Difi
Direktoratet for
forvaltning og ikt

Forsvarsdepartementet
Postboks 8126 Dep
0032 Oslo

Vår dato	27.9.2018
Vår referanse	18/00025-55

Deres dato	2.7.2018
Deres referanse	2015/3139-254/FD V 3/ENWA

Saksbehandler: Remi Longva

Høringssvar - forskrifter til ny sikkerhetslov

Vi viser til høring om forslag til forskrifter til ny sikkerhetslov. Vi gir en innledende kommentar om inndelingen i forskrifter, og en avsluttende kommentar om behovet for veiledning. Andre merknader er knyttet til forskriftene slik de fremstår i høringsnotatet.

Inndeling i forskrifter

Departementet ber om innspill på om forslaget til inndelingen i forskrifter er hensiktsmessig. Vår vurdering er at den foreslåtte strukturen vil fungere godt. Det er en fordel for virksomhetene, som skal finne fram til og forstå bestemmelsene som angår dem, at de er samlet i én forskrift; og at denne er pedagogisk godt oppbygd med «styringsaktiviteter» og «sikkerhetstiltak»[1]. Vi tror dette vil fungere bedre enn eksisterende regelverks inndeling i fagområder.

Myndighetsforskriften og klareringsforskriften kan slås sammen til én, ettersom de primært gir bestemmelser for myndigheter og sentrale funksjoner. Vi tror likevel det er mer brukervennlig med to adskilte forskrifter, slik de foreligger i høringsnotatet.

Myndighetsforskriften

Identifisering av skjermingsverdige informasjonssystemer

Sikkerhetsloven § 6-1 fastsetter at Kongen kan gi forskrifter om identifisering av skjermingsverdige informasjonssystemer. Vi konstaterer at departementet ikke foreslår slike regler i denne omgang.

Etter vårt skjønn kan det være hensiktsmessig å klargjøre hvordan slike systemer skal identifiseres. Vi tenker da særlig på systemer som skal anses som skjermingsverdige av annen grunn enn at de behandler sikkerhetsgradert informasjon. To spørsmål fremstår her som særlig aktuelle:

---

[1] Jf. ISO/IEC 27001 for styringsaktiviteter og ISO/IEC 27002 (Annex A i 27001) for sikkerhetstiltak på informasjonssikkerhetsområdet.

- Når vil alternativet «avgjørende betydning for grunnleggende nasjonale funksjoner», jf § 6-1 første ledd annet alternativ, være aktuelt å benytte? Vi antar at dersom sikkerhetsbrudd vil kunne skade grunnleggende nasjonale funksjoner, så skal systemet (som sådan) klassifiseres som objekt/infrastruktur etter lovens § 7-1. Kan systemet sies å ha «avgjørende betydning» dersom sikkerhetsbrudd ikke vil kunne skade grunnleggende nasjonale funksjoner?
- Når vil alternativet behandling av «skjermingsverdig informasjon», jf § 6-1 første ledd første alternativ, være aktuelt å benytte - ut over for sikkerhetsgradert informasjon? Etter lovens § 5-1 dekker begrepet skjermingsverdig informasjon hvor det kan oppstå skade for nasjonale sikkerhetsinteresser dersom informasjonen ... går tapt, blir endret eller blir utilgjengelig. Også på dette området bør grensen mot lovens § 7-1 gås opp.

Vi tror det er viktig å bidra til klarhet på dette området, og at man skaper regler som er harmoniserte. Forskriftsutkastet foreslår regler om utpeking av objekter/infrastruktur, men etterlater tvil om hvordan identifisering eller utpeking av informasjonssystemer skal foregå. Det vil kunne føre til forvirring om hvordan disse skal identifiseres eller utpekes i tilknytning til grunnleggende nasjonale funksjoner.

Pålegg om tilknytning til VDI (§ 12)

Departementet foreslår å videreføre dagens system for frivillig tilknytning til VDI, varslingssystemet for digital infrastruktur. Departementet ber om synspunkter på om sikkerhetsmyndigheten også bør kunne pålegge tiknytning til VDI for alle virksomheter som underlegges loven.

Om en virksomhet bør knytte seg til VDI eller ikke, bør i utgangspunktet avgjøres på samme måte som vurderingen av andre sikkerhetstiltak. Vi viser til utkastet til § 14 i virksomhetsforskriften, og våre merknader til denne. Høringsnotatet gir ikke grunnlag for å konkludere på om VDI vil være et passende og nødvendig tiltak for alle virksomheter som har skjermingsverdig informasjon, skjermingsverdige informasjonssystemer og/eller klassifiserte objekter/infrastruktur. Vi antar i utgangspunktet at vurderingen av negative sideeffekter vil kunne variere.

