EUROPA-
KOMMISSIONEN

Bruxelles, den 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

BILAG

til

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Fuld udnyttelse af NIS – mod en effektiv gennemførelse af direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen

INDHOLDSFORTEGNELSE

BILAG

1. Indledning

Dette bilag har til formål at bidrage til en effektiv anvendelse, gennemførelse og håndhævelse af direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen[1] (i det følgende benævnt "NIS-direktivet" eller "direktivet") og hjælpe medlemsstaterne med at sikre, at EU-retten anvendes effektivt. Bilagets specifikke målsætninger er nærmere bestemt: a) at give de nationale myndigheder større klarhed om de af direktivets forpligtelser, der gælder for sådanne myndigheder, b) at sikre effektiv håndhævelse af de af direktivets bestemmelser, der gælder for enheder, som er underlagt sikkerhedskrav og underretningspligt, og c) generelt at bidrage til at skabe retssikkerhed for alle relevante aktører.

Bilaget giver i den forbindelse vejledning inden for følgende aspekter, som er afgørende for at nå NIS-direktivets målsætning, nemlig at sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele EU, der understøtter vores samfund og økonomi:

- medlemsstaternes forpligtelse til at vedtage en national strategi for sikkerhed i net- og informationssystemer (afsnit 2)
- etablering af nationale kompetente myndigheder, centrale kontaktpunkter og enheder, der håndterer IT-sikkerhedshændelser (afsnit 3)
- de sikkerhedskrav og den underretningspligt, som gælder for operatører af væsentlige tjenester og udbydere af digitale tjenester (afsnit 4), og
- forholdet mellem NIS-direktivet og anden lovgivning (afsnit 5).

Kommissionen har i sit forberedende arbejde med denne vejledning brugt input og analyser, som blev indsamlet under forberedelsen af direktivet, samt input fra Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) og fra samarbejdsgruppen. Den har også trukket på erfaringer fra specifikke medlemsstater. Hvor det er passende, har Kommissionen taget højde for vejledende principper for fortolkning af EU-retten, nemlig NIS-direktivets ordlyd, kontekst og målsætninger. Eftersom direktivet ikke er blevet gennemført i national ret, har Den Europæiske Unions Domstol eller nationale domstole endnu ikke afsagt nogen domme. Det er følgelig ikke muligt at bruge retspraksis som vejledning.

Ved at samle disse oplysninger i et enkelt dokument kan medlemsstaterne få et godt overblik over direktivet og tage oplysningerne med i betragtning, når de udarbejder deres nationale lovgivning. Samtidig understreger Kommissionen, at dette bilag ikke er bindende og ikke har til formål at fastsætte nye regler. Den Europæiske Unions Domstol har endelig kompetence til at fortolke EU-retten.

[1] 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. Direktivet trådte i kraft den 8. august 2016.

2. National strategi for sikkerheden i net- og informationssystemer

Ifølge artikel 7 i NIS-direktivet skal hver medlemsstat vedtage en national strategi for sikkerheden i net- og informationssystemer, der kan betragtes som ækvivalent til begrebet national cybersikkerhedsstrategi. Formålet med en national strategi er at definere strategiske mål og passende politiske og lovgivningsmæssige foranstaltninger vedrørende cybersikkerhed. Konceptet nationale cybersikkerhedsstrategier er meget udbredt både internationalt og i Europa, navnlig inden for rammerne af ENISA's arbejde med medlemsstaterne om nationale strategier, der for nyligt resulterede i en ajourført udgave af vejledningen i god praksis inden for nationale cybersikkerhedsstrategier[2].

I dette afsnit beskriver Kommissionen, hvordan NIS-direktivet øger medlemsstaternes beredskab ved at kræve, at der skal findes solide nationale strategier for sikkerhed i net- og informationssystemer (artikel 7). Afsnittet handler om a) strategiens anvendelsesområde og b) indholdet og proceduren for vedtagelse.

Som uddybet nedenfor er den korrekte gennemførelse af NIS-direktivets artikel 7 afgørende for at nå direktivets målsætninger, og det forudsætter tildeling af tilstrækkelige finansielle og menneskelige ressourcer til formålet.

2.1. Den nationale strategis anvendelsesområde

Ifølge ordlyden i artikel 7 gælder forpligtelsen til at vedtage nationale cybersikkerhedsstrategier kun for de "i bilag II omhandlede sektorer" (dvs. energi, transport, bankvæsen, finansmarked, sundhed, drikkevandsforsyning og distribution samt digital infrastruktur) og "de i bilag III omhandlede tjenester" (onlinemarkedsplads, onlinesøgemaskiner og cloud computing-tjenester).

Direktivets artikel 3 fastsætter specifikt princippet om minimumsharmonisering, ifølge hvilket medlemsstaterne kan vedtage eller bibeholde bestemmelser, som har til formål at nå et højere sikkerhedsniveau for net- og informationssystemer. Anvendelsen af dette princip på forpligtelsen til at vedtage nationale cybersikkerhedsstrategier gør det muligt for medlemsstaterne at inkludere flere sektorer og tjenester end dem, der er omfattet af direktivets bilag II og III.

I Kommissionens optik og set i lyset af målsætningen med NIS-direktivet, som er at opnå et højt fælles sikkerhedsniveau for net- og informationssystemer i Unionen[3], ville det være ønskeligt at udvikle nationale strategier, som involverer alle relevante dimensioner af samfundet og økonomien og ikke blot de sektorer og digitale tjenester, der er omfattet af henholdsvis bilag II og III i NIS-direktivet. Dette er i tråd med international bedste praksis (se vejledningen fra Den Internationale Telekommunikationsunion (ITU) og OECD's analyse, som der henvises til senere) og NIS-direktivet.

[2] ENISA, *National Cyber-Security Strategy Good Practice* 2016. Findes på https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
[3] Jf. artikel 1, stk. 1.

Som forklaret mere indgående nedenfor er dette navnlig tilfældet med hensyn til offentlige forvaltninger med ansvar for andre sektorer og tjenester end dem, der er oplistet i direktivets bilag II og III. Offentlige forvaltninger kan behandle følsomme oplysninger, hvilket begrunder, at de også bør omfattes af de nationale cybersikkerhedsstrategier og forvaltningsplaner, som forhindrer lækager og sikrer tilstrækkelig beskyttelse af nævnte oplysninger.

2.2. Indhold og procedure for vedtagelse af nationale strategier

Ifølge artikel 7 i NIS-direktivet skal en national cybersikkerhedsstrategi mindst omfatte følgende:

i) målene og de prioriterede områder i den nationale strategi for sikkerhed i net- og informationssystemer
ii) en styringsmæssige ramme for at nå målene og de prioriterede områder i den nationale strategi
iii) fastlæggelse af foranstaltninger vedrørende beredskab, reaktion og genopretning, herunder samarbejde mellem den offentlige og den private sektor
iv) en angivelse af relevante teoretiske og praktiske uddannelsesprogrammer og oplysningsprogrammer
v) en angivelse af forsknings- og udviklingsplaner
vi) en risikovurderingsplan til brug ved identifikation af risici og
vii) en liste over de forskellige aktører, der er involveret i gennemførelsen af strategien.

Hverken artikel 7 eller den tilsvarende betragtning 29 specificerer kravene for vedtagelse af en national cybersikkerhedsstrategi eller giver nærmere detaljer om strategiens indhold. Hvad angår fremskridt og yderligere elementer relateret til den nationale cybersikkerhedsstrategis indhold er det Kommissionens opfattelse, at nedenstående tilgang er en passende måde at vedtage en national cybersikkerhedsstrategi på. Denne baseres på en analyse af medlemsstaterne og tredjelandenes erfaringer med, hvordan medlemsstaterne har udviklet deres egne strategier. En yderligere informationskilde er ENISA's uddannelsesværktøj vedrørende nationale cybersikkerhedsstrategier, der er tilgængeligt som videoklip og medier til downloading på ENISA's websted[4].

2.3. Processer og problemer, der skal håndteres

Processen med udarbejdelse og efterfølgende vedtagelse af en national strategi er kompleks og mangeartet, og den kræver et vedvarende samarbejde med cybersikkerhedseksperter, civilsamfundet og den nationale politiske proces for at være effektiv og vellykket. Politisk opbakning og støtte fra de øverste administrative niveauer, dvs. som minimum ministerniveau eller tilsvarende, er en forudsætning. Med henblik på at nå en vellykket vedtagelse af en national cybersikkerhedsstrategi kan følgende proces i fem trin (se figur 1) tages i betragtning:

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

Første trin – **Opstilling af vejledende principper og strategiske mål, der følger af strategien**

Først og fremmest bør de nationale kompetente myndigheder definere nogle nøgleelementer, som skal inkluderes i den nationale cybersikkerhedsstrategi, dvs. hvad der er de ønskede resultater, jf. direktivets artikel 7, stk. 1, litra a) ("målene og de prioriterede områder"), hvordan sådanne resultater supplerer nationale sociale og økonomiske politikker, og hvorvidt de er kompatible med de privilegier og forpligtelser, der følger af at være en medlemsstat i Den Europæiske Union. Målsætningerne skal være specifikke, målbare, opnåelige, relevante og tidsbestemte. Et illustrativt eksempel er følgende: *"Vi vil sikre, at denne* [tidsbestemte] *strategi er baseret på stramme og omfattende måleenheder, som vi bruger til at måle fremskridtene hen mod de resultater, vi skal nå"*[5].

Ovenstående indbefatter også en politisk vurdering af, hvorvidt der kan opnås et betragteligt budget til finansiering af strategiens gennemførelse. Det indebærer også en beskrivelse af strategiens tilsigtede anvendelsesområde og de forskellige kategorier af interessenter fra offentlige og private sektorer, som bør inddrages i udarbejdelsen af diverse mål og foranstaltninger.

Det første trin vil kunne nås ved at afholde målrettede workshops med deltagelse af ledende embedsmænd fra ministerierne og politikere og under ledelse af cyberspecialister, der kan sætte fokus på, hvilke konsekvenser manglende eller svag cybersikkerhed har for en moderne digital økonomi og et moderne digitalt samfund.

Andet trin – **Udvikling af strategiens indhold**

Strategien bør indeholde understøttende foranstaltninger, tidsbaserede tiltag og nøgleresultatindikatorer til brug ved efterfølgende evaluering, finjustering og forbedring efter en fastsat gennemførelsesperiode. Foranstaltningerne bør støtte den målsætning, de prioriteter og de resultater, der er fremsat som vejledende principper. De skal omfatte understøttende foranstaltninger som fastsat i artikel 7, stk. 1, litra c), i NIS-direktivet.

Det anbefales, at der oprettes en styringsgruppe ledet af det vigtigste ministerium med henblik på at styre udarbejdelsen og fremme input. Dette kan nås gennem en række redaktionsgrupper bestående af relevante embedsmænd og eksperter, som behandler vigtige generiske temaer som f.eks. risikovurdering, beredskabsplanlægning, hændelsesstyring, kompetenceudvikling, oplysning, forskning, industriel udvikling m.m. Hver sektor vil særskilt blive opfordret til at vurdere virkningerne af deres inklusion, herunder tildelingen af ressourcer, og til at involvere de identificerede operatører af væsentlige tjenester og leverandører af væsentlige digitale tjenester i fastsættelsen af prioriteter og fremlæggelse af forslag under udarbejdelsen. Involvering af interessenter fra sektorerne er også afgørende i betragtning af behovet for at sikre en harmoniseret gennemførelse af direktivet på tværs af forskellige sektorer, alt imens der tages hensyn til sektorernes særlige karakteristika.

[5] Uddrag af Det Forenede Kongeriges nationale cybersikkerhedsstrategi for 2016-2021, s. 67.

Tredje trin – **Udvikling af en styringsmæssig ramme**

For at være effektiv bør den styringsmæssige ramme tage udgangspunkt i centrale interessenter, prioriteter identificeret under udarbejdelsen, begrænsninger samt de nationale administrative og politiske strukturers kontekst. Det ville være ønskeligt, at der rapporteres direkte til det politiske niveau, at der inden for rammen kan træffes beslutninger og fordeles ressourcer, og at cybersikkerhedseksperter og interessenter fra industrien kommer med input. I artikel 7, stk. 1, litra b), i NIS-direktivet henvises der til den styringsmæssige ramme, ligesom de *"statslige organers og andre relevante aktørers roller og ansvar"* fastsættes specifikt.

Fjerde trin – **Samling og gennemgang af udkastet til strategi**

Udkastet til strategi bør på dette trin samles og gennemgås ved at analysere de stærke sider, svage sider, muligheder og trusler (SWOT-analyse), som kan afdække, hvorvidt det er nødvendigt at revidere indholdet. Høringen af interessenter bør finde sted efter den interne gennemgang. Det er vigtigt ligeledes at foretage en offentlig høring for at understrege vigtigheden af den foreslåede strategi, modtage input fra alle mulige kilder og søge støtte til den finansiering, der er nødvendig for efterfølgende at føre strategien ud i livet.

Femte trin – **Formel vedtagelse**

Dette sidste trin indebærer formel vedtagelse på politisk niveau med et tilstrækkeligt budget, der afspejler den betydning, som de berørte medlemsstater tillægger cybersikkerhed. For at nå målsætningerne med NIS-direktivet opfordrer Kommissionen medlemsstaterne til at stille oplysninger om budgettet til rådighed, når de meddeler Kommissionen deres nationale strategier i henhold til artikel 7, stk. 3. Forpligtelser vedrørende budgettet og de nødvendige menneskelige ressourcer er altafgørende for en effektiv gennemførelse af strategien og direktivet. Eftersom cybersikkerhed er et ret nyt og hurtigt voksende område for offentlig politik, er der i de fleste tilfælde brug for nye investeringer, også selv om de offentlige finansers generelle situation kræver nedskæringer og besparelser.

Forskellige offentlige og akademiske kilder yder rådgivning om fremskridtene og indholdet af de nationale strategier, f.eks. ENISA[6], ITU[7], OECD[8], det globale forum for IT-ekspertise og Oxford universitet[9].

