Cisco Systems Norway AS
Philip Pedersens vei 1
1366 Lysaker

Lysaker, 28. september 2018

Forsvarsdepartementet
postmottak@fd.dep.no

Høringsinnspill til sikkerhetslovens forskrifter

Lov om nasjonal sikkerhet (sikkerhetsloven) ble vedtatt av Stortinget 6. mars 2018. Cisco vil kommentere noen elementer i utkastene til de tre nye forskriftene til loven som ble sendt på høring av Forsvarsdepartementet 2. juli, med høringsfrist 1. oktober 2018. Vi tillater oss også å fremme noen supplerende forslag vi mener er viktige for å få en mer effektiv implementering av loven.

Det tas forbehold om at det ikke er foretatt en helthetlig gjennomgang av sikkerhetsloven, dens forarbeider, alle elementer i forslagene til forskrifter og øvrig regelverk. Cisco har heller ikke innhentet juridisk kompetanse for å gå gjennom våre innspill, men legger til grunn at departementet selv besitter den beste kompetanse for nærmere vurdering og kvalitetssikring.

Cisco er et av verdens største datasikkerhetsselskaper. Vi ser et stort behov for å forsterke datasikkerhetsarbeidet i Norge. Vi hilser utvidelsen av lovens virkeområde velkommen.

Cisco vil særlig understreke viktigheten av å sikre en effektiv *gjennomføring* av loven slik at man får et høyere gjennomgående sikkerhetsnivå.

- Cybersikkerhetsarbeidet må prioriteres tydelig, blant annet gjennom styringssignaler fra fagdepartementene.
- Regjeringen må gi Nasjonal sikkerhetsmyndighet (NSM) økt kapasitet og autoritet.
- NSM bør årlig utarbeide en rapport for regjeringen med vurderinger av hvordan cybersikkerhetstilstanden utvikler seg i utvalgte sektorer med forslag til oppfølging.
- Det bør signaliseres at den digitale sårbarheten forventes å øke. Virksomheter og myndigheter må ta høyde for dette og legge en føre-var-holdning til grunn.
- Digital sikkerhet er en del av Norges forsvars- og sikkerhetspolitikk. Virksomheter som eier skjermingsverdige verdier og velger leverandører fra et land Norge ikke har et sikkerhetspolitisk samarbeid med må ha en særskilt rapportering av dette.
- Det er i loven lagt opp til at eventuelle uenigheter mellom sektormyndigheter og NSM skal bringes inn for helhetlig avveining i departementet. Tilsvarende skal pålegg, mulkt

og overtredelsesgebyr kunne innklages av virksomhetene til departementet. Det er viktig at disse mekanismene tas i bruk for å sikre et høyere gjennomgående sikkerhetsnivå på tvers av sektorer.

- Myndigheter og næringsliv må samarbeide om å øke tilgangen på kvalifisert personell og tiltak som bidrar til en sterkere sikkerhetskultur.

Behov for styrking av NSM

Gjennom den nye sikkerhetsloven tydeliggjøres ansvaret for å gjøre konkrete vurderinger og sette i verk nødvendige sikkerhetstiltak i den enkelte virksomhet, samt ansvaret det enkelte sektortilsyn og sektordepartement har for å følge opp sikkerhetsarbeidet i virksomhetene i egen sektor.

Det er avgjørende at en slik sektortilnærming kombineres med at Nasjonal sikkerhetsmyndighet (NSM) gis en klar overordnet rolle. I sikkerhetslovens §2-2 heter det:

> *Sikkerhetsmyndigheten har det sektorovergripende ansvaret for at forebyggende sikkerhetsarbeid i virksomhetene utføres i samsvar med loven.*

NSM har det overordnede ansvaret for at sikkerhetstilstanden i alle sektorer er på et tilfredsstillende nivå, og skal se til at andre myndighetsorganer oppfyller sine plikter. NSMs rolle tydeliggjøres ytterligere ved at NSM kan ilegge pålegg, tvangsmulkt og overtredelsesgebyr for å sikre at sikkerhetsloven og forskrifter etterleves overfor departementer, sektormyndigheter med tilsynsansvar og øvrige virksomheter loven gjelder for.

