ERHVERVS- OG VÆKSTMINISTERIET

GRUND- OG NÆRHEDSNOTAT TIL
FOLKETINGETS EUROPAUDVALG

Net- og informationssikkerhedsdirektivet (NIS)

1. Resumé

Forslaget har til formål at sikre et højt niveau for net- og informationssikkerhed i EU ved gennemførelsen af krav til medlemsstaterne. Dette omfatter bl.a. etablering af et nyt samarbejdsnetværk i EU, etablering af en national kompetent myndighed i medlemsstaterne samt krav til offentlige myndigheder og en bred række af private aktører vedrørende sikkerhedsforanstaltninger og anmeldelsespligt ved sikkerhedshændelser.

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

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 en fælles meddelelse fra Kommissionen og Unionens Højtstående Repræsentant for udenrigsanliggender og sikkerhedspolitik om en europæisk strategi for cybersikkerhed, ligeledes fremlagt den 7. februar 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.

Der forelægges Folketingets Europaudvalg et særskilt grund- og nærhedsnotat om den europæiske strategi for cybersikkerhed.

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 afhængig 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. Udbydere, der er omfattet af dette direktiv, er derfor undtaget i det foreliggende forslag til 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 indeholder det foreslåede direktiv følgende centrale emner:

Minimumskapacitet (direktivets kapitel II)
Alle medlemsstater pålægges at sikre, at de hver har et minimum af kapaciteter ved at udpege én national kompetent myndighed for sikkerheden af net og informationssystemer, oprette en it-beredskabsenhed (CERT) og vedtage en national NIS-strategi og NIS-samarbejdsplan.

En national NIS-strategi skal angive strategiske mål og konkrete politiske og lovgivningsmæssige foranstaltninger med henblik på at nå og opretholde et højt niveau for net- og informationssikkerhed. Strategien skal omfatte den nationale NIS-samarbejdsplan, der som minimum skal indeholde:

- En plan til brug ved identifikation af risici og vurdering af potentielle begivenheders (truslers) konsekvenser.
- Definition af roller og ansvarsområder for de forskellige aktører, der er involveret i planens gennemførelse.
- Definition af samarbejds- og kommunikationsprocesser, som sikrer forebyggelse, detektion, reaktion, reparation og genopretning, og er moduleret i forhold til alarmniveauet.
- En køreplan for NIS-øvelser og praktisk uddannelse for at styrke, validere og teste planen.

Samarbejdsnetværk (direktivets kapitel III)
De nationale kompetente myndigheder og Kommissionen skal samarbejde i et netværk, der muliggør sikker og effektiv samordning, herunder også koordineret informationsudveksling via en sikret informationsudvekslingsinfrastruktur samt detektering og indsats på EU-plan. Inden for dette netværk udveksler

medlemsstaterne information og samarbejder for at imødegå trusler og hændelser.

Krav til offentlige myndigheder og markedsaktører (direktivets kapitel IV)
Forslaget sigter – med rammedirektivet om elektronisk kommunikation som forlæg – mod at sørge for, at der udvikles en risikostyringskultur og at der udveksles information om trusler og hændelser mellem den private og offentlige sektor.

Private aktører inden for særligt kritiske områder (se eksempler nedenfor) og offentlige myndigheder forpligtes til:

- at gennemføre risikostyring, dvs. foretage en vurdering af de risici, de står overfor, og til at vedtage passende og forholdsmæssige foranstaltninger til at sikre net- og informationssikkerheden på deres område, samt
- at underrette den nationale kompetente myndighed om enhver hændelse, som i alvorlig grad truer deres net- og informationssystemer, og som har væsentlig indvirkning på kritiske tjenesters kontinuitet og levering af varer.

Særligt kritiske områder er eksempelvis bankvæsen, børser og energiproduktion, -transmission og -distribution samt transport (luftfart, jernbaner, søtransport), sundhed og internettjenester (f.eks. e-handelsplatforme, internetbetalingsportaler, sociale netværk, søgemaskiner, cloud computing-tjenester og applikationsforhandlere) og offentlige myndigheder. Private aktører på disse områder benævnes i direktivforslaget som markedsaktører.

Kravene gælder ikke for såkaldte mikrovirksomheder. Det vil sige virksomheder, der beskæftiger under 10 personer, og som har en årlig omsætning eller samlet årlig balance, der ikke overstiger 15 mio. kr.

4. Europa-Parlamentets udtalelser

Der foreligger endnu ikke en udtalelse fra Europa-Parlamentet.

