Direktoratet for samfunnssikkerhet og beredskap

Dokumentdato	Vår referanse
29.03.2019	2019/3841 CRJA

Vår saksbehandler	Deres dato	Deres referanse
Janniche Cramer, tlf.		

JUSTIS- OG BEREDSKAPSDEPARTEMENTET

Gullhaug Torg 4A
0484 OSLO

Høring - NOU 2018:14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet

Direktoratet for samfunnssikkerhet og beredskap (DSB) viser til brev fra Justis- og beredskapsdepartementet (JD) datert 21. desember 2018 om felles høring av 1) NOU 2018:14 IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet og 2) regjeringens utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett. JD har gitt DSB utsatt høringsfrist til fredag 29.03.2019, og vi oversender med dette vårt høringssvar.

Innledning

Den teknologiske utviklingen i dagens samfunn gir oss mange muligheter og kan bidra til å styrke og bygge opp under sentrale verdier som liv og helse, demokrati og rettssikkerhet, økonomisk velferd og nasjonens suverenitet. Den teknologiske utviklingen og den stadig økende digitaliseringen bidrar til tettere koblinger mellom ulike deler av samfunnet. Avhengighetene mellom ulike sivile sektorer, mellom private og offentlige virksomheter, mellom forsvarssektoren og sivil sektor, mellom inn- og utland blir større. Skillelinjene blir vagere, og vi blir mer sårbare for alvorlige IKT-hendelser.

Samfunnet som helhet, sektormyndigheter og den enkelte virksomhet må gjøre samlede vurderinger av hvordan ulike trusler og sårbarheter kan møtes. Direktoratet for samfunnssikkerhet (DSB) er derfor opptatt av å ha en såkalt "all hazards approach" i sitt arbeid. Sikkerheten i informasjons- og kommunikasjonssystemer er av helt sentral betydning for samfunnssikkerheten på alle forvaltningsnivåer. Økt kompleksitet i det digitale sårbarhetsbildet er ikke minst krevende for de regionale og lokale myndighetene. Avhengigheten av IKT for produksjon av leveranser og kommunale tjenester øker, samtidig som digitale trusler øker både i omfang og alvorlighet. Det stilles alt større krav til kompetanse og kapasitet for å forebygge, detektere og håndtere IKT-sikkerhetshendelser, noe som er spesielt utfordrende for de mange små enhetene på lokalt og regionalt nivå.

DSB understreker viktigheten av å skape bevissthet om skadepotensialet og konsekvensene slike hendelser kan få for grunnleggende samfunnsverdier og befolkningen. Det er derfor sentralt at informasjonsdelingen mellom de tekniske responsmiljøene (NSM NorCERT og de sektorvise responsmiljøene) og det ordinære krisehåndteringsapparatet fungerer optimalt, slik at sektorene selv settes i stand til å ivareta sitt ansvar for håndtering av samfunnskonsekvensene.

Med en utvikling hvor avhengigheten av IKT preger hele samfunnet og koblingene på tvers blir stadig tettere, vil også behovet for tydelige ansvars- og rolleavklaringer, nasjonal samordning og koordinering bli desto viktigere. Hybride trusler er et eksempel som illustrerer den stadige økende kompleksiteten og avhengighetene og utfordringer på tvers av sektorer. DSBs analyser av krisescenarioer og erfaringer fra

Postadresse
Direktoratet for samfunnssikkerhet og beredskap

Postboks 2014
3103 Tønsberg

Kontoradresse
Rambergveien 9
3115 Tønsberg

E-post
postmottak@dsb.no

Telefon
33 41 25 00

Internett
www.dsb.no

Telefaks
33 31 06 60

Organisasjonsnummer
974 760 983

øvelse IKT 16, og den planlagte øvelsen DIGITAL 2020 er sentrale og relevante mht. kunnskapsgrunnlag for ansvars- og rolleavklaringer og vurdering av relevante samordningsmekanismer.

DSBs høringssvar

DSB gir med dette sitt svar på høringen av NOU 2018:14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet. Begge sakene er relevante for direktoratet, både med hensyn til ansvaret som fagmyndighet for produktsikkerhet og vårt samfunnsoppdrag knyttet til å ha oversikt over risiko og sårbarhet i samfunnet og oppgaven med å understøtte Justis- og beredskapsdepartementets (JD) samordningsansvar i arbeidet med samfunnssikkerheten.

Det er en nær sammenheng mellom de to høringssakene, men departementet har bedt om at utkastet til lov om NIS-direktivet vurderes separat. Under gir vi først våre innspill til utkast til lov, deretter til Holte-utvalgets anbefalinger.

