Nasjonal kommunikasjons-myndighet

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Vår ref.:1603864-2 - 008
Vår dato: 13.9.2016

Deres ref.: 15/5866-CFM
Deres dato: 4.7.2016

Saksbehandler: Elise K. Lindeberg

Høring - EU direktiv om tiltak for et høyt felles sikkerhetsnivå i nettverk og informasjonssystemer i EU (NIS-direktivet)

Nkom viser til brev fra Justis- og beredskapsdepartementet av 4. juli 2016, hvor det bes om høringsinstansenes syn på NIS-direktivet, herunder i hvilken grad egen virksomhet og sektor blir berørt og hvilke konsekvenser direktivet kan få for berørte virksomheter og sektorer - både økonomisk og administrativt. Det bes også opplyst i hvilken grad det pr. i dag stilles krav til virksomhetens IKT-sikkerhet.

Nkom er det sentrale utøvende tilsyns- og kontrollorgan innenfor ekomområdet, og vurderer løpende sikkerhets- og beredskapsnivået i elektroniske kommunikasjonsnett og -tjenester. Samfunnet er i dag helt avhengige av elektronisk kommunikasjon og kompleksiteten i IKT-systemer og ekomnett øker stadig. Utviklingen gjør sentrale samfunnsfunksjoner svært sårbare overfor svikt i og tilsiktede angrep både på systemer, nett og tjenester.

NIS-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.

Nasjonal kommunikasjonsmyndighet
Besøksadresse:
Nygård 1, Lillesand

Postadresse:
Postboks 93
4791 LILLESAND

Tel: 22 82 46 00
Fax: 22 82 46 40
firmapost@nkom.no

NO 974 446 871
www.nkom.no

Nasjonal kommunikasjons-myndighet

Etablering av nasjonale rammeverk for IKT-sikkerhet, etablering av internasjonale samarbeidsfora og Nkom CSIRT

Justisdepartementet har vurdert direktivets krav til nasjonale rammeverk, jf. direktivets kap. II, art 7, og henviser her til Nasjonal strategi for informasjonssikkerhet av 18. desember 2012 og NSM NorCERT når det gjelder oppfyllelse av kravene.

I forhold til direktivet kap II, art. 8 vedrørende utpeking av kompetent myndighet, vil det etter Nkoms vurdering være naturlig at ekommyndigheten blir utpekt som ansvarlig for de aktørene som er nevnt i direktivets vedlegg II, pkt. 7 - digital infrastruktur.

I forhold til direktivet kap II, art. 9 vedrørende etablering av en eller flere CSIRT-enheter, vil Nkom vise til etableringen av Nkom CSIRT som vil kunne dekke ekomsektorens aktører slik disse er identifisert i direktivets vedlegg II.

I Nasjonal strategi for informasjonssikkerhet (2012) med tilhørende handlingsplan, fremgår det at hver sektor skal etablere sektorvise responsmiljøer. Strategien er utgitt av Forsvarsdepartementet, Justisdepartementet, Samferdselsdepartementet og Kommunal- og moderniseringsdepartementet. Sektoransvaret står sterkt i norsk forvaltning, og strategien peker på en tredeling av håndtering- og eventuell eskalering av kritiske hendelser mot norsk infrastruktur:

1.linjehåndtering innenfor den enkelte virksomhet
2.linjehåndtering i sektorvise responsmiljøer og
3.linjehåndtering ved nasjonal CSIRT (NorCERT)

Med Nkom CSIRT er det etablert et grunnleggende IKT-varslingsmiljø internt i Nkom. Kompetanse bygges via faglige samarbeidspartnere og nettverk i inn- og utland med tillitt som en grunnleggende faktor. Det foretas automatisk innsamling av data basert på frivillig rapportering fra tilbydere og partnere. Effektiv håndtering av trussel- og sårbarhetsrelatert informasjon er et suksesskriterium for Nkom CSIRT.

Nkom er opptatt av at implementeringen av direktivets bestemmelser ikke må begrense ekomsektorens rolle i sikringen av kritisk infrastruktur. Når NIS-direktivet fremholder «single point of contact» for deling av informasjon mellom medlemslandene, er det viktig med

inkludering av de ulike sektorene - noe som kan sikres ved at representanter for sektormyndighetene inngår i «single point of contact» eller ved at det etableres rutiner for informasjonsdeling med og mellom de sektorielle miljøene. NSM NorCERT, som det nasjonale kontaktpunktet, vil her ha en viktig rolle med å sørge for at de sektorvise CSIRTene blir tilstrekkelig inkludert både nasjonalt og i det europeiske samarbeidet som NIS-direktivet legger opp til.

I forhold til samarbeidsgruppen som skal etableres i henhold til direktivets art. 11, viser Nkom til ekommyndighetens rolle i forbindelse med forebyggende sikkerhetsarbeid og bevisstgjøringsaktiviteter som også er beskrevet i nasjonal strategi for informasjonssikkerhet. Nkom ønsker å bidra inn mot de nevnte aktiviteter som er listet i direktivets art. 11, herunder deling av «best practice» og bevisstgjøringsaktiviteter.