I høringsnotat til forskriftene gis det kommentarer som i praksis kan virke begrensende for i hvilken grad NSM kan kunne utøve en slik overordnet rolle. Det heter blant annet at påleggskompetansen bare vil bli benyttet når «sektortilsynets oppfølging av sikkerheten i sektoren er uforsvarlig». Vi mener det i kommentarene til endelig forskrift bør presiseres at NSM har kompetanse til å komme med slike pålegg i de tilfeller sektortilsynets oppfølging er «utilstrekkelig».

Det er primært gjennom samarbeid man får til en styrking av sikkerhetsarbeidet i og mellom sektorer. Samtidig er det åpenbart lovgivers intensjon 1) å heve sikkerhetsnivået og 2) gi NSM en tydelig overordnet rolle for å sikre et høyere og jevnere sikkerhetsnivå på tvers av sektorer. Man må derfor sikre at muligheten for å ilegge pålegg, mulkt og gebyr oppfattes som reell. At dette er virkemidler som skal brukes bør blant annet reflekteres i departementets kommentarer departementet når endelige forskrifter fastsettes.

Departementet bør gjennomgå utkastet til forskrifter og tilknyttede kommentarer med sikte på å identifisere ytterligere justeringer for å sikre at NSMs sektorovergripende ansvar ivaretas på en effektiv måte.

Flere sektorer domineres av noen få store og ressurssterke selskaper med mye kompetanse. Dette gjelder blant annet telesektoren og energisektoren. Dette er i utgangspunktet en styrke. Vi vil imidlertid understreke viktigheten at NSM og sektortilsynene har tilstrekkelig kompetanse til å kunne å fungere som en tung nok myndighet overfor disse selskapene.

Behov for styring og rapportering

Cisco mener det vil være hensiktsmessig at det hvert år foretas en konkret vurdering av utviklingen i cybersikkerhetssituasjonen i de viktigste samfunnssektorene. Vi mener Nasjonal sikkerhetsmyndighet i samarbeid med sektormyndigheter og øvrige hemmelige tjenester bør utarbeide en rapport som forelegges regjeringen. En slik rapport bør blant annet oppsummere de hemmelige tjenesters trusselvurderinger og anbefalinger, gi nærmere vurdering av hvordan trusselbildet og sårbarheten i utvalgte sektorer utvikler seg, fremdriften i det konkrete arbeidet med å bedre sikkerheten i hver av de utvalgte sektorene og gi anbefalinger om områder som bør vies særlig oppmerksomhet. Dersom det er uenighet mellom sektormyndigheter og nasjonal sikkerhetsmyndighet om vurderinger og anbefalinger kan dette fremkomme. En slik rapportering kan ikke være uttømmende, men må ta for seg de viktigste forholdene.

Cisco har ikke tatt stilling til om det kan være hensiktsmessig at det også rapporteres på andre områder enn cybersikkerhet, men mener det er særskilt behov på dette området.

Det inntas en ny paragraf som et tillegg etter § 1 i myndighetsforskriften

> Nasjonal sikkerhetsmyndighet utarbeider årlig i samarbeid med sektormyndigheter og øvrige hemmelige tjenester en rapport til regjeringen om utviklingen i (cyber)sikkerhetssituasjonen i Norge. Rapporten oppsummerer blant annet de viktigste trussel- og sårbarhetsvurderinger i utvalgte sektorer, gir en oversikt over hvordan arbeidet med å styrke sikkerhetsarbeidet skrider frem, herunder arbeidet med å utpeke skjermingsverdige objekter og informasjonssystemer, og inneholder anbefalinger om områder som bør vies særlig oppmerksomhet. Sektortilsyn og sektordepartement skal bidra med nødvendig underlag til arbeidet.