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 risici 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 nr. 169 af 3. marts 2011 om elektroniske kommunikationsnet og -tjenester (som ændret ved lov nr. 1231 af 18. december 2012) og udmøntet i bekendtgørelse nr. 396 af 21. april 2011 om rammerne for informationssikkerhed og beredskab samt bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og –tjenester (informationssikkerhedsbekendtgørelsen).

Danmark har siden 2011 haft en statslig varslingstjeneste for internettrusler, GovCERT, hvis virksomhed hviler på lov nr. 596 af 14. juni 2011 om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v. samt bekendtgørelse nr. 1304 af 17. december 2012 om vilkår for tilslutning til den statslige varslingstjeneste for internettrusler. GovCERT er en del af Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste. Den nævnte lovgivning administreres af Center for Cybersikkerhed.

7. Lovgivningsmæssige eller statsfinansielle konsekvenser

Lovgivningsmæssige konsekvenser
En vedtagelse af forslaget vil have lovgivningsmæssige konsekvenser, da der indføres nye krav til alle offentlige myndigheder og i vid udstrækning private aktører.

Statsfinansielle konsekvenser
Det vurderes endvidere, at forslaget kan have statsfinansielle konsekvenser, i form af omkostninger til foranstaltninger relateret til risikostyring, etablering af sikringssystemer og anmeldelse af eventuelle hændelser. Jævnfør den gældende budgetvejledning afholdes omkostninger indenfor de relevante ressortministeriers eksisterende rammer.

Kommissionen estimerer, at forslaget kun vil have virkning for EU's budget, hvis medlemsstaterne vælger at tilpasse en bestående infrastruktur til informationsudveksling og ønsker, at Kommissionen skal gennemføre en sådan tilpasning inden for den flerårige finansielle ramme for 2014-2020. Engangsudgiften anslås af Kommissionen til ca. 9,3 mio. kr.. Danmark finansierer i dag ca. 2 pct. af EU's budget. Fastholdes denne finansieringsandel også fremover svarer det til en dansk udgift på ca. 0,2 mio. kr.. Alternativt peger Kommissionen på, at medlemsstaterne kan dele engangsudgiften til tilpasning af en bestående infrastruktur eller beslutte at oprette en ny infrastruktur og afholde omkostningerne hertil, som skønnes at være ca. 75 mio. kr. pr. år.

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 medføre administrative konsekvenser for markedsaktørerne, dvs. de omfattede virksomheder udpeget som markedsaktører. 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 i høring i Specialudvalget for konkurrenceevne, vækst og forbrugerspørgsmål med frist for bemærkninger den 21. februar 2013.

Overordnet støtter Dansk Metal, Dansk Industri/ITEK, Ingeniørforeningen (IDA), 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 direktivets 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 om elektronisk kommunikation) 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 informationsikkerhed 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 skeptiske 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 private aktører.

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. Generelle forventninger til andre landes holdninger

Der er ikke kendskab til andre landes holdninger.

12. Regeringens foreløbige generelle holdning

Det er regeringens foreløbige generelle holdning, at der er behov for regler på EU-niveau, 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 er det væsentligt at sikre lige vilkår for markedsoperatører, som underlægges forpligtelserne. En samordning mellem medlemsstaterne vil kunne sikre, at risici og hændelser håndteres effektivt i den tværnationale sammenhæng på en effektiv og tilfredsstillende måde.

Samtidig er det regeringens foreløbige generelle holdning, at det er vigtigt, at direktivet fastlægger et minimum, for så vidt angår de væsentligste sikkerhedsaspekter. Det bemærkes dog, at det også er regeringens foreløbige generelle holdning, at der skal arbejdes henimod en hensigtsmæssig grænsedragning til spørgsmål af national sikkerhedsmæssig karakter. Der skal endvidere arbejdes for en nærmere tilrettelæggelse og udførelse af opgaverne, herunder eksempelvis fleksibilitet for så vidt angår vilkår, formater og procedurer for anmeldelse af sikkerhedshændelser og i angivelsen af opgaver som en CERT bør varetage.

Det er regeringens foreløbige generelle holdning, at der i højere grad skal sikres et øget samarbejde og øget informationsudvikling vedrørende standarder, og det er i den forbindelse oplagt at skele til allerede eksisterende standarder på området.

Endelig er det regeringens foreløbige generelle holdning, at forslaget bør medføre så få ekstra omkostninger som muligt for medlemsstaterne, samt at der sikres proportionalitet imellem omkostningsniveau og merværdi.

13. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt for Folketingets Europaudvalg.