Fejl! Ukendt betegnelse for dokumentegenskab.

FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

Rådsmøde (telekommunikation) den 11. december 2015

DAGSORDEN

1) Forslag til direktiv om net- og informationssikkerhed (KOM (2013) 48)
   - *Fremskridtsrapport* 2

NET- OG INFORMATIONSSIKKERHEDSDIREKTIVET (NIS)

Revideret notat. Ændringer er markeret med fed og kursiv.

1. Resumé

Forslaget har til formål at sikre et højt niveau for net- og informationssikkerhed i EU ved at pålægge medlemsstaterne, de offentlige myndigheder samt en bred række markedsoperatører at foretage en række organisatoriske og sikkerhedsmæssige foranstaltninger. Medlemsstaterne skal bl.a. ***tilpasse deres nationale myndighedsstruktur,*** *samarbejde med myndighederne i de andre medlemsstater, mens* ***en række*** *offentlige myndigheder og markedsoperatører bliver pålagt sikkerhedskrav samt en* ***rapporteringspligt*** *ved sikkerhedshændelser.*

Forslaget skønnes at have lovgivningsmæssige konsekvenser samt mindre statsfinansielle konsekvenser og administrative konsekvenser for erhvervslivet. Det er forventningen, at forslaget vil have positive samfundsøkonomiske gevinster, da det skal bidrage til øget modstandsdygtighed og færre brud på net- og informationssikkerheden til fordel for den generelle funktion af samfundet.

Forslaget er på dagsordenen for rådsmødet (telekommunikation) den 11. december 2015 til fremskridtsrapport.

2. Baggrund

Kommissionen har ved KOM (2013) 48 af 7. februar 2013 fremsendt forslag til et direktiv om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele EU. Forslaget er fremsat med hjemmel i TEUF artikel 114 og skal behandles efter den almindelige lovgivningsprocedure i TEUF artikel 294. Rådet træffer afgørelse med kvalificeret flertal.

Kommissionen offentliggjorde i 2001 sin første meddelelse om net- og informationssikkerhed (NIS), som sidenhen blev fulgt op af en række andre initiativer på EU-plan, herunder oprettelsen af Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) i 2004.

Det seneste tiltag er den fælles meddelelse fra Kommissionen og Unionens Højtstående Repræsentant for udenrigsanliggender og sikkerhedspolitik om en europæisk strategi for cybersikkerhed*,* der blev fremlagt den 7. februar 2013 og vedtaget på Rådet for Generelle Anliggender (GAC) den 25. juni 2013.

Strategiens mål er at garantere et sikkert og pålideligt digitalt miljø samtidig med, at de grundlæggende rettigheder og værdier i EU fremmes og beskyttes. Det foreslåede direktiv er et væsentligt initiativ under strategien.

3. Formål og indhold

Formålet med direktivforslaget er at sikre et højt fælles niveau for net- og informationssikkerhed i forhold til internettet samt private netværk og informationssystemer. Dette er en del af den infrastruktur for informations- og kommunikationsteknologi (IKT), som medlemsstaterne i dag er afhængige af både på nationalt plan og på tværs af landegrænser.

IKT-infrastrukturen er i dag – bortset fra på teleområdet – præget af medlemsstaternes frivillige tilgang til net- og informationssikkerhed, hvilket i henhold til forslaget ikke yder tilstrækkelig beskyttelse mod hændelser og risici i EU.

Krav til sikkerhed og integritet på teleområdet er i dag reguleret i medlemsstaterne på baggrund af artikel 13a og 13b i rammedirektivet om elektronisk kommunikation (herefter rammedirektivet). Udbydere, der er omfattet af rammedirektivet, er derfor undtaget i det foreliggende forslag til et NIS-direktiv.

En hændelse er i forslaget defineret som "enhver omstændighed eller begivenhed, der har en faktisk negativ indvirkning på sikkerheden" og kan opstå som følge af menneskelige fejl, naturbegivenheder, tekniske fejl eller ondsindede angreb. Disse hændelser bliver stadig mere omfattende, de sker hyppigere, og de er mere komplekse.

