UDKAST

Bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter

I medfør af § 3, stk. 1, § 4 og § 9, stk. 2, i lov nr. xxx af xx. xx 20xx om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v. fastsættes:

Kapitel 1

Definition og anvendelsesområde

§ 1. Ved vurderingen af, om en operatør af et internetudvekslingspunkt kan anses for en væsentlig operatør, jf. § 2, nr. 5, i lov om sikkerhed i net- og informationssystemer, vil der blive lagt vægt på, om operatøren driver et internetudvekslingspunkt, der håndterer en gennemsnitlig daglig datamængde på mere end 200 gigabit pr. sekund.

§ 2. Reglerne i denne bekendtgørelse finder ikke anvendelse på operatører af væsentlige internetudvekslingspunkter, der er omfattet af lov om net- og informationssikkerhed, jf. herved § 1 i lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter mv.

Kapitel 2

Krav til sikkerheden i net- og informationssystemer

§ 3. Operatører af væsentlige internetudvekslingspunkter skal gennemføre en risikovurdering, der skal tage stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i de tjenester, der udbydes.

Stk. 2. Såfremt operatørens 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 tjenester samt sikre, at tredjepart opretholder en tilsvarende sikkerhed i forhold til driftsleverancer til operatørerne 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.

§ 4. Operatører af væsentlige internetudvekslingspunkter skal udarbejde og gennemføre en ledelsesgodkendt net- og informationssikkerhedspolitik med udgangspunkt i en anerkendt international standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende. Informationssikkerhedspolitikken skal herunder beskrive de processuelle og organisatoriske rammer for arbejdet med informationssikkerheden 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 informationssikkerhedspolitikken er kommunikeret til alle relevante medarbejdere.

Stk. 3. Operatørerne skal løbende tilpasse informationssikkerhedspolitikken, 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 informationssikkerhedspolitikken.

§ 5. Operatører af væsentlige internetudvekslingspunkter skal på baggrund af informationssikkerhedspolitikken efter § 4 sikre, at der er etableret en informationssikkerhedsorganisation. Varetagelsen af relevante sikkerhedsopgaver, herunder roller og ansvar, skal i den forbindelse være beskrevet og i fornødent omfang være kommunikeret til operatørernes medarbejdere.

§ 6. Operatører af væsentlige internetudvekslingspunkter skal foretage risikostyring 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 risikovurdering og håndtering af informationssikkerhedsrisici. 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

§ 7. Operatører af væsentlige internetudvekslingspunkter skal underrette Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som operatørerne leverer, jf. § 8.

§ 8. En hændelse har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som en operatør af et væsentligt internetudvekslingspunkt leverer, når hændelsen i den væsentlige tjeneste medfører

1) nedgang i operatørens kapacitet i forhold til at håndtere data på mindst 50 procent i mindst en time, eller
2) tab af autenticitet, integritet eller fortrolighed.

§ 9. Underretning i medfør af § 7 skal ske hurtigst muligt og senest inden udgangen af den førstkommende hverdag efter, at operatøren har konstateret, at hændelsen har fået væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som operatøren leverer, jf. § 8.

Stk. 2. Underretningen skal være skriftlig og indeholde de i bilag 1 angivne oplysninger, jf. dog stk. 3.

Stk. 3. Såfremt de i bilag 1 angivne oplysninger ikke alle er tilgængelige for operatøren på tidspunktet, hvor underretning skal 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 indeholdende alle de i bilag 1 angivne oplysninger.

Kapitel 4

Straffebestemmelser og ikrafttrædelse

§ 10. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde den, der overtræder §§ 3-7 og § 9.

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

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

Center for Cybersikkerhed, den XX. november 2017

THOMAS LUND-SØRENSEN

/Rasmus Krogh Pedersen

Skema til brug for underretning ved væsentlige hændelser, jf. § 9, stk. 2

1. Virksomhed og kontaktoplysninger vedrørende denne underretning:
2. Tidspunkt for og varighed af hændelsen: *(Hvis hændelsen ikke er afsluttet, angives dette)*
3. Beskrivelse af hændelsen: *(Herunder information om årsagen til hændelsen samt information om eventuelle sårbarheder, der måtte have medvirket til at udløse hændelsen)*
4. Beskrivelse af konsekvenserne af hændelsen: *(Hvis der er tale om nedgang i kapacitet, anføres den samlede nedgang. Hvis der er tale om brud på autenticitet, integritet eller fortrolighed, anføres omfanget heraf.)*
5. Vurderes hændelsen at have væsentlige konsekvenser for tjenester i andre EU- eller EØS-lande?:
6. Hvilke tiltag er blevet iværksat?:
7. Er de berørte tjenester blevet retableret? Hvis nej, hvornår forventes dette at ske?:
8. Er de berørte brugere (evt. andre) blevet informeret og hvordan? :
9. Andre oplysninger af betydning: *(Der kan evt. oplyses yderligere om hændelsens konsekvenser, herunder om hændelsen berører samfundsvigtige funktioner m.m.)*
10. Udfærdiget af og udfærdigelsestidspunkt:

Underretningen sendes til cert@cert.cfcs.dk. Såfremt underretningen indeholder sensitive oplysninger, kan der ved henvendelse til Center for Cybersikkerhed træffes nærmere aftale om fremsendelse af underretningen.