DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Adresseliste

Deres ref.	Vår ref.	Dato
	15/5866 - CFM	04.07.2016

Høring - Forslag til EU-direktiv om sikkerhet i nettverk og informasjonssystemer

1. INNLEDNING

Den 7. februar 2013 lanserte EU-kommisjonen EUs strategi for cybersikkerhet, «An Open, Safe and Secure Cyberspace» (JOIN(2013) 1 final). Som ett av flere tiltak for å nå målene i strategien lanserte Kommisjonen samme dag forslag til direktiv om tiltak for et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU (NIS-direktivet) (2013/0027 (COD)). Parlamentet, Rådet og Kommisjonen kom til uformell enighet om en direktivtekst i møte 7. desember 2015, se dok. nr. 5894/16 av 10. februar 2016. Senere har både Kommisjonen og Rådet formelt akseptert denne teksten. Det antas at direktivet vil tre i kraft i EU i august 2016.

Forslaget til Europaparlamentets og Rådets direktiv om tiltak for et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU sendes med dette på alminnelig høring. Siste versjon av direktivteksten av 21. april 2016 (vedlagt), tilgjengelig på blant annet dansk (DA) og engelsk (EN), danner sammen med det foreløpige EØS-posisjonsnotatet (vedlagt) et godt grunnlag for innspill fra

Postadresse	Kontoradresse	Telefon - sentralbord	Avdeling for forebyggende	Saksbehandler
Postboks 8005 Dep	Gullhaug Torg 4a	22 24 90 90	samfunnssikkerhet og	Christian F. Mathiessen
0030 Oslo	0484 Oslo	Org.nr.: 972 417 831	analyse	22245366

høringsinstansene. Det er verdt å merke seg at direktivet vedlegg II og III inneholder lister over hvilke virksomheter som vil bli berørt av direktivet.

Høringsfristen er 15. september 2016.

Les og svar på høringen her: www.regjeringen.no/id2506623
I høringen ønsker Justis- og beredskapsdepartementet å få belyst konsekvensene av å gjennomføre forslaget i norsk rett, slik det lyder i dag.

Høringer er åpne, og alle kan sende innspill til oss. Vi ber om at høringssvar sendes inn digitalt ved å bruke skjemaet for høringssvar på regjeringen.no.

På bakgrunn av høringen vil Justis- og beredskapsdepartementet, i samråd med andre berørte departementer, følge opp arbeidet med NIS-direktivet.

2. OM NIS-DIREKTIVET

2.1 BAKGRUNN OG FORMÅL

Per i dag er det på felleseuropeisk nivå etablert rettslige rammeverk for informasjonssikkerhet innen ekomsektoren, jf. Europaparlaments- og rådsdirektiv 2002/21/EF av 7. mars 2002 om felles rammeregler for elektroniske kommunikasjonsnett og –tjenester (rammedirektivet). Lovgiver (i dette tilfellet EU-parlamentet og Rådet), legger til grunn at det er behov for felleseuropeiske regler om IKT-sikkerhet også for annen type infrastruktur.

Formålet med direktivet er å forbedre det indre markeds funksjon, gjøre EU mer konkurransedyktig i en globalisert verden, skape tillit til digitale tjenester og bidra til økonomisk vekst i Europa.

2.2 DIREKTIVETS HOVEDINNHOLD

Direktivet kan deles i tre hoveddeler, som setter krav til henholdsvis etablering av nasjonale rammeverk for IKT-sikkerhet, etablering av internasjonale samarbeidsfora og IKT-sikkerhet for virksomheter.

2.2.1 Nasjonale rammeverk og internasjonalt samarbeid

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).

Medlemslandene må peke ut en eller flere nasjonale kompetente myndigheter for IKT-sikkerhet, som skal påse at direktivet implementeres nasjonalt. Det går frem av art. 8 at det også skal pekes ut en «single point of contact» som skal ivareta samarbeid mellom medlemslandene, med relevante nasjonale myndigheter i andre land, i samarbeidsgruppen og i CSIRT-gruppen. En eksisterende myndighet kan pekes ut til å være både kompetent myndighet og «single point of contact».