Som det påpekes i høringsnotatet skal departementene til «enhver tid» ha oversikt over de virksomhetene som har betydning for Norges evne til å ivareta nasjonale sikkerhetsinteresser. En slik årlig gjennomgang vil imidlertid skape et system der sektordepartement, sektortilsyn og NSM vil måtte ta konkret stilling til status i arbeidet med et fast intervall.

Det bør også hjemles i virksomhetsforskriften at virksomhetene på forespørsel har plikt til å bidra med informasjon og vurderinger slik at sektortilsyn og NSM kan danne seg et godt helhetsbilde og få grunnlag for anbefalinger til for forbedringer.

Et alternativ til en slik årlig rapportering kan være at NSM gis mandat til å foreta slik rapportering i et slikt omfang og med en slik frekvens som NSM finner hensiktsmessig. Vi tror imidlertid et oppdrag bør forankres i et oppdrag fra regjeringen gjennom tildelingsbrev og at aktørenes plikt til å bidra bør hjemles i forskriftsverket.

Sektortilsyn, sektordepartement og nasjonal sikkerhetsmyndighet må settes i stand til å vurdere om virksomhetene gjør det som er nødvendig for å sikre et tilstrekkelig sikkerhetsnivå

I den utstrekning sektortilsyn, sektordepartement eller nasjonal sikkerhetsmyndighet finner det nødvendig må den enkelte virksomhet bidra med informasjon om de konkrete vurderinger som er gjort og de tiltak som gjennomføres for å sikre et forsvarlig sikkerhetsnivå. Det er noe uklart om dette i tilstrekkelig grad sikres gjennom kapittel 1 i virksomhetsforskriften om system for sikkerhetsstyring i virksomhetene.

Tilsynsmyndighet må på forespørsel gis innsikt i de de konkrete vurderingene som er gjort og som skal dokumenteres av virksomhetene.

Tilsynsmyndigheten og departementet skal altså ikke bare påse at virksomheten har etablert egne rutiner for å sikre et tilfredsstillende sikkerhetsnivå, men skal gjennom tilsyn settes i stand til å vurdere om de vurderinger, avveininger og tiltak som gjennomføres faktisk er tilstrekkelige.

I høringsunderlaget heter det at virksomhetene skal utarbeide trusselscenarier som *bør* være basert på trussel- og risikovurderinger fra EOS-tjenestene.

Det bør presiseres at dersom virksomhetene velger å *ikke* legge til grunn trussel- og risikovurderinger fra EOS-tjenestene, eller velger å *ikke* følge konkrete anbefalinger fra EOS-tjenestene eller tilsynsmyndighet, må dette rapporteres uoppfordret til tilsynsmyndighet og videre til ansvarlig departement med en utfyllende begrunnelse.

Det foreslås inntatt en ny paragraf etter § 4 i virksomhetsforskriften som lyder:

> Virksomheten skal på oppfordring fra tilsynsmyndigheten bidra med informasjon som gjør det mulig for tilsynsmyndigheten å vurdere om det er tatt nødvendige skritt for å sikre et forsvarlig sikkerhetsnivå i virksomheten (, blant annet ved å informere om vurderinger knyttet til trusler og sårbarheter, av om iverksatte sikkerhetstiltak er tilstrekkelige og de avveininger som er gjort mellom kostnader og nytte ut fra den konkrete situasjonen).
>
> I de tilfeller der virksomheten velger å ikke legge til grunn vurderinger og anbefalinger fra EOS-tjenestene eller ansvarlig tilsynsmyndighet skal virksomheten uoppfordret rapportere om dette til tilsynsmyndigheten med en utfyllende begrunnelse for de valg som er tatt.

Virksomheten skal på oppfordring fra tilsynsmyndigheten bidra med informasjon som kan bidra til at myndighetene får grunnlag for å vurdere sikkerhetssituasjonen og behov for tiltak i sektoren generelt.

