Dokument nr. 3-serien

Riksrevisjonen

Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur

Dokument nr. 3:4 (2005–2006)

Dokument nr. 3-serien

Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur

Dokument nr. 3:4 (2005–2006)

Til Stortinget

Riksrevisjonen legger med dette fram Dokument nr. 3:4 (2005–2006), Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur.

Riksrevisjonen 22. november 2005.

For riksrevisorkollegiet

Bjarne Mørk-Eidem
riksrevisor

Innhold

Forsvarsdepartementet, Justis- og politidepartementet, Moderniseringsdepartementet og Samferdselsdepartementet

Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur

1 Innledning

De teknologiske framskrittene innen data- og informasjonssystemer har gitt oss muligheter til å løse en rekke samfunnsoppgaver på nye måter. De har dessuten bidratt til å øke effektiviteten både i offentlig og i privat sektor. Sårbarhetsutvalgets rapport, NOU 2000:24 *Samfunnets sårbarhet*, slår fast at IT-systemer har blitt en av samfunnets bærebjelker. Samfunnet har dermed blitt sårbart for svikt i disse systemene. Sårbarhetsutvalget påpeker at alle IT-systemer er i konstant fare for å bli angrepet, og at tendensen er at stadig flere virksomheter opplever IT-relaterte økonomiske tap. Mørketallsundersøkelsen viste for eksempel at i 2003 ble ca. 60 % av norske virksomheter rammet av datakriminalitet eller andre uønskede hendelser, og at dette kostet norske virksomheter mer enn fem milliarder kroner.[1]

I enkelte tilfeller har svikt i IT-systemer på grunn av tilfeldige feil skapt betydelige problemer for den berørte. Det gjelder for eksempel når banksystemer eller telefonnett har vært utilgjengelige for brukerne. Disse hendelsene illustrerer hvilke potensielle problemer samfunnet kan stå overfor dersom noen ønsker å angripe viktige samfunnsfunksjoner. Sårbarhetsutvalget legger til grunn at andre stater og terrorgrupper med forholdsvis enkle midler kan lamme viktige virksomheter og samfunnsfunksjoner gjennom fiendtlige informasjonsoperasjoner.

Sårbarhetsutvalgets arbeid var en viktig premiss for arbeidet med St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet. Veien til et mindre sårbart samfunn*, jf. Innst. S. nr. 9 (2002–2003). Meldingen gir bl.a. en oversikt over sårbarhetsreduserende tiltak innenfor informasjons- og kommunikasjonsteknologi. Regjeringen signaliserer i meldingen at den også vil ta initiativ til å utarbeide en nasjonal strategi for informasjonssikkerhet. En slik nasjonal strategi for informasjonssikkerhet forelå i juni 2003, og mye av sikkerhetsarbeidet de seneste årene er fanget opp i strategien og tiltakene i denne.

Sikkerhet i teleinfrastrukturen er nært knyttet til IT-sikkerheten i samfunnet. St.meld. nr. 47 (2000–2001) *Telesikkerhet og -beredskap i et telemarked med fri konkurranse,* jf. Innst. S. nr. 329 (2000–2001), peker på en rekke tiltak for å bedre telesikkerheten og -beredskapen i Norge.

Formålet med undersøkelsen har vært å vurdere om myndighetenes arbeid med IT-sikkerhet i samfunnet er i samsvar med Stortingets vedtak og forutsetninger. Dette innebærer å vurdere:

- organiseringen av myndighetenes arbeid
- plan- og gjennomføringsprosessene
- tiltakene som er iverksatt på området

Undersøkelsen omfatter både tiltak for bedre IT-sikkerhet og tiltak for bedre telesikkerhet.

Riksrevisjonens rapport om undersøkelsen følger som trykt vedlegg. Et utkast til rapport ble oversendt Justis- og politidepartementet, Moderniseringsdepartementet, Samferdselsdepartementet og Forsvarsdepartementet i brev av 8. juli 2005. Departementene har avgitt uttalelse til de forholdene som er tatt opp. Mottatte merknader til rapportens faktadel er innarbeidet. Departementenes merknader til rapportens vurderinger er gjengitt i kapittel 3.

2 Oppsummering av undersøkelsen

Undersøkelsen er gjennomført ved analyse av sentrale dokumenter i arbeidet med informasjonssikkerhet innen statsforvaltningen, ved intervjuer og ved en spørreundersøkelse. Intervjuene og spørreundersøkelsen er gjennomført for å få mer detaljert informasjon om tiltak og arbeidsprosesser på området, og for å innhente synspunkter på sentrale problemstillinger i undersøkelsen. Spørreundersøkelsen og intervjuene omfattet de berørte departementene, relevante underliggende virksomheter og organer opprettet av forvaltningen, samt bransjeorganisasjoner som er gitt oppfølgingsansvar i Nasjonal strategi for informasjonssikkerhet.[2]

2.1 Organiseringen av forvaltningens arbeid med IT-sikkerhet

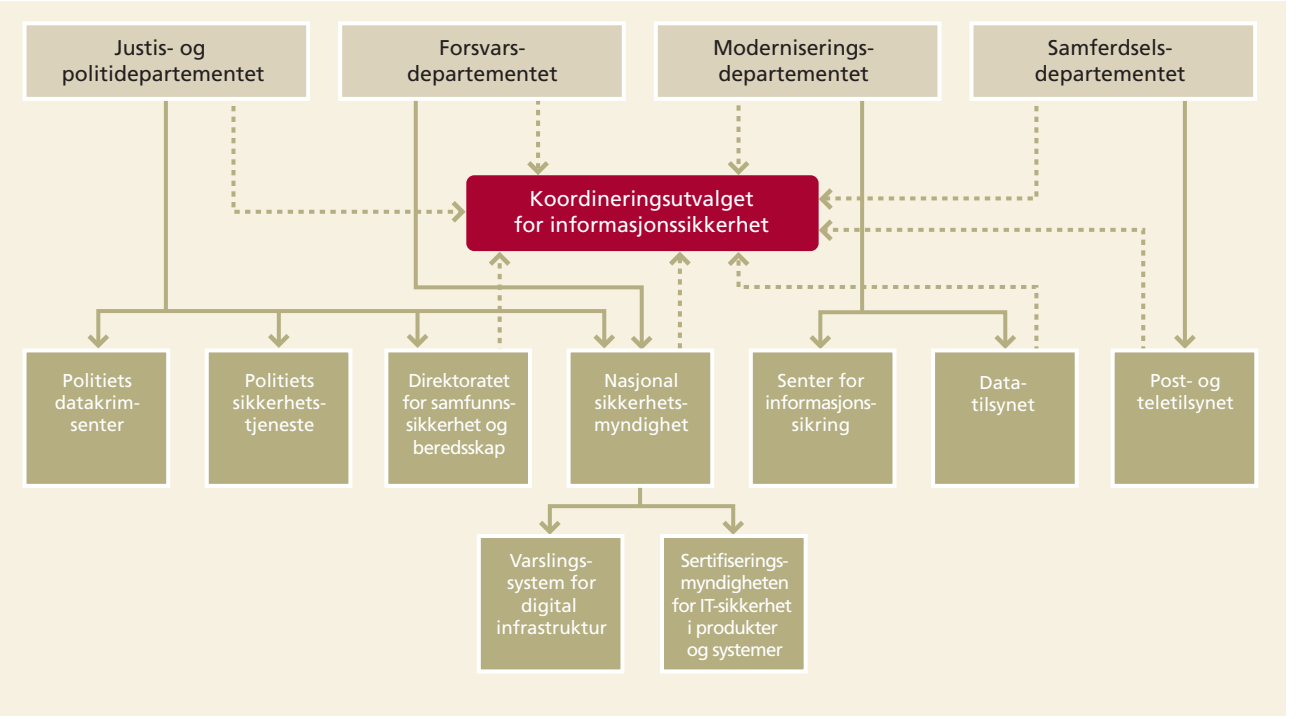
St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* forutsetter at ansvaret for IT-sikkerhet er et virksomhetsansvar. Dette er fulgt opp gjennom organiseringen av arbeidet i staten, der det enkelte departement er ansvarlig for at IT-sikkerheten ivaretas i departementet, i dets underliggende virksomheter og innen egen sektor.

Koordineringsoppgaver og tverrgående tilsynsoppgaver innen IT-sikkerhet er i tillegg tillagt en rekke departementer, etater og utvalg som vist i figuren på neste side.

1) Mørketallsundersøkelsen 2003. Om datakriminalitet og IT-sikkerhet. Økokrim, Næringslivets Sikkerhetsråd og Senter for informasjonssikring. Juni 2004

2) Abelia, IKT-Norge og Næringslivets Sikkerhetsråd ble forespurt i undersøkelsen.

Organer med sentrale oppgaver innenfor IT-sikkerhet



Justis- og politidepartementet har et samordnings- og tilsynsansvar for samfunnets sivile sikkerhet og for beredskap i kritisk infrastruktur. Forsvarsdepartementet har ansvar for utforming og iverksetting av norsk sikkerhets- og forsvarspolitikk, herunder forvaltningsansvar for sikkerhetsloven som retter seg mot trusler i form av spionasje, sabotasje eller terrorhandlinger som kan true rikets selvstendighet og sikkerhet og andre vitale samfunnsinteresser.

Moderniseringsdepartementet har ansvaret for koordinering av regjeringens IT-politikk, herunder arbeidet med IT-sikkerhet. Det skal identifisere og følge opp sektorovergripende spørsmål, samt initiere og koordinere tiltak av tverrsektoriell karakter på dette området. Samferdselsdepartementet har ansvar for telesikkerhet og –beredskap, og er regelverksforvalter av lov om elektronisk kommunikasjon (ekomloven) som setter krav til sikkerhet og beredskap.

St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* og Innst. S. nr. 9 (2002–2003) påpeker betydningen av koordinering og ansvarsklargjøring innenfor IT-sikkerhetsarbeidet. Undersøkelsen viser at det fortsatt mangler avklaringer mellom departementene på følgende områder:

- *Ansvaret for kritisk infrastruktur*: Det er uklart hva Justis- og politidepartementets ansvar for kritisk infrastruktur innebærer, hva ansvaret for IT-sikkerheten i denne strukturen omfatter, og hvilket overordnet ansvar Justis- og politidepartementet har for IT-sikkerheten i en krisesituasjon.
- *Ansvaret for Internett*: Samferdselsdepartementet har ansvar for forhold som er underlagt lov om elektronisk kommunikasjon (ekomloven), herunder Internett. Det er imidlertid ulike oppfatninger mellom departementene når det gjelder Samferdselsdepartements ansvar for sikkerhet for Internett-relaterte tjenester sett i forhold til Moderniseringsdepartementets ansvar for helheten i IT-sikkerhetsarbeidet.
- *Kontakten med næringslivet*: Departementene ble omorganisert i 2004. Hvorvidt Moderniseringsdepartementet eller Nærings- og handelsdepartementet skulle følge opp bruken av IT i næringslivet, ble ikke avklart før i april 2005. Nærings- og handelsdepartementet har nå opprettet en seksjon som bl.a. har ansvar for å følge opp bruken av IT i næringslivet. Samtidig skal Moderniserings-departementet ha pådriveransvar for alle tiltak i Nasjonal strategi for informasjonssikkerhet som retter seg mot eller inkluderer næringslivet.

I undersøkelsen stilles det spørsmål om hvilke konsekvenser manglende ansvarsavklaringer kan få i en krisesituasjon.

Figuren over viser at det er mange fagorganer som har oppgaver innenfor IT-sikkerhet. Ifølge St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet,* Innst. S. nr. 9 (2002–2003) og St.prp. nr. 1 (2002–2003) for Justis- og politidepartementet og Nærings- og handelsdepartementet skal ansvarsforholdet også mellom ulike fagorganer klargjøres. Undersøkelsen viser at det har skjedd en del formelle avklaringer de siste årene mellom disse organene. De fleste fagorganene og bransjeorganisasjonene som inngår i undersøkelsen, mener imidlertid at ansvaret for informasjonssikkerhet i forvaltningen er spredt på en rekke forskjellige aktører, hvorav flere har relativt begrensede ressurser på området. Flere av fagorganene og bransjeorganisasjonene påpeker manglende

avklaringer, fragmentering og at begrensede ressurser brukes til overlappende oppgaver. Bransjeorganisasjonene mener det er vanskelig å finne ut hvilket organ som har ansvar for hvilke forhold innen IT-sikkerhet.

Som en oppfølging av Nasjonal strategi for informasjonssikkerhet ble Koordineringsutvalget for informasjonssikkerhet etablert i 2004 for å sikre koordinering av arbeidet. Moderniseringsdepartementet leder utvalget som består av representanter fra departementer og etater som vist med stiplet linje i figuren, i tillegg til enkelte andre departementer og etater. Utvalget har ingen myndighet til å fatte vedtak, men skal fungere som arena for drøfting og være en rådgivende instans overfor departementer og etater. Det er for tidlig å vurdere om utvalget har bidratt til bedre koordinering av arbeidet med IT-sikkerhet.

2.2 Samfunnskritisk IT-infrastruktur

IT-systemer har de seneste tiårene blitt en viktig del av de fleste samfunnsfunksjoner, for eksempel bank- og finansvesen, kraft- og vannforsyning, trafikkstyringssystemer og systemer innenfor helse- og sosialsektoren. For å effektivisere arbeidet har IT-systemene i stadig større grad blitt knyttet sammen, både innenfor virksomheter og på tvers av organisasjonsgrenser. Dette har økt avhengigheten mellom IT-systemer og mellom virksomheter, og gjort det viktigere å definere hvilke deler av IT-infrastrukturen som er kritiske for samfunnet.

Manglende avgrensning av hva som er samfunnskritisk IT-infrastruktur

Ifølge Innst. S. nr. 9 (2002–2003) er det avgjørende at det utvikles robust infrastruktur i alle samfunnsviktige institusjoner. Dette følges opp i Nasjonal strategi for informasjonssikkerhet, der beskyttelse av kritisk infrastruktur er ett av fire hovedmål. Ifølge strategien er en identifisering av kritisk IT-infrastruktur en forutsetning for å gjennomføre risikovurderinger og implementere nødvendige tiltak. Undersøkelsen viser at det er igangsatt en del arbeid med å definere hva som er samfunnskritisk infrastruktur, men at myndighetene ennå ikke har en klar oversikt over hva som er kritisk IT-infrastruktur, og hvilke systemer denne består av. Gjennomgangen viser også at det fortsatt ikke er klart hva som skal defineres som skjermingsverdige objekter i henhold til sikkerhetsloven, og hva som skal gjøres for å beskytte disse.

Utvikling av kunnskap om IT-infrastrukturens sårbarhet

I Innst. S. nr. 9 (2002–2003) presiserer forsvarskomiteen og justiskomiteen at den grunnleggende kunnskapen om hva som skaper sårbarhet, bør prioriteres i sikkerhetsarbeidet. Det pågående forskningsprosjektet BAS-5 er et av de viktigste tiltakene for å framskaffe mer kunnskap om sårbarhet i nasjonalt viktige IT-systemer. Undersøkelsen viser at selv om prosjektet omtales som viktig av både departementene og fagetatene, tok det vel to år å få finansiert og startet opp prosjektet etter første omtale i forslaget til statsbudsjett høsten 2002. Ifølge Nasjonal strategi for informasjonssikkerhet skal det utarbeides sektorvise normer for å beskytte kritisk IT-infrastruktur. Gjennomgangen viser at det ikke er planlagt eller gjennomført aktiviteter på området.

Undersøkelsen viser at de fleste offentlige organer som arbeider med IT-sikkerhet, har utarbeidet veiledninger for risiko- og sårbarhetsanalyser, og det pågår mange aktiviteter for å videreutvikle metoder og verktøy. Myndighetene har imidlertid i mindre grad lagt vekt på å legge til rette for at metodene faktisk blir brukt. Det er heller ikke lagt opp til at kunnskapen fra analysene skal kunne benyttes i prioriteringen av sikkerhetstiltak uavhengig av sektor.

Systemer for å fange opp trusler

Informasjon om sikkerhetshendelser er nødvendig for å få et bilde av trusler og sårbarhet i IT-infrastrukturen, og for å gi råd i forbindelse med konkrete trusler eller assistanse ved gjenoppretting av tjenester. Varslingssystem for digital infrastruktur (VDI) og Senter for informasjonssikring (SIS) er opprettet på bakgrunn av dette.

Undersøkelsen viser at VDI har lyktes med å få tilgang til informasjon om logiske trusler via Internett. St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* peker på at VDI også skal være mest mulig åpent når det gjelder både hvem som skal kunne være deltakere og brukere, og det at informasjonen skal være mest mulig tilgjengelig. Undersøkelsen viser at systemet har et begrenset antall deltakere, og at informasjonen til allmennheten er begrenset til en kort månedlig oppsummering av registrerte hendelser.

Ifølge St.prp. nr. 1 (2001–2002) for Nærings- og handelsdepartementet skal SIS bidra til en mer robust IT-infrastruktur ved bl.a. å framskaffe et helhetlig bilde av truslene mot norske IT-systemer. Dette skal skje gjennom innrapportering av sikkerhetshendelser fra offentlige og private virksomheter. Ifølge *Mørketallsundersøkelsen* ble norske virksomheter utsatt for ca. 5200 datainnbrudd og 2,7 millioner forsøk på datainnbrudd i 2003.[3] I 2004 ble mindre enn fem sikkerhetshendelser rapportert til SIS.

Myndighetene har gjennom etableringen av VDI og SIS etablert organer som kan fange opp trusler mot IT-systemer, men disse organene har foreløpig ikke nådd vesentlige mål for sin virksomhet. I undersøkelsen stilles det derfor spørsmål ved om departementene har truffet tilstrekkelige tiltak for å sikre måloppnåelse på dette området.

3) Mørketallsundersøkelsen 2003. Om datakriminalitet og IT-sikkerhet. Økokrim, Næringslivets Sikkerhetsråd og Senter for informasjonssikring. Side 20–24

Evne til å håndtere sikkerhetshendelser
Ved behandlingen av St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* uttaler forsvarskomiteen og justiskomiteen at det er viktig å klargjøre beredskapsplaner og krisehåndteringsplaner for bl.a. IT-sikkerhet. I meldingen heter det at Justisdepartementet vil ta initiativ for å sikre at tiltak ved bortfall av IKT blir reflektert i kriseplaner. På nasjonalt plan arbeider Justis- og politidepartementet og Direktoratet for samfunnssikkerhet og beredskap (DSB) med å utvikle et nytt nasjonalt beredskapssystem. Det er ennå ikke klart i hvilken grad risikoen for alvorlig svikt i IT-systemer vil bli reflektert i dette beredskapssystemet.

Undersøkelsen viser videre at oppdaterte beredskapsplaner kun foreligger i et mindretall av virksomhetene i statlig, kommunal og privat sektor. Nasjonal strategi for informasjonssikkerhet inneholder ikke tiltak som er direkte rettet mot å fremme utviklingen av gode beredskaps- og krisehåndteringsplaner. I undersøkelsen stilles det spørsmål om manglende beredskapsplaner i virksomhetene kan være en samfunnsmessig risikofaktor.

I Innst. S. nr. 9 (2002–2003) påpeker forsvarskomiteen og justiskomiteen at det er viktig å gjennomføre øvelser for å få et ledelsesapparat som kan håndtere kriser. Komiteene uttaler videre at også saksbehandlere innen sikkerhet, beredskap og krisehåndtering bør være sidestilt med ledelsesnivået som målgruppe for øvelser. Gjennomgangen viser at øvelser initiert av DSB i stor grad har vært konsentrert om ledelsesapparatet, mens saksbehandlernivået synes å ha vært lavere prioritert. I undersøkelsen stilles det derfor spørsmål ved om øvelsesvirksomheten har vært i samsvar med forutsetningene.

OECDs retningslinjer for sikkerhet i informasjonssystemer og nettverk vektlegger betydningen av å ha systemer som kan forebygge, oppdage og reagere på sikkerhetshendelser. Mange land har derfor etablert en statsfinansiert CERT.[4] St.meld. nr. 39 (2003–2004) *Samfunnssikkerhet og sivilt-militært samarbeid* viser til at flere instanser har påpekt behovet for en slik enhet (CERT) for å sikre effektiv håndtering av kriser der flere samfunnskritiske funksjoner blir angrepet samtidig. Ifølge meldingen vil en slik enhet kunne styrke den nasjonale beredskapen mot IT-angrep gjennom å utvikle et system for koordinert respons og gjenoppretting, først og fremst innenfor virksomheter med samfunnskritiske funksjoner. Undersøkelsen tyder på at det er enighet om at en CERT bør etableres, men at det er uenighet om hvilket fagmiljø som skal ha oppgaven. Det er fortsatt ikke etablert et system som effektivt kan håndtere IT-sikkerhetshendelser. I undersøkelsen spør man om manglende systemer for koordinert respons og gjenoppretting kan få alvorlige samfunnsmessige konsekvenser ved et eventuelt angrep på kritisk infrastruktur.

4) CERT står for Computer Emergency Response Team og er en ekspertgruppe som håndterer IT-sikkerhetshendelser.

2.3 Tilrettelegging for utvikling av god sikkerhetskultur

Utvikling av en god sikkerhetskultur er fundamentet for OECDs retningslinjer for å fremme sikkerheten ved bruk av informasjonssystemer og nettverk. Departementene har lagt disse retningslinjene til grunn for sitt arbeid på området. Ett av de overordnede målene for IT-sikkerhet i Norge er å bygge opp en sikkerhetskultur, ifølge St.prp. nr. 1 (2003–2004) for Justis- og politidepartementet og Nærings- og handelsdepartementet. Nasjonal strategi for informasjonssikkerhet inneholder en rekke tiltak som skal bidra til utviklingen av en slik kultur. Tiltakene er først og fremst knyttet til utvikling av den alminnelige IT-sikkerheten. De vil påvirke sikkerheten i den IT-infrastrukturen som er kritisk for samfunnet, men tiltakene retter seg også mot bedrifter og husholdninger.

Undersøkelsen viser at det er gjennomført eller igangsatt få nye tiltak for å utvikle en god sikkerhetskultur. Internettportalen nettvett.no er etablert, men de andre planlagte tiltakene for å bevisstgjøre allmennheten om IT-sikkerhet er ikke igangsatt. Det foreligger ikke konkrete planer for gjennomføring. De private organisasjonene som inngår i undersøkelsen, vurderer ikke offentlig sektor som en drivkraft og et godt eksempel for privates arbeid med IT-sikkerhet.

Det er tidligere etablert to sertifiseringsordninger for IT-sikkerhet, begge basert på internasjonale standarder. Nasjonal strategi for informasjonssikkerhet inneholder tiltak for å fremme bruken av disse standardene og ordningene. Undersøkelsen viser at standardene fortsatt er lite kjent i næringsliv og forvaltning, og at svært få virksomheter/produkter er sertifisert.

Tilbakemeldinger fra bransjeorganisasjoner tyder på at myndighetenes arbeid med å utvikle en sikkerhetskultur hittil ikke har hatt betydning for privat sektor. I undersøkelsen stilles det derfor spørsmål ved om myndighetenes innsats har vært tilstrekkelig.

2.4 Mulige årsaker til manglende framdrift i arbeidet med IT-sikkerhet

Undersøkelsen viser at det er forskjellige årsaker til manglende framdrift i arbeidet med IT-sikkerhet og i gjennomføringen av tiltak i Nasjonal strategi for informasjonssikkerhet. Manglende avklaringer av ansvarsforhold trekkes fram som en mulig årsak, jf. punkt 2.1. I tillegg framheves følgende forhold:

Begrenset deltakelse i gjennomføringen av tiltak
I Nasjonal strategi for informasjonssikkerhet er utvalgte bransjeorganisasjoner gitt medansvar for å gjennomføre en rekke tiltak. Departementene har fram til mai 2005 ikke hatt kontakt med de utvalgte organisasjonene om gjennomføring av tiltakene. Departementene ble omorganisert i 2004. Hvorvidt Moderniseringsdepartementet eller Nærings- og handelsdepartementet skulle følge opp bruken av IT i næringslivet, ble ikke avklart før i april

2005. Også tiltakene i skole- og universitetssektoren er forsinket, og det er ikke etablert et tilstrekkelig samarbeid mellom Moderniseringsdepartementet og Utdannings- og forskningsdepartementet.

Utilstrekkelige plandokumenter
De mest berørte departementene har utarbeidet handlingsplaner for oppfølging av Nasjonal strategi for informasjonssikkerhet. Planene er imidlertid i stor grad oppsummeringer av hva som gjøres innenfor hvert departementsområde, og er på mange måter ikke mer detaljerte enn strategien. Handlingsplanene inneholder i liten grad prioritering av tiltak eller informasjon om hvordan tiltakene skal realiseres, dvs. kobling til ressursanslag og budsjetter. Verken i strategien eller i handlingsplanene er det satt opp resultatkriterier som gjør det mulig å måle effekten av de enkelte tiltakene eller av flere tiltak samlet, jf. grunnleggende styringsprinsipper i bevilgningsreglementet og i reglementet for økonomistyring i staten.

Krevende samordningsoppgaver
Organiseringen av det offentlige IT-sikkerhetsarbeidet og utformingen av den nasjonale strategien innebærer ingen plikt for den enkelte virksomhet til å gjennomføre tiltak i strategien. Med dette utgangspunktet, og med så mange virksomheter involvert i gjennomføringen av strategiens tiltak, er det en vanskelig oppgave å følge opp at strategien blir realisert på en effektiv måte. Undersøkelsen viser at Moderniseringsdepartementet, som har et koordineringsansvar for området, har få virkemidler knyttet til IT-sikkerhet og har avsatt relativt begrenset med ressurser til denne aktiviteten.

Vanskeligheter med å finansiere tverrsektorielle tiltak
Innenfor IT-sikkerhetsarbeidet er det en rekke tiltak som krever samarbeid og finansiering på tvers av etatsgrenser. Flere etater har påpekt problemer med å få finansiert tverrsektorielle IT-tiltak som mange departementer og etater ser nytten av. Undersøkelsen stiller spørsmål ved om de koordinerende departementene har lagt tilstrekkelig vekt på det økonomiske aspektet ved planleggingen av tiltak på området.

Manglende samordning av regelverk
Nasjonal strategi for informasjonssikkerhet legger vekt på at regelverket for IT-sikkerhet skal samordnes bedre. I undersøkelsen peker flere etater og bransjeorganisasjoner på forhold ved regelverket som kan gjøre samordningen av sikkerhetsarbeidet vanskelig. De peker også på at mange av de administrative problemene som gjelder ansvarsforhold, bunner i et til dels sprikende regelverk. Kompleksitet og fragmentering av regelverket blir trukket fram som et problem for næringslivet/brukerne. Undersøkelsen viser at det har tatt i overkant av halvannet år fra strategien ble framlagt, til det ble etablert et forprosjekt for å gå gjennom regelverket. Det er tidligere gjort flere forsøk på slik samordning uten at dette har hatt ønsket effekt.

2.5 Særskilt om telesikkerhet og -beredskap

I samsvar med St.meld. nr. 47 (2000–2001) *Om telesikkerhet og -beredskap i et telemarked med fri konkurranse* ble det i 2001 opprettet en enhet i Post- og teletilsynet med ansvar for telesikkerhet og -beredskap. Post- og teletilsynet fikk ansvaret for å gjennomføre eller utrede en rekke av tiltakene i meldingen. Undersøkelsen viser at et fåtall av tiltakene er gjennomført, og at de fleste tiltakene fremdeles er under utredning fire år senere. Det gjelder bl.a. følgende:

- Det er fortsatt bare én operatør (Telenor) som leverer teleberedskapstjenester.
- Det foreligger ingen ny ordning som sikrer prioriterte brukere telefonforbindelse i kritiske situasjoner der telenettene (mobilnett eller fastnett) overbelastes.
- Det er ikke gjennomført en samlet vurdering av redundans[5] i telenettene, og det er ikke planlagt eller gjennomført tiltak for økt redundans.
- Post- og teletilsynet har ikke stilt krav til operatørene om å utarbeide oversikter over hvordan viktige produksjons- og driftssystemer er koblet mot det øvrige nettverket, og det er heller ikke satt krav til beskyttelse av disse systemene.
- Post- og teletilsynet har ikke utviklet en klassifiseringsordning for teleinfrastrukturen med definerte sikkerhetskrav til de enkelte klassene.

I undersøkelsen uttaler Samferdselsdepartementet at det var behov for ytterligere konkretisering og utredning av tiltakene i St.meld. nr. 47 (2000–2001), og at dette har ført til at iverksettingen har tatt tid. Departementet peker også på at både brukere og teknologi har endret seg, noe som har ført til et behov for å revurdere innrettingen på tiltakene.

Undersøkelsen viser at Samferdselsdepartementet ikke har fulgt opp de endrede forutsetningene med nye skriftlige styringssignaler til Post- og teletilsynet. For øvrig viser gjennomgangen at det finnes få plan- og styringsdokumenter for arbeidet med tiltakene i meldingen, og at departementet ikke har formulert konkrete mål og resultatkrav overfor tilsynet i henhold til bevilgningsreglementet og økonomireglementet. Post- og teletilsynet har heller ikke utarbeidet noe samlet plandokument for sine aktiviteter.

St.meld. nr. 47 (2000–2001) understreker hvor viktig det er at de finansieringsløsningene som velges, bidrar til klare ansvarsforhold. Meldingen understreker også at Post- og teletilsynet må gi nødvendig handlekraft slik at arbeidet med telesikkerhet og -beredskap ikke blir forsinket eller målene ikke nås. Undersøkelsen viser at finansieringen av enkelttiltak gjennomgående ikke er avklart.

5) Med redundans menes omrutingsalternativer eller reserveløsninger i den enkelte operatørs nett eller mellom ulike operatørers nett.

I Innst. S. nr. 329 (2000–2001) viser samferdselskomiteen til at telenettets betydning for flere vitale samfunnsfunksjoner er stor, og at det derfor er av overordnet betydning å sikre operativitet i telenettet under alle forhold. I undersøkelsen stilles det spørsmål om hvilke konsekvenser manglende gjennomføring av tiltakene i St.meld. nr. 47 (2000–2001) har for operativiteten i telenettene.

3 Departementets kommentarer

3.1 Forsvarsdepartementet

Forsvarsdepartementet har avgitt uttalelse til Riksrevisjonens rapport i brev av 31. august 2005. Departementet framhever at det er et behov for større grad av samarbeid innen IT-sikkerhet, og ser det som positivt at det blir fokusert på uavklarte ansvarsområder innen organiseringen av dette arbeidet.

Departementet mener det er viktig å fokusere på behovet for å ha planer for å håndtere eventuelle kriser, og peker på at det ikke er grunn til å tro at man kan håndtere en større krise bra uten å ha forberedt seg på dette. Planverket må regelmessig testes og evalueres blant annet ved hjelp av øvelser.

Når det gjelder myndighetenes arbeid med å etablere systemer som kan gi et bilde av truslene mot IT-infrastrukturen, viser departementet til at Nasjonal sikkerhetsmyndighet har som strategisk mål å utvikle det offentlig-private samarbeidet om sikkerhetstiltak. Videreutvikling av Varslingssystem for digital infrastruktur (VDI) er sentralt for både nye deltakere og etablerte brukere av informasjonen. Utviklingen av VDI påvirkes av og må etter departementets syn ses i sammenheng med en ansvarsplassering av CERT.

3.2 Justis- og politidepartementet

Justis- og politidepartementet har i brev til Riksrevisjonen av 5. september 2005 avgitt uttalelse til rapporten.

Når det gjelder omtalen av organiseringen av IT-sikkerhetsarbeidet, mener departementet at selv om Riksrevisjonen legger ansvars-, nærhets- og likhetsprinsippet til grunn som revisjonskriterier, kommer ikke disse prinsippene like godt fram i rapportens vurderinger. Departementet understreker at IT-sikkerhet er et virksomhetsansvar, og at hvert departement dermed er ansvarlig for at IT-sikkerheten ivaretas i departementet, i underliggende virksomheter og innenfor egen sektor. Det departementet som ordinært har ansvaret for et fagområde, har også ansvaret for en nødvendig beredskapsplanlegging og eventuell iverksettelse av tiltak i en krisesituasjon.

Justis- og politidepartementet peker videre på at det også er slik at ansvaret for ”kritisk infrastruktur” følger ansvarsprinsippet og ikke er skilt ut som et eget fagområde. Selv om det ikke foreligger en omforent norsk definisjon av begrepet ”kritisk infrastruktur”, mener Justis- og politidepartementet at det har ansvar for virksomheter som har en avgjørende rolle ved håndteringen av ulykker, kriser og katastrofer.

Departementet peker videre på at dets samordningsansvar for samfunnets sivile sikkerhet er tydeliggjort og styrket, blant annet gjennom etableringen av Direktoratet for samfunnssikkerhet og beredskap og ved at Nasjonal sikkerhetsmyndighet har fått en faglig rapporteringslinje i sivil sektor til Justis- og politidepartementet.

Departementets særskilte samordningsfunksjon innebærer et ansvar for å utarbeide overordnede retningslinjer, koordinere og fremme proposisjoner og meldinger til Stortinget, tilrettelegge rammebetingelser, ta initiativ, være pådriver, avklare ansvarsforhold i gråsoner og treffe prinsipielle avgjørelser på samfunnssikkerhets- og beredskapsområdet

Justis- og politidepartementet viser til at det også skal føre tilsyn med at departementene gjennomfører internkontroll på sikkerhets- og beredskapsområdet. Formålet er å gi en systematisk metode for fagdepartementenes eget arbeid med beredskap, og å sikre en samordnet og effektiv bruk av ressursene innenfor beredskapsplanlegging.

Departementet påpeker videre at hver virksomhet, etat og departement er ansvarlig for å gjennomføre og finansiere øvelser innenfor eget fag- og ansvarsområde. Direktoratet for samfunnssikkerhet og beredskap har som hovedoppgave å bistå sentrale og statlige myndigheter slik at disse får øvet sine beredskapsplaner og krisehåndteringssystemer. Direktoratet har utviklet en rammeplan for sivile nasjonale beredskapsøvelser i perioden 2005–2008. Departementet viser til at det nasjonale beredskapssystemet er under kontinuerlig vurdering, og at systemet søker å ta høyde for flest mulig av de utfordringene samfunnet kan bli stilt overfor.

Departementet viser til at tiltakene i Nasjonal strategi for informasjonssikkerhet må gjennomføres og finansieres innenfor de til enhver tid gjeldende budsjettrammene for hver enkelt offentlig virksomhet. Dette innebærer at virksomhetene planlegger, prioriterer og om nødvendig samordner tiltakene i forbindelse med utarbeidelsen og disponeringen av sine årlige budsjetter. Dette er ifølge departementet også gjort, bl.a. ved iverksettingen av forskningsprosjektet BAS 5. Ved iverksettelse av tverrsektorielle tiltak legges tverrsektoriell finansiering til grunn, i tråd med ansvarsprinsippet. Justisdepartementets rolle kan være å ta initiativ til dette, uten nødvendigvis å bære noe finansielt ansvar. På denne måten unngår man uenighet mellom fagdepartementene om prioritering og innretting av tiltak.

3.3 Moderniseringsdepartementet

Moderniseringsdepartementet har i brev av 5. september 2005 til Riksrevisjonen avgitt uttalelse til rapporten.

Departementet uttaler at det høsten 2005 vil nedsette og lede en interdepartemental arbeidsgruppe for å klargjøre berørte departementers koordinerings- og sektoransvar i forbindelse med IT-sikkerhet. Moderniseringsdepartementet understreker videre at Samferdselsdepartementets sektoransvar ikke innebærer at Samferdselsdepartementet har et ansvar for helheten innenfor IT-sikkerhet, selv om Internett som kommunikasjonsmedium favner bredt. Moderniseringsdepartementet understreker at IT-sikkerhet er definert som noe langt mer enn sikring av nettverk, driftssystemer for nettverk og kommunikasjonstjenester.

Departementet viser til at undersøkelsen gjør et poeng av at Senter for informasjonssikring (SIS) har mottatt relativt få rapporter om sikkerhetshendelser. Moderniseringsdepartementet understreker at SIS har vært et pilotprosjekt. Erfaringene med innhenting av sårbarhetsinformasjon har vist at behovet for, eller betydningen av, direkte innrapporteringer fra brukerne har vært mindre enn forutsatt. Departementet viser videre til at regjeringen 18. august 2005 besluttet at SIS skal etableres på permanent basis i Gjøvik, og inngå i et helhetlig nasjonalt konsept for varsling og rådgivning for informasjonssikkerhet.

Moderniseringsdepartementet viser videre til at regjeringen 29. august 2005 vedtok å etablere et permanent nasjonalt koordinerende CERT (Computer Emergency Response Team). CERT skal legges til Varslingssystem for digital infrastruktur (VDI) hos Nasjonal sikkerhetsmyndighet (NSM), og skal ivareta varsling, rådgivning, assistanse og analyse for kritisk infrastruktur/samfunnsviktige funksjoner. Departementet framhever at det er naturlig at NSMs CERT i denne sammenheng opptrer som kontaktpunkt nasjonalt og internasjonalt. Departementet presiserer også at Varslingssystem for digital infrastruktur er innrettet mot kritisk infrastruktur/samfunnsviktige funksjoner. VDI-tjenestene er følgelig ikke ment å skulle betjene allmennheten eller øvrige deler av samfunnet.