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. 11 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. 12 nr. 3.

2.2.2 Sikkerhet for virksomheter

NIS-direktivet stiller i art. 14 og art. 16 krav til at medlemslandene sørger for sikkerheten i nettverkene og informasjonssystemene tilhørende to kategorier av virksomheter – operatører av essensielle tjenester og tilbydere av digitale tjenester. Det stilles forskjellige sikkerhetskrav til de to kategoriene virksomheter. Felles for alle virksomheter uansett kategori, er at de skal beskytte de nettverk og informasjonssystemer som de benytter seg av i sin virksomhet.

Art. 4(1) definerer hva som etter direktivet omfattes av «nettverk og informasjonssystemer» (uoffisiell oversettelse):

(a) elektronisk kommunikasjonsnett, som definert i rammedirektivet art. 2 (a), overføringssystemer og eventuelt utstyr til svitsjing eller ruting samt andre ressurser, inkludert nettverkelementer som ikke er aktive, som gjør det mulig å overføre signaler via kabel, via radio, optisk eller ved hjelp av andre elektromagnetiske midler, herunder satellittnett, jordbaserte fastnett (linje- og pakkesvitsjede, herunder Internett) og jordbaserte mobilnett, elektrisitetsnett, forutsatt at de brukes til å overføre signaler, nett som brukes til kringkasting over radio eller fjernsyn samt kabelfjernsynsnett, uansett hvilken type informasjon som overføres,

(b) enhver enhet eller gruppe av sammenkoblede eller relaterte enheter, der en eller flere, ved hjelp av et program, utfører automatisk behandling av digitale data, og

(c) digital data som lagres, behandles, hentes eller overføres av elementer som nevnt i (a) eller (b), der formålet er elementenes drift, bruk, beskyttelse eller vedlikehold

Virksomheter som faller inn under virkeområdet til Europaparlaments- og rådsdirektiv 2002/21/EF av 7. mars 2002 om felles rammeregler for elektroniske kommunikasjonsnett og –tjenester (rammedirektivet), og dermed må oppfylle sikkerhetskravene i rammedirektivets 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).

2.2.2.1 Operatører av essensielle tjenester

Direktivet art. 5 pålegger medlemsstatene å identifisere operatører av essensielle tjenester som opererer på deres territorium. Virksomheter som oppfyller de to vilkårene i art. 4(4), anses som operatører av essensielle tjenester. Virksomheten må for det første være opplistet i direktivets vedlegg II. For det andre må virksomheten møte kriteriene i art. 5(2):

a) Virksomheten tilbyr en tjeneste som er essensiell for opprettholdelsen av kritiske samfunnsmessige og/eller økonomiske aktiviteter,
b) tjenesteleveransen er avhengig av nettverk og informasjonssystemer, og
c) en hendelse i tjenestens nettverk og informasjonssystemer ville hatt vesentlig forstyrrende virkning på leveransen

2.2.2.2 Tilbydere av digitale tjenester

For tilbydere av digitale tjenester er det ikke lagt opp til en tilsvarende utpekingsprosess. Art. 16 sier at medlemsstatene skal sørge for at tilbydere av tjenester som opplistet i vedlegg III til direktivet, sikrer sine nettverk og informasjonssystemer. Berørte virksomheter er tilbydere av nettbaserte markedsplasser, jf. art. 4(17), nettbaserte søkemotorer, jf. art. 4(18) og skytjenester, jf. art 4(19).

2.2.2.3 Krav til sikkerhet

For begge kategorier stilles det krav om at en risikobasert tilnærming skal danne grunnlaget for iverksetting av sikkerhetstiltak som står i et rimelig forhold til den risiko den enkelte virksomhet står overfor. Videre stilles det krav om varsling av hendelser som har en alvorlig forstyrrende effekt på leveransen av tjenesten.