Tilsynsbestemmelsene (§§ 14-19)

Høringsnotatet legger opp til å forskriftsregulere bestemmelser om ansvars- og oppgavedelingen mellom sikkerhetsmyndigheten og sektortilsyn. Bestemmelsene er lagt på et passende abstraksjonsnivå og gir god veiledning. Ved at bestemmelsene fremgår av forskrift, og ikke bare i instruks, blir de lettere tilgjengelige for brukerne. Det er etter vårt syn også ryddig at ansvarslinjen mellom sektor og sektorovergripende tilsyn fremgår av forskrift.

Virksomhetsforskriften

Forskriften har en god struktur, med krav til styringssystem, generelle krav til beskyttelse, etterfulgt av krav om spesifikke sikkerhetstiltak. Strukturen vil være egnet til at brukerne vil forstå og være i stand til å etterleve bestemmelsene. Dersom det gjøres vesentlige endringer i enkeltbestemmelser, så bør strukturen likevel beholdes.

Vi vil likevel nevne at å vurdere og håndtere risiko er blant de mest sentrale aktivitetene i styringssystemet det stilles krav til i forskriftens kapittel 1. Bestemmelsene om å vurdere og håndtere risiko i kapittel 2 burde flyttes til kapittel 1 «Sikkerhetsstyring», ettersom kapittel 2

omhandler generelle krav til beskyttelse. Det vil gjøre det tydelig for brukerne at aktivitetene for å vurdere og håndtere risiko er blant de mest sentrale styringsaktivitetene.

Helhetlig styring i virksomhetene

Det er fornuftig å basere seg på ISO-standarder for styringsaktiviteter, og la struktur og prinsipper i disse danne utgangspunkt for utforming av bestemmelsene. Det er som kjent anbefalt å basere seg på ISO/IEC 27001 for styring av informasjonssikkerhet[2] i forvaltningsorganer[3], og standarden er i utstrakt brukt i privat sektor nasjonalt og internasjonalt.

Det er viktig med helhetlig tilnærming, fordi loven begrenser seg til tilsiktede handlinger. Traavik-utvalget omtalte dette i NOU 2016:19: «Selv om utvalget ikke foreslår en all hazards-tilnærming i den nye loven, vil utvalget presisere viktigheten av at virksomhetene har en helhetlig tilnærming til hvordan risiko skal håndteres når det kommer til operasjonaliseringene av de krav som stilles til virksomhetene, både etter en ny sikkerhetslov og etter øvrig regelverk som er relevant for den enkelte virksomhet.»

De verdiene som skal beskyttes iht. loven er også utsatt for andre trusler, og virksomhetene skal arbeide med sikkerhet for verdier som loven ikke omfatter. De bør oppfordres til å arbeide helhetlig med dette. En helhetlig tilnærming vil inkludere alle kilder til uønskede hendelser, og alle typer konsekvenser. Vi tenker da på kilder som uhell, menneskelige feil, teknisk svikt og naturhendelser; og konsekvenser som kan angå effektivitet, økonomi, liv og helse, personvern mv. God styring og kontroll i virksomheten som helhet ventes å føre til bedre styring og kontroll med det som faller innenfor sikkerhetsloven område. Dette vil være mest formålseffektivt og kostnadseffektivt for den enkelte virksomhet, og i sum det antatt beste samfunnsøkonomisk og samfunnssikkerhetsmessig.

Etter vår vurdering bør § 2 «Styringssystem for sikkerhet» utvides med krav om at det skal være en del av virksomhetens helhetlige styringssystem.

§ 3 «Styringsdokument for det forebyggende sikkerhetsarbeidet» bør omarbeides fra krav om et spesifikt dokument, til krav om at virksomhetens leder gir føringer for styringsaktivitetene, inkludert roller og ansvar, som er hensiktsmessige for et velfungerende sikkerhetsarbeid, og at disse er dokumentert. Det bør være tydelig at det er føringer for sikkerhetsarbeidet etter sikkerhetsloven, men at de gjerne kan inngå sammen med andre føringer for risikostyring generelt, og sikkerhetsstyring spesielt, slik at sikkerhetslovens krav ivaretas som en del av en effektiv helhet.

Definisjoner (§ 1)

Departementet ber om høringsinstansenes syn på om definisjonene er nødvendig, og på om det er andre begreper som bør defineres.