1. Utkast til lov som gjennomfører NIS-direktivet

DSB stiller seg bak departementet som i sitt høringsnotat gir følgende vurdering: "… [departementet] anser direktivet for å være et godt tiltak for å styrke IKT-sikkerheten i Norge. Gjennomføring av direktivet vil for mange samfunnsviktige virksomheter innebære en styrking av arbeidet med IKT-sikkerhet. Dette vil bidra til å redusere digitale sårbarheter i den enkelte virksomhet, den enkelte sektor og samlet sett for nasjonen."

Direktoratet støtter hovedinnretningen i det foreliggende lovutkastet og mener det er fornuftig at krav til IKT-sikkerhet baserer seg på en risikobasert tilnærming, hvor kravene settes inn i en risikostyringssammenheng. Vi deler departementets og Holte-utvalgets vurdering om at det er enklere og mer tidseffektivt å innføre en ny lov om IKT-sikkerhet enn å gjennomgå og harmonisere allerede eksisterende lovverk.

Vi har imidlertid enkelte merknader og innspill som vi redegjør for under.

§ 1 Formål

Formålsparagrafen inneholder termer og begreper som uten nærmere definisjon kan bidra til usikkerhet hos pliktsubjektene og tilsynsmyndighetene. Vi tenker her spesielt på begrepene "kritisk samfunnsmessig aktivitet" og "samfunnsviktige tjenester". En samfunnsviktig tjeneste skal ut fra lovutkastet forstås som en tjeneste som er viktig for opprettholdelsen av kritiske samfunnsmessige eller økonomiske aktiviteter. Hva det vil si å være viktig for denne opprettholdelsen, fremkommer ikke. I tilfeller hvor presiseringer kan bidra til at å redusere usikkerhet og behov for avklaringer i videre prosesser, bør disse fremkomme av lovteksten.

§ 2 Virkeområde

Generelt mener vi at alle 14 kritiske samfunnsfunksjonene som inngår i KIKS-rammeverket[1] og som presenteres i Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn* bør omfattes av den nye loven. Dette vil bety at virkeområdet utvides til bl.a. å omfatte politiets og påtalemyndighetens ansvarsområder, redningstjenesten, mat- og drivstofforsyning og meteorologiske og satellittbaserte tjenester.

[1] Direktoratet for samfunnssikkerhet og beredskap (2016) *Samfunnets kritiske funksjoner*

DSB mener for øvrig sammenblandingen av infrastruktur og tjenester i § 2 er uheldig og stiller spørsmål ved om for eksempel digital infrastruktur kan betraktes som en "sektor". Lovens terminologi bør også langt mulig harmoniseres med de 14 samfunnskritiske funksjonene.

Med utgangspunkt i foreliggende lovutkastet kan det bli utfordrende for sektordepartementene å identifisere hvilke virksomheter som faller inn under lovens virkeområde. Se også kommentarer til § 4 Definisjoner under.

§ 4 Definisjoner

Kravene som følger av utkast til lov, gjelder de to kategorier: tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Definisjonene av kategoriene er, etter DSBs vurdering, uklare med tanke på hvem som kan være pliktsubjekt. Er det kun ansvarlig tilbyder av en sluttleveranse til sluttbruker, eller omfatter definisjonene også tilbydere av ulike deltjenester og delleveranser i verdikjeden fram til sluttbruker?

Til § 4, femte ledd: DSB anbefaler at departementet vurderer å skrive inn begrepene tilgjengelighet, konfidensialitet og integritet når det gjelder omtale av IKT-sikkerhet i nett og informasjonssystemer.

§ 8 Krav om varsling for tilbydere av samfunnsviktige tjenester

Varsling om hendelser er per i dag frivillig. Krav om varsling av alvorlige digitale sikkerhetshendelser vil blant annet gi tilgang til informasjon om både trusler og sårbarhet – en kunnskap som vil bidra til enda bedre arbeid med IKT-sikkerhet i fremtiden. DSBs erfaring er at varsling ikke nødvendigvis skjer, og vi støtter at krav om varsling lovfestes.

En uønsket digital hendelse kan føre svikt i en eller flere kritiske samfunnsfunksjoner eller på annen måte ha potensial for å gi et konsekvensbilde som krever fysisk håndtering. Konsekvensene for samfunnskritiske funksjoner og befolkningen kan være store. Dette viser både erfaringene fra den nasjonale IKT-øvelsen i 2016 og reelle uønskede digitale hendelser. Koblingen mellom responsmiljøene og "det ordinære forvaltnings- og beredskapssystemet" synes å være en utfordring. DSB mener det ordinære krisehåndteringsapparatet tidlig må kobles på ved uønskede digitale hendelser da dette er helt nødvendig for å sikre god håndtering av samfunnskonsekvensene.

