SUNDHEDS- OG ÆLDREMINISTERIET

UDKAST

Bekendtgørelse om operatører af væsentlige tjenester

I medfør af § 3, stk. 3, § 4, stk. 3, § 5, stk. 5, og § 6, stk. 1 og 3, i lov nr. [x] af [dato] om krav til sikkerhed i net- og informationssystemer inden for sundhedssektoren, fastsættes:

Kapitel 1

Definitioner

§ 1. I denne bekendtgørelse forstås ved:

1) Sundhedsfaglig behandling: Undersøgelse, diagnosticering, sygdomsbehandling, fødselshjælp, genoptræning, sundhedsfaglig pleje samt forebyggelse og sundhedsfremme i forhold til den enkelte patient.
2) Fortrolighed: At information ikke gøres tilgængelig eller afsløres for uautoriserede personer.
3) Integritet: Datas nøjagtighed og fuldstændighed.
4) Tilgængelighed: At tjenesten er tilgængelig og anvendelig ved anmodning fra en autoriseret bruger.
5) Autenticitet: Egenskaben, at identitet eller ægthed af en information er sand og troværdig.
6) Robusthed: Opretholdelse af tilgængelighed, fortrolighed og integritet på trods af, at der konstateres fejl.

Kapitel 2

Identificering af operatører af væsentlige tjenester

§ 2. En enhed betragtes som en operatør af en væsentlig tjeneste, hvis

1) Enheden leverer en tjeneste, der er væsentlig for opretholdelsen af sundhedsfaglig behandling,
2) leveringen af denne tjeneste afhænger af net- og informationssystemer, og
3) en hændelse vil få væsentlige forstyrrende virkninger for leveringen af denne tjeneste, som medfører konsekvenser for:
   a) Sundhedsberedskabet i Danmark, herunder den nationale operative stabs funktion,
   b) det regionale sundhedsberedskab,
   c) mere end 500.000 borgere, der er omfattet af tjenesten,
   d) mere end 50.000 personer, herunder patienter og sundhedspersoner, der er afhængige af tjenesten, eller
   e) mindst en region.

Stk. 2. Ved identificeringen af en operatør af en væsentlig tjeneste efter stk. 1, skal der lægges vægt på, om en hændelses væsentlige forstyrrende virkninger for leveringen af tjenesten kan få konsekvenser for andre samfundskritiske sektorer.

Stk. 3. Stk. 1 finder ikke anvendelse, hvis tjenesten kan leveres uden understøttelse af net- og informationssystemer i mere end 72 timer.

SUNDHEDS- OG ÆLDREMINISTERIET

Kapitel 3

Sikkerhedsforanstaltninger

§ 3. En operatør af en væsentlig tjeneste skal gennemføre en risikovurdering, der skal tage stilling til robusthed og risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i net- og informationssystemer, der understøtter tjenesten.

Stk. 2. Såfremt net- og informationssystemer, der understøtter operatørens væsentlige tjeneste, helt eller delvist drives af en underleverandør, skal eventuelle risici forbundet hermed medtages i risikovurderingen efter stk. 1.

Stk. 3. På baggrund af risikovurderingen efter stk. 1 og 2 skal operatøren implementere passende foranstaltninger til sikring af robusthed, tilgængelighed, autenticitet, integritet og fortrolighed i de net- og informationssystemer, der understøtter den væsentlige tjeneste. Operatøren er forpligtet til at sikre, at en underleverandør opretholder tilsvarende sikkerhed i forhold til driftsleverancer til operatøren.

Stk. 4. Risikovurderingen efter stk. 1 og 2 og foranstaltningerne efter stk. 3 skal løbende tilpasses, herunder ved væsentlige ændringer af operatørens virksomhed eller ved væsentlige ændringer i trusselsbilledet.

§ 4. En operatør af en væsentlig tjeneste skal udarbejde og vedligeholde en ledelsesgodkendt net- og informationssikkerhedspolitik med udgangspunkt de til enhver tid anerkendte internationale standarder herfor, eksempelvis DS/ISO/IEC 27001 eller tilsvarende. Informationssikkerhedspolitikken skal blandt andet beskrive de processuelle og organisatoriske rammer for arbejdet med sikkerheden, herunder operatørens politik for håndtering af beredskabssituationer og andre ekstraordinære situationer. Dette med henblik på at sikre, at tjenesten, og leveringen heraf, i videst muligt omfang kan opretholdes i sådanne situationer.