For digitale tjenester slik disse er identifisert i direktivets vedlegg III, henviser Nkom til den pågående prosess innen EU med revidering av ekomregelverket med mulig utvidelse av både virkeområde og pliktsubjekter. En eventuell utvidelse som omfatter visse typer digitale tjenester vil kunne få betydning for hvem som blir utpekt som ansvarlig for aktørene innen digitale tjenester etter direktivets vedlegg III.

Sikkerhet for virksomheter

Nkom viser til direktivets art. 14 og 16, vedrørende krav til sikkerhet i nettverkene og informasjonssystemene tilhørende to kategorier av virksomheter - operatører av essensielle tjenester og tilbydere av digitale tjenester. Nkom vil først og fremst kommentere direktivets bestemmelser knyttet til essensielle tjenester i art. 14.

I direktivets vedlegg II, pkt. 7 - digital infrastruktur, er det listet opp aktører som hører inn under ekomsektoren. Dette er samtrafikkpunkter på Internett (IXPer), operatører av DNS-tjeneste og registerenheter for toppdomener.

<u>Registerenheter for toppdomener</u>

Registerenheter for toppdomener finnes det bare en av i Norge. Dette er Uninett Norid AS (Norid) som drifter landkodetoppdomenet .no. Tildeling av domenenavn i Norge er regulert gjennom forskrift om domenenavn under norske landkodetoppdomener (domeneforskriften),

som er hjemlet i ekomloven § 7-1 og 10-1. Nkom fører tilsyn med Norid jf. domeneforskriften § 9.

Alle domenenavn under .no er avhengig av at Norids navnetjenere er operative. Mange samfunnsviktige tjenester over internett baserer seg på et velfungerende og tilgjengelig domenenavnsystem. Uten å foregripe vurderingene med hensyn på identifisering av operatører av essensielle tjenester som skal gjøres i henhold til direktivets artikkel 5, nr. 2, anser Nkom det som sannsynlig at deler av tjenestene som Norid tilbyr vil kunne oppfylle kriteriene og bli definert som en operatør av essensielle tjenester. Dette vil i så fall medføre at Norid blir omfattet av krav til sikkerhet og rapportering etter direktivets artikkel 14.

Ekomregelverket har pr. i dag ikke krav til sikkerhet hos Norid tilsvarende det som oppstilles i NIS-direktivet. Det er imidlertid stort fokus på sikkerhet og stabilitet for .no domenet både hos Norid og hos Nkom. Nkom gjennomførte i 2012 et sikkerhetstilsyn hos Norid for å evaluere sikkerhetstilstanden i selve organisasjonen og i de informasjonssystemene som Norid har ansvar for. Norid deltok også i den nasjonale cyberøvelsen for ekom og kraft (NCEK 2015) som Nkom gjennomførte i 2015. Norid rapporterer sikkerhetshendelser til Nkom i henhold til interne sikkerhetsrutiner selv om det pr. i dag ikke foreligger slik plikt etter ekomregelverket.

Med bakgrunn i Nkoms sikkerhetstilsyn i 2012 samt videre oppfølging av sikkerhetstiltak hos Norid, mener Nkom at Norid allerede langt på vei oppfyller de krav til sikkerhet som følger av NIS-direktivet. Etter Nkoms vurdering vil det derfor ikke få større økonomiske eller administrative konsekvenser for Norid å bli identifiseres som en operatør av essensielle og tjenester etter direktivets vedlegg II, pkt. 7.

<u>Operatører av DNS-tjeneste</u>

Operatører av DNS-tjeneste er definert ganske vidt i direktivets artikkel 4 nr 15.

Operatører av DNS-tjeneste vil etter Nkoms oppfatning kunne omfatte tilbydere av internettaksess som samtidig med internettaksess tilbyr DNS-tjeneste til egne kunder. Med bakgrunn i vurderingene som skal gjøres etter direktivets art 5 og videre vurderingen av «Significant disruptive effect» etter artikkel 6, mener Nkom at enkelte tilbydere av internettaksess kan bli definert som operatør av essensielle tjenester.

Nkom fører allerede tilsyn med tilbydere av internettaksess med bakgrunn i ekomregelverket og i de tilfellene tilbydere av internettaksess blir definert som operatør av essensielle tjenester vil tilsvarende sikkerhetsregler som NIS-direktivets bestemmelser allerede gjelde disse tilbyderne. Etter Nkoms mening vil derfor innføring av NIS-direktivet overfor denne gruppen ikke få større administrative og økonomiske konsekvenser.