§ 11 Responsmiljøer

Se kommentarer over til § 8. DSB mener at varsling av uønskede hendelser som rammer nettverk og informasjonssystemer må inngå som del av det ordinære forvaltnings- og krisehåndteringssystemet.

§ 12 Tilsynsmyndigheter

Det er naturlig å se tilsynsordningen etter NIS-loven i sammenheng med den tilsynsordningen det legges opp til etter sikkerhetsloven. Sikkerhetsmyndigheten (i forskriftsverket utpekes Nasjonal sikkerhetsmyndighet (NSM) som "sikkerhetsmyndighet") skal etter sikkerhetsloven føre tilsyn med departementene og med virksomheter som ikke er underlagt tilsyn etter loven fra eget sektortilsyn. Departementene kan bestemme at sektortilsyn skal føre tilsyn innenfor eget sektoransvar.

NIS-loven er mindre inngripende enn sikkerhetsloven, og DSB mener at sektortilsynene i utgangspunktet bør ha ansvar for å føre tilsyn etter denne loven. I tillegg bør det utpekes en myndighet som fører tilsyn med departementene, og i de tilfeller hvor en virksomhet ikke omfattes av et sektortilsyn. Denne myndigheten kan også ved behov gi råd og veiledning til sektortilsynene og delta i tilsyn etter loven når sektortilsynene ber om det. Det er naturlig at denne myndigheten tillegges NSM.

Svar på JDs særskilte spørsmål til utkast til lov

Departementet ber om innspill på enkelte særskilte spørsmål. DSBs innspill til disse følger her fortløpende.

1. *Systematisk arbeid med IKT-sikkerhet i DSB per i dag*

DSB arbeider i hovedsak med IKT-sikkerhet i henhold til NS-ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet – Krav.

DSBs sikkerhetsorganisasjonen arbeider med etablering av et *Styringssystem for informasjonssikkerhet* etter ISO 27001 og har til hensikt å levere et system for kontinuerlig forbedring hvor man identifiserer virksomhetens faktiske behov for sikkerhet, inkludert IKT-sikkerhet og den til enhver tid rådende tilstand og dermed kan treffe riktige tiltak.

DSBs IKT-enhet jobber også etter NSMs grunnprinsipper for IKT-sikkerhet og vil etter hvert kunne nyttiggjøre seg virksomhetens styringssystem for informasjonssikkerhet som er under utvikling.

Nasjonal sikkerhetsmåned er en årlig kampanje og et tiltak som skal øke kompetansen og virksomhetens evne til å håndtere det gjeldende trusselbildet. DSB deltar i denne kampanjen hvert år og gjennomfører en rekke aktiviteter i den forbindelse.

Øvelse SNØ 2020: DIGITAL2020

DSB har også i 2019 fått ansvar for å lede planlegging, gjennomføring og evaluering av en nasjonal tverrsektoriell øvelse i digital sikkerhet, Øvelse Digital 2020, som gjennomføres høsten 2020 og vil være DSBs sivile nasjonale øvelse (SNØ) for 2020.

Hovedhensikten med øvelsen er å redusere samfunnets sårbarhet for digitale hendelser og å forbedre samfunnets evne til å forebygge, avdekke og håndtere digitale hendelser og øke samfunnets digitale sikkerhetskompetanse. Øvelsen vil ta opp i seg relevant innhold i utredningsarbeid, stortingsmeldinger, strategier mv. som er utviklet innen digital sikkerhet de siste årene. Det planlegges et kompetanseutviklingsløp frem mot øvelsen hvor privat-offentlig samarbeid, sivil-militært samarbeid og internasjonalt samarbeid vil få særlig oppmerksomhet. Samlet sett vil arbeidet med øvelsen kunne bli et viktig bidrag i arbeidet med nasjonal IKT-sikkerhet.

Øvelsen vil ha et scenario som treffer flere sektorer og nivåer, og som må håndteres gjennom effektiv hendelseshåndtering og samvirke. Ved at øvelsen planlegges og gjennomføres i tett samarbeid med en rekke private og offentlige virksomheter, etater og myndigheter på lokalt, regionalt og sentralt nivå, vil den også kunne bli en viktig del av arbeidet med en økt og felles risikoforståelse knyttet til uønskede digitale hendelser.

