FOLKETINGSTIDENDE C

FOLKETINGET

Vedtaget af Folketinget ved 3. behandling den 3. maj 2018

Forslag

til

Lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.[1)]

Kapitel 1

Anvendelsesområde og definitioner

§ 1. Loven finder ikke anvendelse på operatører af væsentlige internetudvekslingspunkter, der er omfattet af lov om net- og informationssikkerhed.

§ 2. I denne lov forstås ved:

1) Internetudvekslingspunkt: En netfacilitet, der muliggør sammenkobling af mere end to uafhængige autonome systemer, hovedsagelig med henblik på at lette udvekslingen af internettrafik.
2) Net- og informationssystem:
   a) Et elektronisk kommunikationsnet i form af radiofrekvens- eller kabelbaseret teleinfrastruktur, der anvendes til formidling af tjenester,
   b) enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller
   c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.
3) Sikkerhed i net- og informationssystemer: Evnen for net- og informationssystemer til på et givet sikkerhedsniveau at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.
4) Hændelse: Enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer.
5) Operatør af væsentligt internetudvekslingspunkt: En enhed, der leverer tjenester i form af internetudvekslingspunkter, hvor
   a) tjenesten er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter,
   b) leveringen af denne tjeneste afhænger af net- og informationssystemer og
   c) en hændelse ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste.
6) Digital tjeneste: Enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager og er af typen onlinemarkedsplads, onlinesøgemaskine eller cloud computing-tjeneste.
7) Udbyder af digital tjeneste: Enhver juridisk person, som udbyder en digital tjeneste, og som har hovedsæde eller en repræsentant i Danmark.
8) Nationalt centralt kontaktpunkt: En national kompetent enhed med ansvar for at koordinere spørgsmål vedrørende sikkerheden i net- og informationssystemer samt grænseoverskridende samarbejde i EU herom.
9) CSIRT: En national it-beredskabsenhed, der håndterer hændelser, og som har ansvar for at sikre samarbejdet om sikkerheden i net- og informationssystemer i EU.
10) CSIRT-netværket: Et netværk bestående af repræsentanter fra EU-medlemsstaternes CSIRT'er, som har ansvar for at sikre samarbejdet om sikkerheden i net- og informationssystemer i EU.

[1)] Loven indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, EU-Tidende 2016, nr. L 194, side 1.

Kapitel 2

Sikkerhed i net- og informationssystemer

§ 3. Center for Cybersikkerhed fastsætter regler om minimumskrav til sikkerheden i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter. Reglerne kan omfatte krav om passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som operatører af væsentlige internetudvekslingspunkter anvender til deres aktiviteter. Reglerne kan endvidere omfatte krav om passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i net- og informationssystemer, som operatører af væsentlige internetudvekslingspunkter anvender til levering af væsentlige tjenester, med henblik på at sikre kontinuiteten i disse tjenester. Der kan fastsættes krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Stk. 2. Center for Cybersikkerhed kan påbyde operatører af væsentlige internetudvekslingspunkter at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net- og informationssystemer i deres processer efter stk. 1.

Stk. 3. Center for Cybersikkerhed kan påbyde operatører af væsentlige internetudvekslingspunkter at afhjælpe nærmere påviste mangler i relation til sikkerheden i deres net- og informationssystemer.

§ 4. Center for Cybersikkerhed fastsætter regler om, at operatører af væsentlige internetudvekslingspunkter hurtigst muligt skal underrette Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som operatørerne leverer. Center for Cybersikkerhed kan i den forbindelse fastsætte krav om, hvordan og i hvilken form oplysningerne skal afgives.

Kapitel 3

Tilsyn, orientering, underretning og kommunikation

§ 5. Center for Cybersikkerhed fører tilsyn med overholdelsen af denne lov og regler, der er udstedt i medfør af loven.

Stk. 2. Center for Cybersikkerhed kan som led i sit tilsyn kræve, at operatører af væsentlige internetudvekslingspunkter fremlægger oplysninger og materiale, der er nødvendigt for centerets tilsynsvirksomhed, herunder til afgørelse af, om et forhold er omfattet af denne lov eller regler, der er udstedt i medfør af loven.

Stk. 3. Center for Cybersikkerhed kan stille krav om, hvordan og i hvilken form oplysninger og materiale efter stk. 2 skal afgives.

§ 6. Center for Cybersikkerhed kan orientere offentligheden om en hændelse, som centeret har modtaget underretning om efter § 4, hvis offentlighedens kendskab til hændelsen er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse. Forud for orientering af offentligheden hører Center for Cybersikkerhed den operatør af et væsentligt internetudvekslingspunkt, der har underrettet om hændelsen.

Stk. 2. Center for Cybersikkerhed kan i koordination med de relevante tilsynsmyndigheder i andre sektorer og efter forudgående høring af de operatører af væsentlige tjenester, der har underrettet om en hændelse, orientere offentligheden om hændelser, der berører flere samfundsvigtige sektorer, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Stk. 3. Center for Cybersikkerhed kan i koordination med de relevante tilsynsmyndigheder i andre sektorer og efter forudgående høring af de udbydere af digitale tjenester, der har underrettet om en hændelse, orientere offentligheden om hændelser, der berører flere samfundsvigtige sektorer, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse, eller hvis offentliggørelse af hændelsen i øvrigt er i offentlighedens interesse.

Stk. 4. Center for Cybersikkerheds orientering af offentligheden efter stk. 1-3 må ikke indeholde

1) oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el.lign., for så vidt det er af væsentlig betydning for den operatør af væsentlige tjenester eller udbyder af digitale tjenester, som oplysningerne angår,
2) oplysninger, der er af væsentlig betydning for statens sikkerhed eller rigets forsvar,
3) klassificerede informationer eller
4) oplysninger om enkeltpersoners forhold.

§ 7. Center for Cybersikkerhed kan i forbindelse med modtagelse af underretninger om hændelser af grænseoverskridende karakter fra tilsynsmyndigheder i andre sektorer, operatører af tjenester og udbydere af digitale tjenester videregive oplysninger om disse hændelser til nationale tilsynsmyndigheder, CSIRT'er og nationale centrale kontaktpunkter i andre EU-medlemsstater samt CSIRT-netværket.

Stk. 2. Center for Cybersikkerhed orienterer de operatører af tjenester samt udbydere af digitale tjenester, som underretningerne hidrører fra, om videregivelse efter stk. 1.

§ 8. Center for Cybersikkerhed kan fastsætte regler om, at skriftlig kommunikation til og fra centeret om nærmere bestemte forhold, som er omfattet af denne lov eller af regler udstedt i medfør af loven, skal foregå digitalt.

Stk. 2. Center for Cybersikkerhed kan fastsætte regler om digital kommunikation, herunder om anvendelsen af bestemte it-systemer og særlige digitale formater samt digital signatur el.lign.

Stk. 3. En digital meddelelse anses for at være kommet frem, når den er tilgængelig for adressaten for meddelelsen.

Kapitel 4

Straf

§ 9. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde den, der

1) undlader at efterkomme Center for Cybersikkerheds påbud efter § 3, stk. 2 og 3, eller
2) undlader at efterkomme Center for Cybersikkerheds krav efter § 5, stk. 2.

Stk. 2. I regler, der udstedes i medfør af § 3, stk. 1, og § 4, kan der fastsættes straf af bøde.

Stk. 3. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Kapitel 5

Ikrafttræden m.v.

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

§ 11. Loven gælder ikke for Færøerne og Grønland.

Folketinget, den 3. maj 2018

PIA KJÆRSGAARD

/ Erling Bonnesen