NASJONAL
SIKKERHETSMYNDIGHET

Vår dato 2021-10-20	Vår referanse A03 - S:21/01918-3
Deres dato 2021-07-02	Deres referanse 21/3980-2
Antall vedlegg	Side 1 av 3

Til
Kommunal- og
moderniseringsdepartementet
Postboks 8112 Dep
0032 OSLO

Høring - ny ekomlov

Det vises til Kommunal- og moderniseringsdepartementet sitt høringsnotat om ny ekomlov mv.

Nedenfor følger Nasjonal sikkerhetsmyndighet (NSM) sine merknader.

Cybersikkerhetsforordningen

NSM støtter forslaget til implementering av EUs cybersikkerhetsforordning i norsk rett. For å sørge for en smidig overgang mellom eksisterende og kommende sertifiseringsregimer, samt av hensyn til markedsposisjonen til norske evaluerings- og sertifiseringsorganer anbefaler NSM at forordningen implementeres i norsk rett så snart som mulig.

Datasentre

NSM støtter at datasentre reguleres. Det vises blant annet til NSMs rapport «Helhetlig digitalt risikobilde 2020».

I departementets strategi for datasentre «Norske datasenter», fra i år, foreslås det at datasentre blir vurdert for relevant og formålstjenlig regulering i ekomregelverket for å følge opp den samlede risikoen og sårbarhetene hos en datasenteraktør som samler og drifter aktivitet fra flere ulike virksomheter.

NSM mener det der behov for raskt å få på plass et rettslig rammeverk som stiller krav til sikkerhet i datasentre. Vi støtter derfor den foreslåtte regulering i ekomloven. På sikt bør det imidlertid vurderes om datasentre bør reguleres i egen lov, eller i eventuelt fremtidig regelverk som vil implementere NIS-direktivet i norsk rett.

I forslagets § 3-8 syvende ledd foreslås det en forskriftshjemmel for å kunne gi bestemmelser om sikkerhet i datasentre. Slik bestemmelsen er utformet fremstår det imidlertid for NSM som noe uklart om den fullt ut er dekkende for behovet. Det fremstår ikke klart om bestemmelsen er avgrenset til datasentre som også er «tilbydere» etter forslaget § 1-5 nr. 11, eller er den ment å omfatte også andre aktører og datasentre. Dette bør tydeliggjøres.

Postadresse
Postboks 814
1306 SANDVIKA

Sivil telefon/telefaks
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
postmottak@nsm.no

Militær telefon/telefaks
515 40 00/515 40 09
Internetadresse (URL)
www.nsm.no

Etter NSMs oppfatning er det behov for å regulere alle virksomheter som leverer datasentertjenester i Norge, uavhengig om de er «tilbydere».

NSM antar at den samlede verdien av de data som forvaltes av et datasenter på vegne av offentlige etater og private virksomheter potensielt kan være stor. NSM har imidlertid erfart at det kan være krevende å etablere oversikt over hvilke verdier et datasenter faktisk sett forvalter. Dette forhold, samt hva som er et forsvarlig sikringsnivå for datasentre gitt verdiene de forvalter, bør adresseres i det videre lov- og forskriftsarbeidet.

NSM og de øvrige partene i Felles cyberkoordingeringssenter har tidligere spilt inn behov for rettslig regulering knyttet til identifisering av sluttbruker av IKT-infrastruktur. I håndtering av alvorlig digitale angrep mot virksomheter og myndighetsorganer i Norge har vi ved flere tilfeller opplevd at det er vanskelig å få fastslått hvem som eier infrastruktur som benyttes i slike operasjoner, selv om infrastrukturen står plassert i norske datasentre. En av utfordringene er at det drives fremleie av digital infrastruktur slik at virksomheten som driver datasenteret i Norge ikke kjenner identiteten til sluttbrukeren. NSM ber på denne bakgrunn departementet vurdere om det bør innføres krav om entydig identifisering av sluttbruker også for leie av IKT-infrastruktur, tilsvarende kravet til entydig identifisering av sluttbrukere for person-til-person kommunikasjon i forslaget § 2-8.

NSM anmoder om at det vurderes om forslag til forskriftshjemmel i § 3-8 er tilstrekkelig dekkende for behovet som skissert ovenfor, og om det kan være nødvendig at enkelte forpliktelser lovreguleres.

Til § 11-13

I forslag til § 11-13 tredje ledd (og gjeldende ekomlov § 6-1 første ledd) vises det til at NSM kan ta i bruk frekvenser som er tildelt andre for sikring av konferanserom, jf. sikkerhetsloven § 5-5. Tekniske sikkerhetsundersøkelser som utføres i medhold av sikkerhetsloven § 5-5 kan omfatte «lokaler, bygninger og andre objekter» som en virksomhet alene eller sammen med andre råder over, for å fastslå om uvedkommende kan skaffe seg tilgang til sikkerhetsgradert informasjon ved avlytting, innsyn eller avlesning av signaler. Behovet for unntak etter ekomloven kan tilsvarende gjelde i andre sammenhenger enn kun for sikring av konferanserom. Vi ber om at ordlyden i ny ekomlov å justeres for å reflektere sikkerhetsloven på dette området.

Til kapittel 12

I digitale angrep mot norske virksomheter benytter trusselaktørene i stor grad ondsinnede lenker eller vedlegg for å bryte seg inn hos målet. For å øke sannsynligheten for at brukere hos målet trykker på slike ondsinnede lenker eller åpner vedlegg benytter trusselaktøren e-postdomener som i størst mulig grad etterligner legitime domener, såkalt typosquating. Dette innebærer at trusselaktøren for eksempel oppretter et .no-domene som etterligner navnet til en norsk virksomhet, og dette domenet benyttes så til å sende en e-post til en annen virksomhet. For å avdekke forsøk på kompromittering av norske virksomheter har NSM behov for tilgang til en oversikt over nyopprettede domener. NSM ber om at det vurderes en hjemmel som åpner for at denne informasjonen kan gjøres tilgjengelig for NSM til bruk for oppgaver etter sikkerhetsloven.

Til § 1-5 nr. 21 og 22

I forslag til ny ekomlov § 1-5 nr. 21 og 22 benyttes begrepet «handling». Vi mener begrepet bør endres til «hendelse». Det vises til definisjonen i ekomdirektivet artikkel 2 nummer 42 om enhver «hendelse» som har en reell negativ virkning på sikkerheten i elektroniske

kommunikasjonsnett eller -tjenester. Det er godt dokumentert i de årlige hendelsesrapportene for europeisk ekomsektor som ENISA publiserer at mange av de alvorlige hendelsene er årsaker som vær, vind, skred, flom og teknisk utstyr svikter som følge av slitasje og elde. Slike tilfeldige hendelser kan ramme både ekom-infrastruktur og de eksterne innsatsfaktorer denne infrastrukturen er avhengig av. Alvorlige hendelser som skyldes tilsiktede ondartede handlinger utgjør bare fire prosent av antall alvorlige hendelser som er dokumentert i ENISAs rapport for 2020.

Helg Rager Furuseth
Assisterende direktør

Dette dokumentet er elektronisk godkjent hos Nasjonal sikkerhetsmyndighet og sendes uten signatur.

Mottakerliste

Mottaker	Adresse	Post	Land	Kontaktperson
Kommunal- og moderniseringsdepartementet	Postboks 8112 Dep	0032 OSLO	Norge	

Kopi til:

Justis- og beredskapsdepartementet, Postboks 8005 Dep, 0030 OSLO, Norge