Departementet mener for øvrig at tiltak i Nasjonal strategi for informasjonssikkerhet der Moderniseringsdepartementet har et gjennomføringsansvar, har fått relativt stor plass i rapporten. Departementet uttaler videre at endringene i departementstrukturen høsten 2004 medførte at framdriften for en del av tiltakene mot næringslivet ble forsinket. Moderniseringsdepartementet viser til at det 22. mai 2005 ble avholdt et møte med IKT Norge, Abelia, NHO, Næringslivets sikkerhetsråd og eForum for å drøfte implementering av tiltak og samarbeidsformer. Møtet konkluderte med at det ikke skal opprettes nye samarbeidsfora, men at eksisterende møteplasser skal benyttes. Videre forutsettes samarbeidsformen mellom de offentlige og private aktører å variere fra sak til sak. Møtet konkluderte også med at næringslivsorganisasjonene fortløpende vil vurdere behov, prioritet og omfang av tiltak i strategien som det er forutsatt at næringslivet skal ta initiativ til.

Departementet viser til at innføring av elektronisk signatur/PKI er et svært viktig tiltak for å styrke IT-sikkerheten i forvaltningen og samfunnet som helhet. Tiltaket har følgelig fått høy prioritet i Moderniseringsdepartementet. Arbeidet har ifølge departementet ikke gått på bekostning av det generelle IT-sikkerhetsarbeidet, men ressurssituasjonen medfører at implementeringen av strategitiltak med lavere prioritet har blitt forskjøvet i tid.

3.4 Samferdselsdepartementet

Samferdselsdepartementet har i brev av 5. september 2005 til Riksrevisjonen avgitt uttalelse til rapporten. Departementet har gitt kommentarer til undersøkelsens kapittel om telesikkerhet og -beredskap.

Samferdselsdepartementet viser til at det nye konseptet for levering av teleberedskapstjenester per i dag omfatter alle tilbydere av elektroniske kommunikasjonsnett og -tjenester, og spesielt tilbydere som har kunder med samfunnskritiske funksjoner. Departementet uttaler videre at Post- og teletilsynet kun har inngått avtale med én tilbyder som kompenseres for tiltak.

Departementet kommenterer framdriften og finansieringen av ordningen som skal sikre prioriterte brukere telefonforbindelse i kritiske situasjoner der telenettene overbelastes. Departementet uttaler at ordningen kan iverksettes når den tekniske løsningen er på plass og Direktoratet for samfunnssikkerhet og beredskap har kommet fram til en hensiktsmessig måte å administrere ordningen på. Departementet uttaler videre at finansieringsmåte vil bli avgjort i den forbindelse.

Når det gjelder arbeidet for økt redundans i telenettene, uttaler departementet at redundansen har blitt bedre i de senere år på grunnlag av tilbydernes egne kommersielle interesser. Post- og teletilsynet har derfor så langt ikke sett det nødvendig å gi noe pålegg overfor tilbyderne.

Departementet viser videre til at Post- og teletilsynet har lagt til rette for å tilby samlokalisering i fjellanlegg. Som følge av den teknologiske utviklingen og dagens trusselbilde anser departementet ikke samlokalisering i fjellanlegg som så viktig som det var på 90-tallet. Departementet påpeker at det allerede i St.meld. nr. 47 (2000–2001) ble stilt spørsmål ved hvor mye ressurser det vil være riktig å bruke på beskyttelse mot fysiske trusler.

Samferdselsdepartementet peker på at det faktisk pågår arbeid med:

- å kunne stille krav til operatørene om at de utarbeider en oversikt over hvordan viktige produksjons- og driftssystemer er koblet mot det øvrige nettverket
- å utvikle en klassifiseringsordning for teleinfrastrukturen
- å gjennomføre en sikkerhetsevaluering av teleinfrastrukturen i samarbeid med teleoperatørene

I tillegg viser departementet til at Post- og teletilsynet har igangsatt aktiviteter for å overvåke utviklingen i bruken av Internett.

Når det gjelder Samferdselsdepartementets oppfølging av Post- og teletilsynet, peker departementet på at tildelingsbrevet spesifikt viser til tilsynets oppgaver innenfor samferdselsberedskap. I tråd med styringssystemet for Post- og teletilsynet har endrede forutsetninger og framdrift på tiltakene vært diskutert på hvert kvartalsmøte i perioden 2002–2004. Departementet har etterspurt utredninger på enkelte tiltak som for eksempel nasjonal autonomi, og Post- og teletilsynet har fulgt opp dette. Et statusmøte der alle de viktigste tiltakene i meldingen ble diskutert, ble gjennomført i januar 2005. Departementet viser til at Post- og teletilsynet har rapportert skriftlig og muntlig på etats- og virksomhetsmøtene for beredskap to ganger årlig. I tillegg har tilsynet rapportert på de ordinære tertialmøtene mellom departementet og tilsynet.

Departementet uttaler at hovedutfordringen for framdrift i tiltakene ikke har vært mangel på finansieringsløsninger som påpekt i undersøkelsen, men tekniske og kapasitetsmessige utfordringer hos Post- og teletilsynet og tilbyderne av nett og tjenester.

Samferdselsdepartementet kommenterer spørsmålet om hvorvidt operativiteten i telenettene er tilstrekkelig sikret. Departementet peker på at ekomlovens § 2–10 setter krav til at tilbydere skal sikre nett og tjenester slik at brukeren, selv i de situasjoner der nettet utsettes for ekstraordinære påkjenninger, så langt som mulig skal kunne benytte grunnleggende elektroniske kommunikasjonstjenester. Ifølge departementet har fast- og mobilnettene i Norge meget høy tilgjengelighet og meget god kapasitet. En utbedring for å oppnå enda bedre tilgjengelighet når det gjelder både fastnett og mobilnett, er kostnadskrevende. Ut fra den informasjonen og erfaringen Post- og teletilsynet sitter med, mener departementet at sikkerheten i norske kommunikasjonsnett er god.

4 Riksrevisjonens bemerkninger

Formålet med undersøkelsen har vært å vurdere om myndighetenes arbeid med IT-sikkerhet i samfunnet er i samsvar med Stortingets vedtak og forutsetninger. Undersøkelsen omfatter både tiltak for bedre IT-sikkerhet og tiltak for bedre telesikkerhet.

4.1 Organiseringen av forvaltningens arbeid med IT-sikkerhet

Riksrevisjonen er innforstått med at ansvaret for IT-sikkerhet er et virksomhetsansvar. Undersøkelsen viser imidlertid at det er mange fagorganer som har ulike oppgaver innenfor IT-sikkerhet. I undersøkelsen gir flere fagorganer uttrykk for at avklaringer av ansvar har manglet, at ansvar og oppgaver er fragmentert, og at begrensede ressurser brukes til overlappende oppgaver. Private organisasjoner som er gitt oppfølgingsansvar i Nasjonal strategi for informasjonssikkerhet, mener det er vanskelig å finne ut hvilket organ som har ansvar for ulike forhold innen IT-sikkerhet. Forsvarsdepartementet framhever i sine kommentarer behovet for større grad av samarbeid på dette området, og ser det som positivt at det blir fokusert på uavklarte ansvarsområder.

I St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* og Innst. S. nr. 9 (2002–2003) påpekes betydningen av koordinering og ansvarsklargjøring innenfor IT-sikkerhetsarbeidet. Riksrevisjonen har merket seg at Moderniseringsdepartementet høsten 2005 vil nedsette en interdepartemental arbeidsgruppe for å klargjøre berørte departementers koordinerings- og sektoransvar. En slik klargjøring på departementsnivå og underordnet nivå anses som avgjørende for det videre arbeidet med IT-sikkerheten.

4.2 Samfunnskritisk IT-infrastruktur

Avgrensning av hva som er samfunnskritisk IT-infrastruktur

I Nasjonal strategi for informasjonssikkerhet understrekes det at identifisering og klassifisering av kritiske IT-systemer er en forutsetning for å gjennomføre risikovurderinger og implementere nødvendige sikkerhetstiltak. Undersøkelsen viser at departementene ikke har en klar oversikt over hva som er kritisk IT-infrastruktur, og hvilke systemer denne består av. Det er imidlertid påbegynt et arbeid med å definere hva som er samfunnskritisk infrastruktur, bl.a. gjennom forskningsprosjektet BAS 5. Riksrevisjonen er innforstått med at hvert enkelt departement har ansvar for sikkerheten på sitt ansvarsområde. Avhengighet mellom sektorer kan imidlertid bety at vurderinger av sikkerheten i den enkelte sektor ikke nødvendigvis gir et korrekt bilde av sikkerhetstilstanden for samfunnet som helhet. Riksrevisjonen vil derfor understreke betydningen av erfaringsutveksling og koordinering mellom sektorene på dette området. Det må klargjøres hvilken myndighet som har ansvar for å framskaffe oversikter over IT-sikkerhetstilstanden på tvers av sektorgrensene.

Undersøkelsen viser at det ikke er klart hva som skal defineres som skjermingsverdige objekter i henhold til sikkerhetsloven, og hva som skal gjøres for å beskytte disse. Forsvarsdepartementet har fortsatt ikke utarbeidet forskrift om skjermingsverdige objekter over sju år etter at loven ble vedtatt. Manglende beskyttelse av samfunnsviktige systemer vil etter Riksrevisjonens mening kunne føre til alvorlige problemer ved en eventuell krise.

Systemer for å fange opp trusler
Senter for informasjonssikring (SIS) ble etablert i Trondheim i 2002 som et prøveprosjekt bl.a. for å framskaffe en oversikt over trusler mot IT-systemer i Norge, og for å gi råd knyttet til dette. Trusselbildet skulle kartlegges gjennom innrapportering av hendelser til senteret fra private og offentlige virksomheter. Undersøkelsen påviser at mindre enn fem hendelser ble rapportert til senteret i 2004, og at senteret er lite kjent i målgruppene for senterets tjenester. Riksrevisjonen har merket seg at regjeringen nå har vedtatt å etablere senteret på permanent basis på Gjøvik fra 1. januar 2006. Videre har Riksrevisjonen merket seg Moderniseringsdepartementets kommentar om at direkte innrapporteringer fra brukerne har hatt mindre betydning enn forutsatt, og ser at oppgavene for et permanent SIS vil bli noe endret i forhold til prøveprosjektet. Riksrevisjonen forutsetter at departementet avklarer SIS' ansvar og oppgaver mot andre relevante fagorganer når senteret etableres på permanent basis, og at det iverksettes tiltak for å sikre at senteret blir bedre kjent for målgruppene.

Riksrevisjonen har merket seg at regjeringen 29. august 2005 vedtok å etablere et permanent nasjonalt koordinerende Computer Emergency Response Team (CERT). Riksrevisjonen ser positivt på at det etableres løsninger som kan avhjelpe mangler i systemer for håndtering av alvorlige angrep mot samfunnsviktig IT-infrastruktur. Riksrevisjonen legger til grunn at det må avklares hvilken rolle CERT skal ha, og hvilket forhold det skal ha til andre organer. Riksrevisjonen viser i denne forbindelse til St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet*, der det pekes på at Varslingssystem for digital infrastruktur (VDI) skal være mest mulig åpent både når det gjelder hvem som skal kunne være deltakere og brukere, og når det gjelder det at informasjonen skal være mest mulig tilgjengelig. Undersøkelsen viser at VDI hittil i liten grad har nådd disse målene.

Evne til å håndtere sikkerhetshendelser
Ifølge St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* skal Justis- og politidepartementet ta initiativ til å sikre at tiltak ved bortfall av IKT blir reflektert i kriseplaner. Undersøkelsen viser at det ennå ikke er klart i hvilken grad risikoen for alvorlig svikt i IT-systemer vil bli reflektert i et nytt nasjonalt beredskapssystem. Riksrevisjonen registrerer at departementet uttaler at beredskapssystemet kontinuerlig er under vurdering, og at departementet søker å ta høyde for flest mulig av de utfordringene samfunnet kan bli stilt overfor.

Undersøkelsen viser videre at oppdaterte beredskapsplaner for IT-systemer bare foreligger i et mindre antall virksomheter i statlig, kommunal og privat sektor. Nasjonal strategi for informasjonssikkerhet inneholder ikke tiltak som er direkte rettet mot å fremme utviklingen av gode beredskaps- og krisehåndteringsplaner i virksomhetene. Riksrevisjonen stiller spørsmål ved om manglende beredskapsplaner i virksomhetene kan innebære en risiko for mangelfull beredskap for samfunnet som helhet, og i hvilken grad forvaltningen har planer om å iverksette konkrete tiltak på området.

4.3 Tilrettelegging for utvikling av god sikkerhetskultur

Et viktig mål for Nasjonal strategi for informasjonssikkerhet er å bygge en sikkerhetskultur rundt bruk og utvikling av IT-systemer. Undersøkelsen viser at det er gjennomført eller igangsatt få nye tiltak for å fremme en slik kultur. OECD peker på at offentlig sektor på grunn av sitt omfattende engasjement har et spesielt ansvar for å gå foran som et godt eksempel og en mønsterbruker. Undersøkelsen viser at de private organisasjonene som inngår i undersøkelsen, ikke ser offentlig sektor som en drivkraft på området.

Utvalgte bransjeorganisasjoner er gitt medansvar for å gjennomføre en rekke tiltak i Nasjonal strategi for informasjonssikkerhet, som ble framlagt i juni 2003. Moderniseringsdepartementet uttaler i sitt svar at endringene i departementsstrukturen sommeren 2004 medførte at framdriften for en del av tiltakene mot næringslivet ble forsinket. I mai 2005 avholdt Moderniseringsdepartementet et møte med aktuelle organisasjoner om gjennomføringen av tiltakene. Riksrevisjonen har merket seg konklusjonen fra dette møtet om at næringslivsorganisasjonene fortløpende vil vurdere behov, prioritet og omfang av de tiltakene i strategien som det er forutsatt at næringslivet skal ta initiativ til. Riksrevisjonen understreker betydningen av at departementene sikrer nødvendig oppfølging slik at tiltakene blir gjennomført.

Stortinget ba allerede i B.innst. S. nr. 1 (1996–1997) regjeringen om å legge fram forslag om etablering av en sertifiseringsordning for IT-sikkerhet. Det er senere etablert to ordninger basert på internasjonale standarder: én for sertifisering av produkter og én for sertifisering av organisasjoner. Undersøkelsen viser at standardene er lite kjent i næringsliv og forvaltning, og at ti organisasjoner og to produkter er sertifisert. Departementene har ikke kommentert dette forholdet. Riksrevisjonen stiller spørsmål ved om det bør iverksettes ytterligere tiltak for å fremme bruken av standardene og sertifiseringsordningene.

4.4 Særskilt om telesikkerhet og -beredskap

St.meld. nr. 47 (2000–2001) inneholder en rekke konkrete tiltak for å utvikle en tilfredsstillende sikkerhet i telenettene og gi en beredskap som kan håndtere eventuelle kriser innen telesektoren. Undersøkelsen viser at bare et fåtall av tiltakene i meldingen faktisk er gjennomført. Det er videre ikke satt tidsfrister for gjennomføring av de øvrige tiltakene. Ifølge meldingen skulle bl.a. nye prioritetsordninger som sikrer viktige brukere telefonforbindelse i kritiske situasjoner, innføres raskt både i faste nett og i mobilnett. Ordningene er ikke innført. Riksrevisjonen har merket seg at finansieringen av den planlagte nye prioritetsordningen i mobilnett først vil bli avgjort når en teknisk løsning og administrative prosedyrer foreligger.

Samferdselskomiteen har i Innst. S. nr. 329 (2000–2001) pekt på at telenettet har stor betydning for flere vitale samfunnsfunksjoner, og at det er av overordnet betydning å sikre nettet under alle forhold. På denne bakgrunn vil Riksrevisjonen understreke betydningen av at tiltakene i St.meld. nr. 47 (2000–2001) gjennomføres. Riksrevisjonen stiller i den forbindelse spørsmål om Samferdselsdepartementet bør utvikle en samlet plan for prioritering og iverksetting av tiltakene, med klare resultatkrav til Post- og teletilsynet.

4.5 Årsaker til manglende framdrift i arbeidet med IT-sikkerhet

I undersøkelsen pekes det på mulige årsaker til manglende framdrift i arbeidet med IT-sikkerhet og manglende gjennomføring av tiltak i Nasjonal strategi for informasjonssikkerhet. Undersøkelsen viser bl.a. at departementenes handlingsplaner for oppfølging av Nasjonal strategi for informasjonssikkerhet i liten grad inneholder prioritering av tiltak og informasjon om når og hvordan tiltakene skal realiseres. Departementene har heller ikke satt opp resultatkrav som gjør det mulig å vurdere resultatene av tiltakene. Undersøkelsen viser at Moderniseringsdepartementet, som har et koordineringsansvar for området og strategien, har få virkemidler knyttet til oppfølging av strategien.

Undersøkelsen viser også at uklare ansvarsforhold er årsak til lav framdrift i arbeidet. Behovet for ansvarsavklaringer ble tatt opp ved behandlingen av St.meld. nr. 39 (2003–2004) *Samfunnssikkerhet og sivilt-militært samarbeid*, jf. Innst. S. nr. 49 (2004–2005), der forsvarskomiteens flertall uttaler at meldingen ”ikke på en tilstrekkelig måte tar inn over seg at det offentlige Norges vern mot IT-angrep synes for lite koordinert. Flertallet mener at ansvaret for det offentliges IT-sikkerhet synes for dårlig, og at dette sakskomplekset lider under det faktum at for mange aktører er tildelt ansvar. Dette gjelder ikke bare på underordnet nivå, men det kan også synes som om det på departementalt nivå er for mange som har en rolle i utformingen av den statlige IT-sikkerheten.”

Riksrevisjonen vil på denne bakgrunn understreke betydningen av at det legges til rette for økt samordning og bedre styring av arbeidet med å sikre IT-infrastrukturen i Norge.

5 Departementets svar

5.1 Forsvarsdepartementet

Saken har vært forelagt Forsvarsdepartementet, og statsråden har i brev av 3. november 2005 svart:

"Det vises til Riksrevisjonens brev av 28. september 2005 om ovennevnte, vedlagt dokument til Stortinget til uttalelse.

I sin undersøkelse tar Riksrevisjonen opp at forvaltningens ansvar for IKT-sikkerhet er fragmentert, og at fagorganene på området har overlappende oppgaver. Forsvarsdepartementet støtter behovet for nærmere samarbeid og klargjøring av ansvarsområder. Departementet vil i den forbindelse vise til at det er nedsatt en interdepartemental arbeidsgruppe, som skal presisere og tydeliggjøre oppgaver innen IKT-sikkerhet. Arbeidsgruppen skal rapportere til Moderniseringsdepartementet innen 1. mars 2006.

Riksrevisjonen bemerker for øvrig, jf. kapittel 4.2, at Forsvarsdepartementet fortsatt ikke har utarbeidet forskrift om skjermingsverdige objekter over sju år etter at sikkerhetsloven ble vedtatt. Manglende beskyttelse av samfunnsviktige systemer vil, etter Riksrevisjonenes mening, kunne føre til alvorlige problemer ved en eventuell krise.

Sikkerhetsloven ble vedtatt i 1998 og satt i kraft 1. juli 2001. En interdepartemental arbeidsgruppe som skulle utarbeide et forslag til forskrifter om objektsikkerhet til loven, avgav sin rapport i mai 2002. Det ble anbefalt at sikkerhetsloven burde endres, slik at de mest sentrale bestemmelsene i forskriftsforslaget skulle gis i lovs form. Etter en høring ble det, i august 2004, opprettet en arbeidsgruppe mellom sentrale departementer og etater for å følge opp saken. Arbeidet er stilt i bero i påvente av resultatene fra det utvalget som ble nedsatt i oktober 2004 for sikring av landets kritiske infrastruktur (Infrastrukturutvalget). En rapport fra utvalget forventes å foreligge i januar 2006.

Forsvarsdepartementet vil for øvrig presisere at dagens sektorlovgivning på området fastsetter nærmere krav til beskyttelse av skjermingsverdige objekter. Sikkerhetsloven inneholder, på sin side, sektorovergripende bestemmelser om sikring av eiendom som har betydning for rikets selvstendighet og sikkerhet og vitale nasjonale sikkerhetsinteresser (skjermingsverdige objekter). Loven er imidlertid subsidiær i forhold til sektorlovgivningen. Reguleringen er dessuten meget knapp i loven, og må derfor utfylles med forskrifter. Konsekvensen av manglende forskrifter er en mangelfull helhetlig tilnærming til forebyggende tiltak på området, noe som ikke direkte berører håndteringen av eventuelle kriser."

5.2 Justis- og politidepartementet

Saken har vært forelagt Justis- og politidepartementet, og statsråden har i brev av 20. oktober 2005 svart:

"Jeg viser til brev mottatt 29.09.2005, der Riksrevisjonen oversender "Riksrevisjonens dokument til Stortinget," basert på ovennevnte sak, hvor det bes om Justisdepartementets uttalelse til Riksrevisjonens bemerkninger i dokumentet. Dokumentet til Stortinget er basert på et utkast til rapport som ble oversendt aktuelle departementer til uttalelse i juli, samt på departementenes kommentarer til rapportutkastet. Jeg ser at departementets tidligere kommentarer er gjengitt i dokumentet

til Stortinget, og ser det derfor ikke som nødvendig å kommentere disse forholdene på nytt.

Jeg ønsker likevel å kommentere to forhold i rapporten. Det første forholdet er skjermingsverdige objekter (andre avsnitt under 4.2,) der Riksrevisjonen påpeker at det fortsatt ikke er utarbeidet en forskrift om skjermingsverdige objekter. Justisdepartementet har tidligere gjort Forsvarsdepartementet kjent med at vi vil avvente en eventuell endring av sikkerhetsloven og utarbeidelse av nye forskrifter om objektsikkerhet til Infrastrukturutvalget har avgitt sin rapport.

Videre ønsker jeg å kommentere en setning på side 5 i dokumentet: "Justis- og politidepartementet har et samordnings- og tilsynsansvar for samfunnets sivile sikkerhet og for beredskap i kritisk infrastruktur." Denne setningen stammer fra hovedrapportens setning på side 22: "Departementet har et samordnings- og tilsynsansvar for samfunnets (sivile) sikkerhet med utgangspunkt i kgl.res. 16. september 1994 og 4. juli 2003. Dette samordningsansvaret gjelder ifølge departementet også for beredskap i kritisk infrastruktur." Dette er ifølge Riksrevisjonen sagt i et intervju med Justisdepartementet i mars 2005. Det Justisdepartementets representanter mente i intervjuet var at samordningsansvaret gjelder uansett, og at kritisk infrastruktur ikke er unntatt dette samordningsansvaret. Samordningsansvaret gjelder derimot ikke spesielt for kritisk infrastruktur, og det var derfor ikke meningen å fremheve kritisk infrastruktur spesielt. Justisdepartementet er oppatt av at også ansvar for kritisk infrastruktur skal følge ansvarsprinsippet. Slik setningen står i Riksrevisjonens dokument til Stortinget kan det synes som om Justisdepartementet har et spesielt ansvar for kritisk infrastruktur, noe som ikke er presist."

5.3 Moderniseringsdepartementet

Saken har vært forelagt Moderniseringsdepartementet, og statsråden har i brev av 24. oktober 2005 svart:

"Eg viser til Riksrevisjonens brev m/vedlegg av 28.09.05 gjeldande ovanfor nemnte sak.

1. Organisering av forvaltninga sitt arbeid med IT-sikring
Som eit resultat av aukande samankopling, er informasjonssystem og nettverk i dag utsett for stadig fleire ulike truslar og sårbarheits faktorar. Dette reiser nye spørsmål omkring sikring, og korleis ansvarsforholda i landet på dette området er organisert. Kompleksiteten fordrar ein god nasjonal koordinering av ressursane på dette området. Eg er difor glad for at Riksrevisjonen no har føretatt ein forvaltningsrevisjon av dette fagområdet.

Moderniseringsdepartementet har i oktober 2005 nedsett – og leier – ein interdepartemental arbeidsgruppe for å gjennomgå noverande ansvarsområde for å få presisert gjeldande ansvarsforhold – både sektoransvar og ulike former for samordningsansvar. Arbeidsgruppa skal også identifisere problem knytte til noverande eller uavklara ansvarsforhold, blant anna budsjettmessige utfordringar. Arbeidsgruppa har også fått mandat til å foreslå eventuelle endringar i ansvarsfordelinga. Arbeidsgruppa skal levere rapport til Moderniseringsdepartementet innan 01.03.06. Eg vil ganske snart vurdere om arbeidsgruppa sitt mandat og samansetning tek vare på mine ambisjonar om å klargjere ansvaret for IT-sikring som er ein del av samfunnets beredskapssystem.

2. Samfunnskritisk IT-infrastruktur
I føreliggande St.prp. nr 1 (2005–2006) ligg det inne eit forslag om å styrke den operative IT-sikringa ved å etablera ein eigen eining – CERT (Computer Emergency Response Team), ved Nasjonal sikkerhetsmyndighet. Eininga skal handtere alvorlege dataangrep retta mot kritisk infrastruktur på nasjonalt plan. Den nasjonale CERT skal integrerast mot det eksisterande VDI (Varslingssystem for digital infrastruktur). Den nasjonale CERT/VDI vil bli pålagt å samvirke og utveksle informasjon med tilstøytande verksemder i IT-sikringsfeltet som til dømes Post- og teletilsynet, Senter for informasjonssikring (SIS) m.v.

CERT/VDI skal saman med SIS utgjere eit heilskapleg konsept for nasjonal varsling og rådgjeving for informasjonssikring. SIS – som skal etablerast på permanent basis i tilknyting til Gjøvik Kunnskapspark AS – vil i følgje dette konseptet få ansvar for kompetanseutvikling og informasjonsutveksling av førebyggjande art. SIS sin målgruppe vil primært vere små og mellomstore verksemder i privat og offentlig sektor, inkludert kommunane."

5.4 Samferdselsdepartementet

Saken har vært forelagt Samferdselsdepartementet, og statsråden har i brev av 28. oktober 2005 svart:

"Vi viser til Riksrevisjonens brev av 28. september 2005 om ovennevnte. Samferdselsdepartementet viser til sine kommentarer i brev av 5. september 2005 og har ingen ytterligere kommentarer til Riksrevisjonens rapport."

6 Riksrevisjonens uttalelse

Riksrevisjonens undersøkelse viser at myndighetenes arbeid med IT-sikkerhet preges av mange aktører og uklare ansvarsforhold. Riksrevisjonen vil understreke betydningen av at berørte departementer i større grad samordner dette arbeidet. Riksrevisjonen har merket seg at Moderniseringsdepartementet i oktober 2005 nedsatte en interdepartemental arbeidsgruppe som skal vurdere ansvarsforholdene nærmere.

Samfunnskritisk IT-infrastruktur er preget av sterk gjensidig avhengighet mellom systemer og mellom sektorer. Infrastrukturen blir også utsatt for stadig flere trusler. Etter Riksrevisjonens vurdering er det nå viktig å klargjøre hvilken myndighet som har ansvar for å framskaffe oversikter over sårbarheten i kritisk infrastruktur på

tvers av sektorgrensene og for samordning av sårbarhetsreduserende tiltak.

Riksrevisjonen har merket seg at det skal etableres et helhetlig konsept for nasjonal varsling og rådgivning om IT-sikkerhet basert på opprettelsen av et nasjonalt CERT (Computer Emergency Response Team) og reetablering av Senter for informasjonssikring. Riksrevisjonen vil understreke behovet for klare ansvarsgrenser og gode samarbeidsformer mellom CERT, Senter for informasjonssikring og andre offentlige organer som arbeider med IT-sikkerhet. Riksrevisjonen vil også påpeke betydningen av at håndtering av alvorlig svikt i IT-systemer blir reflektert i beredskapsplaner på forskjellige nivåer, herunder i nytt nasjonalt beredskapssystem.

St. meld. nr. 47 (2000–2001) om telesikkerhet og -beredskap ble lagt fram i mai 2001. Stortingsmeldingen inneholder en rekke tiltak som skal bidra til en tilfredsstillende telesikkerhet. Riksrevisjonen konstaterer at det fortsatt ikke er utarbeidet en samlet plan for prioritering og iverksetting av nødvendige tiltak for å oppnå et tilfredsstillende sikkerhetsnivå på dette området.

Riksrevisjonens undersøkelse viser videre at departementenes handlingsplaner for oppfølging av Nasjonal strategi for informasjonssikkerhet i liten grad inneholder prioritering av tiltak eller angir når og hvordan tiltak skal realiseres. Det er ikke satt resultatkrav som gjør det mulig å vurdere effekten av tiltakene. Undersøkelsen viser også at ansvaret for IT-sikkerheten synes for dårlig koordinert og lider under mangel på helhetlig styring og oppfølging. Riksrevisjonen vil understreke betydningen av at det offentliges vern mot IT-angrep gis høyeste prioritet og at det legges vekt på en koordinert, helhetlig styring og oppfølging av arbeidet med IT-sikkerhet.

Saken sendes Stortinget.

Vedtatt i Riksrevisjonens møte 15. november 2005

Bjarne Mørk-Eidem **Annelise Høegh**

Jan L. Stub **Nils Totland** **Helga Haugen**

Erik Larsen Kvakkestad

Rapport: Myndighetenes arbeid med å sikre IT-infrastruktur

Vedlegg til Dokument nr. 3:4 (2005–2006)

Innhold

1 Innledning

1.1 Bakgrunn

Samfunnets avhengighet av informasjons- og kommunikasjonssystemer og sårbarheten i disse systemene har opptatt norske myndigheter i flere år. Allerede i 1986 konkluderte et utvalg med at det trengtes betydelige ressurser for å gjøre samfunnsviktig databehandling mindre sårbar og redusere konsekvensene av forstyrrelser.[1] Sårbarhetsutvalgets rapport fra juli 2000 slår fast at bruk av informasjons- og kommunikasjonsteknologi har bidratt til å øke effektiviteten i både offentlig og privat sektor de siste tiårene. Samtidig har samfunnet blitt avhengig av IT-systemene, og det har dermed også blitt sårbart for svikt i disse. Sårbarhetsutvalget peker i sin rapport på at IT-systemer har blitt en av samfunnets bærebjelker.[2]

Sårbarhetsutvalgets arbeid var en viktig premiss for arbeidet med St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet. Veien til et mindre sårbart samfunn.* Meldingen gir en oversikt over tiltak som gjennomføres for å gjøre det norske samfunnet mindre sårbart, og gir retning for det videre arbeidet. En del av tiltakene i meldingen er sårbarhetsreduserende tiltak innenfor informasjons- og kommunikasjonsteknologi. Regjeringen signaliserer i meldingen at den også vil ta initiativ til å utarbeide en nasjonal strategi for informasjonssikkerhet.[3] Strategien skal omfatte IT-sikkerhet i hele samfunnet og favne videre enn Sårbarhetsutvalgets forslag. Nasjonal strategi for informasjonssikkerhet forelå i juni 2003, og mye av sikkerhetsarbeidet de seneste årene er fanget opp i strategien og dens tiltak.[4] Telesikkerhet har også betydning for IT-sikkerheten i samfunnet. St.meld. nr. 47 (2000–2001) *Telesikkerhet og -beredskap i et telemarked med fri konkurranse* peker på en rekke tiltak for å bedre telesikkerheten og -beredskapen i Norge. En del av disse tiltakene er tatt inn i Nasjonal strategi for informasjonssikkerhet.

Tekstboks 1

Trusselen mot IT-systemer har økt sterkt de senere årene i form av en rekke datavirus og såkalte ormer og stadig hyppigere forsøk på datainnbrudd. Mørketallsundersøkel-sen viste for eksempel at ca. 60 % av norske virksomheter ble rammet av datakriminalitet eller andre uønskede hendelser i 2003. Hyppigheten av datavirus og ormer er så høy at en datamaskin som kobles til Internett uten noen form for beskyttelse, kan forventes å bli infisert i løpet av 20 minutter.

I tillegg til disse høyfrekvente truslene finnes også trusler som kan ha betydning for nasjonal sikkerhet. Disse truslene vil i større grad utgjøres av organiserte grupper med høy kompetanse som angriper spesifikke mål. Offensiv kapasitet til å angripe IT-systemer bygges opp i militære styrker i mange land. Det er også stadig klarere sammenhenger mellom datakriminalitet og annen organisert kriminalitet.

Kilde: Se vedlegg 1.

1.2 Formål og problemstillinger

Formålet med undersøkelsen har vært å vurdere om myndighetenes arbeid med IT-sikkerheten i samfunnet er i samsvar med Stortingets vedtak og forutsetninger. Følgende problemstillinger er særlig belyst:

A. Hvordan er myndighetenes arbeid med IT-sikkerhet organisert, og i hvilken grad er organisasjonsmessige forutsetninger fulgt opp?
   1. Er ansvarsforholdene avklart på departementsnivå?
   2. Er fagorganenes ansvar avklart?
   3. Har det skjedd en samordning av regelverket?

B. Hvilke plan- og gjennomføringsprosesser er det lagt opp til, og hvordan fungerer disse?

C. I hvilken grad har myndighetene planlagt og iverksatt tiltak for å beskytte samfunnskritisk IT-infrastruktur?
   1. Er det klarlagt hvilken IT-infrastruktur som krever særlig beskyttelse?
   2. Hva gjør sentrale myndigheter for å redusere sårbarheten i kritisk IT-infrastruktur?
   3. I hvilken grad er det etablert systemer og rutiner for å fange opp trusler mot disse systemene?
   4. I hvilken grad er det etablert systemer for å håndtere alvorlige sikkerhetshendelser?

D. Hvordan arbeider myndighetene for å utvikle en sikkerhetskultur innenfor IT-området?
   1. I hvilken grad oppfattes offentlig sektor som drivkraft for informasjonssikkerhet i samfunnet som helhet?
   2. Hvilke tiltak gjennomføres for å øke bevisstheten om og kompetansenivået for informasjonssikkerhet?
   3. Hva gjøres for å fremme bruken av internasjonale standarder og veiledningsmateriale?

E. I hvilken grad har myndighetene planlagt og iverksatt tiltak innenfor telesikkerhet og -beredskap?
   1. I hvilken grad er prioriterte oppgaver på området iverksatt eller planlagt?

1) NOU 1986:12 Datateknikk og samfunnets sårbarhet, side 10

2) NOU 2000:24 Samfunnets sårbarhet

3) St.meld. nr. 17 (2001–2002) Samfunnssikkerhet. Veien til et mindre sårbart samfunn, sidene 7 og 36

4) Forsvarsdepartementet, Nærings- og handelsdepartementet, Justis- og politidepartementet: Nasjonal strategi for informasjonssikkerhet. Utfordringer, prioriteringer og tiltak. Juni 2003

2. Hva er eventuelt årsakene til manglende iverksetting og planlegging?
3. Har Samferdselsdepartementet etablert tilfredsstillende styring på området?

1.3 Definisjoner

1.3.1 Informasjonssikkerhet

Med informasjonssystem menes her systemer der informasjon produseres, lagres og behandles. I Nasjonal strategi for informasjonssikkerhet er informasjonssikkerhet definert som tiltak for å beskytte *informasjon* som behandles av et informasjonssystem, mot brudd på konfidensialitet, integritet og tilgjengelighet, for å beskytte *systemet* i seg selv og for å beskytte *nett* der informasjon utveksles.[5] Definisjonen knytter informasjonssikkerhet til prinsippene konfidensialitet, integritet og tilgjengelighet, som er nærmere presisert på denne måten i Norsk Standard NS-ISO 17799: [6]

- Konfidensialitet: å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang
- Integritet: å sikre at informasjonen og behandlingsmetodene er nøyaktige og fullstendige
- Tilgjengelighet: å sikre autoriserte brukere tilgang til informasjon og tilhørende ressurser ved behov

I Nasjonal strategi for informasjonssikkerhet benyttes begrepet IT-sikkerhet synonymt med informasjonssikkerhet. I andre offentlige dokumenter brukes også begrepet IKT-sikkerhet med en tilsvarende mening. Den ulike begrepsbruken gjenspeiles enkelte steder i undersøkelsen, spesielt i kapitlet om revisjonskriterier, der det siteres fra bl.a. stortingsdokumenter. I likhet med Nasjonal strategi for informasjonssikkerhet velger vi hovedsakelig å bruke begrepet IT-sikkerhet i denne undersøkelsen.

1.3.2 IT-infrastruktur

Begrepene IT-infrastruktur, IKT-infrastruktur og infrastruktur benyttes gjennom hele undersøkelsen. Følgende definisjoner er lagt til grunn i Nasjonal strategi for informasjonssikkerhet og i denne undersøkelsen:[7]

- En *infrastruktur* er en kombinasjon av administrative og organisatoriske tiltak, samt tekniske anlegg og utstyr, som skal til for at et samfunn skal kunne fungere på en tilfredsstillende måte. Et samfunn vil ha behov for flere ulike infrastrukturer som brukes i sammenheng med hverandre.
- *IT-infrastruktur:* I forbindelse med informasjonssikkerhet vil en infrastruktur omfatte datamaskiner, programvare, nettverk, lokaler, omgivelser og spesielle forhold som inngår i utvikling, forvaltning og drift av IT-systemene.