2. *Positive konsekvenser som forslaget til gjennomføring av NIS-direktivet vil få for DSB*

Det forebyggende arbeidet er viktig og kunnskap om trusselbildet er avgjørende for hensiktsmessig ressursbruk og for å vurdere hvilke sikringstiltak som bør iverksettes. Krav om varsling av alvorlige digitale sikkerhetshendelser vil blant annet gi informasjon om både trusler og sårbarhet innen en sektor eller rammen av informasjonssystemer. Dette kan videre danne grunnlag for proaktive tiltak.

Harmonisering av krav til tilbydere vil sannsynligvis øke frekvens og kvalitet i rapporteringen. Nasjonale og sektorvise responsmiljøer er viktige ressurser og verktøy for å treffe riktige forebyggende tiltak og å håndtere hendelser som måtte oppstå. Det er en stor utfordring å gjennomføre gode nok risiko- og sårbarhetsanalyser av alt som ligger utenfor egen fysiske kontroll. I arbeidet med sikring av kritiske samfunnsfunksjoner trenger vi bedre kunnskap om slik risiko. Vi tror direktivet vil kunne bøte noe på dette.

I arbeidet med samordning vil DSB kunne bruke den nye loven som "verktøy" i ulike aktiviteter og oppgaver rettet mot de ulike forvaltningsnivåene. Loven vil dermed kunne bli nyttig i våre ulike oppgaver og funksjoner som pådriver for å se samfunnssikkerhet, herunder IKT-sikkerhet, på tvers av sivile sektorer, nivåer og mellom private og offentlige virksomheter.

Under forutsetning om en harmonisering av lovtekst opp de 14 funksjonene som presenteres i Meld. St. 10 (2016–2017) Risiko i et trygt samfunn (ref. tidligere merknader til § 2 Virkeområde) og en god begrepsavklaring vil loven være et positivt bidrag i vår kommunikasjon med alle aktørene vi møter gjennom vår samordningsrolle og våre samordningsoppgaver på de ulike forvaltningsnivåene. Det gir oss et tydeligere utgangspunkt og rammer for aktiviteter som følger av både tildelingsbrev og løpende oppgaver. Ny lov om IKT-sikkerhet som målbærer en risikotilnærming vil bidra til bedre risikostyring og gjennom dette redusere sårbarheter i samfunnet og konsekvenser hvis hendelser inntreffer.

3. Negative konsekvenser som forslaget til gjennomføring av NIS-direktivet vil få for DSB

Gitt at begrepsbruken harmoniseres med de 14 samfunnskritiske funksjonene ser ikke DSB noen store negative konsekvenser. Dersom begrepsbruken i lovutkastet slik det foreligger forblir uendret vil den nye loven kunne medføre og usikkerhet blant sektormyndighetene og tilbydere av samfunnskritiske virksomheter og følgelig merarbeid for DSB i form av behov for å avklare ulike forhold knyttet til lovens virkeområde.

4. Hvorvidt DSB per i dag er underlagt krav til IKT-sikkerhet og varsling

DSB er underlagt sikkerhetsloven[2] med tilhørende forskrifter. Videre følger vi nasjonale strategier innen området, klare råd og veiledninger fra blant annet Nasjonal sikkerhetsmyndighet (NSM) og Direktoratet for forvaltning og IKT (Difi).

5. Hvorvidt en slik lov som foreslås i høringen bør vedtas selv om vi ikke er forpliktet til det i henhold til EØS-avtalen

Av hensyn til ivaretagelse av IKT-sikkerhet i DSB som virksomhet og arbeidet med å ha oversikt over risiko og sårbarhet i kritiske samfunnsfunksjoner mener DSB en ny IKT-sikkerhetslov bør vedtas selv om vi ikke er forpliktet til det i henhold til EØS-avtalen.

[2] LOV-2018-06-01-24 Lov om nasjonal sikkerhet (sikkerhetsloven)

2. Utredning fra IKT-sikkerhetsutvalget (Holte-utvalget) NOU 2018:14 IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet

DSB redegjør her for sine innspill til utvalgets fem hovedanbefalinger.

1. Forslag om utvidelse av lovens virkeområde

Utvalget foreslår en utvidelse av NIS-direktivet og JDs lovutkasts virkeområde og mener at loven også skal gjelde for offentlig forvaltning. Dette begrunnes med at offentlig forvaltning tilbyr viktige tjenester til befolkningen og har en sentral rolle i digitaliseringen i samfunnet. Videre begrunnes forslaget med at det vil føre til økt grad av etterlevelse av kravene om IKT-sikkerhet.

DSB støtter utvalgets forslag om utvidelse av lovens virkeområde og anbefaler videre at loven harmoniseres med de 14 samfunnskritiske funksjonene som presenteres i Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn*. Se tidligere innspill til høringsuttalelse til ny lov § 1 Formål.