For at øge niveauet for net- og informationssikkerhed ***forventes direktivet til at indeholde følgende centrale elementer:***

Minimumskapacitet (kapitel II)
Alle medlemsstater pålægges at sikre, at de hver har et minimum af kapaciteter ved at udpege ***minimum*** én national kompetent myndighed for sikkerheden af net og informationssystemer ***og minimum én*** it-beredskabsenhed (CERT)***, oprette et nationalt kontaktpunkt ("single point of contact"), der kan stå for den interne og eksterne koordination samt*** vedtage en national NIS-strategi.

Samarbejdsnetværk (kapitel III)
De nationale kompetente myndigheder og Kommissionen ***forpligtes til at samarbejde ved hjælp af henholdsvis en samarbejdsgruppe, der skal fokusere på ensartet implementering af direktivet, samt et CERT-netværk, der skal fokusere på erfaringsudveksling samt assistere hinanden på frivillig basis.***

Krav til offentlige myndigheder og markedsoperatører (kapitel IV)
Forslaget sigter – med rammedirektivet som forlæg – mod at ***pålægge en række særligt samfundsvigtige markedsoperatører sikkerheds- og rapporteringskrav.***

Markedsoperatører afgrænses i ***det oprindelige direktivforslag*** til særligt kritiske infrastrukturer inden for eksempelvis bank-, energi-, transport- og sundhedssektorerne samt leverandører af informationssamfundstjenester såsom e-handelsplatforme, internetbetalingstjenester, sociale netværk, søgemaskiner, cloud computing-tjenester og applikationsforhandlere. ***Derudover var offentlige myndigheder ligeledes omfattet af det oprindelige forslag, mens***

mikrovirksomheder var undtaget. Anvendelsesområdet er et af de områder, der fortsat udestår under forhandlingerne.

4. Europa-Parlamentets udtalelser

Europa-Parlamentets ændringsforslag til direktivforslaget var til afstemning på plenarforsamlingen den 13. marts 2014.

Ændringsforslagene kan kort opsummeres som følger:

- Det skal være muligt for medlemsstaterne at udpege mere end én kompetent myndighed, når blot der også udpeges et koordinerende kontaktpunkt ***("single point of contact")***. Det ønskes også begrænset, hvilke myndigheder der skal kunne udnævnes som kompetent myndighed. Det skal på tilsvarende måde være muligt at have mere end én CERT til at løse opgaverne efter direktivet – evt. fordelt efter sektorer.

- Direktivforslagets anvendelsesområde ønskes begrænset til de særligt samfundskritiske infrastrukturer, der også skal omfatte "internet exchange points", vandforsyning og fødevarekæden. Offentlige myndigheder og informationssamfundstjenesterne tages på den baggrund ud af direktivforslaget. ***Rapportering*** af hændelser på frivillig basis skal dog fortsat være en mulighed.

- Kriterierne for, hvornår en hændelse er tilstrækkeligt alvorlig til at udløse rapporteringspligt, fastsættes direkte i direktivet i stedet for at være udlagt til delegerede retsakter.

Under forhandlingerne med Europa-Parlamentet har parlamentets vigtigste synspunkter derudover været, at man ønskede at sikre mest mulig harmonisering af direktivets anvendelsesområde. Det har således været vigtigt for Europa-Parlamentet, at medlemsstaterne ikke fik en bred skønsmargin til at afgøre, om en markedsoperatør skulle være omfattet af direktivet.

I relation til anvendelsesområdet har Europa-Parlamentet endvidere fortsat ønsket at undtage de såkaldte informationssamfundstjenester, da disse ikke blev anset for at være relevante at dække. Spørgsmålet om, i hvilket omfang de skal være omfattet, udestår dog fortsat, men forhandlingerne bevæger sig på nuværende tidspunkt i retning af, at sikkerheds- og rapporteringskravene formentlig alene kommer til at gælder ex post for disse.

