Forslag

til

Lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester og ændring af lov om finansiel virksomhed m.v.[1]

(Implementering af NIS-direktivet på Erhvervsministeriets område)

Kapitel 1

Formål, anvendelsesområde og definitioner

§ 1. Lovens formål er at fremme sikkerheden i net- og informationssystemer på det digitale område.

§ 2. Loven finder anvendelse på operatører af væsentlige tjenester inden for digital infrastruktur og udbydere af digitale tjenester, jf. dog stk. 2.

Stk. 2. Loven finder ikke anvendelse på udbydere af digitale tjenester i form af mikrovirksomheder eller små virksomheder.

§ 3. I denne lov forstås ved:

1) 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.
   c) Digitale data, som lagres, behandles, fremfindes eller overføres ved brug af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.
2) Sikkerhed i net- og informationssystemer: Net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede, overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.
3) Operatør af væsentlige tjenester: En offentlig eller privat enhed etableret i Danmark, der leverer en DNS-tjeneste eller er administrator af et topdomænenavn, og som opfylder kriterierne fastsat i § 4.
4) Digital tjeneste: Enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager af følgende type: Onlinemarkedsplads, onlinesøgemaskine eller cloud computing-tjeneste.
5) Udbyder af digitale tjenester: Enhver juridisk person, som udbyder en digital tjeneste, og som har hovedsæde eller en repræsentant i Danmark.
6) Hændelse: Enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer.

---

[1] Loven indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 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 1-30.

7) Risiko: Enhver rimelig identificerbar omstændighed eller begivenhed, der har en potentiel negativ indvirkning på sikkerheden i net- og informationssystemer.
8) Repræsentant: Enhver fysisk eller juridisk person, der er etableret i EU, og som udtrykkeligt er udpeget til at handle på vegne af en udbyder af digitale tjenester, som ikke er etableret i EU.
9) Domænenavnesystem (DNS)«: et hierarkisk opbygget navnesystem i et net, som behandler forespørgsler vedrørende domænenavne.
10) DNS-tjenesteudbyder: En enhed, som leverer DNS-tjenester på internettet.
11) Topdomænenavneadministrator: En enhed, som administrerer og driver registreringen af internetdomænenavne under et særligt topdomæne (TLD).
12) Onlinemarkedsplads: En digital tjeneste, som giver forbrugere og/eller erhvervsdrivende mulighed for at indgå aftaler om køb eller tjenester online med erhvervsdrivende enten på onlinemarkedspladsens websted eller på et websted tilhørende en erhvervsdrivende, som anvender computing-tjenester, der udbydes af onlinemarkedspladsen.
13) Onlinesøgemaskine: En digital tjeneste, som giver brugerne mulighed for at foretage søgninger på alle websteder eller websteder på et bestemt sprog på grundlag af en forespørgsel om et ethvert emne ved hjælp af et søgeord, en sætning eller andet input, og som fremviser links, hvor de kan findes oplysninger om det ønskede indhold.
14) Cloud computing-tjeneste: En digital tjeneste, som giver adgang til en skalerbar og elastisk pulje af delbare IT-ressourcer.

Kapitel 2

Operatører af væsentlige tjenester

§ 4. En enhed, der er omfattet af definitionen i § 3, nr. 3, skal i henhold til denne lov betragtes som en operatør af en væsentlig tjeneste, hvis
1) enheden leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter,
2) leveringen af denne tjeneste afhænger af net- og informationssystemer, og
3) en hændelse vil få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste.

Stk. 2. Erhvervsministeren fastsætter nærmere regler for afgrænsningen efter stk. 1, herunder udarbejder og opdaterer en liste over væsentlige tjenester.

§ 5. Operatører af væsentlige tjenester træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som de anvender til deres aktiviteter. Under hensyntagen til teknologiens aktuelle stade skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står i forhold til risikoen.

Stk. 2. Operatører af væsentlige tjenester træffer passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i net- og informationssystemer, som anvendes til levering af sådanne væsentlige tjenester, med henblik på at sikre kontinuiteten i disse tjenester.

Stk. 3. Erhvervsministeren kan fastsætte nærmere regler om sikkerhedsforanstaltninger efter stk. 1 og 2.

§ 6. Operatører af væsentlige tjenester skal hurtigst muligt underrette Erhvervsstyrelsen om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Underretningen skal indeholde oplysninger, der gør det muligt for Erhvervsstyrelsen at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen.

Stk. 2. Med henblik på at fastlægge omfanget af en hændelses konsekvenser efter stk. 1, skal operatøren navnlig tage følgende kriterier i betragtning:

1) Antallet af brugere, der berøres af afbrydelsen af den væsentlige tjeneste.
2) Hændelsens varighed.
3) Den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen.

Stk. 3. Hvis en operatørs levering af en væsentlig tjeneste er afhængig af en tredjepartsudbyder af digitale tjenester, skal operatøren underrette Erhvervsstyrelsen om alle de væsentlige konsekvenser for den væsentlige tjenestes kontinuitet, som følger af en hændelse hos den pågældende udbyder.

Stk. 4. Erhvervsministeren kan fastsætte nærmere regler om underretning efter stk. 1 og 3, og om væsentlige konsekvenser for kontinuiteten i de væsentlige tjenester efter stk. 2.

§ 7*.* Erhvervsstyrelsen kan viderebringe oplysninger til Center for Cybersikkerhed om hændelser, der er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver, i dets egenskab af nationalt kontaktpunkt.

Stk. 2. Hvis omstændighederne tillader det, leverer Erhvervsstyrelsen relevante oplysninger til den underrettende operatør af væsentlige tjenester om opfølgningen på underretningen, herunder oplysninger der kan støtte en effektiv håndtering af hændelsen.

Stk. 3. Center for Cybersikkerhed eller Erhvervsstyrelsen kan efter høring af den underrettende operatør af væsentlige tjenester oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Kapitel 3

Udbydere af digitale tjenester

§ 8. En udbyder af en digital tjeneste, der ikke har hovedsæde i EU, men som tilbyder sin tjeneste i Danmark, skal udpege en repræsentant i Danmark eller i et andet EU-land, hvor tjenesten tilbydes.

§ 9. Udbydere af digitale tjenester skal identificere og træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene i forhold til sikkerheden i de net- og informationssystemer, som de anvender i forbindelse med den digitale tjeneste. Under hensyntagen til teknologiens aktuelle stade skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står i forhold til risikoen, under hensyntagen til følgende elementer:

1) Sikkerheden i systemer og faciliteter.
2) Håndtering af hændelser.
3) Styring af driftskontinuitet.
4) Monitorering, audit og testning.
5) Overholdelse af internationale standarder.

Stk. 2. Udbydere af digitale tjenester skal træffe foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i deres net- og informationssystemer for at sikre kontinuiteten i disse tjenester.

Stk. 3. Erhvervsstyrelsen kan fastsætte nærmere regler om sikkerhedsforanstaltninger efter stk. 1 og 2.

§ 10. Udbydere af digitale tjenester skal hurtigst muligt underrette Erhvervsstyrelsen om enhver hændelse, der har betydelige konsekvenser for leveringen af deres tjeneste. Underretningen skal indeholde oplysninger, der gør det muligt for Erhvervsstyrelsen at vurdere de eventuelle grænseoverskridende konsekvenser ved hændelsen, jf. dog stk. 3.

Stk. 2. Med henblik på at fastlægge, om en hændelses konsekvenser er væsentlige, skal udbyderen navnlig tage følgende kriterier i betragtning:

1) Antallet af brugere, der berøres af hændelsen, navnlig brugere, som er afhængige af tjenesten med henblik på levering af deres egne tjenester.
2) Hændelsens varighed.
3) Den geografiske udbredelse med hensyn til det område, der er berørt af hændelsen.
4) Omfanget af afbrydelsen af tjenestens funktion.
5) Omfanget af konsekvenserne for økonomiske og samfundsmæssige aktiviteter.

Stk. 3. Underretning efter stk. 1 skal kun ske, i det omfang udbyderen af digitale tjenester kan skaffe sig adgang til relevante oplysninger, herunder oplysninger omfattet af stk. 2, nr. 1-5.

Stk. 4. Erhvervsstyrelsen kan fastsætte nærmere regler om underretning efter stk. 1 og 3, og væsentlige konsekvenser efter stk. 2.

§ 11. Erhvervsstyrelsen kan videregive oplysninger til Center for Cybersikkerhed om hændelser, der er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver, i dets egenskab af nationalt kontaktpunkt.

Stk. 2. Center for Cybersikkerhed eller Erhvervsstyrelsen kan efter høring af udbyderen af digitale tjenester oplyse offentligheden om konkrete hændelser eller kræve, at udbyderen af digitale tjenester gør det, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse, eller hvis offentliggørelse i øvrigt er i offentlighedens interesse.

Kapitel 4

Tilsyn

§ 12. Erhvervsstyrelsen fører tilsyn med overholdelsen af denne lov og de regler, der er udstedt i medfør af loven.

Stk. 2. Erhvervsstyrelsen kan kræve, at operatører og udbydere afgiver de oplysninger, der er nødvendige for styrelsens tilsyn efter denne lov.

Stk. 3. Erhvervsstyrelsen kan som led i sit tilsyn med operatører af væsentlige tjenester kræve dokumentation af operatørerne for den faktiske gennemførelse af sikkerhedspolitikker.

Stk. 4. Erhvervsstyrelsen kan som led i sit tilsyn udstede påbud til operatører af væsentlige tjenester og udbydere af digitale tjenester om at afhjælpe mangler i opfyldelsen af de krav, der fremgår af henholdsvis §§ 4- 6 og §§ 8 - 10.

§ 13. Erhvervsstyrelsen offentliggør på sin hjemmeside afgørelser efter § 12. Stk. 4. Afgørelser vedrørende fysiske personer offentliggøres i anonymiseret form.

Stk. 2. Afgørelser vedrørende en juridisk person offentliggøres med oplysning om identiteten på den juridiske person, medmindre offentliggørelsen af identiteten vil være til skade for en igangværende strafferetlig efterforskning eller offentliggørelsen vil forvolde uforholdsmæssig stor skade.

Stk. 3. Anonymisering af identiteten på en juridisk person sker efter 2 år regnet fra og med datoen for offentliggørelse.

§ 14. Erhvervsstyrelsens afgørelser efter § 12, stk. 2 - 4 og § 13, stk. 1, kan ikke indbringes for anden administrativ myndighed.

Kapitel 5

Kommunikation

§ 15. Erhvervsstyrelsen kan fastsætte regler om, at skriftlig kommunikation til og fra styrelsen om forhold, som er omfattet af denne lov eller af regler udstedt i medfør af denne lov, skal foregå digitalt.

Stk. 2. Erhvervsstyrelsen kan fastsætte nærmere regler om digital kommunikation, herunder om anvendelse af bestemte it-systemer, særlige digitale formater og digital signatur el.lign.

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

§ 16. Erhvervsstyrelsen kan fastsætte regler om, at styrelsen kan udstede afgørelser og andre dokumenter efter denne lov eller efter regler udstedt i medfør af denne lov uden underskrift, med maskinelt eller på tilsvarende måde gengivet underskrift eller under anvendelse af en teknik, der sikrer entydig identifikation af den, som har udstedt afgørelsen eller dokumentet. Sådanne afgørelser og dokumenter sidestilles med afgørelser og dokumenter med personlig underskrift.

Stk. 2. Erhvervsstyrelsen kan fastsætte regler om, at afgørelser og andre dokumenter, der udelukkende er truffet eller udstedt på grundlag af elektronisk databehandling, kan udstedes alene med angivelse af Erhvervsstyrelsen som afsender.

§ 17. Hvor det efter denne lov eller regler udstedt i medfør af denne lov er krævet, at et dokument, som er udstedt af andre end Erhvervsstyrelsen, skal være underskrevet, kan dette krav opfyldes ved anvendelse af en teknik, der sikrer entydig identifikation af den, som har udstedt dokumentet, jf. dog stk. 2. Sådanne dokumenter sidestilles med dokumenter med personlig underskrift.

Stk. 2. Erhvervsstyrelsen kan fastsætte nærmere regler om fravigelse af underskriftskrav. Det kan herunder bestemmes, at krav om personlig underskrift ikke kan fraviges for visse typer af dokumenter.

Kapitel 6

Straffebestemmelser

§ 18. Med bøde straffes, med mindre strengere straf er forskyldt efter den øvrige lovgivning, den der
1) undlader at efterkomme Erhvervsstyrelsens krav efter § 12, stk. 2 eller 3, eller som i forhold, der omfattes af loven, meddeler Erhvervsstyrelsen urigtige eller vildledende oplysninger, eller
2) undlader at efterkomme Erhvervsstyrelsens påbud efter § 12, stk. 4.

Stk. 2. I regler, som udfærdiges i medfør af § 4, stk. 2 § 5, stk. 3, § 6, stk. 4, § 9, stk. 3 eller § 10, stk. 4, kan der fastsættes straf i form af bøde for overtrædelse af bestemmelserne i reglerne.

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

Kapitel 7

Ikrafttræden m.v.

§ 19. Loven træder i kraft den 9. maj 2018.

Kapitel 8

Ændringer i anden lovgivning

§ 20. I lov om finansiel virksomhed jf. lovbekendtgørelse nr. 174 af 31. januar 2017, som senest ændret ved § 17 i lov nr. 688 af 8. juni 2017, § 82 i lov nr. 651 af 8. juni 2017 og § 157 i lov nr. 652 af 8. juni 2017, foretages følgende ændringer:

1. I *fodnoten* til lovens titel ændres »[xxx]« til: »dele af Europa-Parlamentets og Rådets direktiv 2013/50/EU af 22. oktober 2012, EU-Tidende 2013, nr. L 294, side 13, Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014, EU-Tidende 2014, nr. L 173, side 349, og dele af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148/EU af 6. juli 2016, EU-Tidende 2016, nr. L 194, side 1«

2. I *§ 71, stk. 2,* indsættes som nyt 2. pkt:
»Finanstilsynet kan derudover fastsætte nærmere regler om hændelsesrapportering ved eventuelle hændelser.«

3. Efter § 307 indsættes før Afsnit IX:

»Afsnit VIII a

Kapitel 18 a

Identifikation af operatører af væsentlige tjenester

§ 307 a. Finanstilsynet udpeger mindst hvert andet år de penge- og realkreditinstitutter, der er operatører af væsentlige tjenester, jf. stk. 2.

Stk. 2. Finanstilsynet skal i forbindelse med udpegningen efter stk. 1, lægge vægt på, at
1. tjenesten er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter,
2. leveringen af tjenesten afhænger af net- og informationssystemer, og

3. en hændelse kan få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Stk. 3. Finanstilsynet kan fastsætte nærmere regler om stk. 1 og 2.«

4. I *§ 354, stk. 6,* indsættes som nyt nr. 44:

»44) Center for Cybersikkerhed under forudsætning af at oplysningerne er nødvendige for dem til opfyldelse af deres lovbestemte opgaver, i deres egenskab af CSIRT.«

5. Efter § 354 g indsættes:

»§ 354 h. Finanstilsynet kan efter høring af den berørte virksomhed, orientere offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendig for at forebygge eller håndtere en igangværende hændelse.«

§ 21. I lov om kapitalmarkeder, jf. lov nr. 650 af 8. juni 2017 som ændret ved § x i lov nr. [X] af [X], foretages følgende ændringer:

1. I *fodnoten* til lovens titel ændres »dele af Europa-Parlamentets og Rådets direktiv 2013/50/EU af 22. oktober 2012, EU-Tidende 2013, nr. L 294, side 13, og Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014, EU-Tidende 2014, nr. L 173, side 349« til: »dele af Europa-Parlamentets og Rådets direktiv 2013/50/EU af 22. oktober 2012, EU-Tidende 2013, nr. L 294, side 13, Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014, EU-Tidende 2014, nr. L 173, side 349, og dele af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148/EU af 6. juli 2016, EU-Tidende 2016, nr. L 194, side 1«.

2. Efter § 58 indsættes før Afsnit V:

»Identifikation af operatører af væsentlige tjenester

§ 58 a. Finanstilsynet udpeger mindst hvert andet år de operatører af markedspladser og centrale modparter (CCP'er), der er operatører af væsentlige tjenester, jf. stk. 2.