---

[6] ENISA, *National Cyber-Security Strategy Good Practice* 2016. Findes på https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[7] ITU, *National Cybersecurity Strategy Guide* (2011). Findes på http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.
ITU vil i 2017 ligeledes offentliggøre en værktøjskasse for nationale cybersikkerhedsstrategier (se præsentation på http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

[8] OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (2012). Findes på http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

2.4. Konkrete skridt, som medlemsstaterne skal tage før fristen for gennemførelse udløber

Forud for vedtagelsen af direktivet havde næsten alle medlemsstater[10] allerede offentliggjort dokumenter, der er angivet som nationale cybersikkerhedsstrategier. I dette bilags afsnit 6 oplistes de strategier, der p.t. findes i medlemsstaterne[11]. De omfatter normalt strategiske principper, vejledninger og målsætninger samt i visse tilfælde specifikke foranstaltninger til afbødning af risici i forbindelse med cybersikkerhed.

Eftersom visse af strategierne blev vedtaget forud for vedtagelsen af NIS-direktivet, indeholder de ikke nødvendigvis alle de i artikel 7 nævnte elementer. For at sikre korrekt gennemførelse er medlemsstaterne nødt til at foretage en mangelanalyse ved at kortlægge indholdet af deres nationale cybersikkerhedsstrategier ud fra de syv særskilte krav i artikel 7 for alle de sektorer, der er omfattet af direktivets bilag II, og alle de tjenester, der er omfattet af bilag III. Der kan efterfølgende tages hånd om de konstaterede mangler gennem en revision af de eksisterende nationale cybersikkerhedsstrategier eller ved at træffe afgørelse om en fuldstændig revision af principperne i de nationale cybersikkerhedsstrategier. Ovenstående retningslinjer for processen med vedtagelse af nationale cybersikkerhedsstrategier er også relevant for revision og ajourføring af eksisterende strategier.

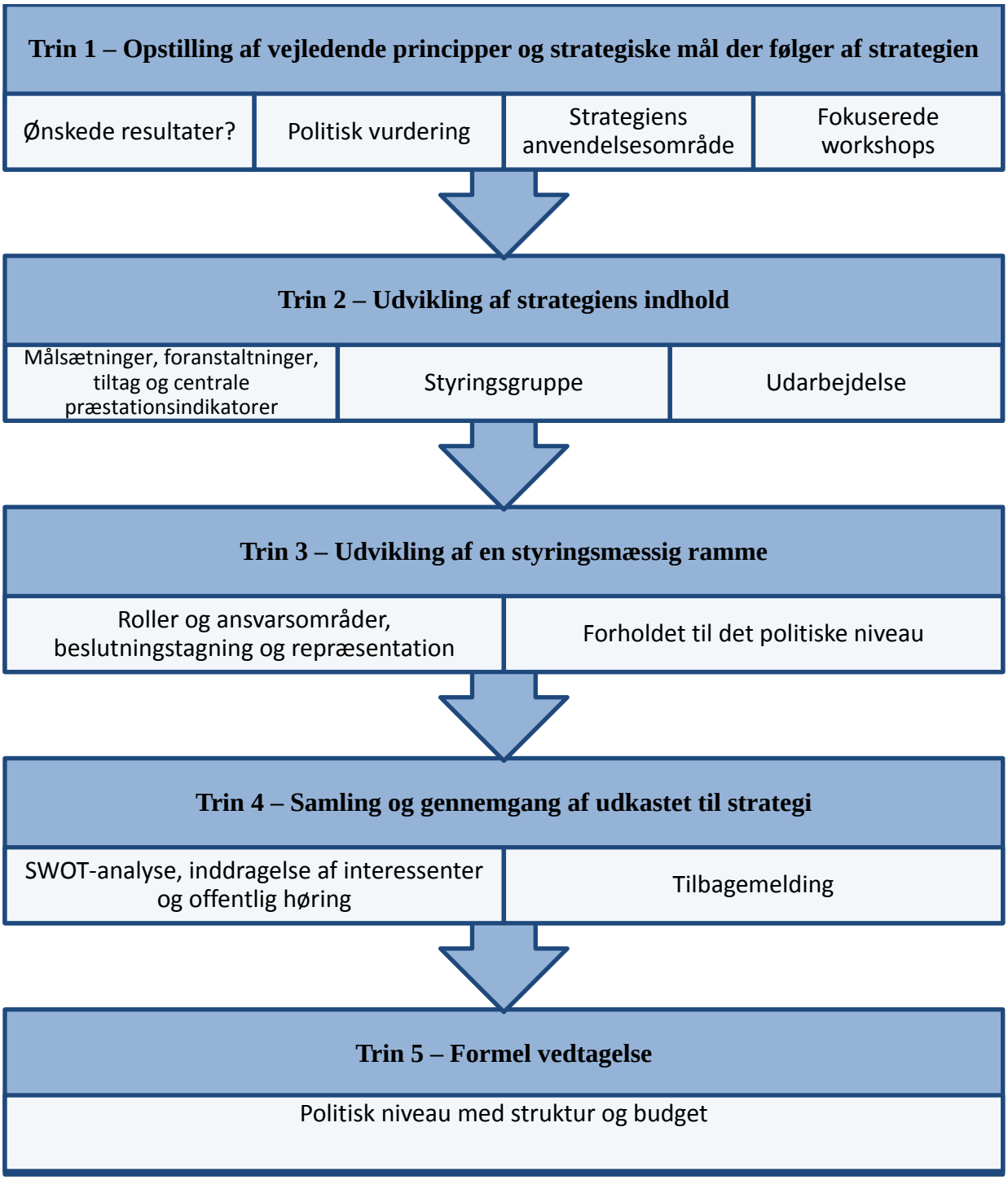
---

[9] Global Cyber Security Capacity Centre and University of Oxford, Global Cyber *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition* (2016). Findes på https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf.

[10] Bortset fra Grækenland, hvor en national cybersikkerhedsstrategi har været under udarbejdelse siden 2014 (se https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Disse oplysninger er baseret på den oversigt over nationale cybersikkerhedsstrategier, der findes på ENISA's websted https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

Figur 1: Fem trin mod vedtagelsen af nationale cybersikkerhedsstrategier



3. NIS-direktivet: Nationale kompetente myndigheder, fælles kontaktpunkter og enheder, der håndterer IT-sikkerhedshændelser

Ifølge artikel 8, stk. 1, skal medlemsstaterne udpege en eller flere nationale kompetente myndigheder, som mindst omfatter de i direktivets bilag II omhandlede sektorer og de i bilag III omhandlede tjenester, og som har til opgave at føre tilsyn med anvendelsen af direktivet. Medlemsstaterne kan tildele en eller flere eksisterende myndigheder denne rolle.

I afsnittet fokuseres der på, hvordan NIS-direktivet øger medlemsstaternes beredskab ved at kræve, at de har effektive nationale kompetente myndigheder og enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er). Mere præcist handler afsnittet om forpligtelsen til at udpege nationale kompetente myndigheder, herunder de centrale kontaktpunkters rolle. Afsnittet omhandler tre emner: a) mulige nationale forvaltningsstrukturer (f.eks. centraliserede, decentraliserede modeller m.m.) og andre krav, b) de centrale kontaktpunkters rolle og c) enheder, der håndterer IT-sikkerhedshændelser.

3.1. Myndighedernes art

Artikel 8 i NIS-direktivet kræver, at medlemsstaterne skal udpege nationale kompetente myndigheder for sikkerheden i net- og informationssystemer, mens det tydeligt fremhæves, at de kan tildele *"en eller flere eksisterende myndigheder"* denne rolle. I direktivets betragtning 30 forklares dette politikvalg således: *"I betragtning af forskellene mellem nationale forvaltningsstrukturer og med henblik på at sikre allerede eksisterende sektorforanstaltninger eller Unionens tilsyns- og kontrolorganer og undgå overlapninger bør medlemsstaterne kunne udpege mere end én national kompetent myndighed med ansvar for udførelsen af de opgaver, som er knyttet til sikkerheden i net- og informationssystemer hos operatører af væsentlige tjenester og udbydere af digitale tjenester i henhold til dette direktiv."*

Medlemsstaterne kan således frit udpege en central myndighed, der håndterer samtlige sektorer og tjenester, der er omfattet af direktivet, eller flere forskellige myndigheder afhængig af, hvilken type sektor der er tale om.

Når medlemsstaterne beslutter, hvad de skal gøre, kan de trække på erfaringerne fra de nationale tilgange inden for rammerne af den eksisterende lovgivning om beskyttelse af kritisk informationsinfrastruktur. Som beskrevet i tabel 1 kan medlemsstaterne hvad angår beskyttelse af kritisk informationsinfrastruktur vælge enten en centraliseret eller en decentraliseret tilgang, når det drejer sig om at tildele kompetencerne på nationalt niveau. De nationale eksempler nævnt her tjener kun til illustration og har til formål at gøre medlemsstaterne opmærksomme på eksisterende organisatoriske rammer. Kommissionen antyder således ikke, at den model, som de pågældende lande bruger til beskyttelse af kritisk informationsinfrastruktur, nødvendigvis bør anvendes til gennemførelse af NIS-direktivet.

Medlemsstaterne kan også vælge forskellige hybridløsninger med elementer fra både centraliserede og decentraliserede tilgange. Valget kan træffes i overensstemmelse med tidligere nationale forvaltningsordninger for de forskellige sektorer og tjenester, der er omfattet af direktivet, eller med nye ordninger fastlagt af de pågældende myndigheder og relevante interessenter, der er identificeret som operatører af væsentlige tjenester og udbydere af digitale tjenester. Særlig ekspertise på cybersikkerhedsområdet, overvejelser om ressourcer, forholdet mellem interessenter og nationale interesser (f.eks. økonomisk udvikling, offentlig sikkerhed m.m.) kan ligeledes være væsentlige faktorer, der begrunder medlemsstaternes valg.

3.2 Offentliggørelse og yderligere relevante aspekter

Ifølge artikel 8, stk. 7, skal medlemsstaterne underrette Kommissionen om udpegelsen af de nationale kompetente myndigheder og disses opgaver. Dette skal ske, inden fristen for gennemførelse udløber.

Ifølge artikel 15 og 17 i NIS-direktivet skal medlemsstaterne sikre, at de kompetente myndigheder har de nødvendige beføjelser og midler til at udføre de i artiklerne fastsatte opgaver.

Derudover skal udpegelsen af særlige enheder som nationale kompetente myndigheder offentliggøres. Direktivet præciserer ikke, hvordan en sådan offentliggørelse skal finde sted. Eftersom målsætningen med dette krav er at nå et højt niveau af kendskab blandt de aktører, der er omfattet af NIS, og den brede offentlighed, og med udgangspunkt i de erfaringer, der er høstet inden for andre sektorer (telekommunikation, bankvæsen, lægevæsen), mener Kommissionen, at offentliggørelse f.eks. kan ske ved hjælp af en bredt annonceret portal.

Ifølge artikel 8, stk. 5, i NIS-direktivet skal sådanne myndigheder have "tilstrækkelige ressourcer" til at kunne udføre de opgaver, de pålægges i medfør af direktivet.

Tabel 1: Nationale tilgange til beskyttelse af kritisk informationsinfrastruktur

I 2016 offentliggjorde ENISA en undersøgelse[12] om de forskellige tilgange, medlemsstaterne har til beskyttelse af kritiske informationsinfrastrukturer. Der er to profiler vedrørende styring af beskyttelsen af kritisk informationsinfrastruktur i medlemsstaterne, som kan anvendes i forbindelse med gennemførelse af NIS-direktivet.

Profil 1: Decentraliseret tilgang – adskillige sektorbaserede myndigheder er kompetente for specifikke sektorer og tjenester som nævnt i direktivets bilag II og III

Den decentraliserede tilgang er karakteriseret ved:

(i) Nærhedsprincippet
(ii) Tæt samarbejde mellem offentlige organer
(iii)Sektorspecifik lovgivning

Nærhedsprincippet

I stedet for at oprette eller udpege et enkelt organ med overordnet ansvar følger den decentraliserede tilgang nærhedsprincippet. Det betyder, at ansvaret for gennemførelse ligger hos en sektorspecifik myndighed, som er den, der bedst forstår den lokale sektor, og som har et allerede etableret forhold til interessenterne. I henhold til dette princip træffes afgørelserne af det organ, som er tættest på dem, der bliver påvirket.

Tæt samarbejde mellem offentlige organer

Fordi der er mange forskellige offentlige organer involveret i beskyttelsen af kritiske informationsinfrastrukturer, har mange medlemsstater udviklet samarbejdsordninger med henblik på at koordinere de forskellige myndigheders arbejde og indsats. Disse samarbejdsordninger kan have form af uformelle netværk eller mere institutionaliserede fora eller foranstaltninger. Disse samarbejdsordninger tjener imidlertid kun til udveksling af information og koordinering mellem forskellige offentlige organer, og har ingen beføjelser.

Sektorspecifik lovgivning

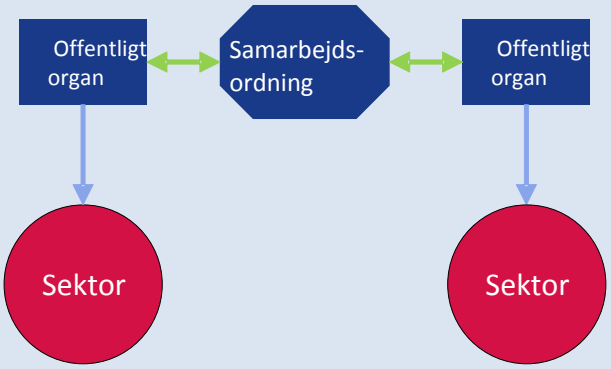
De lande, som følger en decentraliseret tilgang på tværs af kritiske sektorer, afstår ofte fra at lovgive om beskyttelsen af kritiske informationsinfrastrukturer. Vedtagelsen af love og bestemmelser forbliver i stedet sektorspecifik og kan derfor variere kraftigt mellem sektorerne. Denne tilgang har den fordel, at NIS-relaterede foranstaltninger tilpasses eksisterende sektorbaseret lovgivning, således at sektorens accept øges, og den pågældende myndigheds håndhævelse bliver mere effektiv.