Derudover har det i relation til karakteren af samarbejdet mellem medlemsstaterne været vigtigt for Europa-Parlamentet, at der var tale om en reel forpligtelse til at samarbejde.

5. Nærhedsprincippet

Det er Kommissionens opfattelse, at forslaget er i overensstemmelse med nærhedsprincippet. Kommissionen fremhæver, at målet med forslaget ikke i tilstrækkelig grad kan opfyldes af medlemsstaterne alene og derfor bedre nås på EU-plan under henvisning til net- og informationssikkerheds grænseoverskridende karakter. En passende grad af samordning mellem medlemsstaterne vil kunne sikre, at trusler og hændelser takles effektivt i den tværnationale sammenhæng, hvori de opstår. En tilgang baseret på frivillighed har hidtil kun ført til samarbejde mellem et mindretal af medlemsstater med højt kapacitetsniveau. Yderligere vurderer Kommissionen, at forskellene mellem de relevante lovgivninger og politikker udgør en hindring for virksomheder, der ønsker at drive forretning i flere lande, og for opnåelse af globale stordriftsfordele.

På det foreliggende grundlag er det regeringens vurdering, at nærhedsprincippet er overholdt.

6. Gældende dansk ret

Ansvaret for net- og informationssikkerheden i Danmark varetages af de respektive sektorer i henhold til sektoransvarsprincippet. Det reguleres på nuværende tidspunkt kun i relation til telesektoren ved § 8 a og §§ 62-64 i lov om elektroniske kommunikationsnet og -tjenester, jf. lovbekendtgørelse nr. 128 af 7. februar 2014 ***(som ændret ved lov nr. 741 af 1. juni 2015)***, og udmøntet i bekendtgørelse nr. 396 af 21. april 2011 om rammerne for informationssikkerhed og beredskab (som ændret ved bekendtgørelse nr. 1025 af 21. august 2013) samt bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og – tjenester (informationssikkerhedsbekendtgørelsen) ***(som ligeledes ændret ved bekendtgørelse nr. 1025 af 21. august 2013). Det bemærkes endvidere, at forsvarsministeren den 7. oktober 2015 har fremsat et lovforslag (L 10) om net- og informationssikkerhed, der vil medføre, at bestemmelserne flyttes over i en ny lov om net- og informationssikkerhed under Forsvarsministeriet.***

Danmark har desuden siden 2011 haft en statslig netsikkerhedstjeneste under Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste, der hviler på lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed samt bekendtgørelse nr. 772 af 26. juni 2014 om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste.

7. Lovgivningsmæssige eller statsfinansielle konsekvenser

Lovgivningsmæssige konsekvenser

Forslaget vil have lovgivningsmæssige konsekvenser ved gennemførsel af direktivet i dansk ret, da der indføres nye krav til alle offentlige myndigheder og i vid udstrækning til markedsoperatører.

Statsfinansielle konsekvenser

Det vurderes, at forslaget vil have begrænsede statsfinansielle konsekvenser i form af omkostninger til foranstaltninger og etableringer relateret til implementeringen og håndhævelsen af

sikkerheds- og rapporteringskravene samt håndteringen af hændelser og trusler. Jævnfør den gældende budgetvejledning afholdes omkostningerne indenfor de relevante ressortministeriers eksisterende rammer.

8. Samfundsøkonomiske konsekvenser

Det er forventningen, at en højere net- og informationssikkerhed vil føre til færre nedbrud og øget modstandsdygtighed i forhold til internetbaseret kriminalitet. Dette kan være med til at forbedre det indre markeds funktion samt bidrage til udviklingen af et digitalt indre marked, og forslaget vurderes på denne baggrund at kunne have positive samfundsøkonomiske konsekvenser.