Stk. 2. Finanstilsynet skal i forbindelse med udpegningen efter stk. 1, lægge vægt på, at

1. tjenesten er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter,
2. leveringen af tjenesten afhænger af net- og informationssystemer, og
3. en hændelse kan få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Stk. 3. Finanstilsynet kan fastsætte nærmere regler om stk. 1 og 2, herunder fastsætte nærmere regler om krav om underretning af Finanstilsynet ved en hændelse.«

3. I *§ 225, stk. 1,* indsættes efter nr. 16:

»**17)** Center for Cybersikkerhed under forudsætning af at oplysningerne er nødvendige for dem til opfyldelse af deres lovbestemte opgaver, i deres egenskab af CSIRT. «

4. Efter § 236 indsættes før overskriften før § 237:

»§ 236 a. Finanstilsynet kan efter høring af den berørte operatør af en markedsplads eller centrale modpart (CCP), orientere offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge eller håndtere en igangværende hændelse.«

§ 22. Loven gælder ikke for Færøerne og Grønland, jf. dog stk. 2.

Stk. 2. Loven kan ved kongelig anordning sættes helt eller delvist i kraft for Færøerne og Grønland med de ændringer, som de henholdsvis færøske og grønlandske forhold tilsiger.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning
2. Baggrunden for og formålet med lovforslaget
3. Lovforslagets hovedindhold
    3.1. Digitale tjenester
        3.1.1. Operatører af væsentlige tjenester
        3.1.2. Udbydere af digitale tjenester
        3.1.3. Tilsyn
    3.2. Det finansielle område
        3.2.1. Identificering af operatører af væsentlige tjenester
        3.2.2. Indberetningskrav for operatører af væsentlige tjenester
        3.2.3. Videregivelse af oplysninger
        3.2.4. Offentliggørelse af hændelser
4. Økonomiske og administrative konsekvenser for det offentlige
5. Økonomiske og administrative konsekvenser for erhvervslivet mv.
6. Administrative konsekvenser for borgere
7. Miljømæssige konsekvenser
9. Forholdet til EU-retten
10. Hørte myndigheder og organisationer m.v.
11. Sammenfattende skema

1. Indledning

IT-sikkerhedshændelser, såsom cyberangreb og nedbrud af IT-systemer, udgør en alvorlig trussel mod samfundet, der i stigende grad er afhængig af digitale systemer. Omfanget, hyppigheden og konsekvenserne af sådanne hændelser er tiltagende. Rådet og Europa-Parlamentet har på den baggrund vedtaget direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (herefter NIS-direktivet).

Lovforslaget implementerer NIS-direktivet på Erhvervsministeriets område. Lovforslaget implementerer for det første de elementer i direktivet, der vedrører informationssikkerhed for domænenavnssystemer og visse digitale tjenester. For det andet implementerer lovforslaget NIS-direktivet på det finansielle område. Implementeringsfristen i NIS-direktivet er den 9. maj 2018. Loven foreslås derfor at træde i kraft den 9. maj 2018.

Den øgede digitalisering af det danske samfund indebærer, at net- og informationssikkerhed spiller en stadigt mere afgørende rolle i samfundet. Det er i høj grad en forudsætning for de økonomiske og samfundsmæssige aktiviteter, at infrastrukturen for informations- og kommunikationsteknologi (IKT-infrastruktur) samt de digitale tjenester fungerer pålideligt og sikkert.

Erfaringerne viser, at omfanget, hyppigheden og konsekvenserne af hændelser er tiltagende og udgør en alvorlig trussel på det digitale område. Området er således i højere grad blevet et mål for forsætligt skadelige handlinger, som har til formål at ødelægge eller forstyrre driften af digitale systemer. Uanset om hændelserne er tilsigtede eller ej kan forstyrrelser på det digitale område have alvorlige konsekvenser. En hændelse kan fx være et cyberangreb eller oversvømmelse af en operatørs eller udbyders serverrum, således at de digitale tjenester mv. ikke fungerer. Hændelser kan fx hindre gennemførelsen af økonomiske aktiviteter, medføre betydelige finansielle tab og underminere brugernes tillid. Forhold der alle kan medvirke til at skabe skade på samfundsøkonomien.

På teleområdet er net- og informationssikkerhed reguleret gennem lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed med tilhørende bekendtgørelse. Derudover er andre dele af IKT-infrastrukturen samt digitale tjenester – bortset fra topdomænet ".dk" – ikke underlagt regulering på net- og informationssikkerhedsområdet. Der kan derfor være en risiko for, at andre dele af IKT-infrastrukturen samt digitale tjenester ikke på samme måde som i telesektoren er tilstrækkeligt beskyttet mod hændelser.

Lovforslaget har derfor til formål at sikre, at også andre aktører på det digitale område foretager de nødvendige organisatoriske og sikkerhedsmæssige foranstaltninger, der kan imødegå den stigende trussel på området.

Med dette lovforslag indføres der krav til operatører af væsentlige tjenester inden for digital infrastruktur og udbydere af digitale tjenester, der i højere grad tager højde for samfundets afhængighed af sådanne tjenester og afspejler det aktuelle trusselsbillede. Det er samtidig vigtigt for Erhvervsministeriet, at operatørerne eller udbyderne på området kun bliver underlagt proportionale krav, der ikke er unødvendigt byrdefulde, og at operatørerne eller udbyderne i videst muligt omfang baseret, på det aktuelle trusselsbillede, overlades et skøn til selv at beslutte indholdet af deres sikkerhedsstrategier.

For så vidt angår det finansielle område stilles der allerede i dag krav til it-sikkerhed område i overensstemmelse med NIS-direktivets formål. Med lovforslaget foreslås derfor mindre lovændringer af lov om finansiel virksomhed og lov om kapitalmarkeder, med henblik på at sikre en direktivnær implementering af NIS-direktivet på Erhvervsministeriets område for så vidt angår pengeinstitutter, realkreditinstitutter, operatører af markedspladser og centrale modparter (CCP'er).

2. Lovforslagets formål og baggrund

Formålet med lovforslaget er dels at sikre et højt niveau for net- og informationssikkerhed inden for digital infrastruktur og for digitale tjenester med henblik på at skabe endnu mere robuste digitale systemer.

Med lovforslaget foreslås der indført sikkerhedskrav for operatører af væsentlige tjenester inden for digital infrastruktur og udbydere af visse digitale tjenester. Operatører af væsentlige tjenester omfatter i dette lovforslag operatører af domænenavne- og topdomænenavnesystemer. Operatører af domænenavnesystemer medvirker til, at et internetopkald rutes rigtig ved at oversætte et domænenavn til en internetadresse (talkode), som internetnettet forstår. Operatører af topdomænenavne registrerer domænenavne under et topdomænenavn (fx .dk, .com eller .sport). Udbydere af digitale tjenester omfatter onlinemarkedspladser, onlinesøgemaskiner og cloud

computing-tjenester. Lovforslagets bestemmelser gælder ikke for udbydere af digitale tjenester, som er mikrovirksomheder og små virksomheder.

Sikkerhedskravene omfatter overordnet en forpligtelse til at indføre risikostyringsforanstaltninger, der kan sikre et højt sikkerhedsniveau i de pågældende tjenester. Operatørerne og udbyderne skal træffe passende sikkerhedsforanstaltninger på baggrund af en vurdering af de risici virksomheden konkret står over for. Endvidere foreslås der indført et krav om, at de omfattede operatører og udbydere skal underrette myndighederne om eventuelle hændelser, der har forstyrrende virkning på levering af de pågældende tjenester. Som led i Erhvervsstyrelsens tilsyn vil styrelsen af egen drift rette henvendelse til operatører af væsentlige tjenester med henblik på kontrol af operatørernes efterlevelse af loven. Udbyderne af digitale tjenester vil derimod i overensstemmelse med NIS-direktivet være underlagt et reaktivt myndighedstilsyn baseret på dokumenteret manglende overholdelse af lovgivningens krav fra fx. brugere og andre myndigheder, herunder myndigheder i andre lande.

For så vidt angår det finansielle område, har lovforslaget til formål at sikre et højt niveau for net- og informationssikkerhed for så vidt angår de pengeinstitutter, realkreditinstitutter, operatører af markeder og centrale modparter (CCP'er), der karakteriseres som operatører af væsentlige tjenester, med henblik på at opnå en direktivnær implementering af NIS-direktivet.

3. Lovforslagets hovedindhold

3.1. Det digitale område

3.1.1. Operatører af væsentlige tjenester

3.1.1.1 Gældende ret

Operatører af væsentlige tjenester er på nuværende tidspunkt ikke underlagt en samlet regulering i forhold til net- og informationssikkerhed.

Administratorer af topdomænenavne, der særligt er tildelt Danmark eller på anden vis tilknyttet Danmark er i dag omfattet af lov om internetdomæner (Lov nr. 164 af 26. februar 2014). I lovens §§ 19-22 er der fastsat bestemmelser om sikker og stabil drift af internetdomæner, som gælder for tildelingen af topdomænenavnet ".dk". Der er endvidere i bekendtgørelse om internetdomænet ".dk" (Bekendgørelse nr. 1129 af 23. september 2015) i §§10-13 fastsat yderligere bestemmelser om sikkerheds- og tilgængelighedsforhold i den del af domænenavnssystemet, som er omfattet af ".dk". Bestemmelserne vedrører bl.a. krav til certificering efter sikkerhedsstandarder, krav til høj tilgængelighed til topdomænenavnet ".dk" og rapportering af nedbrud af domænenavnsservertjenesten. Det er Erhvervsstyrelsen, der fører tilsyn med overholdelsen af disse regler. Disse bestemmelser vil ikke blive ændret af dette lovforslag. Administratorer af topdomænenavnet ".dk" vil således fortsat skulle overholde bestemmelserne i lov om internetdomæner og de tilhørende bekendtgørelser. Det er dog forventningen, at der med implementeringen af NIS-direktivet skal etableres en fælles indberetningsløsning, som administrator af ".dk" også vil skulle bruge til at rapportere utilsigtet driftsstop og nedbrud af domænenavnsservertjenesten.

Andre topdomænenavne, der i dag er tildelt danske virksomheder, er derimod ikke omfattet af ovenstående regler om sikkerhedsniveauer mv, idet disse topdomænenavne ikke er tildelt efter lov om internetdomæner. Tildelingen er derimod sket direkte til virksomhederne af den almennyttige non-profit organisation Internet Corporation for Assigned Names and Numbers (ICANN), der er etableret i Californien. Der er her tale om generiske topdomænenavne, som ikke er landespecifikke, fx ".com", ".org" og ".sport".

Operatører af domænenavnesystemer, som medvirker til at dirigere internettrafikken, er dertil heller ikke underlagt regulering i forhold til net- og informationssikkerhed.

3.1.1.2. Erhvervsministeriets overvejelser

I henhold til NIS-direktivet skal hver EU-medlemsstat identificere operatører af væsentlige tjenester. Medlemsstaterne skal i forlængelse heraf udarbejde en liste over væsentlige tjenester inden for de omfattede sektorer, herunder digital infrastruktur. Listen over væsentlige tjenester skal opdateres regelmæssigt og samtidig bruges til at identificere operatører af væsentlige tjenester i det pågældende EU-land. I afgrænsningen af operatører vil derudover indgå om tjenesten er afhængig af net- og informationssystemer, og om en hændelse vil få væsentlig forstyrrende virkning for leveringen af den pågældende tjeneste.

NIS-direktivet fastsætter dertil, at medlemsstaterne skal sikre, at operatører af væsentlige tjenester træffer passende og forholdsmæssige foranstaltninger for at styre risiciene for sikkerheden i de net- og informationssystemer, de anvender som led i deres tjeneste. Foranstaltningerne skal både være af teknisk og organisatorisk karakter samt tage højde for det aktuelle teknologiske stadie med det formål at sikre et sikkerhedsniveau, der står mål med risikoen for hændelser. De pågældende virksomheder vil i forlængelse heraf skulle foretage en risikovurdering gennem hele livscyklussen for deres net- og informationssystemer, herunder i forhold til udarbejdelse af kravspecifikationer, udbud, konfigurering, drift og udfasning.

NIS-direktivet fastlægger desuden, at operatører af væsentlige tjenester, for at kunne opretholde kontinuiteten i deres tjenester, skal træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i de net- og informationssystemer, de anvender.

NIS-direktivet fastsætter derudover, at operatører af væsentlige tjenester hurtigst muligt skal foretage en underretning til myndighederne om hændelser, der har væsentlige konsekvenser for kontinuiteten af deres tjenester. Underretningen skal gøre myndighederne i stand til at vurdere, om der er behov for at underrette myndigheder i andre medlemsstater og offentligheden.

NIS-direktivet foreskriver endelig, at myndighederne i det land, hvor en hændelse indtræffer, skal orientere de relevante myndigheder i andre berørte medlemsstater om hændelser hos operatører af væsentlige tjenester, der har væsentlige konsekvenser for kontinuiteten i væsentlige tjenester i de pågældende medlemsstater. Orienteringen vil skulle ske under overholdelse af krav om fortrolighed og sikkerhed. Myndighederne kan endvidere efter høring af operatøren offentliggøre konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Kravene til operatører af væsentlige tjenester er i NIS-direktivet udtryk for minimumsharmonisering, og der vil være et nationalt spillerum for at fastsætte yderligere krav til

operatørerne. Erhvervsministeriet vurderer dog, at der ikke er grundlag for at gå længere end de krav, der følger af NIS-direktivet.

3.1.1.3. Den foreslåede ordning

Lovforslaget gennemfører NIS-direktivets bestemmelser for operatører af væsentlige tjenester inden for digital infrastruktur på Erhvervsministeriets område.

Det foreslås, at erhvervsministeren får bemyndigelse til at fastsætte de nærmere kriterier for identifikationen af operatører af væsentlige tjenester samt til at udarbejde og regelmæssigt at opdatere en liste over væsentlige tjenester.

Det foreslås endvidere, at der indføres sikkerhedskrav til operatører af væsentlige tjenester. Sikkerhedskravene vil indeholde de overordnede forpligtelser for operatører til at træffe risikostyringsforanstaltninger og underrette myndighederne i tilfælde af hændelser. Lovforslaget lægger sig op ad ordlyden i NIS-direktivets bestemmelser og fastlægger dermed ikke yderligere nationale krav.

Lovforslaget indeholder dertil en hjemmel til i bekendtgørelsesform at fastsætte de nærmere regler for operatørernes sikkerheds- og underretningsforpligtelser. Hjemlen skal bruges til nærmere at fastlægge forpligtelserne bl.a. efter de vejledninger, Kommissionen ventes at udstede på området. Dertil vil bemyndigelsen skulle anvendes til nærmere at fastsætte, hvordan operatørerne skal indberette hændelser. Det er i forbindelse med udmøntningen af bemyndigelsen centralt for Erhvervsministeriet, at operatørerne kun bliver underlagt proportionale krav, og i det omfang det er muligt overlades et skøn til selv at beslutte indholdet i deres sikkerhedsstrategier.

Endvidere foreslås det, at Erhvervsstyrelsen kan viderebringe oplysninger om hændelser til Center for Cybersikkerhed under forudsætning af, at oplysningerne er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver, i dets egenskab af nationalt kontaktpunkt i henhold til NIS-direktivet. Det nationale kontaktpunkt vil bl.a. i henhold til NIS-direktivet skulle orientere kontaktpunkter i andre medlemsstater om hændelser, der har væsentlige konsekvenser for kontinuiteten i de væsentlige tjenester, der udbydes i de pågældende lande. Det foreslås endelig, at Erhvervsstyrelsen eller Center for Cybersikkerhed får mulighed for, hvor det er relevant, og efter høring af den pågældende operatør, at orientere offentligheden om hændelser. Center for Cybersikkerhed vil stå for offentliggørelsen i de tilfælde, hvor hændelsen vedrører flere sektorer.

3.1.2. Udbydere af digitale tjenester

3.1.2.1. Gældende ret

Udbydere af digitale tjenester som defineret i NIS-direktivet er på nuværende tidspunkt ikke underlagt regulering i forhold til net- og informationssikkerhed.

3.1.2.2. Erhvervsministeriets overvejelser

NIS-direktivet fastlægger lignende krav for udbydere af digitale tjenester som for operatører af væsentlige tjenester. Udbydere af digitale tjenester skal ligeledes træffe risikostyringsforanstaltninger og foranstaltninger, der forebygger og minimerer konsekvensen af

eventuelle hændelser. Centralt for udbydernes opfyldelse af kravene vil også her være, at de pågældende virksomheder foretager en risikovurdering gennem hele livscyklussen for deres net- og informationssystemer. Mere specifikt følger det af NIS-direktivet, at de nævnte foranstaltninger skal adressere spørgsmål vedrørende sikkerhed i udbyderens systemer og faciliteter, håndtering af hændelser, styring af driftskontinuitet, monitorering, kontrol (audit) og testning samt overholdelse af internationale standarder. Disse elementer specificeres yderligere ved en gennemførelsesretsakt fra Kommissionen.

