DET KONGELIGE KOMMUNAL- OG MODERNISERINGSDEPARTEMENT

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres ref	Vår ref	Dato
15/5866 - CMF	16/3170-4	12.09.2016

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

Vi viser til brev 04.07.2016.

Kommunal- og moderniseringsdepartementet (KMD) har følgende merknader til saken:

Generelt
Vi er enig i JDs foreløpige vurdering om at Norge i dag oppfyller direktivets krav til nasjonale rammeverk. Vi er også enige med JD om at direktivet er EØS-relevant.

For øvrig noterer KMD seg at direktivet også omfatter skytjenester. Dette understøtter bare betydningen av at det direktivet omfatter hele EØS og ikke bare EU. Fra norsk ståsted er det viktig at alle skytjenester innenfor EØS-området tilfredsstiller krav fra EU mht. både informasjonssikkerhet og personvern. Dette gjelder både for de norske virksomhetene som benytter skytjenester innenfor EØS-området, men det er også viktig dersom vi ønsker etablering av store, internasjonale datasentre i Norge. Det at Norge er omfattet av NIS-direktivet og Personvernforordningen vil være med på å redusere usikkerhet knyttet til Norge som vertsnasjon.

Økonomiske og administrative konsekvenser
Hvilke konsekvenser NIS-direktivet kan få KMD-sektoren er pt. uklart. Dette vil bl.a. avhenge av:

- Hvilke virksomheter i Norge – og da spesielt i offentlig sektor – som skal omfattes av direktivet. Av direktivets artikkel 14 og 15 fremgår det at operatører av essensielle tjenester og tilbydere av digitale tjenester skal omfattes. Operatørene er høyst sannsynligvis allerede underlagt sikkerhetsloven, og de økonomiske og administrative

Postadresse
Postboks 8112 Dep
NO-0032 Oslo
postmottak@kmd.dep.no

Kontoradresse
Akersg. 59
http://www.kmd.dep.no/

Telefon*
22 24 90 90
Org no.
972 417 858

Administrasjonsavdelingen

Saksbehandler
Odd Grønvold
22 24 66 75

konsekvensene vil ikke øke vesentlig som følge av at direktivet implementeres. Den andre gruppen – Tilbyderne – er ikke like klart definert i direktivet, og her vil det være rom for tolkning.

- KMD-sektoren er ikke klart definert i denne sammenheng. Hvilke virksomheter skal omfattes av en vurdering mht. relevans for direktivet? Statsforvaltningen? Fylkesmennene? Dette må avklares mht. den nasjonale oppfølgingen.

Krav til virksomhetenes IKT-sikkerhet per i dag

I høringsbrevet ber JD om at høringsinstansene også opplyser i hvilken grad det per i dag stilles krav til virksomhetenes informasjonssikkerhet.

KMD gir føringer til forvaltningens arbeid med informasjonssikkerhet gjennom eforvaltningsforskriften. Forskriften gjelder for all elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen når ikke annet er bestemt i lov eller i medhold av lov.

Av forskriftens § 15 fremgår det at alle virksomheter er pålagt å ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Difi er gitt i oppgave å gi videre anbefalinger. Disse fremgår av oversikten over bruksområdene til de anbefalte og obligatoriske IT-standardene i offentlig sektor (Referansekatalogen) 4.1 pkt. 2.16.

Difi anbefaler at virksomhetene baserer seg på ISO/IEC 27001 ved etablering av internkontroll/styringssystem på informasjonssikkerhetsområdet. Dette er den mest anerkjente og brukte standarden på området. Standarden er en krav-standard organisert rundt temaene kontekst, lederskap, planlegging, støtte, drift, evaluering og forbedring.

Selv om virksomhetene kun er pålagt å basere seg på denne kravstandarden, ser KMD at mange sliter med implementeringen. Standarden sier ikke fullt ut hvilke prosesser som bør etableres og fungere i virksomheten. Den sier heller ikke hvordan disse prosessene skal implementeres og hvilken sammenheng det er til andre internkontroll-/styringssystem i virksomheten. På denne bakgrunn har KMD gitt Difi i oppdrag å utarbeide et praktisk rettet veiledningsmateriell basert på nevnte standard. Dette veiledningsmateriellet beskriver hvordan virksomheter kan etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet. Difi ønsker også å tilrettelegge for at internkontrollen/styringssystemet innen informasjonssikkerhet blir integrert med virksomhetens øvrige styring og internkontroll. Veiledningsmateriellet er nettbasert, og er åpent tilgjengelig for alle virksomheter, - også dem som ikke er omfattet av eforvaltningsforskriften.

Det forutsettes at omfang og innretning på internkontrollen skal være tilpasset den enkelte virksomhets risiko.

Med hilsen

Hanne Finstad (e.f.)
avdelingsdirektør

Odd Grønvold
fagdirektør

Dette dokumentet er elektronisk godkjent og sendes uten signatur.