NITO

Forsvarsdepartementet

01. oktober 2018

Vår ref. 536143

Høring – forslag til forskrifter til ny sikkerhetslov
NITO viser til høringsbrev datert 2.7.18 med forslag til forskrifter til ny sikkerhetslov. NITO er Norges største organisasjon for ingeniører og teknologer på alle nivå; bachelor, master og høyere. Vi har over 87.000 medlemmer i alle sektorer.

Generelle bemerkninger
NITO vil påpeke det store behovet for kompetanse som forutsettes ved innføring av forskriftene. NITO mener vi risikerer at lov og forskrift ikke vil fungere etter hensikten, dersom det ikke satses kraftig på å styrke Norges IKT-sikkerhetskompetanse. En rapport fra forskningsinstituttet NIFU anslår at det i 2030 er behov for 15 000 personer med IKT-sikkerhetskompetanse, mens tilgangen vil være 11 000 personer. Forskriften legger for øvrig opp til omfattende ansvar for Nasjonal Sikkerhetsmyndighet (NSM). NITO forutsetter at NSM tilføres tilstrekkelig kapasitet og kompetanse slik at de har bemanning til å utføre disse oppgavene.

Forskriften operer med lange lagringstider. §13 om personhistorikk i forskrift om klarering av personell og leverandører, opererer med lagringstid på opptil 10 år. NITO vil legge til grunn av forskriftene tar hensyn til bestemmelser i GDPR om lagringstid. Forskriften må gi godt nok behandlingsgrunnlag til å hente disse opplysningene.

Forskriftene mangler definisjon og bestemmelser for informasjonssystemsikkerhet
I gjeldende forskrift om informasjonssikkerhet behandles krav til informasjonssystemsikkerhet i §§ 5.1-5.5. Dette er krav til sikkerhet i selve informasjonssystemene. I Forsvarsdepartementets forslag til forskrift er disse paragrafene fjernet. NITO mener dagens bestemmelser må videreføres. Dette er i tråd med forarbeidene som stiller seg eksplisitt bak dagens regelverk. Forarbeidene til sikkerhetsloven er tydelig på at det ikke er konkrete endringsbehov i dagens krav utover tilpasning til ny lov: «*Dagens system for beskyttelse av sikkerhetsgradert informasjon, herunder gradering og beskyttelse av informasjonssystemer, fungerer godt per i dag og har fungert godt i lang tid. Systematikken bygger på, og er nært tilknyttet, NATO-regelverket. Dette innebærer at den også er vel etablert i en rekke land, også utenfor NATO*» (NOU 2016: 19 - Samhandling for sikkerhet s. 167). NITO oppfatter også at Forsvarsdepartementet sluttet seg til denne vurderingen i sitt fremsendte lovforslag (Prop. 153 L (2016-2017)).

De nye forskriftene mangler en tydelig definisjon av IKT-sikkerhet, og dermed legges det opp til at hver enkelt virksomhet skal definere dette selv. Med manglende IKT-sikkerhetskompetanse i Norge er dette en langt mindre forpliktende enn gjeldende forskrift. Det vil også medføre at de nasjonale graderingsnivåene ikke vil få den tiltenkte standardisering. Dermed vil forsvarets definisjon av «BEGRENSET» potensielt blir noe helt annet enn NSMs definisjon av «BEGRENSET». Dette vil igjen forårsake samarbeidsproblemer med andre land og organisasjoner slik som NATO eller EU. NITO frykter at resultatet blir at virksomheter som har samarbeid med andre land, må følge utenlandsk regelverk og ikke det norske, for å være kompatible med sikkerhetsregimet som er internasjonalt anerkjent.

Det umiddelbare problemet er at man ikke vil kunne behandle utenlandsk informasjon i norske IT-systemer som er godkjent etter de nye forskriftene. Forsvaret har per i dag et stort IT-system for

«BEGRENSET» hvor man behandler både nasjonal informasjon og NATO-informasjon («BEGRENSET» og «NATO RESTRICTED»). Til nå har dette fungert fordi sikkerhetsnivået har vært det samme, og beskyttelseskravene for norsk BEGRENSET-informasjon følger NATO-regelverket. Forsvaret er imidlertid i ferd med å investere i en ny IT-løsning for «BEGRENSET», og dersom den etableres etter de nye forskriftene, kan resultatet bli at Forsvaret ikke lenger kan behandle NATO-informasjon på sin hovedplattform. NITO legger til grunn at Forsvarsdepartementet er oppmerksom på kostnadene og ulempene dersom Forsvaret - og samtlige andre virksomheter underlagt sikkerhetsloven - ikke vil være tillatt å behandle NATO-informasjon i sine norske IT-systemer i framtida.

Til Forskrift om klarering av leverandører og personell (klareringsforskriften)
Til §7 om Egenopplysning ved personkontroll - bokstav k. Paragrafen omtaler en plikt til å gi egenopplysninger for slik å kunne oppnå sikkerhetsklarering. Etter vår vurdering bør det så langt som mulig kontrolleres av utenforstående. I den grad det lar seg gjøre, bør det kontrolleres mot f.eks. offentlige registre slik at det ikke blir en papirbestemmelse uten tilstrekkelig sikkerhetsmessig verdi.