NIS-direktivet fastsætter ligeledes for udbydere af digitale tjenester en forpligtelse til hurtigst muligt at underrette myndighederne om enhver hændelse, der har betydelige konsekvenser for leveringen af deres tjeneste. I vurderingen af, om en hændelse har væsentlige konsekvenser, skal der udover antal brugere, varighed og geografisk udbredelse også inddrages omfanget af afbrydelsen af tjenestens funktion samt konsekvenserne for samfundsmæssige og økonomiske aktiviteter. Disse elementer specificeres nærmere ved en gennemførelsesretsakt fra Kommissionen.

Hvis det vurderes relevant, skal myndighederne i det land, hvor en hændelse indtræffer endvidere i henhold til NIS-direktivet orientere de relevante myndigheder i andre berørte medlemsstater om hændelser hos udbydere af digitale tjenester. Myndighederne vil dertil også efter høring af udbyderen kunne offentliggøre konkrete hændelser eller kræve, at udbyderen gør dette, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse, eller hvis offentliggørelse i øvrigt er i offentlighedens interesse. Medlemsstaterne vil i henhold til NIS-direktivet ikke kunne fastsætte yderligere sikkerhedskrav for udbydere, da NIS-direktivets bestemmelser er udtryk for totalharmonisering. Der vil dog kunne stilles yderligere krav under hensynstagen til rigets sikkerhed. Denne mulighed er dog ikke udnyttet i lovforslaget. Det følger endvidere af NIS-direktivets betragtninger, at der ikke skal stilles lige så høje sikkerhedskrav til udbydere af digitale tjenester som til operatører af væsentlige tjenester, hvilket skal ses i sammenhæng med, at hændelser i digitale tjenester ikke har lige så store konsekvenser for samfundet, som hændelser vil have inden for digital infrastruktur. I forlængelse heraf bør udbyderne overlades et større skøn til selv at fastlægge indholdet af deres informationssikkerhedsstrategier. De foranstaltninger udbyderne skal træffe skal endvidere være procesorienterede og risikobaserede og indebærer ikke en forpligtelse for udbyderne til at udforme deres IKT-produkter og -tjenester på en særlig måde.

3.1.2.3. Den foreslåede ordning

Lovforslaget gennemfører NIS-direktivets bestemmelser for udbydere af digitale tjenester på Erhvervsministeriets område.

Det foreslås, at der indføres sikkerhedskrav til udbydere af digitale tjenester.

Sikkerhedskravene vil indeholde de overordnede forpligtelser for udbydere til at træffe risikostyringsforanstaltninger og underrette myndighederne om hændelser. Lovforslaget vil lægge sig op ad ordlyden i NIS-direktivets bestemmelser, og fastlægger dermed ikke yderligere nationale krav. NIS-direktivets bestemmelser om udbydere er dertil som allerede nævnt udtryk for totalharmonisering, hvorfor det her ikke er muligt at fastlægge yderligere nationale krav.

Lovforslaget indeholder dertil en hjemmel til at fastsætte nærmere regler for udbydernes sikkerheds- og underretningsforpligtelser. Hjemlen vil skulle bruges til at gennemføre

Kommissionens gennemførelsesretsakter, der nærmere specificerer indholdet af de elementer, der indgår i sikkerhedskravene til udbyderne af digitale tjenester. Det er her centralt for Erhvervsministeriet, at udbyderne kun bliver underlagt proportionale krav, der ikke indeholder unødvendige administrative byrder, og at der i videst muligt omfang overlades et skøn til udbyderne til selv at beslutte indholdet af deres sikkerhedsstrategier. Dette er i overensstemmelse med de ovennævnte overvejelser, der også fremgår af NIS-direktivets betragtninger, bl.a. betragtning nr. 44.

Endvidere foreslås det, at Erhvervsstyrelsen kan viderebringe oplysninger om hændelser til Center for Cybersikkerhed under forudsætning af, at oplysningerne er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver, i dets egenskab af nationalt kontaktpunkt i henhold til NIS-direktivet. Det nationale kontaktpunkt vil bl.a. i henhold til NIS-direktivet skulle orientere kontaktpunkter i andre medlemsstater om hændelser, der har betydelige konsekvenser for leveringen af tjenester, der udbydes i de pågældende lande. Det foreslås endelig, at Erhvervsstyrelsen eller Center for Cybersikkerhed får mulighed for, hvor det er relevant, og efter høring af den pågældende udbyder, at orientere offentligheden om hændelser. Center for Cybersikkerhed vil stå for offentliggørelsen i de tilfælde, hvor hændelsen vedrører flere sektorer.

3.1.3. Tilsyn

3.1.3.1. Gældende ret

Operatører af væsentlige tjenester inden for digital infrastruktur og udbydere af digitale tjenester er på nuværende tidspunkt ikke underlagt en samlet regulering i forhold til net- og informationssikkerhed.

Administratorer af topdomænenavne, der særligt er tildelt Danmark eller på anden vis tilknyttet Danmark er i dag omfattet af lov om internetdomæner (Lov nr. 164 af 26. februar 2014). Erhvervsstyrelsen er tilsynsmyndighed i forhold til denne regulering og kan i henhold til lovens § 37 udstede påbud om overholdelse af bestemmelser og vilkår til de omfattede operatører. I henhold til § 41, stk. 2, kan Erhvervsstyrelsen kræve af de omfattede administratorer enhver oplysning og ethvert materiale, som styrelsen skønner relevant i forbindelse med administration af loven og tilsynet hermed. Styrelsen kan endvidere indhente oplysningerne hos operatøren med henblik på offentliggørelse af statistik over bl.a. det samlede antal registrerede domænenavne og antal klagesager, jf. § 41, stk. 3. Endelig kan Erhvervsstyrelsen efter § 45 pålægge de omfattede administratorer tvangsbøder og efter § 46 tilbagekalde tilladelser tildelt til administratorer. Som nævnt ovenfor under afsnit 3.1.1.1 vil lov om internetdomæner og tilhørende bekendtgørelser ikke blive ændret med dette lovforslag.

3.1.3.2. Erhvervsministeriets overvejelser

Lovforslaget gennemfører NIS-direktivets bestemmelser om offentliggørelse og tilsyn på Erhvervsministeriets område.

NIS-direktivet foreskriver, at medlemsstaterne skal sikre, at de kompetente myndigheder griber ind over for operatører og udbydere, der ikke opfylder deres forpligtelser. Myndighederne vil i forlængelse heraf skulle kunne pålægge operatørerne og udbyderne, at de forelægger de nødvendige

oplysninger til brug for myndighedernes tilsyn, og at operatørerne og udbyderne afhjælper eventuelle mangler. For udbydere af digitale tjenester følger det af NIS-direktivet, at der skal være tale om et reaktivt tilsyn, hvilket skal ses i sammenhæng med, at hændelser for udbydere af digitale tjenester ikke vil have samme samfundsmæssige konsekvenser som ved hændelser hos operatører af væsentlige tjenester.

3.1.3.3. Den foreslåede ordning

Det foreslås med lovforslaget, at Erhvervsstyrelsen skal føre tilsyn med overholdelsen af loven.

Erhvervsstyrelsen vil som led i sit tilsyn overordnet få adgang til at kræve oplysninger fra operatører af væsentlige tjenester og udbydere af digitale tjenester, der er nødvendige for at vurdere sikkerheden i deres net- og informationssystemer. Styrelsen vil endvidere få mulighed for at udstede påbud til operatører og udbydere om, at de fx skal afhjælpe mangler i deres efterlevelse af lovens bestemmelser.

Det foreslås derudover, at der i overensstemmelse med NIS-direktivets bestemmelser anlægges et mere aktivt tilsyn over for operatører af væsentlige tjenester end udbydere af digitale tjenester. Forskellen skal ses i sammenhæng med, at hændelser i digitale tjenester ikke har lige så store konsekvenser for samfundet, som hændelser vil have inden for digital infrastruktur. I forlængelse heraf foreslås, at Erhvervsstyrelsen som led i sit tilsyn med operatører får mulighed for at kræve dokumentation af operatører for den faktiske gennemførelse af sikkerhedspolitikker.

For udbydere af digitale tjenester vil tilsynet i overensstemmelse med NIS-direktivet være baseret på dokumenteret manglende overholdelse af lovgivningens krav fra fx. brugere og andre myndigheder, herunder myndigheder i andre lande.

Med lovforslaget indføres endelig, at Erhvervsstyrelsen efter høring af de pågældende operatører og udbydere har mulighed for at offentliggøre de afgørelser, som styrelsen træffer som led i sit tilsyn under hensyntagen til bl.a. persondatabeskyttelse og strafferetlig efterforskning.

3.2. Det finansielle område

3.2.1. Identificering af operatører af væsentlige tjenester

3.2.1.1. Gældende ret

I medfør af lov om finansiel virksomhed § 308 udpeger Finanstilsynet hvert år de systemisk vigtige finansielle institutter (SIFI) i Danmark. Et pengeinstitut, et realkreditinstitut og et fondsmæglerselskab I, hvis fondsmæglerselskabet I har tilladelse til at udøve de aktiviteter, der er nævnt i bilag 4, afsnit A, nr. 3 og 6, der er omfattet af Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber, udpeges som et systemisk vigtigt finansielt institut (SIFI), hvis det i 2 på hinanden følgende år, enten har en balance, der udgør mere end 6,5 pct. af Danmarks bruttonationalprodukt, eller hvis instituttets udlån i Danmark udgør mere end 5 pct. af de danske penge- og realkreditinstitutters samlede udlån i Danmark, eller hvis instituttets indlån i Danmark udgør mere end 5 pct. af de danske pengeinstitutters samlede indlån i Danmark.

3.2.1.2. NIS-direktivet

Det følger af direktivets artikel 5, stk. 1, at medlemsstaterne skal føre en liste over operatører af væsentlige tjenester, der er etableret for hver sektor og delsektor, som er omhandlet i direktivets bilag II. Denne identificering skal ajourføres mindst hvert andet år.

For så vidt angår den finansielle sektor omhandler direktivets bilag II sektorerne bankvæsen og finansielle markedsinfrastrukturer. Typen af enheder i disse sektorer er kreditinstitutter, markedspladsoperatører og centrale modparter (CCP), jf. NIS-direktivets bilag II.

Det følger endvidere af direktivets artikel 5, stk. 2, at ved identificering af operatører af væsentlige tjenester, skal der lægges vægt på følgende tre kriterier. Der skal være tale om en enhed, der leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter. Derudover skal leveringen af denne tjeneste afhænge af net- og informationssystemer. Som det sidste kriterie følger det af direktivet, at en hændelse ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste. Ved vurderingen af om en hændelse er væsentlig forstyrrende, vil der bl.a. skulle lægges vægt på det antal af brugere der påvirkes, samt de konsekvenser en hændelse kan have i omfang og varighed på økonomiske og samfundsmæssige aktiviteter m.v., jf. direktivets artikel 6, stk. 1.

Direktivet er et minimumsharmoniseringsdirektiv, og der vil dermed være et nationalt spillerum for at fastsætte yderligere krav til operatørerne af væsentlige tjenester.

3.2.1.3. Erhvervsministeriets overvejelser
Det følger af NIS-direktivets bilag II, at kreditinstitutter, markedspladsoperatører og centrale modparter (CCP'er), er omfattet af NIS-direktivet. Det følger endvidere af direktivets artikel 5, stk. 2, at medlemsstaterne mindst hvert andet år skal udpege de kreditinstitutter, markedspladsoperatører og centrale modparter (CCP'er), som kan identificeres som operatører af væsentlige tjenester.

Et kreditinstitut er en virksomhed, hvis aktivitet består i fra offentligheden at modtage indlån eller andre midler, som skal tilbagebetales, samt i at yde lån for egen regning, jf. lov om finansiel virksomhed § 5, stk. 1, nr. 2. Det vil sige penge- og realkreditinstitutter.

Finanstilsynet udpeger i dag efter § 308 de pengeinstitutter, realkreditinstitutter og fondsmæglerselskaber, som er systemisk vigtige (SIFI).

For så vidt angår identificering af væsentlige tjenester på det finansielle område, fremgår det af NIS-direktivets præambel nr. 28, at med henblik på at fastslå, hvorvidt en hændelse ville have væsentlig forstyrrende virkning på leveringen af en væsentlig tjeneste, bør medlemsstaterne i tillæg til de tværsektorielle forhold også tage højde for sektorspecifikke forhold. Direktivet siger videre, at for så vidt angår det finansielle område, skal der tages hensyn til de pågældende virksomheders systemiske betydning baseret på de samlede aktiver eller de samlede aktiver i forhold til BNP.

Det bemærkes, at dette i høj grad er de samme kriterier, som i dag anvendes til udpegning af en SIFI.

En SIFI er et institut, hvis sammenbrud eller vanskeligheder rummer risiko for systemiske konsekvenser. Systemisk risiko er en risiko for forstyrrelse af det finansielle system, som kan få alvorlige negative konsekvenser for det finansielle system og realøkonomien.

En SIFI udpeges på baggrund af størrelse, betydning for unionens eller en relevant medlemsstats økonomi, betydningen af grænseoverskridende aktiviteter og instituttets eller koncernens sammenkobling med det finansielle system.

En SIFI måles på, at instituttets balance udgør mere end 6,5 pct. af Danmarks bruttonationalprodukt, at instituttets udlån i Danmark udgør mere end 5 pct. af de danske penge- og realkreditinstitutters samlede udlån i Danmark, og at instituttets indlån i Danmark udgør mere end 5 pct. af de danske pengeinstitutters samlede indlån i Danmark.

3.2.1.4. Den foreslåede ordning

Det foreslås at indføre en ny § 307 a i lov om finansiel virksomhed og en ny § 58 a i lov om kapitalmarkeder, hvorefter Finanstilsynet mindst hvert andet år udpege de penge- og realkreditinstitutter samt de operatører af markedspladser og centrale modparter (CCP'ere), der er operatører af væsentlige tjenester. I den forbindelse skal Finanstilsynet lægge vægt på, at tjenesten er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, at leveringen af tjenesten afhænger af net- og informationssystemer, og at en hændelse kan få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Det foreslås endvidere, at Finanstilsynet kan fastsætte nærmere regler om kravene til identifikationen af operatører af væsentlige tjenester, herunder fastsætte nærmere regler om krav om underretning af Finanstilsynet ved en hændelse.

Med de foreslåede bestemmelser sikres en direktivnær implementering af NIS-direktivet. Det forventes, at eftersom kriterierne for udpegning af operatører af væsentlige tjenester svarer til kriterierne for udpegning af SIFI'er, vil de institutter, der udpeges som SIFI'er efter § 308 i lov om finansiel virksomhed, tillige blive udpeget som operatører af væsentlige tjenester i NIS-direktivets forstand. Men ved at have en selvstændig udpegningsbestemmelse i § 307 a i lov om finansiel virksomhed, vurderes bestemmelsen at være fremtidssikret, såfremt der på et tidspunkt vurderes at være operatører i den finansielle sektor, som vurderes at være væsentlige, men dog ikke vurderes at være en SIFI.

3.2.2. Indberetningskrav for operatører af væsentlige tjenester

3.2.2.1. Gældende ret

For så vidt angår penge- og realkreditinstitutter, følger det af § 71, stk. 1, i lov om finansiel virksomhed, at en finansiel virksomhed, en finansiel holdingvirksomhed og en forsikringsholdingvirksomhed skal have effektive former for virksomhedsstyring, herunder bl.a. betryggende kontrol- og sikrings-foranstaltninger på it-området.

Det følger videre af § 71, stk. 2, at Finanstilsynet kan fastsætte nærmere regler om de foranstaltninger, som en finansiel virksomhed, en finansiel holdingvirksomhed og en forsikringsholdingvirksomhed skal træffe for at have effektive former for virksomhedsstyring, herunder betryggende kontrol- og sikringsforanstaltninger på it-området. Denne bemyndigelse er bl.a. udnyttet ved bekendtgørelse nr. 1026 af 30. juni 2016 om ledelse og styring af pengeinstitutter m.fl. (herefter kaldet ledelsesbekendtgørelsen), hvoraf bekendtgørelsens bilag 5 blandt andet stiller nærmere krav til it-sikkerhed.