9. Administrative konsekvenser for erhvervslivet

Forslaget vurderes at få mindre administrative konsekvenser for de omfattede virksomheder, der i forslaget er udpeget som markedsoperatører. De administrative konsekvenser vurderes til dels at bestå af omstillingsbyrder, dels at bestå af løbende byrder. Omstillingsbyrden består i at indføre et øget niveau af informationssikkerhed, herunder med henblik på at efterleve de sikkerhedskrav, der følger af forslaget. De løbende byrder består i at sikre en opdateret risikovurdering og dermed sikringsforanstaltninger, der bl.a. svarer til den teknologiske udvikling, samt anmelde hændelser til den nationale kompetente myndighed.

10. Høring

Forslaget har været sendt i høring i Specialudvalget for Konkurrenceevne-, Vækst- og Forbrugerspørgsmål.

Der er modtaget høringssvar fra Dansk Metal, Dansk Industri/ITEK, Finansrådet, Ingeniørforeningen (IDA), KL, Landbrug og Fødevarer, LO, Rådet for Digital Sikkerhed, Dansk Aktionærforening og FSR–danske revisorer.

Overordnet støtter Dansk Metal, Dansk Industri/ITEK, Ingeniørforeningen (IDA), KL, Landbrug og Fødevarer, LO og Rådet for Digital Sikkerhed forslagets formål om at sikre et højt fælles niveau for net- og informationssikkerheden, men med visse bemærkninger. Finansrådet støtter op om initiativer, der kan dæmme op for den stigende kriminalitet på IT-området, men finder det ikke hensigtsmæssigt at bruge regulering som det vigtigste middel. Dansk Aktionærforening og FSR–danske revisorer har svaret, at de ingen bemærkninger har til forslaget.

Dansk Metal påpeger, at direktivforslagets formål er afgørende vigtig både i forhold til enkeltindividers tillid til digitale tjenester og i forhold til at opnå de mål for informationstjenesters anvendelse, som bl.a. skitseres i Europas Digitale Dagsorden. Endvidere noterer Dansk Metal tilfredshed med, at direktivforslaget lægger op til, at bestemmelserne i direktiv 2002/21/EF (rammedirektivet) udvides til også at gælde for vigtige udbydere af informationssamfundstjenester som defineret i direktiv 98/34/EF (informationsproceduredirektivet).

Dansk Industri/ITEK anbefaler, at der tages initiativer til en grundig offentlig debat om net- og informationssikkerhed fremadrettet, f.eks. ved en konference. DI/ITEK fremhæver området for standarder, og pointerer, at der i det europæiske arbejde kan inddrages materiale, som allerede foreligger fra USA, f.eks. CIP-standarderne lavet af NERC (North American Electric Reliability Corporation) og NIST (National Institute of Standards and Technology), der har udviklet standarder inden for kritisk infrastruktur. DI/ITEK anfører desuden, at grænsen mellem cyberkriminalitet og cyberkrig er ved at blive udvisket, og at EU bør tage initiativer på internationalt niveau i den forbindelse, ligesom at NATO bør inddrages som en væsentlig spiller på dette område i fremtiden.

DI/ITEK foreslår, at strategien og forslaget bør bringes i overensstemmelse med hinanden i forhold til en oplistning af, hvad der er kritiske sektorer, og at området vedrørende vand og varme medtages. Derudover peges der på, at de indbyrdes afhængigheder mellem forskellige kritiske samfundsfunktioner i forbindelse med NIS-strategi og risikovurdering er vigtige og bør adresseres (f.eks. "uden el ingen teleinfrastruktur og betalingsinfrastruktur"). DI/ITEK erkender, at forslaget kan medføre visse omkostninger for dele af det private erhvervsliv, men at det er "penge givet godt ud", fordi det er et vigtigt samfundsproblem, der skal løses. DI/ITEK anbefaler, at sikkerhed gøres til en aktiv del af dansk erhvervspolitik. Sluttelig peges der på, at der generelt bør harmoniseres så meget som muligt af hensyn til virksomheder, der har aktiviteter på alle europæiske markeder.