Ved en ren decentraliseret tilgang er der en betydelig risiko for begrænset sammenhæng i anvendelsen af direktivet på tværs af diverse sektorer og tjenester. Direktivet giver her mulighed for et centralt kontaktpunkt, der fungerer som bindeled i grænseoverskridende

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (2016). Findes på https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis.

spørgsmål. Den pågældende medlemsstat vil også kunne give kontaktpunktet til opgave at sikre intern koordinering og internt samarbejde mellem flere nationale kompetente myndigheder, jf. direktivets artikel 10.

Figur 2 – decentraliseret tilgang



Eksempler på den decentraliserede tilgang

Sverige er et godt eksempel på et land, som anvender en decentraliseret tilgang til beskyttelsen af kritiske informationsinfrastrukturer. Landet anvender et "systemperspektiv", hvilket betyder, at de vigtigste opgaver i forbindelse med beskyttelse af kritisk informationsinfrastruktur såsom identificering af væsentlige tjenester og kritiske infrastrukturer, koordinering af og støtte til operatører, reguleringsopgaver såvel som beredskabsforanstaltninger er de forskellige organers og kommuners ansvar. Blandt disse organer er det svenske civile beredskabsagentur (Myndigheten för samhällsskydd och beredskap (MSB)), den svenske post- og telestyrelse (PTS) og adskillige svenske forsvars- og retshåndhævelsesorganer samt militære organer.

Med henblik på at koordinere tiltagene mellem de forskellige organer og offentlige enheder har den svenske regering etableret et samarbejdsnetværk bestående af myndigheder "med særligt ansvar for samfundets informationssikkerhed". Den svenske samarbejdsgruppe, Samverkansgruppen för informationssäkerhet (SAMFI), består af repræsentanter fra de forskellige myndigheder og mødes flere gange om året for at drøfte emner vedørende national informationssikkerhed. SAMFI's fokus er primært på de politisk-strategiske områder og dækker bl.a. tekniske spørgsmål og standardisering, national og international udvikling på informationssikkerhedsområdet samt styring og forebyggelse af IT-hændelser (Myndigheten för samhällsskydd och beredskap (MSB) 2015).

Sverige har ikke offentliggjort nogen central lovgivning om beskyttelse af kritisk informationsinfrastruktur, som gælder for operatører af kritisk informationsinfrastruktur på tværs af sektorer. Vedtagelsen af lovgivning med forpligtelser for virksomheder inden for specifikke sektorer er i stedet de respektive offentlige myndigheders ansvar. MSB har således ret til at udstede bestemmelser for regeringsmyndigheder på informationssikkerhedsområdet,

mens PTS på grundlag af afledt ret kan pålægge operatører at gennemføre visse tekniske eller organisatoriske sikkerhedsforanstaltninger.

Et andet eksempel på et land med denne profil er Irland. Irland følger en "nærhedsprincipsdoktrin", hvor hvert ministerium er ansvarligt for identificering af kritisk informationsinfrastruktur og risikovurdering inden for sit eget område. Derudover er der ikke indført nogen særlige bestemmelser om beskyttelse af kritisk informationsinfrastruktur på nationalt niveau. Lovgivningen forbliver sektorbestemt og eksisterer primært inden for energi- og telekommunikationssektoren (2015). Andre eksempler er Østrig, Cypern og Finland.

Profil 2: Centraliseret tilgang – en central myndighed er kompetent inden for alle sektorer og tjenester som nævnt i direktivets bilag II og III

Den centraliserede tilgang er karakteriseret ved:

i) En central myndighed på tværs af sektorer
ii) Omfattende lovgivning

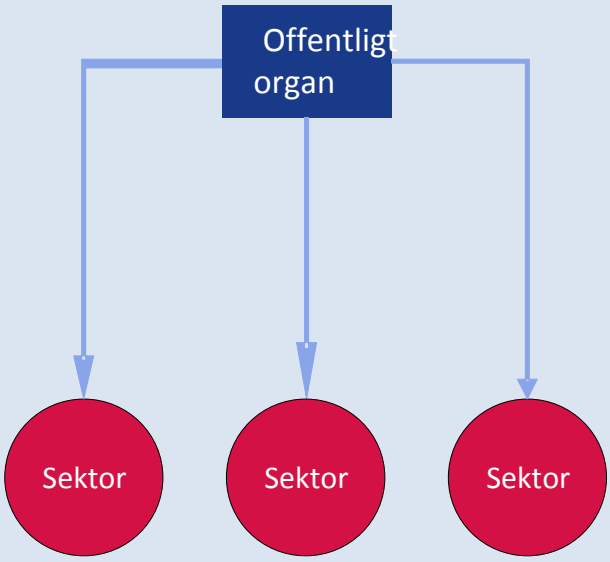
Central myndighed på tværs af sektorer

Medlemsstater med en centraliseret tilgang har etableret myndigheder med ansvar og brede kompetencer for flere eller samtlige sektorer eller har udvidet de eksisterende myndigheders beføjelser. Disse primære myndigheder med ansvar for beskyttelse af kritisk informationsinfrastruktur kombinerer forskellige opgaver som eksempelvis beredskabsplanlægning, styring af nødsituationer, reguleringsopgaver og støtte til private operatører. I mange tilfælde er nationale eller statslige CSIRT'er del af den myndighed, der har det primære ansvar for beskyttelse af kritisk informationsinfrastruktur. En central myndighed har sandsynligvis større ekspertise inden for cybersikkerhed end flere sektorielle myndigheder grundet den generelle mangel på færdigheder inden for cybersikkerhed.

Omfattende lovgivning

En omfattende lovgivning medfører både krav og forpligtelser for alle operatører af kritiske informationsinfrastrukturer i alle sektorer. Dette kan nås via nye, omfattende love eller supplering af eksisterende sektorspecifik lovgivning. Denne tilgang vil fremme en konsekvent anvendelse af NIS-direktivet på tværs af alle omfattede sektorer og tjenester. Dermed undgås den risiko for huller i gennemførelsen, som kan opstå, når flere myndigheder har specifikke kompetenceområder.

Figur 3 – centraliseret tilgang



Eksempler på den centraliserede tilgang

Frankrig er et godt eksempel på en EU-medlemsstat med en centraliseret tilgang. Det franske Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) blev i 2011 udpeget som primær national myndighed med ansvar for beskyttelse af informationssystemer. ANSSI spiller en stærk tilsynsførende rolle for "væsentlige operatører": Organet kan beordre de væsentlige operatører at overholde sikkerhedsforanstaltninger og har beføjelser til at foretage sikkerhedsrevision af dem. Derudover er organet det centrale kontaktpunkt for de væsentlige operatører, som er forpligtet til at indberette sikkerhedshændelser til organet.

I tilfælde af sikkerhedshændelser fungerer ANSSI som beredskabsorgan i forbindelse med beskyttelse af kritisk informationsinfrastruktur, og det beslutter, hvilke foranstaltninger operatørerne skal træffe for at tackle krisen. Regeringens tiltag koordineres med ANSSI's operationscenter. Sporing af trusler og håndtering af hændelser på operationelt niveau foretages af CERT-FR, som er en del af ANSSI.

Frankrig har opstillet en omfattende lovramme for beskyttelsen af kritisk informationsinfrastruktur. I 2006 gav premierministeren ordre til at oprette en liste over sektorer med kritisk infrastruktur. Regeringen har med udgangspunkt i denne liste, som omfatter tolv meget vigtige sektorer, defineret omkring 250 væsentlige operatører. I 2013 blev

loven om militær programmering[13] offentliggjort. Heri fastsættes forskellige forpligtelser for de væsentlige operatører såsom indberetning af hændelser og gennemførelse af sikkerhedsforanstaltninger. Disse krav er obligatoriske for alle væsentlige operatører i alle sektorer (det franske senat 2013).

3.3. NIS-direktivet, artikel 9: Enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)

I henhold til artikel 9 skal medlemsstaterne udpege en eller flere CSIRT'er, som er ansvarlige for at håndtere hændelser og risici for de sektorer, der er oplistet i NIS-direktivets bilag II, og de tjenester, der er oplistet i samme direktivs bilag III. Under hensyntagen til det krav om minimumsharmonisering, der er fastsat i direktivets artikel 3, kan medlemsstaterne frit benytte CSIRT'erne til andre sektorer, der ikke er omfattet af direktivet, såsom offentlige forvaltninger.

Medlemsstaterne kan vælge at oprette en CSIRT som en del af den nationale kompetente myndighed[14].

3.4. Opgaver og krav

Opgaverne for de udpegede CSIRT'er, der er oplistet i bilag til NIS-direktivet, omfatter følgende:

- monitorering af hændelser på nationalt plan
- tidlig varsling, advarsler, meddelelser og formidling af information til relevante interessenter om risici og hændelser
- håndtering af hændelser
- udarbejdelse af dynamiske risiko- og hændelsesanalyser og situationsrapporter, og
- deltagelse i netværket af nationale CSIRT'er (CSIRT-netværket) som oprettet ved artikel 12.

Specifikke yderligere opgaver er fastsat i artikel 14, stk. 3, 5 og 6, samt artikel 16, stk. 3, 6 og 7, hvad angår underretning om hændelser, hvis en medlemsstat beslutter, at CSIRT'en som supplement til eller i stedet for nationale kompetente myndigheder kan varetage sådanne opgaver.

[13] La loi de programmation militaire.
[14] Jf. artikel 9, stk. 1, sidste punktum.

Ved gennemførelse af direktivet har medlemsstaterne flere muligheder hvad angår CSIRT'ers rolle i forbindelse med underretningspligten. Direkte, obligatorisk rapportering til CSIRT'erne er mulig og har bl.a. administrativ effektivitet som fordel. Alternativt kan medlemsstaterne vælge direkte rapportering til de nationale kompetente myndigheder, hvor CSIRT'erne har adgang til de indrapporterede oplysninger. CSIRT'er er i sidste ende interesseret i at løse problemer med hensyn til at forhindre, opdage, reagere på og afbøde virkningerne af cyberhændelser (herunder hændelser, som ikke er afgørende for den obligatoriske indberetning) i samarbejde med deres interessenter, mens kontrol med regeloverholdelsen sorterer under de nationale kompetente myndigheder.

Ifølge artikel 9, stk. 3, i direktivet skal medlemsstaterne ligeledes sikre, at CSIRT'erne har adgang til sikker og robust kommunikations- og informationsinfrastruktur.

Ifølge artikel 9, stk. 4, i direktivet skal medlemsstaterne oplyse Kommissionen om de udpegede CSIRT'ers kompetenceområde og de vigtigste elementer i procedurerne for håndtering af hændelser.

Kravene til de CSIRT'er, som udpeges af medlemsstaterne, er fastsat i bilag I til NIS-direktivet. En CSIRT skal sikre et højt tilgængelighedsniveau for dens kommunikationstjenester. Dens lokaler og de underliggende informationssystemer skal være placeret i sikrede områder og sikre driftskontinuitet. Derudover bør CSIRT'en kunne deltage i internationale samarbejdsnetværk.

3.5. Bistand til udvikling af CSIRT'er

Connecting Europe-facilitetens (CEF) program om digitaltjenesteinfrastrukturer kan sørge for betydelig EU-støtte til medlemsstaternes CSIRT'er, så de kan forbedre deres kapaciteter og samarbejde med hinanden via en samarbejdsmekanisme om informationsudveksling. Den samarbejdsmekanisme, der er under udvikling inden for rammerne af SMART 2015/1089-projektet, skal fremme hurtigt og effektivt operationelt samarbejde på frivillig basis mellem medlemsstaternes CSIRT'er, navnlig som støtte i forbindelse med de opgaver, som CSIRT-netværket er pålagt i henhold til direktivets artikel 12.

Nærmere oplysninger om de relevante indkaldelser af forslag vedrørende kapacitetsopbygning i medlemsstaternes CSIRT'er findes på webstedet for Europa-Kommissionens Forvaltningsorgan for Innovation og Netværk (INEA)[15].

Connecting Europe-facilitetens rådgivende organ for digitaltjenesteinfrastrukturer er en uformel struktur for vejledning på politisk niveau og bistand til medlemsstaternes CSIRT'er med henblik på kapacitetsopbygning og gennemførelse af den frivillige samarbejdsmekanisme.

En nyoprettet CSIRT eller en, der er udpeget til at udføre de opgaver, der er fastsat i bilag I til NIS-direktivet, kan forlade sig på ENISA's ekspertise og rådgivning, så resultaterne forbedres

[15] Findes på https://ec.europa.eu/inea/en/connecting-europe-facility.

og arbejdet udføres effektivt[16]. Det er i den forbindelse værd at fremhæve, at medlemsstaternes CSIRT'er kan bruge noget af det arbejde, som ENISA for nyligt har udført, som reference. Agenturet har, jf. afsnit 7 i dette bilag, navnlig udarbejdet en række dokumenter og undersøgelser, som beskriver god praksis, henstillinger på teknisk niveau, herunder vurderinger af CSIRT'ernes modenhedsniveau, for adskillige af CSIRT'ernes kapaciteter og tjenester. Derudover er vejledninger og bedste praksis også blevet delt i netværket af CSIRT'er både på globalt (FIRST[17]) og europæisk niveau (Trusted Introducer, TI[18]).

3.6. De centrale kontaktpunkters rolle

Ifølge NIS-direktivets artikel 8, stk. 3, skal hver medlemsstat udpege et nationalt centralt kontaktpunkt, der skal fungere som forbindelsesled til at sikre grænseoverskridende samarbejde mellem de relevante myndigheder i andre medlemsstater, samt med samarbejdsgruppen og det CSIRT-netværk[19], der er oprettet ved direktivet. Betragtning 31 og artikel 8, stk. 4, forklarer rationalet bag dette krav, som er at fremme grænseoverskridende samarbejde og kommunikation. Der er især brug herfor, fordi medlemsstaterne kan beslutte at have mere end én national myndighed. Et centralt kontaktpunkt vil følgelig lette identificeringen af og samarbejdet mellem myndigheder fra forskellige medlemsstater.