Det følger bl.a. af bekendtgørelsens bilag 5, at bestyrelsen skal beslutte en it-sikkerhedspolitik for virksomheden, som ud fra den ønskede risikoprofil på it-området skal indeholde en overordnet stillingtagen til alle væsentlige forhold vedrørende it-sikkerheden. Hvad der er væsentligt, afhænger bl.a. af virksomhedens størrelse samt omfanget og kompleksiteten af virksomhedens it-anvendelse.

For så vidt angår operatører af markedspladser følger det af § 71, stk. 1, i lov om kapitalmarkeder, at en operatør af et reguleret marked er ansvarlig for, at det pågældende marked drives på en betryggende og hensigtsmæssig måde. Videre følger det af stk. 2, nr. 2, at en operatør skal kunne styre risici, som operatøren og markedet udsættes for, herunder kunne påvise alle væsentlige risici for markedets drift og indføre effektive foranstaltninger til at mindske disse risici. Det følger videre af stk. 2, nr. 3, at en operatør skal sikre en ordentlig forvaltning af den tekniske funktion af markedspladsens systemer, herunder etablere effektive nødssystemer.

Der følger ikke af ledelsesbekendtgørelsen et regulatorisk krav om indberetning af hændelser, men det skal fremhæves, at hændelsesrapportering er en væsentlig del af det løbende tilsyn og herunder en del af, at have effektive former for virksomhedsstyring. Finanstilsynet har som vejledning for de omfattede virksomheder beskrevet på sin hjemmeside, hvornår Finanstilsynet forventer at blive orienteret.

Det er som udgangspunkt virksomheden selv, som vurderer, hvornår en hændelse er væsentlig. Dog er der nogle klare indikatorer, hvor Finanstilsynet umiddelbart vurderer, at tilsynet bør orienteres. Det kan f.eks. være, når hændelsen har potentiale til at udvikle sig til en katastrofesituation, der involverer gældende kriseberedskab, når hændelsen påvirker/kan påvirke den kritiske danske betalingsinfrastruktur eller komponenter heraf eller når hændelsen kan give anledning til politianmeldelse.

For så vidt angår operatører af markedspladser og centrale modparter (CCP'ere), følger det af § 89, stk. 1, i lov om kapitalmarkeder, at en operatør af en multilateral handelsfacilitet (MHF) eller en organiseret handelsfacilitet (OHF) er ansvarlig for, at det pågældende marked drives på en

betryggende og hensigtsmæssig måde. Af § 89, stk. 2, nr. 3, fremgår det videre, at operatøren skal sikre en ordentlig forvaltning af facilitetens tekniske drift, herunder etablere effektive nødsystemer.

Det følger endvidere, af § 81 i lov om kapitalmarkeder, at en operatør af et reguleret marked hurtigst muligt skal underrette Finanstilsynet hvis operatøren bliver bekendt med eller har formodning om systemfejl i forbindelse med et finansielt instrument.

For så vidt angår centrale modparter (CCP'er) har vi i dag ikke disse i Danmark. En central modpart skal have en tilladelse og er underlagt tilsyn i henhold til Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 (EMIR-forordningen), som suppleres af tekniske standarder.

Ifølge artikel 26, stk. 6, i EMIR-forordningen skal en central modpart (CCP) have IT-systemer, der er egnede til at håndtere kompleksiteten, variationen og typen af serviceydelser, som den centrale modpart (CCP'en) udbyder. Dette med henblik på at sikre en høj IT-sikkerhed, integritet og fortrolighed omkring den data, som den centrale modpart (CCP'en) håndterer.

3.2.2.2. NIS-direktivet

I medfør af NIS-direktivet skal medlemsstaterne sikre, at operatører af væsentlige tjenester træffer passende og forholdsmæssige foranstaltninger for at styre risiciene for sikkerheden i de net- og informationssystemer, de anvender som led i deres tjeneste. Foranstaltningerne skal både være af teknisk og organisatorisk karakter samt tage højde for det aktuelle teknologiske stade med det formål at sikre et sikkerhedsniveau, der står mål med risikoen for hændelser.

I medfør af NIS-direktivet skal operatører af væsentlige tjenester, for at kunne opretholde kontinuiteten i deres tjenester, træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i de net- og informationssystemer, de anvender.

Direktivet fastsætter derudover, at operatører af væsentlige tjenester hurtigst muligt skal foretage en underretning til de kompetente myndigheder om hændelser, der har væsentlige konsekvenser for kontinuiteten af deres tjenester. Underretningen skal gøre myndighederne i stand til at vurdere, om der er behov for at underrette kompetente myndigheder i andre medlemsstater og offentligheden.

Direktivet foreskriver endelig, at de kompetente myndigheder skal kunne orientere myndighederne i andre berørte medlemsstater om hændelser hos operatører af væsentlige tjenester, der har væsentlige konsekvenser for kontinuiteten i væsentlige tjenester i de pågældende medlemssta-ter. Orienteringen vil skulle ske under overholdelse af krav om fortrolighed og sikkerhed.

3.2.2.3. Erhvervsministeriets overvejelser

For så vidt angår kreditinstitutter, det vil sige penge- og realkreditinstitutter, gælder der allerede i dag en række krav til de foranstaltninger, som en finansiel virksomhed, skal træffe for at have effektive former for virksomhedsstyring, herunder betryggende kontrol- og sikringsforanstaltninger

på it-området. Disse krav fastsættes nærmere af Finanstilsynet i bekendtgørelse nr. 1026 af 30. juni 2016 om ledelse og styring af pengeinstitutter m.fl. (herefter ledelsesbekendtgørelsen) i medfør af lov om finansiel virksomhed § 71, stk. 2.

Der gælder ikke i dag et regulatorisk krav om indberetning af hændelser for kreditinstitutter, men hændelsesrapportering er en væsentlig del af det løbende tilsyn. Det er i dag som udgangspunkt virksomheden selv, som vurderer, hvornår en hændelse er væsentlig. Finanstilsynet har som vejledning for de omfattede virksomheder beskrevet på sin hjemmeside, hvornår Finanstilsynet forventer at blive orienteret.

Det vurderes derfor at være mest hensigtsmæssigt, at der i ledelsesbekendtgørelsen indsættes en bestemmelse om, at operatører af væsentlige tjenester, skal underrette Finanstilsynet om hændelser.

For så vidt angår operatører af markedspladser og centrale modparter (CCP'ere) gælder i dag alene et underretningskrav i § 81 i lov om kapitalmarkeder, hvorefter en operatør af markedspladser skal underrette Finanstilsynet om systemfejl i forbindelse med et finansielt instrument. Der gælder ikke regler for de centrale modparter (CCP'ere), da en central modpart skal have en tilladelse og er underlagt tilsyn i henhold til Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 (EMIR-forordningen), som suppleres af tekniske standarder.

Det vurderes derfor at være mest hensigtsmæssigt, at der indsættes en hjemmel til at kunne udarbejde en bekendtgørelse, hvori der indsættes en bestemmelse om, at de operatører af markedspladser og centrale modparter (CCP'ere), der udpeges til at være væsentlige operatører, skal underrette Finanstilsynet om hændelser.

3.2.2.4. Den foreslåede ordning
Lovforslaget gennemfører NIS-direktivets bestemmelser for operatører af væsentlige tjenester på det finansielle område på Erhvervsministeriets område for så vidt angår indberetningspligt.

Med henblik på en direktivnær implementering af NIS-direktivet foreslås det, at Finanstilsynet i lov om finansiel virksomhed § 71, stk. 2, bemyndiges til også at kunne fastsætte nærmere regler for underretning om hændelsesrapportering ved eventuelle hændelser. Dermed vil Finans-tilsynet i ledelsesbekendtgørelsen kunne fastsætte nærmere krav til indberetning fra de kreditinstitutter der er operatører af væsentlige tjenester, når der er tale om hændelser, der har væsentlige konsekvenser for kontinuiteten af tjenester, og som er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.

For så vidt angår operatører af markedspladser og centrale modparter (CCP'er) foreslås det at Finanstilsynet kan fastsætte nærmere regler i en bekendtgørelse for underretning af Finanstilsynet ved en hændelse hos en operatør af markedspladser eller en central modpart (CCP), der er operatører af væsentlige tjenester, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som leveres.

3.2.3. Videregivelse af oplysninger

3.2.3.1. Gældende ret

I medfør af § 354, stk. 1, i lov om finansiel virksomhed er Finanstilsynets ansatte underlagt en særlig tavshedspligt. Finanstilsynets ansatte er således under ansvar efter straffelovens §§ 152-152 e forpligtet til at hemmeligholde fortrolige oplysninger.

Finanstilsynet kan dog i visse lovbestemte tilfælde videregive fortrolige oplysninger til bestemte modtagere i medfør af § 354, stk. 6, i lov om finansiel virksomhed.

Finanstilsynet kan dog ikke i dag videregive oplysninger til Center for Cybersikkerhed i medfør af lov om finansiel virksomhed.

3.2.3.2. NIS-direktivet

NIS-direktivet indeholder krav om udpegning af kompetente myndigheder, der skal føre tilsyn med direktivet på nationalt plan for de omfattede sektorer, jf. artikel 8, stk. 1 og 2. Da Finanstilsynet i dag er den kompetente myndighed op det finansielle område, vil det være Finanstilsynet, der skal føre tilsyn med NIS-direktivets overholdelse for så vidt angår det finansielle område.

Direktivet indeholder endvidere krav om myndighedernes samarbejde på EU-niveau og nationalt niveau. Ifølge direktivets artikel 9, skal hver medlemsstat udpege en såkaldt CSIRT (Computer Security Incident Response Team). En CSIRTs rolle skal som minimum omfatte monitorering af hændelser på nationalt plan, tidlig varsling, advarsler, meddelelser og formidling af information til relevante interessenter om risici og hændelser, at reagere på hændelser, udarbejdelse af dynamisk risiko- og hændelsesanalyser og situationsrapporter.

I medfør af direktivets artikel 12, stk. 1, skal et CSIRT-netværk oprettes for at bidrage til skabelsen af tillid mellem medlemsstaterne og at fremme et hurtigt og effektivt operationelt samarbejde. Det følger endvidere af NIS-direktivets artikel 10, at enten de kompetente myndigheder eller CSIRT'erne skal modtage underretninger om hændelser fra operatørerne af væsentlige tjenester. Hvis underretninger fra de væsentlige operatører sendes til de kompetente myndigheder, skal CSIRT'erne, i det omfang det er nødvendigt, for at de kan udføre deres opgaver, have adgang til de oplysninger om hændelser, der er underrettet af operatørerne af væsentlige tjenester, jf. artikel 10, stk. 2.

Det følger endvidere af direktivets artikel 1, nr. 5, at oplysninger der er fortrolige i henhold til EU-regler og nationale regler, kan udveksles med forbehold af artikel 346 i TEUF, hvis en sådan udveksling er nødvendig for anvendelsen af dette direktiv.

3.2.3.3. Erhvervsministeriets overvejelser

NIS-direktivet indeholder en række krav om myndighedernes samarbejde på EU-niveau og på nationalt niveau og indeholder bl.a. i artikel 9 et krav om, at hver medlemsstat udpeger en såkaldt

CSIRT (Computer Security Incident Response Team). I Danmark forventes Center for Cybersikkerhed, at blive udpeget som CSIRT.

Ifølge NIS-direktivet, skal en CSIRT som minimum monitorere hændelser på nationalt plan, modtage tidlige varslinger, advarsler og meddelelser om risici og hændelser og reagere på hændelser m.v.

Det indebærer, at en CSIRT skal modtage oplysninger om hændelser, som går fra operatørerne af væsentlige tjenester til de kompetente myndigheder.

Finanstilsynet er underlagt en skærpet tavshedspligt efter henholdsvis § 354 i lov om finansiel virksomhed og § 224 i lov om kapitalmarkeder, hvorefter Finanstilsynet er forpligtet til at hemmeligholde fortrolige oplysninger, som Finanstilsynet kommer i besiddelse af i medfør af tilsynsvirksomheden. I medfør af § 354, stk. 6, i lov om finansiel virksomhed og § 225, kan Finanstilsynet dog videregive en række oplysninger under nærmere fastsatte betingelser.

Henset til at det i øvrigt følger af NIS-direktivet, at oplysninger, der er fortrolige i henhold til EU-regler og nationale regler, kan udveksles, hvis en sådan udveksling er nødvendig for anvendelsen af dette direktiv, bør Finanstilsynets få mulighed for at videregive oplysninger om hændelser, som modtages fra operatørerne af væsentlige tjenester.

3.2.3.4. Den foreslåede ordning
For at sikre det nationale samarbejde, er det nødvendigt at Finanstilsynet skal kunne udveksle oplysninger med Center for Cybersikkerhed.

Med lovforslaget foreslås det derfor at indføre mulighed for, at Finanstilsynet i medfør af henholdsvis lov om finansiel virksomhed og lov om kapitalmarkeder, kan videregive oplysninger til Center for Cybersikkerhed, under forudsætning af at oplysningerne er nødvendige for Center for Cybersikkerhed til opfyldelse af deres lovbestemte opgaver, i deres egenskab af CSIRT og dermed national enhed, der håndterer hændelser.

3.2.4. Offentliggørelse af hændelser
3.2.4.1. Gældende ret
Der er ikke i dag mulighed for, at Finanstilsynet kan offentliggøre konkrete oplysninger om hændelser.

3.2.4.2. NIS-direktivet
Det fremgår af NIS-direktivets artikel 14, stk. 6, at den kompetente myndighed efter høring af den underrettende operatør af væsentlige tjenester kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hæn-delse eller håndtere en igangværende hændelse.

3.2.4.3. Erhvervsministeriets overvejelser
Finanstilsynet har ikke i dag mulighed for at offentliggøre konkrete oplysninger om hændelse, hvorfor en sådan bestemmelse bør indføres, både for så vidt angår lov om finansiel virksomhed og lov om kapitalmarkeder.

3.2.4.4. Den foreslåede ordning
Det foreslås at indsætte en ny § 354 h i lov om finansiel virksomhed, hvorefter Finanstilsynet kan orientere offentligheden om konkrete hændelser, efter høring af den berørte virksom-hed, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge eller håndtere en igangvæ-rende hændelse.

4. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget medfører, at Erhvervsstyrelsen skal varetage nye opgaver. Disse opgaver forudsættes imidlertid afholdt inden for den eksisterende økonomiske ramme. Lovforslaget vurderes på den baggrund ikke at have økonomiske eller administrative konsekvenser for det offentlige.

I det omfang stat, kommuner og regioner er operatører af væsentlige tjenester eller udbyder digitale tjenester, vil de krav, der efter lovforslaget stilles til operatører og udbydere, også omfatte stat, kommuner og regioner. Det vil kunne medføre økonomiske og administrative konsekvenser i samme omfang som for private udbydere.

Lovforslaget medfører endvidere, at Finanstilsynet skal varetage nye opgaver, i form af udpegninger af operatører af væsentlige tjenester. Lovforslaget vurderes dog ikke i sig selv at have økonomiske eller administrative konsekvenser for det offentlige. Finanstilsynet vil derudover også skulle etablere et samarbejde med Center for Cybersikkerhed for så vidt angår håndtering og indberetninger af hændelser. Dette kan medføre behov for øgede ressourcer, men det er dog ikke muligt at kvantificere yderligere på nuværende tidspunkt.

5. Økonomiske og administrative konsekvenser for erhvervslivet mv.
Det digitale område

Lovforslaget medfører økonomiske konsekvenser for operatører af væsentlige tjenester og udbydere af digitale tjenester.

Det vurderes, at lovforslaget medfører administrative konsekvenser under 4 mio. kr. årligt. Vurderingen bygger blandt andet på det relativt begrænsede antal hændelser årligt, der skal indberettes.

I forhold til de øvrige efterlevelseskonsekvenser vurderes disse at være under bagatelgrænsen på 10 millioner kroner årligt. Byrderne vil kunne angå omkostninger til fx: it-udstyr, lønomkostninger til medarbejdere, der skal stå få opfyldelse af kravene mv. For en stor dels vedkommende vil dette være omkostninger, som operatørerne og udbyderne måtte forventes at have i forvejen.

Det finansielle område

I medfør af lovforslaget bemyndiges Finanstilsynet endvidere til at kunne fastsætte nærmere regler om indberetning af hændelser for operatører af væsentlige tjenester. Disse regler vil blive fastsat på bekendtgørelsesniveau og kan medføre økonomiske konsekvenser for de pengeinstitutter,

realkreditinstitutter, operatører af markedspladser og centrale modparter (CCP'ere), der udpeges som operatører af væsentlige tjenester.

