UDKAST

Bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige tjenester på domænenavnsområdet

I medfør af § 3, stk. 3, § 4, stk. 3, § 5, stk. 4 og § 17, stk. 2, i lov nr. yyy af xx. xx 2018 om sikkerhed i net- og informationssystemer for domænenavnssystemer og visse digitale tjenester, fastsættes:

Kapitel 1

Definition og anvendelsesområde

§ 1. Denne bekendtgørelse finder anvendelse på operatører af væsentlige tjenester, jf. lov om sikkerhed i net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester.

Stk. 2. En topdomænenavnsadministrator anses for at være en operatør af væsentlige tjenester, hvis administratoren og dennes koncernforbundne selskaber har mere end 500.000 andenordens internetdomænenavne registreret under topdomænenavnet.

Stk. 4. En DNS-tjenesteudbyder anses for at være en operatør af væsentlige tjenester, hvis udbyderen og dennes koncernforbundne selskaber har

1) rekursive navneservere som mere end 100.000 brugere anvender, eller

2) autoritative navneservere, som har mere end 100.000 andenordens internetdomænenavne tilsluttet.

Kapitel 2

Krav til sikkerheden i net- og informationssystemer

§ 2. Operatører af væsentlige tjenester skal gennemføre en risikovurdering, der skal tage stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i de væsentlige tjenester, som fremgår af bilag 1.

Stk. 2. Såfremt operatørens væsentlige 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 operatørerne implementere passende foranstaltninger til sikring af tilgængelighed, autenticitet, integritet og fortrolighed i de væsentlige tjenester samt sikre, at tredjepart opretholder en tilsvarende sikkerhed i forhold til driftsleverancer til operatøren efter stk. 2.

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

§ 3. Operatører af væsentlige tjenester skal udarbejde og gennemføre en ledelsesgodkendt net- og sikkerhedspolitik med udgangspunkt i en anerkendt international standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende. Sikkerhedspolitikken skal herunder beskrive de processuelle og organisatoriske rammer for arbejdet med sikkerheden og operatørens 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.

Stk. 2. Operatørerne skal sikre, at sikkerhedspolitikken er kommunikeret til alle relevante medarbejdere.

Stk. 3. Operatørerne skal løbende tilpasse sikkerhedspolitikken, herunder ved væsentlige ændringer af operatørernes virksomhed og i trusselsbilledet. Der skal dog mindst én gang om året foretages en vurdering af behovet for at tilpasse sikkerhedspolitikken.

§ 4. Operatører af væsentlige tjenester skal på baggrund af sikkerhedspolitikken efter § 3 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 operatørernes medarbejdere.

§ 5. Operatører af væsentlige tjenester skal foretage risikostyring i forbindelse med de væsentlige tjenester, som fremgår af bilag 1, med udgangspunkt i en anerkendt international standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende.

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

Stk. 3. Ved fastlæggelsen af risikovillighed efter stk. 2 skal der tages højde for, at operatørerne i videst muligt omfang skal opretholde udbuddet af deres væsentlige tjenester i beredskabssituationer og i andre ekstraordinære situationer med henblik på at sikre samfundets internettrafik.

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

Kapitel 3

Underretningspligt

§ 6. Operatører af væsentlige tjenester skal underrette Erhvervsstyrelsen og Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de tjenester, som fremgår af bilag 1, jf. § 7.

§ 7. En hændelse anses for at have væsentlige konsekvenser for kontinuiteten af de tjenester, der fremgår af bilag 1, hvis hændelsen medfører,

1) at domænenavneservertjenesten har en oppetid på mindre end 100% eller

2) at en rekursiv server i DNS-tjenesten ikke har været tilgængelig i over 6 timer eller i over 2.000.000 brugertimer, idet udtrykket "brugertime" henviser til antallet af berørte brugere i en periode på 60 minutter eller

3) at en autoritativ navneserve i DNS-tjenesten ikke har været tilgængelig i over 6 timer eller,

4) tab integritet, autenticitet eller fortrolighed i forbindelse med lagrede, overførte eller behandlede data i forbindelse med domænenavneservertjenesten eller DNS-tjenesten, som berører mere end 10.000 brugere

§ 8. Underretning i medfør af § 6 skal ske hurtigst muligt efter, at operatøren har konstateret, at hændelsen har fået væsentlige konsekvenser for kontinuiteten af de tjenester, som fremgår af bilag 1, jf. § 7.

Stk. 2. Underretningen af hændelser skal ske gennem den fælles digitale løsning for indberetning af hændelser til offentlige myndigheder på www.virk.dk, jf. dog stk. 3.

Stk. 3. Såfremt alle oplysninger til brug for underretningen ikke er tilgængelige for operatøren på tidspunktet, hvor underretning foretages, jf. stk. 1, afgiver operatøren en delvis underretning med de tilgængelige oplysninger. En delvis underretning skal snarest muligt følges op af en komplet underretning.

Kapitel 4

Straffebestemmelser og ikrafttrædelse

§ 9. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde den, der overtræder §§ 2-6 og § 8.

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

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

Erhvervsministeriet, den XX. maj 2018
XX XXXXX

/XX

Bilag 1

Liste over væsentlige tjenester på TLD- og DNS-området udarbejdet i medfør af § 3, stk. 2 i lov om net- og informationssikkerhed for domænenavssystemer og visse digitale tjenester.

1. Væsentlig tjenester på TLD-området

Domænenavneservertjenesten: Den tjeneste, som en topdomænenavneadministrator har, og som leverer information om alle andenordens internetdomænenavne, der er registreret under topdomænenavnet, herunder den tilhørende database med registrerede domænenavne og tilhørende henvisninger til autoritative navneservere og DNSSEC-nøgler.

2. Væsentlig tjenester på DNS-området

DNS-tjeneste: Den tjeneste, som en DNS-tjenesteudbyder leverer på internettet, og som muliggør, at et internetdomænenavn konverteres til en IP-adresse, herunder rekursive og autoritative navneservere.

Rekursiv navneserver: En server, der er ansvarlig for at levere den IP-adresse, som er knyttet til et domænenavn til en bruger eller et system, ved enten selv at have oplysninger om IP-adressen (cache svar) eller ved at indhente IP-adressen gennem rekursiv proces i det hierarkiske autoritative domænenavnssystem.

Autoritativ navneserver: En server, som har den autoritative oplysning, om sammenknytningen mellem en IP-adresse og et domænenavn.

DNSSEC (DNS Security Extensions): Et sæt af faciliteter, som tilføjer et ekstra niveau af sikkerhed til domænenavnssystemet.