EØS-notatbasen

Europaparlamentets og Rådets direktiv om tiltak for et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU

Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union

EØS-foreløpig posisjonsnotat — Status: Prepublisert

Nøkkelinformasjon

Kortnavn på saken	NIS-direktivet
Institusjon	Parlament og Råd
Type rettsakt	Direktiv
Gruppe	Rettsakter som krever lov- eller budsjettendring samt rettsakter som krever forskriftsendring som vurderes å gripe vesentlig inn i norsk handlefrihet
Dokument-nr	
KOM-nummer	KOM(2013)48
Basis rettsaktnummer	
Vedlegg/protokoll i EØS-avtalen	**Kapittel i EØS-avtalen**

Spesialutvalgsinformasjon

Spesialutvalg	Kommunikasjoner
Hovedansvarlig(e) departement(er)	JD
Saksbehandler	Christian Mathiessen
Sak opprettet	17.09.2014
Dato sist endret	03.02.2016
Dato sist behandlet i spesialutvalg	19.09.2014

Norsk regelverk

Høringsstart	
Høringsfrist	
Frist for gjennomføring	

Fylker og kommuner

Berører fylker og kommuner	Nei

Lenker

Kommisjonsforslag

PreLex

OEIL

Annen dokumentasjon

Høringsbrev

Høringssvar

Beskrivelse

Sammendrag av innhold

Direktivet pålegger medlemsstatene å sørge for et visst nivå for landets IKT-sikkerhet ved å lage en strategi for sikkerhetsarbeidet, etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) som blant annet skal samarbeide med andre lands CSIRTer, og pålegge operatører og leverandører av samfunnsviktige tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser.

Bakgrunn og formål

EU-kommisjonen fremla 7. februar 2013 et forslag til direktiv om tiltak for å sikre et høyt felles nivå for nettverk- og informasjonssikkerhet i EU. Europaparlamentet og Rådet ble 18. desember 2015 enig om en omforent tekst (se vedlegg «CONSIL-ST_15229_2015_REV_2-EN-TXT» eller EURLEX com 2013 48), som den videre fremstilling baserer seg på. Det går frem av innledningen at teksten ble utferdiget under et visst tidspress, at enkelte forhold ikke er endelig avgjort og at det fortsatt kan komme mindre endringer.

Bakgrunnen for forslaget til direktivet er at det i dag, innen EU, ikke er implementert tilstrekkelige og helhetlige beskyttelsestiltak for å oppnå god nok sikkerhet i nettverk og informasjonssystemer som er særlig viktige for det indre markeds funksjon. Utfordringene er ikke bare grenseoverskridende, men globale. Medlemslandene har ulik kvalitet på de beskyttelsestiltak som er implementert, hvilket medfører en fragmentert tilnærming på EU-nivå. I dag er det på felleseuropeisk nivå kun etablert rettslige rammeverk for informasjonssikkerhet innen ekom-sektoren, jf. Europaparlaments- og rådsdirektiv 2002/21/EF av 7. mars 2002 om felles rammeregler for elektroniske kommunikasjonsnett og –tjenester (rammedirektivet). Det er behov for felleseuropeisk regler om IKT-sikkerhet også for annen type infrastruktur.

Formålet med direktivet er å forbedre det indre markeds funksjon gjennom etableringen av et høyt felles sikkerhetsnivå i viktige nettverks- og informasjonssystemer. Direktivet setter krav til medlemslandenes arbeid med IKT-sikkerhet, til virksomheter som leverer tjenester som er essensielle for det indre markeds samfunnsmessige og økonomiske aktiviteter og til tilbydere av enkelte digitale tjenester. Det er særlig fokus på å sikre kontinuitet i leveransen av de aktuelle tjenestene.

Innhold

1. Nasjonale rammer for nettverks- og informasjonssikkerhet (NIS), jf. kap. II (art. 4 - 7).

Medlemsstatene skal sørge for at de har et minimum av nasjonal kapasitet for å møte IKT-sikkerhetsutfordringer ved å utarbeide en nasjonal NIS-strategi, opprette en nasjonal kompetent myndighet for nettverks- og informasjonssikkerhet og etablere en IKT-beredskapsenhet (Computer Security Incident Response Team - CSIRT).

