

Vår saksbehandler

Vår dato
2006-10-30
Deres dato
2006-06-26Vår referanse
Deres referanse
200604470-RBA-K/LB/BHHJustis- og politidepartementet
Postboks 8005 Dep
0030 Oslo

NOU 2006:6 Når sikkerhet er viktigst - Kommentarer fra Standard Norge

Standard Norge støtter hovedkonklusjonene i forslaget fra Infrastrukturutvalget slikt det fremkommer i NOU 2006:6 Når sikkerhet er viktigst.

I utredningen er bruk av standarder og standardiserte metoder allerede nevnt som mulig virkemiddel. Mye av utviklingen innenfor dette fagområdet skjer internasjonalt. Det vil derfor være viktig at Norge og norske interessenter deltar aktivt i dette arbeidet.

Innledningsvis vil vi nevne at definisjonen av kritisk infrastruktur er i tråd med hvordan dette begrepet er definert i internasjonalt standardiseringsarbeid (kapittel 3). Omfanget av sikkerhetsutfordringene, nevnt i kapittel 4 er også i tråd med utgangspunktet for det pågående standardiseringsarbeidet.

Til de enkelte kapitlene i meldingen har vi følgende kommentarer:

3 Definisjoner av sentrale begreper

Risiko

Forklaringen av begrepet risiko er i samsvar med definisjonen i NS-ISO/IEC Guide 73 *Risikostyring - Terminologi - Retningslinjer til bruk i standarder* og ISO/IEC Guide 51 *Safety aspects - Guidelines for their inclusion in standards*.

I NOU 2006:6 er risiko knyttet til en uønsket hendelse, dette samsvarer med temaet i Guide 51. I Guide 73 er risiko nøytralt i den forstand at det handler om risiko knyttet til hendelser der hendelsen kan representere noe uønsket så vel som muligheter for gevinst. NOU'en virker åpen for at begrepet risiko kan forstås, måles og beskrives på forskjellig måte.

Den internasjonale standardiseringsorganisasjonen ISO utarbeider nå en standard for risikostyring (*Risk Management*). Standarden vil være en veiledning om risikostyring og skal omhandle hvilke generelle elementene som inngår i risikostyring, rammefaktorer som påvirker arbeidet og trinnene i en prosess for risikostyring. Standarden forventes publisert i 2009. Standarden vil være egnet som grunnlag for å utarbeide sektor- eller bransjeorienterte standarder for risikostyring. Standard Norge er også i ferd med å revidere NS 5814 *Risikoanalyser*. Standarden vil bli endret i forhold til samfunnsutviklingen innenfor dette området. Det er også utarbeidet en rekke sektorspesifikke standarder i tilknytning til området risiko.

Et felles begrepsapparat nedfelt i standarder er vesentlig for å etablering av et unngå misforståelser arbeidet innenfor dette området.

4 Sikkerhetsutfordringer

Klimaendringer/naturkatastrofer

Klimaendringer i form av økt nedbør og flere døgn med høy vindhastighet må antas å ha betydning for flom, rasfare og utforming/detaljering av byggverkets ytterhud. I kravene angitt i standardene innenfor dette området er det imidlertid ikke forventet at maksimal snømengde eller de dimensjonerende vindlaster øker på en slik måte at de påvirker byggverksikkerheten.

Omorganisering, omregulering og bortsetting

Nasjonal og internasjonal standardisering har arbeidet med ITIL (IT Infrastructure Library) hvor en forsøker å få informasjonen tilgjengelig bare for den som er autorisert og at informasjonen beskyttes slik at den ikke kommer uvedkommende i hende.

Konfidensialitetssikring forutsetter vel fungerende organisasjoner som har tilgangsrettigheter etter klare roller, rutiner og prosedyrer. I tillegg må det sørges for at det ikke er mulig å få tilgang gjennom alternative kanaler. Fellesstandarder for IT-drift er viktig ved bortsetting og i forbindelse med økte krav til virksomhetene (eks tilgjengelighet). Det er stor enighet om at ITIL, ISO 20000-serien *Information technology -- Service management*, er gode standarder for å dekke livssyklus for IT – også ut over selve driften eller deler av den.