Det centrale kontaktpunkts rolle som bindeled vil formentlig indebære interaktion med sekretariaterne for samarbejdsgruppen og CSIRT-netværket i de tilfælde, hvor det nationale centrale kontaktpunkt hverken er en CSIRT eller et medlem af samarbejdsgruppen. Derudover skal medlemsstaterne sikre, at de centrale kontaktpunkter oplyses om de modtagne underretninger fra operatører af væsentlige tjenester og udbydere af digitale tjenester[20].

Hvis en medlemsstat vælger en centraliseret tilgang ved kun at udpege én kompetent myndighed, fungerer denne kompetente myndighed ligeledes som det centrale kontaktpunkt, jf. artikel 8, stk. 3, i direktivet. Hvis en medlemsstat vælger en decentraliseret indsats, kan den udpege en af de forskellige kompetente myndigheder som centralt kontaktpunkt. Uanset den valgte institutionelle model er medlemsstaterne, i det tilfælde at CSIRT'en og det centrale kontaktpunkt er adskilte enheder, forpligtede til at sikre et effektivt samarbejde mellem disse enheder med henblik på at opfylde de i direktivet fastsatte forpligtelser[21].

Senest den 9. august 2018 og derefter en gang om året forelægger det centrale kontaktpunkt samarbejdsgruppen en sammenfattende rapport om de underretninger, som det har modtaget, herunder antallet af underretninger og arten af de underrettede hændelser, samt de tiltag, myndighederne har iværksat. Der kan være tale om underretning af de øvrige berørte medlemsstater om hændelsen eller videregivelse af oplysninger til den underrettende

[16] Jf. artikel 9, stk. 5, i NIS-direktivet.
[17] Forum of Incident Response and Security Teams (https://www.first.org/).
[18] https://www.trusted-introducer.org/
[19] Et netværk af nationale CSIRT'er vedrørende det operationelle samarbejde mellem medlemsstaterne i henhold til artikel 12.
[20] Jf. artikel 10, stk. 3.
[21] Jf. artikel 10, stk. 1.

virksomhed om håndtering af hændelsen[22]. På den kompetente myndigheds eller CSIRT's anmodning videresender de centrale kontaktpunkter underretningerne fra operatørerne af væsentlige tjenester til de centrale kontaktpunkter i de andre berørte medlemsstater[23].

Medlemsstaterne skal underrette Kommissionen om udpegelsen af deres centrale kontaktpunkt og dets opgaver, inden fristen for gennemførelse udløber. Udpegelsen af det centrale kontaktpunkt skal offentliggøres ligesom det er tilfældet med de nationale kompetente myndigheder. Kommissionen offentliggør listen over udpegede centrale kontaktpunkter.

3.7. Sanktioner

Artikel 21 giver medlemsstaterne mulighed for selv at fastsatte de sanktioner, der skal anvendes i tilfælde af overtrædelser, forudsat at disse er effektive, står i et rimeligt forhold til overtrædelsen og har afskrækkende virkning. Medlemsstaterne kan med andre ord i princippet selv fastsætte det maksimale sanktionsbeløb i deres nationale lovgivning, men det valgte beløb eller den valgte procentsats skal i hver eneste konkrete sag gøre det muligt for de nationale myndigheder at pålægge effektive, forholdsmæssige og afskrækkende sanktioner, idet der tages højde for forskellige faktorer såsom overtrædelsens alvor og hyppighed.

4. Enheder, som er underlagt sikkerhedskrav og underretningspligt

Enheder, der spiller en vigtig rolle for samfundet og økonomien som nævnt i artikel 4, stk. 4 og 5, i direktivet, idet de er operatører af væsentlige tjenester og udbydere af digitale tjenester, skal træffe passende sikkerhedsforanstaltninger og indberette alvorlige hændelser til de relevante nationale myndigheder. Rationalet er, at konsekvenserne af sikkerhedshændelser inden for sådanne tjenester kan udgøre en enorm trussel mod tjenesternes drift, hvilket kan medføre omfattende forstyrrelser af de økonomiske aktiviteter og samfundet som helhed, potentielt underminere brugernes tillid og forårsage stor skade på Unionens økonomi[24].

Dette afsnit giver et overblik over de enheder, der er omfattet af anvendelsesområdet for NIS-direktivets bilag II og III, og oplister deres forpligtelser. Identificeringen af operatører af væsentlige tjenester behandles grundigt, eftersom denne proces er vigtig for en harmoniseret gennemførelse af NIS-direktivet i hele EU. Afsnittet indeholder ligeledes omfattende forklaringer af definitionerne på digitale infrastrukturer og udbydere af digitale tjenester. Endvidere undersøges muligheden for at inkludere yderligere sektorer, og den specifikke tilgang med hensyn til udbydere af digitale tjenester forklares nærmere.

4.1. Operatører af væsentlige tjenester

NIS-direktivet definerer ikke udtrykkeligt, hvilke enheder der betragtes som operatører af væsentlige tjenester under direktivets anvendelsesområde. Der opstilles i stedet kriterier, som

[22] Som ovenfor.
[23] Jf. artikel 14, stk. 5.
[24] Jf. betragtning 2.

medlemsstaterne skal bruge for at foretage en identificering, der i sidste ende vil bestemme, hvilke individuelle virksomheder henhørende under de forskellige typer af enheder i bilag II, der vil blive betragtet som operatører af væsentlige tjenester og således er underlagt direktivets forpligtelser.

4.1.1. Typer af enheder opført i NIS-direktivets bilag II

I artikel 4, stk. 4, defineres operatør af væsentlige tjenester som offentlige eller private enheder af en type som omhandlet i direktivets bilag II, der opfylder kriterierne i artikel 5, stk. 2. I bilag II er de sektorer, delsektorer og typer af enheder opført, for hvilke hver medlemsstat skal udføre den i artikel 5, stk. 2, nævnte identificering[25]. Sektorerne omfatter energi, transport, bankvæsen, finansielle markedsinfrastrukturer, sundhed, vand og digital infrastruktur.

For de fleste enheder henhørende under de "traditionelle sektorer" indeholder EU's lovgivning veludviklede definitioner, som bilag II henviser til. Dette er ikke tilfældet for sektoren for digital infrastruktur, der er opført under punkt 7 i bilag II, herunder internetudvekslingspunkter, domænenavnesystemer og topdomænenavneadministratorer. Med henblik på at præcisere disse definitioner gives der derfor i det følgende en detaljeret forklaring.

1) Internetudvekslingspunkt (IXP)

Begrebet internetudvekslingspunkt er defineret i artikel 4, stk. 13, og yderligere forklaret i betragtning 18, og kan beskrives som en netfacilitet, som muliggør sammenkobling af mere end to uafhængige autonome systemer, hovedsageligt med henblik på at lette udvekslingen af internettrafik. Internetudvekslingspunktet kan også beskrives som et fysisk sted, hvor en række netværk kan udveksle internettrafik med hinanden via en switch. Det primære formål med et internetudvekslingspunkt er at gøre det muligt for netværk at blive forbundet direkte via udveksling i stedet for at gå igennem en eller flere tredjepartsnetværk. Internetudvekslingspunktets udbyder er normalt ikke ansvarlig for dirigering af internettrafikken. Trafikken dirigeres af netværksudbyderne. Der er talrige fordele ved direkte forbindelser, men de primære er pris, latenstid og båndbredde. Trafik, som passerer ved udveksling, bliver typisk ikke faktureret af nogen af parterne, hvorimod trafik til en opstrømsinternetudbyder gør. Den direkte sammenkobling, der ofte befinder sig i samme by som begge netværk, betyder, at data ikke skal bevæge sig over store afstande fra et netværk til et andet, hvilket forkorter latenstiden.

Det skal bemærkes, at definitionen af internetudvekslingspunkter ikke omfatter fysiske steder, hvor blot to fysiske netværk er indbyrdes forbundet (f.eks. netværksudbydere som BASE og PROXIMUS). Når medlemsstaterne gennemfører direktivet skal de derfor skelne mellem operatører, der fremmer udvekslingen af aggregeret internettrafik mellem operatører af flere

[25] Se nedenstående afsnit 4.1.6 for yderligere oplysninger om identificeringen.

netværk og operatører af et enkelt netværk, som fysisk forbinder deres netværk baseret på en sammenkoblingsaftale. I sidstnævnte tilfælde er netværksudbyderne ikke omfattet af definitionen i artikel 4, stk. 13. En præcisering af dette forhold findes i betragtning 18, ifølge hvilken et IXP ikke giver netadgang og eller fungerer som transitleverandør eller -operatør. Den sidste kategori af leverandører er virksomheder, der stiller offentlige kommunikationsnetværk og/eller tjenester til rådighed, som er genstand for de i artikel 13a og 13b i direktiv 2002/21/EF fastsatte sikkerhedskrav og underretningsforpligtelser, og som derfor er udelukket fra NIS-direktivets anvendelsesområde[26].

2) Domænenavnesystem (DNS)

Begrebet "domænenavnesystem" er defineret i artikel 4, stk. 14, som *"et hierarkisk opbygget navnesystem i et net, som behandler forespørgsler vedrørende domænenavne"*. Mere præcist kan domænenavnesystemet beskrives som et hierarkisk opbygget navnesystem for computere, tjenester eller enhver anden ressource, der er forbundet med internettet, og som gør det muligt at indkode domænenavne i IP-adresser (internetprotokol). Systemets primære rolle er at oversætte de tildelte domænenavne til IP-adresser. Med henblik herpå driver DNS en database og anvender navneservere og resolvere for at muliggøre denne form for "oversættelse" af domænenavne til operationelle IP-adresser. Om end indkodning af domænenavne ikke er DNS's eneste opgave, er det en af systemets væsentligste opgaver. Den juridiske definition i artikel 4, stk. 14, fokuserer på systemets primære rolle set fra brugerens synspunkt uden at gå i mere tekniske detaljer som eksempelvis driften af domænenavne, navneservere, resolvere osv. Endelig præciserer artikel 4, stk. 15, hvem der kan betragtes som DNS-tjenesteudbyder.

3) Topdomænenavneadministrator (TLD-navneadministrator)

Topdomænenavneadministrator er defineret i artikel 4, stk. 16, som en enhed, som administrerer og driver registreringen af internetdomænenavne under et særligt topdomæne. Administration og forvaltning af domænenavne omfatter indkodning af TLD-navne i IP-adresser.

IANA (Internet Assigned Numbers Authority) er ansvarlig for den globale koordinering af DNS-roden, IP-adresser og andre internetprotokolressourcer. IANA er navnlig ansvarlig for tildeling af generiske topdomæner (gTLD) som eksempelvis ".com" og landekode-topdomæner (ccTLD) som eksempelvis ".be" til operatører (registre) og vedligeholdelsen af deres tekniske og administrative oplysninger. IANA vedligeholder et globalt register over tildelte topdomæner og spiller en rolle for offentliggørelsen af denne liste til internetbrugere over hele verden såvel som for indførelsen af nye topdomæner.

En vigtig opgave for registrene er at tildele domænenavne på andet niveau til de såkaldte registranter under deres respektive topdomæner. Hvis registranterne ønsker det, kan de også på egen hånd tildele domænenavne på tredje niveau. Landekode-topdomænerne repræsenterer

[26] Se afsnit 5.2 for flere detaljer vedrørende forholdet mellem NIS-direktivet og direktiv 2002/21/EF.

et land eller et område baseret på ISO 3166-1-standarden. De "generiske" topdomæner har ikke normalt en geografisk betydning eller tilknytning til et bestemt land.

Det skal bemærkes, at opgaven som topdomænenavneadministrator kan omfatte tilrådighedsstillelse af domænenavnesystemer. Eksempelvis skal den enhed, der er udpeget til at håndtere landekode-topdomæner, ifølge IANA's bestemmelser om delegation bl.a. overvåge domænenavnene og drive det pågældende lands domænenavnesystem[27]. Medlemsstaterne skal tage sådanne omstændigheder i betragtning, når de identificerer operatører af væsentlige tjenester i henhold til artikel 5, stk. 2.

4.1.2. Identificering af operatører af væsentlige tjenester

I overensstemmelse med kravene i direktivets artikel 5 skal hver medlemsstat for hver enhed af de typer, som er omhandlet i bilag II, identificere de operatører af væsentlige tjenester, der er etableret på deres område. Som et resultat af vurderingen skal alle enheder, der opfylder kriterierne i artikel 5, stk. 2, identificeres som operatører af væsentlige tjenester og pålægges de i artikel 14 fastsatte sikkerhedskrav og underretningsforpligtelser.

Medlemsstaterne har indtil den 9. november 2018 til at identificere operatører for hver sektor og delsektor. For at støtte medlemsstaterne i denne proces er samarbejdsgruppen i færd med at udarbejde en vejledning med relevante oplysninger om de nødvendige skridt og bedste praksis i forbindelse med identificering af operatører af væsentlige tjenester.

I henhold til artikel 24, sk. 2, skal samarbejdsgruppen derudover drøfte processen, indholdet og typen af nationale foranstaltninger, som gør det muligt at identificere operatører af væsentlige tjenester. En medlemsstat kan forud for den 9. november 2018 forelægge sine nationale foranstaltninger, der muliggør identificering af operatører af væsentlige tjenester, til drøftelse i samarbejdsgruppen.

4.1.3. Inkludering af yderligere sektorer

Medlemsstaterne kan, under hensyntagen til det krav om minimumsharmonisering, der er fastsat ved artikel 3, vedtage eller bibeholde lovgivning, som sikrer et højere niveau af sikkerhed i net- og informationssystemer. I den forbindelse er medlemsstaterne generelt frit stillet med hensyn til at udvide de i artikel 14 fastsatte sikkerhedskrav og underretningsforpligtelser til at omfatte enheder, der hører under andre sektorer og delsektorer end dem, der er oplistet i bilag II til NIS-direktivet. Adskillige medlemsstater har besluttet eller er p.t. ved at overveje at inkludere visse af følgende yderligere sektorer:

i) Offentlige forvaltninger

Offentlige forvaltninger kan tilbyde væsentlige tjenester som omhandlet i direktivets bilag II, der opfylder kriterierne i artikel 5, stk. 2. I disse tilfælde vil offentlige forvaltninger, der tilbyder sådanne tjenester, være omfattet af de relevante sikkerhedskrav og underretningsforpligtelser. Omvendt er sådanne tjenester ikke omfattet af de relevante

[27] Yderligere oplysninger findes på: https://www.icann.org/resources/pages/delegation-2012-02-25-en.

forpligtelser, når de offentlige forvaltninger tilbyder tjenester, som ikke henhører under ovennævnte anvendelsesområde.