Finansrådet er skeptisk overfor regulering som middel til at harmonisere sikkerhedsforanstaltninger, idet lovgivning som oftest tager udgangspunkt i en allerede eksisterende teknologi, hvilket kan virke hæmmende, da teknologien hele tiden udvikler sig. Finansrådet anfører endvidere, at man må sikre, at sikkerhedsinitiativer ikke i sig selv udgør en risiko set i lyset af, at bankerne skal udlevere fortrolige oplysninger om sikkerhedshændelser, og at oplysninger hos den offentlige forvaltning er underlagt offentlighedsloven. Finansrådet nævner i relation til forslagets anvendelsesområde om afgrænsningen i forhold til EU-regulering om persondatabeskyttelse, at det er væsentligt at dele informationer om identificerede ulovlige handlinger eller handlinger, hvor der er konkret begrundet mistanke. Databeskyttelsesretten må ikke kunne benyttes som et skalkeskjul for kriminel aktivitet. Vedrørende definition af "risiko" bemærkes, at en privat virksomhed skal tage udgangspunkt i sine egne risici, som ikke nødvendigvis er sammenfaldende med risici i offentligt regi. Slutteligt anfører Finansrådet en række forslag vedrørende sikring af ressourcer til opklaring af it-kriminalitet.

Ingeniørforeningen, IDA, bemærker, at et sikkert og pålideligt digitalt miljø er afgørende for den eksisterende brug af internettet samt for borgeres tillid til at bruge digitale tjenester. Dette er vigtigt for det fremtidige velfærdssamfund, som delvist baserer sig på muligheden for, at både Danmarks og Europas borgere bliver endnu mere digitale i adfærd end tilfældet er i dag. IDA understreger, at der ikke må tillades adgang til at udfordre den enkeltes ret til privatliv eller tillades adgang til private oplysninger udenom normal gældende lovgivning. Det fremhæves også, at forslaget kun er attraktivt, hvis det faktisk medvirker til at sikkerhedsniveauet også i Danmark forhøjes eller i det mindste bevares på det nuværende niveau. Om etablering af samarbejdsnetværket på EU-plan mener IDA, at der kan suppleres med nationale enheder i form af et samarbejde mellem myndigheder og markedsoperatører.

KL peger på, at en indberetningspligt af hændelser til den statslige varslingstjeneste GovCERT vil kræve ressourcer, men at standarder for indberetningen vil gøre omkostningerne overskuelige. KL konstaterer, at der i dag ikke er krav til kommunerne om anvendelse standarder og certificering af det kommunale sikkerhedsniveau. KL har anbefalet ISO27.001-standarden, som anvendes i vid udstrækning i kommunerne i landet. Et krav om stringent anvendelse heraf må forventes at koste ressourcer i kommunerne.

Landbrug og Fødevarer henleder opmærksomheden på, at eventuelle krav rettet mod virksomheder i relation til it-sikkerhedsmæssige foranstaltninger skal afvejes og vurderes med hensyn til deres effektivitet i forhold til de byrder og tekniske begrænsninger, foranstaltningerne medfører.

LO anmoder om, at regeringen er opmærksom på eventuelle administrative konsekvenser for A-kasserne.

Rådet for Digital Sikkerhed anbefaler som DI/ITEK, at der tages initiativer til en grundig offentlig debat om net- og informationssikkerhed, samt at indbyrdes afhængigheder mellem kritiske funktioner kortlægges. Rådet for Digital Sikkerhed finder det i øvrigt både oplagt og nødvendigt med en struktur, der adskiller det civile beredskab fra den nationale myndighed. Rådet for Digital Sikkerhed gør endvidere opmærksom på, at der allerede foregår et stort standardiseringsarbejde inden for it-sikkerhed og peger på amerikanske organer som NERC og NIST.

11. Forhandlingssituationen

Stort set alle bestemmelserne i direktivforslaget har været genstand for meget langvarige og tekniske drøftelser.