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

Stk. 3. Operatøren skal løbende tilpasse informationssikkerhedspolitikken, herunder ved væsentlige ændringer af operatørens virksomhed eller ved væsentlige ændringer i trusselsbilledet. Der skal dog mindst én gang om året foretages en vurdering af behovet for at tilpasse informationssikkerhedspolitikken.

§ 5. En operatør af en væsentlige tjeneste skal på baggrund af informationssikkerhedspolitikken efter § 4 sikre, at der er etableret en sikkerhedsorganisation. Varetagelsen af relevante sikkerhedsopgaver, herunder roller og ansvar, skal i den forbindelse være beskrevet og i fornødent omfang være kommunikeret til operatørens medarbejdere.

§ 6. En operatør af en væsentlig tjeneste skal foretage risikostyring i forbindelse med de net- og informationssystemer, der understøtter den væsentlige tjeneste, med udgangspunkt i de til enhver tid anerkendte internationale standarder, eksempelvis DS/ISO/IEC 27001 eller tilsvarende.

Stk. 2. Som led i risikostyringen skal operatøren fastlægge en samlet risikostyringsproces, der omfatter risikovurderingen efter § 3 og håndtering af sikkerhedsrisici. Der skal i den forbindelse tages stilling til kriterier for operatørens risikovillighed.

Stk. 3. Ved fastlæggelsen af risikovillighed efter stk. 2 skal der tages højde for, at operatøren i videst muligt omfang skal opretholde den væsentlige tjeneste og leveringen heraf i beredskabssituationer og i andre ekstraordinære situationer med henblik på at sikre opretholdelse af sundhedsfaglig behandling.

Stk. 4. Risikostyringsprocessen skal i fornødent omfang dokumenteres og tilpasses, herunder ved væsentlige ændringer af operatørens virksomhed eller ved væsentlige ændringer i trusselsbilledet.

Kapitel 4

Registrering hos sundhedsministeren

§ 7. En operatør af en væsentlig tjeneste skal lade sig registrere hos sundhedsministeren.

Stk. 2. En operatør af en væsentlig tjeneste skal i forbindelse med registreringen angive:

1) Navn og kontaktoplysninger på operatøren,
2) begrundelse for, at operatøren leverer en væsentlig tjeneste,
3) oplysninger om det anvendte net- og informationssystem og
4) oplysninger om eventuelle underleverandører.

Kapitel 5

Underretning

§ 8. En operatør af en væsentlig tjeneste skal foretage underretning til sundhedsministeren og Center for Cybersikkerhed om en hændelse, der har væsentlige konsekvenser for kontinuiteten af leveringen af den væsentlige tjeneste.

Stk. 2. Underretningen skal ske under hensyntagen til operatørens arbejde med at minimere konsekvenserne af hændelsen.

Stk. 3. Underretningen skal ske gennem én digital indgang for indberetning af it-sikkerhedshændelser, der stilles til rådighed af Erhvervsstyrelsen.

Stk. 4. Underretningen skal indeholde oplysninger, der er nødvendige for, at sundhedsministeren kan vurdere hændelsens omfang, herunder som minimum:

1) Navn og kontaktoplysninger på operatøren,
2) oplysninger om hændelsens årsag, karakter, varighed, forløb og konsekvenser,
3) oplysninger om foranstaltninger, som operatøren har truffet, eller foreslår truffet, for at håndtere hændelsen,
4) oplysninger om omfanget af hændelsen og
5) oplysninger om eventuelle grænseoverskridende konsekvenser af hændelsen.

Stk. 5. Er operatøren ikke i besiddelse af de nødvendige oplysninger på tidspunktet for underretningen, jf. stk. 1, afgiver operatøren en delvis underretning. Den delvise underretning skal hurtigst muligt følges op af en komplet underretning.

SUNDHEDS- OG ÆLDREMINISTERIET

Kapitel 6

Ikrafttræden

§ 9. Bekendtgørelsen træder i kraft den 10. maj 2018.

Sundheds- og Ældreministeriet, [dato]

XX