5) Nasjonal strategi for informasjonssikkerhet, side 9

6) Definisjonen er hentet fra Norsk Standard NS-ISO 17799 Informasjonsteknologi – Administrasjon av informasjonssikkerhet, side 9.

7) Nasjonal strategi for informasjonssikkerhet, vedlegg 1 – Aktuelle begreper

IKT betegner ifølge St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* sammensmeltingen mellom informasjonsteknologi og telekommunikasjon. Begrepene IT-infrastruktur og IKT-infrastruktur benyttes synonymt i denne undersøkelsen.

1.3.3 Risiko, sårbarhet og trusler

Undersøkelsen omtaler *risiko* i IT-infrastrukturen i Norge. Risiko uttrykker faren for tap av viktige verdier som følge av uønskede hendelser. Det er en funksjon av sannsynligheten for mulige uønskede hendelser og konsekvensene av disse. Sannsynligheten for at en uønsket hendelse skal skje, kan videre ses på som en funksjon av mulige trusler mot infrastrukturen, og hvor sårbar infrastrukturen er i forhold til disse truslene.

Trusler kan defineres som ethvert forhold eller enhver enhet med potensial til å forårsake en uønsket hendelse i IT-infrastrukturen.[8] Det er hensiktsmessig å skille mellom trusler basert på henholdsvis tilsiktede og utilsiktede hendelser. Tilsiktede hendelser vil omfatte terrorisme, kriminalitet, vandalisme og annen destruktiv aktivitet. Feil, ulykker og naturkatastrofer er de vanligste truslene basert på utilsiktede hendelser.

Tekstboks 2

Logiske og fysiske angrep

Fysiske angrep retter seg mot selve utstyret, mens logiske trusler retter seg mot IT-systemenes logiske funksjoner. Det kan være både programvareangrep og direkte systemangrep. Programvareangrep er virus, ormer og lignende ødeleggende kode som ved en rekke tilfeller har spredt seg til store antall systemer tilknyttet Internett i løpet av kort tid. Direkte systemangrep innebærer at angriperen gjennom Internett eller annen ekstern tilkobling prøver å trenge inn i et bestemt IT-system for eksempel for å stjele informasjon eller for å bruke systemet som en lagringsplass for musikk- og andre mediefiler.

Sosiale angrep

I slike angrep utnyttes den menneskelige faktoren i stedet for eller i tillegg til svakheter i programvare. Et klassisk eksempel er angriperen som ringer en bruker og utgir seg for å være fra virksomhetens IT-avdeling, og klarer å få brukeren til å oppgi sitt passord. Dette brukes så til å bryte seg inn i virksomhetens IT-system, f.eks. for å stjele informasjon.

Kilde: Se vedlegg 1.

Sårbarhet er et uttrykk for de svakheter og mangler som finnes i systemene, og som øker sannsynligheten for at trusler materialiserer seg i sikkerhetshendelser.[9] Det kan hevdes at sårbarheten har økt de senere årene som følge

8) Definisjonen av trusler samsvarer med definisjonen i NOU 2000:24 Et sårbart samfunn, side 21.

9) Jf. Nasjonal strategi for informasjonssikkerhet, vedlegg 1

av at samfunnet er blitt mer avhengig av en IT-infrastruktur som blir stadig mer kompleks: Det skjer en stadig tettere sammenkobling mellom IT-systemer både innenfor virksomheter og på tvers av organisasjonsgrenser, teknologiutviklingen skjer raskere enn tidligere, og IT-systemene har økende funksjonalitet.

Ikke all risiko på et område kan fjernes, men det er mulig å redusere risikoen. I prinsippet bør man søke å redusere risikoen til et nivå som man er villig til å akseptere, gitt kostnadene for reduksjonen. Det vil alltid være en avveining mellom sikkerhet og andre egenskaper man ønsker fra et IT-system.

Tekstboks 3

Potensielle konsekvenser av sikkerhetshendelser vil variere sterkt. Det ene ytterpunktet er angrep eller feil i kritisk IT-infrastruktur som kan lamme store deler av samfunnet. Forsvarets forskningsinstitutt har i en analyse av infrastrukturen for telekommunikasjon i Norge påpekt at på grunn av sterke avhengigheter kan selv små problemer på ett samfunnsområde forplante seg videre og bygge seg opp til et stort, omfattende problem for hele samfunnet.

Det andre ytterpunktet er de daglige sikkerhetshendelsene som følge av datavirus og lignende som enhver virksomhet med tilknytning til Internett vil oppleve. Disse hendelsene har ikke isolert sett noen store konsekvenser for samfunnet. Samlet kan imidlertid selv disse små hendelsene gi store økonomiske tap. *Mørketallsundersøkelsen 2003* estimerte at datakriminalitet og uønskede IT-hendelser kostet virksomheter i Norge mer enn fem milliarder kroner i 2003.

Kilde: Se vedlegg 1.

Scanpix Creative/Masterfile

1.4 Avgrensninger

Undersøkelsen retter seg mot myndighetenes arbeid for å fremme IT-sikkerhet i samfunnet. Dette er et omfattende tema som gjør det nødvendig å foreta visse avgrensninger:

- Undersøkelsen ser spesielt på arbeid utført av myndighetsorganer som har koordinerende eller sektorovergripende roller innenfor IT-sikkerhet. Samferdselsdepartementets og Post- og teletilsynets arbeid med telesikkerhet og -beredskap er inkludert i undersøkelsen siden sikkerheten i infrastrukturen som denne sektoren er ansvarlig for, har betydning for IT-sikkerheten i samfunnet som helhet. Annet arbeid for å fremme IT-sikkerhet i enkeltsektorer i samfunnet inngår imidlertid ikke i undersøkelsen.

- Undersøkelsen vurderer sentralforvaltningens arbeid med IT-sikkerhet, og legger ikke opp til en kartlegging av IT-sikkerhetsnivået i samfunnet.

- Private bedrifter og organisasjoner arbeider også for å fremme IT-sikkerhet og forvalter deler av den kritiske IT-infrastrukturen i Norge. Undersøkelsen ser på samspillet mellom myndighetene og de private organisasjonene i arbeidet for å fremme IT-sikkerhet, men den går ellers ikke nærmere inn på det arbeidet som utføres i privat sektor.

- Myndighetenes arbeid med å legge til rette for allmenn bruk av elektroniske signaturer (PKI) omtales ikke i undersøkelsen, fordi dette anses som et tiltak under utvikling, og det er ikke direkte knyttet til den generelle IT-sikkerheten.

- Arbeidet med å få etablert et eget kommunikasjonsnettverk for nødetatene inngår ikke i undersøkelsen, og heller ikke andre spesialiserte kommunikasjonsnett, som for eksempel Forsvarets digitale nettverk.

Andre forhold som ikke berøres direkte i undersøkelsen, er:

- Politiets arbeid med datakriminalitet

- Personvernrelaterte problemstillinger

- Problemstillinger knyttet til uanmodet elektronisk post eller meldinger

- Spørsmål rundt beskyttelse av opphavsrettigheter i en digital verden

2 Metodisk tilnærming og gjenføring

Undersøkelsen er gjennomført ved hjelp av dokumentanalyser, statistikk, intervjuer og spørreundersøkelse hos etater og organisasjoner. Vi har ikke gjennomført egne undersøkelser av IT-sikkerhetsnivået i samfunnet, men benytter bl.a. utsagn fra viktige aktører til å belyse statusen på området.

2.1 Dokumentanalyser

Sentrale dokumenter i arbeidet med informasjonssikkerhet i statsforvaltningen er analysert. Det gjelder bl.a.:

- Sårbarhetsutvalgets utredning NOU 2000:24 *Et sårbart samfunn* og oppfølgingen av denne gjennom St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet*, jf. Innst. S. nr. 9 (2002–2003)
- Nasjonal strategi for informasjonssikkerhet
- St.meld. nr. 39 (2003–2004) *Samfunnssikkerhet og sivilt-militært samarbeid*
- St.meld. nr. 47 (2000–2001) *Telesikkerhet og -beredskap i et telemarked med fri konkurranse*

Vi har også gått gjennom det tilhørende bakgrunnsmaterialet og planene for gjennomføring av tiltak knyttet til disse dokumentene. I tillegg er andre relevante stortingsdokumenter, lover, regelverk, instrukser, handlingsplaner, virksomhetsplaner og -rapporter, tildelingsbrev, møtereferater og evalueringer gjennomgått. For å få en forståelse av området er dessuten relevant faglitteratur, aktuelle forskningsrapporter og artikler i dags- og fagpressen gjennomgått.

IT-infrastrukturen i Norge er nært knyttet til en internasjonal infrastruktur, og det er vanskelig å se den nasjonale infrastrukturen isolert. Det er derfor innhentet en del informasjon om status og erfaringer fra andre lands IT-sikkerhetsarbeid, og hvilke tiltak myndighetene i de forskjellige landene har gjennomført eller planlegger å gjennomføre. Det er også innhentet informasjon om IT-sikkerhetsarbeidet i internasjonale organisasjoner, særlig EU og OECD. Materialet benyttes i begrenset grad i rapporten, men noe presenteres i form av eksempler underveis i framstillingen.

2.2 Intervjuer underveis i arbeidet

For å få en oversikt over arbeidet med IT-sikkerhet i staten er det gjennomført intervjuer med følgende departementer: Samferdselsdepartementet, Nærings- og handelsdepartementet, Justis- og politidepartementet, Forsvarsdepartementet, Arbeids- og administrasjonsdepartementet og senere Moderniseringsdepartementet (etter omorganiseringen av departementsstrukturen i juni 2004). I tillegg er det gjennomført intervjuer med følgende aktører som har en rolle i arbeidet: Post- og teletilsynet, Nasjonal sikkerhetsmyndighet, Direktoratet for samfunnssikkerhet og beredskap, Politiets datakrimsenter, Senter for informasjonssikring, Datatilsynet og Statens forvaltningstjeneste. Det foreligger verifiserte referater fra alle intervjuene.

Det er dessuten gjennomført intervjuer med Forsvarets forskningsinstitutt og Statskonsult, som begge har hatt roller i arbeidet med IT-sikkerhet. Av bransje- og næringsorganisasjoner er Abelia, IKT-Norge og Næringslivets sikkerhetsorganisasjon intervjuet. Disse organisasjonene har vært involvert i myndighetenes arbeid med å sikre IT-infrastrukturen i Norge. De er også gitt oppgaver og ansvar i oppfølgingen av Nasjonal strategi for informasjonssikkerhet. Ett av formålene med disse intervjuene var å få et bilde av hvordan viktige aktører utenfor den sentrale forvaltningen ser på informasjonssikkerheten i Norge og myndighetenes tiltak på området.

2.3 Bruk av statistikk

Statistisk sentralbyrå (SSB) presenterer jevnlig statistikk der også spørsmål om informasjonssikkerhet er tatt inn. SSBs undersøkelser og statistikk innen IT-området gir et bilde av sikkerhetssituasjonen i privat, kommunal og statlig sektor. Denne statistikken er relevant for å måle sikkerhetstilstanden. Mørketallsundersøkelsene gir grunnlag for å vurdere sikkerhetstilstanden. *Mørketallsundersøkelsen 2003* er gjennomført som et samarbeid mellom Næringslivets Sikkerhetsråd, Økokrim og Senter for informasjonssikring på bakgrunn av data som ble samlet inn i januar 2004. Undersøkelsen omhandler både mørketall (ikke anmeldte hendelser) for datakriminalitet og andre uønskede IT-hendelser. Data fra *Mørketallsundersøkelsen 2003* er til en viss grad benyttet i undersøkelsen der det er relevant.

2.4 Spørreundersøkelse og avsluttende intervjuer

I sluttfasen av arbeidet med denne rapporten ble det gjennomført en spørreundersøkelse hos de etatene og organisasjonene som har oppfølgingsansvar i Nasjonal strategi for informasjonssikkerhet. Følgende organer inngikk i undersøkelsen: Post- og teletilsynet, Nasjonal sikkerhetsmyndighet, Direktoratet for samfunnssikkerhet og beredskap, Senter for informasjonssikring og

Datatilsynet. Spørrelister ble sendt til følgende organisasjoner: Abelia, IKT-Norge og Næringslivets Sikkerhetsråd/Næringslivets sikkerhetsorganisasjon under Næringslivets Hovedorganisasjon (NHO). Dette er som nevnt organisasjoner som har vært involvert i myndighetenes arbeid med å sikre IT-infrastrukturen, og som er gitt oppgaver og ansvar i oppfølgingen av Nasjonal strategi for informasjonssikkerhet. Organisasjonene representerer både IT-bransjen og næringslivet mer generelt.

Hensikten med spørreundersøkelsen var å få synspunkter på organisering og planprosess, å få oppdatert informasjon om statusen i de ulike delene av arbeidet med IT-sikkerhet, og å få synspunkter på hvilke deler som er godt ivaretatt, og hvilke deler som er mindre ivaretatt. Alle forespurte ga svar på spørrelistene.

Etter spørreundersøkelsen ble det i mars 2005 gjennomført avsluttende intervjuer med Moderniseringsdepartementet, Samferdselsdepartementet og Justis- og politidepartementet. Det foreligger verifiserte referater fra disse møtene. Hensikten med intervjuene var å få forklaringer og kommentarer til synspunkter og fakta fra spørreundersøkelsen hos etater og organisasjoner. Brev fra Riksrevisjonen med oppklarende spørsmål ble i tillegg besvart av Forsvarsdepartementet.

I tillegg til dette har de nevnte departementene, etatene og organisasjonene underveis i undersøkelsen vært behjelpelige med å svare på e-postforespørsler fra oss, og med å tilrettelegge og verifisere informasjon til bruk i undersøkelsen.

3 Revisjonskriterier

Revisjonskriteriene er utledet fra stortingsmeldinger og -proposisjoner og Stortingets behandling av disse, samt fra aktuelle lover og forskrifter. Herunder benyttes bevilgningsreglementet og reglementet for økonomistyring i staten med tilhørende bestemmelser.[10] Kriteriene er på en del punkter operasjonalisert ved bruk av Nasjonal strategi for informasjonssikkerhet og OECDs *Retningslinjer for sikkerhet i informasjonssystemer og nettverk* med tilhørende iverksettingsplan.[11] OECDs retningslinjer ble vedtatt som en anbefaling av OECDs råd, der Norge er medlem, 25. juli 2002. Nasjonal strategi for informasjonssikkerhet bygger på OECDs retningslinjer.[12]

3.1 Organisering og planlegging av arbeidet med IT-sikkerhet

3.1.1 Prinsipper for organisering

Organiseringen av samfunnssikkerhetsarbeidet er lagt opp etter følgende prinsipper, omtalt bl.a. i St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet*:

- Ansvarsprinsippet betyr at den som har et ansvar i en normalsituasjon, også har et ansvar ved ekstraordinære hendelser.
- Likhetsprinsippet betyr at den organisasjonen man opererer med til daglig, skal være mest mulig lik den organisasjonen man har under kriser.
- Nærhetsprinsippet betyr at kriser skal håndteres på et lavest mulig nivå.[13]

Dette innebærer at ansvaret for IT-sikkerhet er et virksomhetsansvar. Det vil si at det enkelte departement er ansvarlig for at IT-sikkerheten ivaretas i departementet, i dets underliggende virksomheter og innen egen sektor.

3.1.2 Avklaringer av ansvars- og samarbeidsforhold

Behovet for samordning og avklaring av ansvarsforhold er tatt opp i ulike sammenhenger. Ifølge St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* og komiteens behandling av denne skal beredskapen være så godt samordnet at de ulike sektorenes tiltak på sikkerhets- og beredskapsområdet framstår som en helhet. I meldingen heter det videre at ansvarsforholdene mellom Senter for informasjonssikring, Varslingssystem for digital infrastruktur, Post- og teletilsynet og Nasjonal sikkerhetsmyndighet (NSM) vil bli vurdert. Klargjøring av ansvarsforhold blir også tatt opp i St.prp. nr. 1 (2002–2003) for Justis- og politidepartementet, der det heter at ansvarsforholdet mellom Nasjonal sikkerhetsmyndighet og det nye Direktoratet for samfunnssikkerhet og beredskap må avklares. Det påpekes i samme proposisjon at det er svært viktig å etablere gode samarbeidsformer mellom prøveprosjektene Senter for informasjonssikring og Varslingssystem for digital infrastruktur, samt Politiets datakrimsenter. I St.prp. nr. 1 (2003–2004) for både Justis- og politidepartementet og Nærings- og handelsdepartementet uttales det at koordineringen mellom de myndighetene som arbeider med informasjonssikkerhet, skal styrkes.

Komiteene behandler St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* i Innst. S. nr. 9 (2002–2003). Der skriver komiteene at visjonen om et trygt og robust samfunn som avverger trusler og overvinner kriser, betinger tilgjengelige ressurser som kan settes inn på fleksibel måte, men med klare kommandolinjer og sentralt definert ansvar. Komiteene uttaler videre at arbeidet med samfunnssikkerhet skal ha høy prioritet, og det organisatoriske ansvaret skal gjenspeile dette. Ved omtale av Nasjonal sikkerhetsmyndighet påpeker flertallet i komiteene viktigheten av klare kommandolinjer og ansvarsforhold. Komiteene påpeker også viktigheten av klare kommandolinjer og ansvarsforhold ved omtalen av nasjonal krisehåndtering.

Komiteene mener videre at bl.a. IKT-sikkerhet bør ha en særlig oppmerksomhet i de tilbakemeldinger om samfunnets sårbarhet som regjeringen legger fram for Stortinget. Komiteene understreker at klargjøring av ansvarsforhold, beredskapsplaner og krisehåndteringsplaner innenfor området er viktig.[14]

Nasjonal strategi for informasjonssikkerhet legger også vekt på koordinering. Strategien har bl.a. som formål å legge til rette for en bedre koordinering av myndighetene som arbeider med informasjonssikkerhet. Koordineringen av arbeidet med IT-sikkerhet skal bl.a. skje gjennom at man oppretter et permanent utvalg: Koordineringsutvalget for IT-sikkerhet (KIS). Strategien legger også vekt på at regelverket for IT-sikkerhet skal samordnes bedre.

10) Reglement for økonomistyring i staten, fastsatt ved kronprinsregentens resolusjon 12. desember 2003, og Bestemmelser om økonomistyring i staten, fastsatt av Finansdepartementet 12. desember 2003

11) OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security fra 25. juli 2002, og Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security fra 2. juli 2003

12) Forsvarsdepartementet, Nærings- og handelsdepartementet, Justis- og politidepartementet: Nasjonal strategi for informasjonssikkerhet. Utfordringer, prioriteringer og tiltak. Juni 2003

13) Med lavest nivå menes her laveste organisatoriske nivå.

14) Innst. S. nr. 9 (2002–2003)

3.1.3 Planlegging og gjennomføring

I OECDs *Retningslinjer for sikkerhet i informasjonssystemer og nettverk* anbefales det at medlemslandene etablerer ny eller endrer gjeldende politikk, rutiner, tiltak og prosedyrer for å avspeile og ta i betraktning OECDs retningslinjer.[15] Betydningen av helhetlig politikk og handlingsplaner på dette området er videre understreket i OECDs plan for iverksettelse av retningslinjene. I denne planen heter det at det er avgjørende å utvikle godt planlagte og samordnede effektive handlingsprogrammer for å fremme en sikkerhetskultur og iverksette retningslinjene. Videre er det lagt vekt på at utviklingen av en sikkerhetskultur krever bred deltakelse fra alle styringsnivåene, næringslivet og det sivile samfunnet.[16]

I St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet*, pkt. 6.2.4, står det: "Nærings- og handelsdepartementet og Justisdepartementet vil i samarbeid med Forsvarsdepartementet og i forlengelsen av de utredninger som er gjort om sårbarheten innen IKT, ta initiativ til å utarbeide en nasjonal strategi for informasjonssikkerhet. Strategien skal omfatte IT-sikkerhet i hele samfunnet og favne videre enn Sårbarhetsutvalgets forslag. Arbeidet med strategien skal være bredt forankret i flere departementer og også søke å inkludere privat sektor."

I juni 2003 forelå regjeringens nasjonale strategi for informasjonssikkerhet.[17] Strategien fokuserer på utfordringer, prioriteringer og tiltak, og har et tidsperspektiv på to–tre år. Formålet med strategien er:

- å sikre en helhetlig tilnærming til arbeidet med informasjonssikkerhet som grunnlag for politiske beslutninger og prioriteringer
- å legge til rette for bedre koordinering av myndighetene som arbeider med informasjonssikkerhet

Ifølge strategien har regjeringen fire overgripende mål for informasjonssikkerhet, og strategien består av tolv overordnede og prioriterte punkter/tema. De målene og temaene som er relevante for denne undersøkelsen, presenteres senere i dette kapitlet.

I strategien forutsettes det at tiltakene må gjennomføres og finansieres innenfor de budsjettrammene som til enhver tid gjelder for hver enkelt virksomhet. I private virksomheter vil eventuelle kostnader måtte tas under ordinære driftsrammer for virksomheten. Det tas sikte på å innlede en dialog med privat sektor med tanke på samfinansiering av enkelte av tiltakene. I tilknytning til hvert tema er det listet opp flere konkrete tiltak, og det er utpekt én eller flere gjennomføringsansvarlige. Dette ansvaret er først og fremst plassert i sentrale departementer og underliggende etater. For noen tiltak er bransjeorganisasjoner tillagt et gjennomføringsansvar. Alle instanser med gjennomføringsansvar forutsettes å lage en handlingsplan som skal brukes for å realisere strategien.

Det vises i denne sammenheng til bevilgningsreglementet, som fastslår at de resultatene som tilsiktes oppnådd, skal beskrives i budsjettforslaget, og at opplysninger om oppnådde resultater for siste regnskapsår skal gis i vedkommende budsjettproposisjon sammen med annen regnskapsinformasjon som har betydning for vurderingen av budsjettforslaget for kommende år.[18] I reglement for økonomistyring i staten heter det videre at alle virksomheter skal sikre at fastsatte mål og resultatkrav oppnås på en effektiv måte innenfor sitt ansvarsområde. Videre stilles det krav om at alle virksomheter skal sørge for at det gjennomføres evalueringer for å få informasjon om effektivitet, måloppnåelse og resultater innenfor hele eller deler av virksomhetens ansvarsområde og aktiviteter.[19]

3.2 Beskyttelse av kritisk IT-infrastruktur

Ifølge St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* skal arbeidet med samfunnssikkerhet sikre en systematisk identifisering av truslene mot samfunnet og sårbarheten i samfunnet. Arbeidet skal videre sørge for at det blir satt i gang forebyggende tiltak for å forhindre uønskede hendelser og avhjelpe den sårbarheten som er uakseptabel. I behandlingen av meldingen slutter komiteen seg til dette og presiserer at den grunnleggende kunnskapen om hva som skaper sårbarhet, bør prioriteres. Det er avgjørende å utvikle robust infrastruktur i alle samfunnsviktige institusjoner.[20]

3.2.1 Avgrensning av hva som krever særlig beskyttelse

Ett av regjeringens fire overordnede mål for informasjonssikkerhet er ifølge St.prp. nr. 1 (2002–2003) for Nærings- og handelsdepartementet knyttet til å beskytte kritisk infrastruktur: "Samfunnskritisk infrastruktur for elektronisk informasjonsutveksling skal være robust og sikker." I Nasjonal strategi for informasjonssikkerhet heter det i tillegg: "Kritiske informasjonssystemer skal være sikret slik at skadevirkningene ved sikkerhetsbrudd ikke er større enn hva som kan defineres som akseptabel risiko."[21]

15) OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security fra 25. juli 2002

16) Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, punkt I-2 og I-3. Fra 2. juli 2003

17) Nærings- og handelsdepartementet: eNorge, Nasjonal strategi for informasjonssikkerhet. Utfordringer, prioriteringer og tiltak. Juni 2003

18) Bevilgningsreglementet av 26. mai 2005, § 9, jf. §§2 og 13 i tidligere reglement av 19. november 1959

19) Reglement for økonomistyring i staten, § 9 og 16 i fastsatt ved kronprinsregentens resolusjon 12. desember 2003

20) Innst. S. nr. 9 (2002–2003)

21) Nasjonal strategi for informasjonssikkerhet, side 3

Nasjonal strategi for informasjonssikkerhet omtaler videre kritisk IT-infrastruktur på følgende måte: ”Informasjonssystemer eller infrastruktur kan betegnes som kritiske dersom samfunnets, virksomheters eller individers funksjonsevne i stor grad påvirkes av svikt. Det er viktig å identifisere slike systemer og plassere dem på en skala i forhold til hvor kritiske de er. Dette er en forutsetning for å gjennomføre risikovurderinger og implementere nødvendige tiltak.”[22] Som en del av Nasjonal strategi for informasjonssikkerhet er det planlagt å lage et felles sett av kriterier som gjør det mulig å identifisere samfunnskritisk IT-infrastruktur og -systemer.[23]

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) med tilhørende forskrifter gir regler for håndtering av sikkerhetsgradert informasjon og objekter, og foreskriver sikkerhetstiltak som skal fjerne eller redusere sårbarhet mot trusler i form av spionasje, sabotasje og terrorhandlinger.[24] Loven har en egen bestemmelse (§ 17) om den enkelte virksomhets plikt til å beskytte skjermingsverdige objekter. Den enkelte virksomhet plikter å utpeke skjermingsverdige objekter som virksomheten eier eller på annen måte har kontroll over eller fører tilsyn med, bl.a. som et grunnlag for tilsynsvirksomheten til Nasjonal sikkerhetsmyndighet overfor virksomheten.[25] I § 17 annet ledd heter det at Kongen gir nærmere bestemmelser om plikt til å beskytte skjermingsverdige objekter.

3.2.2 Reduksjon av sårbarhet

Det er gjennomført en serie forskningsprosjekter om beskyttelse av samfunnet når det gjelder unormale påkjenninger: BAS-prosjektene (Beskyttelse av samfunnet).[26] Forskningsarbeidet har i stor grad vært premissgivende for samfunnssikkerhetsarbeidet i de senere årene og anses av Justis- og politidepartementet som et viktig bidrag til kompetansehevingen innenfor samfunnssikkerhets- og beredskapsarbeidet. Forskningen skal legge til rette for målrettet innretting og prioritering av tiltak innenfor safunnssikkerhetsarbeidet.[27] Det har vært planlagt et BAS-prosjekt også når det gjelder sårbarheten i nasjonalt viktige IT-systemer. IT-sikkerhet og sårbarhet som et område for forskningsoppdrag ble først omtalt i St.prp. nr. 1 (2002–2003) for Justis- og politidepartementet.

Det framgår av Nasjonal strategi for informasjonssikkerhet at det skal utarbeides en metode for risiko- og sårbarhetsvurderinger. Ut fra fastsatte kriterier og metoder skal man foreta risiko- og sårbarhetsvurderinger av samfunnskritisk infrastruktur. For å kunne redusere skader fra uønskede hendelser anses det som en forutsetning at risiko og sårbarhet kartlegges først. De enkelte sektorene skal videre utarbeide normer for sikring med hensyn til konfidensialitet, integritet og tilgjengelighet.[28]

3.2.3 Systemer og rutiner for å fange opp trusler

Informasjon om sikkerhetshendelser er nødvendig for å få et bilde av foreliggende trusler og sårbarhet i IT-infrastrukturen, og for å kunne gi råd om konkrete trusler eller assistanse ved gjenoppretting av tjenester.

Etableringen av Varslingssystem for digital infrastruktur (VDI) som en del av virksomheten til Nasjonal sikkerhetsmyndighet er ett av tiltakene for å styrke informasjonen om sikkerhetshendelser. Ordningen omfatter analyse av trafikkmønstre på nettet for å fange opp mulige angrep og hendelser.[29] Etablering av VDI omtales på følgende måte i St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet*: ”Det vil være et mål at det systemet som endelig etableres vil kunne tjene både offentlige og private aktører og at det kan bygge på et internasjonalt samarbeid. Det vil bli lagt vekt på at et varslingssystem må være mest mulig åpent både i forhold til hvem som skal kunne være deltakere og brukere og i forhold til at informasjonen skal være mest mulig tilgjengelig.”[30] I Nasjonal strategi sies det at erfaringene fra analysene bør gjøres tilgjengelige for aktuelle samarbeidspartnere og eventuelle andre etter behov.[31]

Et annet tiltak er etableringen av Senter for informasjonssikring, som også er omtalt i St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet*: ”Det er et mål at senteret skal bidra til mer robust IKT-infrastruktur og være et ressurs- og kompetansesenter for offentlige og private aktører som kan ivareta nødvendige funksjoner for informasjonsutveksling, varsling og analyse av sikkerhetsbrudd og trusler.” Senterets oppgaver er nærmere presisert i St.prp. nr. 1 (2001–2002) for Nærings- og handelsdepartementet: ”For at senteret skal fungere etter intensjonene, er det en forutsetning at sikkerhetsbrudd og hendelser meldes inn raskt, og at senteret har god kontakt med ressurspersoner og -miljøer, bl.a. i universitets- og høyskolesektoren og relevante organer for IT-sikkerhet i nasjonal sammenheng. Senterets hovedoppgaver i forsøksperioden skal være å framskaffe et helhetlig bilde av truslene mot norske IKT-systemer, formidle informasjon, kompetanse og kunnskap om trusler og mottiltak, og ha kontakt og samarbeid med tilsvarende organisasjoner i andre land.” Senterets målgrupper er store og små bedrifter, etater og virksomheter, sikkerhetsmyndighetene, politikere og andre.

22) Nasjonal strategi for informasjonssikkerhet, side 12

23) Nasjonal strategi for informasjonssikkerhet, side 19

24) Loven ble vedtatt av Stortinget 20. mars 1998 og trådte i kraft 1. juli 2001.

25) Ot.prp. nr. 49 (1996–97), kapittel 11: Merknader til de enkelte paragrafer

26) I St.meld. nr. 17 (2001–2002) Samfunnssikkerhet, kap.12, er det gjort rede for disse prosjektene.

27) Jf. omtale i St.prp. nr. 1 (2002–2003) for Justis- og politidepartementet, side 116

28) Nasjonal strategi for informasjonssikkerhet, side 19

29) Nasjonal strategi for informasjonssikkerhet, side 23

30) Punkt 6.2.4 i meldingen

31) Nasjonal strategi for informasjonssikkerhet, side 23

I Nasjonal strategi for informasjonssikkerhet er varsling og rådgivning, for eksempel gjennom etablering av varslingsordninger, satt opp som et av hovedområdene. Ordningene bør primært være tilgjengelige for eiere av samfunnskritiske systemer og infrastruktur, men alminnelige bedrifter og offentlige etater bør også ha tilgang til slik informasjon.[32] Når det gjelder Senter for informasjonssikring, skal det ifølge strategien stimuleres til at flest mulig virksomheter, offentlige som private, innrapporterer sikkerhetshendelser til senteret i forsøksperioden.[33]

3.2.4 Håndtering av sikkerhetshendelser

Ifølge St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* skal samordningen av (beredskaps-) planleggingen styrkes slik at alvorlige beredskaps- og sikkerhetsutfordringer reflekteres i de tiltakene man planlegger å iverksette ved kriser. Dette kan for eksempel gjelde en samordnet vurdering av hvilke tiltak som bør iverksettes ved alvorlig svikt i IKT, særlig knyttet til samfunnskritiske funksjoner. I meldingen heter det videre at Justisdepartementet vil ta initiativ for å sikre at tiltak som skal settes i verk ved bortfall av IKT, blir reflektert i kriseplaner. Dette gjelder også tiltak i forhold til situasjoner der det pågår eller er mistanke om angrep via informasjonssystemer.

I Innst. S. nr. 9 (2002–2003) skriver komiteene at de ser viktigheten av å ha et ledelsesapparat som kan håndtere kriser. Øvelser er viktig, for både bevisstgjøring, erfaring og høy grad av aktsomhet. Komiteene mener at saksbehandlere innen sikkerhet, beredskap og krisehåndtering er sidestilt med ledelsesnivået som målgruppe for øvelser.

Håndtering av sikkerhetshendelser er også omtalt i *OECDs retningslinjer for sikkerhet i informasjonssystemer og nettverk*.[34] Som følge av sammenkoblingen mellom informasjonssystemer og nettverk og muligheten for en rask og omfattende spredning av skade, må aktørene handle raskt og på en samarbeidsvillig måte for å ta hånd om sikkerhetshendelser. De må dele informasjon om trusler og sårbarhetsfaktorer på en hensiktsmessig måte og innføre prosedyrer som sikrer et raskt og effektivt samarbeid for å kunne forebygge, oppdage og reagere på sikkerhetshendelser. [35]

3.3 Sikkerhetskultur

I St.prp. nr. 1 (2003–2004) for Justis- og politidepartementet og Nærings- og handelsdepartementet heter det at det skal bygges en sikkerhetskultur med henblikk på å

Scanpix Creative/Masterfile

få bevisstgjort alle aktører. *OECDs retningslinjer for sikkerhet i informasjonssystemer og nettverk* ligger til grunn for utarbeidelsen av Nasjonal strategi for informasjonssikkerhet og arbeidet med utvikling av sikkerhetskultur i Norge. OECD har sett det som viktig å fremme sikkerheten ved bruk av informasjonssystemer og nettverk. Utvikling av sikkerhetskultur innebærer at man fokuserer på sikkerheten når man utvikler informasjonssystemer og nettverk, og at det innføres nye tenke- og handlemåter ved bruk av disse og ved utveksling av informasjon. Bevisstgjøring rundt sikkerhet, ansvar, etikk og risikovurderinger er sentrale prinsipper.[36]

Ifølge Nasjonal strategi for informasjonssikkerhet har regjeringen følgende mål for sikkerhetskultur: "Det skal bygges en sikkerhetskultur rundt bruk og utvikling av informasjonssystemer og elektronisk informasjonsutveksling i Norge. IT-sikkerhet skal være en sentral faktor ved forbrukernes og norske virksomheters bruk av IT."[37]

3.3.1 Offentlig sektor som drivkraft

I OECDs iverksettingsplan for retningslinjene er det understreket at offentlig sektor må ta ansvar for å sikre egne systemer og nettverk på lik linje med andre sektorer.[38] I tillegg sies det i iverksettingsplanens punkt 19 at offentlig sektor på grunn av sitt omfattende engasjement har et spesielt ansvar for å gå foran som et godt eksempel og mønsterbruker. Offentlig sektor kan bruke sin ekspertise til å bidra i utviklingen av beste praksis og til forbedringer som alle deltakere kan ha nytte av. I den

32) Nasjonal strategi for informasjonssikkerhet, side 5

33) Nasjonal strategi for informasjonssikkerhet, side 21

34) OECD retningslinjer for sikkerhet i informasjonssystemer og nettverk – Mot en sikkerhetskultur, oversettelse av NHD 2002

35) OECD retningslinjer for sikkerhet i informasjonssystemer og nettverk – Mot en sikkerhetskultur, oversettelse av NHD 2002, side 7

36) OECD retningslinjer for sikkerhet i informasjonssystemer og nettverk – Mot en sikkerhetskultur, oversettelse av NHD 2002, side 5

37) Nasjonal strategi for informasjonssikkerhet, side 3

38) OECD: Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, side 5–6

nasjonale strategien er det lagt opp til at det bl.a. skal utarbeides generelle offentlige IT-sikkerhetsnormer.[39]

3.3.2 Bevisstgjøring og kompetanseheving

I St.prp. nr. 1 (2003–2004) for Justis- og politidepartementet og for Nærings- og handelsdepartementet sies det, som nevnt over, at det skal bygges en sikkerhetskultur med henblikk på å få bevisstgjort alle aktører. Ifølge OECDs iverksettingsplan er det nødvendig for myndighetene å gjennomføre tiltak rettet mot bevisstgjøring og å støtte andre initiativ rettet mot dette målet.[40]

I den nasjonale strategien legges det opp til at bevisstgjøring om trusselbilde, muligheter, begrensninger og mulige tiltak skal være en oppgave for myndighetene, men at alle har et selvstendig ansvar for å skaffe nødvendig kunnskap.[41] Strategien peker bl.a. på følgende tiltak som er rettet mot bevisstgjøring:[42]

- Det skal utvikles og spres informasjons- og veiledningsmateriell om IT-sikkerhet ved bruk av IT i husstandene.
- Det skal etableres en informasjonstjeneste på nett med generell informasjon, lenker og mulighet til å få svar på spørsmål fra publikum.
- Det bør gjennomføres en informasjonskampanje for å spre kjennskap til god praksis for IT-sikkerhet i husstandene.
- Det skal utvikles en "undervisningspakke" for grunnskole og videregående skole med vekt på IT-sikkerhet.
- Det skal arbeides for at produkter og systemer rettet mot massemarkedet skal ledsages av lettfattelig opplysnings- og opplæringsmateriale innen IT-sikkerhet.