Offentlige forvaltninger er ansvarlige for, at statslige organer, regionale og lokale myndigheder samt agenturer og tilknyttede virksomheder leverer offentlige tjenester korrekt. Disse tjenester indebærer ofte oprettelse og forvaltning af person- og virksomhedsdata om enkeltpersoner og organisationer, der kan deles og gøres tilgængelige for adskillige offentlige enheder. Overordnet set har samfundet og økonomien som helhed stor interesse i et højt sikkerhedsniveau i net- og informationssystemer, der anvendes af offentlige forvaltninger. Kommissionen mener derfor, at det vil være fornuftigt af medlemsstaterne at overveje at inkludere offentlige forvaltninger i anvendelsesområdet for den nationale lovgivning til gennemførelse af direktivet, så den går videre end bestemmelserne om væsentlige tjenester som fastsat i bilag II og artikel 5, stk. 2.

ii) Postsektoren

Postsektoren sørger for levering af posttjenester såsom indsamling, sortering, transport og distribution af postforsendelser.

iii) Fødevaresektoren

Fødevaresektoren vedrører produktion af landbrugsvarer og andre fødevarer, og den vil kunne omfatte væsentlige tjenester såsom fødevaresikkerhed og sikring af fødevarekvalitet og -sikkerhed.

iv) Den kemiske og nukleare industri

Den kemiske og nukleare industri vedrører særligt lagring, produktion og forarbejdning af kemiske og petrokemiske produkter eller nukleare materialer.

v) Miljøsektoren

Miljøaktiviteter omfatter levering af de varer og tjenesteydelser, der er nødvendige for at beskytte miljøet og forvalte ressourcer. Derfor har aktiviteterne til formål at forhindre, reducere og fjerne forurening og bevare beholdningen af tilgængelige naturlige ressourcer. Væsentlige tjenester under denne sektor kunne følgelig være overvågning og kontrol af forurening (f.eks. af luft og vand) og meteorologiske fænomener.

vi) Civilbeskyttelse

Civilbeskyttelsessektorens mål er forebyggelse, forberedelse og håndtering af naturkatastrofer og menneskeskabte katastrofer. De tjenester, der er tale om, kan være aktivering af alarmnumre og gennemførelse af tiltag vedrørende information om, håndtering af og reaktion på nødsituationer.

4.1.4. Jurisdiktion

Ifølge artikel 5, stk. 1, skal medlemsstaternes identificere operatører af væsentlige tjenester, der er etableret på deres område. Bestemmelsen indeholder ikke en yderligere præcisering af den retlige etablering, men i betragtning 21 tydeliggøres det, at der ved etablering i en medlemsstat forstås en effektiv og reel udøvelse af aktiviteter gennem stabile ordninger, og at den retlige form ikke har afgørende betydning. Dette betyder, at en medlemsstat ikke blot har

jurisdiktion over en operatør af en væsentlig tjeneste, hvis denne har sit hovedsæde på den pågældende medlemsstats område, men at den også har jurisdiktion i tilfælde, hvor en operatør f.eks. har en filial eller en anden type retlig etablering.

Som konsekvens kan adskillige medlemsstater have jurisdiktion over den samme enhed samtidigt.

4.1.5. Oplysninger, der skal forelægges Kommissionen

Med henblik på den revision, som Kommissionen skal udføre i overensstemmelse med artikel 23, stk. 1, i NIS-direktivet, skal medlemsstaterne senest den 9. november 2018 og hvert andet år herefter forelægge følgende oplysninger for Kommissionen:

- nationale foranstaltninger, som gør det muligt at identificere operatører af væsentlige tjenester
- listen over væsentlige tjenester
- antallet af operatører af væsentlige tjenester, som er identificeret for hver sektor, der er omhandlet i bilag II, og en angivelse af deres betydning for den pågældende sektor, og
- tærskler, hvis sådanne findes, til fastlæggelse af det relevante forsyningsniveau ved henvisning til antallet af brugere, der er afhængige af denne tjeneste, jf. artikel 6, stk. 1, litra a), eller til enhedens vigtighed, jf. artikel 6, stk. 1, litra f).

Den ved artikel 23, stk. 1, fastsatte revision, som går forud for den omfattende revision af direktivet, afspejler den betydning, Europa-Parlamentet og Rådet tillægger den korrekte gennemførelse af direktivet for så vidt angår identificeringen af operatører af væsentlige tjenester med henblik på at undgå fragmentering af markedet.

For at processen forløber på bedst mulig vis, opfordrer Kommissionen medlemsstaterne til at drøfte emnet og udveksle relevante erfaringer inden for rammerne af samarbejdsgruppen. Derudover opfordrer Kommissionen medlemsstaterne til, om nødvendigt fortroligt, at dele listerne over identificerede operatører af væsentlige tjenester med Kommissionen, som supplement til alle de oplysninger, som medlemsstaterne i henhold til direktivet skal fremlægge for Kommissionen. Tilgængeligheden af sådanne lister vil lette Kommissionens vurdering af sammenhængen i identificeringsprocessen og øge vurderingens kvalitet, ligesom det vil gøre det muligt at foretage en sammenligning af de forskellige medlemsstaters tilgange, hvorved direktivets målsætninger bedre kan nås.

4.1.6. Hvordan foregår identificeringsprocessen?

Som det fremgår af figur 4, er der seks nøglespørgsmål, som nationale myndigheder skal undersøge, når de foretager identificering af en given enhed. I det følgende svarer hvert spørgsmål til et trin, der skal gennemføres i overensstemmelse med artikel 5 sammenholdt med artikel 6, under hensyntagen til, om artikel 1, stk. 7, finder anvendelse.

Trin 1 – **Tilhører enheden en sektor/delsektor, og er den af den type, der er omfattet af bilag II til direktivet?**

En national myndighed bør vurdere, hvorvidt en enhed, der er etableret på dens område, tilhører en af de sektorer og delsektorer, der er opført i bilag II til direktivet. Bilag II omfatter forskellige økonomiske sektorer, der betragtes som havende afgørende betydning for et velfungerende indre marked. Bilag II omfatter navnlig følgende sektorer og delsektorer:

- energi: elektricitet, olie og gas
- transport: luft, jernbane, vand og vej
- bankvirksomhed: kreditinstitutter
- finansielle markedsinfrastrukturer: markedspladser, centrale modparter
- sundhed: sundhedstjenester (herunder hospitaler og private klinikker)
- vand: drikkevandsforsyning og distribution
- digital infrastruktur: internetudvekslingspunkter, domænenavnesystemer, topdomænenavneadministratorer[28].

Trin 2 – **Finder lex specialis anvendelse?**

På det følgende trin skal den nationale myndighed vurdere, hvorvidt bestemmelsen om lex specialis, der er fastsat i artikel 1, stk. 7, finder anvendelse. Denne bestemmelse fastsætter navnlig, at det, når en EU-retsakt pålægger udbydere af digitale tjenester og operatører af væsentlige tjenester sikkerhedskrav og underretningspligt, der har mindst samme virkning som forpligtelserne i NIS-direktivet, er forpligtelserne under den pågældende retsakt, der finder anvendelse. Derudover præciseres det i betragtning 9, at medlemsstaterne, hvis kravene i artikel 1, stk. 7, er opfyldt, bør anvende bestemmelserne i sådanne sektorspecifikke EU-retsakter, herunder bestemmelserne vedrørende jurisdiktion. De relevante bestemmelser i NIS-direktivet finder dermed ikke anvendelse. I dette tilfælde skal den kompetente myndighed ikke fortsætte den i artikel 5, stk. 2[29], fastsatte identificering.

Trin 3 – **Leverer operatøren en væsentlig tjeneste i den i direktivet omhandlede betydning?**

I henhold til artikel 5, stk. 2, litra a), skal den enhed, som er genstand for identificering, levere en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter. Medlemsstaterne skal ved foretagelse af denne vurdering tage højde for, at en enhed kan levere både væsentlige og ikke-væsentlige tjenester. Det betyder, at NIS-direktivets sikkerhedskrav og underretningspligt kun gælder for en given operatør i det omfang, denne operatør leverer væsentlige tjenester.

I henhold til artikel 5, stk. 3, skal hver medlemsstat udarbejde en liste over alle de væsentlige tjenester, som operatører leverer på dens område. Listen skal forelægges for Kommissionen senest den 9. november 2018 og herefter hvert andet år[30].

---

[28]Disse enheder forklares yderligere i afsnit 4.1.1.

[29] Yderligere detaljer om anvendeligheden af lex specialis findes i afsnit 5.1.

[30] Jf. artikel 5, stk. 7, litra b).

Trin 4 – **Er tjenesten afhængig af et net- og informationssystem?**

Derudover skal det klarlægges, hvorvidt denne tjeneste opfylder det andet kriterium i artikel 5, stk. 2, litra b), og navnlig hvorvidt leveringen af den væsentlige tjeneste afhænger af net- og informationssystemer som defineret i artikel 4, stk. 1.

Trin 5 – **Vil en sikkerhedshændelse have en væsentlig forstyrrende virkning?**

Artikel 5, stk. 2, litra c), kræver, at den nationale myndighed vurderer, hvorvidt en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten. I artikel 6, stk. 1, fastsættes der adskillige tværsektorielle forhold, som der skal tages højde for i forbindelse med vurderingen. Endvidere fastsættes det i artikel 6, stk. 2, at der i forbindelse med vurderingen også bør tages højde for sektorspecifikke forhold.

De tværsektorielle forhold opført i artikel 6, stk. 1, er som følger:

- antal af brugere, der er afhængige af de tjenester, som udbydes af den pågældende enhed
- afhængighed i andre sektorer som omhandlet i bilag II af den tjeneste, der leveres af den nævnte enhed
- de konsekvenser, som hændelser kan have med hensyn til omfang og varighed på økonomiske og samfundsmæssige aktiviteter eller den offentlige sikkerhed
- den nævnte enheds markedsandel
- den geografiske udbredelse med hensyn til det område, som kunne berøres af en hændelse
- enhedens betydning med henblik på at opretholde et tilstrækkeligt tjenesteniveau under hensyntagen til tilgængelige alternative måder til levering af denne tjeneste.

Hvad angår de **tværsektorielle forhold** giver betragtning 28 nogle eksempler (se tabel 4), der kan være en nyttig rettesnor for de nationale myndigheder.

Tabel 4: Eksempler på sektorspecifikke faktorer, der skal tages i betragtning, når det fastslås, hvorvidt en hændelse har en væsentlig forstyrrende virkning

Sektor	Eksempler på sektorspecifikke faktorer
Energileverandører	omfanget eller andelen af elektricitet, der produceres på nationalt plan
Olieleverandører	mængden af olie leveret pr. dag
Lufttransport (herunder lufthavne og luftfartsselskaber) **Jernbanetransport** **Søhavne**	den nationale andel af trafikmængden antallet af passagerer eller fragtoperationer årligt
Banksektoren og sektoren for finansielle markedsinfrastrukturer	systemisk betydning baseret på de samlede aktiver samlede aktiver i forhold til BNP

Sundhedssektoren	antallet af patienter under tjenesteyderens pleje pr. år
Vandproduktion, -behandling og -forsyning	mængden og antallet samt typerne af brugere, der forsynes (herunder for eksempel hospitaler, organisationer for offentlige tjenester eller enkeltpersoner) eksistensen af alternative vandkilder til dækning af samme geografiske område

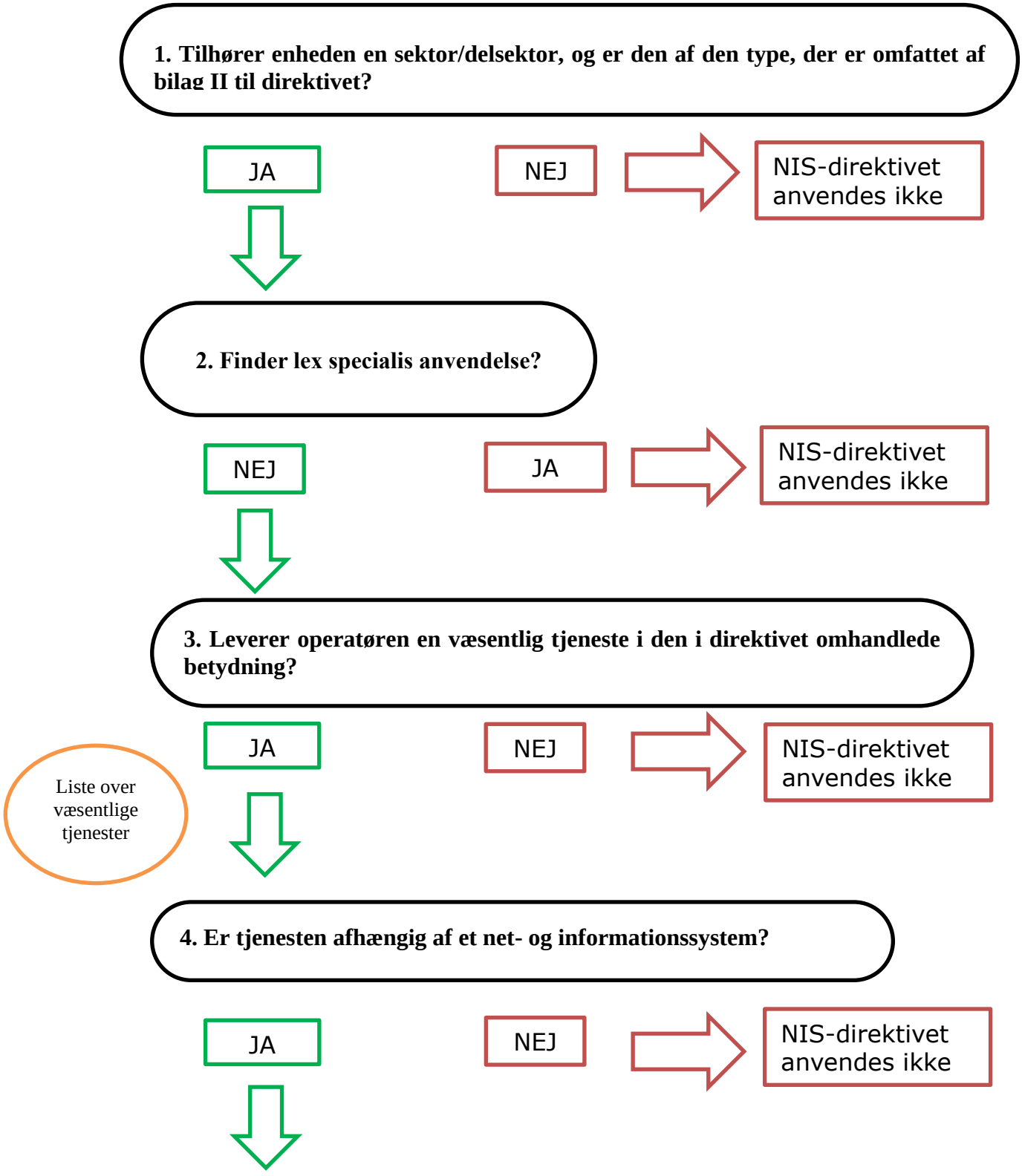
Det skal understreges, at medlemsstaterne, når de foretager vurderingen i henhold til artikel 5, stk. 2, ikke bør tilføje yderligere kriterier end dem, der er nævnt i bestemmelsen, da dette vil kunne begrænse antallet af identificerede operatører af væsentlige tjenester og bringe den i artikel 3 fastsatte minimumsharmonisering i fare.