2. Krav til IKT-sikkerhet ved alle offentlige anskaffelser

Utvalget legger til grunn at det innenfor rammene av anskaffelsesregelverket er fullt mulig å stille krav om IKT-sikkerhet ved anskaffelse av IKT-produkter og -tjenester. For utvalget er det ikke like tydelig om det er anledning til å stille krav om IKT-sikkerhet ved anskaffelse av andre produkter og tjenester som ikke like intuitivt kan innebære en digital risiko. Videre mener utvalget at det må stilles krav om IKT-sikkerhet ved alle offentlige anskaffelser, og at anskaffelsesregelverket bør endres slik at oppdragsgiver får en slikt plikt.

Krav der det er relevant og tydeliggjøring av oppdragsgivers plikt til å vurdere behovet for å stille krav

DSB er enig i utvalgets forslag om å tydeliggjøre og flytte ansvaret for IKT-sikkerheten i anskaffelser fra kunde til leverandør. Vi mener imidlertid at det må stilles krav til leverandøren *der dette er relevant*. Det synes ikke hensiktsmessig å innføre dette som en generelle regel som skal gjelde alle offentlige anskaffelser, da det ikke vil være relevant for alle typer varer og tjenester. Det er derfor mer hensiktsmessig å tydeliggjøre at oppdragsgiver har plikt til vurdere om det er behov for krav om IKT-sikkerhet ved anskaffelsene, på lik linje med samme modell som fremgår av forskrift om offentlige anskaffelser (anskaffelsesforskriften) § 7-9.

I høringsnotatet fremkommer det at oppdragsgiveren skal legge vekt på å minimere miljøbelastningen og fremme klimavennlige løsninger ved sine anskaffelser og kan stille miljøkrav og kriterier i alle trinn av anskaffelsesprosessen der det er relevant og knyttet til leveransen (vår utheving). I tråd med dette bør også krav til IKT-sikkerhet kun gjelde der dette er relevant og knyttet til leveransen. En generell plikt til å stille krav til IKT-sikkerhet vil, for de anskaffelsene der dette ikke er direkte relevant eller knyttet til leveransen, kunne virke både konkurransebegrensende/-vridende og prisdrivende. Det er en rekke kjøp av varer og tjenester hvor krav til IKT-sikkerhet også vil utelukke mindre leverandører fra konkurransen, fordi dette ikke er en integrert del av leverandørens kvalitetssikringssystem/leveransekjede.

Statens standardavtaler (SSA-avtaler) – ikke bare krav til IKT-sikkerhet, men også iverksetting uten ugrunnet opphold

Når det gjelder Statens standardavtaler (SSA-avtaler), så bør det ikke bare vurderes å innføre krav til IKT-sikkerhet, men også krav om at de iverksettes uten ugrunnet opphold. SSA-avtalene er primært utviklet for ivareta det offentliges behov for et standardisert avtaleverk for kjøp av IT og konsulenttjenester. Per i dag er det opp til hver enkelt oppdragsgiver å vurdere og formalisere krav til IKT-sikkerhet ut over det som i dag er regulert (personopplysninger som en følge av ny personvernforordning, samt informasjonssikkerhet). Det bør derfor inntas standardbestemmelser når det gjelder krav som fremgår i ny lov om nasjonal sikkerhet og forskrift om virksomheters arbeid med

forebyggende sikkerhet. Dette bør inntas i Statens standardavtalenes bilagsstruktur slik at det kun kommer til anvendelse der dette er relevant og har tilknytning til leveransen.

Behov for kompetanseheving

Et generelt krav vil gjelde alle kommuner og mindre offentlige virksomheter, og ikke bare de større statlige virksomhetene. En generell plikt til å stille krav om IKT-sikkerhet for alle anskaffelser vil derfor kreve heving av kompetanse og kunnskap om IKT-sikkerhet og risiko knyttet til anskaffelser av IKT-produkter og tjenester hos alle offentlige oppdragsgivere. DSB deler utvalgets vurdering om at manglende kompetanse, risikoforståelse og -erkjennelse er utfordrende. Anbefalingen om opprettelse av et nasjonalt IKT-sikkerhetssenter er etter DSB vurdering et godt tiltak for å gi anskaffende myndigheter tilgang på bistand, råd og veiledning knytte til fremtidige utfordringer innenfor IKT sikkerhet og i anskaffelser hvor krav om IKT-sikkerhet som påvirker leverandøren er relevant.