Nettverksutfordringene er store og opplagt mer utfordrende enn det utredningen indikerer. Her er mulighetene mange for å få klargjort både trusler og muligheter i internett og i andre nett. Det er for eksempel lite i utredningen omkring mobile nett. En rekke paradokser springer ut av nettbruk og økt nettavhengighet. Kryptering og programmer som egner seg lite for kryptering, brannmurer som er komplekse å installere, kommunikasjonsprotokoller som er lite tilrettelagt for sikkerhet (TCP/IP), og at enkle grensesnitt som gir større tilgjengelighet for alle faktisk kan ha en problematisk side. Flere av disse forholdene kunne vært behandlet mer inngående.

5 Ansvar for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner

Ivaretagelse av samfunnsansvar

NOU-en drøfter i flere sammenhenger næringslivets samfunnsansvar med utgangspunkt i at næringslivets hovedoppgave er å skape verdier og økonomiske resultater.

Den siden av samfunnsansvar som hittil har vært mest i fokus går i hovedsak på næringslivets anseelse i forhold til etikk, salgsvirksomhet og etablering i utlandet, forholdet til menneskerettigheter og opptreden i forhold til miljø i vid forstand. På dette området arbeider den internasjonale standardiseringsorganisasjonen ISO med å utvikle en standard som skal gi retningslinjer for hvordan næringslivet og organisasjoner kan oppfylle det samfunnsansvar som virksomheten har påtatt seg. Dette er et eksempel på hva NOU-en selv er inne på om bruk av standarder som frivillige instrumenter for at bedrifter og organisasjoner tilpasser seg lover og regler eller andre retningslinjer for å oppfylle markeds mål eller mål for samfunnsgagnlig virksomhet

En fokusering på samfunnsansvar i sammenheng med sikkerhet og beredskap har som det fremgår av NOU-en, stort sett vært fraværende. Hva et slikt samfunnsansvar kan innebære er også et sentralt tema innenfor standardiseringen, for eksempel i det arbeidet som nå er startet opp i ISOs tekniske komité *Societal Security* (ISO/TC 223). Dette omfatter bl.a. en mulig standard for *Social security management*. De skillelinjer mellom kommersielt ansvar og statlig ansvar som fremgår av fig. 10.1 i NOU-ens vedlegg 10, illustrerer godt de momentene som står sentralt i den pågående diskusjon i dette ISO-arbeidet. I det forberedende arbeid med en slik standard har Standard Norge en lederfunksjon.

Dette illustrerer den rolle standardiseringen kan spille i et samspill med ulike reguleringstiltak og det er viktig at norske interessenter er engasjert i utviklingen av slike standarder.

Samarbeid på tvers av offentlig og privat sektor

Dette avsnittet viderefører drøftelsen i avsnitt 5.3.1 og peker på behovet for at det finnes arenaer for utforming av frivillige ordninger og strategier som bidrar til at næringslivet kan leve opp til samfunnets og bedriftenes eget krav til ansvarlighet. Myndighetene oppfordres til å se potensialet i denne arbeidsformen som bl.a. kan lede til oppfyllelse av omforente minstestandarder.

Igjen illustrerer dette nytten av den frivillige standardiseringen som vi har gitt konkrete eksempler på i avsnittet foran. Vi vil også peke på at standardiseringen gjennom sin arbeidsform etablerer komiteer som fungerer som nasjonale eller internasjonale arenaer for deltakere fra alle parter som har nytte og interesse av de standardene som er målet for arbeidet. Arbeidet bygger på konsensusprinsippet som er nøkkelen til at disse frivillige standardene blir tatt i bruk.