I NOU 2016:19 kunne vi lese at «Med begrepet informasjonssystem menes systemer som anvendes for å løse en oppgave eller utføre en funksjon i en organisasjon. Det omfatter

---

[2] Når vi omtaler «informasjonssikkerhet» så mener vi både det lovproposisjonen kaller «informasjonssikkerhet» og «informasjonssystemsikkerhet», for alle typer informasjonssystemer.
[3] Jf. eForvaltningsforskriften § 15 og referansekatalogen for IT-standarder i offentlig forvaltning.

menneskelige, organisatoriske og tekniske ressurser, metoder og teknikker». Lovproposisjonen klargjør at det er denne definisjonen som legges til grunn. Beskrivelsen ligner på den føderale myndigheter i USA benytter[4]. Definisjonen av «informasjonssystem» i den gamle sikkerhetslovens § 3 begrenser seg til teknologi – tilsvarende slik begrepet «IKT-system» ofte benyttes. Begrepet er nok ikke å anse som selvforklarende, det er ikke definert i loven, og ettersom begrepet har nytt innhold i det nye regelverket bør det klargjøres i forskriften.

Vurdering av risiko (§ 11)

Iht. lovens § 4-2 så danner vurdering av risiko grunnlaget for virksomhetens iverksetting av forebyggende sikkerhetstiltak. I høringsnotatets kapittel 7.3.1 går det frem at «Formålet er å kunne fastslå mulig konsekvens av og tilhørende sannsynlighet for potensielle hendelser.» Det man ønsker å oppnå med forskriftsbestemmelsen er altså å gi føringer hvor hvordan virksomhetene skal vurdere risiko, slik at de er i stand til å fastslå mulige konsekvenser og tilhørende sannsynlighet for potensielle hendelser som kan påvirke sikkerheten; som videre er vurderingsgrunnlaget for behovet for å gjøre endringer for å oppnå eller opprettholde «forsvarlig sikkerhetsnivå».

For å kunne arbeide med, vurdere og forstå risiko benytter man som regel en form for risikomodell – der forskjellige elementer eller faktorer inngår. Eksempler på dette er NISTs risikomodell[5], og de elementene som er beskrevet i ISO/IEC 27005, IRAM2 eller NS 583x.

Utkastet til § 11 begrenser seg imidlertid til å peke på noen få av de relevante elementene i risikovurderingen. Det er bra at man peker på behov for å vurdere trusler og sårbarheter, men elementene som listes opp i bestemmelsen er i seg selv ikke tilstrekkelig for å få en god forståelse av risikoen[6].

De som skal etterleve regelverket kan bli forledet til å tro at de elementene som listes opp i bestemmelsen er tilstrekkelig for å vurdere risiko, og kan komme til å se bort fra elementer som høringsnotatet trekker fram som viktige for formålet. Vi anbefaler derfor at man eksplisitt nevner konsekvenser og deres tilhørende sannsynlighet i listen over elementer som skal hensyntas i vurderingene[7]. Høringsnotatet er tydelig på at dette er viktige elementer, og disse bør derfor nevnes eksplisitt i bestemmelsen.

Føringer for vurdering av sannsynlighet bør ikke være mer omfattende enn at det vil være tilstrekkelig om virksomhetene gjør fornuftige anslag, så langt det er mulig, basert på tilgjengelig kunnskap.

For øvrig vil vi peke på behovet for en viss fleksibilitet slik at virksomhetene kan benytte metoder og fremgangsmåter som er hensiktsmessig i forskjellige sammenhenger, og iht. fremtidige behov som vi ikke har oversikt over i dag.

---

[4] NISTIR 7298 Revision 2 – Glossary of Key Information Security Terms
[5] NIST SP 800-30 Revision 1, figur 3 i kapittel 2.
[6] Vi går ut fra at «verdi» også inngår, implisitt, ettersom forskriften omtaler «skjermingsverdige verdier».
[7] Eks. inneholder NISTs modell alle elementene som her er nevnt: trusler (threat source/threat event), sårbarheter (vulnerability/effectiveness of controls), konsekvenser (adverse impact) og sannsynlighet knyttet til konsekvensen (likelihood - de benytter også to andre sannsynligheter i sin modell).

Valg av sikkerhetstiltak (§ 14)

Utformingen av bestemmelsen er god, og vi er enig i at slike prinsipper hører hjemme i forskriften.