Sårbarhetsutvalget så manglende bevissthet og kompetanse i mange virksomheter som et hovedproblem innen IKT-sikkerhet.[43] Utvalget la til grunn at det var behov for å styrke IT-utdanningen ved å fokusere på sikkerhet på alle nivåer fra videregående skole til universitet. Iverksettingsplanen til OECD peker på at det er nødvendig med videre innsats for å utvikle utdanningsprogrammer for informasjonssikkerhet innenfor alle utdanningsretninger som bruker IT.[44]
Nasjonal strategi for informasjonssikkerhet inneholder tiltak for kompetanseutvikling innen IT-sikkerhet og inkorporering av temaet i relevante utdannelser. Dette er noen av tiltakene:[45]

- Utdanning der bruk av IT er en integrert del, bør styrkes ved å utvide denne delen med undervisning i IT-sikkerhet. Det bør utarbeides læreplaner og materiell til støtte for undervisningen.
- Det skal etableres flere høyere utdanninger innen IT-sikkerhet på mastergradsnivå med godkjenning i norske institusjoner for høyere utdanning.
- Det skal gjennomføres et forskningsprogram innen IT-sikkerhet.
- Det skal etableres et forskningsprosjekt i BAS-serien.
- Det skal arbeides for at ledere i private og offentlige virksomheter tar ansvar for at virksomheten har tilstrekkelig kompetanse innen IT-sikkerhet.

3.3.3 Internasjonale standarder og veiledning

I B.innst. S. nr. 1 (1996–1997) ber Stortinget regjeringen om å legge fram en egen sak om oppretting av et sertifiseringsorgan for sikre dataløsninger i løpet av våren 1997. Ved behandlingen av St.prp. nr. 1 (1998–99) fra Nærings- og handelsdepartementet samtykker Stortinget i at departementet etablerer to ordninger for sertifisering av IT-sikkerhet, én for produkter og systemer og én for organisasjoner. Høsten 2002 ble SERTIT etablert som sertifiseringsordning under Nasjonal sikkerhetsmyndighet.[46]

I Nasjonal strategi for informasjonssikkerhet heter det at sertifiseringsordningene bør tas i bredere bruk av norske virksomheter.[47] Strategien nevner også at etablerte standarder for IT-sikkerhet bør tas i bruk i offentlige og private IT-anskaffelser ved kjøp av bl.a. produkter, og at informasjonen om standarder og deres anvendelsesområde skal styrkes.

OECDs iverksettingsplan framhever at offentlig sektor kan bruke sin ekspertise til å bidra i utviklingen av god praksis og til forbedringer som alle deltakere kan ha nytte av. I planens punkt 10 legges det opp til at myndighetene bør vurdere støtte til å utvikle god praksis. God praksis kan uttrykkes i form av internasjonale standarder eller i form av retningslinjer eller veiledninger.[48]

Veiledninger basert på god praksis

I OECDs plan for å bygge en god sikkerhetskultur er det tatt opp flere forhold som kan fremme god praksis. Utveksling av god praksis blir sett på som viktig for å øke brukeres forståelse for og evne til å nå målet om effektive og oppdaterte sikkerhetstiltak.[49] Planen nevner også at ytterligere innsats er nødvendig for å bidra til at brukere av systemer og nettverk skal vite hvordan de

39) Nasjonal strategi for informasjonssikkerhet, side 20

40) Jf. OECD: Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, side 4

41) Nasjonal strategi for informasjonssikkerhet, side 5

42) Nasjonal strategi for informasjonssikkerhet, side 22 og 24

43) NOU 2000:24 Et sårbart samfunn, side 72

44) OECD: Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, punkt 16

45) Nasjonal strategi for informasjonssikkerhet, side 22–25

46) Jf. pressemelding fra SERTIT 14. oktober 2002, Offentlig godkjenning av sikkerhet i IT-produkter

47) Nasjonal strategi for informasjonssikkerhet, side 24

48) Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, punkt 19

49) Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, punkt 13

bør sette opp og vedlikeholde disse.[50] Nasjonal strategi for informasjonssikkerhet inneholder bl.a. følgende tiltak på dette området:[51]

- Det skal gjennomføres risiko- og sårbarhetsanalyser.
- Informasjon og informasjonssystemer skal klassifiseres.
- Det skal utvikles en veiledning for hvordan IT-sikkerhet skal implementeres i systemer og iverksettes i private virksomheter.
- Leverandører av IT-systemer bør følge anerkjente sikkerhetsnormer og standarder og tilrettelegge for enklest mulig bruk av sikkerhetsfunksjonalitet i sine systemer.
- Leverandører av Internett-aksess bør følge anerkjente sikkerhetsnormer og standarder og synliggjøre hvilken grad av tilgjengelighet, kapasitet og driftsstabilitet som tilbys, samt hvilken brukerhjelp som kan ytes ved feilsituasjoner.
- Tjenesteleverandører bør følge anerkjente sikkerhetsnormer og standarder og gjøre kjent hvilket sikkerhetsnivå tjenesten tilbyr.
- Enhver som stiller IT-utstyr og IT-systemer til rådighet for andre, bør følge anerkjente sikkerhetsnormer og standarder, klargjøre sikkerhetsegenskaper og krav for dette, samt tydeliggjøre eget og brukernes ansvar.

3.4 Telesikkerhet og -beredskap

I St.meld. nr. 47 (2000–2001) *Telesikkerhet og -beredskap i et telemarked med fri konkurranse* blir det lagt fram en ny strategi for telesikkerhet og -beredskap. I den nye strategien inngår en rekke fysiske og teletekniske tiltak, i tillegg til administrative og organisatoriske tiltak.[52]

3.4.1 Delegering av oppgaver

Samferdselsdepartementet vil bl.a. utvide Post- og teletilsynets myndighetsansvar til å omfatte følgende oppgaver i tilknytning til telesikkerhet og teleberedskap:[53]

- sette krav til telesikkerhet og teleberedskap og vurdere investeringer i tiltak for å gjøre telenettene mer robuste
- føre tilsyn med at pålagte tiltak blir iverksatt
- drive med bevisstgjøring, kompetanseheving og veiledning overfor operatører, brukere og andre aktører
- arrangere samøvelser og utvikle samarbeid mellom teleoperatørene

I meldingen regner Samferdselsdepartementet med at man bør ha en bemanning på minimum 4–7 personer for å få et kompetent sikkerhets- og beredskapsmiljø.

3.4.2 Tiltak for økt telesikkerhet og -beredskap

Telenor har i kraft av selskapets ledende posisjon på det norske telemarkedet vært pålagt av Samferdselsdepartementet å levere spesielle samfunnspålagte oppgaver (SSO) som bl.a. omfatter ytelser til Totalforsvaret og nød- og sikkerhetstjenester knyttet til kystradioen. Samferdselsdepartementet peker i St.meld. nr. 47 (2000–2001) på at det må etableres et nytt SSO-konsept der det settes krav som omfatter alle samfunnsviktige teleoperatører. Samferdselsdepartementet peker videre på at framtidige teleberedskapstiltak også vil innbefatte tiltak rettet mot mobiltelefoni som ikke var dekket av SSO-avtalen på dette tidspunktet.

Ifølge St.meld. nr. 47 (2000–2001) vil Post- og teletilsynet få ansvar for å påse at en rekke andre tiltak for å øke sikkerheten og beredskapen i telenettene blir iverksatt:[54]

a) raskt innføre en ny prioritetsordning i telenettene
b) legge til rette for at det for framtidige installasjoner finnes en mulighet for samlokalisering i fjellanlegg for de operatørene som leverer tjenester til Totalforsvaret
c) følge utviklingen i utbyggingen av teleinfrastrukturen nøye, og gjennom pålegg og ulike samarbeidstiltak sørge for økt redundans i telenettene[55]
d) drive med bevisstgjøring, kompetanseheving og veiledning
e) utvikle en klassifiseringsordning for teleinfrastrukturen
f) gjennomføre en sikkerhetsevaluering av teleinfra strukturen i samarbeid med teleoperatørene
g) planlegge og gjennomføre samøvelser for operatørene
h) etablere beredskapslagre med transportabelt beredskapsutstyr
i) fastsette forskrift om beskyttelse av telekommunikasjonsanlegg mot elektromagnetisk puls (EMP-forskriften)
j) utrede forutsetningene for og konsekvensene av å innføre et krav om nasjonal autonomi for alle samfunnsviktige teleoperatører[56]
k) stille krav til operatørene om at det skal utarbeides oversikt over hvordan viktige system er koblet mot det øvrige nettverket, og krav om bedre beskyttelse av viktige delsystemer

50) Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, punkt 15

51) Nasjonal strategi for informasjonssikkerhet, side 23–24

52) St.meld. nr. 47 (2000–2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse, side 8

53) St.meld. nr. 47 (2000–2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse, side 8

54) St.meld. nr. 47 (2000–2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse, side 8–9 og 50–55

55) Med redundans menes omrutingsalternativer eller reserveløsninger i den enkelte operatørs nett eller mellom ulike operatørers nett.

56) Nasjonal autonomi innebærer at det skal være mulig å kommunisere innenfor nasjonens grenser uten å være avhengig av driftsstøtte fra utlandet.

l) utarbeide et opplegg for bruk av «red teams» for å avdekke svakheter i informasjonssystemenes sikkerhet
m) overvåke utviklingen i bruken av Internett og fortløpende vurdere behovet for å implementere sikkerhets- og beredskapstiltak

I Innst. S. nr. 329 (2000–2001) viser komiteen til at telenettets betydning for flere vitale samfunnsfunksjoner er stor, og at det derfor er av overordnet betydning å sikre operativitet i telenettet under alle forhold. I innstillingen peker komiteen også på at siden telenettet stadig blir mer komplekst, og siden flere operatører etter hvert tilbyr telekommunikasjonstjenester, er det behov for en gjennomgang av de eksisterende beredskaps- og sikkerhetsrutinene i nettet. Komiteen slutter seg til at Post- og teletilsynet tillegges ansvar for telesikkerhet og beredskap, og merker seg de tiltakene som er aktuelle å iverksette.

Samferdselsdepartementet ga retningslinjer for Post- og teletilsynets planlegging og oppfølging av St.meld. nr. 47 (2000–2001) i brev av 20. desember 2001. I brevet påpekte departementet at det var avgjørende at Post- og teletilsynet så raskt som mulig kom i gang med å implementere tiltakene i meldingen. Departementet ønsket at Post- og teletilsynet i første omgang prioriterte tiltakene a), b), c), f), i) og m).

3.4.3 Virkemidler

Lov om elektronisk kommunikasjon (ekomloven) av 4. juli 2003 gir myndighetene hjemmel til å sette krav til sikkerhet og beredskap overfor teleoperatørene. I lovens § 2-10 heter det at tilbyderen skal tilby elektronisk kommunikasjonsnett og -tjeneste med nødvendig sikkerhet for brukerne i fred, krise og krig, samt opprettholde nødvendig beredskap. Det er spesifisert at viktige samfunnsaktører skal prioriteres ved behov. Forvaltningen gis mulighet til å fastsette forskrift, treffe enkeltvedtak eller inngå avtale for å nå disse målene. Lovens krav til sikkerhet er utdypet noe i kapittel 8 i ekomforskriften som trådte i kraft 1. mars 2004.

Når det gjelder finansieringen av tiltakene i St.meld. nr. 47 (2000–2001), sier Samferdselsdepartementet at valget av finansieringsmåte vil avhenge av hva slags tiltak det dreier seg om, og vil måtte avgjøres konkret i forbindelse med at man beslutter å implementere de enkelte tiltakene. Departementet framhever at det er viktig at de finansieringsløsninger som velges bidrar til klare ansvarsforhold, og at Post- og teletilsynet gis nødvendig handlekraft slik at arbeidet med telesikkerhet og -beredskap ikke blir forsinket eller målene ikke nås. I lov om elektronisk kommunikasjon § 2-10 slås det fast at tilbyderen i utgangspunktet skal dekke kostnadene ved sikkerhets- og beredskapstiltak, men at tilbyderens reelle merkostnader forbundet med levering av sikkerhets- og beredskapstiltak skal kompenseres av staten.

3.4.4 Samferdselsdepartementets oppfølging

Det prinsipielle kravet om å formulere mål og rapportere om oppnådde resultater ble fastlagt ved Stortingets behandling av St.prp. nr. 52 (1984–85) og Innst. S. nr. 135 (1984–85) om reformer i statens budsjettsystem og endringer i bevilgningsreglementet. Det vises i denne sammenheng til bevilgningsreglementet som fastslår at de resultatene som tilsiktes oppnådd, skal beskrives i budsjettforslaget, og at opplysninger om oppnådde resultater for siste regnskapsår skal gis i vedkommende budsjettproposisjon sammen med annen regnskapsinformasjon av betydning for vurderingen av budsjettforslaget for kommende år.[57] Kravene er operasjonalisert i reglementet for økonomistyring i staten. Reglementets § 4 fastslår at virksomhetene skal fastsette mål og resultatkrav innenfor rammen av disponible ressurser og forutsetninger gitt av overordnet myndighet, sikre at fastsatte mål og resultatkrav oppnås, og sikre at ressursbruken er effektiv. Videre skal styringssystemene sikre tilstrekkelig styringsinformasjon og forsvarlig beslutningsgrunnlag. Departementet skal fastsette overordnede mål og styringsparametere for underliggende virksomheter for å kunne vurdere måloppnåelse og resultater.

I punkt 1.5.1 i bestemmelser om økonomistyring i staten heter det at departementet i samråd med virksomheten skal definere behov for og avtale omfang og innhold i rapporteringen. Omfanget av rapporteringen skal være i henhold til tildelingsbrevet og fokusere på måloppnåelse og resultater.

I reglementets § 16 stilles det krav om at alle virksomheter skal sørge for at det gjennomføres evalueringer for å få informasjon om effektivitet, måloppnåelse og resultater innenfor hele eller deler av virksomhetens ansvarsområde og aktiviteter.

57) Bevilgningsreglementet av 26. mai 2005, § 9, jf. §§2 og 13 i tidligere reglement av 19. november 1959

4 Fakta: Organisering og planlegging av myndighetenes arbeid

4.1 Oversikt over organiseringen av myndighetenes arbeid

I Norge er ansvaret for IT-sikkerhet et virksomhetsansvar. Det vil si at det enkelte departement er ansvarlig for at IT-sikkerheten ivaretas i departementet, i dets underliggende virksomheter og innen egen sektor. Det enkelte fagdepartement skal også påse at nødvendige virkemidler tas i bruk slik at målene for informasjonssikkerhet i størst mulig grad nås innen egen sektor. Det innebærer også å påse at aktuelt regelverk etterleves av både offentlige og private virksomheter.[58]

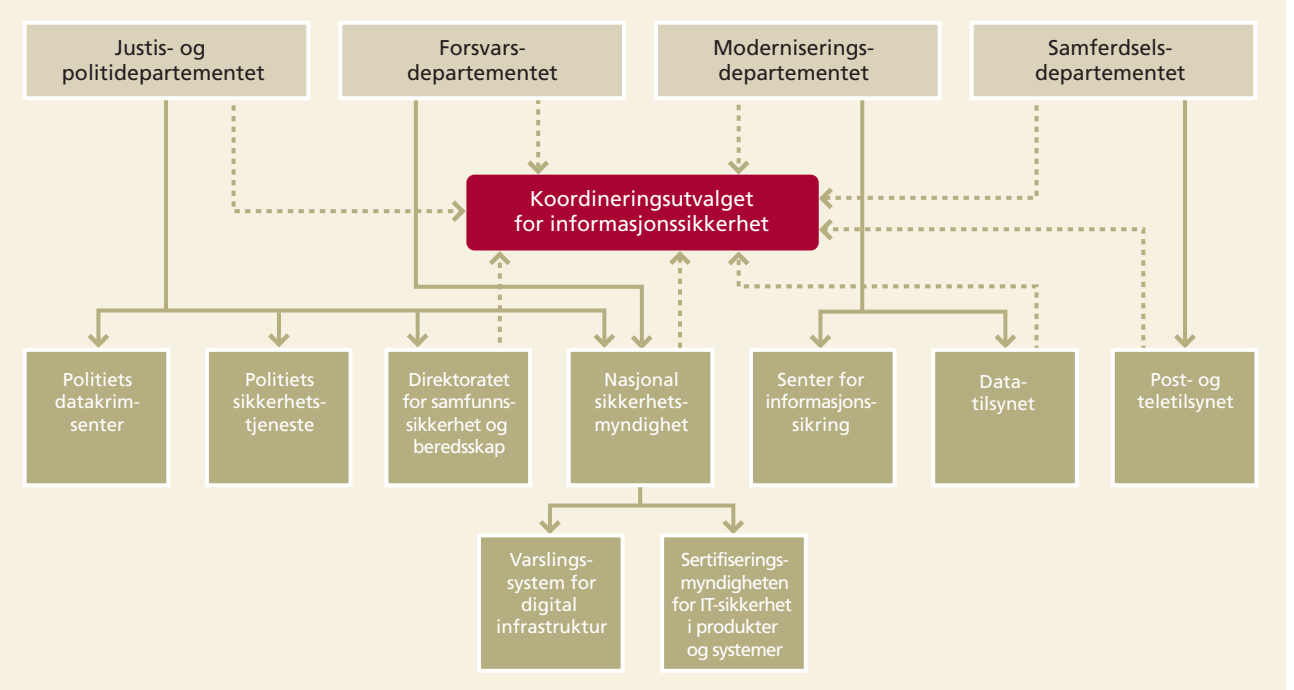
Koordinerings- eller tilsynsoppgaver innen IT-sikkerhet er i tillegg tillagt en rekke departementer, etater og utvalg. Figuren nedenfor gir en oversikt over de mest sentrale aktørene med koordinerings- eller tilsynsansvar, i tillegg til Samferdselsdepartementet og den underliggende etaten med sektoransvar for telesikkerhet og -beredskap.[59] De ulike myndighetene og organene i figuren har i ulik grad oppgaver knyttet til:[60]

- rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser
- sikkerhet for kritiske samfunnsfunksjoner i sivil sektor
- alminnelig IT-sikkerhet

4.1.1 Moderniseringsdepartementet

Ved endringer i departementsstrukturen ble Moderniseringsdepartementet opprettet med virkning fra 1. oktober 2004. Moderniseringsdepartementet overtok ansvaret for å koordinere regjeringens IT-politikk og arbeidet med IT-sikkerhet fra Nærings- og handelsdepartementet. Moderniseringsdepartementet skal identifisere og følge opp sektorovergripende spørsmål, og initiere og koordinere tiltak av tverrsektoriell karakter på dette området.[61] Departementet har også en pådriverrolle overfor fagdepartementene.[62]

Organer med sentrale oppgaver innenfor IT-sikkerhet



Kilde: Omtale av ansvaret for IT-sikkerhet i staten i St.meld. nr. 17 (2001–2002) Samfunnssikkerhet.Veien til et mindre sårbart samfunn, St.meld. nr. 39 (2003–2004) Samfunnssikkerhet og sivilt-militært samarbeid og Nasjonal strategi for informasjonssikkerhet, justert for senere endringer i organisasjonsstrukturen

58) St.meld. nr. 39 (2003–2004) *Samfunnssikkerhet og sivilt-militært samarbeid,* side 43

59) På sidene 43–45 i St.meld. nr. 39 (2003–2004) omtales også disse aktørene som sentrale aktører.

60) Punkter hentet fra Nasjonal strategi for informasjonssikkerhet. Forsvarsdepartementet, Nærings- og handelsdepartementet og Justis- og politidepartementet, juni 2003

61) St.meld. nr. 39 (2003–2004) Samfunnssikkerhet og sivilt-militært samarbeid. Moderniseringsdepartementet har deretter overtatt Nærings- og handelsdepartementets oppgaver omtalt i meldingen.

62) Nasjonal strategi for informasjonssikkerhet, juni 2003, side 17

Nærings- og handelsdepartementet hadde i kraft av sin rolle som fagdepartement også ansvaret for å koordinere arbeidet med IT-sikkerhet i næringslivet. Departementet ledet arbeidet med utvikling og oppfølging av Nasjonal strategi for informasjonssikkerhet, og ledet Koordineringsutvalget for informasjonssikkerhet (KIS) fram til Moderniseringsdepartementet overtok dette arbeidet høsten 2004. I denne undersøkelsen brukes betegnelsen Nærings- og handelsdepartementet på den aktiviteten departementet hadde på dette området fram til oktober 2004.

Ved omorganiseringen fikk Moderniseringsdepartementet i tillegg tilført oppgaver innenfor IT-sikkerhet som tidligere var tillagt Arbeids- og administrasjonsdepartementet. Det gjelder bl.a. forvaltningen av forskrift om elektronisk kommunikasjon med og i forvaltningen, og forskriften til personopplysningsloven. Departementet fikk også overført ansvaret for tverrgående spørsmål som gjelder IT i offentlig sektor, samt IT for alle departementene.[63]

Datatilsynet er underlagt Moderniseringsdepartementet. I tillegg styrer departementet prosjektet *Senter for informasjonssikring*. Senteret ble etablert som et treårig forsøksprosjekt i 2002. Det har ingen myndighetsrolle, men er en selvstendig enhet lagt til SINTEF i Trondheim med samarbeid mot UNINETT. Formålet med prosjektet har vært å etablere et senter som på lengre sikt kan få ansvar for den nasjonale koordineringen av oppgaver innenfor hendelsesrapportering, varsling, analyse og erfaringsutveksling når det gjelder trusler mot IT-systemer.[64]

4.1.2 Justis- og politidepartementet

Departementet har et samordnings- og tilsynsansvar for samfunnets (sivile) sikkerhet med utgangspunkt i kgl. res. 16. september 1994 og 4. juli 2003. Dette samordningsansvaret gjelder ifølge departementet også for beredskap i kritisk infrastruktur.[65]

Departementet har overordnet ansvar for *Direktoratet for samfunnssikkerhet og beredskap* (DSB), som ble opprettet 1. september 2003. Direktoratet har oppgaver innen både forebygging og gjennomføring av tiltak på samfunnssikkerhetsområdet: bl.a. utvikling og vedlikehold av nasjonalt beredskapsplanverk, systemrettet tilsyn med beredskapsarbeidet hos fylkesmennene og i departementene, og planlegging og gjennomføring av øvelser. Ifølge departementet har DSB ikke fagansvar for informasjonssikkerhet, men direktoratet arbeider med å ta inn informasjonssikkerhet og -beredskap i det nasjonale beredskapsplanverket. Informasjonssikkerhet og -beredskap skal også integreres i DSBs øvelsesvirksomhet.[66]

Justis- og politidepartementet har i tillegg et overordnet faglig ansvar for forebyggende sikkerhetstjeneste i sivil sektor gjennom styringen av Nasjonal sikkerhetsmyndighets oppgaver knyttet til bl.a. informasjonssikkerhet.[67] Nasjonal sikkerhetsmyndighets oppgaver beskrives nærmere i omtalen av Forsvarsdepartementet nedenfor.

Under Justis- og politidepartementet ligger også *Politiets datakrimsenter*, som er den sentrale enheten i politiet for etterforskning og påtale av datakriminalitet, og *Politiets sikkerhetstjeneste*, som bl.a. utarbeider trusselvurderinger.[68]

4.1.3 Forsvarsdepartementet

Forsvarsdepartementet har ansvar for utformingen og iverksettingen av norsk sikkerhets- og forsvarspolitikk, herunder forvaltningsansvar for sikkerhetsloven. Denne retter seg mot trusler i form av spionasje, sabotasje eller terrorhandlinger som kan true rikets selvstendighet og sikkerhet og andre vitale samfunnsinteresser.

Nasjonal sikkerhetsmyndighet ble opprettet 1. januar 2003 som et eget direktorat administrativt underlagt Forsvarsdepartementet. Nasjonal sikkerhetsmyndighet rapporterer faglig til Forsvarsdepartementet i militær sektor og til Justis- og politidepartementet i sivil sektor. Direktoratet skal i henhold til sikkerhetsloven ha et kontrollerende og koordinerende ansvar for sikkerhetstiltak i tilknytning til forebyggende sikkerhetstjeneste.[69] Den forebyggende sikkerhetstjenesten omfatter i Norge alle tiltak for å sikre skjermingsverdig informasjon og beskytte objekter mot sikkerhetstruende virksomhet. Organet SERTIT, som sertifiserer IT-produkter og IT-systemer, er en del av Nasjonal sikkerhetsmyndighet.

Nasjonal sikkerhetsmyndighet er også tillagt ansvar for *Varslingssystem for digital infrastruktur* (VDI), som ble etablert permanent i 2003. Både offentlige etater og private bedrifter med ansvar for samfunnskritiske funksjoner er deltakere i VDI. Systemet skal kartlegge uønsket trafikk inn mot deltakernes datanettverk.

4.1.4 Samferdselsdepartementet

Samferdselsdepartementet har et sektoransvar for telesikkerhet og -beredskap, og er regelverksforvalter av lov om elektronisk kommunikasjon, som setter krav til sikkerhet og beredskap.[70] Departementets ansvar dekker

63) Nasjonal strategi for informasjonssikkerhet. Juni 2003

64) Referat fra møte mellom Senter for informasjonssikring og Riksrevisjonen 18. september 2003

65) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen 15. mars 2005

66) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen 21. oktober 2003

67) Kronprinsregentens resolusjon av 4. juli 2003

68) St.meld. nr. 39 (2003-2004) Samfunnssikkerhet og sivilt-militært samarbeid, side 44 og 45

69) Lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste

70) Opplysningene er hentet fra St.meld. nr. 39 (2003–2004) Samfunnssikkerhet og sivilt-militært samarbeid.

alle tilbydere av elektroniske kommunikasjonsnett og -tjenester knyttet til overføring av elektronisk kommunikasjon med tilhørende infrastruktur, tjenester, utstyr og installasjoner.

Post- og teletilsynet er et forvaltningsorgan under Samferdselsdepartementet. Siden 2001 har tilsynet hatt et særskilt myndighetsansvar for telesikkerhet og -beredskap.[71]

4.1.5 Koordineringsutvalget for IT-sikkerhet

Sentralt i arbeidet med IT-sikkerhet står Koordineringsutvalget for informasjonssikkerhet (KIS). Utvalget ble etablert i mai 2004 som en oppfølging av Nasjonal strategi for informasjonssikkerhet. Utvalget kan ses på som en videreføring av tidligere koordineringsutvalg:[72] først Rådet for IT-sikkerhet og deretter Forum for IT-sikkerhet. Rådet for IT-sikkerhet var sammensatt av departementer og underliggende organer. Det ble etablert i 1996 og lagt ned i 1999 da Forum for IT-sikkerhet ble etablert. Forumet hadde representanter også fra næringslivet, utvalgte organisasjoner og akademia, i tillegg til departementer og offentlige etater. Det ble lagt ned i 2004 da arbeidet i KIS startet.

Moderniseringsdepartementet leder KIS, og Nasjonal sikkerhetsmyndighet har sekretariatsoppgaven. I tillegg til Moderniseringsdepartementet, Forsvarsdepartementet, Justis- og politidepartementet, Samferdselsdepartementet, Finansdepartementet og Utenriksdepartementet deltar også Statsministerens kontor, Nasjonal sikkerhetsmyndighet, Oljedirektoratet, Kredittilsynet, Sosial- og helsedirektoratet, Norges vassdrags- og energidirektorat, Datatilsynet, Post- og teletilsynet, Direktoratet for samfunnssikkerhet og beredskap og Politidirektoratet i utvalget.

Utvalget har ingen myndighet til å fatte vedtak, men skal fungere som arena for drøfting og være en rådgivende instans overfor departementer og etater. Utvalgets mandat omfatter både alminnelig IT-sikkerhet, spørsmål knyttet til rikets sikkerhet, vitale nasjonale sikkerhetsinteresser og kritiske samfunnsfunksjoner. Ifølge møtereferatene fra 2004 og 2005 er oppfølging av Nasjonal strategi for informasjonssikkerhet et gjennomgående punkt i utvalgets møter.

4.2 Er ansvars- og samarbeidsforholdene klare?

Etter behandlingen av St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* og St.meld. nr. 47 (2000–2001) *Om telesikkerhet og -beredskap* er det etablert en del nye organisatoriske enheter som har oppgaver innenfor IT-sikkerhet. I Innst. S. nr. 9 (2002–2003), som omhandler St.meld. nr. 17, har komiteen flere ganger påpekt viktigheten av klare kommandolinjer og ansvarsforhold. Nedenfor følger en gjennomgang av statusen i de organisatoriske forutsetningene og ansvarsklargjøringene som departementene har lagt til grunn i meldinger og proposisjoner til Stortinget.[73] Først presenteres imidlertid en del vurderinger av dagens organisering av arbeidet med IT-sikkerhet.

4.2.1 Hvordan vurderes dagens organisering?

Som en del av undersøkelsen ble det sendt ut spørrelister til etater og bransjeorganisasjoner, der de ble bedt om å kommentere dagens organisering av IT-sikkerhetsarbeidet. De fleste etatene og organisasjonene mener at ansvaret for informasjonssikkerhet i forvaltningen er spredt på en rekke forskjellige aktører, hvorav flere har relativt begrensede ressurser på området.

Etatenes vurderinger

Senter for informasjonssikring peker på at mange av de begrensede ressursene brukes til overlappende oppgaver. Post- og teletilsynet mener at fragmenteringen ikke bare er uhensiktsmessig, men at uklare ansvarsforhold og dårlig koordinering også representerer en klar svekkelse av tilstanden. Post- og teletilsynet mener videre at det ville vært en fordel å få klargjort ansvaret for Internett. Regelverket som Post- og teletilsynet forvalter, ekomloven,[74] er ifølge etaten helt klart ment å skulle regulere området. Likevel ser tilsynet at andre instanser anser dette for å være deres ansvar, til dels under henvisning til uklare regelverk.

DSB peker på at hver enkelt statlig virksomhet har ansvar for forebyggende tiltak, beredskap og krisehåndtering innenfor sine ansvarsområder, også innenfor IT-sikkerhet og -beredskap. Direktoratet er enig i at enkelte grensesnitt mellom statlige myndigheter er noe uklare. Direktoratet mener det er viktig av hensyn til brukervennlighet å forsøke å samordne informasjon og rådgivning fra myndighetenes side, og viser til at flere kompetansemiljøer arbeider med å framskaffe oversikter over trusler mot og sårbarheter i IT-systemer. Etter DSBs oppfatning bør det være mulig å samordne på en bedre måte enn i dag arbeidet med å framskaffe og formidle en oversikt over trusler mot og svakheter i IT-systemer. Dette innbefatter også spørsmålet om hurtig og god varsling og rådgivning til bedrifter, kommuner og statlige virksomheter ved for eksempel nye trusler mot IT-systemer.

Datatilsynet oppfatter også arbeidsdelingen og ansvarsforholdene som noe uklare, men tror samtidig det er vanskelig å løse dette fullt ut. Tilsynet peker på at utfordringen for koordineringsarbeidet består i å få reell tilslutning til Nasjonal strategi for IT-sikkerhet, og å avklare hvordan den enkelte aktør alene eller i fellesskap med tilstøtende aktører kan realisere strategien.

71) St.meld. nr. 47 (2000–2001) Telesikkerhet i et telemarked med fri konkurranse, side 28

72) Referat fra 1. møte i KIS, 4. mai 2004

73) Forutsetningene er nærmere presentert i kapitlet om revisjonskriterier.

74) Lov om elektronisk kommunikasjon av 4. juli 2003

Nasjonal sikkerhetsmyndighet framhever at arbeidsdelingen og ansvarsforholdene ved første øyekast kan synes uklare og uoversiktlige, men påpeker at de etter en nøyere analyse er komplekse fordi organiseringen ivaretar flere hensyn: etablering og videreutvikling av en rekke forskjellige regelverk som også vil ha betydning for private aktører, tilsyn med etterlevelse av regelverkene, tilrettelegging for næringslivet, akademia og befolkningen generelt, og beskyttelse av det offentliges egen aktivitet. Nasjonal sikkerhetsmyndighet mener at beslutningstakere og aktører må forholde seg til denne komplekse virkeligheten.

Nasjonal sikkerhetsmyndighet peker videre på at det er behov for å avklare hvor langt Moderniseringsdepartementets ansvar for IT-politikken og IT-sikkerheten i samfunnet, herunder informasjonssikkerhet, strekker seg i forhold til ansvar som tilligger regelverksforvaltere innen informasjonssikkerhet.

Bransjeorganisasjonenes vurderinger

Abelia framhever at arbeid med IT-sikkerhet er sektor- og departementsovergripende problemstillinger som ikke kan betjenes av ett enkelt myndighetsorgan. Organisasjonen opplever imidlertid myndighetenes aktørbilde som unødig uoversiktlig, og det er ikke uten videre lett å vite hvilket myndighetsorgan som er ansvarlig for hvilken problemstilling. Dette påpekes også av IKT-Norge. I møte med Koordineringsutvalget for IT-sikkerhet har Næringslivets Sikkerhetsråd etterlyst et mer oversiktlig myndighetsbilde og kontaktpunkt mot det offentlige, fordi det generelt er vanskelig for private virksomheter å få svar på sikkerhetsrelaterte spørsmål fra offentlige etater.[75]

Abelia peker videre på at man mangler oversikt over hvilke myndighetsorganer som er rene informasjonstiltak eller samordningsorganer, og hvilke myndighetsorganer som kan fatte beslutninger og/eller håndheve et lovverk, dvs. er tilsynsorganer. En slik uklarhet oppfattes som åpenbart uheldig for myndighetenes ambisjoner om å oppnå bestemte resultater innenfor IT-sikkerhetsområdet. Det er ifølge Abelia særlig viktig for bedriftene å ha et klart kontaktpunkt mot det offentlige på områder der bedriftene har et lovpålagt ansvar for bestemte oppgaver og/eller er økonomisk ansvarlige for å gjennomføre tiltak, sørge for sertifisering osv. Men det er selvsagt også en fordel å ha oversikt over myndighetenes aktiviteter på områder der en kan hente inspirasjon og ideer til IT-sikkerhetstiltak.

Også Næringslivets Sikkerhetsråd mener det kan være vanskelig for deres medlemmer å skille arbeids- og ansvarsområdene til de ulike aktørene, som Senter for informasjonssikring, Varslingssystem for digital infrastruktur, Koordineringsutvalget for informasjonssikkerhet, BAS-5 osv. Når det gjelder kontaktpunkt i det offentlige, er Næringslivets Sikkerhetsråd opptatt av den strafferettslige siden ved IT-sikkerhet, der bedriftene gjør eller blir utsatt for straffbare handlinger. I forebyggingsarbeidet er medlemmene ofte i tvil om hvor de skal henvende seg med problemstillingene. Har man oppdaget et alvorlig straffbart forhold ved bruk av egne systemer, kan det være vanskelig å eksponere svakhetene eller forholdet i dialog med kontrolletater.

Tekstboks 4

Flere land har problemer med å samordne og koordinere arbeidet med informasjonssikkerhet. Den svenske Krisberedskapsmyndigheten tar i en rapport opp at det er et stort behov for å forsterke samordningen av arbeidet med informasjonssikkerhet og gjøre ansvarsfordelingen tydeligere på både departements- og direktoratsnivå.

Den amerikanske riksrevisjonen (GAO) har også tatt opp behovet for en mer koordinert og samlet tilnærming til arbeidet med å beskytte kritisk IT-infrastruktur. En undersøkelse i 2002 viste at det var mer enn 50 føderale organisasjoner som hadde nasjonale eller koordinerende roller på dette området. Revisjonsrapporten etterlyste en strategi som identifiserer hvor ansvaret ligger for alle tiltak som skal sikre IT-infrastrukturen, og en klargjøring av forbindelsene mellom tiltakene. Department of Homeland Security ble opprettet bl.a. for å samle og klargjøre ansvaret også for IT-sikkerhetsarbeidet. I en rapport fra 2005 påpeker GAO at det fortsatt er problemer knyttet til at departementet har manglende autoritet og lite organisatorisk stabilitet, og at det har problemer med å etablere effektivt samarbeid med andre virksomheter i privat og offentlig sektor.

Kilde: Se vedlegg 1.