Til §29 om Klareringsmyndighet for leverandørklarering. Her heter det at «*Nasjonal sikkerhetsmyndighet klarerer norske leverandører i sikkerhetsgraderte anskaffelser. Utenlandske leverandører klareres av myndighetene i sitt hjemland*». For Norge vil dette kunne slå uheldig ut når det gjelder klarering av leverandører fra land vi ikke har sikkerhetspolitisk samarbeid med. NITO mener at leverandører som er registrert i land vi ikke har sikkerhetspolitisk samarbeid med må klareres av Norske myndigheter, eller land vi har sikkerhetspolitisk samarbeid med.

Det er også uklart om §30 om egenopplysninger fra leverandør gjelder både norske og utenlandsk leverandører. NITO mener det bør tydeliggjøres at krav om egenopplysninger gjelder alle leverandører.

Til Forskrift om myndighetenes roller og ansvar for nasjonal sikkerhet (myndighetsforskriften)

Til kapittel 3
NITO har en kommentar til §§17 – 19. Når det gjelder nasjonal responsfunksjon og nasjonalt varslingssystem for digital infrastruktur mener NITO virksomheter bør ha en mulighet til å anke til JBD/FD, dersom man mener seg urettmessig behandlet av NSM/NorCERT.

Forskrift om virksomhetens arbeid med sikkerhet (Virksomhetsforskriften)

Til kapittel 2
Kapittelet omhandler generelle krav til beskyttelse av skjermingsverdige verdier som dermed danner utgangspunktet og rammen for virksomhetens håndtering av risiko. Høringsnotatet påpeker at de generelle kravene i dette kapitelet vil gjelde for alle virksomheter som blir underlagt loven, uavhengig av hva slags verdier som skal beskyttes.

NITO mener kravet om evaluering er viktig, men kravet bør kun gjelde de produkter som utvikles spesielt for graderte systemer. Det vil si militære kommunikasjonssystem, kryptoprodukter o.l. Slik det nå er formulert vil kravet om evaluering av produkter favne svært bredt.

Kapasiteten som behøves for å evaluere en slik mengde produkter vil kreve store ressurser. I praksis vil det kunne innebære behov for å evaluere tusenvis av produkter, og med en mulig årlig frekvens. Til denne typen evaluering benyttes en rekke fagfelt som krever høy spesialisering. Det vil kreve tilgang på spesialkompetanse og spesialiserte laboratorier. Dette vil kunne bli svært kostbart og tidkrevende å gjennomføre, i den grad det i det hele tatt lar seg gjøre.

En rapport fra EUs byrå for informasjonssikkerhet (ENISA) anslår den totale evalueringskapasiteten i Europa og viser oppnådde resultater slik[1]:

- 2016: 83 produkter
- 2015: 147 produkter
- 2014: 163 produkter

Behovet for evaluering som følge av forslaget i ny forskrift vil altså øke dramatisk, og det bare i Norge. ENISA presiserer også at en rekke av disse evalueringene er re-evalueringer noe som er adskillig mindre i omfang enn en evaluering. Selv om man kan si at kravet om evaluering kan erstattes av sertifiserte produkter, er disse også forholdsvis få.

NITO vil også påpeke at faglig sett er evaluering av tjenester et ukjent begrep i den sammenhengen det benyttes i. Det virker å falle utenfor paragrafens hensikt. Tjenester bør derfor ikke være en del av omfanget i paragrafen.

Kapittel 5
Kapittelet omhandler beskyttelse av informasjon gradert KONFIDENSIELT eller høyere. Kommentar gjelder §44 om Beskyttelse av rom eller lokaler for tale gradert Konfidensielt eller høyere. Det er ikke nevnt noe om at det ikke bør være lov å bringe med seg pc, telefon eller annet utstyr som kan være infiltrert. NITO mener dette ikke bør være mulig.

Generell kommentar til virkeområde og beskyttelse av skjermingsverdig objekt og infrastruktur

NITO merker seg at forskriften presiserer hvilke krav som stilles til departementenes oversikt over virksomheter som behandler sikkerhetsgradert informasjon, eller som råder over informasjonssystemer, objekter og infrastruktur som har betydning for Norges evne til å ivareta nasjonale sikkerhetsinteresser. NITO mener det er svært viktig, slik forskriften beskriver, at departementene har en slik oversikt uavhengig av samfunnsutviklingen, og uavhengig av hvilke avhengighetsforhold som opprettes eller bortfaller på tvers av sektorene. Det finnes alvorlige eksempler på en slik manglende oversikt knyttet til offshoring av IKT-oppgaver.

Med vennlig hilsen

Trond Markussen
President

Steinar Sørlie
Generalsekretær

Saksbehandler:
Lars Ø. Eriksen
lars.eriksen@nito.no

[1] https://www.enisa.europa.eu/publications/overview-of-the-practices-of-ict-certification-laboratories-in-europe/