunder ved væsentlige ændringer af udbydernes virksomhed og i trusselsbilledet.

Erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

§ 3. Erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal udarbejde og gennemføre en ledelsesgodkendt informationssikkerhedspolitik efter en anerkendt international standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende. Informationssikkerhedspolitikken skal herunder beskrive de processuelle og organisatoriske rammer for arbejdet med sikkerheden i net og tjenester.

Stk. 2. Udbyderne skal sikre, at informationssikkerhedspolitikken er kommunikeret til alle relevante medarbejdere.

Stk. 3. Udbyderne skal løbende tilpasse informationssikkerhedspolitikken, herunder ved væsentlige ændringer af udbydernes virksomhed og i trusselsbilledet. Der skal dog mindst én gang om året foretages en vurdering af behovet for revision af informationssikkerhedspolitikken. Informationssikkerhedspolitikken skal på den baggrund revideres i fornødent omfang.

§ 4. Erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal på baggrund af informationssikkerhedspolitikken efter § 3 sikre, at der er etableret en informationssikkerhedsorganisation. Varetagelsen af relevante sikkerhedsopgaver, herunder roller og ansvar, skal i den forbindelse være beskrevet samt i fornødent omfang være kommunikeret til udbydernes medarbejdere.

Stk. 2. Udbyderne skal sikre, at Center for Cybersikkerhed til enhver tid er orienteret om kontaktoplysninger til lederen af informationssikkerhedsorganisationen.

§ 5. Erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal foretage risikostyring efter en anerkendt international standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende.

Stk. 2. Som led i risikostyringen skal udbyderne fastsætte en samlet risikostyringsproces, der omfatter risikovurdering og -håndtering af informationssikkerhedsrisici. Der skal i den forbindelse tages stilling til kriterier for udbydernes risikovillighed.

Stk. 3. Risikostyringsprocessen skal i fornødent omfang dokumenteres samt tilpasses, herunder ved væsentlige ændringer af udbydernes virksomhed.

Væsentlige erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

§ 6. Væsentlige erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal styre sikkerheden i net og tjenester gennem et ledelsessystem, der skal etableres efter en anerkendt international standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende.

§ 7. For væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal informationssikkerhedspolitikken efter § 3 desuden beskrive udbydernes politik for håndtering af beredskabssituationer og andre ekstraordinære situationer med henblik på at sikre, at net og tjenester i videst muligt omfang kan opretholdes i sådanne situationer.

§ 8. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal sikre, at informationssikkerhedsorganisationen efter § 4 desuden kan håndtere beredskabssituationer og andre ekstraordinære situationer.

§ 9. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal som en del af fastlæggelsen af risikovillighed i risikostyringsprocessen efter § 5 desuden tage højde for, at udbyderne i videst muligt omfang skal opretholde udbuddet af net og tjenester i beredskabssituationer og i andre ekstraordinære situationer med henblik på at sikre samfundets teleforsyning.

Kapitel 3

Generelle informationssikkerhedsforanstaltninger i net og tjenester

§ 10. Væsentlige erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal sikre, at medarbejdere og samarbejdspartnere i fornødent omfang er bekendte med det aktuelle trusselsbillede for udbyderen, herunder at de har et generelt kendskab til trusler, der kan påvirke udbuddet af net og tjenester.

§ 11. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal til brug for risikostyringen efter §§ 5 og 9 have etableret og vedligeholde et register over udbyderens kritiske netkomponenter, systemer og værktøjer.

Stk. 2. Væsentlige erhvervsmæssige udbydere af NUIK-tjenester skal til brug for risikostyringen efter § 5 have etableret og vedligeholde et register over udbyderens kritiske netkomponenter, systemer og værktøjer.

§ 12. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal på baggrund af risikostyringen efter §§ 5 og 9 udarbejde og implementere en sikringsplan for beskyttelse af udbydernes kritiske netkomponenter, systemer og værktøjer.