2. Samarbeid mellom medlemslandene og mellom CSIRTene, se kap. III (art. 8 - 13).

Det skal etableres en samarbeidsgruppe med representanter fra medlemslandene, Kommisjonen og det europeiske byrået for nettverks- og informasjonssikkerhet (ENISA). Samarbeidsgruppens arbeidsoppgaver vil blant annet bestå av utarbeidelsen av handlingsplan for implementering av direktivet, strategiske råd til CSIRT-nettverket, utveksle best-practice om informasjonsdeling relatert til hendelseshåndtering og utveksling av best-practice om kapasitetsbygging, se videre art. 8a nr. 3.

Det skal også etableres et nettverk av nasjonale CSIRTer med representanter fra de nasjonale CSIRTene og CERT-EU. Kommisjonen deltar som observatør og ENISA står for sekretariatet. Nettverkets arbeidsoppgaver vil blant annet bestå av informasjonsdeling om CSIRTenes tjenester, operasjoner og samarbeidskapasiteter, informasjonsdeling om hendelser, samarbeid om felles respons mot hendelser, se videre art. 8b nr. 3.

3. Virksomheters nettverks- og informasjonssystemsikkerhet, se kap IV og IVa (art. 14 – 15)

Virksomheter som faller inn under virkeområdet til rammedirektivet 2002/21/EF og dermed må oppfylle sikkerhetskravene i art. 13a og 13b, er uttrykkelig unntatt fra NIS-direktivet, jf. NIS-direktivet art. 1(3). Det samme gjelder tilbydere av tillitstjenester som faller inn under virkeområdet i Europaparlaments- og Rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og opphevelse av direktiv 1999/93/EF (EIDAS-forordningen).

3.1 Sikkerhet i nettverk og informasjonssystemer tilhørende operatører av essensielle tjenester (operators of essential services), se kap. IV.

Direktivet pålegger medlemsstatene å sørge for at operatører av essensielle tjenester, jf. vedlegg II til direktivet, iverksetter flere sikkerhetstiltak, herunder risikostyring og varslingsplikt om hendelser som har vesentlig virkning (significant impact). Dette er virksomheter som anses særlig viktige for opprettholdelsen av et funksjonsdyktig indre marked og hvis bortfall kan få alvorlige negative konsekvenser for samfunnssikkerheten og økonomiske og samfunnsmessige aktiviteter.

3.1.1 Operatører av essensielle tjenester

Det endelige virkeområdet for direktivet blir fastlagt gjennom en utpekingsprosess i regi av hver enkelt medlemsstat, jf. art. 3a. Som et minimum skal virksomheter som faller inn under underkategoriene i vedlegg II vurderes. En virksomhet defineres som operatør av en essensiell tjeneste dersom følgende kumulative kriterier er oppfylt, jf. art. 3a(1a) :
1. Virksomheten tilbyr en tjeneste som er essensiell for opprettholdelsen av kritiske samfunnsmessige og/eller økonomiske aktiviteter,
2. tjenesteleveransen er avhengig av nettverk og informasjonssystemer, og
3. en hendelse i tjenestens nettverk og informasjonssystemer ville hatt vesentlig forstyrrende virkning på leveransen

For å oppfylle punkt 1 synes det ut i fra direktivets premiss «Linked to article 3a(1)», s. 14, tilstrekkelig å fastslå at virksomheten faktisk leverer en essensiell tjeneste innen en av de nevnte kategoriene.

Medlemsstatene plikter å opprette en liste over alle operatører av essensielle tjenester. Listen skal oppdateres jevnlig og minst hvert andre år.

Ved vurderingen av om en sikkerhetshendelse kan få vesentlig forstyrrende effekt på tjenesteleveransen skal både tverrsektorielle og sektorspesifikke momenter tas i betraktning. Art 3b oppstiller en ikke uttømmende liste med tverrsektorielle momenter som skal vurderes:
a. Antallet brukere som baserer seg på tjenesten
b. Andre vedlegg II-sektorers avhengighet av tjenesten
c. Omfanget og varigheten av hendelsers mulige virkning på økonomiske og samfunnsmessige aktiviteter og samfunnssikkerhet
d. Virksomhetens markedsandel
e. Geografisk område som kan rammes av hendelsen

f. Viktigheten av virksomhetens bidrag til leveranse av tjenesten, med tanke på alternative tjenestetilbydere

3.1.2 Sikkerhetstiltak

Blant annet gjennom innføring av krav om risikostyring, skal medlemsstatene sørge for at operatører av essensielle tjenester iverksetter sikkerhetstiltak som står i rimelig forhold til risikoen de står overfor. Det skal også iverksettes tiltak for å forebygge og minimere virkningen av hendelser i nettverk og informasjonssystemer, med henblikk på opprettholdelse av tjenesteleveransen.