Økonomiske konsekvenser for erhvervslivet

Det vurderes, at lovforslaget medfører minimale øvrige efterlevelsesomkostninger for erhvervslivet, under bagatelgrænsen på 10 millioner kroner årligt. Vurderingen bygger blandt andet på det relativt begrænsede antal hændelser årligt, der vil blive stillet specifikke krav til indberetningen af. Dette vil imidlertid blive kvantificeret i forbindelse med udarbejdelsen af eventuelle nye regler.

Administrative konsekvenser for erhvervslivet

De administrative konsekvenser ved forslaget er blevet vurderet af Erhvervsstyrelsens Team Effektiv Regulering (TER), der vurderer, at forslaget ikke i sig selv medfører administrative konsekvenser på mere end 4 mio. kr. årligt. Konsekvenserne bliver derfor ikke kvantificeret nærmere.

6. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

9. Forholdet til EU-retten

Loven og de bekendtgørelser, der vil blive udstedt i medfør af loven, gennemfører dele af Europaparlamentets 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.

10. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra den 25. august 2017 til den 29. september 2017 været sendt i høring hos følgende myndigheder og organisationer m.v.:

11. Sammenfattende skema

	Positive konsekvenser/mindre udgifter (hvis ja, angiv omfang)	**Negative konsekvenser/merudgifter (hvis ja, angiv omfang)**
Økonomiske konsekvenser for det offentlige	Ingen	Ingen
Administrative konsekvenser	Ingen	Ingen

for stat, kommuner, og regioner		
Økonomiske konsekvenser for erhvervslivet mv.		Det vurderes, at lovforslaget i forhold til de øvrige efterlevelseskonsekvenser medfører byrder under bagatelgrænsen på 10 millioner kroner årligt.
Administrative konsekvenser for erhvervslivet mv.		Det vurderes, at lovforslaget medfører administrative byrderunder 4 mio. kr. årligt.
Administrative konsekvenser for borgerne	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Loven og de bekendtgørelser, der vil blive udstedt i medfør af loven, 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.	
Overimplementering af EU-retlige minimumsforpligtelser (sæt x)	Ja	Nej X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Den foreslåede bestemmelse i § 1 beskriver lovens formål, som er at fremme sikkerheden i net- og informationssystemer på det digitale område. Den øgede digitalisering af det danske samfund indebærer, at net- og informationssikkerhed spiller en stadigt mere afgørende rolle i samfundet. Der er således behov for et højt og ensartet sikkerhedsniveau for net- og informationssystemer for herigennem at sikre virksomheder og borgere i Danmark mod hændelser. Formålet med lovforslaget

er på den baggrund at medvirke til at sikre en robust IKT-infrastruktur ved at fremme informationssikkerheden i net- og informationssystemer.

Til § 2

Den foreslåede bestemmelse i § 2 beskriver anvendelsesområdet for lovforslaget. Efter § 2, stk. 1, omfatter lovforslaget operatører af væsentlige tjenester inden for den digitale infrastruktur og udbydere af digitale tjenester.

Operatører af væsentlige tjenester er væsentlige domænenavnssystemer og topdomænenavneadministratorer, der er etableret i Danmark. Med etableret menes en effektiv og reel udøvelse af aktiviteter gennem stabile ordninger. Den retlige form er ikke afgørende og kan udover operatører med hjemsted i Danmark også omfatte ordninger med status som juridisk person i form af fx filialer og datterselskaber.

Udbydere af digitale tjenester er udbydere af online-markedspladser, online-søgemaskiner eller cloud computing-tjenester, der enten har hovedsæde i Danmark eller har en repræsentant i landet. Udbydere af digitale tjenester, der tilbyder deres tjenester i Danmark, men som ikke har hovedsæde i landet eller en anden EU-medlemsstat, vil således skulle udpege en repræsentant, jf. lovforslagets § 8.

Lovforslagets § 2, stk. 1, gennemfører på denne baggrund NIS-direktivets bestemmelser om operatører af væsentlige tjenester inden for den digitale infrastruktur og udbydere af digitale tjenester i Danmark på Erhvervsministeriets område.

Den foreslåede bestemmelse i stk. 2, gennemfører artikel 16, stk. 11, i NIS-direktivet, hvorefter mikrovirksomheder og små virksomheder ikke er omfattet af kravene til udbydere af digitale tjenester. Mikrovirksomheder og små virksomheder defineres i overensstemmelse med definitionen i Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder. Det vil således være udbydere af digitale tjenester med mindst 50 ansatte og en årlig omsætning eller en årlig balance over 10 mio. EUR, der vil være omfattet af kravene. Denne undtagelse skal ses i sammenhæng med, at det skal undgås, at udbydere pålægges en uforholdsmæssig stor finansiel og administrativ byrde, og at kravene til udbyderne skal stå i rimeligt forhold til den konkrete risiko.

Til § 3

Den foreslåede § 3 definerer 14 centrale begreber i loven. Definitionerne bygger på de tilsvarende definitioner i NIS-direktivet.

Efter *nr. 1* er definitionen af net- og informationssystemer indholdsmæssigt identisk med definitionen af net- og informationssystemer i NIS-direktivets artikel 4, nr.1. Definitionen af elektroniske kommunikationsnet er enslydende med den definition af elektroniske kommunikationsnet, der anvendes i lov om elektroniske kommunikationsnet og – tjenester. Sidstnævnte lov implementerer Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) som definitionen i NIS-direktivet artikel 4, nr. 1 er baseret på.

Efter *nr. 2* er definitionen af sikkerhed i net- og informationssystemer indholdsmæssigt identisk med definitionen af sikkerhed i net- og informationssystemer i NIS-direktivets artikel 4, nr. 2.

Efter *nr. 3* er definitionen af operatører af væsentlige tjenester indholdsmæssigt identisk med definitionen af væsentlige operatører i NIS-direktivets artikel 4, nr. 4.

Efter *nr. 4* er definitionen af digital tjeneste indholdsmæssigt identisk med definitionen af digitale tjenester i NIS-direktivets artikel 4, nr. 5.

Efter *nr. 5* er definitionen af udbyder af digital tjeneste indholdsmæssigt identisk med definitionen af udbydere af digitale tjenester i NIS-direktivets artikel 4, nr. 6.

Efter *nr. 6* er definitionen indholdsmæssigt identisk med definitionen af hændelser i NIS-direktivets artikel 4, nr. 7.

Efter *nr. 7* er definitionen af risiko indholdsmæssigt identisk med definitionen i artikel 4, nr. 9.

Efter *nr. 8* er definitionen af repræsentant indholdsmæssigt identisk med definitionen af repræsentant i NIS-direktivets artikel 4, nr. 10.

Efter *nr. 9* er definitionen af domænenavnesystem indholdsmæssigt identisk med definitionen af domænenavnesystemer i NIS-direktivets artikel 4, nr. 14.

Efter *nr. 10* er definitionen af DNS-tjenesteudbyder indholdsmæssigt identisk med definitionen af DNS-tjenesteudbydere i NIS-direktivets artikel 4, nr. 15.

Efter *nr. 11* er definitionen af topdomænenavneadministrator indholdsmæssigt identisk med definitionen af topdomænenavneadministratorer i NIS-direktivets artikel 4, nr. 16.

Efter *nr. 12* er definitionen af onlinemarkedsplads indholdsmæssigt identisk med definitionen af onlinemarkedsplads i NIS-direktivets artikel 4, nr. 17. Af NIS-direktivets betragtning 15 fremgår det yderligere, at onlinemarkedsplads ikke omfatter onlinetjenester, der kun tjener til at formidle tredjepartstjenester, hvor en kontrakt kan indgås i sidste ende. Definitionen af onlinemarkedsplads omfatter heller ikke onlinetjenester, der sammenligner prisen på bestemte varer eller tjenester fra forskellige erhvervsdrivende og derefter omdirigerer brugeren til den foretrukne erhvervsdrivende for at købe produktet. Computing-tjenester leveret af onlinemarkedspladsen kan omfatte behandling af transaktioner, aggregering af data eller analyse af brugere. App-butikker, der fungerer som onlineforretninger med henblik på digital distribution af applikationer eller softwareprogrammer fra tredjemand, anses som værende en form for onlinemarkedsplads.

Efter *nr. 13* er definitionen af onlinesøgemaskine indholdsmæssigt identisk med definitionen af onlinesøgemaskine i NIS-direktivets artikel 4, nr. 18. Af NIS-direktivets betragtning 16 fremgår det yderligere, at definitionen af onlinesøgemaskine ikke omfatter søgefunktioner, der er begrænset til indholdet af et særligt websted, uanset om søgefunktionen er fra en ekstern søgemaskine. Den omfatter heller ikke onlinetjenester, der sammenligner prisen på bestemte varer eller tjenester fra forskellige erhvervsdrivende og derefter omdirigerer brugeren til den foretrukne erhvervsdrivende for at købe produktet.

Efter *nr. 14* er definitionen af cloud computing-tjeneste indholdsmæssigt identisk med definitionen af cloud computing-tjeneste i NIS-direktivets artikel 4, nr. 19. Af NIS-direktivets betragtning 17 fremgår det yderligere, at IT-ressourcer omfatter ressourcer som fx netværk, servere eller anden infrastruktur, lagring, applikationer og tjenester. Udtrykket skalerbar henviser til IT-ressourcer, som kan tildeles fleksibelt af udbyderen af cloud computing-tjenester uanset ressourcernes geografiske placering med henblik på at håndtere udsving i efterspørgslen. Udtrykket elastisk pulje bruges til at beskrive de IT-ressourcer, der tilvejebringes og stilles til rådighed alt efter efterspørgslen for hurtigt at øge eller mindske de tilgængelige ressourcer alt efter arbejdsbyrden.

Udtrykket delbar bruges til at beskrive de IT-ressourcer, der leveres til flere brugere, som deler en fælles adgang til tjenesten, men hvor databehandlingen foretages særskilt for hver bruger, selv om tjenesten leveres fra samme udstyr.

Til § 4

Den foreslåede § 4 i lovforslaget gennemfører artikel 5 i NIS-direktivet.

I lovforslagets § 4, stk. 1, fastlægges de overordnede kriterier for, hvornår en offentlig eller privat enhed, der udbyder en tjeneste inden for administration af domænenavne- eller topdomænenavnesystemer, skal betragtes som en operatør af en væsentlig tjeneste.

I afklaringen af om en tjeneste er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter vil den ansvarlige for en enhed skulle tage udgangspunkt i den liste over væsentlige tjenester, som erhvervsministeren udarbejder i henhold til lovforslagets § 4, stk. 2. I vurderingen skal derudover indgå om tjenesten er afhængig af net- og informationssystemer, og om en hændelse vil få væsentlig forstyrrende virkning for leveringen af den pågældende tjeneste. Net- og informationssystemer skal forstås i overensstemmelse med definitionen i lovforslagets § 3, nr. 1.

I vurderingen af, hvorvidt en hændelse vil få væsentlig forstyrrende virkning, vil en række faktorer skulle indgå, som fx det antal brugere, der er afhængige af tjenesten til private eller erhvervsmæssige formål. Brugen af tjenesten kan her være direkte, indirekte eller ved formidling. Ved vurderingen af, hvilke konsekvenser en hændelse kunne have rent omfangs- og varighedsmæssigt på økonomiske og samfundsmæssige aktiviteter eller den offentlige sikkerhed, vil ligeledes kunne indgå, hvor lang tid der skønnes at ville gå, før afbrydelsen af tjenesten vil have negative konsekvenser. Kriterierne for hvornår en hændelse har væsentligt forstyrrende virkning vil blive nærmere fastsat af erhvervsministeren i henhold til bemyndigelsesbestemmelsen i lovforslagets § 4, stk. 2.

Med lovforslagets § 4, stk. 2, får erhvervsministeren endvidere bemyndigelse til at udarbejde og regelmæssigt ajourføre en liste over tjenester inden for den digitale infrastruktur, der er væsentlige for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter. Listens formål er at identificere de typer af væsentlige tjenester, der findes inden for administration af domænenavne-systemer eller topdomænenavne systemer. Dette betyder, at den ansvarlige enhed inden for denne sektor kan holde de væsentlige tjenester adskilt fra de ikke-væsentlige aktiviteter. Den nærmere afgrænsning af væsentlige tjenester vil tage udgangspunkt i tjenester, der er vigtige for samfundets funktionalitet, og hvor en afbrydelse fx vil hindre gennemførelsen af økonomiske aktiviteter, underminere brugernes tillid og på anden måde gøre skade på samfundsøkonomien.

Til § 5

Den foreslåede § 5 i lovforslaget gennemfører dele af artikel 14 i NIS-direktivet. Med lovforslaget fastlægges sikkerhedskravene for operatører af væsentlige tjenester.

Efter det foreslåede *§ 5, stk. 1*, skal operatører af væsentlige tjenester træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i de net- og informationssystemer, som de anvender til deres aktiviteter. Bestemmelsen gennemfører artikel 14, stk. 1, i NIS-direktivet.

Efter lovforslagets *§ 5, stk. 2*, skal operatører endvidere træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser i de net- og informationssystemer, de bruger til at levere deres tjeneste. Bestemmelsen gennemfører NIS-direktivets artikel 14, stk. 2.

Bestemmelserne i lovforslagets § 5, stk. 1 og 2, skal ses i sammenhæng. Formålet med begge bestemmelser er således at fremme en risikostyringskultur med risikovurdering og gennemførelse af sikkerhedsforanstaltninger, som står i forhold til risiciene. Det er her afgørende, at operatørerne ikke pålægges en uforholdsmæssig stor økonomisk og administrativ byrde, hvorfor kravene skal stå i et rimeligt forhold til den risiko, der er forbundet med det pågældende net- og informationssystem, under hensyntagen til sådanne foranstaltningers aktuelle stade.

Bestemmelserne i lovforslagets § 5, stk. 1 og 2, vil indebære, at operatørerne skal arbejde systematisk og risikobaseret med sikkerheden i deres net- og informationssystemer. Risikostyringsforanstaltningerne vil omfatte foranstaltninger til at identificere alle risici for hændelser, forebygge, detektere og håndtere hændelser og begrænse deres konsekvenser. Sikkerheden i net- og informationssystemer omfatter lagrede, overførte og behandlede datas sikkerhed og skal ses som evnen til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i systemerne.

I tilfælde hvor der er tale om behandling af personhenførbare oplysninger, vil lovgivningen for databeskyttelse, jf. Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger finde tilsvarende anvendelse. Reglerne i databeskyttelsesforordningen vil finde anvendelse, når disse træder i kraft den 25. maj 2018.

Foranstaltningerne skal tage højde for den teknologiske udvikling. Operatørerne vil i forlængelse heraf i deres tilrettelæggelse og ajourføring af deres sikkerhedsforanstaltninger skulle inddrage de tekniske løsninger, der er tilgængelige på markedet.

Med tekniske foranstaltninger sigtes her til foranstaltninger, der er med til at sikre IT-sikkerheden (datasikkerhed og kommunikationssikkerhed) og den fysiske sikkerhed. Tekniske foranstaltninger vil i forlængelse heraf fx være foranstaltninger, der skal beskytte enten net- og informationssystemerne og operatørernes fysiske lokaliteter mod uberettiget adgang for udefrakommende, eller sikre at data kan overføres sikkert. Organisatoriske foranstaltninger sigter til fx styredokumenter, manualer, monitorering og evaluering af sikkerhedsindsatsen.

Hvilke foranstaltninger indenfor lovgivningens rammer, der konkret skal træffes, overlades til operatørerne. Bestemmelsen indfører ikke en forpligtelse til at konstruere, udvikle eller fremstille et bestemt kommercielt informations- og kommunikationsteknologiprodukt. Sikkerhedskravene gælder endelig uanset om operatørerne selv står for vedligeholdelsen af deres net- og informationssystemer eller har outsourcet denne opgave. Efter lovforslagets § 5, *stk. 3*, vil erhvervsministeren få bemyndigelse til at fastsætte nærmere sikkerhedskrav til operatørerne. Bemyndigelsen vil skulle anvendes til at præcisere lovforslagets krav i § 5, stk. 1 og 2, om risikostyringsforanstaltninger på baggrund af bl.a. de vejledninger Kommissionen forventes at udstede om operatørernes sikkerhedsforpligtelser i henhold til NIS-direktivet. Bemyndigelsen kan fx anvendes til at fastsætte bestemmelser om adgang til fysisk- og miljømæssig sikkerhed såsom beskyttelse mod indbrud og brand, samt bestemmelser om forsyningssikkerhed såsom udarbejdelse af politikker for adgang til elforsyning.