Stk. 2. Væsentlige erhvervsmæssige udbydere af NUIK-tjenester skal på baggrund af risikostyringen efter § 5 udarbejde og implementere en sikringsplan for beskyttelse af udbydernes kritiske netkomponenter, systemer og værktøjer.

Stk. 3. De i stk. 1 og 2 nævnte sikringsplaner skal som minimum tage stilling til logisk og fysisk adgangskontrol, fysisk perimetersikring, brandsikring, klimasikring samt varslingssystemer til detektion af uautoriseret adgang.

§ 13. Væsentlige erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal i fornødent omfang etablere procedurer for og implementere logning og monitorering med henblik på at sikre sporbarhed ved eventuelle sikkerhedshændelser.

Stk. 2. Udbyderne skal sikre, at al aktivitet i forbindelse med logisk adgang til kritiske netkomponenter, systemer og værktøjer udført af medarbejdere med administratorrettigheder logges.

Stk. 3. Logfilerne skal sikres mod manipulation, og alene et begrænset antal særligt betroede medarbejdere må kunne ændre på, hvilke informationer der logges.

Stk. 4. Udbyderne skal regelmæssigt gennemgå logfilerne med henblik på identifikation af mulige sikkerhedshændelser.

Stk. 5. Center for Cybersikkerhed kan dispensere fra kravene i stk. 2-4. Dispensationen kan betinges af, at udbyderen implementerer nærmere fastsatte kompenserende sikkerhedsforanstaltninger.

§ 14. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal i fornødent omfang implementere processer for installation, flytning og fjernelse af eller ændringer i øvrigt i systemer og udstyr.

Stk. 2. Ved ændringer i kritiske netkomponenter, systemer og værktøjer skal udbyderne gennemføre en risikovurdering med henblik på at definere, hvilke tests der skal udføres forud for ændringen. De herefter identificerede tests skal være gennemført og evalueret forud for ændringen.

Stk. 3. Ved ændringer efter stk. 2 skal der være etableret procedurer for genskabelse til en tidligere version, hvis en ændring fejler.

§ 15. Væsentlige erhvervsmæssige udbydere af NUIK-tjenester skal i fornødent omfang implementere processer for installation, flytning og fjernelse af eller ændringer i øvrigt i systemer og udstyr.

Stk. 2. Ved ændringer i kritiske netkomponenter, systemer og værktøjer skal udbyderne gennemføre en risikovurdering med henblik på at definere, om der skal gennemføres tests og i givet fald, hvilke tests der skal udføres forud for ændringen. De herefter identificerede tests skal være gennemført og evalueret forud for ændringen.

Stk. 3. Ved ændringer efter stk. 2 skal der i fornødent omfang være etableret procedurer for genskabelse til en tidligere version, hvis en ændring fejler.

§ 16. Væsentlige erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal etablere procedurer for håndtering af sikkerhedshændelser. Som led heri skal udbyderne sikre, at roller og ansvarsområder for håndtering af sikkerhedshændelser er fastlagt. Procedurerne skal herudover beskrive håndtering og kategorisering af sikkerhedshændelser, sikring af nødvendige informationer til brug for efterfølgende sikkerhedshændelsesanalyser samt intern og ekstern rapportering.

§ 17. Væsentlige erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal til enhver tid holde sig orienteret om nye sårbarheder, der vil kunne have konsekvenser for udbydernes net og tjenester.

Stk. 2. Med henblik på at sikre, at de etablerede informationssikkerhedsforanstaltninger i net og tjenester fortsat er effektive, skal udbyderne gennemføre relevante tekniske tests for potentielle sårbarheder, eksempelvis i form af sårbarhedsscanninger.

§ 18. Væsentlige erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal sikre, at der er relevante procedurer for backup og genskabelse af data, og at disse procedurer regelmæssigt afprøves. Backupsystemets opbygning samt procedurer for backupdatas opbevaring, transport og destruktion skal dokumenteres. Dokumentationen skal opdateres ved væsentlige ændringer i backupsystemet.

§ 19. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal sikre en hensigtsmæssig adskillelse mellem udbydernes net, herunder produktions-, administrations-, styrings- og testnet.