Medlemsstatene skal også sørge for at operatører av essensielle tjenester uten ugrunnet opphold varsler om alvorlige hendelser. Vurderingskriteriene for hendelsens alvorlighet er:
a. Antallet brukere som er rammet av hendelsen
b. Hendelsens varighet
c. Det geografiske området som er rammet

Dette betyr altså at det kun skal varsles om hendelser som faktisk innvirker negativt på tjenesteleveransen. Det skal ikke varsles om fare for slik virkning, ei heller kompromittering av konfidensialitet, tilgjengelighet eller integritet der dette ikke har betydning for tjenesteleveransen. Det er den forhåndsbestemte kompetente myndigheten eller CSIRTen som skal varsles.

3.2 Sikkerhet i nettverk og informasjonssystemer tilhørende tilbydere av digitale tjenester, se kap. IVa.

Direktivet pålegger medlemsstatene å sørge for at også tilbydere av digitale tjenester, jf. vedlegg III til direktivet, iverksetter flere sikkerhetstiltak, herunder risikostyring og varslingsplikt om svært alvorlige hendelser. Det går tydelig frem av motivene at det skal stilles lavere sikkerhetskrav til disse tjenestene da de anses noe mindre viktige enn tjenestene omtalt i 3.1. Det er imidlertid også klare likhetstrekk mellom bestemmelsene for de to kategoriene.

3.2.1 Tilbydere av digitale tjenester

For denne kategorien skal medlemsstatene ikke foreta en utpeking av virksomheter. Dirketivbestemmelsene skal gjelde alle virksomheter som faller inn under vedlegg III:
1. Nettbaserte markedsplasser, jf. art. 3(11e)
2. Nettbaserte søkemotorer, jf. art. 3(11g)
3. Skytjenester, jf. art. 3(11j)

3.2.2 Sikkerhetstiltak

Medlemsstatene skal sørge for at tilbydere av digitale tjenester iverksetter sikkerhetstiltak som står i rimelig forhold til risikoen virksomheten står overfor. Også overfor denne gruppen virksomheter skal det stilles krav om risikostyring. Det skal også iverksettes tiltak for å forebygge og minimere virkningen av hendelser i nettverk og informasjonssystemer, med henblikk på opprettholdelse av tjenesteleveransen.

Til forskjell fra operatører av essensielle tjenester kan medlemslandene, med visse unntak, ikke innføre strengere sikkerhetstiltak for tilbydere av digitale tjenester enn det direktivet legger opp til. Noe av begrunnelsen er at det for tilbydere av digitale tjenester er behov for unionsuniforme sikkerhetskrav.

En annen forskjell er hvilke momenter som skal tas i betraktning ved vurdering av om hendelse skal varsles til kompetent myndighet. For tilbydere av digitale tjenester skal det i tillegg til nevnte momenter for operatører av essensielle tjenester også ses hen til:
d. Omfanget av forstyrrelsen for tjenestens funksjon
e. Omfanget av virkningen for økonomiske og samfunnsmessige aktiviteter

4. Kort om andre regler

NIS-direktivet skal ikke legge begrensninger på medlemsstatenes muligheter til å iverksette tiltak for å ivareta essensielle statsfunksjoner, særlig nasjonal sikkerhet, og opprettholde lov og orden, særlig adgangen til å etterforske, oppdage og iretteføre kriminelle handlinger, jf. art. 1(6b).

Art. 1(7) regulerer forholdet mellom NIS-direktivet og annet sektorspesifikt EU-regelverk. Dersom sektorregelverket medfører minst like god effekt som NIS-direktivet, skal sektorregelverket anvendes.