Finansiering av tverrsektorielle tiltak

Både Post- og teletilsynet, Nasjonal sikkerhetsmyndighet og DSB har pekt på problemene med å få finansiert tverrsektorielle tiltak innenfor IT-sikkerhet. Også Moderniseringsdepartementet har gitt uttrykk for at det er vanskelig å innhente midler til fellestiltak når midlene ikke er øremerket for dette formålet, men har uttalt at finansiering av tiltak for informasjonssikkerhet ikke skiller seg fra andre områder.[76] Finansdepartementet understreket at det ikke var aktuelt å tildele friske midler til å gjennomføre tiltakene i Nasjonal strategi for informasjonssikkerhet, og at tiltakene dermed skulle gjennomføres og finansieres innenfor de til enhver tid gjeldende budsjettrammer for hver enkelt offentlig virksomhet.[77] Justis- og politidepartementet mener at finan-

75) Referat fra møte mellom KIS og Næringslivets Sikkerhetsråd 24. august 2004

76) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

77) Brev av 5. september 2005 fra Moderniseringsdepartementet til Riksrevisjonen

siering av tverrdepartementale tiltak alltid er en utfordring, men at dagens finansieringsopplegg innen IT-sikkerhet bidrar til ansvarliggjøring og gjør eierskapet og forankringen tydelig.[78] Samferdselsdepartementet har pekt på at virksomhetene har begrensede midler til bruk i spleiselag, og at det kan være tidkrevende å få finansiert tverrsektorielle IT-sikkerhetstiltak.[79]

4.2.2 Er ansvarsforholdene avklart på departementsnivå?

De intervjuede departementene understreker at alle virksomheter har ansvar for IT-sikkerheten innenfor sitt ansvarsområde. Moderniseringsdepartementet peker på at den enkelte bruker må ha ansvar for sikkerheten i eget system, leverandørene har ansvar for at systemet har tilstrekkelig funksjonalitet når det gjelder sikkerhet, mens offentlig sektor har ansvar for den samfunnskritiske infrastrukturen. Grensedragningen for ansvar for IT-sikkerhet er vanskelig og må i mange tilfeller styres av hva som er hensiktsmessig, men alle inndelinger vil uansett ha noen svakheter. Moderniseringsdepartementet framhever at fordelingen av ansvar for informasjonssikkerhet har vært og fortsatt er i en prosess.[80]

Ansvar for kritisk infrastruktur

Moderniseringsdepartementet har i møte med Riksrevisjonen uttalt at det er diskusjoner mellom Moderniseringsdepartementet og Justis- og politidepartementet om ansvaret for kritisk infrastruktur. Mens departementene tidligere var enige om at Justis- og politidepartementet har ansvaret for kritisk infrastruktur, og at det er unaturlig å ekskludere IT fra denne infrastrukturen, har Justis- og politidepartementet nå stilt spørsmål ved denne ansvarsfordelingen. Det er derfor ifølge Moderniseringsdepartementet et reelt behov for å tydeliggjøre ansvarskartet.[81] Justis- og politidepartementet har i møte med Riksrevisjonen påpekt at departementets samordnings- og tilsynsansvar for samfunnets sikkerhet inkluderer beredskap i kritisk infrastruktur.[82] Justis- og politidepartementet har videre presisert at ansvaret for kritisk infrastruktur i henhold til ansvarsprinsippet ligger hos eieren eller operatøren av den kritiske infrastrukturen, og at ansvaret for kritisk infrastruktur således ikke er skilt ut som et eget fagområde løsrevet fra det øvrige ansvaret innenfor en sektor.[83] Ifølge Samferdselsdepartementet har det også vært enkelte diskusjoner på departementsnivå om Justis- og politidepartementets ansvar for IT-sikkerhet i en krisesituasjon.[84]

Statskonsult sier i en evalueringsrapport: ”Det er vårt inntrykk at Justis- og politidepartementet og DSB foreløpig ikke i særlig grad har orientert seg i retning av IKT og informasjonssikkerhet i forhold til samfunnssikkerhet og beredskap. [..] Det finnes såvidt vi vet heller ikke mye kompetanse, foreløpig, på IKT og informasjonssikkerhet i Justis- og politidepartementet eller DSB.”[85]

Forsvarsdepartementet sier at det til tider kan synes som om ansvarsforholdet i sivil sektor er noe uklart. Departementet trekker fram som eksempel grensen mellom Justis- og politidepartementets sektorovergripende ansvar for samfunnssikkerhet og Moderniseringsdepartementets fagansvar.[86]

Nasjonal sikkerhetsmyndighet rapporterer til Forsvarsdepartementet i militær sektor og til Justis- og politidepartementet i sivil sektor. Alle oppdrag til Nasjonal sikkerhetsmyndighet gis av Forsvarsdepartementet som etatsstyrende departement. Det er utarbeidet retningslinjer for gjennomføringen av etatsstyringen, og disse presiserer ytterligere hva Forsvarsdepartementets ansvar for å sikre en klar rollefordeling mellom Forsvarsdepartementet og Justis- og politidepartementet innebærer. Ifølge Justis- og politidepartementet er det er en tett dialog mellom de to departementene for å koordinere oppgavene til Nasjonal sikkerhetsmyndighet, og de har ti samordningsmøter i året. Justis- og politidepartementet deltar også i arbeidet med å utarbeide iverksettelsesbrevet til Nasjonal sikkerhetsmyndighet.[87]

Ansvar for Internett

Samferdselsdepartementet har ansvar for forhold som er underlagt ekomloven, herunder Internett. Moderniseringsdepartementet oppfatter det slik at loven og Samferdselsdepartementets ansvar først og fremst dreier seg om fysiske nett og levering av kommunikasjon. Moderniseringsdepartementet mener at tjenester, produkter og anvendelser som bygger videre på dette grunnlaget, faller utenfor Samferdselsdepartementets ansvarsområde, og at Moderniseringsdepartementet her har et koordineringsansvar. Moderniseringsdepartementet har en løpende dialog med Samferdselsdepartementet om ansvarsfordelingen. Ifølge Moderniseringsdepartementet har Samferdselsdepartementet tatt noen initiativ når det gjelder sikkerhet, og Moderniseringsdepartementet støtter disse.

78) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen 15. mars 2005

79) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

80) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

81) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

82) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen 15. mars 2005

83) Brev fra Justis- og politidepartementet til Riksrevisjonen av 2. september 2005

84) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

85) Rapport fra evalueringen av ordningen for sertifisering av IT-sikkerhet i produkter og systemer. Statskonsult, 1. oktober 2004. Side 27

86) Brev fra Forsvarsdepartementet til Riksrevisjonen av 8. april 2005

87) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen 15. mars 2005

Departe-mentet ser imidlertid at det utenfra kanskje kan virke uryddig at flere departementer tar ulike initiativ som kan synes nært beslektet.[88]

Samferdselsdepartementet mener at deres ansvar for all elektronisk kommunikasjon, herunder Internett, kom tydeligere fram etter at ekomloven i 2003 erstattet teleloven. Internett og all elektronisk kommunikasjon er en del av Samferdselsdepartementets sektoransvar, noe som også medfører et ansvar for helheten innenfor IT-sikkerhet. Gjennom ekomloven og Post- og teletilsynet har Samferdselsdepartementet tilgang til virkemidler som kan benyttes innenfor IT-sikkerhet. Moderniseringsdepartementet har som koordinator av IT-politikken og dermed også IT-sikkerheten ansvar for Senter for informasjonssikring, men har ifølge Samferdselsdepartementet få andre direkte virkemidler innenfor IT-sikkerhet. Etter Samferdselsdepartementets mening medfører dette at Samferdselsdepartementet og Post- og teletilsynet har lettere for å få gjennomført tiltak på området enn Moderniseringsdepartementet.[89]

Kontakt med næringslivet
Før omorganiseringen av departementsstrukturen i juni 2004 lå ansvaret for kontakt med næringslivet om IT-sikkerhet i sin helhet hos Nærings- og handelsdepartementet. Ved omorganiseringen ble Avdeling for IT-politikk flyttet fra Nærings- og handelsdepartementet til Moderniseringsdepartementet. Ansvarsfordelingen mellom de to departementene ble ifølge Moderniseringsdepartementet ikke avklart på dette tidspunktet. I et møte 4. april 2005 ble de to departementene enige om at Moderniseringsdepartementet skal ha pådriveransvar for alle tiltakene i Nasjonal strategi for informasjonssikkerhet som retter seg mot eller inkluderer næringslivet. De ble videre enige om at Nærings- og handelsdepartementet skal bistå Moderniseringsdepartementet i de tilfeller der det anses å være formålstjenlig.[90] Nærings- og handelsdepartementet har ifølge Moderniseringsdepartementet våren 2005 opprettet en seksjon som har ansvar for bl.a. å følge opp bruken av IT i næringslivet.[91]

4.2.3 Er fagorganenes ansvar avklart?
St.meld. nr. 17 (2001–2002) påpeker at ansvarsforholdene mellom Senter for informasjonssikring, Varslingssystem for digital infrastruktur (VDI), Post- og teletilsynet og Nasjonal sikkerhetsmyndighet vil bli vurdert.[92] I St.prp. nr. 1 (2002–2003) for Justis- og politidepartementet heter det at det er svært viktig å etablere gode samarbeidsformer mellom prøveprosjektene Senter for informasjonssikring og VDI, samt Politiets datakrimsenter.[93] St.meld. nr. 39 (2003–2004) *Samfunnssikkerhet og sivilt-militært samarbeid* gir en beskrivelse av de ulike organenes oppgaver, og viser til at det er etablert et samarbeid mellom VDI og Senter for informasjonssikring. Ansvarsforholdene mellom de øvrige organene er i liten grad beskrevet.

Formelle avklaringer
Undersøkelsen viser at det er inngått en del samarbeidsavtaler mellom de ulike fagorganene de siste årene:

- Samarbeidsavtalen mellom DSB og Nasjonal sikkerhetsmyndighet fra juni 2004 regulerer informasjonsutveksling og samarbeid om tilsyn, forskningsprosjekter og brukerundersøkelser.
- Samarbeidsavtalen mellom Nasjonal sikkerhetsmyndighet og Senter for informasjonssikring fra januar 2003 klargjør bl.a. virksomhetenes ulike roller og inneholder punkter om gjensidig utveksling av informasjon.
- Samarbeidsavtalen mellom Nasjonal sikkerhetsmyndighet/VDI og Økokrim/Politiets datakrimsenter gjelder primært faglig samarbeid om teknologi og metodikk som underlag for de respektive organisasjonenes egen oppgaveløsning. Avtalen skulle vare ut 2004, og det arbeides nå med en oppdatering/justering av avtalen. I forlengelsen av avtalen er det opprettet et faglig samarbeidsforum med månedlige møter mellom Politiets datakrimsenter og VDI. Dette forumet planlegges videreført i den nye avtalen.

Det er ikke etablert noen skriftlig avtale mellom Post- og teletilsynet og Senter for informasjonssikring eller mellom Post- og teletilsynet og Nasjonal sikkerhetsmyndighet.

Vurderinger av samarbeidet [94]
Nasjonal sikkerhetsmyndighet vurderer oppgavedelingen og ansvarsforholdene mellom VDI og Politiets datakrimsenter som uproblematiske og avklart. Det er også etablert samarbeid på flere nivåer mellom Nasjonal sikkerhetsmyndighet og DSB: I tillegg til regelmessige møter mellom ledelsen i de to direktoratene har det vært møter mellom direktoratene om deres tilsynsarbeid. Direktoratenes tilsyn samordnes nå gjennom kjennskap og tilpasning til det andre direktoratets planer, men det er foreløpig ikke vurdert som relevant å gjennomføre felles tilsyn. Koordineringen er ifølge direktoratene viktig for å unngå at en virksomhet blir utsatt for to tilsyn samtidig. Spørsmålet om graden av samordning må imidlertid vurderes fortløpende etter som man får mer erfaring med slike tilsyn.

88) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

89) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

90) Brev fra Moderniseringsdepartementet til Riksrevisjonen av 18. april 2005

91) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

92) Punkt 6.2.4 i meldingen

93) Side 115 i meldingen

94) Avsnittene bygger på virksomhetenes svar på Riksrevisjonens spørrerunde i februar 2005.

Det er som nevnt ovenfor ikke etablert noen skriftlig avtale mellom Post- og teletilsynet og Senter for informasjonssikring eller mellom Post- og teletilsynet og Nasjonal sikkerhetsmyndighet. Nasjonal sikkerhetsmyndighet har som mål å få på plass en avtale med Post- og teletilsynet i 2005. Til tross for manglende avtale foregår det noe samarbeid mellom disse organene: Senter for informasjonssikring peker på at senteret har samarbeidet med Post- og teletilsynet om Internett-portalen nettvett.no, som ble lansert 26. april 2005, og at senteret har tilgang til noen sikkerhetsfora som styres av tilsynet. Post- og teletilsynet mener det har en kontinuerlig dialog, først og fremst med Nasjonal sikkerhetsmyndighet, bl.a. ved at begge parter er representert i Koordineringsutvalget for informasjonssikkerhet. Nasjonal sikkerhetsmyndighet/VDI deltar dessuten i referansegruppen for prosjektgruppen Nettvett og i en arbeidsgruppe under Post- og teletilsynet.

Senter for informasjonssikring og Post- og teletilsynet peker på at de manglende avklaringene mellom de tre virksomhetene kan ha sammenheng med spørsmålet om hvor en nasjonal CERT skal lokaliseres. Alle de tre aktørene er mulige kandidater. Dette støttes av utsagn fra Nasjonal sikkerhetsmyndighet som i forbindelse med utvikling av en CERT-funksjon (se punkt 5.1.4) har prøvd å etablere fungerende kontaktpunkter i Post- og teletilsynet, med tanke på håndtering av sårbarhetsinformasjon og kritiske hendelser. Post- og teletilsynet har ifølge Nasjonal sikkerhetsmyndighet ikke fulgt opp deres henvendelse.

Samferdselsdepartementet mener at ansvarsfordelingen mellom de tre virksomhetene (Post- og teletilsynet, Senter for informasjonssikring og Nasjonal sikkerhetsmyndighet) er klar, og at samarbeidet mellom Post- og teletilsynet og Nasjonal sikkerhetsmyndighet/VDI fungerer godt. Departementet peker imidlertid på at de delvis arbeider mot de samme målgruppene, så noe overlapping kan forekomme.

4.2.4 Samordning av regelverk

Det foreligger en rekke regelverk med bestemmelser som er relevante for informasjonssikkerhet. Ved endringer i regelverk de senere årene har myndighetene diskutert samordning av forskjellige regelverk.

Det er gjort forsøk på å samordne regelverk også ved en rekke tidligere anledninger, helt tilbake til 1980-tallet.[95] I 1981 la Justisdepartementet fram et utkast til forskrift om sikringstiltak ved anlegg for drift av personregistre. I høringsuttalelser til dette forslaget tok flere instanser opp behovet for samordning med daværende datasikkerhetsdirektiv, sikkerhetsinstruks og beskyttelsesinstruks. Reglene ble ikke vedtatt.

95) Jf. omtale i Samordning av regelverk for beskyttelse av informasjon, en rapport fra en arbeidsgruppe nedsatt av Forsvarsdepartementet, Justisdepartementet og Arbeids- og administrasjonsdepartementet, desember 1991

Scanpix Creative/Masterfile

Behovet for å samordne regler ble også tatt opp i NOU 1986:12 *Datateknikk og samfunnets sårbarhet*. På bakgrunn av blant annet ovennevnte innspill nedsatte regjeringen i 1990 et utvalg som hadde til formål å utarbeide et felles regelverk for sikring av data. Arbeidet skulle ta utgangspunkt i datasikkerhetsdirektivet og utkastet til sikringsforskrift for personregistre. Utvalget la fram sin rapport med forslag til et samlet regelverk i desember 1991.[96] Forslaget møtte stor motstand, og de berørte departementene ble enige om at samordningsbehovet ikke skulle ivaretas gjennom et felles regelverk.[97] I stedet ble det besluttet at behovet for samordning skulle ivaretas ved å opprette et tverrdepartementalt råd: Rådet for IT-sikkerhet. Senere er det kommet separate regelverk på området, bl.a. sikkerhetsloven og personopplysningsloven og regelverk utledet av disse.

Etatenes vurdering av regelverket

Post- og teletilsynet mener at forhold ved regelverket vanskeliggjør samordningen av IT-sikkerhetsarbeidet. Tilsynet viser til at dette for eksempel gjelder i forholdet mellom spesifikke sektorreguleringer og sikkerhetsloven med forskrifter.[98] Post- og teletilsynet uttaler at mange av de administrative problemene knyttet til ansvarsforhold bunner i et til dels sprikende regelverk. Samferdselsdepartementet vurderer sikkerhetsloven som

96) Samordning av regelverk for beskyttelse av informasjon, en rapport fra en arbeidsgruppe nedsatt av Forsvarsdepartementet, Justisdepartementet og Arbeids- og administrasjonsdepartementet, desember 1991

97) Omtalt i Ot.prp. nr. 49 (1996–97) Om lov om forebyggende sikkerhetstjeneste, pkt. 7.3.2 og St. meld. nr. 27 (1995–96), side 7

98) Svar på Riksrevisjonens spørreliste fra Post- og teletilsynet av 25. februar 2005

delvis overlappende i forhold til ekomlovens bestemmelser, fordi sikkerhetsloven kan sette krav til sikkerhetstiltak også for private aktører. Dette kan medføre diskusjoner rundt hvem som skal betale for tiltakene, jf. også bestemmelse om finansiering i ekomlovens § 2-10.[99]

Datatilsynet mener at i den grad det er behov for klargjøring av ansvar, bør klargjøringen omfatte det å skape et enhetlig regelverk.[100] Tilsynet peker på at det dessverre er slik at hver etat utvikler sine regelverk innen informasjonssikkerhet etter de prinsippene den enkelte etaten finner hensiktsmessig. Det å utarbeide et enhetlig regelverk synes derfor å være en riktig vei å gå for å fremme en optimalisering av myndighetsutøvelsen. Datatilsynet synes det er klare behov for å foreta grep for å legge til rette for en styrket samordning, og tilsynet har i dialog med andre etater som har foretatt regelverksutvikling, pekt på behovet for å styrke samordningen av regelverk. De fleste etatene tufter regelverket sitt på et internasjonalt fundament. Problemet er imidlertid ifølge Datatilsynet at det er ulike preferanser når det gjelder hvilket fundament dette skal være. Datatilsynet mener det er ønskelig å lande på et felles fundament.

Nasjonal sikkerhetsmyndighet peker på at Norge gjennom sitt medlemskap i NATO er forpliktet til å håndtere NATO-informasjon i henhold til organisasjonens krav.[101] Tilsvarende er Norge gjennom en rekke bilaterale sikkerhetsavtaler forpliktet til å beskytte andre nasjoners graderte informasjon. I avtalene forutsettes det at Norges regelverk er basert på, og tilfredstiller, visse internasjonalt definerte standarder. IT-sikkerhet er ett av områdene der det stilles krav til Norge, og det forutsettes i dag at sikkerhetsloven ivaretar disse kravene. Nasjonal sikkerhetsmyndighet er opptatt av at slike internasjonale forpliktelser fortsatt må ivaretas ved en eventuell samordning av arbeidet med IT-sikkerhet.

DSB mener at regelverket bør gi tydelige krav til minimum sikkerhet på tvers av sektorene.[102] Samtidig framhever direktoratet at det er viktig å få til et regelverk som framstår mest mulig ryddig, enkelt og hensiktsmessig for brukerne.

Betydningen av samordnet regelverk for næringslivet
Privat næringsliv har ifølge Moderniseringsdepartementet ofte behov for å finne ut hvilket regelverk som gjelder, og hvilket forvaltningsorgan som er ansvarlig for ulike regelverk for IT-sikkerhet. Departementet viser til at IT-sikkerhetsforum, som er et forum for private bedrifter, har utført en undersøkelse der de påpeker at regelverkene samlet sett ikke alltid er entydige.[103]

IKT-Norge påpeker at manglende samordning av regelverket bidrar til et lite oversiktlig myndighetsbilde og uklare kontaktpunkter for næringen.[104] Abelia slutter seg til dette og uttaler at dette naturligvis er et stort problem for en bedrift som er underlagt ulike regelverk.[105] Abelia mener at noe av årsaken til uklarheten sannsynligvis ligger i at regelverket og de underliggende myndighetsorganene henger igjen i en tid der 1) IT og sikkerhet var to forskjellige verdener og 2) IT, tele og kringkasting var helt forskjellige verdener. I dag kunne man ifølge Abelia sannsynligvis hatt mer generelle lover og regler – og et utvidet ansvar for bedriftene til å bestemme hvordan man skal gjennomføre kravene som er satt.

Senter for informasjonssikring uttaler også at regelverket kan vanskeliggjøre samordningen av arbeidet med IT-sikkerhet.[106] Senteret trekker fram forskrifter fra Datatilsynet og Kredittilsynet som eksempel: Det ene settet er bygget på BS7799, mens det andre er bygget på COBIT.[107] Dette skaper problemer for virksomheter som skal legge fram dokumentasjon ved tilsyn. Senter for informasjonssikring mener at ettersom Nasjonal strategi for informasjonssikkerhet ønsker å fremme sertifisering etter BS7799, bør alle statlige kravdokumenter legge denne standarden til grunn.

Tiltak for samordning av regelverk
I Nasjonal strategi for informasjonssikkerhet er ett av fire overgripende mål at regelverket knyttet til informasjonssikkerhet skal håndheves og utvikles på en samordnet og for brukerne enkel og oversiktlig måte. Som en oppfølging av dette nedsatte Koordineringsutvalget for informasjonssikkerhet (KIS) vinteren 2005 en arbeidsgruppe for regelverksgjennomgang. Ifølge mandatet av 24. februar 2005 skal gruppen:

- skaffe til veie oversikt over regelverk med betydning for informasjonssikkerheten
- peke på mulige problemområder med hensyn på mangler, overlappinger og/eller motsetninger, samt etterlevbarhet av eksisterende regelverk. Brukere/regelverksforvaltere/tilsynsmyndigheter bør konsulteres.
- utarbeide anbefalinger for hvordan de identifiserte problemområdene kan angripes på kort og lang sikt
- presentere resultatene/anbefalingene for KIS, som drøfter videre oppfølging

99) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

100) Svar på Riksrevisjonens spørreliste fra Datatilsynet av 28. februar 2005

101) Svar på Riksrevisjonens spørreliste fra Nasjonal sikkerhetsmyndighet av 23. februar 2005

102) Svar på Riksrevisjonens spørreliste fra DSB av 1. mars 2005

103) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

104) Svar på Riksrevisjonens spørreliste fra IKT-Norge av 28. februar 2005

105) Svar på Riksrevisjonens spørreliste fra Abelia av 4. mars 2005

106) Svar på Riksrevisjonens spørreliste fra Senter for informasjonssikring av 28. februar 2005

107) COBIT er en forkortelse for Control Objectives for Information and related Technology, et rammeverk utgitt av The IT Governance Institute. Se omtale av BS7799 under punkt 5.2.3.

Prosjektet skal være ferdig 3. juni 2005, og det skal samtidig avlevere en rapport til sekretariatet for KIS. Ifølge Justis- og politidepartementet er det snakk om et forprosjekt. Forprosjektet skal vurdere hvordan man skal arbeide videre med samordning og avklaringer rundt regelverket. Det er i Moderniseringsdepartementets handlingsplan av mai 2005 lagt opp til en videreføring av regelverksarbeidet ut 2006.

4.3 Planlegging og gjennomføring

Justis- og politidepartementet, Forsvarsdepartementet og Nærings- og handelsdepartementet ble i slutten av 2002 enige om å utvikle en nasjonal strategi. Denne skulle være forankret i en oppfølging av tidligere utredninger om informasjonssikkerhet, og skulle ses i sammenheng med St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet.*[108]

Strategien ble utarbeidet som et prosjekt med en styringsgruppe ledet av Justis- og politidepartementet. Gruppen hadde representanter fra Finansdepartementet, Arbeids- og administrasjonsdepartementet, Forsvarsdepartementet, Helsedepartementet, Sosial- og helsedirektoratet, Nærings- og handelsdepartementet, Olje- og energidepartementet, Norges vassdrags- og energidirektorat, Sosialdepartementet, Samferdselsdepartementet og Statsministerens kontor. I tillegg var Forum for IT-sikkerhet referansegruppe for prosjektet. Regjeringens nasjonale strategi for informasjonssikkerhet forelå i juni 2003.[109]

Strategien er først og fremst myntet på myndigheter, næringsliv og organisasjoner, men vil også kunne være relevant for enkeltpersoner. Strategien består av tolv overordnede/prioriterte punkter/tema med en rekke tilknyttede tiltak, der det er utpekt én eller flere gjennomføringsansvarlige. Ansvaret er først og fremst plassert i sentrale departementer som Nærings- og handelsdepartementet, Justis- og politidepartementet, Forsvarsdepartementet og Samferdselsdepartementet, og underliggende etater som Post- og teletilsynet, Nasjonal sikkerhetsmyndighet og DSB, men sektordepartementene har fått ansvar for tiltak som spesielt berører deres ansvarsområder. For noen tiltak er bransjeorganisasjoner som Abelia og IKT-Norge tillagt et gjennomføringsansvar. Hver enkelt sektor er forutsatt å lage en handlingsplan som skal brukes for å realisere strategien.[110]

4.3.1 Oppfølging av Nasjonal strategi for informasjonssikkerhet

Utarbeidelse av handlingsplaner

Nasjonal strategi for informasjonssikkerhet ble lagt fram i juni 2003. I desember samme år ba Nærings- og handelsdepartementet de berørte departementene om å sende inn oppfølgingsplaner for sine ansvarsområder.[111] De mest berørte departementene utarbeidet handlingsplaner vinteren 2004.

Justis- og politidepartementet og Forsvarsdepartementet hadde på dette tidspunktet koordinert sine oppfølgingsplaner. Også Samferdselsdepartementet og Nærings- og handelsdepartementet utarbeidet planer. Arbeids- og administrasjonsdepartementet, med bistand fra Statskonsult, arbeidet vinteren 2004 med en handlingsplan for å bedre informasjonssikkerheten i offentlig sektor. Dette arbeidet er fulgt opp av Moderniseringsdepartementet gjennom departementets reviderte handlingsplan fra mars 2005, senere oppdatert i mai 2005. Den reviderte planen er sammensatt av delplaner for Arbeids- og administrasjonsdepartementet og Nærings- og handelsdepartementet.

Strategien hadde et tidsperspektiv på to–tre år da den ble lagt fram i juni 2003, men den ga i liten grad informasjon om når det forventes at tiltak eller enkeltaktiviteter knyttet til tiltak skal være gjennomført. En gjennomgang av handlingsplanene viser at det for enkelte tiltak er oppgitt sluttdato. For en rekke tiltak er sluttidspunkt ikke definert, eller oppgaven er definert som ”løpende” eller ”gjennomføres i 2005/2006”. Enkelte tiltak var imidlertid iverksatt eller avsluttet vinteren 2004. Dette har bl.a. sammenheng med at strategien, i tillegg til å foreslå nye tiltak, også oppsummerte tiltak som allerede var igangsatt innenfor IT-sikkerhet.

Handlingsplanene angir i liten grad hvilke tiltak som har høyest prioritet. I Nærings- og handelsdepartementets plan fra 2004 og Moderniseringsdepartementets plan fra 2005 finnes en prioritering fra 1 (høyest) til 4 (lavest), men slike vurderinger finnes i liten grad i de øvrige handlingsplanene. Planene angir ikke kostnader og behovet for ressurser og heller ingen nytte–kostnadsvurderinger. Ifølge Moderniseringsdepartementet er det forutsatt at de ansvarlige for tiltakene i strategien gjennomfører en nytte–kostnadsvurdering før iverksettelse. Moderniseringsdepartementet kunne eventuelt ha laget generelle retningslinjer for dette arbeidet, men departementet har foreløpig vurdert det som lite hensiktsmessig ettersom det er meget stor variasjon i tiltaksstørrelse og -type.[112]

108) Grunnlagsdokument for Nasjonal strategi for informasjonssikkerhet, datert 21. oktober 2002

109) Forsvarsdepartementet, Nærings- og handelsdepartementet, Justis- og politidepartementet: Nasjonal strategi for informasjonssikkerhet. Utfordringer, prioriteringer og tiltak. Juni 2003

110) Nasjonal strategi for informasjonssikkerhet. Juni 2003

111) Brev fra Nærings- og handelsdepartementet til berørte departementer datert 19. desember 2003

‹12) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

Strategien forutsetter at tiltakene skal finansieres av de ansvarlige departementene, eventuelt i samarbeid med privat sektor. Det er ikke nærmere angitt i handlingsplanene hvordan finansieringsansvaret skal fordeles.

I handlingsplanene er det ikke satt opp resultatkriterier som gjør det mulig å måle effekten av de enkelte tiltakene eller av flere tiltak samlet.

Samordning av oppfølgingen
Arbeidet med å følge opp den nasjonale strategien ble fra mai 2004 tillagt Koordineringsutvalget for informasjonssikkerhet (KIS). Sekretariatet for KIS fører nå en løpende statusoversikt over tiltakene i handlingsplanene. Formålet med denne oversikten er å gi medlemmene en felles forståelse av hva som er status, og å identifisere tiltak/oppfølging som krever koordinering mellom ulike myndigheter.[113]

Med unntak av Moderniseringsdepartementets handlingsplan fra mars 2005 har ikke departementene framlagt reviderte planer i 2005. Det ble gjennomført en oppsummerende statusrunde ved møtet i KIS mai 2005. Denne runden resulterte i en ny statusoversikt som ikke er vesentlig mer detaljert enn tidligere oversikter og planer. Den gir bl.a. følgende statusangivelser for tiltakene: ukjent, ikke påbegynt, pågående, ferdigstilt. Moderniseringsdepartementet har fortsatt et oppfølgingsansvar på overordnet nivå, men påpeker at KIS kan brukes til å presse departementene til å være tilstrekkelig konkrete i sine handlingsplaner.[114]

Sekretariatet for KIS har ifølge Moderniseringsdepartementet en ressursramme på ett årsverk. Dette anser Moderniseringsdepartementet som et minimum, og man er usikker på om dette er tilstrekkelig på lengre sikt. Dersom deltakerne stiller med en god del egeninnsats slik det er forventet, anses dette allikevel for å kunne være nok. Samferdselsdepartementet har pekt på at Moderniseringsdepartementet som leder av gruppen har begrensede virkemidler å benytte i arbeidet.[115] Justis- og politidepartementet mener KIS har tilstrekkelig ressurser til koordineringsarbeidet, siden det er de deltakende departementene og etatene som skal gjøre jobben.[116]

Evaluering av arbeidet
Spørsmålet om evaluering av strategien ble tatt opp i møte med Nærings- og handelsdepartementet i oktober 2003. Departementet viste til avtale med Statistisk sentralbyrå (SSB) om å inkorporere relevante spørsmål om informasjonssikkerhet i SSBs ordinære undersøkelser innen IT-området. Disse undersøkelsene vil kunne gi et bilde av situasjonen i privat, kommunal og statlig sektor. Nærings- og handelsdepartementet opplyste at også mørketallsundersøkelsene kunne gi grunnlag for å evaluere strategien, og at gallupundersøkelser kan gi innblikk i situasjonen på området.[117] Også tilsynsrapporter fra fagmyndighetene kan si noe om tilstanden i ulike virksomheter. Noen av disse kildene er brukt i denne undersøkelsen for å belyse sikkerhetstilstanden på utvalgte områder.

Ut fra de ovennevnte kildene mente Nærings- og handelsdepartementet at man kunne skape et grunnlag for å foreta en generell vurdering av strategiens effekt, samt vurdere på hvilke områder sikkerheten er tilfredsstillende, og på hvilke områder det er behov for tiltak. Moderniseringsdepartementets handlingsplan fra mai 2005 synes ikke å ha fulgt opp dette videre i konkrete planer om å framskaffe statusoversikter.

I møte med Moderniseringsdepartementet i mars 2005 ble spørsmålet om evalueringer tatt opp på nytt. Moderniseringsdepartementet påpekte da at man foreløpig ikke har diskutert hva som skal skje med Nasjonal strategi for informasjonssikkerhet når virkeperioden formelt utløper ved utgangen av 2005. Noen av tiltakene i strategien vil da fremdeles være under gjennomføring og forventes å løpe utover denne tidsgrensen. Tilsvarende tema ble tatt opp i møte med Justis- og politidepartementet, som uttaler at man foreløpig ikke har diskutert evaluering og videreføring av strategien, men fokusert på å gjennomføre tiltakene i strategien. Justis- og politidepartementet uttaler at på møtene i KIS rapportertes det som er gjort, men ikke i særlig grad oppgaver og planer framover.[118]

DSB har opplyst at OECD vil gjennomføre en case-studie av IT-sikkerhet i Norge som en del av OECD-studien *The OECD Futures Project on Risk Management Policies*. OECD-studien er et samarbeid mellom OECD og flere land om policy innenfor samfunnssikkerhet. DSB deltar fra Norge. Formålet med hovedprosjektet er å definere en policy for risikoledelse på tvers av OECD-landene.[119] Case-studien gjennomføres i 2005, og innebærer bl.a. en gjennomgang av arbeidet med IT-sikkerhet i Norge.[120]

4.3.2 Forholdet til næringslivet
I OECDs plan for iverksettelse av *Retningslinjer for sikkerhet i informasjonssystemer og nettverk* er det lagt

1113) Sekretariatet i KIS: Status i oppfølgingen og koordineringen av Nasjonal strategi for informasjonssikkerhet, per 12. november 2004

114) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

115) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

116) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen 15. mars 2005

117) Referat fra møte mellom Nærings- og handelsdepartementet og Riksrevisjonen 29. oktober 2003

118) Referater fra møter mellom Moderniseringsdepartementet og Riksrevisjonen og mellom Justis- og politidepartementet og Riksrevisjonen 15. mars 2005

119) Brev av 20. februar 2004 fra Justis- og politidepartementet til Nærings- og handelsdepartementet

120) E-post av 12. april 2005 med vedlegg fra DSB til Riksrevisjonen

vekt på at utviklingen av en sikkerhetskultur krever bred deltakelse fra alle styringsnivåer, næringsliv og det sivile samfunn.[121] Dette er også lagt til grunn i St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet*, der det i pkt. 6.2.4 heter at arbeidet med strategien skal søke å inkludere privat sektor. Koblingen til privat sektor er fulgt opp i strategien, der bransjeorganisasjoner er tillagt gjennomføringsansvar for enkelte tiltak. I tillegg legger strategien opp til å innlede en dialog med privat sektor med tanke på samfinansiering av enkelte av tiltakene.

Er næringslivet trukket med i oppfølgingen?
Som en del av undersøkelsen ble det i 2004 og i mars 2005 innhentet informasjon fra bransjeorganisasjoner som deltok i arbeidet med å utarbeide strategi og/eller står som ansvarlige for enkelttiltak.

Ifølge Abelia, IKT-Norge og Næringslivets sikkerhetsorganisasjon har det ikke vært noen diskusjon mellom myndighetene og dem om hva som forventes av oppfølging av strategien, og det er ikke etablert rutiner for samarbeid. IKT-Norge peker imidlertid på at de for enkelte tiltak har etablert et bra samarbeid med Post- og teletilsynet. Etter at strategien ble lagt fram, har organisasjonene ikke fått noen formell eller uformell tilbakemelding fra noen av departementene om gjennomføringen av tiltakene de har fått ansvar/delansvar for. IKT-Norge mener de deltok aktivt i prosessen med å utarbeide strategi, men er etterpå ikke blitt bedt om å koordinere sine oppgaver med andre. Organisasjonen savner en oppfølging fra de ansvarlige myndighetene.

Abelia og IKT-Norge uttaler at myndighetene heller ikke har tatt kontakt for å diskutere og avklare ressursbruk og finansiering av de enkelte tiltakene. IKT-Norge sier det har vært noe kontakt fra Samferdselsdepartementets side, men denne kontakten med næringen har vært rettet mot at bransjen skal bidra med penger til informasjonsarbeid. Abelia har i høringsuttalelser osv. hevdet at myndighetene har et stort problem ved at økonomiske forhold ikke er tatt alvorlig i strategien. Ifølge Abelia er det ikke gjort noe seriøst forsøk på å beregne kostnader, og organisasjonen mener at det heller ikke er gjort tilstrekkelig for å beskrive hva bedriftene skal betale selv av samfunnspålagte oppgaver, og hva staten skal dekke.

Abelia uttaler at de ikke vet hvordan myndighetene ligger an i gjennomføringen av strategien. Videre mener Abelia at strategien har en såpass generell og upresis karakter at det ikke er lett å måle status verken for Abelia eller for myndighetene. IKT-Norge påpeker at myndighetenes tempo/framdrift i arbeidet med å implementere strategien ikke har vært imponerende. Organisasjonen mener at man har fokusert lite på gjennomføringen av strategien, og uttaler i den forbindelse: "Det virket som om jobben var gjort da strategien ble presentert, men det var egentlig da jobben skulle begynne."

Tiltak fra departementenes side
I henhold til ansvarsfordelingen mellom departementene var det Nærings- og handelsdepartementet som hadde ansvar for å følge opp næringslivet. Departementet skulle hatt et møte med bransjeorganisasjonene om oppfølgingen av tiltakene i strategien sommeren 2004.[122] Dette møtet ble ifølge Moderniseringsdepartementet utsatt på grunn av omorganiseringen av departementsstrukturen. Møtet er tatt opp i Moderniseringsdepartementets nye handlingsplan, og er planlagt avholdt før sommeren 2005. Moderniseringsdepartementet mener at det er viktig å ha en dialog med næringslivet, og at det er uheldig at man ikke har kommet lenger med arbeidet overfor næringslivet. Departementet mener at omorganiseringen av departementene har ført til at ting ikke har gått så raskt som de burde. Ifølge Moderniseringsdepartementet kan den nåværende fokuseringen på PKI/elektronisk signatur også ha medført et skifte i ressursbruk fra generell/annen IT-sikkerhet over til PKI/elektronisk signatur.[123] (Jf. omtale av opprettelsen av portalen nettvett.no under punkt 5.2.2)

121) Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, punkt I-2 og I-3. Fra 2. juli 2003

122) Nærings- og handelsdepartementets handlingsplan fra 2004

123) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2004

5 Fakta: Sikring av samfunnskritisk IT-infrastruktur og utvikling av sikkerhetskultur

5.1 Beskyttelse av samfunnskritisk infrastruktur

Ett av regjeringens fire overordnede mål for informasjonssikkerhet er knyttet til beskyttelse av kritisk infrastruktur: "Samfunnskritisk infrastruktur for elektronisk informasjonsutveksling skal være robust og sikker i forhold til de trusler den utsettes for. Kritiske informasjonssystemer skal være sikret slik at skadevirkningene ved sikkerhetsbrudd ikke er større enn hva som kan defineres som akseptabel risiko."[124]

Ansvaret for beskyttelse av kritisk infrastruktur er som tidligere nevnt fordelt på de enkelte sektorene. Forsvarsdepartementet og Nasjonal sikkerhetsmyndighet har imidlertid et særskilt ansvar for å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Justis- og politidepartementet, med støtte fra Direktoratet for samfunnssikkerhet og beredskap (DSB), har et samordnings- og tilsynsansvar for samfunnets sikkerhet, også når det gjelder beredskap i kritisk infrastruktur.