Forventing om økt sårbarhet og føre-var-holdning

Farten i den digitale utviklingen blir stadig raskere og integrasjonen og avhengigheten mellom ulike systemer øker. Vi må derfor forvente økt digital sårbarhet. Som departementet påpeker i høringsnotatet vil det som er forsvarlig sikkerhetsnivå i dag ikke nødvendigvis være det i morgen. Det kan tenkes forhold som vil redusere sårbarheten, men vi må planlegge for at sårbarheten vil være økende.

Kombinasjonen av sterk vekst i overføringskapasitet, mobile løsninger (5G), stordata, Internet of Things (IoT), kunstig intelligens og skyløsninger fører til at små og store digitale nettverk kobles sammen. Det blir altså ikke bare en kraftig vekst i digitale løsninger på mange samfunnsområder, vi får en helt annen kobling og integrasjon mellom disse. Hver av disse koblingene representerer en ny sikkerhetsrisiko, og grensene for hva som er skjermingsverdig informasjon, informasjonssystem, objekt og infrastruktur vil utvides.

Vi må forvente at flere virksomheter gradvis vil komme inn under sikkerhetslovens virkeområde. Vi må forvente at virksomheter som allerede er omfattet av loven må gjennomføre mer effektive sikkerhetstiltak. Systemer som i dag ikke defineres som sikkerhetskritiske vil få en integrasjon mot sikkerhetskritiske systemer eller i seg selv vil bli definert som sikkerhetskritisk.

Investeringer som gjøres i dag vil kunne ha stor betydning for sikkerhetsnivået som kan bygges inn i systemene til en akseptabel pris i fremtiden.

Det bør derfor signaliseres i kommentarer til forskriftene og veiledningsmateriell at myndigheter og virksomheter i sine vurderinger må ha en føre-var-holdning hvor man tar høyde for at trusselnivået *kan* øke og at sårbarheten *må forventes* å øke. Dette er ikke i strid med de prinsipper som er definert gjennom loven og dens forarbeider, men en praktisk føring som er rimelig basert på den aktuelle situasjonen.

Som departementet skriver på side 24 i høringsnotatet kan det ved kjøp av «kritiske komponenter» til de skjermingsverdige verdiene «oppstå en ikke ubetydelig risiko for at det er lagt inn en bakdør i komponentene som vil kunne gi tilgang til systemet, objektet eller infrastrukturen på et senere tidspunkt».

Departementet skriver at det ikke inntrer en varslingsplikt dersom virksomheten håndterer risikoen på en slik måte at den blir ubetydelig. I lys av den risikoen det innebærer å bruke ikke-klarerte leverandører og leverandører fra land vi ikke har sikkerhetsavtale med at

virksomhetene bør en plikt til å rapportere i hvert fall på i hvilket omfang man benytter leverandører fra land vi ikke har sikkerhetspolitisk samarbeid med og vurderingene knyttet til dette.

Vi foreslår at følgende tas inn i forskriften:

> Virksomheter som har skjermingsverdige verdier og som benytter leverandører fra land Norge ikke har sikkerhetspolitisk samarbeid med skal gjøre en konkret vurdering av risikoen knyttet til dette og årlig rapportere til tilsynsmyndigheten. Også bruk av denne typen leverandører i de delene av virksomhetene som i utgangspunktet ikke defineres som skjermingsverdig skal inngå i vurderingen.

Systemrevisjon er ikke alltid nok

Det er dessverre eksempler på at det kan eksistere vesentlige sikkerhetshull til tross for at virksomheter har etablert gode interne prosedyrer og tilsynelatende opptrer i tråd med gjeldende standarder og lovkrav.

Selv om systemrevisjon og dialog mellom tilsynsmyndighet og virksomhet må være hovedmodellen, bør det ikke utelukkes at tilsynsmyndigheten kan stille krav om at det skal utføres testing. I tråd med den åpning som gis i loven foreslås det å gi et konkret hjemmelsgrunnlag for dette i forskriftsverket.