Behandling av personopplysninger skal etter art. 1a gjennomføres i samsvar med personverndirektivet 95/46/EF.

Merknader og betydning for Norge forutsatt EØS-relevans

Nasjonale rammer for nettverks- og informasjonssikkerhet

Nasjonal strategi for informasjonssikkerhet, med handlingsplan, som ble utgitt 18. desember 2012, dekker langt på vei de krav som direktivet stiller til den nasjonale nettverks- og informasjonssikkerhetsstrategien. De oppgavene som direktivet tillegger den kompetente myndigheten er langt på vei sammenfallende med de oppgaver NSM utfører i dag som fag- og tilsynsmyndighet innenfor sikkerhetslovens rammer. Mottakelse av varsler og oppfølging av gjennomføring av direktivet er nye oppgaver som må delegeres til en eller flere myndigheter.

De oppgaver direktivet tillegger den nasjonale CERTen, slik disse fremgår av direktivets artikkel 7 og av vedlegg 1, sammenfaller i stor grad med de oppgaver som allerede ivaretas av NSMs NorCERT funksjon. Norge har dermed allerede på plass de grunnleggende kapasitetene direktivet pålegger hver medlemsstat å opprette.

Samarbeid mellom medlemslandene og mellom CSIRTene

Opprettelsen av en samarbeidsgruppe skal, i tillegg til å bygge tillit mellom medlemslandene, støtte opp under og legge til rette for strategisk samarbeid mellom medlemslandene, for å realisere direktivet. 18 måneder etter direktivets ikrafttreden, og deretter annethvert år, skal gruppen utforme en arbeidsplan for gjennomføring av gruppens oppgaver i henhold direktivet, jf. art. 8a(3a). Gruppen skal også bidra med strategisk rådgivning for CSIRT-nettverket.

CSIRT-nettverket skal – som samarbeidsgruppen – bidra til å utvikle tillit mellom medlemslandene, og i tillegg fremheve raskt og effektivt operativt

samarbeid mellom medlemslandene. Informasjonsdelingen skal være frivillig, kun ikke-sensitiv informasjon forutsettes delt og medlemslandene kan av hensyn til etterforskning avstå fra å bidra til informasjonsdelingen. Felles respons kan også diskuteres og iverksettes i enkelte tilfeller. Videre skal nettverket selv diskutere et samarbeid utover det direktivet legger opp til.

Det nærmere innholdet i og omfanget for begge former for samarbeid er ment å utvikles over tid, og vil uansett ikke være klart før samarbeidet faktisk setter i gang. Per i dag er det for Norges del allerede etablert et godt samarbeid innen eksempelvis hendelseshåndtering med flere nasjoner, som forvaltes av NSM. Hvorvidt direktivet vil føre til nye eller endrede samarbeidsformer – eventuelt begge deler – må vurderes nærmere senere.

Virksomheters nettverks- og informasjonssytemsikkerhet

Det går frem av kommentarene til direktivet at begrepet sikkerhet i nettverk og informasjonssystemer omfatter både lagret, sendt og behandlet data. Videre er evne til å identifisere risiko for, forebygge, oppdage, håndtere og gjenopprette etter hendelser angitt som aktuelle sikkerhetstiltak. Direktivet fastsetter ikke konkrete og spesifikke krav til sikkerhet utover dette. I stedet skal den enkelte virksomhet som faller inn under direktivets virkeområde gjennomføre en risiko- og sårbarhetsanalyse. Resultatet av analysen skal danne grunnlaget for å iverksette proporsjonale og hensiktsmessige konsekvensreduserende tiltak tilpasset den enkelte virksomhet. I hvilken grad direktivet får konsekvenser for norske virksomheter vil i stor grad avhenge av dagens sikkerhetsnivå i den enkelte virksomhet.

Det kan likevel legges til grunn at flere norske vedlegg II-virksomheter allerede har et sikkerhetsnivå som helt eller delvis tilfredsstiller direktivets krav. Virksomheter som er underlagt sikkerhetsloven vil antakelig overoppfylle direktivets krav. Personopplysningsloven stiller krav til informasjonssikkerheten for virksomheter som etter personopplysningsloven behandler eller er ansvarlig for behandlings av personopplysninger. Kravene oppfyller antakelig langt på vei direktivets krav. Andre virksomheter er underlagt forskjellige grader av krav til sikkerhet. For å få full oversikt må hver virksomhet vurderes konkret. Ikke bare hvilket regelverk virksomheten er underlagt, men det faktiske sikkerhetsnivået. Fravær av regelverk innebærer ikke nødvendigvis fravær av sikkerhetstiltak og motsatt.

