HELSE VEST

Justis- og beredskapsdepartementet

Deres ref:	Vår ref:	Saksbehandler:	Dato:
	2016/3012 - 20563/2016	Elisabeth Meland 51963819	15.09.2016

Høring - Forslag til EU-direktivet

Helse Vest RHF viser til ovennevnte.

Vi har bedt om innspill fra våre helseforetak og Helse Vest IKT AS og har mottatt innspill/merknader fra Helse Stavanger HF, Helse Fonna HF og Helse Vest IKT AS.

Helse Vest RHF legger ved innspillene og har for øvrig ingen merknader.

Vennlig hilsen

Ivar Eriksen
eierdirektør

Elisabeth Meland
seniorrådgiver

All elektronisk post til Helse Vest skal sendes til postmottak: post@helse-vest.no

Vedlegg

Kopi til:

Postadresse:
Helse Vest RHF
Postboks 303 Forus
4066 Stavanger

Elektronisk adresse:
post@helse-vest.no
www.helse-vest.no

Besøksadresse:
Nådlandskroken 11
4066 Forus

Generell informasjon:
Sentralbord: 51 96 38 00
Org.nr: 983 658 725

Meland, Elisabeth

Fra: bradley.kevin.folsom@sus.no
Sendt: 9. september 2016 15:54
Til: Meland, Elisabeth
Emne: Høring - Gjennomføring av EUs forordning om elektronisk identifisering - eID - og tillittjenester for elektroniske transaksjoner i det indre marked

Hei,

Helse Stavanger mener at det burde vektlegges kommentar til innhold i direktivet fra nasjonale organer, da virkningen er på statlig nivå. Vi ser at innhold i direktivet har bl.a. kategorisering som er noe annerledes enn det som praktiseres i dag i Norge (f.eks. sikkerhetsnivå for identifikasjon) men at disse forhold vil ikke bli problematisk for Helse Stavanger HF å ta innover seg.

m.v.h.
Brad Folsom

IT-sikkerhetsleder
Helse Stavanger HF

Fra: Baugstø-Hartvigsen, Lars Erik (lars.erik.baugsto-hartvigsen@helse-vest-ikt.no)
Sendt: 14.09.2016 21:00:47
Til: Helse Vest, Postmottak
Kopi: Helse Vest IKT AS, Resepsjon/Postmottak

Emne: Høringssvar fra Helse Vest IKT AS på Forslag til EU-direktiv om sikkerhet i nettverk og informasjonssystemer
Vedlegg: image001.jpg
På basis av utsendt høring knyttet til forslag til EU-direktiv om sikkerhet i nettverk og informasjonssystemer har HVIKT blitt anmodet av regionalt sikkerhetsutvalg å gå igjennom dokumentene i høringen og komme med våre innspill.

Dette har blitt gjort ved at Andreas Espelid (seksjonsleder datakommunikasjon) og Lars Erik Baugstø-Hartvigsen (IKT-sikkerhetsleder) har hatt en gjennomgang av direktivet som er på høring. Vi kommer til at dette i all hovedsak er relevant for HelseCERT og NHN med følgende unntak:

Operatører og leverandører av samfunnsviktige tjenester **kan pålegges IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser**. Begge deler er noe vi tilslutter all den tid man legger opp til *_heving_* av nivået på IKT-sikkerhetskrav i det indre marked. Det fremkommer også at eventuelle strengere krav i enkelte sektorer/løsninger ikke skal trekkes ned som konsekvens av kravene i direktivet som er på høring.

Om økte IKT-sikkerhetskrav
Fra posisjonsnotatet: *«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.»*

Om varsling:
Når det gjelder varsling av alvorlige IKT-sikkerhetshendelser oppfatter vi i utgangspunktet at slike hendelser i Helse Vest da skal varsles til HelseCERT. Vårt samarbeid med HelseCERT er i dag godt, og bør utvides. **Vi kan godt vurdere å allerede nå innarbeide interne krav om varsling til HelseCERT ved alvorlige hendelser – altså i forkant av et pålegg.**

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.

-oOo-

Kort sammendrag av innholdet (fra posisjonsnotatet):
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.

Videre:

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.

-oOo-

Oppsummert: HVIKT tilslutter forslaget til EU-direktiv og ser frem til at dette kommer i drift. HVIKT foreslår også at vi allerede nå etablerer rutiner for varsling av alvorlige hendelser til HelseCERT – i tråd med kravene som vil komme. Vi finner det ikke nødvendig å avgi noen høringsuttalelse ut over dette.

Med vennlig hilsen

Lars Erik Baugstø-Hartvigsen
IKT-sikkerhetsleder
+47 90098999 / lars.erik@helse-vest-ikt.no
Helse Vest IKT
www.helse-vest-ikt.no
HELSE VEST IKT

Fra: haldis.johanne.okland.lier@helse-fonna.no
Sendt: 24.08.2016 10:30:24
Til: Helse Vest, Postmottak
Kopi:

Emne: Innspel til høring - Forslag til EU-direktiv om sikkerhet i nettverk og informasjonssystemer
Vedlegg:

Viser til brev dagsett 07.07.2016 (dykkar ref. 2016/3012-19499/2016). Forslag til EU-direktiv om sikkerhet i nettverk og informasjonssystemer er gjennomgått av IKT-sikkerhetsleiar i Helse Fonna.

Vi ser ikkje at innføringa av direktivet vil medføre ytterligere kostnader for føretaket, og heller ikkje administrative endringar, eller endring av sikkerhetsnivå. Det som kjem fram i forslaget er i stor grad allereie på plass i Norge, underlagt NSM. Krav til sikkerhet finnes i eksisterande lovverk, og helseføretak som handsamar helse- og personopplysningar, er underlagt dette lovverket.

Det som manglar er lovverk som er gjeldande for alle typar verksemder i Norge (private verksemder òg), og dette er venta at departementet vil kome tilbake til seinare. Dette vil ikkje vedrøre helseføretak i stor grad, anna enn eventuelt mer/nytt lovverk å forhalde seg til. Krava er vi allereie underlagt i lovverk som omhandlar helseopplysningar og personvern.

Helse Fonna har ingen ytterlegare kommentarar/innspel til forslaget.

Med helsing
Haldis Ø. Lier
Fagdirektør
Helse Fonna HF