Forslag knyttet til prinsipper for god sikkerhetskultur

Dette avsnittet peker på en rekke tiltak som bør legges til grunn for alle virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner. Vi har i vår kommentar til avsnitt 5.3.1, pekt på det standardiseringsarbeidet som nå startes opp i ISO /TC 223. For tiden bearbeides utkast til en standard om *Emergency Preparedness and Operational Continuity*. Alle de punktene som er listet opp i NOU-en omhandles i utkastet og setter dette inn i en sammenheng som ligger nær opp til strukturen i de styringssystemstandardene som ISO har utviklet for kvalitetsledelse NS-ISO 9000 og miljørettet ledelse NS-ISO 14000. Disse standardene er i omfattende bruk i næringslivet både internasjonalt og i Norge. Derved er grunnlaget for en implementering av styringssystemstandarder for "security" i bedrifter og organisasjoner langt på vei på plass.

6 Virkemidler

Forslag knyttet til plan- og bygningsloven

Standard Norge er positiv i forhold til forslaget om at samfunnssikkerhetsperspektivet i større grad enn i dag legges inn i ny Plan- og bygningslov. Vi viser i den forbindelse også til bestemmelsene i teknisk forskrift kapittel V om bruk av standarder til å dokumentere oppfyllelse av Plan- og bygningslovens materielle regler og av Teknisk Forskrifts tekniske krav.

Norske standarder har spilt en betydelig rolle i myndighetenes rolle for å sikre tilstrekkelig byggverksikkerhet i Norge siden 1960-tallet. I Europa er det nå utviklet et nytt felles sett standarder; Eurokoder som skal ivareta sikkerhet av produkter benyttet i bygningsformål så vel som det ferdige byggverks sikkerhet. Vi har i Norge gjennom en årrekke differensiert krav til sikkerhet ut fra konsekvens ved sammenbrudd ved bruk av tre pålitelighetsklasser som skal innebære reduksjon i sannsynligheten for skade ut fra alvorligheten av konsekvens. Dette systemet vil bli videreført når Eurokodene tas i bruk.

Byggverk dimensjoneres ut fra normal bruk, samt ikke tilsiktede uønskede hendelser, ulykkeslaster, men ikke ut fra planlagte ikke ønskede hendelser; terroraktivitet. Dette med forbehold at det gjøres en del tiltak for å binde konstruksjoner sammen på en slik måte at en uønsket hendelse ikke skal føre til uforholdsmessig skadeomfang. Å prosjektere normale byggverk for massiv terroraktivitet er ikke praktisk hensiktsmessig. Ved slike

anslag er avstand det mest hensiktsmessige virkemiddel, de generelle tiltak for å binde konstruksjoner sammen vil imidlertid begrense ringvirkningene av en massiv terroraktivitet.

Forslag knyttet til bruk av standarder og standardiserte metoder

NOU-ens forslag til bruk av standarder som virkemiddel støtter opp under Standard Norges egne strategier og prioriteringer for arbeidet innenfor dette området. Standard Norges arbeid følger i stor grad den internasjonale standardiseringsaktiviteten på området.

Forslag knyttet til offentlige innkjøp

ISO 17799 *Administrasjon av informasjonssikkerhet* og ISO 20000 *Information technology -- Service management* er viktige, men her bør en kan hende ha en strategi for å følge med på nye områder, som biometri. Mange standarder er under utvikling og ikke minst er det vesentlig å kunne arbeide med vokabular etc (semantisk).

7 Sikkerhetsloven og den forebyggende sikkerhetstjenesten

Personellsikkerhet

Et standardiseringsprosjekt innenfor *ID Management* er igangsatt i en nystartet arbeidsgruppe i tillegg til det pågående arbeidet i ISO/IEC JTC1 SC 17 IT *Identifikasjon av personer*. Arbeidet innenfor ISO/IEC JTC1 SC 37 IT *Biometri*, WG 6 *Juridiske og sosiale sider ved bruk av biometri*, er også viktig i denne forbindelse.

Forskrift om personellsikkerhet

I 7.3.4 er det mulig en bør ha en utvidelse til produkter (og prosesser) som er framarbeidet slik at de kan evalueres i overensstemmelse med prinsippene i ISO 15408 *Common Criteria*.