Forslag til tillegg i § 3 i myndighetsforskriften:

> Ansvarlig tilsynsmyndighet skal innenfor sin sektor årlig vurdere behovet for og eventuelt ta initiativ til at det gjennomføres inntrengingstesting, kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak i et utvalg av virksomheter i den aktuelle sektor. Det skal søkes å oppnå tilslutning fra den enkelte virksomhet om og på hvilken måte slik testing skal gjennomføres, men sektormyndighet og Nasjonal sikkerhetsmyndighet har myndighet til å stille krav til testing.

Forslag til tillegg til myndighetsforskriften § 17 (… Tilsyn skal som hovedregel gjennomføres som systemrevisjon.)

> Ansvarlig tilsynsmyndighet eller Nasjonal sikkerhetsmyndighet kan imidlertid stille krav om at det gjennomføres testing jf. §3

Varslingsplikt om anskaffelser til skjermingsverdig informasjonssystem, objekt eller infrastruktur

Det bør inntas et tillegg til §18 i virksomhetsforskriften:

> Før en anskaffelsesprosess starter skal virksomheten foreta en vurdering av om man ønsker å invitere leverandører som ikke er oppført i klareringsmyndighetens register over klarerte leverandører. Dersom man ønsker å innlede en prosess med leverandører som ikke allerede er klarert skal det avklares med klareringsmyndigheten hvordan prosessen kan legges opp slik at aktuelle leverandører eventuelt kan oppnå nødvendig klarering.
>
> Virksomheten plikter å informere aktuelle leverandører om at det kan bli stilt nærmere krav på senere stadier i prosessen som kan komme til å utelukke enkelte leverandører.

Nasjonal sikkerhetsmyndighets rolle ved fastsettelse av tilsynsmyndighet

Det er det enkelte departement som skal avgjøre hvem som skal føre tilsyn etter sikkerhetsloven med ulike virksomheter som hører inn under departementet. I forslaget til § 14 i myndighetsforskriften heter det at:

> En uttalelse fra Nasjonal sikkerhetsmyndighet skal inngå i helhetsvurderingen.

Vi foreslår å endre dette til:

> Det skal innhentes en uttalelse fra Nasjonal sikkerhetsmyndighet som skal vektlegges i en helhetsvurdering. Dersom det er avvik mellom Nasjonal sikkerhetsmyndighets anbefalinger og de rammer ansvarlig sektordepartement ønsker å sette for tilsyn i sektoren skal saken bringes inn for avgjørelse i Justis- og beredskapsdepartementet.

§ 47 i virksomhetsforskriften bør endres på tilsvarende måte:

> Det skal innhentes en uttalelse fra Nasjonal sikkerhetsmyndighet som skal vektlegges i en helhetsvurdering. Dersom det er avvik mellom Nasjonal sikkerhetsmyndighets anbefalinger og de rammer ansvarlig sektordepartement ønsker å sette for tilsyn i sektoren skal saken bringes inn for avgjørelse i Justis- og beredskapsdepartementet.

Det er en utfordring å ha tilstrekkelig kompetanse og kapasitet på alle fagområder innenfor de ulike sektortilsyn. Det er viktig å erkjenne dette og ved behov samle oppgaver hos NSM.

I høringsnotatet til forskriftene heter det: «Fremfor å lære opp sektormyndigheten, bør det på enkelte områder hvor det ikke er hensiktsmessig å bygge opp egen kompetanse hos sektormyndigheten avtales at NSM bidrar med forberedelse og gjennomføring av tilsyn.»

Cisco støtter denne tilnærmingen og mener den foreslåtte endringen i §14 bidrar til at man kan få en bedre samlet ressursutnyttelse.