Tekstboks 5

Britiske myndigheter ved National Infrastructure Security Co-ordination Centre sendte i juni 2005 ut advarsler om systematiske angrep fra hackere mot virksomheter som styrer kritisk infrastruktur i landet. Angrepene gjennomføres ved at det blir sendt e-post til utvalgte medarbeidere i berørte virksomheter. E-postene ser ut som de kommer fra kjente avsendere og inneholder tilsynelatende interessant informasjon. I realiteten installeres programvare som samler og sender ut konfidensiell informasjon fra virksomheten når noen trykker på vedlegg eller linker i e-postene. Tilsvarende angrep synes også å ha vært rettet mot kritisk infrastruktur i flere land, men det er ikke kjent om denne typen angrep har vært rettet mot kritisk infrastruktur i Norge.

I en rapport om sivil infrastruktur fra Forsvarets forskningsinstitutt (FFI) framgår det at man så langt ikke har sett omfattende angrep mot informasjonssystemer som styrer kritisk infrastruktur. FFI framhever imidlertid avhengigheten av informasjonsteknologi i den moderne økonomien, samtidig som flere nasjoner og til dels ikke-statlige aktører synes å være i ferd med å utvikle kapasiteter for angrep mot informasjonssystemer. I Norge antyder DSBs rapport etter strømbruddene i USA og Europa høsten 2003 at norsk kraftforsyning har vært utsatt for daglige dataangrep fra hackere.

Kilde: Se vedlegg 1.

124) Nasjonal strategi for informasjonssikkerhet, side 3

Gjennomgangen nedenfor fokuserer på følgende forhold:

- Er det klarlagt hvilken IT-infrastruktur som krever særlig beskyttelse?
- Hva gjør sentrale myndigheter for å redusere sårbarheten til kritisk IT-infrastruktur?
- I hvilken grad er det etablert systemer og rutiner for å fange opp trusler mot disse systemene?
- I hvilken grad er det etablert systemer for å håndtere alvorlige sikkerhetshendelser?

5.1.1 Oversikt over samfunnskritisk IT-infrastruktur

Har myndighetene oversikt over hva som er samfunnskritisk IT-infrastruktur?

Nasjonal strategi for informasjonssikkerhet definerer kritisk IT-infrastruktur slik: "Informasjonssystemer eller infrastruktur kan betegnes som kritiske dersom samfunnets, virksomheters eller individers funksjonsevne i stor grad påvirkes av svikt." Strategien påpeker at det er viktig å identifisere slike systemer og plassere dem på en skala etter hvor kritiske de er. Dette ses på som en forutsetning for å kunne gjennomføre risikovurderinger og implementere nødvendige tiltak.[125] I den nasjonale strategien er telenettet og IT-systemer innenfor bl.a. transport, energiforsyning og helsevesen brukt som eksempler på kritisk infrastruktur.

Fagorganene Nasjonal sikkerhetsmyndighet og Direktoratet for samfunnssikkerhet og beredskap bekrefter at myndighetene per i dag ikke har en klar, entydig oversikt over hva som er kritisk IKT-infrastruktur, og hvilke systemer denne består av.[126] Direktoratene viser til at bl.a. BAS-studiene har gitt verdifull informasjon som belyser problemstillingen, og til at spesielt prosjektet BAS-5 forventes å gi en del informasjon på området, jf. omtale av dette prosjektet nedenfor.

DSB viser også til det pågående arbeidet i Infrastrukturutvalget. Utvalget skal vurdere hvordan hensynet til rikets sikkerhet og vitale nasjonale interesser på best mulig vis kan ivaretas overfor virksomheter som ikke er offentlige.[127] Det skal bl.a. kartlegge virksomheter som

125) Nasjonal strategi for informasjonssikkerhet, side 12

126) Svar på Riksrevisjonens spørreliste fra Nasjonal sikkerhetsmyndighet av 23. februar 2005 og fra Direktoratet for samfunnssikkerhet og beredskap av 1. mars 2005

127) Jf. kongelig resolusjon av 29. oktober 2004: Etablering av utvalg for sikring av landets kritiske infrastruktur

antas å ha betydning for rikets sikkerhet og vitale nasjonale interesser, og de virkemidlene som i dag brukes for å sikre infrastruktur i virksomheter som ikke er offentlige. Utvalget skal avlegge rapport til Justis- og politidepartementet i januar 2006. DSB nevner at det i forbindelse med utvalgets arbeid er utarbeidet et dokument som drøfter hva som innholdsmessig ligger i begrepet kritisk infrastruktur.[128]

Nasjonal sikkerhetsmyndighet antar at årsaken til at en oversikt over samfunnskritisk IKT-infrastruktur ikke foreligger, kan være en kombinasjon av bl.a. utilstrekkelig forskning på området, få publiserte hendelser som kunne ha skapt et samfunnsmessig og politisk press, frykt for økonomiske og andre kostnader som følge av krav til sikring, samt at sikkerhetslovens objektsikkerhetsbestemmelser ikke er gitt materielt innhold ennå.[129]

DSB mener at det er viktig for den nasjonale sikkerheten at det er en kontinuerlig oversikt over kritisk IKT-infrastruktur både innenfor og mellom sektorene med sikte på å få prioritert nødvendige forebyggende og skadebegrensende tiltak.[130] Nasjonal sikkerhetsmyndighet uttaler at mangelfull oversikt gir en risiko for at den sikkerhetsmessige innsatsen og dermed ressursbruken rettes mot feil beskyttelsesmål. Nasjonal sikkerhetsmyndighet mener at kostbare sikkerhetstiltak kan bli etablert til ingen nytte i et slikt scenario. Direktoratet framhever videre at reelt samfunnskritisk IT-infrastruktur som ikke er klassifisert som dette, vil kunne ha en for dårlig defensiv sikkerhet og svak beredskap sett i forhold til de påkjenningene infrastrukturen med en viss sannsynlighet kan tenkes å bli utsatt for.

Uklarheten rundt hva samfunnskritisk infrastruktur består av, er også tatt opp av Senter for informasjonssikring.[131] Senteret uttaler at siden det ikke finnes noen oversikt som navngir virksomheter som omfattes, fører dette til at mange virksomheter ikke vet at de tilhører denne kategorien. Tiltakene som rettes mot kritisk infrastruktur, er ifølge senteret i mange tilfeller bare rettet mot den delen av virksomhetene som er av betydning for samfunnet. Avhengighet mellom virksomheter og systemer kan innebære svakheter i slike tilfeller.

Justis- og politidepartementet opplyser at man ikke har en klar, entydig og tverrsektoriell oversikt over hva som er samfunnskritisk IT-infrastruktur, men stiller spørsmål ved om dette er nødvendig. Hver enkelt sektor anses å ha relativt god oversikt over hvor "kritiske" IT-systemene innen deres sektor er, og departementet mener at forebyggende tiltak vil bli gjennomført av den enkelte sektor. Departementet påpeker også at innholdet i begrepet samfunnskritisk infrastruktur ikke er klart. [132]

Departementet viser for øvrig til at BAS-5-prosjektet vil kunne gi en overgripende oversikt over sårbarheten for IKT-infrastruktur.

Hvilke objekter er skjermingsverdige ifølge sikkerhetsloven?

Sikkerhetsloven med tilhørende forskrifter gir regler for håndtering av sikkerhetsgradert informasjon og objekter. Loven foreskriver sikkerhetstiltak som skal fjerne eller redusere sårbarhet mot trusler i form av spionasje, sabotasje og terrorhandlinger. Loven ble vedtatt av Stortinget 20. mars 1998 og trådte i kraft 1. juli 2001. Ved ikrafttredelse var det utarbeidet forskrifter om sikkerhetsadministrasjon, personellsikkerhet, sikkerhetsgraderte anskaffelser og informasjonssikkerhet.

Sikkerhetsloven har en egen bestemmelse (§ 17) om den enkelte virksomhets plikt til å beskytte skjermingsverdige objekter (av andre grunner enn å beskytte informasjonen knyttet til objektene).[133] Olje- og gassinstallasjoner, kraftforsyningsanlegg og telekommunikasjonsanlegg er eksempler på skjermingsverdige objekter. Det som defineres som skjermingsverdige objekter i sikkerhetslovens forstand, behøver ikke nødvendigvis å samsvare med hva som defineres som kritisk infrastruktur. De enkelte virksomhetene plikter å utpeke skjermingsverdige objekter som virksomheten eier eller på annen måte har kontroll over eller fører tilsyn med, bl.a. som et grunnlag for Nasjonal sikkerhetsmyndighets tilsynsvirksomhet overfor virksomhetene.[134]

Forsvarsdepartementet sendte den 8. april 1999 ut en orientering til alle departementene om arbeidet med objektsikkerhet, og anmodet om at mulige skjermingsverdige objekter ble identifisert innenfor ansvarsområdene til hvert enkelt departement. Få departementer ga utfyllende svar innen tidsfristen.[135] Forsvarsdepartementet nedsatte i juni 2000 en tverrdepartemental arbeidsgruppe som fikk som mandat å utarbeide et forslag til en forskrift om objektsikkerhet. Arbeidsgruppen avla sin rapport i mai 2002, og i august 2003 ble arbeidsgruppens forslag sendt ut på høring.

Arbeidsgruppens rapport konkluderte med at regulering av forebyggende objektsikkerhet i stor grad framsto

128) Svar på Riksrevisjonens spørreliste fra Direktoratet for samfunnssikkerhet og beredskap av 1. mars 2005

129) Svar på Riksrevisjonens spørreliste fra Nasjonal sikkerhetsmyndighet av 23. februar 2005

130) Svar på Riksrevisjonens spørreliste fra Direktoratet for samfunnssikkerhet og beredskap av 1. mars 2005

131) Svar på Riksrevisjonens spørreliste fra Senter for informasjonssikring av 28. februar 2005

132) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen den 15. mars 2005

133) Med skjermingsverdig objekt menes eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser, jf. sikkerhetsloven § 3.

134) Ot.prp. nr. 49 (1996–97), kapittel 11: Merknader til de enkelte paragrafer

135) Rapport fra arbeidsgruppe om objektsikkerhet: Forebyggende sikring av objekter mot terror- og sabotasjehandlinger, 24. mai 2002, punkt 2.1

som fragmentarisk.[136] Utover enkelte generelle regelverk var det innen en del sektorer gitt særlige bestemmelser i lover, forskrifter, instrukser eller andre hjemmelsdokumenter. Utformingen av bestemmelsene og kravene i dem varierte mellom sektorene.

Forsvarsdepartementet opplyser at høringsrunden avdekket en rekke innvendinger mot arbeidsgruppens forslag. Justis- og politidepartementet mente bl.a. at en forskrift om objektsikkerhet ikke burde gis før nødvendige endringer av sikkerhetsloven er på plass.[137] For å følge opp høringsrunden ble det opprettet en felles arbeidsgruppe med deltakelse fra Forsvarsdepartementet, Justis- og politidepartementet og Nasjonal sikkerhetsmyndighet. Arbeidsgruppen har foreslått endringer i sikkerhetsloven, og Forsvarsdepartementet forbereder forslag til lovendring. Forsvarsdepartementet opplyser at hovedårsaken til det lange tidsforløpet er at forskriftsforslagene som har blitt utarbeidet, har vist seg å forutsette endringer av loven.

Forsvarsdepartementet og Nasjonal sikkerhetsmyndighet har begge gitt uttrykk for at dagens regulering i sikkerhetsloven er meget knapp og ikke dekker behovet for et sektorovergripende regelverk for utpeking og beskyttelse av skjermingsverdige objekter. Det legges til grunn at skjermingsverdige objekter i dag i hovedsak beskyttes gjennom særlovgivningen der aktuelle bestemmelser om dette finnes, men at det ikke foreligger tilstrekkelig tverrsektoriell oversikt, tilsyn eller koordinert regelverk på området. Nasjonal sikkerhetsmyndighet mener at det helt siden sikkerhetsloven ble vedtatt, har vært erkjent at det er et problem at det mangler utfyllende bestemmelser på dette området. Etaten anser dette som særlig problematisk i forhold til rådgivning, håndheving og tilsyn på objektsikkerhetsområdet. På grunn av manglende bestemmelser har Nasjonal sikkerhetsmyndighet ikke utarbeidet konkrete veiledninger, og det har heller ikke vært mulig for direktoratet å gjennomføre tilsyn på en god måte. Direktoratet finner denne situasjonen lite tilfredsstillende.[138]

Nasjonal sikkerhetsmyndighet mener at manglende eller dårlig gjennomført forebyggende sikkerhet vil kunne påvirke sannsynligheten for at anslag lykkes, og at konsekvensene av uønskede hendelser blir større enn de ellers ville blitt.[139] Dette kan ifølge etaten skje ved at objektene faktisk ikke blir identifisert som skjermingsverdige og dermed oversett i sikkerhetsarbeidet, eller ved at sikkerhetstiltakene ikke er gode nok. Direktoratet framhever betydningen av et tilfredsstillende regelverk sett i lys av at det generelle trusselbildet har endret seg og gitt nye utfordringer for samfunnet. Forsvarsdepartementet mener at dagens regulering skaper utfordringer for en sektorovergripende tilnærming til objektsikkerhet, men ser ikke at dette nødvendigvis medfører en risiko for manglende identifisering av objekt med tilhørende tiltak.[140]

5.1.2 Tiltak for å redusere sårbarheten i IT-infrastrukturen

Etablering av forskningsprosjektet BAS-5

Forsvarets forskningsinstitutt (FFI) har på oppdrag fra bl.a. Justis- og politidepartementet og Direktoratet for samfunnssikkerhet og beredskap gjennomført en serie forskningsprosjekter om beskyttelse av samfunnet i forbindelse med unormale påkjenninger. Det første BAS-prosjektet ble avsluttet i 1997, og utredningen anbefalte bl.a. økt innsats innenfor områdene telekommunikasjon/IT, kraftforsyning og ledelse/informasjon.[141] Senere har Forsvarets forskningsinstitutt foretatt vurderinger av elektrisitets-, telekom- og transportsektorene.[142]

Et BAS-prosjekt som skal utrede sårbarhet i nasjonalt viktige IT-systemer, har også vært planlagt. IT-sikkerhet og sårbarhet som et område for forskningsoppdrag ble først omtalt i St.prp. nr. 1 (2002–2003) for Justis- og politidepartementet. Det har hele tiden vært en forutsetning at prosjektet skal være finansiert som et spleiselag. Justis- og politidepartementet gikk i begynnelsen av mai 2003 ut med brev til en rekke departementer og offentlige etater med forespørsel om å bidra til finansieringen av et BAS-prosjekt om sårbarhet i nasjonalt viktige IT-systemer.[143] I september 2003 sendte departementet over et oppdragsbrev til DSB og Nasjonal sikkerhetsmyndighet der etatene blir bedt om å igangsette et arbeid for å skaffe til veie økonomiske midler til å gjennomføre forskningsprosjektet BAS-5.[144] Departementet uttaler at det viste seg vanskelig å skaffe til veie økonomiske midler til prosjektet gjennom forespørselen som ble sendt ut i mai.

Våren 2004 ble det søkt om støtte til prosjektet fra Norges forskningsråd.[145] I oktober 2004 ble prosjektet

136) Rapport fra arbeidsgruppe om objektsikkerhet: Forebyggende sikring av objekter mot terror- og sabotasjehandlinger, 24. mai 2002, punkt 6.1

137) Forsvarsdepartementets svar på Riksrevisjonens spørrelister av 8. april 2005

138) Svar på Riksrevisjonens spørrelister fra Forsvarsdepartementet av 8. april 2005 og fra Nasjonal sikkerhetsmyndighet av 23. februar 2005

139) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 23. februar 2005

140) Forsvarsdepartementets svar på Riksrevisjonens spørreliste av 8. april 2005

141) Hæsken, O.M., T.G. Olsen og H. Fridheim: Beskyttelse av samfunnet (BAS) – sluttrapport. FFI/Rapport-97/01459

142) BAS-2: Hagen J.M. og K.O. Nystuen: Beskyttelse av samfunnet med vekt på offentlig telekommunikasjon, FFI/Rapport-99/00240. BAS-3: Fridheim H., J. Hagen og S. Henriksen: En sårbar kraftforsyning – sluttrapport etter BAS-3, FFI/Rapport-2001/02381. BAS-4: Hagen J.M., G.H. Rodal, E. Hoff, B. Lia, J.E. Torp og S. Gulichsen: Beskyttelse av samfunnet med fokus på transportsektoren, FFI/Rapport-2003/00929

143) Jf. brev om BAS-5 Beskyttelse av samfunnet 5 – Sårbarhet i nasjonalt viktige IKT-systemer sendt fra Justis- og politidepartementet 2. mai 2003

144) Brev fra Justis- og politidepartementet til DSB og NSM av 25. september 2003, oppdragsbrev knyttet til BAS-5

145) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 24. februar 2005

tildelt ca. fem millioner kroner fra forskningsrådet, som dermed finansierer nesten halvparten av prosjektet.[146] Departementer og offentlige etater bidrar med i overkant av seks millioner kroner.

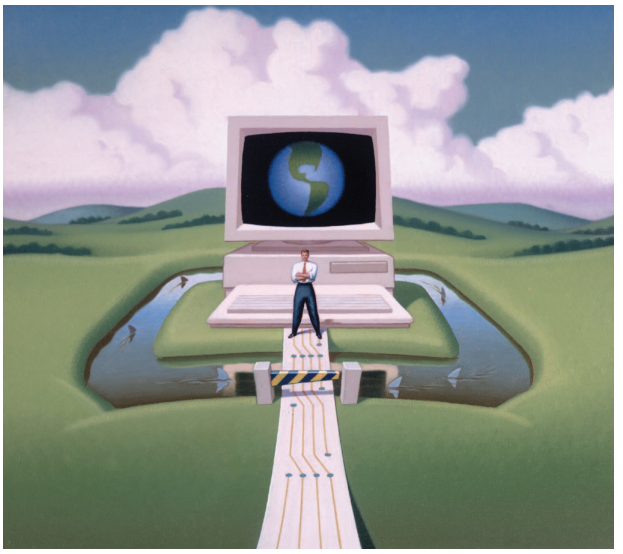
Justis- og politidepartementet opplyste i brev til Nærings- og handelsdepartementet av 20. februar 2004, om oppfølgingsplaner for Nasjonal strategi for informasjonssikkerhet, om at prosjektet skulle igangsettes sommeren 2004, og at en delrapport der man presenterer et felles sett med kriterier for identifisering av samfunnskritisk IT-infrastruktur, burde kunne være klar innen utgangen av 2004. De nevnte problemene med å finne finansiering medførte forsinkelser i forhold til denne planen. I den gjeldende prosjektbeskrivelsen framgår det at metode og grunnlag for case-studier skal være avklart i løpet av 1. halvår 2005.[147] Deretter skal tre case-studier være avsluttet innen utgangen av 1. kvartal 2006. Hovedresultatene fra prosjektet vil bli en analyse av kostnadseffektiviteten av forskjellige tiltak, samt en rangering av samfunnssektorer/virksomheter ut fra risiko. Både analysen og rangeringen skal være avsluttet i løpet av 1. halvår 2006.

Både Nasjonal sikkerhetsmyndighet og DSB bekrefter at det var en tidkrevende prosess å finansiere prosjektet.[148] Direktoratene peker på flere årsaker til dette, bl.a. at IT i kritisk infrastruktur favner om svært mange forskjellige interessenter fra flere sektorer. Det medfører at de administrative og finansielle avklaringene tar lang tid. Nasjonal sikkerhetsmyndighet peker videre på at flere etater og virksomheter hadde vanskeligheter med å finne budsjettmidler i inneværende år, samt at få var villige til "å gå foran". Direktoratene nevner også at avventingen av resultatet av søknaden til Norges forskningsråd førte til at full oppstart av prosjektet ble forsinket i forhold til den opprinnelige planen.

Mange metoder for risiko- og sårbarhetsanalyser

I Nasjonal strategi for informasjonssikkerhet legges det til grunn at virksomheters sikkerhetstiltak bør være dimensjonert etter en vurdering av den aktuelle risikoen. Ifølge strategien skal det utarbeides en metode for risiko- og sårbarhetsvurdering av samfunnskritisk IT-infrastruktur, og utvikles verktøy og metode for risiko- og sårbarhetsvurdering for små og mellomstore bedrifter.[149]

Metodikk for risiko- og sårbarhetsanalyser eller -vurderinger er utviklet av en rekke virksomheter, bl.a. følgende:



Scanpix Creative/Masterfile

- Direktoratet for samfunnssikkerhet og beredskap har utgitt veiledninger for gjennomføring av risiko- og sårbarhetsvurderinger for grupper av offentlige virksomheter.[150]
- Nasjonal sikkerhetsmyndighet har i samarbeid med NTNU arbeidet med metoder og veiledning for risiko- og sårbarhetsanalyse. Dette resulterte først i publisert metode for risiko- og sårbarhetsanalyse (ROS-analyse) av informasjons- og objektsikkerhet i henhold til sikkerhetsloven, utgitt i 2000 (ROS 2000).[151] Denne metoden ble videreutviklet i et resultat som ble publisert i 2004 (ROS 2004), mens direktoratet i april 2005 utga en veiledning som er nært knyttet til≈ ROS 2004.[152]
- Næringslivets sikkerhetsorganisasjon har utarbeidet en metode for risikoanalyse som kan være mindre tidkrevende å følge enn ovennevnte metodikk.[153]
- Datatilsynet har laget en veileder om risikovurdering av informasjonssystemer med utgangspunkt i forskrift til personopplysningsloven.[154]
- Kompetansesenter for IT i helsevesenet har utgitt en veiledning for risikoanalyse for sin sektor.[155]

146) BAS-5 – Critical Information Infrastructure Protection, Project description

147) BAS-5 – Critical Information Infrastructure Protection, Project description

148) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 23. februar 2005

149) Nasjonal strategi for informasjonssikkerhet, side 12, 19, 21–22

150) Jf. Systematisk samfunnssikkerhet og beredskap – en veileder i internkontroll for beredskapsarbeid i departementene og Veileder for kommunale risiko- og sårbarhetsanalyser

151) Objekt- og informasjonssikkerhet. Metode for risiko- og sårbarhetsanalyse, utformet av NTNU på oppdrag fra Nasjonal sikkerhetsmyndighet, 20. desember 2000

152) Jf. Risikohåndtering. Bruk av risiko- og sårbarhetsanalyser i det kontinuerlige sikkerhetsarbeidet, av Anders Øksne og Helge Rager Furuseth, utgitt av NTNU i 2004 (ROS 2004), samt Veiledning i risiko- og sårbarhetsanalyse, utgitt av Nasjonal sikkerhetsmyndighet april 2005

153) Risikoanalyse. Næringslivets sikkerhetsorganisasjons metode for risikoanalyse (faghefte 3), august 2000

154) Risikovurdering av informasjonssystem med utgangspunkt i forskrift til personopplysningsloven (TV-506:2002), utgitt 15. februar 2002

155) Risikoanalyse. Metodegrunnlag og bakgrunnsinformasjon, utgitt 8. september 2000

En sentral del i BAS-5-prosjektet er å utvikle og teste ut en metodikk for gjennomføring av risiko- og sårbarhetsanalyse av komplekse IT-systemer i kritisk infrastruktur. Metoden vil bli utviklet for å gjennomføre risiko- og sårbarhetsanalyser på et mer overordnet nivå enn metodene nevnt over, for eksempel for en hel sektor. Prosjektet vil imidlertid studere tilgjengelig metodikk og benytte dette som innspill.[156] Metodikk skal anvendes i enkelte case-studier i prosjektet.[157] Det er ikke klart hvordan metoden eventuelt skal benyttes videre av sentrale myndigheter.

På oppdrag fra Nærings- og handelsdepartementet ble det i august 2004 gjennomført en kartlegging av aktuelle metoder for risiko- og sårbarhetsanalyser med vekt på behov i små og mellomstore bedrifter. Planen er at dette arbeidet skal følges opp med utvikling av en verktøykasse for sårbarhetsanalyser. Ifølge Moderniseringsdepartementets handlingsplan fra mai 2005 skal verktøykassen være utviklet innen utgangen av 2005.

Nasjonal sikkerhetsmyndighet er gjennom iverksettelsesbrevet for 2005 pålagt å søke å samordne sin metodikk for risiko- og sårbarhetsanalyse med tilsvarende fra DSB.[158] DSB har tatt initiativ til å utarbeide en veileder til sin metodikk i form av et elektronisk verktøy, og vil vurdere om det er mulig å utvikle felles veiledningsmateriell. I forbindelse med videreutvikling av egen metode vurderte Nasjonal sikkerhetsmyndighet i samarbeid med NTNU bl.a. metoden utviklet av DSB på kommunenivået. Men metoden ble vurdert å være for enkel og overordnet for noen av virksomhetene som omfattes av sikkerhetsloven.

Nasjonal sikkerhetsmyndighet gir uttrykk for at det ikke er uvanlig at enhver virksomhet som skal gjennomføre risiko- og sårbarhetsanalyser, skaffer seg en oversikt over metoder fra forskjellig hold, siden det som regel er nødvendig med lokale tilpasninger. Hvilke modeller som velges, vil avhenge av formålet med og omfanget av analysen. I denne sammenhengen mener direktoratet at "verktøykassen" som Moderniseringsdepartementet utvikler, kan være verdifull.[159] Abelia mener for øvrig at risiko- og sårbarhetsanalyser er et svært viktig område, som sannsynligvis vil kunne gi langt større gevinst enn mye annet innenfor IT-sikkerhet.[160]

156) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 24. februar 2005

157) BAS-5: Critical information Protection – Project description

158) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 24. februar 2005

159) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 24. februar 2005

160) Abelias svar på Riksrevisjonens spørreliste av 4. mars 2005

Gjennomføring av risiko- og sårbarhetsvurderinger av samfunnskritisk IT-infrastruktur

Risiko- og sårbarhetsanalyser er et sentralt virkemiddel i beredskapsarbeidet i Norge, og det er grunnleggende for arbeidet med å sikre samfunnskritisk IKT-infrastruktur. Ifølge Nasjonal strategi for informasjonssikkerhet skal det lages et felles sett av kriterier som gjør det mulig å identifisere samfunnskritisk IT-infrastruktur og -systemer. Videre framgår det av strategien at det skal utarbeides en metode for risiko- og sårbarhetsvurderinger, samt gjennomføres slike vurderinger av samfunnskritisk IT-infrastruktur.[161]

Hoveddelene av dette tiltaket er lagt til forskningsprosjektet BAS-5, som skal rapportere hovedfunn i løpet av 1. halvår 2006. Prosjektets mål er å utvikle en metodikk og analysere sårbarheten for de infrastrukturene som er avhengige av IT.[162] Delmålene for prosjektet er å:

- analysere risiko og sårbarhet for et utvalg samfunnskritiske systemer/infrastrukturer
- utvikle og benytte en metodikk for å rangere virkemidler som har som formål å redusere sårbarhet
- utvikle og benytte en metodikk for å rangere kritiske systemer og sektorer som er avhengige av IT, etter hvor alvorlige konsekvensene er ved bortfall av tjenester fra de respektive systemene/sektorene

Tekstboks 6

Det finnes en rekke eksempler der kritisk infrastruktur har blitt berørt av IT-sikkerhetshendelser: IT-systemene til den svenske trygdeetaten var utilgjengelige i flere dager i juni 2004 etter at de ble rammet av ormen Korgo. Mot slutten av januar 2003 rammet ormen Slammer en stor mengde servere tilknyttet Internett, og den forårsaket at systemer ved atomkraftverket Davis-Besse i Ohio i USA, en nødtelefonsentral og en rekke minibanker ble utilgjengelige. I Australia ble det i april 2000 sluppet ut flere millioner liter kloakk etter at en mann som hadde vært med på å installere kontrollsystemet, brøt seg inn i systemet som en protest mot at han ikke fikk fast jobb ved anlegget. Ikke-ville-de hendelser kan også gi store problemer: Svikt i rutinene for oppgradering av systemer ved det norske Fellesdata førte i august 2001 til at to millioner kunder var uten betalingsforbindelse i lengre perioder.

Kilde: Se vedlegg 1.

Justis- og politidepartementet opplyser at man legger opp til at den enkelte sektor må følge opp resultatene av BAS-5-prosjektet innenfor sitt ansvarsområde.[163] Departementets oppfølging er avhengig av resultatene

161) Nasjonal strategi for informasjonssikkerhet, side 19

162) BAS-5: Critical Information Infrastructure Protection - Project description, rev. 14. oktober 2004

163) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen 15. mars 2005

fra forskningsprosjektet, herunder spesielt case-studiene i prosjektet. DSB mener det er viktig at BAS-5-prosjektet er omtalt i stortingsdokumenter, og at ansvarlige departementer er med på å "eie", finansiere og gi råd underveis i arbeidet.[164]

Forskningsprosjektet BAS-5 skal gi et oppdatert og tverrsektorielt oversiktsbilde over sårbarhet i IT-infrastrukturen i samfunnet. Det foreligger ikke planer for å koordinere de enkelte sektorenes risiko- og sårbarhetsanalyser på IT-området. Justis- og politidepartementet mener at en samlet oversikt med aggregerte risiko- og sårbarhetsanalyser antagelig vil være av begrenset verdi, bl.a. fordi den ikke vil bli anvendt i det daglige arbeidet, jf. at ansvaret for forebyggende tiltak er tillagt de enkelte sektorene. [165]

Virksomheter som berøres av sikkerhetsloven, skal rapportere til Nasjonal sikkerhetsmyndighet dersom de, for eksempel i forbindelse med risikovurdering, oppdager bl.a. sikkerhetstruende hendelser.[166] Denne typen informasjon aggregeres og presenteres i Nasjonal sikkerhetsmyndighets årlige risikovurdering. Direktoratet opplyser at det foreløpig ikke har planlagt mer omfattende og systematiske aggregeringer basert på de kontinuerlig gjennomførte risikovurderingene ute i virksomhetene.[167]

Utarbeiding av sektorvise normer
Ifølge Nasjonal strategi for informasjonssikkerhet skal de enkelte sektorene utarbeide normer for sikring med hensyn til konfidensialitet, integritet og tilgjengelighet. Dette tiltaket er knyttet til gjennomføringen av risiko- og sårbarhetsvurdering av samfunnskritisk IT-infrastruktur, og sektordepartementene er gitt ansvar for tiltaket.

Ifølge statusoversikt av 12. november 2004 fra Koordineringsutvalget for informasjonssikkerhet er det ikke planlagt eller gjennomført tiltak på dette området. Det er det heller ikke i departementenes handlingsplaner.

5.1.3 Systemer for å fange opp trusler mot IT-infrastrukturen

Informasjon om sikkerhetshendelser er nødvendig for å kunne danne et bilde av foreliggende trusler og sårbarhet i IT-infrastruktur, og for å kunne gi råd om konkrete trusler eller assistanse ved gjenoppretting av tjenester.

Myndighetene har etablert Varslingssystem for digital infrastruktur (VDI) og Senter for informasjonssikring (SIS) for å sikre identifikasjon av trusler mot IT-systemer. Det er også andre etablerte institusjoner som arbeider med å identifisere trusler mot det norske samfunnet, jf. for eksempel EOS-tjenestene, men disse blir ikke omtalt her. Nedenfor følger en gjennomgang av hvordan VDI og SIS utfører sine oppgaver med å identifisere trusler.

Varslingssystem for digital infrastruktur
Varslingssystem for digital infrastruktur (VDI) ble etablert som et samarbeid mellom e-tjenestene. Fra 2003 er VDI en del av virksomheten til Nasjonal sikkerhetsmyndighet.

Varslingssystemet fungerer ved at det plasseres en "boks" for innbruddsdetektering ved Internett-forbindelsen til virksomhetene som deltar. Disse "boksene" overfører data til en sentral som er underlagt Nasjonal sikkerhetsmyndighet. Her analyseres dataene, og dette gir myndighetene mulighet til å få et bilde av hvilke trusler norske virksomheter står overfor, og til å avdekke koordinerte angrep. VDI har fokus mot koordinerte angrep av nasjonal betydning. Deltakende virksomheter kan oppnå fordeler gjennom samarbeidet ved at det meldes tilbake om identifiserte angrep eller alvorlige trusler som er oppdaget.

Da VDI ble opprettet, var antallet deltakere begrenset; ca. 10–15 større norske virksomheter deltok i samarbeidet.[168] Det ble lagt vekt på å oppnå et representativt utvalg for sentral infrastruktur i Norge. I tillegg er det etablert et annet utvalg virksomheter som ikke er koblet direkte til VDI-sentralen, men der det utveksles informasjon om oppdagede sårbarheter og trusler. Nasjonal sikkerhetsmyndighet legger til grunn at VDI kan miste fokus dersom antall bedriftsmedlemmer økes betydelig, og påpeker at det også er tekniske begrensninger knyttet til utvidelser. Direktoratet mener det har vært nødvendig med et begrenset utvalg for å opparbeide tillit og åpenhet mellom VDI og deltakende virksomheter, men opplyser at man nå arbeider med en forsiktig økning i antall deltakere. Nasjonal sikkerhetsmyndighet håper dette skal gi et bedre og enda mer representativt bilde av den reelle trusselen som dataangrep over Internett representerer mot ulike samfunnssektorer. [169]

På grunn av systemets oppbygging vil det bare fange opp logiske angrep via Internett som er rettet mot en virksomhets tilknytning til nettet. Interne trusler, sosiale trusler og kombinasjoner av disse håndteres ikke av teknologien i varslingssystemet. Nasjonal sikkerhetsmyndighet mener imidlertid at VDI fokuserer på datasikkerhet i en videre forstand enn bare dataangrep fra Internett, blant annet gjennom VDI-sikkerhetsforum, som arrangeres 3–4 ganger hvert år, og som samler både

164) Direktoratet for samfunnssikkerhet og beredskaps svar på Riksrevisjonens spørreliste av 1. mars 2005

165) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen 15. mars 2005

166) Forskrift om sikkerhetsadministrasjon § 5-6

167) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 24. februar 2005

168) Referat fra møte mellom Nasjonal sikkerhetsmyndighet og Riksrevisjonen 12. april 2004.

169) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 23. februar 2005.

teknisk personell og strategisk ledelse fra deltakende virksomheter. Ifølge direktoratet har dette bidratt til å øke bevisstheten omkring disse nye truslene, og til å redusere sårbarheten i videre forstand enn det VDIs *tekniske* løsning skulle tilsi. Nasjonal sikkerhetsmyndighet mener VDI har bidratt til økt fokusering på nettverkssikkerhet, både hos offentlige etater og i samfunnsviktige private virksomheter.[170]

Forholdet mellom VDI og deltakerne er ifølge Nasjonal sikkerhetsmyndighet preget av svært høy tillit, bygget opp gjennom snart fem år med åpenhet og gjensidig deling av informasjon. Direktoratet ser på åpenhet og gjensidig vilje til å redusere sårbarheten innen kritisk infrastruktur som en absolutt forutsetning for et vellykket system.[171]

Oversikt over utviklingen av trusler gis gjennom månedlige rapporter som viser registrerte sikkerhetshendelser i den foregående perioden. Fram til høsten 2003 var rapportene gradert 'begrenset', og ble kun distribuert til deltakerne i prosjektet og sentrale offentlige myndigheter. Fra desember 2003 har månedsrapporter fra VDI vært offentlig tilgjengelige på nettsidene til Nasjonal sikkerhetsmyndighet. Innholdet i disse rapportene er innrettet mot et taktisk nivå med IT-personell som målgruppe.[172]

Kommersielle aktører tilbyr også rapporter som ligner på månedsrapportene fra VDI. Bl.a. er trusselrapporter fra Secode Norge AS fritt tilgjengelige på Internett.[173] Nasjonal sikkerhetsmyndighet ser at det finnes mange rapporter om trender og trusler mot IT-sikkerheten, men mener det er viktig for myndighetene at bakgrunnen og metodikken i rapportene er kjent. Videre legger direktoratet til grunn at trafikkinformasjonen i rapportene fra VDI er hentet fra sensorer knyttet til datasystemer i norsk samfunnskritisk infrastruktur, med kort tid mellom oppdagelse og varsel. Direktoratet ser også et poeng i at myndighetene får anledning til å bekrefte, eventuelt avkrefte, informasjon fra kommersielle kilder.[174]

Justis- og politidepartementet har gitt uttrykk for at det ser på VDI som en tjeneste for samfunnet, men mener at denne delen har vært for lite tilrettelagt og kommunisert. Departementet mener man har en jobb å gjøre her for å vise hva som er VDIs samfunnsoppdrag.[175]

170) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 23. februar 2005

171) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 23. februar 2005

172) Se nettstedet http://www.nsm.stat.no/.