2.2.3 Forholdet til annet regelverk

NIS-direktivet legger ikke begrensninger på medlemslandenes muligheter for å sikre kritiske samfunnsfunksjoner, særlig med henblikk på ivaretakelse av nasjonal sikkerhet, eller opprettholde lov og orden, herunder kriminalitetsbekjempelse, jf. art. 1(6). Det følger av art. 1(7) at dersom eksisterende sektorregelverk stiller krav om IKT-sikkerhet eller hendelsesvarsling, og reglene har minst like god effekt som NIS-direktivet, da skal sektorregelverket anvendes.

2.3 FORELØPIG VURDERING AV DIREKTIVETS EØS-RELEVANS

Det er Justis- og beredskapsdepartementets foreløpige vurdering at Norge i dag oppfyller direktivets krav til nasjonale rammeverk. Vi viser blant annet til Nasjonal strategi for informasjonssikkerhet av 18. desember 2012 og NSM NorCERT.

Det er videre vår foreløpige vurdering at direktivet er EØS-relevant. Det innebærer i så fall at det som nå er et direktiv kun for EU, vil kunne bli gjeldende også for EFTA-landene og deres virksomheter.

3. SÆRLIGE SPØRSMÅL TIL HØRINGSINSTANSENE

Justis- og beredskapsdepartementet ber om høringsinstansenes syn på NIS-direktivet. Vi vil også høre deres syn på i hvilken grad deres virksomhet og sektor vil bli berørt og hvilke konsekvenser direktivet kan få for berørte virksomheter og sektorer, herunder økonomiske og administrative konsekvenser. Som en del av høringsinnspillet ber vi om at høringsinstansene opplyser om i hvilken grad det per i dag stilles krav til virksomhetens IKT-sikkerhet.

Direktivet favner vidt og vil potensielt berøre mange virksomheter. Vi ber derfor om at alle høringsinstanser bidrar til at høringen treffer alle som bør høres. Send derfor høringen videre til instanser som er relevante, men som ikke står på den vedlagte høringslisten.

Med vennlig hilsen

Martin Kjellsen
avdelingsdirektør

Christian F. Mathiessen
seniorrådgiver

Dokumentet er godkjent og sendes uten signatur

Høringsinstanser:

Departementene
Statsministerens kontor
Fylkesmennene
Kommunene

Abelia
Accenture
Advokatforeningen
Akademikerne
Akershus universitetssykehus HF
Altibox
Arbeidsgiverforeningen Spekter
Avinor
Bankenes standardiseringskontor (BSK)
Basefarm

BDO
Bedriftsforbundet
BFI
Bluecoat
Boston Consulting Group (BCG)
Bouvet
Broadnet
Brønnøysundregistrene
Cap Gemini
CargoNetAS
Carnegie
CCIS
Computas
Datametrix
Datatilsynet
Deloitte
Den Norske Bank
Den Norske Dataforeningen
Devoteam
Difi
Direktoratet for e-helse
Direktoratet for nødkommunikasjon
Direktoratet for samfunnsikkerhet og beredskap
DNV GL
Elektronisk forpost Norge
Energi Norge
Evry
Experis
EY
Falck Nutec
Finans Norge
FinansCERT
Finanstilsynet
Finnmarkssykehuset HF

Flytoget
Folkehelseinstituttet
Forskningsrådet
Forum for informasjonssikkerhet i kraftsektoren
Garantiinstituttet for eksportkreditt
Gartner Group
Gassco
Green Cargo AB
Grenland Rail AS
Hafslund
Handelshøyskolen BI
Handelshøyskolen i Bergen
Hector Rail AB
Helgelandssykehuset HF
Helse Bergen HF
Helse Fonna HF
Helse Førde HF
Helse Midt-Norge RHF
Helse Møre og Romsdal HF
Helse Nord IKT
Helse Nord RHF
Helse Nord-Trøndelag HF
Helse Stavanger HF
Helse Sør-Øst RHF
Helse Vest Innkjøp HF
Helse Vest RHF
Helse Vest-IKT
HelseCIRT
Helsedirektoratet
Helseregistrene
Helsetilsynet
HEMIT
Hovedredningssentralen Nord
Hovedredningssentralen Sør