Bemyndigelsen vil ikke blive anvendt til at fastsætte yderligere krav end de krav, der følger af NIS-direktivet. Endvidere vil der i udmøntningen af bemyndigelsen blive lagt vægt på at sikre, at operatørerne kun underlægges proportionale krav, der i videst muligt omfang overlader et skøn til udbyderne til selv at beslutte indholdet af deres sikkerhedsforanstaltninger, så længe de er tilstrækkelige til at leve op til sikkerhedsforpligtelserne.

Til § 6

Den foreslåede § 6 i lovforslaget gennemfører dele af artikel 14 i NIS-direktivet. Med lovforslaget fastlægges operatørers forpligtelse til at underrette myndighederne i tilfælde af hændelser.

Efter lovforslagets *§ 6, stk. 1,* skal operatører hurtigst muligt underrette Erhvervsstyrelsen om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Underretningen skal indeholde oplysninger, der gør Erhvervsstyrelsen i stand til at vurdere om hændelsen har betydning for andre EU-lande fx antal brugere af de berørte systemer i de pågældende lande og varigheden af hændelsen.

Hændelser defineres her i overensstemmelse med lovforslagets § 3, nr. 6, hvorefter en hændelse er enhver begivenhed, der har egentlig negativ indvirkning på sikkerheden i net- og informationssystemer.

Med hurtigst muligt sigtes til, at operatøren under hensyntagen til arbejdet med at minimere konsekvenserne af hændelsen skal foretage underretningen, så snart denne har de nødvendige oplysninger til at kunne vurdere omfanget af hændelsen. Det gælder særligt, hvis hændelsen vurderes at kunne påvirke flere operatører eller til at være grænseoverskridende.

Underretningen vil ikke i sig selv føre til et øget ansvar for operatøren.

Efter det foreslåede *stk. 2,* skal operatøren i vurderingen af, om en hændelse har væsentlige konsekvenser navnlig inddrage: a) antallet af brugere, der er berørt af hændelsen, b) hændelsens varighed og c) hvor stort et geografisk område, der er berørt af hændelsen. De nærmere kriterier for, hvornår og hvordan en underretning vil skulle ske samt indholdet af underretningen, vil blive fastlagt af erhvervsministeren i henhold til bemyndigelsesbestemmelsen i lovforslagets § 6, stk. 4.

Efter det foreslåede *stk. 3* skal operatøren også foretage en underretning, hvis dennes net- og informationssystemer er påvirkede af en hændelse i en digital udbyders tjeneste, som operatøren er afhængig af. Herigennem sikres, at Erhvervsstyrelsen får kendskab til hændelser og mangler i sikkerheden hos udbydere af digitale tjenester, der har en negativ indvirkning på væsentlige tjenester. Underretningen vil kunne indgå som dokumentation for, at en udbyder ikke har levet op til kravene efter dette lovforslag. Bestemmelsen i *stk. 3* er indholdsmæssig identisk med artikel 16, stk. 5 i NIS-direktivet.

Til § 7

Den foreslåede § 7 i lovforslaget gennemfører dele af artikel 14 i NIS-direktivet.

Med bestemmelsen i *stk. 1* foreslås det, at Erhvervsstyrelsen kan videregive oplysninger om hændelser til Center for Cybersikkerhed under forudsætning af, at oplysningerne er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver, i dets egenskab af nationalt kontaktpunkt i henhold til NIS-direktivet. Et nationalt kontaktpunkts rolle skal som minimum

omfatte monitorering af hændelser på nationalt plan, tidlig varsling, advarsler, meddelelser og formidling af information til relevante interessenter om risici og hændelser, at reagere på hændelser, udarbejdelse af dynamisk risiko- og hændelsesanalyser og situationsrapporter. Det nationale kontaktpunkt vil i forlængelse heraf i henhold til NIS-direktivet skulle orientere kontaktpunkter i andre medlemsstater om hændelser, der har væsentlige konsekvenser for kontinuiteten i de væsentlige tjenester, der udbydes i de pågældende lande - fx hændelser i forhold til tilgængeligheden af domænenavnsservertjenesten hos administratoren for ".dk". Orienteringen vil ske under hensyntagen til operatørens sikkerhed og kommercielle interesser. Efter det foreslåede *stk. 2*, vil Erhvervsstyrelsen i det omfang, det er muligt, skulle give oplysninger til operatøren om, hvordan styrelsen behandler den indrapporterede hændelse. Formålet med bestemmelsen er først og fremmest at sikre, at operatøren får en tilbagemelding, der kan understøtte operatørens videre arbejde med at begrænse hændelsen.

Med bestemmelsen i *stk. 3* foreslås det, at Erhvervsstyrelsen eller Center for Cybersikkerhed får mulighed for at offentliggøre hændelser, hvor det vurderes, at offentliggørelse vil være nødvendigt for at kunne forebygge eller håndtere en hændelse. Offentliggørelse vil kun kunne ske efter høring af operatøren, og der skal foretages en afvejning af på den ene side offentlighedens interesse i at blive informeret om trusler og på den anden side mulig kommerciel skade samt skade for omdømmet for den pågældende operatør. Center for Cybersikkerhed vil stå for offentliggørelsen i de tilfælde, hvor hændelsen vedrører flere sektorer.

Til § 8

Den foreslåede § 8 i lovforslaget gennemfører dele af artikel 18 i NIS-direktivet. Bestemmelsen skal sikre, at Erhvervsstyrelsen i spørgsmål om overtrædelse af bestemmelserne i dette lovforslag vil kunne kontakte en repræsentant for den digitale udbyder, hvis digitale udbydere ikke har hjemsted i Danmark.

Med henblik på at afgøre, om udbyderen tilbyder sin digitale tjeneste i Danmark, skal der lægges vægt på, om det er åbenbart, at udbyderen af digitale tjenester påtænker at tilbyde tjenester til personer i Danmark. Alene det forhold, at der i Danmark er adgang til udbyderens eller en mellemmands websted eller til andre kontaktoplysninger er utilstrækkeligt til at fastslå en sådan hensigt. Imidlertid kan faktorer såsom information på dansk, priser angivet i danske kroner eller omtale af kunder eller brugere i Danmark, gøre det åbenbart, at udbyderen påtænker at tilbyde sine digitale tjenester i Danmark. Det er den enkelte udbyder af digitale tjenesters ansvar at udpege en repræsentant.

Repræsentanten skal udtrykkeligt udpeges ved en skriftlig fuldmagt fra udbyderen til at handle på vegne af udbyderen for så vidt angår dennes forpligtelser i medfør af bestemmelserne i dette direktiv, herunder i forbindelse med underretning om hændelser. Udpegelsen af en repræsentant af udbyderen af digitale tjenester berører ikke eventuelle retlige skridt mod selve udbyderen af digitale tjenester.

Til § 9

Den foreslåede § 9 i lovforslaget gennemfører dele af artikel 16 i NIS-direktivet. Med lovforslaget fastlægges sikkerhedskravene for udbydere af digitale tjenester.

Efter lovforslagets *§ 9, stk. 1*, skal udbydere af digitale tjenester identificere og træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i de net- og informationssystemer, som de anvender til deres aktiviteter. Bestemmelsen gennemfører artikel 16, stk. 1, i NIS-direktivet.

Efter lovforslagets *§ 9, stk. 2*, skal udbydere af digitale tjenester endvidere træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser i de net- og informationssystemer, de bruger til at levere deres tjeneste. Bestemmelsen gennemfører NIS-direktivets artikel 16, stk. 2.

Bestemmelserne i lovforslagets § 9, stk. 1 og 2, skal ses i sammenhæng. Formålet med begge bestemmelser er lig lovforslagets § 5, stk. 1 og 2, at fremme en risikostyringskultur med risikovurdering og gennemførelse af sikkerhedsforanstaltninger, som står i forhold til risiciene. Det er ligesom for operatører afgørende, at udbyderne ikke pålægges en uforholdsmæssig stor økonomisk og administrativ byrde, hvorfor kravene skal stå i et rimeligt forhold til den risiko, der er forbundet med det pågældende net- og informationssystem, under hensyntagen til sådanne foranstaltningers aktuelle stadie.

Bestemmelserne i lovforslagets § 9, stk. 1 og 2, vil indebære, at udbyderne skal arbejde systematisk og risikobaseret med sikkerheden i deres net- og informationssystemer. Risikostyringsforanstaltningerne vil omfatte foranstaltninger til at identificere alle risici for hændelser, forebygge, detektere og håndtere hændelser og begrænse deres konsekvenser. Hvilke foranstaltninger indenfor lovgivningens rammer, der konkret skal træffes, overlades lig hvad der foreslås for operatørerne til udbyderne. Til forskel for lovforslagets § 5 for operatører præciseres det imidlertid i den foreslåede § 9, stk. 1, at udbyderne i deres tilrettelæggelse af deres foranstaltninger skal inddrage følgende elementer: sikkerheden i systemer og faciliteter, håndtering af hændelser, styring af driftskontinuitet, monitorering, audit (kontrol) og testning samt overholdelse af internationale standarder. Disse elementer vil blive præciseret nærmere i de gennemførelsesretsakter Kommissionen forventes at udstede i henhold til NIS-direktivet. For yderligere bemærkninger henvises til bemærkningerne til den forslåede § 5, stk. 1 og 2.

Efter lovforslagets *§ 9, stk. 3*, vil Erhvervsstyrelsen få bemyndigelse til at fastsætte nærmere sikkerhedskrav til udbyderne. Bemyndigelsen vil skulle anvendes til at præcisere lovforslagets krav i § 9, stk. 1 og 2, om risikostyringsforanstaltninger på baggrund af de gennemførelsesretsakter Kommissionen forventes at udstede om udbydernes sikkerhedsforpligtelser i henhold til NIS-direktivet. Bemyndigelsen kan fx anvendes til at fastsætte bestemmelser om adgang til fysisk- og miljømæssig sikkerhed såsom beskyttelse mod indbrud og brand, samt bestemmelser om forsyningssikkerhed såsom udarbejdelse af politikker for adgang til elforsyning. Bemyndigelsen vil ikke blive anvendt til at fastsætte yderligere krav end de krav, der følger af NIS-direktivet. Endvidere vil der i udmøntningen af bemyndigelsen blive lagt vægt på at sikre, at udbyderne kun underlægges proportionale krav, der i videst muligt omfang overlader et skøn til udbyderne til selv at beslutte indholdet af deres sikkerhedsforanstaltninger.

Til § 10

Den foreslåede § 10 i lovforslaget gennemfører dele af artikel 16 i NIS-direktivet. Med lovforslaget fastlægges udbyderes forpligtelse til at underrette myndighederne i tilfælde af hændelser.

Efter lovforslagets *§ 10, stk. 1,* skal udbyderen af digitale tjenester hurtigst muligt underrette Erhvervsstyrelsen om hændelser, der har betydelige konsekvenser for de tjenester, som de leverer. Underretningen skal indeholde oplysninger, der gør Erhvervsstyrelsen i stand til at vurdere om hændelsen har betydning for andre EU-lande.

Hændelser defineres her i overensstemmelse med lovforslagets § 3, nr. 6, hvorefter en hændelse er enhver begivenhed, der har egentlig negativ indvirkning på sikkerheden i net- og informationssystemer.

Med hurtigst muligt sigtes til, at udbyderen under hensyntagen til arbejdet med at minimere konsekvenserne af hændelsen skal foretage underretningen så snart denne har de nødvendige oplysninger til at kunne vurdere omfanget af hændelsen. Det gælder særligt, hvis hændelsen vurderes at kunne påvirke flere udbydere eller til at være grænseoverskridende.

Underretningen vil ikke i sig selv medføre et øget ansvar for udbyderen.

Efter lovforslagets *§ 10, stk. 2*, skal udbydere i vurderingen af, om en hændelse har væsentlige konsekvenser, inddrage navnlig: a) antallet af brugere, der er berørt af hændelsen, b) hændelsens varighed, c) hvor stort et geografisk område, der er berørt af hændelsen, d) omfanget af afbrydelsen af tjenestens funktion, og e) omfanget af konsekvenserne for økonomiske og samfundsmæssige aktiviteter.

I henhold til lovforslagets *§ 10, stk. 3*, vil udbyderen ikke skulle underrette myndighederne, hvis ikke udbyderen kan skaffe de oplysninger, herunder de af § 10, stk. 2, omfattede oplysninger, der er nødvendige for at fastlægge om en hændelse har væsentlige konsekvenser.

De nærmere kriterier for, hvornår og hvordan en underretning vil skulle ske samt indholdet af underretningen, vil blive fastlagt af Erhvervsstyrelsen i henhold til bemyndigelsesbestemmelsen i lovforslagets *§ 10, stk. 4.* Bemyndigelsen vil blive anvendt til at præcisere kriterierne for, hvornår en hændelse skal indberettes på baggrund af de gennemførelsesretsakter Kommissionen forventes at udstede om udbydernes underretningspligt efter NIS-direktivet. Bemyndigelsen vil endvidere anvendes til at præcisere, hvordan indberetningen skal foregå – fx gennem en fælles indberetningsløsning på virk.dk.

Efter det foreslåede stk. 3, skal udbyderen kun underrette Erhvervsstyrelsen i det omfang, at udbyderen har adgang til de nødvendige oplysninger i forhold til at afklare, om hændelsen er væsentlig. Det forhold, at udbyderen ikke har adgang til oplysninger om alle de nævnte kriterier i stk. 2, fx antal brugere, medfører ikke, at udbyderens forpligtelse til at underrette bortfalder alene af den grund. Udbyderen vil således skulle foretage en samlet vurdering af de oplysninger, der er til rådighed, og på den baggrund foretage en vurdering af hændelsens væsentlighed.

Til § 11

Den foreslåede § 11 i lovforslaget gennemfører dele af artikel 16 i NIS-direktivet.

Med bestemmelsen i *stk. 1* foreslås det, at Erhvervsstyrelsen kan viderebringe oplysninger om hændelser til Center for Cybersikkerhed under forudsætning af, at oplysningerne er nødvendige for Center for Cybersikkerhed til opfyldelse af dets lovbestemte opgaver, i dets egenskab af nationalt

kontaktpunkt i henhold til NIS-direktivet. Et nationalt kontaktpunkts rolle skal som minimum omfatte monitorering af hændelser på nationalt plan, tidlig varsling, advarsler, meddelelser og formidling af information til relevante interessenter om risici og hændelser, at reagere på hændelser, udarbejdelse af dynamisk risiko- og hændelsesanalyser og situationsrapporter. Det nationale kontaktpunkt vil i forlængelse heraf i henhold til NIS-direktivet skulle orientere kontaktpunkter i andre medlemsstater om hændelser, der har betydelige konsekvenser for leveringen af de tjenester, der udbydes i de pågældende lande. Orienteringen vil ske under hensyntagen til udbyderens sikkerhed og kommercielle interesser samt krav på fortrolig behandling af oplysninger.

Med bestemmelsen i *stk. 2* foreslås det, at Erhvervsstyrelsen eller Center for Cybersikkerhed får mulighed for at offentliggøre hændelser, hvor det vurderes, at offentliggørelse vil være nødvendigt for at kunne forebygge eller håndtere en hændelse. Offentliggørelse vil kun kunne ske efter høring af udbyderen, og der skal foretages en afvejning af på den ene side offentlighedens interesse i at blive informeret om trusler og på den anden side mulig imageskade og kommerciel skade for den pågældende udbyder. Center for Cybersikkerhed vil stå for offentliggørelsen i de tilfælde, hvor hændelsen vedrører flere sektorer.

Til § 12

Den foreslåede § 12 har til formål at skabe rammerne for et tilsyn med operatørernes og udbydernes overholdelse af kravene til informationssikkerhed. Bestemmelsen gennemfører dele af NIS-direktivets artikel 15 og 17.

Med bestemmelsen i *stk. 1* foreslås det, at Erhvervsstyrelsen fører tilsyn med overholdelsen af loven og regler udstedt i medfør af loven.

Erhvervsstyrelsen sikres med det foreslåede *stk. 2* adgang til enhver oplysning, der er nødvendige til gennemførelse af styrelsens tilsynsvirksomhed. Sådanne oplysninger kan eksempelvis være til brug for identificeringen af operatører af væsentlige tjenester samt i forhold til at indhente operatørers eller udbyderes informationssikkerhedspolitik, risikovurderinger, beredskabsplaner, netarkitektur- og designdokumenter samt testrapporter.

Efter *stk. 3* kan Erhvervsstyrelsen endvidere for operatører af væsentlige tjenester kræve, at de afgiver dokumentation for den faktiske gennemførelse af sikkerhedspolitikker.