Lovens § 4-3 er svært tydelig på at kostnadene ved sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås ved tiltaket. Pedagogiske hensyn taler for å inkludere dette sentrale lovkravet i forskriftens liste over relevante momenter, ved at kost/nytte-prinsippet føyes til listen. Det vil bidra til bedre etterlevelse, og gi en mer brukervennlig forskrift – ved at prinsippene er samlet på ett sted.

Sikkerhetstiltak har en forventet ønsket effekt, en kostnad og potensielle negative sideeffekter. Vurdering av potensielle negative sideeffekter bør legges til listen over prinsipper som skal legges til grunn ved valg av sikkerhetstiltak. Dette er spesielt viktig ettersom negative sideeffekter kan påføre virksomhetene indirekte kostnader, f.eks. mindre effektiv gjennomføring av oppgaver, jf. lovens § 4-3. Bestemmelsens siste ledd omhandler deler av det som kan være negative sideeffekter. Vi tror likevel det er bedre om det først stilles et generelt krav til å ta potensielle negative sideeffekter med i vurderingen. Videre kan det stilles krav til spesifikke sideeffekter som skal vurderes.

Dette kan f.eks. gjøres ved å føye til ny bokstav f) kost-nytte: tiltakets forventede effekt skal stå i et rimelig forhold til dets kostnader, herunder også tiltakets potensielle negative sideeffekter.

Om offentlige anskaffelser (§ 17 og §§ 70-78)

§ 17 stiller krav om at det skal avtales hvordan sikkerheten ivaretas generelt, også når det gjelder anskaffelser som ikke faller inn under reglene for sikkerhetsgraderte anskaffelser. Det fremgår av merknadene til bestemmelsen at det her siktes til de samme krav om sikkerhetsavtale som i sikkerhetsloven § 9-2. Forskriftsutkastet tar ikke med denne henvisningen, og bruker også andre uttrykk («avtale sikkerheten», istf. sikkerhetsavtale). Vi anbefaler at ordlyden klarere reflekterer hvordan lovens § 9-2 kan være relevant for tolkningen av forskriftens § 17.

Det burde gå klarere frem av forskriften hvordan virksomhetene skal forholde seg til regelverket for offentlige anskaffelser i forbindelse med anskaffelser som ikke faller inn under reglene for sikkerhetsgraderte anskaffelser[8]. Dette gjelder spesielt unntak fra regelverket av hensyn til nasjonale sikkerhetsinteresser, og forholdet til EØS-avtalen artikkel 123.

Behovet for veiledning

I høringsnotatet bemerker departementet at «regelverkets funksjonelle innretning gjør det nødvendig at det utarbeides veiledere». Mye ansvar legges til den enkelte virksomhet, ved at det først og fremst er virksomhetenes egne vurderinger av risiko som skal legges til grunn for «forsvarlig sikkerhetsnivå» og de sikkerhetstiltakene som etableres. Dersom regelverket skal ha den ønskede effekt må virksomhetene ha god oversikt, evne til å prioritere, og ha tilstrekkelig kompetanse til å gjøre gode vurderinger og fatte beslutninger om håndtering av

[8] Eks. anskaffelser til skjermingsverdige informasjonssystemer som ikke behandler sikkerhetsgradert informasjon, eller i seg selv er klassifisert som objekt/infrastruktur.

risiko. Det er snakk om forskjellige typer kunnskap og kompetanse, i hele spennet fra ledelse til valg av, og innretning på, spesifikke tekniske sikkerhetstiltak. Vi deler departementets syn på at veiledning er helt nødvendig, og ønsker å peke på behovet for god sammenheng i veiledning rettet mot forskjellige roller og kompetanseområder – og også god sammenheng i veiledning på sikkerhetslovens område og andre tilstøtende og delvis overlappende områder, hvor virksomhetene har behov for å arbeide helhetlig.

Eventuelle anbefalinger om sikkerhetstiltak bør det veiledes om i sammenheng med tiltakene som er påkrevd i forskriften, slik at virksomhetene får en god oversikt over helheten. Eventuelle anbefalinger bør også beskrive potensielle negative sideeffekter ved hvert tiltak, slik at virksomhetene kan ta dette med i sine vurderinger før tiltak etableres.

Vennlig hilsen
for Difi

Grete Orderud
avdelingsdirektør

Øyvind Grinde
seksjonssjef

Dokumentet er godkjent elektronisk og har derfor ingen håndskrevne signaturer.

Kopi til:

Avdeling for virksomhetsstyring	Linn Aungrind	Postboks 1382 Vika	0114 OSLO