Virksomhetenes egen evaluering og øving

Til virksomhetsforskriftens § 8 første avsnitt foreslås følgende tillegg:

> Virksomheten skal herunder foreta en vurdering av behovet for inntrengingstesting, testing av kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak testing av sine sikkerhetstiltak.

Beskyttelse av skjermingsverdige informasjonssystemer

Forslag til tillegg i § 45 i virksomhetsforskriften etter punkt e):

> sikre at data er tilgjengelig

Reel tilknytning må være avgjørende for om leverandør kan godkjennes

Politiets sikkerhetstjeneste (PST) og NSM er tydelige på at det er en sikkerhetsrisiko forbundet med å bruke leverandører fra land Norge ikke har et sikkerhetspolitisk samarbeid med.

Etablering av datterselskap i Norge eller et land Norge har sikkerhetspolitisk samarbeid med kan ikke være tilstrekkelig for å oppnå godkjenning som leverandør, dersom den reelle kontrollen med og/eller kjernen i virksomheten utøves fra et land Norge ikke har sikkerhetspolitisk samarbeid med.

Cisco oppfatter at dette må være intensjonen og dekket av dagens forslag til formulering i §75 i virksomhetsforskriften. Eventuelt kan det tas inn ett tillegg i forlengelsen av første avsnitt (…som har jurisdiksjon der lokalene ligger eller der virksomheten drives fra.):

> Hvor leverandøren har sin reelle tilknytning vil være det avgjørende for om nødvendig leverandørklarering kan oppnås.

Norge har etter vår kjennskap per i dag ikke en sikkerhetsavtale med USA, men et tett sikkerhetspolitisk samarbeid. Det legges til grunn at selskap med hovedbase i USA vil kunne oppnå leverandørklarering som i dag. Cisco vil be departementet foreta en vurdering om det er behov for å foreta justeringer i forskriftsutkastet for å sikre dette.

Krav om leverandørklarering

Forslag til §74 b) i virksomhetsforskriften lyder i dag:

> Leverandøren skal uansett ha leverandørklarering dersom den skal ha elektronisk tilgang til objekter eller infrastruktur klassifisert KRITISK eller MEGET KRITISK fra sine egne informasjonssystemer eller lokaler

Vi mener det bør settes enda klarere krav til når leverandørklarering er påkrevet og mener § 74 b) bør lyde som følger:

> Leverandøren skal uansett ha leverandørklarering dersom den skal ha fysisk eller elektronisk tilgang til objekter eller infrastruktur klassifisert KRITISK eller MEGET KRITISK

Dette innebærer et generelt krav til leverandørklarering i alle situasjoner der en leverandør skal ha leveranser til en sikkerhetsgradert anskaffelse. Kombinert med de unntaksbestemmelser forskriftene har mener vi dette vil være praktikabelt.

Virksomhetenes varslingsplikt (punkt 4.6.4)

Vi tror det vil være hensiktsmessig at NSM utvikler en mal med momenter for hvordan virksomheter bør gå frem for å gjøre nødvendige vurderinger. En slik mal fra NSM kan danne utgangspunkt for konkrete veiledere fra ansvarlige sektormyndigheter. I tillegg til mer åpne vurderingskriterier bør både NSM og sektormyndighetene ha mulighet til å liste opp krav som virksomhetene må innfri, slik disse følger av lover og forskrifter og som NSM og sektormyndighetene for øvrig finner påkrevet for å oppnå tilstrekkelig sikkerhetsnivå. Dersom sektormyndigheten utformer veiledere NSM mener ikke er tilstrekkelig bør NSM påpeke dette og om nødvendig gi sektortilsynet pålegg om nødvendige forbedringer i veilederen.

Cisco vil takke for muligheten til å komme med innspill. Ta gjerne kontakt ved behov for avklaringer. Vi ønsker departementet lykke til med det videre forskriftsarbeidet.

Vennlig hilsen

Sven Størmer Thaulow
Administrerende direktør Cisco Norge