Hvis Erhvervsstyrelsen på baggrund af de oplysninger, styrelsen modtager som led i sit tilsyn, konstaterer, at en operatør eller en udbyder ikke har efterlevet kravene til sikkerhedsforanstaltninger og underretning af hændelser efter denne lov, kan styrelsen efter det foreslåede *stk. 4*, påbyde udbydere og operatører, at de afhjælper de pågældende mangler.

Til § 13

Med den foreslåede § 13 vil Erhvervsstyrelsen skulle offentliggøre alle afgørelser, hvori påbud udstedes.

Det foreslåede *stk. 1, 1. pkt.*, medfører, at offentliggørelsen af afgørelsen skal ske på Erhvervsstyrelsens hjemmeside. Offentliggørelsen skal ske så hurtigt som praktisk muligt og straks efter, at den fysiske eller juridiske person er blevet underrettet om afgørelsen. Erhvervsstyrelsen kan bestemme, om hele afgørelsen eller kun dele af afgørelsen skal offentliggøres. Dog skal

Erhvervsstyrelsens pålagte påbud og overtrædelsens art offentliggøres. Offentliggørelsen af oplysningerne vil være tilgængelig på styrelsens hjemmeside i mindst fem år efter offentliggørelsen.

Det foreslås i *stk. 1, 2. pkt*., at offentliggørelse af afgørelser, hvori en fysisk person pålægges et påbud efter den foreslåede § 12, stk. 4, anonymiseres for så vidt angår personoplysninger, herunder identiteten på den fysiske person. En afgørelse må derfor ikke indeholde personoplysninger. En afgørelse må heller ikke indeholde oplysninger om en person, der direkte eller indirekte kan identificere personen, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for en given persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Offentliggørelse af påbud, som pålægges en fysisk person, skal således ikke indeholde oplysning om identiteten af den fysiske person. Formålet er, at den fysiske person ikke må kunne identificeres. Det tilsikres hermed, at der ikke sker en offentliggørelse af personoplysninger,, idet offentliggørelse af, at fysiske personer har modtaget et påbud, vil ske i anonymiseret form. Da enkeltmandsvirksomheder normalt drives af en fysisk person, vil der tilsvarende skulle ske anonymisering af navnet på en enkeltmandsvirksomhed svarende til, hvad der gælder for fysiske personer.

Erhvervsstyrelsen vil ved hver enkelt offentliggørelse af oplysninger om, at en fysisk person har modtaget et påbud, overveje, om offentliggørelsen indeholder oplysninger, der er personhenførbare. Oplysninger om, at den fysiske person, som har modtaget påbuddet, arbejder i en bestemt afdeling, har en bestemt stilling eller udfører bestemte funktioner kan efter omstændighederne udgøre personoplysninger i persondatalovens forstand, hvis det fra disse oplysninger sammenholdt med andre offentliggjorte oplysninger er muligt at identificere personen.

Det foreslås efter *stk. 2*, at afgørelser, hvori en juridisk person pålægges et påbud, som udgangspunkt offentliggøres med oplysning om navnet på den juridiske person. Der foreligger dog undtagelser til dette.

For det første skal identiteten på den juridiske person ske i anonymiseret form af hensyn til en igangværende strafferetlig efterforskning. Beslutning om offentliggørelse bør alene ske efter høring af den relevante politimyndighed, dog således at der eventuelt kan indgås en mere generel aftale om offentliggørelse af visse sagstyper. Ved tvivl forelægges spørgsmålet om offentliggørelse for den relevante politimyndighed.

For det andet kan anonymisering ske, hvis offentliggørelsen vil forvolde uforholdsmæssig stor skade, f.eks. for den juridiske person, afgørelsen vedrører, investorer eller andre. Det forhold, at offentliggørelse af en juridisk persons navn vil kunne medføre tab af kunder, eller at offentliggørelse vil kunne bane vej for et erstatningskrav mod den juridiske person, vil ikke i sig selv være tilstrækkeligt til, at offentliggørelse skal ske i anonymiseret form. Undtagelsen bør således kun finde anvendelse på de tilfælde, hvor den juridiske persons fortsatte drift vil blive truet, eller hvis meget væsentlige interesser krænkes.

Da udkast til Erhvervsstyrelsens afgørelser i deres helhed sendes i partshøring hos de berørte juridiske personer, vil de berørte virksomheder i forbindelse med høringen få mulighed for at kommentere på spørgsmålet om offentliggørelse, herunder hvis det indstilles, at afgørelsen offentliggøres med angivelse af identiteten på operatøren eller udbyderen, hvilket er det altovervejende udgangspunkt. Beslutningen om at offentliggøre virksomhedens navn er endelig og

kan således ikke indbringes for højere administrativ myndighed, jf. lovforslagets § 14 og bemærkninger hertil.

Det foreslås i *stk. 3*, at der skal ske anonymisering af identiteten på den juridiske person efter 2 år regnet fra og med datoen for offentliggørelsen. Herved skabes der klarhed over, hvor lang tid en offentliggørelse vil være tilgængelig i ikke-anonymiseret form.

Til § 14

Med den foreslåede § 14 kan afgørelser truffet af Erhvervsstyrelsen efter § 12, stk. 2, 3 og 4, og § 13, stk. 1, ikke indbringes for andre administrativ myndigheder. Bestemmelsen afskærer den administrative klageadgang fra Erhvervsstyrelsen til erhvervsministeren. Det gælder også for klager vedrørende retlige mangler.

Baggrunden for den foreslåede bestemmelse er, at de afgørelser, som Erhvervsstyrelsen vil træffe efter loven, vil være af teknisk karakter og forudsætter betydelig teknisk indsigt på området, som det ikke kan forventes, at Erhvervsministeriets departement er i besiddelse af. Der kan således f.eks. være tale om afgørelser om, at operatører af væsentlige tjenester ikke har truffet de nødvendige foranstaltninger for at styre risiciene for sikkerheden i deres net- og informationssystemer. At træffe disse afgørelser vil forudsætte betydelig IT-sikkerhedsmæssig indsigt på området, som det ikke kan forventes, at ministeriets departement er i besiddelse af. Erhvervsstyrelsen har i henhold til lovforslaget ikke mulighed for at træffe afgørelser, der ikke kræver teknisk indsigt.

Det er derfor vurderingen, at departementet typisk ikke vil kunne foretage en realitetsbehandling af eventuelle klager over Erhvervsstyrelsens afgørelser, der træffes med hjemmel i den foreslåede lov. Bestemmelsen afskærer dog ikke den almindelige adgang til at få afgørelser prøvet ved domstolene.

Til § 15

Med lovforslagets *§ 15, stk. 1*, skabes der hjemmel til, at Erhvervsstyrelsen kan fastsætte regler om, at skriftlig kommunikation til og fra styrelsen om alle forhold skal foregå digitalt.

Lovforslaget indebærer bl.a., at skriftlige henvendelser m.v. til styrelsen om forhold, som er omfattet af loven eller regler udstedt i medfør af loven, ikke anses for behørigt modtaget i styrelsen, hvis de indsendes på anden vis end den foreskrevne digitale måde.

Samtidig indebærer lovforslaget, at meddelelser m.v. til eller fra Erhvervsstyrelsen, der sendes på den foreskrevne digitale måde, anses for at være kommet frem til modtageren på det tidspunkt, hvor meddelelsen m.v. er tilgængelig digitalt for modtageren, jf. det foreslåede stk. 3. Det vil sige med samme retsvirkninger som fysisk post, der anses for at være kommet frem, når den pågældende meddelelse m.v. er lagt i adressatens fysiske postkasse.

Af bekendtgørelsen, som udmønter den foreslåede bemyndigelse, vil det komme til at fremgå, hvem der omfattes af pligten til at kommunikere digitalt med styrelsen, om hvilke forhold og på hvilken måde.

Ved henvendelser til styrelsen kan styrelsen stille krav om, at den pågældende oplyser en e-mailadresse, som den pågældende kan kontaktes på i forbindelse med behandlingen af en konkret sag eller henvendelse til styrelsen. I den forbindelse kan der også pålægges den pågældende en pligt til at underrette styrelsen om en eventuel ændring i e-mailadressen, inden den konkrete sag afsluttes

eller henvendelsen besvares, medmindre e-mails automatisk bliver videresendt til den nye e-mailadresse.

I bekendtgørelsen, som udmønter den foreslåede bemyndigelse i stk. 1, kan der fastsættes regler om, at Erhvervsstyrelsen kan sende visse meddelelser, herunder afgørelser og påbud m.v., til adressatens digitale postkasse med de retsvirkninger, der følger af Lov om Offentlig Digital Post.

I bekendtgørelsen kan der desuden fastsættes regler om fritagelse for pligten til digital kommunikation. Da der er tale om kommunikation om erhvervsforhold, vil fritagelsesmuligheden blive stærkt begrænset. Fritagelsesmuligheden tænkes navnlig anvendt, hvor det er påkrævet at anvende en dansk digital signatur, og der er tale om en person uden dansk CPR-nummer eller en virksomhed med hjemsted i udlandet, som ikke kan få en dansk digital signatur.

Fritagelsesmuligheden kan endvidere tænkes anvendt, hvis materialet på grund af sin særlige beskaffenhed ikke er egnet til digital fremsendelse. Det kan f.eks. være tilfældet i forbindelse med en undersøgelsessag, hvor der kan være tale om udveksling af en meget omfattende mængde dokumentation m.v.

Det forhold, at en virksomhed eller en person oplever, at den pågældendes egen computer ikke fungerer, at den pågældende har mistet koden til sin digitale signatur eller oplever lignende hindringer, som det er op til den pågældende at overkomme, kan ikke føre til fritagelse for pligten til digital kommunikation. Efter det foreslåede *stk. 2* kan der i bekendtgørelsen specificeres krav om anvendelse af bestemte it-systemer, digitale formater og digital signatur eller lignende.

Det foreslåede *stk. 3* fastsætter, hvornår en digital meddelelse må anses for at være kommet frem til adressaten for meddelelsen, dvs. modtageren af meddelelsen. For meddelelser, der sendes til en myndighed, er myndigheden adressat for meddelelsen. For meddelelser, som myndigheden sender, er den pågældende virksomhed etc., som meddelelsen sendes til, adressat for meddelelsen.

En meddelelse vil normalt anses for at være kommet frem til en myndighed på det tidspunkt, hvor meddelelsen er tilgængelig for myndigheden, dvs. når styrelsen kan behandle meddelelsen. Dette tidspunkt vil normalt blive registreret automatisk i en modtagelsesanordning eller et datasystem. En meddelelse vil normalt anses for at være kommet frem til en virksomhed eller person på det tidspunkt, hvor meddelelsen er tilgængelig for den pågældende. En meddelelse vil blive anset for at være tilgængelig, selvom den pågældende ikke kan skaffe sig adgang til meddelelsen, hvis dette skyldes hindringer, som det er op til den pågældende at overkomme. Som eksempler herpå kan nævnes, at den pågældendes egen computer ikke fungerer, eller den pågældende har mistet koden til sin digitale signatur.

Til § 16

Med lovforslagets *§ 16, stk. 1*, kan der fastsættes regler om, at Erhvervsstyrelsen kan udstede afgørelser og andre dokumenter efter denne lov eller regler udstedt i medfør af denne lov uden underskrift, med maskinel eller på tilsvarende måde gengivet underskrift eller under anvendelse af en teknik, der sikrer entydig identifikation af den, som har udstedt afgørelsen eller dokumentet.

Desuden kan der efter *§ 16, stk. 2* fastsættes regler om, at afgørelser og andre dokumenter, der udelukkende er truffet eller udstedt på grundlag af elektronisk databehandling, kan udstedes alene med Erhvervsstyrelsen som afsender. Bestemmelsen finder anvendelse både på dokumenter, som Erhvervsstyrelsen sender digitalt, og på dokumenter, som sendes på papir med almindelig post.

Til § 17

Den foreslåede § 17 vedrører dokumenter, som er omfattet af denne lov eller forskrifter udstedt i medfør heraf, og som er udstedt af andre end en myndighed, hvor det efter loven eller regler udstedt i medfør af loven er krævet, at dokumentet er underskrevet. Underskriftskravet kan fremgå udtrykkeligt eller forudsætningsvist af de pågældende regler.

For at der ikke skal kunne opstå tvivl om, at underskriftskravet kan opfyldes på anden måde end ved en personlig underskrift, foreslås det, at der indsættes en udtrykkelig bestemmelse i loven om, at underskriftskravet som anført i *stk. 1* kan opfyldes ved, at underskriveren anvender en teknik, der sikrer entydig identifikation af den pågældende, f.eks. digital signatur.

Det foreslås i *stk. 2*, at Erhvervsstyrelsen kan fastsætte nærmere regler om, hvordan kravet om personlig underskrift kan fraviges. Med hjemmel i den foreslåede bestemmelse kan der desuden fastsættes regler om, at krav om personlig underskrift ikke kan fraviges for visse typer af dokumenter.

Til § 18

Den foreslåede § 17 i lovforslaget gennemfører artikel 21 i NIS-direktivet, hvor medlemsstaterne forpligtes til at fastsætte sanktioner for overtrædelse af de nationale regler, der vedtages i medfør af NIS-direktivet. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have præventiv virkning.

Efter det foreslåede *stk. 1*, kan undladelse af at efterkomme Erhvervsstyrelsens krav i forbindelse med styrelsens tilsyn efter påbud efter § 12, stk. 2 eller 3, straffes med bøde. Endvidere foreslås det at undladelse af at efterkomme styrelsens påbud efter § 12, stk. 4, kan straffes med bøde.

Erhvervsstyrelsen bemyndiges med det foreslåede stk. 2 til at fastsætte straf i form af bøde for overtrædelse af bestemmelser i regler, som udfærdiges i medfør af § 4, stk. 3 og 4, § 5, stk. 3, § 6, stk. 4, § 9, stk. 3 eller § 10, herunder for undladelse af at styrelsens påbud.

Efter det foreslåede stk. 3 kan der pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel. Bestemmelsen indebærer, at der også i regler, som udfærdiges i medfør af loven, kan fastsættes regler om, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Til § 19

Bestemmelsen fastsætter tidspunktet for lovens ikrafttræden.

I medfør af NIS-direktivets artikel 25, skal medlemsstaterne vedtage og offentliggøre de love og administrative bestemmelser, der er nødvendige for at efterkomme direktivet, senest den 9. maj 2018.

Det foreslås derfor, at loven træder i kraft den 9. maj 2018 i overensstemmelse med NIS-direktivet.

Til § 20

Til nr. 1 (fodnoten i lov om finansiel virksomhed)

Med den foreslåede ændring af fodnoten til lov om finansiel virksomhed indsættes en henvisning til, at der med denne lov foretages en gennemførelse af 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 (herefter kaldet NIS-direktivet), idet lovforslaget implementerer de dele af direktivet i lov om finansiel virksomhed, der omfatter penge- og realkreditinstitutter.

Til nr. 2 (§ 71, stk. 2, 2. pkt., i lov om finansiel virksomhed)

I medfør af § 71 i lov om finansiel skal en finansiel virksomhed have effektive former for virksomhedsstyring, herunder betryggende kontrol- og sikringsforanstaltninger på it-området.

I medfør af § 71, stk. 2, i lov om finansiel virksomhed, kan Finanstilsynet fastsætte nærmere regler om de foranstaltninger, som en finansiel virksomhed skal træffe for at have effektive former for virksomhedsstyring, herunder betryggende kontrol- og sikringsforanstaltninger på it-området. Denne bemyndigelse er bl.a. udnyttet ved bekendtgørelse nr. 1026 af 30. juni 2016 om ledelse og styring af pengeinstitutter m.fl. (herefter kaldet ledelsesbekendtgørelsen), hvoraf bekendtgørelsens bilag 5 stiller nærmere krav til it-sikkerhed.

Det følger bl.a. af bekendtgørelsens bilag 5, at bestyrelsen skal beslutte en it-sikkerhedspolitik for virksomheden, som ud fra den ønskede risikoprofil på it-området skal indeholde en overordnet stillingtagen til alle væsentlige forhold vedrørende it-sikkerheden. Hvad der er væsentligt, afhænger bl.a. af virksomhedens størrelse samt omfanget og kompleksiteten af virksomhedens it-anvendelse.