Hydro
Høgskolen i Gjøvik
Høgskolen i Nesna
Høgskolen i Oslo og Akershus
Høgskolen i Sør-Trøndelag
Høgskolen i Østfold
Høgskulen i Sogn og Fjordane
Høyskolen i Bergen
Høyskolen i Buskerud og Vestfold
Høyskolen i Harstad
Høyskolen i Narvik
Høyskolen i Telemark
IBM
Ice
IKT-Norge
ITAKT
Jernbanetilsynet
Jernbaneverket
Jotne
Jottacloud
Justervesenet
Kartverket
KBO
KINS
Kommunenes Sentralforbund (KS)
Kongsberg
Konkurransetilsynet
KPMG
KraftCERT
Kripos
Ksat
Kystverket
LKAB Malmtrafikk AB
LO

Luftfartstilsynet
Lyse Elnett
Mattilsynet
McKinsey
Metrologisk institutt
Microsoft
Mnemonic
NAMMO
Nasjonal IKT HF
Nasjonal sikkerhetsmyndighet
NAV
NC Spektrum
Nets
NHO/Næringslivets sikkerhetsorg.
Nkom
NorConsult
Nord Pool AS
Nordea
Nordlandssykehuset HF
Norges Bank
Norges geologiske undersøkelser
Norges miljø- og biovitenskapelige universitet
NorSIS
Norsk Forening for Automatisering
Norsk helsenett
Norsk Helsenett SF
Norsk Olje og Gass
Norsk personvernforening
Norsk regnesentral
Norsk romsenter
Norsk Vann
NRK
NSB AS
NSB Gjøvikbanen

NTNU
NTT Com Security
NUPI
NVE
Næringslivets sikkerhetsorganisasjon
Næringslivets sikkerhetsråd
Oljedirektoratet
Oslo Børs
Oslo kommune
Oslo politidistrikt
Oslo universitetssykehus HF
Petroleumstilsynet
Politidirektoratet
Politiets sikkerhetstjeneste
Politihøyskolen
Posten Norge AS
Proactima
PWC
Registrarforeningen dot-enno
Riksadvokaten
Riksrevisjonen
Safetec
Senter for IKT i utdanningen
SIMULA
Sintef
SJ AB
Sjukehusapoteka Vest HF
Sjøfartsdirektoratet
Skagerak energi
Skatteetaten
Software innovation
Space Norway
Sparebank1
St. Olavs Hospital HF

Standard Norge
Statens helsetilsyn
Statens legemiddelverk
Statens strålevern
Statens vegvesen
Statkraft
Statnett
Statoil
Steria
Sunnaas sykehus HF
Sykehusapotek Nord HF
Sykehusapotekene HF
Sykehusapotekene i Midt-Norge HF
Sykehuset i Vestfold HF
Sykehuset Innlandet HF
Sykehuset Telemark HF
Sykehuset Østfold HF
Sykehuspartner
Sykehuspartner HF
Sørlandet sykehus HF
Tampnet
TDC/Get
Teknologirådet
Teknologisk institutt
Tele 2
Telenor
Telia
Tieto
Toll- og avgiftsetaten
Tågåkeriet I Bergslaget AB
UNINETT CERT
UNINETT/NORID
Unio
Universitetet i Agder

Universitetet i Bergen
Universitetet i Nordland
Universitetet i Oslo
Universitetet i Stavanger
Universitetet i Tromsø
Universitetssykehuset Nord-Norge HF
USIT (NIX)
Vestre Viken HF
Viken fiber
Virke
VPS (verdipapirsentralen)
Watchcom
Westerdals
YS
Økokrim