Av hensyn til at tilbydere av digitale tjenester i stor grad operer i flere land, må de konkrete sikkerhetskravene harmoniseres i størst mulig grad i hele EU. ENISA og EU-kommisjonen skal bistå i dette arbeidet. Operatører av essensielle tjenester skiller seg fra dette, og kjennetegnes først og fremst ved sin nære tilknytning til fysisk infrastruktur. Dette begrunner en annen tilnærming til harmonisering av sikkerhetsnivå, hvilket for deres tilfelle i større grad vil være opp til det enkelte medlemsland.

Rettslige konsekvenser

En eventuell implementering av direktivet i norsk rett vil forutsette at det etableres en lovhjemmel for de krav direktivet oppstiller. Idet direktivet pålegger private virksomheter plikter, må direktivet alene av hensyn til legalitetsprinsippet, gjennomføres ved lov. Det må vurderes nærmere om gjennomføringen bør skje i egen lov eller gjennom tilpasning av allerede eksisterende regelverk. Gjeldende lov- og forskriftsverk vil måtte gjennomgås og forholdet til eksisterende sektorlovgivning vil måtte vurderes nærmere. Da det per i dag ikke eksisterer regelverk med samme virkeområde som NIS-direktivet, og sikkerhetslovgivningen med unntak av sikkerhetsloven er sektorspesifikk og forskjelligartet, taler hensynet til harmonisering for gjennomføring i én lov. Departementet vil komme tilbake til dette senere.

Økonomiske og administrative konsekvenser

Som det fremgår av gjennomgangen ovenfor vil det endelige virkeområdet for direktivet og omfanget av sikkerhetskravene først bli klart etter en nasjonal prosess. Uten disse to faktorene kan direktivets økonomiske og administrative konsekvenser ikke beregnes nøyaktig, og de følgende betraktningene må anses både foreløpige og ufullstendige.

EU-kommisjonens stab utarbeidet sammen med forslag til direktivtekst en konsekvensanalyse, SWD(2013) 31(executive summary) og 32. Videre er det innhentet en foreløpig konsekvensanalyse fra UK og innspill fra NSM hva gjelder egen virksomhet. NSM bemerker innledningsvis at i den grad det skal utføres en fullstendig analyse av økonomiske og administrative konsekvenser av direktivet, bør dette settes ut til et rådgivningsselskap med god kompetanse innen samfunnsøkonomiske beregninger. NSM bemerker også at deres innspill forutsetter at direktivets funksjon som Nasjonal kompetent myndighet samt funksjon som nasjonal CERT, ivaretas av NSM.

Direktivets overordnede formål er å støtte opp under det indre markeds funksjon og å styrke europeiske virksomheters konkurransedyktighet i en global kontekst. Det uttrykkes i EUs digitale agenda at fortsatt økt digitalisering skal bidra til økonomisk vekst i Europa. En helhetlig og felles tilnærming til sikkerhet i EU er en forutsetning for en vellykket digitalisering. God sikkerhet gjør offentlige og private i bedre stand til å stå imot ulike former for digitale trusler og skaper nødvendig tillit for brukerne av tjenester og mellom samarbeidspartnere.

Det fremholdes i SWD (2013) 31 at det får negative økonomiske konsekvenser om de foreslåtte tiltakene ikke iverksettes. Det påpekes at de mindre utviklede medlemsstatenes konkurranseevne og økonomiske vekst vil undermineres av et lavt sikkerhetsnivå. Gitt nåværende trender vil IKT-sikkerhetshendelser bli mer og mer synlig for både virksomheter og befolkningen, hvilket vil hindre fullføringen av det indre marked.
Derimot forventes det at økt tilgjengelighet, pålitelighet og kvalitet i samfunnskritiske sektorer som i stor grad er avhengig av IKT, vil være fordelaktig for hele EUs konkurranseevne. Videre vil et økt sikkerhetsnivå redusere kostnadene forbundet med sikkerhetsbrudd og IKT-kriminalitet. I tillegg vil økt fokus på risikostyring blant virksomheter kunne stimulere til økt vekst innen sikkerhetsindustrien.