3. Nytt nasjonalt IKT-sikkerhetssenter

Utvalget mener at et IKT-sikkerhetssenter kan bidra til å styrke den nasjonale IKT-sikkerheten og legge til rette for bedre oppgaveløsning og mer effektivt samarbeid mellom etater med tverrsektorielt ansvar for nasjonal IKT-sikkerhet og mellom disse og sektormyndighetene. DSB deler denne vurderingen, og ser også behovet for økt samarbeid mellom offentlige myndigheter, private infrastruktureiere og næringslivet.

Utvalget peker på behovet for økt kompetanse og bevissthet om risiko knyttet til IKT-hendelser og IKT-sikkerhet. DSBs kunnskapsgrunnlag[3] viser det sammen, og vi ser behovet for å samle IKT-sikkerhetskompetansen og koordinere ressursene. En mulighet kan være å opprette et nytt senter slik som utvalget anbefaler, en annen mulighet kan være å videreutvikle NSMs påbegynte etablering av et nasjonalt cybersikkerhetssenter. Til det sistnevnte alternativet understreker vi imidlertid nødvendigheten av å bredde ut perspektivet sammenlignet med NSMs planlagte innretning av cybersikkerhetssenteret. I tillegg til å fokusere på forebygging, detektering og håndtering er det nødvendig med oppmerksomhet mot og kunnskap om avhengigheter mellom ulike samfunnsfunksjoner, mulige følgehendelser og ikke minst hvilke konsekvenser dette kan få for befolkningen.

I et samfunnssikkerhetsperspektiv krever IKT-hendelser og risiko og sårbarhet knyttet til digitale verdikjeder særskilt oppmerksomhet. Dette fordi det er vanskelig å få oversikt over sårbarhet i de digitale verdikjedene og siden kaskadeeffektene etter IKT-hendelser inntreffer svært raskt og forplanter seg videre. Hybride trusler er et eksempel som viser viktigheten av å involvere bredt og sikre at de "riktige" aktørene er med. Dette bl.a. for å sikre nødvendig informasjonsdeling, koordinering og et felles situasjonsbilde så tidlig som mulig i håndteringen av en hendelse.

4. Tydelig regulering og ansvar for tilkoblede produkter og tjenester

Antallet produkter og tjenester som er koblet til internett er stort og i sterk økning. Utvalget er opptatt av at produkter og tjenester som selges i Norge, skal ha akseptabel IKT-sikkerhet og at myndighetsansvaret på dette området må tydeliggjøres.

Produkter med innebygd programvare, hvor programvaren påvirker sikkerheten, er avhengig av at sikkerheten til produktet er testet med aktuelle programvare. Ved oppgradering av programvare fra produsenten vil produsenten være ansvarlig for sikkerheten også etter oppgraderingen. Dersom brukeren

[3] Blant annet DSBs gjennomgang av situasjonsbeskrivelser, spørreundersøkelse om IKT-sikkerhet i kommunene, dialog og tilbakemeldinger med fylkesmannsembetene

oppgraderer produktet med tredjepartsprogramvare vil dette kunne påvirke sikkerheten til produktene og man kan få uklare ansvarsforhold i tilfelle dette skaper et farlig produkt. Videre vil slike produkt være sårbar for "hacking" som i verste fall sette brukeren i farlige situasjonen. Hvordan datasikkerheten i disse produktene er ivaretatt er følgelig vesentlig for sikkerheten.

Manglende IKT-sikkerhet i produkter og tjenester kan utgjøre en trussel for den enkelte forbrukeren, for virksomheter og for samfunnssikkerheten. Utvalget løfter frem fire anbefalinger som skal øke IKT-sikkerheten på dette området.

DSB mener utvalget i liten grad omtaler rammer og premisser for regulering på produktsikkerhetsområdet. Dette er imidlertid viktig som bakgrunn for å vurdere hvorvidt DSB bør ha en tydeligere rolle når det gjelder varsling, rapportering, tilbakekalling og håndtering ved manglende IKT-sikkerhet i tilkoblede produkter og tjenester.

Overordnede rammer og premisser for regulering på produktsikkerhetsområdet

Produktområdet er i stor grad underlagt harmonisert regelverk. EUs hovedregler om fritt varebytte er nedfelt i EØS-avtalen, og gjennom den har vi fått et omfattende harmonisert regelverk for produkter innlemmet i norsk rett. Regelverket dekker ulike aspekter og egenskaper ved selve produktet, prosedyrer for samsvarsvurderinger og regler for utpeking av tekniske kontrollorganer (TKOer) mv.