I forhold til opbygningen af kapacitet i medlemsstaterne synes der at være generel opbakning til, at det i stor udstrækning skal være op til medlemsstaterne selv at afgøre, hvordan deres myndighedsstruktur indrettes, samt hvordan opgaverne fordeles mest hensigtsmæssigt mellem myndighederne. I relation til samarbejdet på tværs af medlemsstaterne er der desuden bred enighed om, at medlemsstaterne kun forpligtes til at samarbejde i det omfang, det er relevant, samt at dette ikke må ske på bekostning af hensynet til national sikkerhed, herunder særligt i forbindelse med udvekslingen af oplysninger.

Det primære udestående er således sikkerheds- og rapporteringskravenes anvendelsesområde.

I relation til den mere traditionelle gruppe af særligt kritiske infrastrukturer inden for eksempelvis bank-, energi-, transport- og sundhedssektorerne, har der været bred opbakning til at foretage en række præciseringer, således at anvendelsesområdet nu er mere klart, ligesom flertallet af medlemsstater støtter, at "internet exchange points" og vandforsyning bliver tilføjet til listen over markedsoperatører. Derudover har der været generel enighed om at erstatte undtagelsen af de såkaldte mikrovirksomheder med en løsning, hvorved den enkelte medlemsstat vurderer,

om den pågældende markedsoperatør konkret er tilstrækkeligt særligt samfundsvigtig og derfor bør være omfattet af kravene. Ved vurderingen skal der bl.a. lægges vægt på antallet af potentielt berørte brugere, størrelse af markedsandel mv. Der er således tale om en helhedsvurdering, hvor fokus ikke alene bliver på antallet af ansatte samt størrelse af omsætning.

I relation til informationssamfundstjenesterne har der været længerevarende diskussioner om, hvorvidt de skal være omfattet af direktivet, samt i givet fald i hvilket omfang de skal være omfattet af samme sikkerheds- og rapporteringskrav som de mere traditionelle særligt kritiske infrastrukturer. Forhandlingssituationen synes på nuværende tidspunkt at bevæge sig i retning af, at informationssamfundstjenesterne – dog med undtagelse af mikrovirksomheder og små virksomheder – forbliver omfattet af direktivet, samt at de vil blive underlagt lempeligere krav, således at medlemsstaternes tilsynsforpligtelse alene kommer til at gælde ex post, det vil sige, hvis håndhævelsesmyndigheden konkret bliver opmærksom på problemer.

Endelig kan det generelt i forhold til offentlige myndigheder nævnes, at flertallet alene ønsker at beholde disse som en del af anvendelsesområdet, når de leverer samme ydelser som de markedsoperatører, som direktivet ellers vil omfatte.

12. Regeringens generelle holdning

Regeringen støtter, at der er behov for regler i EU, der sikrer et ensartet og højt niveau af net- og informationssikkerhed på tværs af medlemsstaterne. Dette skal ikke mindst ses i lyset af internettets og private netværks grænseoverskridende karakter og betydning for det indre marked. Således støtter regeringen overordnet set, at medlemsstaterne, de offentlige myndigheder samt markedsoperatørerne gennem direktivforslaget pålægges at foretage en række organisatoriske og sikkerhedsmæssige foranstaltninger.

I relation til afgrænsningen af sikkerheds- og rapporteringskravenes anvendelsesområde arbejder regeringen for, at der sikres proportionalitet, således at kun særligt samfundsvigtige markedsoperatører, omfattes af sikkerheds- og rapporteringskravene. I forhold til indholdet af kravene arbejder regeringen ligeledes for, at der sikres proportionalitet.

Overordnet set arbejder regeringen ***således fortsat*** for, at forslaget bør gennemføres via omkostningseffektive løsninger, som ikke medfører unødvendige ekstraomkostninger for medlemsstaterne eller uproportionelle administrative byrder for de omfattede markedsoperatører og offentlige myndigheder.

13. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen har senest været forelagt Folketingets Europaudvalg den 24. maj 2013, 29. november 2013 samt 28. maj 2014 til orientering. ***Forhandlingsmandat blev indhentet den 19. september 2014.***