Direktivets elementer som kan medføre økte administrative og økonomiske kostnader:

1. NASJONALE RAMMER FOR NETTVERKS- OG INFORMASJONSSIKKERHET
Norge har i stor grad allerede gjennomført de tiltak Kommisjonen her foreslår. Med unntak av at kompetente myndigheter skal ta imot varsler om sikkerhetshendelser, medfører ikke disse tiltakene økonomiske og administrative konsekvenser av betydning, ifølge SWD (2013) 32. Det legges der til grunn at for stater som per i dag har en godt etablert kapasitet - hvilket er tilfelle for Norge v/NSM - vil innføring av direktivet ikke medføre ytterligere kostnader.

NSM har spilt inn at de etablerte grunnstrukturene er på plass, men at disse må styrkes for å oppfylle direktivets krav til den nasjonale kompetente myndigheten. NSM anslår at håndtering og oppfølging av innrapporterte hendelser, minimum vil kreve en økning på 2-3 årsverk, investeringer knyttet til tilrettelegging av IKT-infrastruktur og styrking av NSMs analysekapasitet. Konsekvensene av gjennomføring av reglene om sikkerhetsrevisjoner vil avhenge av antall, omfang, hyppighet og metodikk. Dette må beregnes nærmere når det endelige direktivet er klart.

NSM NorCERT ivaretar langt på vei de oppgaver som direktivet forutsetter skal ligge til en nasjonal CSIRT-funksjon. Antakelig vil ikke direktivet medføre vesentlige konsekvenser på dette området. NSM har spilt inn at det kan bli aktuelt med infrastrukturinvesteringer og å styrke evnen til redundans og varians i sikker kommunikasjon med eksterne aktører. Nærmere beregninger må avvente til behovet og omfanget er avklart.

SWD (2013) 32 legger til grunn at hver NIS-øvelse vil koste 55 555 euro per medlemsland, samarbeid mellom nasjonale kompetente myndigheter vil koste 6000 per år per medlemsland og arbeid med en felles nettside vil koste 5000 euro for oppstarten og 2400 euro per år for hele EU.

2. SAMARBEID MELLOM MEDLEMSKOMPETENTE MYNDIGHETER

Det må påregnes møter internasjonalt for å ivareta Norges rolle både i samarbeidsgruppen og i CSIRT-nettverket. Det er foreløpig ikke klart hvor mange møter det blir per år i samarbeidsgruppen. Dersom møter i CSIRT-nettverket vil komme i tillegg til dagens internasjonale møtevirksomhet for NorCERT, må det beregnes kostnader utover dagens nivå. Heller ikke her er det klart hvor mange møter det legges opp til hvert år.

3. OFFENTLIGE MYNDIGHETERS OG MARKEDSAKTØRERS NETTVERKS- OG INFORMASJONSSIKKERHET

En aktuell metode for beregning av hvilke økonomiske konsekvenser direktivet vil ha for aktuelle virksomheter, er å se dagens sikkerhetsnivå i den enkelte berørte virksomhet opp mot de krav som det endelige direktivet oppstiller. Dette vil antakelig bli en relativt omfattende oppgave da den enkelte virksomhet må vurderes for seg. For mange berørte virksomheter er det allerede innført flere krav til informasjonssikring, jf. eksempelvis personopplysningsregelverket. Det er grunn til å anta at de sikkerhetstiltak som er gjennomført vil dekke i hvert fall deler av de krav som direktivet oppstiller. Disse virksomhetene vil antakelig måtte investere forholdsmessig mindre i nye sikkerhetstiltak for å oppfylle direktivets krav, sammenlignet med virksomheter som per i dag har en mindre systematisk tilnærming til IKT-sikkerhet.