173) Se http://www.secode.no og http://www.itpro.no/rapporter.php.

174) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 23. februar 2005

175) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen 15. mars 2005

Senter for informasjonssikring

Senter for informasjonssikring (SIS) ble opprettet som et prøveprosjekt fra april 2002. Senterets hovedoppgave har vært å framskaffe et helhetlig bilde av truslene mot norske IT-systemer basert på innrapportering av hendelser fra norske virksomheter. Det er forutsatt at sikkerhetsbrudd og -hendelser skal meldes inn raskt, og at senteret skal ha god kontakt med ressurspersoner og -miljøer.

Senteret har inngått avtaler med 21 virksomheter om innrapportering av sikkerhetshendelser. Avtalene gir forsikringer om at innrapportert informasjon vil bli behandlet konfidensielt. Senteret har opplyst at det i løpet av 2004 mottok mindre enn fem rapporter om sikkerhetshendelser.[176] I senterets årsrapport for 2004 konstaterer man at det fortsatt er mangel på vilje i norske virksomheter til å rapportere konkrete hendelser.[177]

Rapportering av sikkerhetshendelser til eksterne instanser er også tatt opp i *Mørketallsundersøkelsen for 2003*.[178] Spørreundersøkelsen viste at 74 % av norske virksomheter ikke har rutiner for ekstern rapportering. Rapportering til Senter for informasjonssikring nevnes av mindre enn 1 % av virksomhetene. Nesten en tredjedel av virksomhetene opplyser at grunnen til at de ikke rapporterte, var at de ikke kjente til instansen. Andre årsaker til manglende rapportering var at hendelsen var ubetydelig, at rapportering ikke ga merverdi, eller at rapportering var for ressurskrevende. Senter for informasjonssikring mener at utvalget i spørreundersøkelsen ikke gir grunnlag for å trekke en direkte konklusjon om at manglende rapportering skyldes manglende kjennskap til senteret. Senteret kan vise til en rekke virksomheter som kjenner til senteret og har hatt hendelser, men som ikke vil rapportere dette.[179]

Senter for informasjonssikring har gitt uttrykk for at dets suksess ikke bør måles i antall innrapporterte hendelser. Senteret er opptatt av å oppnå kvalitet i grunnlagsdata gjennom tilgang til nødvendige detaljer rundt enkelthendelser, framfor kvantitet i hendelsesregistreringen. Senteret mener at det ikke er realistisk å få inn rapporter om mange hendelser. Senteret søker å bedre innrapporteringshyppigheten ved spesiell bearbeiding av utvalgte sektorer: Det har etablert referansegrupper for sektorene bank/finans og transport, og senteret deltar i tillegg i referansegrupper i følgende sektorer: telekomsektoren (grupper opprettet av Post- og teletilsynet), universitetene (gruppe opprettet av

176) Svar på Riksrevisjonens spørreliste fra Senter for informasjonssikring av 28. februar 2005

177) Årsrapport 2004 fra Senter for informasjonssikring, side 9

178) Mørketallsundersøkelsen 2003 – om datakriminalitet og IT-sikkerhet, Økokrim/Næringslivets Sikkerhetsråd/Senter for informasjonssikring, side 72–73 og 96–97

179) Svar på Riksrevisjonens spørreliste fra Senter for informasjonssikring av 28. februar 2005

Uninett), kommunene (ved hjelp av foreningen Kommunal informasjonssikkerhet), oljesektoren og kraftsektoren.[180] Senteret mener at det å delta i gruppene har gitt betydelig innsikt i sikkerhetsmessige problemstillinger innen de forskjellige sektorene. Vi viser for øvrig til omtale av senterets veiledningsoppgaver under punkt 5.2.3.

Senteret viser også til at manglende rapportering er et forhold som går igjen i alle land som har startet frivillig rapportering av sikkerhetshendelser. Senteret uttrykker forståelse for at virksomheter ikke vil benytte ressurser til rapportering etter at problemer er løst, uten at de ser noen merverdi av dette. På denne bakgrunn har senteret foreslått at virksomheten må knyttes tettere opp mot en CERT der virksomheter kan få direkte hjelp ved hendelser, og dermed en merverdi ved innrapportering.

Bransjeorganisasjonene IKT-Norge og Abelia, samt Næringslivets Sikkerhetsråd, gir alle uttrykk for at Senter for informasjonssikring er lite kjent i næringslivet, noe som vil påvirke mengden av hendelser som rapporteres inn.[181] Abelia nevner i tillegg at de som kjenner til senteret, kanskje ikke har noe godt insentiv for å rapportere, og peker på at rapportering alltid innebærer en viss risiko for at problemer man ikke ønsker at kunder og leverandører skal merke, blir kjent. Organisasjonen mener at man her har et typisk gratispassasjerproblem, der det er fint om andre rapporterer, men ikke like opplagt at det er lurt å gjøre det selv. Datatilsynet peker på at manglende innrapportering kan skyldes at det er krav til rapportering av hendelser i mange regelverk med forskjellige adressater.[182]

Tekstboks 7

Den amerikanske riksrevisjonen (GAO) la i mai 2005 fram en rapport om amerikanske myndigheters arbeid for å sikre kritisk IT-infrastruktur. Rapporten viser bl.a. at statsadministrasjonen ennå ikke har utarbeidet fullstendige risiko- og sårbarhetsanalyser, og rapporten tar spesielt opp at fullstendige sektorvise analyser og identifisering av tverrsektorielle avhengigheter ikke er ferdigstilt. Rapporten peker videre på at det er lite utveksling av informasjon om sikkerhetshendelser og trusler mellom offentlig og privat sektor, til tross for en rekke initiativ på dette feltet. GAO mener administrasjonen har forbedret sin evne til å koordinere håndtering av sikkerhetshendelser, men at planer og øvelsesaktiviteter for å gjenopprette tjenester etter angrep er utilstrekkelige. For eksempel finnes det ingen plan for å gjenopprette nøkkelfunksjoner for Internett.

Kilde: Se vedlegg 1.

180) Svar på Riksrevisjonens spørreliste fra Senter for informasjonssikring av 28. februar 2005

181) Svar på Riksrevisjonens spørrelister fra IKT-Norge av 28. februar 2005, Abelia av 4. mars 2005 og Næringslivets Sikkerhetsråd av 14. mars 2005

182) Svar på Riksrevisjonens spørreliste fra Datatilsynet av 28. februar 2005

Moderniseringsdepartementet bekrefter at utgangspunktet ved opprettelsen av SIS var at senteret skulle få inn informasjon om sikkerhetshendelser i næringsliv og forvaltning som et grunnlag for å utarbeide et trusselbilde. Departementet mener at SIS ikke har hatt tilstrekkelige aktiviteter for å fremme rapportering av hendelser så langt. Ifølge departementet vil utviklingen av en nasjonal CERT innebære større rapporteringsinsentiver ettersom bedriftene her kan få hjelp, dvs. at rapporteringen ikke bare er for "the common good". Departementet vurderer det også slik at enkeltrapporteringen kanskje ikke er så viktig tross alt, og at hendelsesrapporteringen kun vil være en del av et større bilde der SIS kan få tilgang til nødvendig informasjon gjennom andre kilder.

5.1.4 Systemer for å håndtere sikkerhetshendelser

I behandlingen av St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* uttaler forsvarskomiteen og justiskomiteen at klargjøring av beredskapsplaner og krisehåndteringsplaner for bl.a. IT-sikkerhet er viktig.[183] Betydningen av øvelser tas også opp her. Ifølge meldingen vil Justis- og politidepartementet ta initiativ for å sikre at tiltak ved bortfall av IKT blir reflektert i kriseplaner. OECD har også lagt til grunn at det må finnes prosedyrer som sikrer et raskt og effektivt samarbeid, for å kunne forebygge, oppdage og reagere på sikkerhetshendelser.[184]

Håndtering av sikkerhetshendelser kan involvere en rekke tiltak. I det følgende gir vi en omtale av beredskaps- og krisehåndteringsplaner, øvelser og behovet for et senter som kan støtte håndteringen av sikkerhetshendelser ved svikt i IT-systemer.

Beredskaps- og krisehåndteringsplaner

Beredskapsplanlegging skjer både på overordnet nasjonalt nivå og på virksomhetsnivå, dvs. i offentlige virksomheter og i bedrifter.

Overordnet nivå

Det samlede beredskapssystemet for militær og sivil sektor har vært under revisjon for å tilpasse det bedre til sikkerhetspolitiske utfordringer, inkludert angrep mot informasjonssystemer.[185] Ifølge Nasjonal strategi for informasjonssikkerhet skal DSB utrede spørsmålet om hvordan IT-sikkerhet kan integreres i gjeldende planverk.

DSB har opplyst at et stort arbeid med å utvikle et nytt nasjonalt beredskapssystem er i sluttfasen. Arbeidet omfatter samtlige departementer. Risikoen for alvorlig svikt i IT-systemer er ifølge direktoratet drøftet gjennom

183) Innst. S. nr. 9 (2002–2003)

184) OECD retningslinjer for sikkerhet i informasjonssystemer og nettverk – Mot en sikkerhetskultur, oversettelse av Nærings- og handelsdepartementet, side 7

185) Jf. St.meld. nr. 39 (2003–2004) Samfunnssikkerhet og sivilt-militært samarbeid, side 50

Scanpix Creative/Masterfile

prosjektet, og er til en viss grad reflektert i det foreliggende utkastet til hoveddokument. DSB understreker at tiltak i planverket må bygge på de ordningene og kapasitetene som er etablert. Videre poengterer direktoratet at det vil være svært viktig at departementene og direktoratene følger opp et nytt nasjonalt beredskapssystem i mer operative beredskapsplaner, herunder i forhold til tenkte situasjoner med alvorlig svikt i IT-systemer. DSB har gitt retningslinjer til fylkesmennene om å gi risikoforhold knyttet til IT-sikkerhet økt oppmerksomhet.[186]

Virksomhetsnivå

Beredskapsplanlegging eller kontinuitets- og katastrofeplanlegging i enkeltvirksomheter er ikke spesifikt behandlet i Nasjonal strategi for informasjonssikkerhet.

Statistisk sentralbyrå gjennomførte i 2. kvartal 2004 en undersøkelse om bl.a. IT-sikkerhet i statlig sektor, og byrået undersøkte om de enkelte virksomhetene hadde en beredskapsplan på IT-området som var ajourført i løpet av de to siste årene.[187] I statlig sektor hadde 40 % av virksomhetene en slik plan. I en tilsvarende undersøkelse på kommunenivå i 2003 oppga 41 % at de hadde en beredskapsplan på IT-området som var ajourført de to siste årene.[188] Statistisk sentralbyrå har også stilt spørsmål rundt temaet i en undersøkelse i 2004 som var rettet mot privat næringsliv. Her viser resultatene at bare 16 % av foretak med mer enn ti ansatte hadde en kriseplan som var oppdatert de to siste årene.[189]

Nasjonal sikkerhetsmyndighet mener at undersøkelsene viser at altfor mange virksomheter bare har den daglige grunnsikringen å falle tilbake på selv i situasjoner der trusler er mer sannsynlig enn normalt, og i situasjoner der sikkerheten av andre grunner ikke lar seg opprettholde med vanlige tiltak.[190] Etaten ser på dette som bekymringsfullt. DSB mener at manglende beredskapsplaner (eksistens og/eller kvalitet) er et problem for virksomheten selv og bekymringsfullt når det gjelder potensielle samfunnsmessige konsekvenser.[191] DSB viser til at deres veiledninger i risiko- og sårbarhetsanalyse, beredskapsplanlegging og gjennomføring av kurs og øvelser kan bidra til å bedre situasjonen.

IKT-Norge mener at manglende kriseplanlegging i virksomhetene kan få svært dramatiske konsekvenser, og at mørketallene her er store. Organisasjonen uttaler at den har ventet på et koordinert utspill fra myndighetene, men kan ikke se at et slikt utspill har kommet. Organisasjonen oppfatter myndighetenes arbeid for å øke andelen virksomheter med oppdaterte beredskapsplaner som ikke-eksisterende annet enn i planer.[192] Datatilsynet mener at tallene som viser andelen virksomheter som har etablert beredskapsplaner, er nedslående, men tilsynet mener at det dessverre beskriver en reell virkelighet.[193] Erfaringer fra Datatilsynets tilsynsvirksomhet oppgis å peke ganske entydig i retning av en lite planmessig tilnærming til informasjonssikkerhet i virksomhetene, i både privat og offentlig sektor.

Verken Moderniseringsdepartementet eller Justis- og politidepartementet ønsket å kommentere resultatene av undersøkelsene fra Statistisk sentralbyrå.[194] Departementene understreker at planer for gjenoppretting er den enkelte virksomhets ansvar. Moderniseringsdepartementet mener det kan stilles spørsmål ved hvor langt departementets ansvar strekker seg når det gjelder å følge opp at forvaltningen, inkludert kommunene, virkelig utarbeider slike planer. For øvrig opplyser departementet at det finner det mer hensiktsmessig å utvikle verktøy som forvaltningen kan bruke til risiko- og sårbarhetsanalyser, enn å utarbeide maler for kontinuitetsplaner. Departementet legger til grunn at virksomhetene selv vil finne det nødvendig å utarbeide kontinuitetsplaner som følge av disse analysene. Justis- og politidepartementet viser for øvrig til DSBs arbeid overfor kommuner og fylkesmenn og Næringslivets Sikkerhetsråds arbeid mot næringslivet.

186) Direktoratet for samfunnssikkerhet og beredskaps svar på Riksrevisjonens spørreliste av 1. mars 2005

187) Bruk av IKT (Informasjons- og kommunikasjonsteknologi) i staten. 2. kvartal 2004. Frigitt 16. november 2004. Undersøkelsen omfattet sektorene stats- og trygdeforvaltningen, statens forretningsdrift, statlige låneinstitusjoner, statsforetak (100 prosent eid av staten) samt Norges Bank.

188) Statistisk sentralbyrå: Bruk av IKT (Informasjons- og kommunikasjonsteknologi) i kommunene, 2003. Frigitt 28. juni 2004

189) Statistisk sentralbyrå: Bruk av IKT (Informasjons- og kommunikasjonsteknologi) i næringslivet, 2004. Frigitt 8. desember 2004

190) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 24. februar 2005

191) Direktoratet for samfunnssikkerhet og beredskaps svar på Riksrevisjonens spørreliste av 1. mars 2005

192) IKT-Norges svar på Riksrevisjonens spørreliste av 28. februar 2005

193) Datatilsynets svar på Riksrevisjonens spørreliste av 28. februar 2005

194) Referater fra møter mellom Justis- og politidepartementet og Riksrevisjonen, og Moderniseringsdepartementet og Riksrevisjonen, begge avholdt 15. mars 2005

Øvelser
Øvelser har til formål å vedlikeholde og utvikle evnen til å håndtere uønskede hendelser gjennom å:

- bevisstgjøre den enkelte og virksomhetens ansvar og roller
- utvikle virksomhetens evner til å ivareta ansvar i kritiske situasjoner
- avdekke om forberedelsene er tilfredsstillende synliggjøre forbedringsbehov[195]

DSB initierer øvelser i departementene og i kommunal sektor (med støtte av fylkesmannen). Øvelser arrangeres både sektorvis og på tvers av sektorer. De baserer seg på scenarier som utarbeides av direktoratet, og som skal ta utgangspunkt i aktuelle trusselvurderinger. Det er opplyst at en del av disse øvelsene har inkludert scenarier om svikt i sentral IT-infrastruktur.[196]

Øvelsene foregår på ulike måter – som "table top"-øvelser (en tenkt krise som håndteres rundt et skrivebord) eller som operative øvelser ute i felten.[197] Ressursbruken og kompleksiteten vil være ulik for de forskjellige måtene å gjennomføre øvelser på. Antallet virksomheter som deltar i øvelsene, påvirker også dette. DSB har påpekt at det er viktig å avsette ressurser ved øvelser tilsvarende hva det ville blitt gjort dersom det var en virkelig krise, blant annet med hensyn til reelle beslutningstakere, lokaliteter og ressurser.[198]

Øvelser rettet mot IT-infrastruktur har ifølge Justis- og politidepartementet hovedsakelig vært papirbaserte.[199] Justis- og politidepartementet legger til grunn at disse øvelsene ikke dekker alle aspekter man kunne ønske, men ser dette i sammenheng med at det er vanskelig å gjennomføre større operative øvelser på området. Det kan være problematisk å få enkelte øvelser til å bli realistiske, siden det er begrensede muligheter for å benytte eksisterende IT-infrastruktur i øvelsen uten at det samtidig går på bekostning av sikkerheten.[200] DSB har uttalt at øvelsene som direktoratet initierer, hvor vekt hittil har vært på beslutningstakere, ikke kan sies å være tilstrekkelig for å identifisere konkrete forebyggende tiltak.

I Innst. S. nr. 9 (2002–2003) uttaler komiteene at det er viktig å ha et ledelsesapparat som kan håndtere kriser, men at saksbehandlere innen sikkerhet, beredskap og krisehåndtering bør være sidestilt med ledelsesnivået som målgruppe for øvelser. Justis- og politidepartementet mener DSB bør inkludere andre enn bare ledelsen i øvelsesvirksomheten, for eksempel ved å arrangere øvelser rettet mot saksbehandlere.[201]

Øvelsene som er initiert av DSB de seneste årene, har ifølge direktoratet fokusert på å skape bevissthet og å styrke kompetansen hos ledere.[202] Direktoratet uttaler at det så langt har valgt å gjennomføre tidsavgrensede øvelser for beslutningstakere. Direktoratet mener at dette generelt er et kostnadseffektivt virkemiddel for å generere kunnskap og fremme motivasjon til systematisk, langsiktig arbeid for å høyne beredskapen.[203] DSB påpeker imidlertid viktigheten av at øvelsesstrukturen i både form og innhold over tid er kompletterende, slik at summen av øvelser sikrer en helhetlig utprøving der alle nivåer og målgrupper blir involvert.[204] Ifølge DSB er Sivil nasjonal øvelse i 2006 primært planlagt å involvere saksbehandlernivået og i mindre grad ledelsen. DSB viser også til at fylkesmannsembetene har stående rutiner og praksis knyttet til prøving av IT-infrastrukturen, forhold som saksbehandlere ved de respektive embetene prøver og tester under øvelser.

Computer Emergency Response Team (CERT)
Dette punktet omtaler organisasjoner som har spesialisert seg på varsling, håndtering og respons til alvorlige sikkerhetshendelser. En slik organisasjon betegnes som en CERT, som er en forkortelse for *Computer Emergency Response Team*. Når en virksomhet oppdager et alvorlig sikkerhetsbrudd og ønsker assistanse for å behandle dette, er en CERT et naturlig kontaktpunkt for hjelp.

Det finnes en del virksomheter i Norge som har arbeidsoppgaver som nærmer seg oppgavene til en CERT. Uninett er en CERT, men begrenset til universitets- og høgskolesektoren. *Mørketallsundersøkelsen for 2003* undersøkte om norske virksomheter har en egen vaktordning for å håndtere brudd på IT-sikkerheten (for eksempel tilgang til en CERT). Bare 9 % svarte at de hadde etablert en slik vaktordning. [205]

Varslingssystem for digital infrastruktur (VDI), som er underlagt Nasjonal sikkerhetsmyndighet, har visse

195) Jf. Direktoratet for sivilt beredskap: Systematisk samfunnssikkerhet og beredskap – en veileder i internkontroll for beredskapsarbeid i departementene, side 16

196) Referat fra møte mellom Direktoratet for samfunnssikkerhet og Riksrevisjonen 21. november 2003

197) Jf. Direktoratet for samfunnssikkerhet og beredskap: Faktaark – Øvelser i regi av DSB

198) Jf. Direktoratet for sivilt beredskap: Policy for styrking av generell krisehåndteringskompetanse på lokalt, regionalt og sentralt nivå – Hvordan bedre evnen til å håndtere kriser, side 9

199) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen den 15. mars 2005

200) Jf. for eksempel redegjørelse for beredskapstiltak i kraftsektoren ved Tor Aalberg fra Statnett, i prosjektrådsmøte for BAS-5-prosjektet 14. desember 2004

201) Referat fra møte mellom Justis- og politidepartementet og Riksrevisjonen den 15. mars 2005

202) Referat fra møte mellom Direktoratet for samfunnssikkerhet og beredskap og Riksrevisjonen 21. november 2003

203) Direktoratet for samfunnssikkerhet og beredskaps svar på Riksrevisjonens spørreliste av 1. mars 2005

204) Direktoratet for samfunnssikkerhet og beredskaps svar av 1. april 2005 på spørsmål fra Riksrevisjonen

205) Mørketallsundersøkelsen 2003 – om datakriminalitet og IT-sikkerhet, Økokrim/Næringslivets Sikkerhetsråd/Senter for informasjonssikring, side 71–72

Tekstboks 8

Den første CERT-en ble opprettet i 1988 som en reaksjon på den første Internett-ormen – en hendelse som demonstrerte svakhetene i nettet og behovet for å kunne samordne informasjon og håndtering av slike hendelser. Offentlige eller private virksomheter med CERT-funksjon finnes i de fleste vestlige land:

- I Sverige ble en offentlig CERT, Sveriges IT-incidentcentrum (SITIC), etablert i 2003. I tillegg finnes to andre CERT-organisasjoner knyttet til universitets- og forskningsnettet og til Telia-Sonera.
- Danmark har tre organisasjoner innen dette feltet: DK-CERT, CSIRT.DK og KMD Internet Alarm Center. Disse har tilknytning til henholdsvis forsknings- og undervisningsnettet, TeleDanmark og en datasentral eid av danske kommuner. Alle har kommersielle tilbud om sikkerhetstjenester.
- I Tyskland finnes ca. 15 CERT-organisasjoner. Dette inkluderer CERT-Bund med oppgaver overfor offentlig sektor, og CERTBw som er knyttet til Forsvaret. De øvrige er knyttet til større private virksomheter.
- I Storbritannia finnes ca. 13 registrerte CERT-organisasjoner. Dette inkluderer UNIRAS, som ble etablert i 1992 som en CERT for offentlig sektor. Ansvarsområdet har senere blitt utvidet til også å inkludere private virksomheter som representerer en del av den kritiske infrastrukturen.

Kilde: Se vedlegg 1.

funksjoner som ofte vil tilligge en CERT. VDI gir advarsler til virksomhetene systemet betjener, når alvorlige hendelser oppdages, men skal ikke gi respons og gjenoppretting etter sikkerhetshendelser. En fullt utbygget CERT vil for øvrig ofte ha tilnærmet døgnkontinuerlig vakt, noe som ikke har vært tilfelle for VDI. Senter for informasjonssikring innehar ansvaret for en del aktiviteter knyttet til håndtering av sikkerhetshendelser, men da senteret ble opprettet, ble det bestemt at det ikke skulle ha noen CERT-funksjon i prøveprosjektperioden (utgangen av 2004).[206]

St.meld. nr. 39 (2003–2004) *Samfunnssikkerhet og sivilt-militært samarbeid* tar opp spørsmålet om etablering av en CERT-funksjon på følgende måte: "Det eksisterer ingen koordinerende enhet for håndtering av koordinerte IKT-angrep på samfunnskritiske funksjoner i Norge. Flere instanser har påpekt et behov for en slik enhet for å sikre effektiv håndtering av en krise der flere samfunnskritiske funksjoner blir angrepet samtidig. […] En slik enhet vil kunne styrke den nasjonale beredskapen mot IKT-angrep gjennom å utvikle et system for koordinert respons og gjenoppretting, først og fremst innenfor virksomheter med samfunnskritiske funksjoner. […] Det vil bli vurdert om en slik enhet bør etableres og hvilken myndighet som eventuelt bør ha ansvaret for den."[207]

Som en oppfølging av St.meld. nr. 39 ble det nedsatt en interdepartemental arbeidsgruppe for å drøfte hvordan og hvor man bør etablere en nasjonal enhet for varsling og rådgivning vedrørende informasjonssikkerhet (CERT). Rapporten *Nasjonal koordinering av varsling og rådgivning for informasjonssikkerhet* forelå 8. mars 2005. Ifølge rapporten er det enighet i arbeidsgruppen om at en CERT bør etableres snarest mulig, men det er ikke enighet om hvilket fagmiljø funksjonen bør legges til.

Den nevnte rapporten kan for øvrig også ses på som en vurdering av den framtidige rollen til Senter for informasjonssikring. Styringsgruppen for senteret gjennomførte en evaluering av senteret i 2004. En høringsrunde blant departementene viste ifølge Moderniseringsdepartementet en positiv holdning til å videreføre SIS-funksjonen, men en viss uenighet omkring hvordan enheten burde organiseres, lokaliseres og finansieres. Det er enighet om at senterets funksjoner bør inngå i et koordinert nasjonalt opplegg for varsling og rådgivning (CERT). I påvente av en avklaring av spørsmålet om etablering av en virksomhet med CERT-funksjon besluttet Moderniseringsdepartementet å forlenge prøveperioden for Senter for informasjonssikring fram til 1. juli 2005.[208] Senere har prøveperioden blitt ytterligere forlenget til utgangen av 2005.[209]

Nasjonal sikkerhetsmyndighet har arbeidet for å opprette en CERT i statlig regi.[210] Direktoratet mener at ved å opprette en myndighetsforankret CERT vil Norge ha et sentralt kontaktpunkt for mottak og analyse av informasjon om IT-sikkerhetsangrep og sårbarheter knyttet til samfunnskritiske systemer, og en påfølgende koordinert og samfunnsøkonomisk kostnadseffektiv håndtering og gjenoppretting. En myndighetsforankret CERT vil ifølge Nasjonal sikkerhetsmyndighet være en viktig aktør i den samlede beredskapen, fordi den kan styrke evnen til å motvirke og begrense effekten av alvorlige IT-angrep, og gjenopprette samfunnskritisk infrastruktur og informasjon etter slike angrep. Nasjonal sikkerhetsmyndighet mener at virksomheter med samfunnskritiske systemer trenger og ønsker en koordinering av vital informasjon om f.eks. sikkerhetshull og hvordan slike kan tettes (patching), teknisk angrepsinformasjon og nye alvorlige IT-sikkerhetsutfordringer generelt.

206) Senter for informasjonssikring. Rapport fra forprosjekt, Nærings- og handelsdepartementet, 6. juni 2001

207) St.meld. nr. 39 (2003–2004) Samfunnssikkerhet og sivilt-militært samarbeid, side 45–46208) Notat fra Moderniseringsdepartementet av 15. desember 2004 om Evaluering av SIS – status pr. 15.12.04

209) St.prp. nr. 65 (2004–2005) Tilleggsbevilgninger og omprioriteringer i statsbudsjettet medregnet folketrygden 2005, side 164–165

210) Nasjonal sikkerhetsmyndighets svar på Riksrevisjonens spørreliste av 24. februar 2005

Senter for informasjonssikring mener det er et sterkt behov for at en CERT-tjeneste tilbys også til virksomheter utenom kritisk infrastruktur, fordi mange av disse inngår i verdikjeder som til slutt ender i kritisk infrastruktur. Moderniseringsdepartementet ser at arbeidet hittil har fokusert på etablering av en nasjonal CERT, og at man i mindre grad har tatt hensyn til "resten av samfunnet" (den enkelte sluttbruker, små og mellomstore bedrifter, osv.). Dette kan ifølge departementet være en potensiell svakhet.

St.prp. nr. 65 (2004–2005) opplyser at arbeidet med å finne en helhetlig, permanent løsning for organiseringen av informasjonssikkerhetsarbeidet har vært mer tidkrevende enn forutsatt, og at regjeringen planlegger å legge fram et forslag til organisering i statsbudsjettet for 2006.

5.2 Utvikling av en sikkerhetskultur

OECD har sett det som viktig å fremme sikkerheten ved bruk av informasjonssystemer og nettverk gjennom å utvikle en sikkerhetskultur. Dette innebærer å fokusere på sikkerhet ved utvikling av informasjonssystemer og nettverk, og at det innføres nye tenke- og handlemåter ved bruken av disse og ved utveksling av informasjon.[211] Bevisstgjøring rundt sikkerhet, ansvar, etikk og risikovurderinger er sentrale prinsipper. Dette er fulgt opp gjennom Nasjonal strategi for informasjonssikkerhet, som inneholder flere tiltak som skal bidra til å utvikle en sikkerhetskultur. Tiltakene er i stor grad knyttet til utvikling av den alminnelige IT-sikkerheten. De vil påvirke sikkerheten i den samfunnskritiske IT-infrastrukturen, men nedslagsfeltet er bredere for denne gruppen tiltak, dvs. at de bl.a. også retter seg mot bedrifter og husholdninger.

Tilbakemeldinger fra spørreundersøkelsen som ble gjennomført hos organisasjoner i næringslivet i februar/mars 2005, tyder på at myndighetenes arbeid for å etablere en sikkerhetskultur er lite synlig i privat sektor. Næringslivets Sikkerhetsråd uttaler at synbarheten av dette arbeidet er svært beskjeden, og at deres medlemsbedrifter i liten grad er klar over engasjementet.[212] IKT-Norge mener at myndighetenes mest offensive satsing til nå har vært etableringen av en guide for å unngå spam (uanmodet e-post), men for øvrig oppfatter ikke organisasjonen at myndighetene i særlig utstrekning jobber med spørsmålet. [213] IKT-Norge tror imidlertid at lansering av portalen nettvett.no vil kunne bidra til å synliggjøre myndighetenes arbeid. Abelia ser et problem ved at suksess måles i å ha en hjemmeside med informasjon,

Tekstboks 9

En god sikkerhetskultur kan bidra til å forhindre sikkerhetshendelser av forskjellige slag

- Mange infeksjoner av datavirus og ormer kan unngås ved at virksomheter er oppmerksomme på behovet for å oppdatere systemer, og ved at brukere er forsiktige ved bruk av tjenester tilknyttet Internett. Ifølge Mørketallsundersøkelsen for 2003 ble norske virksomheter utsatt for 150 000 virusinfeksjoner i løpet av dette året.
- Oppmerksomme brukere og virksomheter kan bidra til å hindre den økende mengden svindelforsøk som forekommer på Internett. Norske bankkunder har for eksempel i 2005 blitt utsatt for forsøk på såkalt phishing, der kunden gjennom en e-post blir forsøkt lurt til å legge inn personlige data på en nettside som framstår som vedkommendes bank eller lignende, men som i realiteten kontrolleres av en svindler.
- Å legge vekt på sikkerhet er også viktig når man utvikler systemer, for å unngå for eksempel hendelser av den typen som Hardanger Sunnhordlandske Dampskipsselskap opplevde i september 2004: En ny plassbestillings- og billettjeneste på Internett ga muligheter til å skrive ut gratis billetter og hente ut personopplysninger om andre kunder som hadde kjøpt billetter.
- En kultur for å overholde retningslinjer som utarbeides, kan bidra til å hindre sikkerhetshendelser. For eksempel ble anslagsvis 40 millioner kredittkortnummer, herunder også en del utstedt i Norge, eksponert for inntrengere da hackere brøt seg inn i systemene til den amerikanske betalingssentralen CardSystems Solutions mot slutten av 2004. Innbruddet ble først oppdaget i mai 2005. Ifølge selskapets retningslinjer skulle ikke kredittkortnumrene vært lagret i deres systemer.

Kilde: Se vedlegg 1.

og ikke i om man har informasjon og tjenester som fører til faktisk handling og bedre resultater i bedriftene.[214]

Gjennomgangen nedenfor fokuserer på følgende forhold:

- offentlig sektors rolle som drivkraft for informasjonssikkerhet for samfunnet som helhet
- hvilket arbeid som gjennomføres for å øke bevissthetene om og kompetansenivået for informasjonssikkerhet
- hva som gjøres for å fremme bruken av internasjonale standarder og veiledningsmateriale

5.2.1 Offentlig sektor som drivkraft for informasjonssikkerhet

Offentlig sektor er en betydelig aktør i informasjonsbehandling i Norge, og en god sikkerhetskultur i offentlig sektor vil ha betydning for landet som helhet. OECDs

211) OECD retningslinjer for sikkerhet i informasjonssystemer og nettverk – Mot en sikkerhetskultur, oversettelse av NHD 2002, side 5

212) Næringslivets Sikkerhetsråds svar på Riksrevisjonens spørreliste av 14. mars 2005

213) IKT-Norges svar på Riksrevisjonens spørreliste av 28. februar 2005

214) Abelias svar på Riksrevisjonens spørreliste av 4. mars 2005

handlingsplan viser til at det offentlige kan bidra til utvikling og bruk av standarder for god praksis ved å framstå som en mønsterbruker. Handlingsplanen nevner også at offentlig sektor kan benytte rollen som stor innkjøper til å påvirke utviklingen av sikre produkter og tjenester og økt tilgjengelighet for slike. Som et ledd i offentlig sektors ansvar for informasjonssikkerhet understreker OECD at det er viktig at sektoren tar ansvar for å sikre egne systemer og nettverk på lik linje med andre sektorer.[215]

Vurderinger av IT-sikkerhet i offentlig sektor
Moderniseringsdepartementet er enig med OECD i at det offentlige bør ha en rolle som mønsterbruker, men mener at OECDs utsagn bør tolkes slik at det er ønskelig at offentlig sektor bruker ressurser på dette området.[216] Departementet mener at offentlig sektor har et ansvar for å påvirke og utvikle en sikkerhetskultur, bl.a. basert på at IT-sikkerhet er et dynamisk felt der det ikke finnes noen tradisjoner for eller kunnskap om hvordan man bør agere. Men etter departementets mening er det vanskelig å vurdere i hvor stor grad det offentlige bør satse på dette området.

Moderniseringsdepartementet mener det er mulig at overføringsverdien mellom offentlig sektor og næringslivet er begrenset, men understreker viktigheten av at allmennheten har tiltro til offentlige systemløsninger rettet mot offentligheten.[217] Offentlige systemløsninger som kan nevnes i denne sammenheng, er *MinSide* og *Felles sikkerhetsportal for offentlig sektor*. Det framgår for øvrig også av departementets handlingsplan for oppfølging av Nasjonal strategi for informasjonssikkerhet at det vektlegger å etablere et informasjonssikkerhetsarbeid og -nivå som gir tillit til forvaltningens informasjonssikkerhet. Slik tillit blir sett på som en nødvendig forutsetning for å gjennomføre elektronisk forvaltning.[218]

Bransjeorganisasjonene har gitt uttrykk for at sikkerhetskulturen i det offentlige i dag ikke er et forbilde for private virksomheter. Næringslivets Sikkerhetsråds erfaring er at det er de offentlige organene som slurver mest med IT-sikkerhet.[219] Abelia mener at private virksomheter stort sett har fått på plass en bedre sikkerhetskultur og en mer moderne ansvarstenking enn offentlig sektor.[220]

Datatilsynet mener at offentlig sektor er spesielt viktig for oppbyggingen av en sikkerhetskultur i samfunnet.[221] Tilsynet tror at staten i mye større grad kunne utnyttet de styringskanalene som faktisk er til disposisjon, for å påvirke i riktig retning. Det er da en forutsetning at det tas velfunderte beslutninger, at klare mål etableres, og at disse følges opp.

For øvrig kan vi nevne at Den Norske Dataforening i samarbeid med Rambøll Management i 2004 gjennomførte en spørreundersøkelse om IT-anvendelsen i de 500 største private og offentlige virksomhetene i Norge. Når det gjelder prioriterte satsingsområder for virksomhetene, viser undersøkelsen at virksomheter i offentlig sektor mener at forbedring av IT-sikkerheten vil få en langt lavere prioritet i 2007 enn i dag. [222] I privat sektor er det liten endring i prioriteringen av området.

Tiltak for å fremme IT-sikkerhet innen offentlig sektor
Nasjonal strategi for informasjonssikkerhet har ikke knyttet egne mål til offentlig sektors rolle som drivkraft for samfunnet ellers. De enkelte offentlige etatene har i utgangspunktet ansvar for informasjonssikkerheten innenfor egen virksomhet. Strategien inneholder enkelte tiltak som kan ha betydning for informasjonssikkerhet i offentlig sektor og for sektorens rolle i samfunnet.[223] Det skal bl.a. utarbeides generelle IT-sikkerhetsnormer for offentlige virksomheter og en generell mal for policy for IT-sikkerhet i offentlige virksomheter.[224]

I Norge finnes det i liten grad regler eller normer for IT-sikkerhet som er spesifikke for offentlig sektor. Reglene i og i medhold av sikkerhetsloven og personopplysningsloven har betydning for IT-sikkerhet i deler av offentlig sektor, selv om reglene også gjelder ut over offentlig sektor. Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) gjelder hele offentlig sektor og inneholder krav til IT-sikkerhet, men fokuserer hovedsakelig på sikker kommunikasjon ved hjelp av elektroniske signaturer. [225] Det foreligger for øvrig normer for IT-sikkerhet innen enkelte sektorer. Nasjonal strategi for informasjonssikkerhet omtaler for eksempel utvikling av IT-sikkerhetsnormer for helsesektoren. Disse normene forventes lansert høsten 2005.