Trin 6 – **Leverer den pågældende operatør væsentlige tjenester i andre medlemsstater?**

Trin 6 henviser til tilfælde, hvor en operatør leverer væsentlige tjenester til to eller flere medlemsstater. De berørte medlemsstater skal i henhold til artikel 5, stk. 4, høre hinanden før afslutningen af identificeringsprocessen[31].

[31] For yderligere oplysninger om høringsprocessen se afsnit 4.1.7.

Figur 4: Identificeringsprocessens 6 trin



5. Vil en sikkerhedshændelse have en væsentlig forstyrrende virkning?

Tværsektorielle forhold (artikel 6, stk. 1)

- **Antal brugere**, der er afhængige af tjenesten
- Andre væsentlige sektorers **afhængighed** af tjenesten
- Konsekvenser, som hændelser kan have på **økonomiske og samfundsmæssige aktiviteter** eller **den offentlige sikkerhed**
- Mulig **geografisk udbredelse**
- Enhedens betydning med henblik på at opretholde et tilstrækkeligt **tjenesteniveau**

Sektorspecifikke faktorer (eksempler nævnt i betragtning 28)

- **Energi**: omfanget eller andelen af elektricitet, der produceres på nationalt plan
- **Transport**: den nationale andel af trafikmængden og antallet af fragtoperationer årligt
- **Sundhed**: antallet af patienter under tjenesteyderens pleje pr. år

JA

NEJ → NIS-direktivet anvendes ikke

6. Leverer den pågældende operatør væsentlige tjenester i andre medlemsstater?

JA

NEJ → NIS-direktivet anvendes ikke

Obligatorisk høring af den/de pågældende medlemsstater

Vedtagelse af nationale foranstaltninger (f.eks. liste over operatører af væsentlige tjenester, politiske og retlige foranstaltninger)

4.1.7. Grænseoverskridende høringsproces

Hvis operatører af væsentlige tjenester leverer væsentlige tjenester i to eller flere medlemsstater, skal disse medlemsstater i henhold til artikel 5, stk. 4, høre hinanden forud for afslutningen af identificeringsprocessen. Formålet med denne høring er at lette vurderingen af operatørens kritiske karakter med hensyn til grænseoverskridende konsekvenser.

Det ønskede resultat af høringen er, at de involverede nationale myndigheder udveksler argumenter og synspunkter og ideelt kommer til samme konklusion vedrørende identificeringen af den pågældende operatør. NIS-direktivet udelukker imidlertid ikke, at medlemsstaterne kan nå til forskellige konklusioner om, hvorvidt en given enhed kan identificeres som operatør af væsentlige tjenester eller ej. Ifølge betragtning 24 kan medlemsstaterne i den forbindelse anmode om samarbejdsgruppens bistand.

Det er Kommissionens holdning, at medlemsstaterne bør stræbe efter at nå til enighed om disse spørgsmål for at undgå en situation, hvor samme virksomhed har forskellig retlig status i forskellige medlemsstater. Uoverensstemmelser bør være en absolut undtagelse og begrænset til tilfælde, hvor f.eks. en enhed, der er identificeret som en operatør af væsentlige tjenester i en medlemsstat, har en marginal og ubetydelig aktivitet i en anden.

4.2. Sikkerhedskrav

Ifølge artikel 14, stk. 1, skal medlemsstaterne sikre, at operatører af væsentlige tjenester, under hensyntagen til teknologiens aktuelle stade, træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som de anvender til deres aktiviteter. Ifølge artikel 14, stk. 2, skal passende foranstaltninger forebygge og minimere konsekvensen af en hændelse.

Samarbejdsgruppen arbejder p.t. engageret på en ikke-bindende vejledning vedrørende sikkerhedsforanstaltninger for operatører af væsentlige tjenester[32]. Samarbejdsgruppen vil færdiggøre vejledningen i fjerde kvartal 2017. Kommissionen opfordrer medlemsstaterne til tæt at følge den vejledning, som samarbejdsgruppen udarbejder, således at de nationale bestemmelser om sikkerhedskrav kan tilnærmes i så vid udstrækning som muligt. Harmonisering af sådanne krav vil i høj grad gøre overholdelsen af bestemmelserne lettere for operatører af væsentlige tjenester, der ofte leverer væsentlige tjenester i mere end én medlemsstat, ligesom det vil gøre det lettere for de nationale kompetente myndigheder og CSIRT'erne at føre tilsyn.

4.3 Underretningspligt

Ifølge artikel 14, stk. 3, skal medlemsstaterne sikre, at operatørerne af væsentlige tjenester foretager underretning om *"hændelser, der har væsentlige konsekvenser for kontinuiteten af*

[32] Med henblik på dette arbejde er lister over internationale standarder, god praksis og risikovurderings-/risikostyringsmetoder for alle sektorer, der er omfattet af NIS-direktivet, blevet sendt rundt og brugt som input til de foreslåede sikkerhedsområder og sikkerhedsforanstaltninger.

de væsentlige tjenester, som de leverer." Operatørerne af væsentlige tjenester skal følgelig ikke underrette om mindre hændelser, men kun om alvorlige hændelser, som påvirker kontinuiteten af den væsentlige tjeneste. I artikel 4, stk. 7, defineres en hændelse som *"enhver begivenhed, der har en egentlig negativ indvirkning på sikkerheden i net- og informationssystemer"*. Begrebet "sikkerhed i net- og informationssystemer" defineres yderligere under artikel 4, stk. 2, som *"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 eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer"*. Som følge heraf vil enhver begivenhed, der har en negativ virkning på tilgængeligheden, autenciteten, integriteten eller fortroligheden i forbindelse med data eller de dermed forbundne tjenester, potentielt kunne udløse indberetningskravet. Kontinuiteten af tjenesten som omtalt i artikel 14, stk. 3, kan reelt kompromitteres, ikke blot i tilfælde, der handler om fysisk tilgængelighed, men også i tilfælde, hvor enhver anden sikkerhedshændelse påvirker den korrekte levering af tjenesten[33].

Samarbejdsgruppen arbejder p.t. engageret på ikke-bindende retningslinjer vedrørende underretning, der vedrører de omstændigheder, under hvilke operatører af væsentlige tjenester skal underrette om hændelser i henhold til artikel 14, stk. 7, samt formatet og proceduren for nationale underretninger. Vejledningen forventes færdig i fjerde kvartal 2017.

Nationale forskelle med hensyn til underretningspligt kan medføre retlig usikkerhed, mere komplicerede og omstændelige procedurer og betydelige administrative omkostninger for udbydere, der opererer på tværs af landegrænserne. Kommissionen ser derfor positivt på samarbejdsgruppens indsats. Ligesom det er tilfældet for sikkerhedskravene, opfordrer Kommissionen medlemsstaterne til tæt at følge den vejledning, som samarbejdsgruppen udarbejder, således at de nationale bestemmelser om underretning om hændelser kan tilnærmes i så vid udstrækning som muligt.

4.4. NIS-direktivet, bilag III: Udbydere af digitale tjenester

Udbydere af digitale tjenester er den anden kategori af enheder, der er omfattet af NIS-direktivets anvendelsesområde. Disse enheder betragtes som vigtige økonomiske spillere, fordi de leverer tjenester til mange virksomheder, og forstyrrelser af de digitale tjenester kan påvirke de vigtigste økonomiske og samfundsmæssige aktiviteter.

4.4.1. Kategorier af udbydere af digitale tjenester

I artikel 4, stk. 5, som definerer digital tjeneste, henvises der til artikel 1, stk. 1, litra b), i direktiv (EU) 2015/1535, som indskrænker anvendelsesområdet til de typer af tjenester, der er opført i NIS-direktivets bilag III. I artikel 1, stk. 1, litra b), i direktiv (EU) 2015/1535 defineres disse tjenester som *"enhver tjeneste i informationssamfundet, dvs. enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager"*, og i bilag III til NIS-direktivet oplistes tre specifikke

[33] Det samme gælder for udbydere af digitale tjenester.

typer af tjenester: onlinemarkedspladser, onlinesøgemaskiner og cloud computing-tjenester. I sammenligning med operatørerne af væsentlige tjenester kræver direktivet ikke, at medlemsstaterne identificerer udbyderne af digitale tjenester, som så skal pålægges de relevante forpligtelser. Derfor finder de relevante forpligtelser i direktivet, navnlig de sikkerhedskrav og den underretningspligt, der er fastsat i artikel 16, anvendelse på alle udbydere af digitale tjenester inden for direktivets anvendelsesområde.

I følgende afsnit gives der yderligere forklaringer vedrørende de tre typer af digitale tjenester, der er omfattet af direktivets anvendelsesområde.

1. Udbyder af onlinemarkedsplads

Onlinemarkedspladsen gør det muligt for et stort antal og en bred vifte af virksomheder at udøve deres handelsaktiviteter over for kunderne og indgå i forbindelser med andre virksomheder. Den giver virksomhederne en grundlæggende infrastruktur, hvor der kan handles online og på tværs af grænserne. Onlinemarkedspladser spiller en afgørende rolle i økonomien ved især at give SMV'erne adgang til det bredere digitale indre marked i EU. Levering af fjerndatabehandlingstjenester, der fremmer kundens økonomiske aktivitet, herunder behandling af transaktioner og aggregering af informationer om købere, leverandører og produkter, kan også høre under aktiviteterne for udbydere af onlinemarkedspladser. Det samme gælder facilitering af søgninger efter egnede produkter, levering af produkter, transaktionsekspertise og matchning af købere og sælgere.

Begrebet onlinemarkedsplads er defineret i artikel 4, stk. 17, og yderligere præciseret i betragtning 15. Det beskrives som en tjeneste, der giver forbrugere og erhvervsdrivende mulighed for at indgå aftaler om køb eller tjenester online med erhvervsdrivende, og den er det endelige bestemmelsessted for indgåelse af sådanne kontrakter. Eksempelvis kan en udbyder som *E-bay* betragtes som en onlinemarkedsplads, idet den gør det muligt for andre at etablere butikker på dens platform, så de kan gøre deres produkter og tjenester tilgængelige online for forbrugere og virksomheder. Online applikationsbutikker, hvorfra der distribueres applikationer og softwareprogrammer, betragtes også som onlinemarkedspladser, fordi de gør det muligt for udviklere af applikationer at sælge eller distribuere deres tjenester til forbrugere og andre virksomheder. Til gengæld er mellemled for tredjepartstjenester såsom *Skyscanner* og prissammenligningstjenester, der omdirigerer brugeren til den erhvervsdrivendes websted, hvor den reelle aftale om levering af tjenesten eller produktet indgås, ikke omfattet af definitionen i artikel 4, stk. 17.

2. Udbyder af onlinesøgemaskine

Begrebet onlinesøgemaskine er defineret i artikel 4, stk. 18, og yderligere præciseret i betragtning 16. Den beskrives som en digital tjeneste, som giver brugerne mulighed for at foretage søgninger på principielt alle websteder eller websteder på et bestemt sprog på grundlag af en forespørgsel om et hvilket som helst emne. Søgefunktioner, der er begrænset til søgning internt på websteder og websteder med prissammenligning er ikke omfattet. En

søgemaskine som den EUR-Lex[34] tilbyder, kan f.eks. ikke betragtes som en søgemaskine i direktivets betydning, da dens søgefunktion er begrænset til indholdet af det konkrete websted.

3. Udbyder af cloud computing-tjenester

I artikel 4, stk. 19, defineres cloud computing-tjenester som *"en digital tjeneste, som giver adgang til en skalerbar og elastisk pulje af delbare IT-ressourcer"*, og i betragtning 17 præciseres begreberne IT-ressourcer, skalerbar og elastisk pulje.