DSB har i dag et myndighetsansvar for 17 ulike rettsakter/produktområder innenfor det harmoniserte vareområdet. Sektorspesifikke rettsakter på vareområdet blir gjennomført i norsk rett, avhengig av hvor de innholdsmessig hører til. For DSBs del innebærer det forvaltningsansvar for et stort antall sektorspesifikke rettsakter innenfor våre ansvarsområder. De nasjonale forskriftene som gjennomfører direktivene i norsk rett er hjemlet i produktkontrolloven, el-tilsynsloven og brann- og eksplosjonsvernloven som DSB forvalter.

Vareområdet/produktområdet er gjennom vår EØS forpliktelse i stor grad gjennomregulert av felleseuropeiske krav i direktiver og forordninger. Forenklet kan man si at en del av de "tradisjonelle" farlige egenskapene/risiko og/eller virkning av ulike produkter knyttet til helse, miljø og sikkerhet er omfattet av de ulike sektorspesifikke rettsaktene.

DSB har eksempelvis sammen med Miljødirektoratet et myndighetsansvar for leketøyforskriften som gjennomfører leketøydirektivet i norsk rett. DSB fører tilsyn med de deler av forskriften som omhandler fysiske og mekaniske egenskaper, brann- og eksplosjonsegenskaper og elektriske og radioaktive egenskaper ved leketøy, mens Miljødirektoratet har ansvar for de kjemiske, hygieniske, støyende og biologiske egenskapene.

Det er i dag ikke fastsatt krav i de ulike harmoniserte sektorregelverk som ivaretar de "nye" farlige egenskaper som for eksempel fare for hacking, manipulasjon mv. Leketøyregelverket og de harmoniserte standardene under direktivet har for eksempel ikke konkrete krav knyttet til IKT-sikkerhet.

Produktkontrolloven er også sentral ved at den oppstiller et generelt sikkerhetskrav til alle produkter som ikke er særskilt regulert ved annen lovgivning. Dette omtales gjerne som det ikke-harmoniserte vareområdet. Loven pålegger markedsaktørene å sørge for sikre produkter, og har generelle bestemmelser om aktsomhetsplikt, kunnskapsplikt og meldeplikt. På det ikke-harmoniserte området har også prinsippet om gjensidig godkjenning betydning for reguleringen. Prinsippet om gjensidig godkjenning innebærer at en vare som er lovlig produsert og eventuelt omsatt i en EØS-stat, i utgangspunktet også skal kunne omsettes i alle andre EØS-stater uten å måtte oppfylle ytterligere vare- eller kontrollkrav. Dersom nasjonale myndigheter forbyr varer som er lovlig omsatt i andre EØS-stater, er dette en handelshindring som i utgangspunktet er forbudt etter EØS-avtalens artikkel 11.

Myndighetene har likevel mulighet til å forby en vare, for å ivareta viktige samfunnsmessige hensyn, jf. EØS-avtalen artikkel 13. Tiltaket må da begrunnes i hensynet til blant annet menneskers og dyrs helse, forbruker- og miljøvern. Samtidig må tiltaket oppfylle proporsjonalitetsprinsippet som innebærer at tiltaket må være egnet for å oppnå sitt angitte formål, og ikke gå lenger enn nødvendig.

Utvalget viser til klage på manglende sikkerhet ved lekene Cayla-dukken og I-que, og at Forbrukerrådet i 2016 erfarte at ingen tilsyn tok tak i disse sakene til tross for kontakt med DSB og andre myndigheter.

DSB hadde i 2016 flere møter og dialog med Forbrukerrådet i forbindelse med deres funn. På bakgrunn av bekymringsmelding fra Forbrukerrådet gjennomførte DSB produkttilsyn med de aktuelle lekene. Importøren ble pålagt å dokumentere at lekene oppfylte kravene i leketøyforskriften. Direktoratet fant imidlertid ikke at det var grunnlag eller hjemmel i dagens regelverk for å forby omsetning eller tilbakekalle produktene. Saken avdekket en type risiko/farlig egenskap som per i dag ikke direkte omfattes av sikkerhetskrav i leketøyforskriften eller gjeldende harmoniserte standarder for leketøy. Det finnes altså ingen konkrete krav til digital sikkerhet i leketøyforskriften.

Utvalget peker på at det er viktig å bidra til et oppdatert regelverk på EU-nivå. Heller det enn at Norge unilateralt endrer regelverket på feltet. I den sammenheng kan det nevnes at problemstillingen knyttet til risiko ved internettbasert leketøy ble reist på ekspertgruppemøte for leketøydirektivet 22. juni 2017; av både ANEC og Norge ved DSB, som en oppfølging etter den konkrete saken Forbrukerrådet avdekket med Cayla-dukken og I-que. I møtet var det enighet blant medlemslandene og Kommisjonen om at leketøydirektivet (herunder leketøystandarden) ikke omfatter/regulerer denne type risiko - og at datasikkerhet og personvern bør løses gjennom en horisontal tverssektoriell tilnærming til internettbaserte produkter generelt. Kommisjonen ga i møte tilbakemelding om at de ville følge opp dette ved å sende en henvendelse til både DG CNECT og DG Justice and consumer. DSB er kjent med at problemstillingen diskuteres i flere sektorer, både i Adco- og ekspertmøter og CSN. DSB følger i dag diskusjonene innenfor sine sektorspesifikke ansvarsområder.