Det er relevant å vurdere hvorvidt norske registrarer under .no vil omfattes av direktivets bestemmelser [1]. Registrarer er private virksomheter som har inngått avtale med Norid om adgang til å selge og foreta endringsmeldinger for domeneregistreringer under .no. Registrarer tilbyr ofte tilleggstjenester som losji og e-post til sine kunder for de domenenavnene som er registrert hos dem. Norid opplyser at det pr. i dag er 347[2] registrarer under .no. Blant disse er det noen få med store markedsandeler og mange små og mellomstore aktører med mindre markedsandeler. Konsentrasjonen av registrarer i lys av markedssituasjonen er her relevant i forhold til direktivets art. 5 og direktivets art. 6 «Significant disruptive effect» og vurderinger rundt konsekvenser av hendelser hos den enkelte registrar.

Registrarleddet er pr. i dag uten ekomrettslig regulering og er således ikke underlagt sikkerhetskrav eller rapporteringsplikt etter ekomregelverket. Norid har imidlertid flere krav knyttet til stabilitet og drift i sine registraravtaler. Et av kravene som Norid setter ved registrering av domener under .no er at hvert domene «skal betjenes av minst to separate navnetjenere, som kjører på fysisk separate maskiner», jf. navnepolitikken til Norid vedlegg F[3]. Dersom registrarleddet defineres som operatør av essensielle tjenester, vil det etter Nkoms mening få administrative og økonomiske konsekvenser for registrarene.

Samtrafikkpunkter på Internett (IXPs)

Samtrafikkpunkter (IXPs) på internett tilbys i Norge i dag av Universitetet i Oslo ved Universitetets senter for informasjonsteknologi (USIT) som har etablert to samtrafikkpunkter[4] i Oslo (NIX1 og NIX2) samt mindre samtrafikkpunkter i Tromsø, Trondheim, Bergen og Stavanger.

---

[1] https://www.norid.no/no/domeneregistrering/om-registrarer/

[2] https://www.norid.no/no/domeneregistrering/registrarliste/

[3] https://www.norid.no/no/regelverk/navnepolitikk/vedlegg-f/

[4] http://www.uio.no/tjenester/it/nett/fastnett/nix/

Nkom har kontakt med USIT om tilbud av tjenester og drift av denne infrastrukturen, men samtrafikkpunktene er ikke gjenstand for ekomrettslig regulering eller krav til sikkerhet. Dersom en vurdering med bakgrunn i artikkel 5 ender opp med at ett eller flere av samtrafikkpunktene i Norge skal omfattes av direktivets bestemmelser, vil dette kunne få administrative og økonomiske konsekvenser for UiO/USIT.

Implementering av direktivets krav til sikkerhet og hendelserapportering i ekomregelverket

Krav til sikkerhet og hendelserapportering i gjeldende ekomregelverk, har sitt opphav i rammedirektivet 13a og 13b og som har så å si likelydende ordlyd som sikkerhetskravene som oppstilles i NIS-direktivets kap. IV art 14.

For å implementere direktivets bestemmelser om krav til sikkerhet og hendelserapportering for operatører av essensielle tjenester opplistet i vedlegg II - digital infrastruktur, henviser Nkom til ekomloven § 2-10, som stiller overordnede krav til ekomtilbydere vedrørende sikkerhet og beredskap. Nkom vurderer at gjeldende forskriftskompetanse i ekomloven § 2-10 femte ledd gir mulighet til å utvide virkeområdet for sikkerhetsbestemmelsene til også å omfatte essensielle tjenester etter NIS direktivet.

«Myndigheten kan gi forskrifter om oppfyllelsen av pliktene etter paragrafen her, herunder om finansiering. Myndigheten kan i forskrift fastsette at bestemmelsen gjelder andre enn tilbydere.»

Spesifikt i forhold til implementering av direktivets krav til hendelserapportering viser Nkom til varslingsplikten som pr. i dag påligger tilbydere etter i ekomforskriften § 8-5. Nkom skal varsles så raskt som mulig etter hendelser. Dette for å kunne koordinere eventuelle tiltak, samt styre informasjonsflyten mellom de som er involvert i og omfattet av hendelsen.

§ 8-5. Varsel

Tilbyder skal varsle Post- og teletilsynet om hendelser som vesentlig kan redusere eller har redusert tilgjengeligheten til elektroniske kommunikasjonstjenester.

Post- og teletilsynet kan fastsette nærmere prosedyrer for varsling

Nasjonal kommunikasjons-myndighet

Økonomiske og administrative konsekvenser

Vi viser til tidligere kommentarer vedrørende økonomiske og administrative konsekvenser for de enkelte operatører/tilbydere i ekomsektoren. Når det gjelder økonomiske og administrative konsekvenser for Nkom som følge av en implementering av direktivets krav for ovennevnte operatører av essensielle tjenester, vurderes det at slik implementering kan foreta innen etablerte rammer dersom Nkoms satsningsforslag for budsjett 2017 realiseres.

Med hilsen

Torstein Olsen
direktør

Einar Lunde
avdelingsdirektør

Kopi Samferdselsdepartementet, Postboks 8010 Dep., 0030 OSLO