NIS-direktivets sikkerhedskrav i artikel 14, stk. 1 og 2 vurderes ikke, at række videre end den nugældende § 71 i lov om finansiel virksomhed og tilhørende ledelsesbekendtgørelse, herunder ledelsesbekendtgørelsens bilag 5. NIS-direktivets artikel 14, stk. 3 og 4, indeholder derudover også krav om, at operatører af væsentlige tjenester hurtigst muligt foretager en underretning til den kompetente myndighed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Med henblik på at implementere artikel 14, stk. 3 og 4, foreslås det derfor at udvide § 71, stk. 2, i lov om finansiel virksomhed, således at Finanstilsynet kan fastætte nærmere regler om hændelsesrapportering ved eventuelle hændelser.

Med den foreslåede indførelse af *§ 71, stk. 2, 2. pkt.*, vil Finanstilsynet i bilag 5 til ledelsesbekendtgørelsen kunne fastsætte nærmere regler for underretning om hændelsesrapportering ved eventuelle hændelser.

Med bestemmelsen gennemføres NIS-direktivets artikel 14, stk. 3, hvorefter en operatør af væsentlige tjenester hurtigst muligt skal foretage en underretning til den kompetente myndighed, af hændelser, der har væsentlig konsekvenser for kontinuiteten af de væsentlige tjenester, som virksomheden leverer.

I medfør af NIS-direktivets artikel 5, stk. 2, gælder der tre kriterier for identificering af en operatør af væsentlige tjenester. Disse kriterier er, når den pågældende virksomhed leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter, og leveringen af denne tjeneste afhænger af net- og informationssystemer, og en hændelse ville få væsentlige forstyrrende virkninger for leveringen af den nævnte tjeneste.

Endvidere fremgår det af NIS-direktivets præambel nr. 28, at med henblik på at fastslå hvorvidt en hændelse vil have en forstyrrende virkning på leveringen af en tjeneste, bør medlemsstaterne i tillæg til tværsektorielle forhold også tage højde for sektorspecifikke forhold.

I medfør af NIS-direktivets artikel 5, stk. 5, udarbejder hver medlemsstat mindst hvert andet år efter den 9. maj 2018 en liste over identificerede operatører af væsentlige tjenester, og ajourfører hvis relevant.

I medfør af den foreslåede § 307 a, skal Finanstilsynet udpege operatører af væsentlige tjenester mindst hvert andet år, ud fra de kriterier der følger af forslaget til § 307 a, stk. 2. Der henvises i øvrigt til bemærkningerne hertil.

Med den foreslåede ændring af § 71, stk. 2, 2. pkt., vil Finanstilsynet udnytte den bemyndigelsen til at fastsætte nærmere krav om indberetninger til Finanstilsynet fra et kreditinstitut, der er udpeget som operatør af væsentlige tjenester, når der er tale om hændelser, der har væsentlige konsekvenser for kontinuiteten af tjenester, og som er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.

Til nr. 3 (§ 307 a, i lov om finansiel virksomhed)

Forslaget til *§ 307 a*, gennemfører NIS-direktivets artikel 5, stk. 1-3 og stk. 5, hvorefter medlemsstaterne identificerer operatører af væsentlige tjenester ud fra, at tjenesten er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, at leveringen af tjenesten afhænger af net- og informationssystemer, og at en hændelse kan få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Det følger endvidere af direktivets artikel 5, stk. 5, at listen over identificerede operatører af væsentlige tjenester tages op til revision mindst hvert andet år og ajourføres hvis relevant.

Med den foreslåede *§ 307 a, stk. 1*, skal Finanstilsynet mindst hvert andet år udpege de operatører af markedspladser og centrale modparter (CCP'er), der er operatører af væsentlige tjenester.

Dermed skal Finanstilsynet mindst hvert andet år offentliggøre en liste over de penge- og realkreditinstitutter, der er operatører af væsentlige tjenester. Det indebærer at listen skal ajourføres løbende og mindst hvert andet år.

Med den foreslåede *§ 307 a, stk. 2*, skal Finanstilsynet i forbindelse med udpegningen efter stk. 1, lægge vægt på tre kriterier.

Finanstilsynet skal således lægge vægt på, at de penge- og realkreditinstitutter udbyder en tjeneste, som er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.

Finanstilsynet skal endvidere lægge vægt på, at de pågældende penge- og realkreditinstitutters levering af tjenesten afhænger af net- og informationssystemer.

Endelig skal Finanstilsynet lægge vægt på, at en hændelse kan få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Med den foreslåede *§ 307 a, stk. 3*, kan Finanstilsynet fastsætte nærmere regler om identificeringen af operatører af væsentlige tjenester.

I medfør af den foreslåede § 307 a, stk. 3, vil Finanstilsynet dermed kunne fastsætte nærmere regler for udpegningen efter stk. 1, herunder nærmere fastsætte hvilke kriterier der skal være opfyldt, for at et penge- eller realkreditinstitut udpeges som en operatør af væsentlige tjenester.

Bemyndigelsen i § 307 a, stk. 3, vil blive udnyttet på bekendtgørelsesniveau.

Til nr. 4 (§ 354, stk. 6, nr. 43, i lov om finansiel virksomhed)

I medfør af § 354, stk. 1, i lov om finansiel virksomhed er Finanstilsynets ansatte underlagt en særlig tavshedspligt. Finanstilsynets ansatte er således under ansvar efter straffelovens §§ 152-152 e forpligtet til at hemmeligholde fortrolige oplysninger.

§ 354, stk. 6, i lov om finansiel virksomhed fastsætter i hvilke tilfælde og til hvem Finanstilsynet kan videregive fortrolige oplysninger, uanset § 354 stk. 1.

Med lovforslaget foreslås det at indsætte et nyt *nr. 43* i § 354, stk. 6, hvorefter Finanstilsynet kan videregive oplysninger til Center for Cybersikkerhed, under forudsætning af at oplysningerne er nødvendige for dem til opfyldelse af deres lovbestemte opgaver, i deres egenskab af CSIRT/national enhed, der håndterer hændelser.

Med bestemmelsen gennemføres NIS-direktivets artikel 10, stk. 1 og 2, hvorefter den kompetente myndighed samarbejder med den enhed, der håndterer hændelser, den såkaldte CSIRT (herefter kaldet CSIRT). Det følger endvidere af direktivets artikel 1, nr. 5, at oplysninger der er fortrolige i henhold til EU-regler og nationale regler, kan udveksles med forbehold af artikel 346 i TEUF, hvis en sådan udveksling er nødvendig for anvendelsen af dette direktiv.

Med henblik på at sikre et sådant samarbejde, foreslås det at Finanstilsynet kan videregive oplysninger til Center for Cybersikkerhed, i det omfang oplysningerne er nødvendige for, at Center for Cybersikkerhedkan varetage sine opgaver som CSIRT. Det er forventningen, at Center for Cybersikkerhed, vil blive udpeget af Forsvarsministeriet som den nationale CSIRT. [Såfremt Forsvarsministeriets lovforslag om implementering af NIS-direktivet viser noget andet inden dette lovforslags vedtagelse, vil den foreslåede § 354, stk. 6, nr. 43, blive justeret i overensstemmelse hermed.]

Med den foreslåede bestemmelse sikres det bl.a., at Finanstilsynet kan samarbejde med Center for Cybersikkerhed, herunder oplyse om de eventuelle indberetninger, som penge- eller realkreditinstitutter har foretaget til Finanstilsynet. Det skal dog bemærkes, at fortroligheden følger oplysningerne hvilket indebærer, at for så vidt angår de oplysninger, som Finanstilsynet videregiver til Center for Cybersikkerhed, så indebærer videregivelsen, at Center for Cybersikkerhed omfattes af den samme skærpede tavshedspligt som Finanstilsynet efter § 354 i lov om finansiel virksomhed. Dertil kommer, at Center for Cybersikkerhed ikke må videregive disse oplysninger.

Til nr. 5 (§ 354 h i lov om finansiel virksomhed)

Forslaget til *§ 354 h* gennemfører NIS-direktivets artikel 14, stk. 6, hvorefter den kompetente myndighed kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Med den foreslåede bestemmelse vil Finanstilsynet dermed kunne offentliggøre konkrete hændelser, såfremt offentlighedens kendskab hertil er nødvendigt for at forebygge eller håndtere en igangværende hændelse. Det er Finanstilsynet, der vurderer, hvornår en given hændelse er relevant for offentligheden.

Det er endvidere Finanstilsynets vurdering om det er nødvendigt for at forebygge eller håndtere en igangværende hændelse at offentliggøre navnet på den berørte virksomhed, eller om det samme resultat kan nås med en anonymiseret offentliggørelse, som alene omfatter den konkrete hændelse. En offentliggørelse vil dog altid være afhængig af, at den berørte virksomhed er blevet hørt herom.

Til § 21

Til nr. 1 (fodnoten i lov om kapitalmarkeder)

Med den foreslåede ændring af fodnoten til lov om kapitalmarkeder indsættes en henvisning til, at der med denne lov foretages en gennemførelse af 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 (NIS-direktivet), idet lovforslaget implementerer de dele af direktivet i lov om kapitalmarkeder, der vedrører operatører af markedspladser og centrale modparter (CCP'er).

Til nr. 2 (§ 58 a i lov om kapitalmarkeder)

Forslaget til *§ 58 a, stk. 1 og 2,* gennemfører NIS-direktivets artikel 5, stk. 1-3 og stk. 5, hvorefter medlemsstaterne identificerer operatører af væsentlige tjenester ud fra, at tjenesten er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, at leveringen af tjenesten afhænger af net- og informationssystemer, og at en hændelse kan få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Det følger endvidere af direktivets artikel 5, stk. 5, at listen over identificerede operatører af væsentlige tjenester tages op til revision mindst hvert andet år og ajourføres hvis relevant.

Med den foreslåede *§ 58 a, stk. 1*, skal Finanstilsynet bestemmelse skal Finanstilsynet mindst hvert andet år udpege de operatører af markedspladser og centrale modparter (CCP'er), der er operatører af væsentlige tjenester.

Det indebærer, at Finanstilsynet mindst hvert andet år offentliggør en liste over de operatører af markedspladser og centrale modparter (CCP'er), der er operatører af væsentlige tjenester. Det indebærer at listen skal ajourføres løbende, og mindst hvert andet år.

Med den foreslåede *§ 58 a, stk. 2*, skal Finanstilsynet i forbindelse med udpegningen efter stk. 1, lægge vægt på tre kriterier.

Finanstilsynet skal således lægge vægt på, at de pågældende operatører af markedspladser og centrale modparter (CCP'er) udbyder en tjeneste, som er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.

Finanstilsynet skal endvidere lægge vægt på, at de pågældende operatører af markedspladser og centrale modparters (CCP'ers) levering af tjenesten afhænger af net- og informationssystemer.

Endelig skal Finanstilsynet lægge vægt på, at en hændelse kan få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Med den foreslåede *§ 58 a, stk. 3*, kan Finanstilsynet fastsætte nærmere regler om identificeringen af operatører af væsentlige tjenester, herunder fastsætte nærmere krav om underretning af Finanstilsynet ved en hændelse.

Med bestemmelsen gennemføres NIS-direktivets artikel 14, stk. 3, hvorefter en operatør af væsentlige tjenester hurtigst muligt skal foretage en underretning til den kompetente myndighed, af hændelser der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som virksomheden leverer.

I medfør af den foreslåede § 58 a, stk. 3, vil Finanstilsynet dermed kunne fastsætte nærmere regler for udpegningen efter stk. 1, herunder nærmere fastsætte hvilke kriterier der skal være opfyldt, for at en operatør af en markedsplads og en central modpart (CCP) udpeges som en operatør af væsentlige tjenester.

En operatør af en markedsplads kan enten være en operatør af et reguleret marked, en multilateral handelsfacilitet (MHF) eller en organiseret handels facilitet (OHF). En central modpart (CCP) er i § 3, nr. 11, defineret i artikel 2, nr. 1, i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre. Vi har i dag ingen centrale modparter i Danmark.

Bemyndigelsen i § 58 a, stk. 3, vil blive udnyttet ved en bekendtgørelse, som i medfør af det foreslåede stk. 3, endvidere vil indeholde regler om, hvornår en udpeget operatør af væsentlige tjenester skal underrette Finanstilsynet om en hændelse, herunder hvilke oplysninger underretningen skal indeholde, og hvilke kriterier virksomheden skal lægge vægt på for at fastsætte konsekvenserne af en hændelse.

En hændelse for en operatør af en markedsplads vil for eksempel kunne blive omfattet af underretningspligten, såfremt der er tale om en hændelse, der har negativ indvirkning på sikkerheden i virksomhedens net- og informationssystem, og hvor virksomheden kan blive udsat for et hacking angreb eller et svigt i it-systemet.

En anden hændelse der for eksempel vil kunne blive omfattet af underretningspligten, kan være en hændelse, der har væsentlige konsekvenser for kontinuiteten af driften af markedspladsen og den multilaterale handel med finansielle instrumenter, såsom en hændelse hvormed markedspladsens handelssystem svigter i en længere periode. Denne periode skal ses i forhold til, at der på en markedsplads bliver handlet finansielle instrumenter inden for nanosekunder, hvorfor en hændelse

kan have haft væsentlige konsekvenser for driften af handelssystemet, hvis denne blot har været i nogle minutter.

For så vidt angår en central modpart (CCP), vil et svigt i den centrale modparts (CCP'ens) interne systemer, som hindrer fortsættelsen af korrekt sikkerhedsudveksling eller den clearede transaktions rettidige gennemførsel, bl.a. være at betragte som væsentlige hændelser.

Til nr. 3 (§ 225, stk. 1, nr. 17, i lov om kapitalmarkeder)

§ 225 i lov om kapitalmarkeder fastsætter i hvilke tilfælde og til hvem Finanstilsynet kan videregive fortrolige oplysninger, uanset Finanstilsynets særlige tavshedspligt som fremgår af § 224 i lov om kapitalmarkeder.

Med lovforslaget foreslås det at indsætte et nyt *nr. 17* i § 225, hvorefter Finanstilsynet kan videregive oplysninger til Center for Cybersikkerhed, under forudsætning af at oplysningerne er nødvendige for dem til opfyldelse af deres lovbestemte opgaver, i deres egenskab af CSIRT/national enhed, der håndterer hændelser.

Med bestemmelsen gennemføres NIS-direktivets artikel 10, stk. 1 og 2, hvorefter den kompetente myndighed samarbejder med den enhed, der håndterer hændelser, den såkaldte CSIRT (herefter kaldet CSIRT).

Med henblik på at sikre et sådant samarbejde, foreslås det at Finanstilsynet kan videregive oplysninger til Center for Cybersikkerhed, i det omfang oplysningerne er nødvendige for, at Center for Cybersikkerhedkan varetage sine opgaver som CSIRT. Det er forventningen, at Center for Cybersikkerhed, vil blive udpeget af Forsvarsministeriet som den nationale CSIRT. [Såfremt Forsvarsministeriets lovforslag om implementering af NIS-direktivet viser noget andet inden dette lovforslags vedtagelse, vil den foreslåede § 354, stk. 6, nr. 43, blive justeret i overensstemmelse hermed.]

Med den foreslåede bestemmelse sikres det bl.a., at Finanstilsynet kan samarbejde med Center for Cybersikkerhed, herunder oplyse om de eventuelle indberetninger, som enten operatører af markedspladser eller centrale modparter (CCP'er) har foretaget til Finanstilsynet, jf. lovforslagets § 58 a, stk. 1.

Til nr. 4 (§ 236 a i lov om kapitalmarkeder)

Forslaget til *§ 236 a* gennemfører NIS-direktivets artikel 14, stk. 6, hvorefter den kompetente myndighed kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Med den foreslåede bestemmelse vil Finanstilsynet dermed kunne offentliggøre konkrete hændelser, såfremt offentlighedens kendskab hertil er nødvendigt for at forebygge eller håndtere en igangværende hændelse. Det er Finanstilsynet, der vurderer, hvornår en given hændelse er relevant for offentligheden.

Det er endvidere Finanstilsynets vurdering om det er nødvendigt for at forebygge eller håndtere en igangværende hændelse at offentliggøre navnet på den berørte virksomhed, eller om det samme

resultat kan nås med en anonymiseret offentliggørelse, som alene omfatter den konkrete hændelse. En offentliggørelse vil dog altid være afhængig af, at den berørte virksomhed er blevet hørt herom.

Til § 22

Med § 22 fastlægges lovens territoriale gyldighed.

Det foreslås med *stk. 1*, at loven ikke skal gælde for Færøerne og Grønland.

Det foreslås imidlertid med *stk. 2*, at loven ved kongelig anordning kan sættes helt eller delvis i kraft for Færøerne og Grønland med de ændringer, som de færøske og grønlandske forhold tilsiger.