Mange tilkoblede produkter brukes på tvers av landegrenser og DSB støtter derfor utvalgets anbefaling om viktigheten av å bidra til et oppdatert regelverk på EU-nivå enn at Norge unilateralt endrer regelverket på feltet. Regulering må etter DSBs vurdering skje innenfor rammene som gjelder varelovgivningen i EØS, da unilateralt regelverk kan komme i konflikt med EØS-avtalens bestemmelser om fri flyt av varer og tjenester.

I denne forbindelse ønsker vi imidlertid også å bemerke at EØS-vareloven gir overordnede bestemmelser om oppfølging av potensielt farlige produkter og tilsyn på produktsikkerhetsområdet, herunder bruk av reaksjonsmidler. Loven gjennomfører forordning (EF) nr. 765/2008 om fastsettelse av krav til akkreditering og markedstilsyn for markedsføring av varer i norsk rett og inneholder bestemmelser som gir rammer for tilsyn og oppfølging av produkter.

Risiko og sårbarhet knyttet til IKT-sikkerhet i tilkoblede produkter vil kunne påvirke samfunnssikkerheten i bredt. Det vil kunne få store konsekvenser innen en rekke samfunnsområder, og det vil i sin ytterste konsekvens kunne utfordre den grunnleggende tryggheten i vårt samfunn. DSB mener det er en stor og svært omfattende oppgave som utvalget anbefaler DSB skal ta et tydeligere ansvar for. For å kunne ivareta en slik rolle må direktoratet tilføres både hjemler, kompetanse og ressurser. Det er derfor DSB klare oppfatning at det først og fremst er behov for en egen bredere utredning når det gjelder roller, ansvar, konsekvenser og kompetanse- og ressursbehov knyttet til et utvidet ansvar for IKT-sikkerhet i tilkoblede produkter. Deretter kan man vurdere hvor det er mest hensiktsmessig at et slikt ansvar plasseres.

Vedrørende IKT-sikkerhet og medisinskteknisk utstyr

I dag reguleres dette i de medisinske direktivene og gjennom standarder utarbeidet for å håndtere sikkerheten. Fra og med 8. mars 2019 er ansvaret for produktregelverket knyttet til elektromedisinsk utstyr overført fra Justis- og beredskapsdepartementet til Helse- og omsorgsdepartementet og ansvaret for forvaltningen av produktregelverket samles i Statens legemiddelverk.

5. Tydeligere styring og bedre koordinering nasjonal IKT-sikkerhet

Utvalget viser til utfordringene knyttet til JDs samordningsansvar i vårt konstitusjonelle system hvor ministeransvaret er en grunnleggende forutsetning. I følge utvalget må departementet utøve et tydeligere lederskap for det samordningsansvaret de allerede har for IKT-sikkerhet i sivil sektor.

Som samfunn må vi hele tiden tilpasse oss et utfordringsbilde i endring. Blant annet øker behovet for en mer samlet og tverrsektoriell oppmerksomhet om IKT-sikkerhet i takt med utviklingen mot et stadig mer digitalisert samfunn. Endringer i etatsstrukturer som er gjennomført etter at utvalget leverte sin utredning kan bidra til en økt og samlet oppmerksomhet om IKT-sikkerhet. DSB er positive til at ansvaret for IKT-sikkerhet, som politikkområde i sivil sektor nå er samlet under JD og ser mulighetene dette gir med tanke på utvikling av arbeidet med IKT-sikkerhet tverrsektorielt. Satsningsområder, prioriteringer og veivalg kan enklere samordnes og ses under ett. DSB understreker imidlertid viktigheten av at koblingen mellom sivil sektor og forsvarssektoren beholdes og videreutvikles, og funksjonene som først og fremst understøtter forsvarets behov ivaretas i det videre arbeidet.

Med hilsen
for Direktoratet for samfunnssikkerhet og beredskap

Cecilie Daae
direktør

Elisabeth Longva
avdelingsdirektør

Dokumentet er godkjent elektronisk og sendes derfor uten underskrift.

Kopi til:
roger.kolbotn@jd.dep.no.