Cloud computing kan kort sagt beskrives som en særlig type IT-tjeneste, der anvender delte ressourcer med henblik på at behandle data on-demand, hvor der ved delte ressourcer forstås enhver form for hardware- eller softwarekomponenter (f.eks. netværk, servere eller anden infrastruktur, lagring, applikationer og tjenester), som frigives til brugerne on-demand til databehandling. Ved begrebet delbar forstås IT-ressourcer, hvor mange brugere anvender samme fysiske infrastruktur til databehandling. En IT-ressource kan defineres som delbar, hvis den pulje af ressourcer, som udbyderen anvender, kan gøres større eller mindre afhængigt af brugerens behov. Datacentre eller enkelte komponenter i et datacenter kan således eventuelt tilføjes eller fjernes, hvis den samlede databehandlings- eller lagringskapacitet skal ajourføres. Begrebet elastisk pulje kan beskrives som ændringer i arbejdsbyrden, hvor der tildeles og fratages ressourcer på automatisk vis, således at de tilgængelige ressourcer til enhver tid afspejler det aktuelle behov så præcist som muligt[35].

Der findes p.t. tre hovedtyper af modeller over cloudtjenester, som en udbyder kan levere:

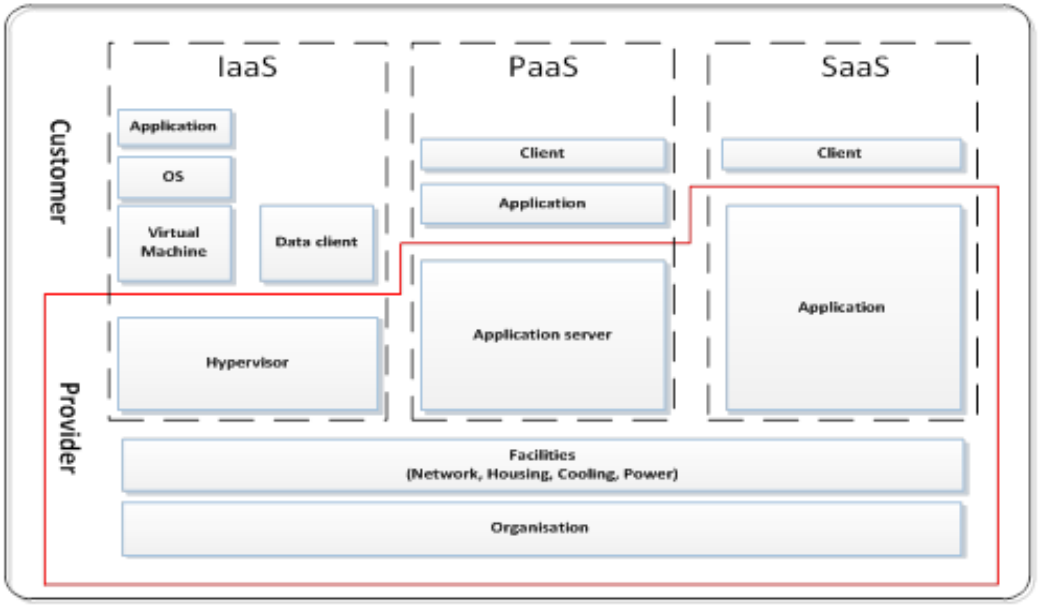
- Infrastructure as a Service (IaaS): En kategori af cloudtjenester, hvor den kapacitet, clouden tilbyder kunden, er en infrastruktur. Der er tale om virtuel levering af IT-ressourcer i form af hardware-, netværks- og lagringsydelser. IaaS understøtter servere, lagring, netværk og driftssystemer. Det giver virksomheder en infrastruktur, hvor de kan lagre deres data og køre de applikationer, der er nødvendige for den daglige drift.

- Platform as a Service (PaaS): En kategori af cloudtjenester, hvor den kapacitet, clouden tilbyder kunden, er en platform. Der er tale om online IT-platforme, som gør det muligt for virksomheder at køre eksisterende applikationer eller udvikle og teste nye.

- Software as a service (SaaS): En kategori af cloudtjenester, hvor den kapacitet, clouden tilbyder kunden, er en applikation eller software, der bliver brugt via internettet. Denne type cloudtjeneste afskaffer slutbrugerens behov for at købe, installere og håndtere software, og har den fordel, at softwaren kan tilgås fra alle steder, hvor der er en internetforbindelse.

[34] Findes på http://eur-lex.europa.eu/homepage.html.
[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, *Elasticity in Cloud Computing:* What It Is, and What It Is Not", findes på: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Se ligeledes s. 2-5 i COM(2012) 529.

Figur 5: Tjenestemodeller og aktiver inden for cloud computing



ENISA har udarbejdet omfattende retningslinjer om specifikke emner inden for cloudområdet[36] og en vejledning om grundprincipperne for cloud computing[37].

4.4.2. Sikkerhedskrav

Ifølge artikel 16, stk. 1, skal medlemsstaterne sikre, at udbydere af digitale 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. Disse sikkerhedsforanstaltninger skal tage hensyn til teknologiens aktuelle stade og følgende fem elementer: i) systemers og faciliteters sikkerhed ii) håndtering af hændelser iii) styring af driftskontinuitet iv) monitorering, audit og testning v) overholdelse af internationale standarder.

Kommissionen har i den henseende beføjelser til at vedtage gennemførelsesretsakter, jf. artikel 16, stk. 8, for at fastsætte en yderligere specifikation af disse elementer og sikre en høj grad af harmonisering for disse tjenesteudbydere. Gennemførelsesretsakten forventes at blive vedtaget af Kommissionen i efteråret 2017. Det kræves ydermere, at medlemsstaterne sikrer, at udbydere af digitale tjenester træffer foranstaltninger for at forebygge og minimere konsekvensen af hændelser for at sikre kontinuiteten i deres tjenester.

[36] Findes på https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Cloud Security Guide for SMEs* (2015). Findes på https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

4.4.3. Underretningspligt

Udbydere af digitale tjenester bør være forpligtet til at underrette de kompetente myndigheder eller CSIRT'erne om alvorlige hændelser. I henhold til artikel 16, stk. 3, i NIS-direktivet er udbydere af digitale tjenester forpligtet til underretning, når en sikkerhedshændelse har betydelige konsekvenser for leveringen af tjenesten. Med henblik på at fastlægge, om en hændelses konsekvenser er betydelige, oplistes der i artikel 16, stk. 4, fem parametre, som udbyderne af digitale tjenester skal tage hensyn til. Kommissionen har i den henseende beføjelser til at vedtage gennemførelsesretsakter, jf. artikel 16, stk. 8, hvor der gives mere detaljerede beskrivelser af parametrene. Den videre specifikation af disse parametre vil være omfattet af den gennemførelsesretsakt om fastlæggelse af de i afsnit 4.4.2 nævnte sikkerhedselementer, som Kommissionen agter at vedtage i efteråret.

4.4.4. Risikobaseret reguleringsmæssig tilgang

Det understreges i artikel 17, at udbydere af digitale tjenester er genstand for de nationale kompetente myndigheders efterfølgende tilsynsforanstaltninger. Medlemsstaterne skal sikre, at de kompetente myndigheder skrider til handling, når de har fået dokumentation for, at en udbyder af digitale tjenester ikke opfylder kravene i direktivets artikel 16.

I henhold til artikel 16, stk. 8 og 9, har Kommissionen beføjelser til at vedtage gennemførelsesretsakter hvad angår underretnings- og sikkerhedskravene, hvilket vil øge graden af harmonisering for udbyderne af digitale tjenester. Desuden må medlemsstaterne i henhold til artikel 16, stk. 10, ikke indføre yderligere sikkerhedskrav eller underretningspligt for udbydere af digitale tjenester udover dem, der er fastsat i direktivet, undtagen i tilfælde hvor sådanne foranstaltninger er nødvendige for at sikre centrale statslige funktioner og tillade efterforskning, afsløring og retsforfølgelse af strafbare handlinger.

Under hensyntagen til den grænseoverskridende karakter af udbydere af digitale tjenester følger direktivet ikke modellen med flere parallelle jurisdiktioner, men en tilgang baseret på kriteriet om, at virksomhedens hjemsted skal ligge i EU[38]. Denne tilgang gør det muligt at anvende et enkelt sæt regler for udbydere af digitale tjenester, hvor en kompetent myndighed er ansvarlig for tilsyn, hvilket er særlig vigtigt, eftersom mange udbydere af digitale tjenester tilbyder deres tjenester i mange medlemsstater samtidigt. Anvendelsen af denne tilgang minimerer byrden ved overholdelse for udbydere af digitale tjenester og sikrer et velfungerende digitalt indre marked.

4.4.5. Jurisdiktion

Som forklaret ovenfor har den medlemsstat, hvor udbyderen af digitale tjenester har sit hjemsted, jurisdiktion over virksomheden, jf. artikel 18, stk. 1, i NIS-direktivet. I tilfælde, hvor den konkrete udbyder tilbyder tjenester i EU, men ikke er etableret på EU's område, skal udbyderen udpege en repræsentant i Unionen, jf. artikel 18, stk. 2. Det er i så fald den medlemsstat, hvor repræsentanten er etableret, der har jurisdiktion over virksomheden. I tilfælde, hvor en udbyder leverer tjenester i en medlemsstat, men ikke har udpeget en repræsentant i Unionen, kan medlemsstaten i princippet træffe foranstaltninger mod denne

[38] Jf. især artikel 18 i direktivet.

udbyder af digitale tjenester, fordi vedkommende tilsidesætter sine forpligtelser i henhold til direktivet.

4.4.6. Undtagelse for udbydere, der leverer digitale tjenester i begrænset omfang, fra anvendelsesområdet for sikkerhedskrav og underretningspligt

I henhold til artikel 16, stk. 11, er mikrovirksomheder og små virksomheder som defineret i Kommissionens henstilling 2003/361/EF[39] udelukket fra anvendelsesområdet for sikkerhedskravene og underretningspligten som fastsat i artikel 16. Det betyder, at virksomheder, som beskæftiger mindre end 50 personer, og som har en årlig omsætning og/eller en samlet årlig balance på ikke over 10 mio. EUR, ikke er bundet af et sådant krav. Ved fastsættelse af en enheds størrelse er det ikke relevant, hvorvidt den pågældende virksomhed udelukkende leverer digitale tjenester i NIS-direktivets forstand, eller om den også leverer andre tjenester.

5. Forholdet mellem NIS-direktivet og anden lovgivning

Dette afsnit fokuserer på lex specialis-bestemmelsen i NIS-direktivets artikel 1, stk. 7, illustreret ved de tre eksempler på lex specialis, som Kommissionen indtil videre har vurderet, og det præciseres, hvilke sikkerhedskrav og hvilken underretningspligt, der gælder for telekommunikationsudbydere og tillidstjenesteudbydere.

5.1. NIS-direktivet, artikel 1, stk. 7: Lex specialis-bestemmelse

I henhold til artikel 1, stk. 7, i NIS-direktivet er bestemmelserne om sikkerhedskrav og underretningspligt for udbydere af digitale tjenester og operatører af væsentlige tjenester i henhold til direktivet ikke gældende, når en sektorspecifik EU-retsakt stiller krav om sikkerhed og underretning om hændelser, forudsat at sådanne krav har mindst samme virkning som de tilsvarende forpligtelser i NIS-direktivet. Medlemsstaterne skal tage højde for artikel 1, stk. 7, i den overordnede gennemførelsen af direktivet og sende Kommissionen oplysninger om anvendelsen af lex specialis-bestemmelser.

Metoder

Når det vurderes, hvorvidt en sektorspecifik EU-retsakt har bestemmelser, der svarer til bestemmelserne i NIS-direktivet, skal der lægges særlig vægt på spørgsmålet om, hvorvidt sikkerhedsforpligtelserne i den sektorspecifikke lovgivning omfatter foranstaltninger, der sørger for sikkerheden i net- og informationssystemer som defineret i direktivets artikel 4, stk. 2.

For så vidt angår underretningspligten, understreges det i artikel 14, stk. 3, og artikel 16, stk. 3, i NIS-direktivet, at operatører af væsentlige tjenester og udbydere af digitale tjenester hurtigst muligt skal foretage en underretning til den kompetente myndighed eller CSIRT af enhver hændelse, der har væsentlige/betydelige konsekvenser for leveringen af tjenesten. Her

[39] EUT L 24 af 20.5.2003, s. 36.

skal der lægges særligt mærke til operatørens/udbyderens forpligtelse til at medtage oplysninger i underretningen til den kompetente myndighed eller CSIRT'en, der gør det muligt at fastslå eventuelle grænseoverskridende konsekvenser af en sikkerhedshændelse.

Der findes for øjeblikket ikke nogen sektorspecifik lovgivning for kategorien udbydere af digitale tjenester, der indeholder bestemmelser om sikkerhedskrav- og underretningspligt, som er sammenlignelige med kravene i artikel 16 i NIS-direktivet, og som kan tages i betragtning ved anvendelsen af artikel 1, stk. 7, i NIS-direktivet[40].

For så vidt angår operatører af væsentlige tjenester, er finanssektoren og især sektorerne bankvæsen og finansielle markedsinfrastrukturer som nævnt i punkt 3 og 4 i bilag II p.t. underlagt de krav om sikkerhed og underretning om hændelser, der er fastsat i EU's sektorspecifikke lovgivning. Det skyldes den kendsgerning, at sikkerheden og soliditeten af de IT-, net- og informationssystemer, som de finansielle institutioner anvender, er en væsentlig del af de krav vedrørende operationelle risici, som EU-retten pålægger de finansielle institutioner.

Eksempler

i) Det reviderede betalingstjenestedirektiv

Hvad angår banksektoren og navnlig hvad angår bestemmelsen om betalingstjenester leveret af kreditinstitutter som defineret i artikel 4, stk. 1, i forordning (EU) nr. 575/2013, indeholder artikel 95 og 96 i det reviderede direktiv om betalingstjenester[41] bestemmelser om sikkerhed og indberetning.

Mere præcist kræves det i artikel 95, stk. 1, at betalingstjenesteudbydere indfører begrænsende foranstaltninger og kontrolmekanismer til styring af drifts- og sikkerhedsrisici, der er forbundet med de betalingstjenester, som de udbyder. Disse foranstaltninger bør omfatte fastlæggelse og opretholdelse af effektive procedurer for håndtering af hændelser, herunder for opdagelse og klassificering af større drifts- og sikkerhedshændelser. I betragtning 95 og 96 i det reviderede direktiv om betalingstjenester præciseres disse sikkerhedsforanstaltninger yderligere. Det fremgår tydeligt af disse bestemmelser, at formålet med de fastsatte foranstaltninger er at håndtere sikkerhedsrisici i forbindelse med de net- og informationssystemer, der anvendes ved levering af betalingstjenester. Disse sikkerhedskrav kan derfor anses for at have mindst samme virkning som de tilsvarende krav i artikel 14, stk. 1 og 2, i NIS-direktivet.