Stk. 2. Ved opdeling af udbydernes net i flere logiske net skal dette ske i overensstemmelse med internationalt anerkendte retningslinjer. På baggrund af udbydernes risikovurderinger skal der etableres adgangskontrol for hvert logiske net.

§ 20. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal, baseret på risikostyringsprocessen efter §§ 5 og 9, sikre, at der i forhold til kritiske netkomponenter, systemer og værktøjer er etableret den nødvendige nødstrømsforsyning, redundans, understøttende forsyning eller anden sikring med tilsvarende virkning.

Stk. 2. Væsentlige erhvervsmæssige udbydere af NUIK-tjenester skal, baseret på risikostyringsprocessen efter § 5, sikre, at der i forhold til kritiske netkomponenter, systemer og værktøjer i fornødent omfang er etableret den nødvendige nødstrømsforsyning, redundans, understøttende forsyning eller anden sikring med tilsvarende virkning.

§ 21. Væsentlige erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal sikre, at der så tidligt som muligt sker inddragelse af informationssikkerhedsaspekter ved anskaffelse, udvikling, ændring og vedligeholdelse af netkomponenter, systemer og værktøjer, der anvendes i net og tjenester.

§ 22. Såfremt der etableres et samarbejde mellem erhvervsmæssige udbydere, hvoraf mindst en af parterne er en væsentlig erhvervsmæssig udbyder af NUIK-tjenester eller offentligt tilgængelige elektroniske kommunikationsnet og -tjenester, finder de krav, som henholdsvis en væsentlig erhvervsmæssig udbyder af NUIK-tjenester eller offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal efterleve efter denne bekendtgørelse, anvendelse på de dele af net og tjenester, der er omfattet af aftalen.

Stk. 2. Den aftalepart, der driver det net eller den tjeneste, som samarbejdet vedrører, er ansvarlig for, at kravene efter denne bekendtgørelse efterleves.

Stk. 3. Aftaleparternes aftalegrundlag skal tage højde for informationssikkerhedsaspekter i forhold til udbuddet af net og tjenester ved samarbejdet. Aftalegrundlaget skal i fornødent omfang opdateres, hvis der sker ændringer af informationssikkerhedsmæssig betydning.

§ 23. Såfremt der etableres et samarbejde mellem en væsentlig erhvervsmæssig udbyder af NUIK-tjenester eller offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og en leverandør, er den pågældende udbyder fortsat ansvarlig for, at kravene efter denne bekendtgørelse efterleves.

Stk. 2. Aftaleparternes aftalegrundlag skal tage højde for informationssikkerhedsaspekter i forhold til udbuddet af net og tjenester ved samarbejdet. Aftalegrundlaget skal i fornødent omfang opdateres, hvis der sker ændringer af informationssikkerhedsmæssig betydning.

Stk. 3. Udbyderen skal på baggrund af risikovurderingen efter § 2 i fornødent omfang foretage verifikation af, at der er overensstemmelse mellem aftalepartens leverancer, herunder konfigurationen af leverancerne, og det mellem parterne aftalte.

Stk. 4. Verifikationen efter stk. 3 kan ske som en stikprøvekontrol, såfremt det står i forhold til udbyderens risikovurdering efter § 2.

§ 24. Ved etablering at et samarbejde efter §§ 22 og 23 skal de deltagende udbydere sikre, at der sker intern auditering af efterlevelsen af de informationssikkerhedskrav, der fremgår af aftalegrundlaget.

§ 25. Bestemmelsen i § 23, stk. 1, finder tilsvarende anvendelse på erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester.

Kapitel 4

Påbud om konkrete informationssikkerhedsforanstaltninger

Udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

§ 26. Center for Cybersikkerhed kan, når en betydelig trussel er identificeret, og det er nødvendigt for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, påbyde udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at gennemføre en risikovurdering, der skal tage stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i de net og tjenester, der udbydes.

Erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

§ 27. Center for Cybersikkerhed kan, når en betydelig trussel er identificeret, og det er nødvendigt for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, påbyde erhvervsmæssige udbydere af NUIK-tjenester og offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at træffe en eller flere af følgende foranstaltninger:

1) Etablering eller styrkelse af logisk adgangskontrol til nærmere angivne og særligt kritiske netkomponenter, systemer og værktøjer, herunder krav til proces for adgangsstyring og kontrol med leverandørers adgang.
2) Etablering eller styrkelse af foranstaltninger til fysisk sikring af nærmere angivne og særligt kritiske netkomponenter, systemer og værktøjer, herunder fysisk adgangskontrol.

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.

§ 28. Center for Cybersikkerhed kan, såfremt det er af væsentlig samfundsmæssig betydning, efter en konkret vurdering påbyde erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at foretage en eller flere af følgende foranstaltninger:
1) Etablering eller styrkelse af logisk adgangskontrol til kritiske netkomponenter, systemer og værktøjer, herunder krav til proces for adgangsstyring og kontrol med leverandørers adgang.
2) Etablering eller styrkelse af foranstaltninger til fysisk sikring af kritiske netkomponenter, systemer og værktøjer, herunder fysisk adgangskontrol.
3) Sikring af sporbarhed eller logning af fysisk eller logisk adgang til kritiske netkomponenter, systemer og værktøjer, herunder krav om analyse af logfiler.
4) Sikring af redundans for kritiske netkomponenter, systemer og værktøjer samt backup af konfigurationsdata.
5) At udstyr, der benyttes til at foretage indgreb i meddelelseshemmeligheden, skal opsættes i og drives fra Danmark.
6) At udstyr, der benyttes til at foretage indgreb i meddelelseshemmeligheden, ikke må leveres af en leverandør, som er identisk med udbyderens primære leverandører af kritiske netkomponenter, systemer og værktøjer.
7) Sikring af, at indlejret funktionalitet, der vil kunne benyttes til at foretage indgreb i meddelelseshemmeligheden, fjernes fra en leverance af netkomponenter, systemer og værktøjer.

Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

§ 29. Center for Cybersikkerhed kan, såfremt det er af væsentlig samfundsmæssig betydning, efter en konkret vurdering påbyde væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at foretage en eller flere af følgende foranstaltninger:
1) Gennemførelse af uafhængig sikkerhedsevaluering i forbindelse med leverancer af kritiske netkomponenter, systemer og værktøjer fra en specifik leverandør, såfremt den pågældende leverandør eller den pågældende leverance ud fra en generel sikkerhedsmæssig betragtning eller det aktuelle trusselsbillede vurderes at udgøre en særlig sikkerhedsrisiko. Center for Cybersikkerhed kan i den forbindelse stille krav om, at sikkerhedsevalueringen gennemføres af et anerkendt evalueringsorgan, efter en anerkendt international standard og indenfor nærmere fastsatte rammer.
2) Sikring af, at der ikke kan etableres direkte elektroniske supportforbindelser mellem en leverandør og en udbyder, såfremt den pågældende leverandør ud fra en generel sikkerhedsmæssig betragtning eller det aktuelle trusselsbillede vurderes at udgøre en særlig sikkerhedsrisiko.
3) Sikring af, at personale, der har adgang til kritiske netkomponenter, systemer og værktøjer, er sikkerhedsgodkendt af den relevante danske sikkerhedsmyndighed.
4) Indstationering af personale, der er sikkerhedsgodkendt af den relevante danske sikkerhedsmyndighed, hos udenlandske leverandører, som en udbyder har outsourcet hele eller dele af udbyderens net og tjenester eller varetagelsen af driften heraf til. Der kan stilles krav om, at det indstationerede personale, såfremt dette er i overensstemmelse med national lovgivning, skal have adgang til alle relevante systemer og informationer hos leverandøren med henblik på at udføre sikkerhedskontrol for udbyderen.