10 Kartlegging av kritisk infrastruktur og sektorvise anbefalinger

Olje og gass

Under overskriften regulatoriske virkemidler (10.5.4.2) skriver utvalget at det mener det er behov for å vurdere tilsynsvirkomheten for å avklare gråsoner. Det anføres at det har oppstått uklare grenseflater mellom berørte myndigheter i forbindelse med at Petroleumstilsynet ble gitt ansvar for tilsyn med åtte petroleumsrelaterte anlegg på land.

Standard Norge ønsker å peke på de gode erfaringene som er gjort med et funksjonsrettet regelverk der det henvises til anerkjente normer og standarder, slik som det har vært praktisert av Petroleumstilsynet på kontinentalsokkelen. Det er grunn til å understreke verdien av at normer og standarder utvikles gjennom et trepartsamarbeid mellom myndigheter, industrien og arbeidstakerne. Myndighetene avlastes i forhold til å måtte utforme og vedlikeholde detaljerte forskrifter, industrien bidrar med beste praksis gjennom erfaringer og arbeidstakere deltar i sikring av eierskap. Denne modellen for kunnskaps- og arbeidsdeling bør vurderes anvendt i større grad også utenom olje og gass området.

11 Kartlegging av kritiske samfunnsfunksjoner og sektorvise anbefalinger

Nød- og redningstjeneste

Når mange forskjellige mennesker skal kommunisere under stress og på tvers av fagområder og geografiske grenser er det viktig at kommunikasjonen er entydig standardisert gjennom termer og definisjoner. Arbeidet utført i Kollegiet for brannfarlig terminologi er et ledd i tilfredsstillelse av dette behovet. Arbeidet bør videreføres gjennom standardisering.

Kriseledelse

Til avsnittet har Standard Norge ingen direkte kommentarer, men vi vil likevel nevne at det bredt anlagte standardiseringsarbeid i CEN og ISO spenner over en rekke aktiviteter og systemer som er relevante i krisehåndteringssammenheng. Dette gjelder for eksempel det europeiske arbeidet innenfor CEN/BT/WG 161 *Protection and security of the citizen* der det etableres et standardiseringsprogram innenfor samfunnssikkerhet og der et av områdene er *Emergency services*. Globalt er det innenfor ISO/TC 223 *Societal Security* etablert standardiseringsprosjekter innenfor kriseledelse som tidligere omtalt.

Igjen vil vi oppfordre til at myndighetene vurdere hvordan Norge kan bidra til dette internasjonale arbeidet og nyttiggjøre seg de resultater som kommer ut av dette. Beredskap og krisehåndtering er ikke et nasjonalt anliggende alene og en stadig mer globalisert verden krever global tenkning og samordning for å finne løsninger på felles utfordring. Standardiseringsarbeidet tar sikte på praktiske løsninger som nettopp kan være til hjelp i den krisehåndtering også norske myndigheter vil måtte være forberedt på å stå overfor. Da må det være av betydning for norske interesser og være med på å utvikle slike løsninger gjennom en aktiv deltakelse i det internasjonale standardiseringsarbeidet.

Litteraturliste

Det er nylig utkommet en lærebok (2 opplag i 2006) fra Daler, Guldbrandsen, Høie og Sjølstad, Håndbok i datasikkerhet. Tapir. Denne er, ikke minst, god på tjenester, serviceledelse, ut(bort)setting, datanett samt bruk av mobilt utstyr.

Standard Norge støtter viktigheten av å utforme prinsipper for god sikkerhetskultur. Standarder kan være et virkemiddel for å oppnå dette slik som beskrevet i kapittel 6. For eksempel på IT området har det i lang tid vært arbeid med innsamling, vurdering og formulering av god praksis. Slike prosesser for etablering av god praksis har resultert i standardene ISO 17799 *Administrasjon av informasjonssikkerhet* og ISO 20000 *Information technology – Service Management*. Standard Norge vil derfor kunne bidra til utarbeidelsen av den anbefalte informasjonshåndboken.

Med hilsen
for Standard Norge
Anne Kristoffersen
akr@standard.no