Hvad angår underretningspligt, fastsættes det i artikel 96, stk. 1, i det reviderede direktiv om betalingstjenester, at betalingstjenesteudbydere uden unødig forsinkelse skal underrette den kompetente myndighed om større sikkerhedshændelser. Derudover kræves det i artikel 96, stk. 2, i det reviderede direktiv om betalingstjenester, ligesom det er tilfældet i artikel 14, stk.

[40] Dette berører ikke den anmeldelse af brud på persondatasikkerheden til Den Europæiske Tilsynsførende for Databeskyttelse, der er omfattet af artikel 33 i den generelle forordning om databeskyttelse.
[41] Direktiv (EU) 2015/2366 (EUT L 337 af 23.12.2015, s. 35).

5, i NIS-direktivet, at den kompetente myndighed underretter de andre medlemsstaters kompetente myndigheder, hvis hændelsen har relevans for dem. Denne forpligtelse indebærer samtidig, at rapporteringen af sikkerhedshændelser skal indeholde oplysninger, der gør det muligt for myndighederne at vurdere de grænseoverskridende konsekvenser af en hændelse. Ved artikel 96, stk. 3, litra a), i det reviderede direktiv om betalingstjenester tillægges EBA beføjelser til i samarbejde med ECB at udarbejde retningslinjer for underretningens format og indhold.

Som følge heraf kan det konkluderes, at i henhold til artikel 1, stk. 7, i NIS-direktivet bør både sikkerhedskravene og underretningspligten i artikel 95 og 96 i det reviderede direktiv om betalingstjenester finde anvendelse i stedet for de tilsvarende bestemmelser i artikel 14 i NIS-direktivet for så vidt angår betalingstjenester leveret af kreditinstitutter.

ii) Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre

Hvad angår finansielle markedsinfrastrukturer, indeholder forordning (EU) nr. 648/2012 sammenholdt med Kommissionens delegerede forordning (EU) nr. 153/2013 bestemmelser om sikkerhedskrav for centrale modparter (CCP'er), der kan betragtes som lex specialis. Retsakterne fastsætter navnlig tekniske og organisatoriske foranstaltninger vedrørende sikkerheden i net- og informationssystemer, som med hensyn til detaljeringsgrad går videre end kravene i artikel 14, stk. 1 og 2, i NIS-direktivet og derfor kan anses for at opfylde betingelserne i artikel 1, stk. 7, i NIS-direktivet for så vidt angår sikkerhedskrav.

Mere præcist slår artikel 26, stk. 1, i forordning (EU) nr. 648/2012 fast, at en enhed skal have *"solide forvaltningsordninger, hvilket omfatter en klar organisatorisk struktur med en veldefineret, gennemskuelig og konsekvent ansvarsfordeling og effektive procedurer til at identificere, styre, overvåge og indberette de risici, som den er eller kan blive udsat for, samt hensigtsmæssige interne kontrolmekanismer, herunder solide administrative og regnskabsmæssige procedurer."* Ifølge artikel 26, stk. 3, skal den organisatoriske struktur sikre kontinuitet og regelmæssighed i leveringen af tjenesteydelser og udøvelsen af aktiviteter ved at anvende hensigtsmæssige og forholdsmæssigt afpassede systemer, ressourcer og procedurer.

Desuden præciseres det i artikel 26, stk. 6, at en CCP skal opretholde *"passende informationsteknologiske systemer til at kunne håndtere kompleksiteten, forskelligartetheden og typen af tjenesteydelser, der leveres, og aktiviteter, der udføres, for således at sikre et højt sikkerhedsniveau og beskytte opbevarede oplysningernes integritet og fortrolighed."* Ifølge artikel 34, stk. 1, skal der desuden udarbejdes, gennemføres og opretholdes en passende forretningskontinuitetsplan og en katastrofeberedskabsplan, der skal sikre rettidig genopretning af transaktionerne.

Der gøres nærmere rede for disse forpligtelser i Kommissionens delegerede forordning (EU) nr. 153/2013 af 19. december 2012 om udbygning af Europa-Parlamentets og Rådets

forordning (EU) nr. 648/2012 for så vidt angår reguleringsmæssige tekniske standarder for krav for centrale modparter[42]. Navnlig pålægges centrale modparter ved artikel 4 en forpligtelse til at udvikle passende risikostyringsværktøjer, så de kan styre og indberette alle relevante risici og yderligere præcisere typen af foranstaltninger (f.eks. anvendelse af solide informations- og risikokontrolsystemer, nødvendige ressourcer og den nødvendige myndighed, ekspertise og adgang til alle relevante oplysninger for risikostyringsfunktionen, tilstrækkelige interne kontrolmekanismer såsom forsvarlige administrative og regnskabsmæssige procedurer med henblik på at bistå CCP'ens bestyrelse med overvågning og vurdering af, at CCP'ens risikostyringsregler, -procedurer og -systemer er hensigtsmæssige og effektive).

Derudover henvises der i artikel 9 udtrykkeligt til IT-systemers sikkerhed, og der pålægges konkrete tekniske og organisatoriske foranstaltninger vedrørende opretholdelse af en solid informationssikkerhedsramme for håndtering af IT-sikkerhedshændelser. Sådanne foranstaltninger omfatter mekanismer og procedurer, som sørger for, at tjenesterne er tilgængelige, og at autenticiteten, integriteten og fortroligheden i forbindelse med data beskyttes.

iii) Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU[43]

Hvad angår markedspladser, skal operatører i henhold til artikel 48, stk. 1, i direktiv 2014/65/EU sikre opretholdelse af markedets tjenester i tilfælde af et svigt af dets handelssystemer. Denne generelle forpligtelse er for nyligt blevet yderligere præciseret og suppleret ved Kommissionens delegerede forordning (EU) 2017/584[44] af 14. juli 2016 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2014/65/EU for så vidt angår reguleringsmæssige tekniske standarder om præcisering af organisatoriske krav til markedspladser[45]. Ifølge artikel 23, stk. 1, i nævnte forordning skal markedspladserne etablere procedurer og ordninger for fysisk og elektronisk sikkerhed, der er udformet med henblik på at beskytte deres systemer mod misbrug eller uautoriseret adgang og med henblik på at sikre integriteten af data. Disse foranstaltninger skal gøre det muligt at forebygge eller minimere risiciene for angreb på informationssystemer.

Ifølge artikel 23, stk. 2, skal de foranstaltninger og ordninger, som operatørerne indfører, endvidere gøre det muligt hurtigt at identificere og forebygge eller minimere risici, der er forbundet med uautoriseret adgang, systemforstyrrelser, der i alvorlig grad hindrer eller afbryder et informationssystems funktion, og dataforstyrrelser, der er til skade for tilgængeligheden, integriteten og autenciteten af data. Desuden fastsættes det ved artikel 15 i nævnte forordning, at markedspladserne skal have effektive driftsstabilitetsordninger, der

[42] EUT L 52 af 23.2.2013, s. 41.
[43] EUT L 173 af 12.6.2014, s. 349.
[44] EUT L 87 af 31.3.2017, s. 350
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

sikrer, at systemerne har tilstrækkelig kapacitet, og kan håndtere forstyrrende hændelser. Disse foranstaltninger skal navnlig sikre, at handelen kan genoptages i inden for eller tæt på to timer, og samtidig sørge for, at mængden af tabte data er tæt på nul.

Artikel 16 fastslår desuden, at foranstaltningerne til håndtering og styring af forstyrrende hændelser bør indgå i markedspladsernes driftsstabilitetsplan, og fastsætter også de særlige elementer, som operatøren skal tage i betragtning i forbindelse med indførelse af en driftsstabilitetsplan (f.eks. oprettelse af et særligt sikkerhedsteam, foretagelse af en konsekvensanalyse, der identificerer risiciene, og som gennemgås regelmæssigt).

Indholdet af disse sikkerhedsforanstaltninger taget i betragtning lader det til, at de har til formål at styre og håndtere risici relateret til tilgængeligheden, autenticiteten, integriteten og fortroligheden i forbindelse med data eller leverede tjenester, og det kan derfor konkluderes, at ovennævnte sektorspecifikke EU-lovgivning indeholder sikkerhedskrav, som reelt har mindst samme virkning som de tilsvarende krav i artikel 14, stk. 1 og 2, i NIS-direktivet.

5.2 NIS-direktivet, artikel 1, stk. 3: Telekommunikationsudbydere og tillidstjenesteudbydere

I henhold til artikel 1, stk. 3, anvendes direktivets sikkerhedskrav og underretningspligt ikke for virksomheder, som er omfattet af kravene i artikel 13a og 13b i direktiv 2002/21/EF. Artikel 13a og 13b i direktiv 2002/21/EF gælder for virksomheder, der stiller offentlige kommunikationsnetværk eller offentlige elektroniske kommunikationstjenester til rådighed. Hvad angår levering af offentlige kommunikationsnetværk eller offentlige elektroniske kommunikationstjenester skal de pågældende virksomheder følgelig overholde de sikkerhedskrav og den underretningspligt, der er fastsat i direktiv 2002/21/EF.

Hvis samme virksomheder også leverer andre tjenester såsom digitale tjenester (f.eks. leverer cloud computing-tjenester eller udbyder onlinemarkedspladser), der er omfattet af bilag III til NIS-direktivet, eller tjenester som eksempelvis domænenavnesystemer eller internetudvekslingspunkter, jf. punkt 7 i bilag II til NIS-direktivet, er de imidlertid underlagt sikkerhedskravene og underretningspligten som fastsat i NIS-direktivet for så vidt angår leveringen af disse specifikke tjenester. Det bør bemærkes, at medlemsstaterne grundet det faktum, at udbyderne af de tjenester, der er oplistet under punkt 7 i bilag II, tilhører kategorien operatører af væsentlige tjenester, skal foretage en identificering i henhold til artikel 5, stk. 2, og fastslå, hvilke individuelle udbydere af domænenavnesystemer, internetudvekslingspunkter eller topdomæner skal overholde kravene i NIS-direktivet. Det betyder, at det efter en sådan vurdering kun er de udbydere af domænenavnesystemer, internetudvekslingspunkter eller topdomæner, som opfylder kriterierne i artikel 5, stk. 2, i NIS-direktivet, der skal overholde kravene i NIS-direktivet.

I artikel 1, stk. 3, fastsættes det endvidere, at direktivets sikkerhedskrav og underretningspligt heller ikke anvendes for tillidstjenesteudbydere, som er omfattet af kravene i artikel 19 i forordning (EU) nr. 910/2014.

6. Offentliggjorte nationale strategidokumenter om cybersikkerhed

	Medlemsstat	Strategiens titel og tilgængelige links
1	Østrig	*Austrian Cybersecurity Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgien	*Securing Cyberspace* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulgarien	*Cyber Resilient Bulgaria 2020* (2016) http://www.cyberbg.eu/ (BG)
4	Kroatien	*The national cyber security strategy of the republic of Croatia* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Tjekkiet	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Cypern	*Cybersecurity Strategy of the Republic of Cyprus* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Danmark	*The Danish Cyber and Information Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Estland	*Cyber Security Strategy* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Finland	*Finland´s Cyber security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Frankrig	*French national digital security strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Irland	*National Cyber Security Strategy 2015-2017* (2015)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Italien	*National Strategic Framework for Cyberspace Security* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Tyskland	*Cyber-security Strategy for Germany* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Ungarn	*National Cyber Security Strategy of Hungary* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Letland	*Cyber Security Strategy of Latvia 2014–2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Litauen	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luxembourg	*National Cybersecurity Strategy II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*National Cyber Security Strategy Green Paper* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Nederlandene	*National Cyber Security Strategy 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Polen	*Cyberspace Protection Policy of the Republic of Poland* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Rumænien	*Cybersecurity Strategy of Romania* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Portugal	*National Cyberspace Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view

		(EN)
23	Den Slovakiske Republik	*Cyber Security Concept of the Slovak Republic for 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Slovenien	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Spanien	*National Cyber Security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Sverige	*The Swedish National Cybersecurity Strategy* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Det Forenede Kongerige	*National Cyber Security Strategy (2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Liste over god praksis og henstillinger udstedt af ENISA

Håndtering af hændelser

- ✓ Strategier for håndtering af hændelser og cyberkrisesamarbejde[46]

Håndtering af hændelser

- ✓ Projekt om automatisering i forbindelse med håndtering af hændelser[47]
- ✓ Vejledning i god praksis for håndtering af hændelser[48]

Klassifikation og taksonomi af hændelser

- ✓ Overblik over eksisterende taksonomier[49]
- ✓ Vejledning i god praksis vedrørende anvendelse af taksonomier i forbindelse med forebyggelse og opdagelse af hændelser[50]

CSIRT modenhed

- ✓ Undersøgelse af modenheden af de nationale CSIRT'er i Europa 2016[51]
- ✓ Undersøgelse af CSIRT'ernes modenhed – evalueringsproces[52]
- ✓ Retningslinjer for nationale og reguleringsmæssige CSIRT'er om vurdering af modenhed[53]

CSIRT'ernes kapacitetsopbygning og uddannelse

- ✓ Vejledning i god praksis inden for uddannelsesmetoder[54]

Oplysninger om eksisterende CSIRT'er i Europa – Overblik over CSIRT'er pr. land[55]

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016). Findes på:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation.
[47] Yderligere oplysninger på: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[48] ENISA, *Good Practice Guide for Incident Management* (2010). Findes på:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[49] Yderligere oplysninger på: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies
[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Findes på:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). Findes på:https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). Findes på:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
[53] ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). Findes på https://www.enisa.europa.eu/publications/csirt-capabilities
[54] ENISA, *Good Practice Guide on Training Methodologies* (2014). Findes på:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies
[55] Yderligere oplysninger på: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map