5) Sikring af, at der på udbyderens foranstaltning i tilfælde af misligholdelse af en kontrakt om outsourcing kan ske hjemtagning af opgaver, der er outsourcede til en udenlandsk leverandør. Der kan herunder stilles krav om, at udbyderen skal fastlægge procedurer for hjemtagning af outsourcede områder.
6) Sikring af, at kritiske styringsprocesser skal godkendes af udbyderen, hvis der er sket outsourcing af drift af net og tjenester.
7) Fastholdelse hos udbyderen af de nødvendige kompetencer til at gennemføre risikovurdering efter § 2, hvis der er sket outsourcing af drift af net og tjenester. Der kan herunder stilles krav om, at udbyderen skal fastholde de nødvendige kompetencer til at foretage validering af, at den leverede driftsydelse svarer til det aftalte.
8) Sikring af, at konfiguration af nærmere bestemte kritiske netkomponenter, systemer og værktøjer på baggrund af nærmere angivne konkrete trusler og sårbarheder sker i henhold til nærmere fastsatte internationale standarder eller anbefalinger.

Kapitel 5

Krisestyring i beredskabssituationer og i andre ekstraordinære situationer

Udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

§ 30. Udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal foretage planlægning og træffe foranstaltninger for krisestyring med henblik på i videst muligt omfang at kunne opretholde net og tjenester i beredskabssituationer og i andre ekstraordinære situationer.

§ 31. Udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal, såfremt udbyderne vurderer, at dette er nødvendigt, udarbejde en krisestyringsplan.

Stk. 2. Krisestyringsplanen efter stk. 1 skal som minimum omfatte udbydernes håndtering af følgende områder:

1) Organisering af udbydernes interne beredskab.
2) Aktivering og eskalering af beredskabet.
3) Varetagelse af krisekommunikation.
4) Ressourcestyring, herunder tilkaldelse af medarbejdere i en beredskabssituation eller i en anden ekstraordinær situation.
5) Alternative muligheder for fremskaffelse af reserveudstyr.
6) Behov for serviceaftaler.

Stk. 3. Hvis der i krisestyringsplanen er identificeret behov for konkrete forberedende foranstaltninger, skal udbyderne gennemføre disse foranstaltninger uden ugrundet ophold.

Stk. 4. Krisestyringsplanen skal løbende revideres i det omfang, udviklingen tilsiger dette, herunder ved væsentlige ændringer af udbydernes virksomhed og i trusselsbilledet, dog som minimum hvert andet år.

Stk. 5. Hvis en udbyder ikke har udarbejdet en krisestyringsplan, skal vurderingen efter stk. 1 som minimum gennemføres hvert andet år.

§ 32. Udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester kan vælge at overlade beredskabsplanlægningen efter § 30, herunder udarbejdelsen af en krisestyringsplan efter § 31, til tredjemand. Ansvaret for beredskabsplanlægningen påhviler dog fortsat udbyderne.

Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

§ 33. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal udarbejde en krisestyringsplan.

Stk. 2. Krisestyringsplanen skal udarbejdes i overensstemmelse med § 31, stk. 2, og skal herudover som minimum beskrive:

1) Etablering og drift af en krisestyringsorganisation, herunder ansvar, roller og opgaver i en beredskabssituation eller i en anden ekstraordinær situation.
2) Procedurer for håndtering af påbud fra Center for Cybersikkerhed om gennemførelse af akutte sikkerhedsforanstaltninger og om retablering af nærmere bestemte dele af net og tjenester samt om iværksættelse af på forhånd forberedte konkrete foranstaltninger til prioritering i net og tjenester med henblik på at sikre beredskabsaktørers samfundsvigtige kommunikation, jf. bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.
3) Beskrivelse af samarbejdet med Center for Cybersikkerhed i en beredskabssituation eller i en anden ekstraordinær situation, herunder beskrivelse af proceduren for underretning af centeret i forbindelse med aktivering af udbyderens interne beredskab, jf. § 35, angivelse af kontaktinformation til centeret samt procedure for afgivelse af situationsrapporter til centeret, jf. § 36.
4) Udbyderens procedure for modtagelse og håndtering af oplysninger, herunder klassificeret information, fra Center for Cybersikkerhed om en beredskabssituation eller en anden ekstraordinær situation.
5) Beskrivelse af anvendelse af kommunikationsmidler i situationer, hvor de gængse kommunikationsmidler ikke er tilgængelige.