Først når nærmere detaljer om krav til sikkerhet, hvilke hendelser som skal varsles og omfang av berørte virksomheter, kan det foretas en nærmere analyse av de økonomiske og administrative konsekvenser.
Kommisjonsstabens beregninger i SWD (2013) 32 kan gi en pekepinn på kostnadsnivået for berørte virksomheter. Overføringsverdien for norske forhold må imidlertid vurderes nærmere. Det er også en viss forskjell mellom Kommisjonens opprinnelige direktivforslag og det foreliggende. Departementet legger til grunn at tallene uansett er omtrentelige og at de kan tjene som en pekepinn på kostnadsnivå. Oppsummeringsvis legger Kommisjonsstaben til grunn følgende kostnadsbilde for innføring av regler om risikostyring og rapportering:

- Sikkerhetskostnadene er beregnet til å måtte utgjøre 6,61% av en virksomhets totale IKT-budsjett
- Totalt for alle berørte virksomheter i EU, vil etterfølgelse av direktivet medføre kostnader på til sammen mellom 1 og 2 millarder euro.
- I snitt medfører direktivet økte kostnader for små og mellomstore bedrifter (10-250 ansatte) med mellom 2500 og 5000 euro.
- For energisektoren medfører direktivet ingen økte kostnader, da det antas at tilstrekkelig IKT-sikkerhet er på plass.
- Berørte virksomheter i transportsektoren må øke sin totale IKT-sikkerhetssatsing med 3 prosentpoeng
- I finanssektoren må man øke med 1,2 prosentpoeng
- I helsesektoren må man øke med 2,3 prosentpoeng
- I IKT-sektoren må man øke med 0,7 prosentpoeng
- I offentlig sektor må man øke med 2,4 prosentpoeng
- Rapporteringskostnadene beregnes til 212 500 euro samlet for alle berørte virksomheter i EU.

Departementet kommer tilbake til nærmere om øk/adm-konsekvenser ved utarbeidelsen av det endelige posisjonsnotatet.

Sakkyndige instansers merknader

Forslaget har ikke vært på høring.

Merknader fra SU kommunikasjoner:

Det ble orientert om rettsakten på møte i SU Kommunikasjoner 19. september 2014.

Status

Status per 3. februar 2016:

Ifølge pressemelding fra Rådet 18. desember 2015 hadde Coreper gitt sin tilslutning til Rådets og Paralamentets uformelle enighet om direktivteksten 8. desember 2015.

Teksten skal gjennomgås teknisk og godkjennes formelt først av Rådet og så av Parlamentet. Endelig vedtakelse antas å skje i løpet av våren 2016. Etter ikrafttredelse har medlemsstatene 21 måneder på seg for å gjennomføre direktivet nasjonalt. I løpet av de 6 påfølgende månedene skal operatører av essensielle tjenester pekes ut.

Vurdering

EØS-relevans

Nettverks- og informasjonssystemer globalt og innen EU og EØS er forbundet med hverandre. Store forstyrrelser i ett land kan få konsekvenser for andre land. Nettverks- og informasjonssystemers robusthet og stabilitet, samt kontinuiteten i de sentrale tjenestene er avgjørende for et velfungerende indre marked, og særlig for det digitale indre markeds videreutvikling.

Direktivets hovedformål er å forbedre det indre markeds funksjon. Direktivet har direkte innvirkning på berørte virksomheters rammevilkår og indirekte for alle andre virksomheter ved at sikkerheten i sentral infrastruktur blir bedret. Gjennomføring av direktivet i EU, men ikke i EFTA-landene, vil føre til ulike rammevilkår for virksomheter innad i EØS, og er følgelig ikke i tråd med EØS-avtalens intensjon.

At det er etablert EØS-samarbeid innen områder som har nær sammenheng med det foreslåtte NIS-direktivet - eksempelvis eID og andre elektroniske tillitstjenester, personvern og ekomsektoren, tilsier at det også bør samarbeides om tiltak for å sikre et høyt felles nivå for nettverks- og informasjonssikkerheten.

Det er dessuten grunn til å tro at direktivets intensjon ivaretas bedre ved at det gjennomføres i hele EØS enn kun i EU. Ett av flere eksempler er at Norge vil kunne bidra positivt til og dra nytte av CSIRT-nettverket.

Foreløpig konklusjon:

Forslaget er EØS-relevant og akseptabelt.

Andre opplysninger

Vedlegg

Navn	Filnavn	Type	Opprettet av	Opprettet dato	