§ 34. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal sikre, at Center for Cybersikkerhed døgnet rundt kan komme i kontakt med udbyderne i forbindelse med en beredskabssituation eller en anden ekstraordinær situation. Det skal ved kontakt fra Center for Cybersikkerhed kunne foranlediges, at udbyderens interne beredskab straks aktiveres.

§ 35. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal straks underrette Center for Cybersikkerhed ved enhver aktivering og efterfølgende de-aktivering af udbyderens interne beredskab.

§ 36. Hvis en beredskabssituation eller en anden ekstraordinær situation har medført, at en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester har aktiveret udbyderens interne beredskab, skal udbyderen herefter løbende afgive situationsrapporter til Center for Cybersikkerhed. Situationsrapporterne skal fremsendes mindst hver fjerde time, medmindre andet er aftalt med Center for Cybersikkerhed.

Stk. 2. Situationsrapporterne skal, så vidt det er teknisk muligt, afgives elektronisk, og skal som minimum indeholde følgende oplysninger:
1) Virksomhedens kontaktoplysninger.
2) Tidsrummet, som situationsrapporten omfatter.
3) Beskrivelse af, hvad der er sket, eksempelvis berørte dele af net og tjenester, antallet af berørte slutbrugere eller berørte geografiske områder, eventuelt siden den seneste situationsrapport.
4) Beskrivelse af, hvilke foranstaltninger udbyderen har truffet, eventuelt siden den seneste situationsrapport.
5) Beskrivelse af, hvilke foranstaltninger udbyderen fremadrettet forventer at træffe.

§ 37. Efter de-aktivering af udbyderens interne beredskab skal væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester efter påbud fra Center for Cybersikkerhed fremsende en rapport om udbydernes hændelseshåndtering, herunder eventuelt planlagt opfølgning.

§ 38. Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal som minimum én gang hvert andet år afholde en intern beredskabsøvelse, som omfatter anvendelse af udbyderens krisestyringsplan.

Stk. 2. Senest tre måneder efter en afholdt øvelse skal udbyderne have udarbejdet en rapport, som beskriver øvelsens formål, forløb, opnåede erfaringer og planlagt opfølgning. Udbyderne skal efter påbud fra Center for Cybersikkerhed fremsende rapporten til centeret.

§ 39. Center for Cybersikkerhed kan påbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at deltage i en national eller international krisestyringsøvelse.

Stk. 2. Påbud efter stk. 1 kan højest udstedes to gange om året og højest fire gange indenfor en periode på fem år. Påbuddet skal indeholde et varsel på mindst tre måneder.

Kapitel 6

Straffebestemmelser og ikrafttrædelse

§ 40. Med bøde straffes, medmindre strengere straf er forskyldt efter den øvrige lovgivning, den, der

1) overtræder §§ 2-12, § 13, stk. 1-4, §§ 14-21, § 22, stk. 3, § 23, stk. 2 og 3, § 24, §§ 30 og 31, §§ 33-36 og § 38, stk. 1 og stk. 2, 1. pkt., eller
2) undlader at efterkomme et påbud efter §§ 26-28, § 29, § 37, § 38, stk. 2, 2. pkt., og § 39, stk. 1.

Stk. 2. Der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

§ 41. Bekendtgørelsen træder i kraft den 1. marts 2021.

Stk. 2. Bekendtgørelse nr. 567 af 1. juni 2016 om informationssikkerhed og beredskab i net og tjenester ophæves.

Center for Cybersikkerhed, den 22. februar 2021

THOMAS LUND-SØRENSEN

/ Anette Arnsted

[1)] Bekendtgørelsen indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning), EU-Tidende 2018, nr. L 321, side 36.