Det framgår av Moderniseringsdepartementets handlingsplan for Nasjonal strategi for informasjonssikkerhet at departementet ikke planlegger å utarbeide generelle IT-

215) OECD: Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

216) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

217) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

218) Moderniseringsdepartementet: Handlingsplan for oppfølging av Nasjonal strategi for informasjonssikkerhet, mars 2005

219) Næringslivets Sikkerhetsråds svar på Riksrevisjonens spørreliste av 14. mars 2005

220) Abelias svar på Riksrevisjonens spørreliste av 4. mars 2005

221) Datatilsynets svar på Riksrevisjonens spørreliste av 28. februar 2005

222) IT i praksis – strategi, trender og erfaringer i norske virksomheter, Den Norske Dataforening/Rambøll Management, side 41–42

223) En stor del av tiltakene i strategien er rettet mot samfunnet som helhet. Disse kan også få betydning for offentlig sektor.

224) Nasjonal strategi for informasjonssikkerhet, side 20

225) Forskriften er gitt i medhold av forvaltningsloven og lov om elektronisk signatur.

Tekstboks 10

Det foreligger regler og normer for IT-sikkerhet innen offentlig sektor i mange land. Krav til sikkerhet har vært særlig i fokus i USA, der kongressen har lovfestet krav til IT-sikkerhet i føderale virksomheter. Kravene følges opp ved at en rapport om overholdelse av loven årlig legges fram for kongressen, og en komité i kongressen setter på grunnlag av rapporten karakterer på IT-sikkerheten i de enkelte departementene. I februar 2005 fikk syv departementer strykkarakter, og flere andre departementer fikk svake karakterer.

I Europa har arbeidet med retningslinjer for IT-sikkerhet blitt intensivert i forbindelse med utbyggingen av elektronisk forvaltning. Danske myndigheter har vedtatt at offentlige virksomheter skal følge dansk standard for IT-sikkerhet fordi god sikkerhet anses som en forutsetning for å lykkes med elektronisk forvaltning. I Storbritannia har The Office of the e-Envoy utgitt flere standarder for hvordan offentlige virksomheter skal sikre sine tilbud om elektronisk samhandling, mens Bundesamt für Sicherheit in der Informationstechnik i Tyskland har utarbeidet en omfattende e-forvaltningshåndbok der sikkerhet er gitt en sentral plass.

Kilde: Se vedlegg 1.

sikkerhetsnormer for offentlige virksomheter. Departementet planlegger derimot å gjennomføre eksempelprosjekter som skal vise hvordan kommuner og statlige etater kan nyttiggjøre seg internasjonale standarder på området.[226] Handlingsplanen nevner også at det skal utvikles en generell mal for policy for IT-sikkerhet. Disse tiltakene skal ifølge planen gjennomføres i løpet av 2005 og 2006 uten nærmere angivelse av tidsfrist.

I løpet av 2005/2006 skal Moderniseringsdepartementet også vurdere om det skal settes i gang et eksempelprosjekt for identifisering og klassifisering av systemer og infrastruktur i statlige og kommunale virksomheter. Prosjektet kan gi grunnlag for å utvikle retningslinjer for vurdering av risiko og overordnede retningslinjer for IT-sikkerhet. Departementet skal følge opp klassifisering av systemer og infrastruktur i hele offentlig sektor i 2006. I løpet av 2005/2006 skal departementet for øvrig også vurdere om det skal utarbeides en sjekkliste og veiledning for gjennomføring av egenvurdering av intern kontroll.

Ifølge Nasjonal strategi for informasjonssikkerhet skal det arbeides for at etablerte standarder for IT-sikkerhet tas i bruk ved offentlige og private IT-anskaffelser.[227] Moderniseringsdepartementets handlingsplan fra mai 2005 angir at dette skal følges opp løpende, uten at det er gitt noen nærmere angivelse av hvilke tiltak som skal gjennomføres. Under dette temaet kan vi for øvrig nevne at Nasjonal sikkerhetsmyndighet, med hjemmel i forskrift gitt i medhold av sikkerhetsloven, har stilt krav om at enkelte systemer i Forsvaret skal være sertifisert i henhold til Common Criteria, jf. omtale av standard for sertifisering av produkter nedenfor.[228] Nasjonal sikkerhetsmyndighet mener det vil være en stor fordel om det settes krav til sertifiserte produkter også utover dette i offentlig sektor og i samfunnskritiske virksomheter. Dette kan gi drahjelp til sertifiseringsordningen og være et eksempel til etterfølgelse for næringslivet. [229]

5.2.2 Tiltak for bevisstgjøring og kompetanseheving

Bevisstgjøringstiltak overfor allmennheten

Utvikling av en sikkerhetskultur krever at myndighetene gjennomfører tiltak rettet mot bevisstgjøring og støtter andre initiativ rettet mot økt forståelse for informasjonssikkerhet.[230] Nasjonal strategi for informasjonssikkerhet inneholder enkelte tiltak rettet mot bevisstgjøring som et grunnlag for å utvikle en sikkerhetskultur. Tabell 1 gir en oversikt over tiltakene og status for iverksettelse av disse.

Tabell 1 viser at bare ett av fem bevisstgjøringstiltak er gjennomført. Det ene tiltaket som delvis er gjennomført, er knyttet til etablering av en informasjonstjeneste på nett (b). Det var opprinnelig planer om en kampanje for økt bevissthet om IT-sikkerhet for husholdninger (c) og små og mellomstore bedrifter som en del av lanseringen av portalen nettvett.no. I samarbeid med Nærings- og handelsdepartementet prøvde Samferdselsdepartementet å få leverandører av IT-produkter og -tjenester til å finansiere en kampanje til ca. 7–8 millioner kroner. De private virksomhetene som ble forespurt, var ikke villige til å delta i finansiering av en kampanje av denne størrelse, og kampanjen blir derfor ikke gjennomført. Departementene ønsket ikke å finansiere kampanjen utelukkende med offentlige midler, fordi de mente at også leverandørene har et viktig ansvar innenfor dette området.[231] Portalen nettvett.no ble lansert 26. april 2005, men den gir i mindre grad muligheter for å få svar på spørsmål enn opprinnelig planlagt. Ved lanseringen ble det avholdt et seminar i samarbeid med næringslivsaktørene, og man søkte å skape interesse i media rundt lanseringen av portalen (”nettvett-dag”).

Hovedkilden for angitt status i Tabell 1 er Moderniseringsdepartementets handlingsplan av mai 2005. Nærings- og handelsdepartementets handlingsplan av

226) Moderniseringsdepartementet: Handlingsplan for oppfølging av Nasjonal strategi for informasjonssikkerhet, mars 2005

227) Nasjonal strategi for informasjonssikkerhet, side 24

228) Forskrift om informasjonssikkerhet § 5-20. Forskriften bestemmer at fellesnivå-informasjonssystemer får graderingen hemmelig eller høyere, flernivå-informasjonssystemer og kryptoutstyr skal sertifiseres.

229) Jf. e-post fra Nasjonal sikkerhetsmyndighet ved dir. Jan Erik Larsen til Riksrevisjonen 3. juni 2004

230) Jf. OECD: Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, side 4

231) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

Tabell 1 Oversikt over bevisstgjøringstiltak i Nasjonal strategi for informasjonssikkerhet, ansvar og status

Tiltak	Ansvarlig[232]	Status
a) Utvikle og spre informasjons- og veilednings materiell om IT-sikkerhet til husstandene	NHD, JD	Vurderes løpende, ingen nærmere angivelse
b) Etablere en informasjonstjeneste på nett med generell informasjon, lenker og mulighet til å få svar på spørsmål fra publikum	NHD, JD	Portalen nettvett.no lansert april 2005 av SD/PT. Det er begrenset mulighet for publikum til å stille spørsmål
c) Gjennomføre en informasjonskampanje for å spre kjennskap til god praksis for IT-sikkerhet i husstandene	NHD, JD	SD/NHD fant ikke finansiering til å gjennomføre tiltaket. "Nettvett-dag" arrangert 26. april 2005
d) Utvikle en "undervisningspakke" for grunnskole og videregående skole med vekt på IT-sikkerhet	NHD, UFD, NLS	Planlagt våren 2006
e) Arbeide for at produkter og systemer rettet mot massemarkedet ledsages av lettfattelig opplysnings- og opplæringsmateriale innen IT-sikkerhet	NHD, bransjeorg. (Abelia, IKT-Norge)	Innlede samarbeid med bransje-organisasjonene og NHO med oppstart i juni 2005. Ingen konkret tids-angivelse for dette tiltaket

Kilder: Nasjonal strategi for informasjonssikkerhet og Moderniseringsdepartementets handlingsplan av mai 2005

februar 2004 viste imidlertid en tidligere gjennomføring av flere av disse tiltakene:

- Utvikling og spredning av informasjons- og veiledningsmateriale (a) skulle gjennomføres høsten 2004, med senere løpende oppdateringer. Det er ikke gjennomført tiltak på dette området, og det er i siste handlingsplan ikke gitt en nærmere tidsangivelse eller konkretisering av gjennomføringen.
- Undervisningspakken til skoleverket (d) var planlagt utarbeidet våren 2005, men tidspunktet har senere blitt forskjøvet til våren 2006. Undervisningspakken er tenkt knyttet til SAFT-prosjektet, som er et europeisk samarbeid ledet av Medietilsynet i Norge.[233] Det skal spre kunnskap om trygg bruk av Internett til barn og unge, foreldre, lærere og andre. Moderniseringsdepartementet hatt noe kontakt med Utdannings- og forskningsdepartementet og prosjektlederen for SAFT-prosjektet, og vurderer det slik at Utdannings- og forskningsdepartementet er positivt til at det informeres om IT-sikkerhet i skolene, men at det ikke ønsker å ha ansvar for å utarbeide undervisningsmaterialet. Moderniseringsdepartementet har gitt uttrykk for at det er en dragkamp mellom departementene om hvem som skal finansiere dette, og det har vært en tyngre prosess enn hva departementet forutså.[234]
- Det er ikke gjennomført aktiviteter for å utvikle lettfattelig opplysnings- og opplæringsmateriale innen IT-sikkerhet for produkter og systemer rettet mot massemarkedet (e). Oppstart av samarbeidet med bransje-organisasjonene og NHO er forskjøvet fra mai 2004 til juni 2005.

Kompetanse og utdanning

Sårbarhetsutvalget så manglende bevissthet og kompetanse innen mange virksomheter som et hovedproblem innen IKT-sikkerhet.[235] Utvalget la til grunn at det var et behov for å styrke IT-utdanningen med fokus på sikkerhet på alle nivåer fra videregående skole til universitet, fordi kompetent personell ble ansett som mangelvare. Denne konklusjonen samsvarer med resultatene fra arbeidet til IT-sårbarhetsutvalget fra oktober 2000.[236] OECD har også pekt på betydningen av videre innsats for å utvikle utdanningsprogrammer for informasjonssikkerhet.

Status for planlagte tiltak

Nasjonal strategi for informasjonssikkerhet inneholder enkelte tiltak for å forbedre kompetansen på IT-sikkerhet i Norge. Tabell 2 gir en oversikt over tiltakene og status i disse.

Tabell 2 viser at det har vært en del aktivitet på dette området de senere årene. Tre av tiltakene som er iverksatt, var imidlertid delvis etablert og/eller planlagt før strategien ble lansert i 2003. Det gjelder studium i IT-sikkerhet (c), forskningsprogram (d) og forskningsprosjekt (e).

To av disse tiltakene var oppfølging av forhold tatt opp av Sårbarhetsutvalget og IT-sårbarhetsutvalget: Studiet i informasjonssikkerhet på mastergradsnivå ved Høgskolen i Gjøvik (c) ble støttet av en rekke private virksomheter, Statens nærings- og distriktsutviklings-

232) Tiltak og ansvar hentet fra Nasjonal strategi for informasjonssikkerhet, side 22 og 24. Moderniseringsdepartementet har senere overtatt ansvaret for de fleste av tiltakene fra Nærings- og handelsdepartementet. Samferdselsdepartementet har fått noe større ansvar for gjennomføringer av tiltak enn angitt i strategien.

233) Jf. Moderniseringsdepartementets handlingsplan av mars 2005, samt referat fra møte i Koordineringsutvalget for informasjonssikkerhet 23. november 2004. SAFT er en forkortelse for Safety, Awareness, Facts and Tools.

234) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

235) NOU 2000:24 Et sårbart samfunn, side 72

236) Samfunnets sårbarhet som følge av avhengighet til IT, Nærings- og handelsdepartementet, oktober 2000, side 103

Tabell 2 Oversikt over kompetansehevende tiltak i Nasjonal strategi for informasjonssikkerhet, ansvar og status

Tiltak	Ansvarlig [239]	Status
a) Arbeide for at ledere i private og offentlige virksomheter tar ansvar for at virksomheten har tilstrekkelig kompetanse innen IT-sikkerhet	NHD, AAD, bransjeorg.	MOD mener tiltaket dekkes gjennom eksempelprosjekter og verktøykasse for ROS-metodikk .
b) Styrke undervisningen i IT-sikkerhet i utdannelser der bruk av IT er en integrert del. Utarbeide læreplaner og materiell til støtte for undervisningen	UFD, NHD	Løpende oppgave. Konkrete tiltak ikke angitt
c) Etablere flere høyere utdanninger innen IT-sikkerhet på mastergradsnivå med godkjenning	UFD, FD, JD NHD, SD, FD	Norwegian Information Security Laboratory, som grunnlag for et studium i IT-sikkerhet ved HiG, ble stiftet i januar 2003. Formelt akkreditert i 2004. Ingen initiativ for øvrig om studier på dette nivået
d) Gjennomføre et forskningsprogram innen IT-sikkerhet. Privat næringsliv skal delta, og doktorgradskandidater skal utdannes.	NFR, NHD, JD, FD	Programmet ble iverksatt før strategien ble lagt fram. NFR legger vekt på å involvere næringslivet og utdanne doktorgrads-kandidater.[240]
e) Sette i gang et forskningsprosjekt om tiltak for å sikre samfunnskritisk IT-infrastruktur og systemer (BAS-5)	DSB, NSM, JD, FD, NHD	Forskningsprosjekt igangsatt og planlagt avsluttet i 2007

Kilder: Nasjonal strategi for informasjonssikkerhet, Moderniseringsdepartementets handlingsplan av mai 2005, programbeskrivelse for forskningsprosjektet IKT Sikkerhet og Sårbarhet, opplysninger på nettsidene til Høgskolen i Gjøvik (HiG).

fond og Norges forskningsråd. De første studentene ble tatt opp høsten 2002. Moderniseringsdepartementet har uttalt at dette tilbudet kom på plass mer eller mindre av seg selv, fordi flere aktører så behovet og man klarte å få til en samfinansiering.[237] Det er ikke tatt initiativ til å utvikle flere høyere studier innen IT-sikkerhet. Sårbarhetsutvalget foreslo videre at det burde opprettes et strategisk forskningsprogram innen IT-sikkerhet. På oppdrag fra Nærings- og handelsdepartementet etablerte Norges forskningsråd i 2003 et nytt forskningsprogram innenfor IT-sikkerhet og sårbarhet som skal løpe fram til 2007.[238]

Tabellen viser for øvrig at det ikke er tatt initiativ for å styrke undervisningen i IT-sikkerhet/utarbeide læreplaner osv. (b). Det er satt opp noen aktiviteter som skal bidra til å heve kompetansen om IT-sikkerhet i det offentlige og i virksomhetene (a). I Nærings- og handelsdepartementets handlingsplan fra februar 2004 ble det lagt til grunn en noe annen tidsplan og ansvarsdeling for dette tiltaket; det skulle settes i gang et samarbeid med bl.a. IKT-Norge og Abelia med etablering av en prosjektgruppe i juni 2004 for å planlegge en tiltakspakke. Dette samarbeidet ble imidlertid ikke etablert.

Vurderinger av kompetanse og utdannelsestilbud

Behovet for kompetanse om IT-sikkerhet ble tatt opp i vår spørreundersøkelse til alle virksomheter og organisasjoner med gjennomføringsansvar i den nasjonale strategien. Betydningen av IT-sikkerhetskompetanse understrekes av flere av virksomhetene. Nasjonal sikkerhetsmyndighet uttaler for eksempel at kompetanse er den viktigste faktoren for å oppnå tilfredsstillende informasjonssikkerhet. Senter for informasjonssikring mener at årsaken til svært mange av de uønskede sikkerhetshendelsene som inntreffer, kan tilskrives manglende kompetanse i utviklingsprosessen.

Virksomhetene mener det er et stort behov for kompetanse. Senter for informasjonssikring beskriver behovet som skrikende. Både Nasjonal sikkerhetsmyndighet og Datatilsynet mener det er et stort behov for grunnleggende kompetanse innen dette området, både for de som skal håndtere informasjonssikkerhet rent praktisk ute i organisasjonene, og for beslutningstakere. IKT-Norge uttaler at det er et meget stort behov for mer kompetanse når det gjelder sikkerhet på alle nivåer. Abelia anser at behovet er størst for gode og relevante kurs- og etterutdanningstilbud, ikke minst for ledere/mellomledere. Abelia anser ikke teknologi som utfordringen, men kunnskap om lover/regler, innsikt i sikkerhetsarbeid, kunnskap om personvern, osv.

Det tilbudet om utdanning i IT-sikkerhet som er utviklet ved Høgskolen i Gjøvik, omtales positivt av flere virksomheter. IKT-Norge nevner for eksempel at Gjøvikmiljøet virker meget positivt, og mener at dette bør

237) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

238) Forskningsprogrammet er omtalt i St.prp. nr. 1 (2003–2004) for Nærings- og handelsdepartementet i tilknytning til bevilgninger til Norges forskningsråd under kapittel 920.

239) Tiltak og ansvar hentet fra Nasjonal strategi for informasjonssikkerhet, side 22–25. Moderniseringsdepartementet har senere overtatt ansvaret for de fleste av tiltakene fra Nærings- og handelsdepartementet.

240) IKT Sikkerhet og Sårbarhet (IKT SoS), programbeskrivelse, revidert februar 2004

Scanpix Creative/Corbis

utnyttes mer. De fleste av virksomhetene gir imidlertid uttrykk for at IT-sikkerhet ikke ivaretas godt nok når det gjelder andre relevante studier. IKT-Norge uttaler at det er altfor lite fokusering på sikkerhet i utdanningen. Datatilsynet er av den oppfatning at informasjonssikkerhet ikke er godt nok ivaretatt i studier, utover de studiene som har direkte med informasjonssikkerhet å gjøre. Senter for informasjonssikring er spesielt opptatt av utdanningen av utviklingspersonell, der senteret har tatt til orde for en større vektlegging av sikkerhet. Senteret mener at det tilbys god utdanning i sikkerhet ved en rekke høgskoler og universitet, men at flere av disse retningene tilbys isolert og ikke settes sammen med utdanning i utviklingsfag. Abelia gir uttrykk for at det eksisterende IT-utdannelsestilbudet er bra, men mener at behovet for denne typen kompetanse i samfunnet vil øke kraftig framover, og at det således er viktig også å øke utdanningstilbudet.

Moderniseringsdepartementet mener at informasjonssikkerhet er godt dekket innen høyskolesektoren, og viser til utdannelsestilbudet på mastergradsnivå ved Høgskolen i Gjøvik som vil bli utvidet til å inkludere et tilbud på bachelor-nivå. Dette fungerer ifølge departementet godt.[241]

5.2.3 Bruk av internasjonale standarder og veiledningsmateriale

God praksis kan uttrykkes i form av internasjonale standarder, men kan også ha en enklere form i retningslinjer eller veiledninger for hvordan relevante fagmiljøer mener visse funksjoner bør utføres. Begge disse aspektene av begrepet omtales under dette punktet.

Det finnes en rekke internasjonale standarder av betydning for informasjonssikkerhet. Blant disse er det spesiell grunn til å nevne ISO15408 om sertifisering av produkter og ISO17799 om administrasjon av informasjonssikkerhet. I tilknytning til ISO15408 er det etablert et system for sertifisering av produkter, der et avtaleverk sikrer at sertifiseringer av produkter i et land anerkjennes også i andre land som deltar i ordningen. Organisasjoner kan ikke sertifiseres i henhold til ISO17799, men sertifisering kan gjennomføres i henhold til den tilknyttede standarden BS7799 del 2.[242] Tiltak for å fremme disse standardene er tatt inn i Nasjonal strategi for informasjonssikkerhet.[243]

Innføring av sertifiseringsordninger for IT-produkter og organisasjoner

Stortinget ba i B. Innst. S. nr. 1 (1996–1997) regjeringen om å legge fram for Stortinget en egen sak om oppretting av et sertifiseringsorgan for sikre dataløsninger i løpet av våren 1997. Rådet for IT-sikkerhet utredet saken og la fram et forslag høsten 1997.[244] Rådet foreslo å opprette én ordning for sertifisering av produkter og én ordning for å sertifisere IT-sikkerhet i organisasjoner. St.prp. nr. 1 (1998?99) for Nærings- og handelsdepartementet slo fast at det skulle opprettes en sertifiseringsmyndighet for IT-produkter og -systemer. Denne myndigheten skulle legges til daværende Forsvarets overkommando/Sikkerhetsstaben, noe som ga grunnlaget for å etablere Sertifiseringsmyndigheten for IT-sikkerhet (SERTIT). SERTIT er nå en del av Nasjonal sikkerhetsmyndighet, som er underlagt Forsvarsdepartementet.

I den samme proposisjonen ble det også foreslått å etablere en ordning for sertifisering av IT-sikkerhet i organisasjoner. Denne skulle legges til Norsk Akkreditering. Akkrediteringsdelen av ordningen ble etablert i november 1999. De første pilotprosjektene for sertifisering ble gjennomført i 2001, da ordningen ble operativ. Per juni 2005 er ti norske virksomheter sertifisert i henhold til BS7799 del 2.[245]

Nærmere om etableringen av SERTIT

Etter at SERTIT ble opprettet, tok det en viss tid før enheten var operativ; det ble ikke ansatt personell før

241) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

242) ISO17799 beskriver hvilke kontroller som bør foreligge, mens BS7799 del 2 i tillegg gir anvisninger for hvordan en virksomhet etablerer et styringssystem basert på disse kontrollene. BS7799 del 2 skal også utgis som internasjonal standard (ISO27001). Den forventes å foreligge senhøsten 2005, jf. http://www.bsi-global.com/ICT/Security/bs7799-2.xalter.

243) I strategien omtales BS7799 i stedet for ISO17799.

244) Rådet for IT-sikkerhet: Sertifisering av IT-sikkerhet i produkter, systemer og organisasjoner (sluttrapport), 13. november 1997

245) Følgende virksomheter er sertifisert: BBS, Conax AS, Elopak AS, ErgoIntegration AB, Larvik kommune, Mnemonic AS, Norsk Informasjonssikkerhet AS, System Sikkerhet AS, Thales Communications AS og VincIT AS, jf. http://www.xisec.com/.

sommeren 2000, og sertifiseringsordningen ble etablert først høsten 2002.[246] Det praktiske arbeidet med evalueringer gjennomføres av evalueringsfirmaer som er godkjent av SERTIT. Da ordningen ble opprettet, ble det gjennomført to prøveevalueringer. Disse resulterte ikke i sertifiseringer av produkter. I mai 2004 utstedte SERTIT det første sertifikatet.[247]

Da forslaget om å etablere SERTIT ble lagt fram i St.prp. nr. 1 (1998–99) for Nærings- og handelsdepartementet, foreslo man samtidig at ordningen burde evalueres etter tre år. Evalueringen forelå i oktober 2004.[248] Den konkluderer med at ordningen oppleves som faglig god, men at den har uklare interne ansvarsforhold og er for lite markedsfokusert. Evalueringen påpeker at ordningen er lite kjent og markedsført, at det er få brukere som etterspør sertifiserte produkter, og at evaluering er kostnadskrevende for produsentene. Evalueringen bemerker videre at når antallet sertifiseringer er så lavt som hittil, gir ikke dette evalueringsfirmaene mulighet til å beholde sin kompetanse og et kommersielt grunnlag til å opprettholde sin aktivitet. Ordningens framtid anses avhengig av at flere produkter blir evaluert og sertifisert. Evalueringen tar til orde for at sertifiseringsordningen bør ses på som en del av den nasjonale infrastrukturen som er nødvendig for å ivareta IT-sikkerhet. Rapporten legger til grunn at Stortingets og regjeringens forutsetninger for organisatorisk plassering, rammebetingelser og forankring langt på vei er oppfylt, men at det gjenstår å få til status som gir internasjonal aksept for norske sertifikater, og at det i høy grad gjenstår å få til etterspørsel etter sertifiserte produkter.

Forsvarsdepartementet mener at det, ut fra de ressursene som nedlegges i ordningen, er bekymringsfullt at det gjenstår mye for å få gjort ordningen tilstrekkelig kjent. Departementet gir uttrykk for at nye tiltak for en langsiktig og målrettet markedsføring er nødvendig.[249]

Tiltak for å fremme sertifiseringsordningene
Ifølge Nasjonal strategi for informasjonssikkerhet bør sertifiseringsordningene tas i bredere bruk av norske virksomheter, etablerte standarder for IT-sikkerhet bør tas i bruk ved offentlige og private IT-anskaffelser, og informasjon om standarder og deres anvendelsesområde skal styrkes.[250] Moderniseringsdepartementet og Justis- og politidepartementet har opplyst at dette er langsiktige oppgaver som følges opp løpende.[251] I oppfølgingsplanene til Nasjonal strategi for informasjonssikkerhet framhever departementene at regelverk skal utvikles i samsvar med internasjonale standarder. Det er imidlertid ikke oppgitt hvilke regelverk det er aktuelt å harmonisere med standardene.[252] For øvrig viser oppfølgingsplanene til et eksempelprosjekt som skal vise hvordan kommuner og offentlige etater kan nyttiggjøre seg internasjonale standarder, jf. omtale i punkt 5.2.1.[253]

Nasjonal sikkerhetsmyndighet er gjennom iverksettingsbrevet for 2005 pålagt å bidra aktivt til å skape økt

Tekstboks 11

Internasjonale erfaringer viser at det er vanskelig å få virksomheter til å benytte standarder som ISO17799. Per juni 2005 er 1315 virksomheter sertifisert etter BS7799 del 2 på verdensbasis. Det siste året har det vært en klar vekst i sertifiserte virksomheter i asiatiske land, slik at nesten halvparten av de sertifiserte virksomhetene i verden er japanske.

Britiske myndigheter har i flere år arbeidet for å øke utbredelsen av dens britiske utgangspunkt, BS7799. En undersøkelse i 2004 viste at bare 39 % av store virksomheter var klar over at standarden fantes, og hadde kunnskap om innholdet. For mindre virksomheter var andelen langt mindre, og disse betraktet standarden som krevende og kostbar å innføre. Undersøkelsen viste imidlertid at mange av virksomhetene som kjente standardens innhold, la denne til grunn for sikkerhetsarbeidet.

I Sverige og Danmark er det gjennomført tiltak som sikrer utbredelse av standarder tilsvarende ISO17799. I Sverige setter Krisberedskapsmyndigheten krav om at alle sivile virksomheter som er underlagt deres kontroll, skal følge standarden "Allmänna råd till föreskrifter om grundsäkerhet för samhällsviktiga datasystem hos beredskapsmyndigheter". Ifølge Krisberedskapsmyndigheten er kravene i denne standarden sammenfallende med den internasjonale standarden ISO17799. I Danmark ble det i januar 2004 obligatorisk for alle statlige virksomheter å følge en felles standard for informasjonssikkerhetsprosesser etter en tre-årig innføringsperiode. Standarden "Norm for edb-sikkerhed del 1" har sterke likhetstrekk med ISO17799.

Kilde: Se vedlegg 1.

246) Jf. pressemelding fra SERTIT 14. oktober 2002: Offentlig godkjenning av sikkerhet i IT-produkter

247) Ifølge opplysninger på SERTITs nettsider ble Thales Operator Terminal Adapter (OTA) godkjent 19. mai 2004. Jf. pressemelding fra SERTIT 1. juni 2004: Første norskutviklede IT-produkt sikkerhetssertifisert

248) Statskonsult: Evaluering av ordningen for sertifisering av IT-sikkerhet i produkter og systemer, 1. oktober 2004

249) Notat i Forsvarsdepartementet av 10. januar 2005: Evaluering av SERTIT – Kommentarer til evalueringsrapporten

250) Nasjonal strategi for informasjonssikkerhet, side 24

251) Jf. Nasjonal strategi for informasjonssikkerhet ? NHDs oppfølgingsplan, notat av 4. februar 2004, MOD: Handlingsplan for oppfølging av Nasjonal strategi for informasjonssikkerhet, mars 2005, e-post fra Moderniseringsdepartementet til Riksrevisjonen av 10. juni 2005, og brev fra Justis- og politidepartementet til Nærings- og handelsdepartementet av 20. februar 2004 med tittelen Nasjonal strategi for informasjonssikkerhet – Oppfølgingsplaner

252) Jf. Status i oppfølgingen og koordinering av Nasjonal strategi for informasjonssikkerhet per 4. mai 2005, utarbeidet av sekretariatet for KIS

253) Jf. MOD: Handlingsplan for oppfølging av Nasjonal strategi for informasjonssikkerhet, mars 2005

forståelse for og bruk av sertifiserte produkter. Nasjonal sikkerhetsmyndighet har gitt uttrykk for at det ville vært en stor fordel om det offentlige i sin innkjøpspolicy satte sikkerhetsmessige krav til produkter basert på standarden Common Criteria (ISO15408). Direktoratet mener dette ville gi drahjelp til ordningen og være et eksempel til etterfølgelse for næringslivet.[254]

Moderniseringsdepartementet ser på sertifiseringsordningene som et tilbud det er opp til brukerne å benytte seg av. Departementet kan bare legge forholdene til rette. Utover dette har ikke Moderniseringsdepartementet noen konkrete planer for å fremme ordningene, som er forutsatt å være markedsbaserte.[255]

Vurderinger av sertifiseringsordningene
I spørreundersøkelsen til virksomheter og organisasjoner ba Riksrevisjonen om vurderinger av sertifiseringsordningene slik de er implementert i Norge. Virksomhetene gir uttrykk for at sertifiseringsordningene og standardene disse bygger på, er lite kjent i forvaltningen og i næringslivet. Både IKT-Norge og Næringslivets Sikkerhetsråd mener at det særlig er små og mellomstore bedrifter som ikke kjenner standardene. Datatilsynet uttaler at det må tas helt andre grep enn det som har vært gjort så langt, om ordningen skal få den tiltenkte verdi.

Senter for informasjonssikring nevner at få sertifikater er utstedt i Norge basert på standard for administrasjon av informasjonssikkerhet, og at bare et fåtall store virksomheter har opplyst til senteret at de legger standarden til grunn for sitt sikkerhetsarbeid. Senteret mener at antallet kan øke når en ny versjon av denne standarden kommer i løpet av 2005.[256]

Senter for informasjonssikring peker også på andre årsaker til at sertifisering ikke er mer utbredt. Det er ifølge senteret så langt ingen markedsmessige fordeler med å være sertifisert. Siden kostnadene ved å sertifisere en virksomhet er forholdsvis store, vil dette dempe utbredelsen. IKT-Norge nevner som en årsak at noen kunder, særlig det offentlige, har hovedfokus på pris. Ifølge organisasjonen øker kostnadene ved omfattende krav til standarder, og det velges dermed bort. Næringslivets sikkerhetsorganisasjon er også bekymret for at kostnadene ved implementering av standarder vil overstige de positive effektene, særlig for de minste bedriftene.

Moderniseringsdepartementet mener at standarden for administrasjon av informasjonssikkerhet har større betydning enn hva antall sertifiserte virksomheter indikerer.[257] Departementet viser til at Datatilsynets regelverk er basert på standarden, men at det her ikke er nødvendig med sertifisering. Imidlertid peker departementet på faren for at regelverk med slike krav kan bidra til å undergrave ordningen fordi det ikke skaper etterspørsel etter sertifisering. Sertifisering basert på standarden for produkter og systemer kan ifølge departementet være et mindre hensiktsmessig verktøy i arbeidet med å fremme IT-sikkerhet, fordi ordningen er så komplisert at det hindrer at den benyttes. Departe-mentet ser imidlertid betydningen av å opprettholde ordningene som en del av en nasjonal infrastruktur for IT-sikkerhet.

Myndighetenes veiledningsarbeid for å fremme IT-sikkerhet
OECDs plan for å fremme god sikkerhetskultur tar opp at det er viktig å utveksle god praksis for å fremme brukernes forståelse for og evne til å oppnå målet om effektive og oppdaterte sikkerhetstiltak.[258]

Tiltak i Nasjonal strategi for informasjonssikkerhet
Nasjonal strategi for informasjonssikkerhet inneholder enkelte tiltak som kan ha betydning for utviklingen av god praksis. Disse er hovedsakelig knyttet til utvikling av veiledninger. Tabell 3 gir en oversikt over disse tiltakene og status for iverksettelse.

Tabell 3 viser at det er satt i gang aktiviteter under bare ett av tiltakene. Det gjelder utvikling av verktøy og metoder for risiko- og sårbarhetsvurdering, der det er gjennomført en kartlegging av eksisterende metoder, og der det i løpet av 2005 skal lages en "verktøykasse". De fleste tiltakene i tabellen krever at det etableres kontakt og samarbeid med aktuelle bransjeorganisasjoner, men i undersøkelsesperioden har det ikke vært etablert slikt samarbeid.

Opplysningene om status i Tabell 3 er i hovedsak hentet fra Moderniseringsdepartementets handlingsplan fra mai 2005. Nærings- og handelsdepartementets handlingsplan fra februar 2004 angir en noe annen framdrift; det var planlagt å innlede et samarbeid med bransjeorganisasjonene i mai 2004 med løpende oppfølging av tiltak fra høsten 2004. "Verktøykasse" for gjennomføring av risiko- og sårbarhetsanalyser skulle foreligge i september 2004.

Veiledningsvirksomhet fra Senter for informasjonssikring
Senter for informasjonssikring har publisert en rekke veiledninger om informasjonssikkerhet som er tilgjengelige på senterets nettsted. Hovedmålgruppen for veiledningene er små og mellomstore bedrifter. Utarbeidelsen av materialet kan ses i sammenheng med at senteret har som oppgave å formidle informasjon, kompetanse og kunnskap om trusler og mottiltak. Veiledningene er laget for både ledelse, driftere, utviklere og sluttbrukere.

254) Jf. referat fra møte mellom Nasjonal sikkerhetsmyndighet og Riksrevisjonen 22. april 2004 og e-post fra NSM til Riksrevisjonen 3. juni 2004255) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

256) Ny versjon av ISO17799 ble publisert 15. juni 2005.

257) Referat fra møte mellom Moderniseringsdepartementet og Riksrevisjonen 15. mars 2005

258) Implementation Plan for the OECD Guidelines for the Security of Information Systems and Network: Towards a Culture of Security, punktene 13 og 15

Tabell 3 Oversikt over ulike veiledningstiltak, ansvar og status

Tiltak	Ansvarlig[259]	Status
Utvikle veiledninger for hvordan IT-sikkerhet skal implementeres i systemer og iverksettes i private virksomheter	Bransjeorganisasjoner, sektormyndigheter, NSO	Det foreligger ikke planer for tiltaket.
Utvikle verktøy og metoder for risiko- og sårbarhetsvurdering	NHD, bransjeorganisasjoner, regelverksforvaltere, internasjonale org.	Kartlegging av eksisterende metoder er gjennomført. "Verktøykasse" skal utarbeides innen 31. desember 2005.
Utvikle klassifikasjonsordninger og sikkerhetsnormer for private virksomheters informasjonsbehandling	Bransjeorganisasjoner, NSO	Behov skal vurderes høsten 2005, eventuell oppfølging i 2006.
Leverandører av Internett-aksess bør følge anerkjente sikkerhetsnormer og standarder og synliggjøre hvilken grad av tilgjengelighet, kapasitet og driftsstabilitet som tilbys.	Bransjeorganisasjoner, PT, NHD	Alle disse tiltakene er avhengige av ansvarsavklaring mellom MOD og NHD. Samarbeid med bransjeorganisasjoner og NHO skal innledes i juni 2005. Tiltakspakke skal planlegges fra sept. 2005.
Tjenesteleverandører bør følge anerkjente sikkerhetsnormer og standarder og gjøre kjent hvilket sikkerhetsnivå tjenesten tilbyr.		
Leverandører av IT-systemer bør følge anerkjente sikkerhetsnormer og standarder og tilrettelegge for enklest mulig bruk av sikkerhetsfunksjonalitet i sine systemer.		
Enhver som stiller IT-utstyr og IT-systemer til rådighet for andre, bør følge anerkjente sikkerhetsnormer og standarder, klargjøre sikkerhetsegenskaper og krav for dette, samt tydeliggjøre eget og brukernes ansvar.	Bransjeorganisasjoner, NHD	

Kilder: Nasjonal strategi for informasjonssikkerhet, Moderniseringsdepartementets handlingsplan av mai 2005, programbeskrivelse for forskningsprosjektet IKT Sikkerhet og Sårbarhet, opplysninger på nettsidene til Høgskolen i Gjøvik

Senteret ble i 2004 evaluert av senterets styringsgruppe. Ifølge Moderniseringsdepartementet viser denne evalueringen at erfaringene med senteret stort sett har vært gode. Brukerne etterspør likevel:

- mer aktivt arbeid for å øke bevisstheten rundt sikkerhet hos ledelsen og de ansatte i virksomhetene
- en varslingstjeneste
- formidling av informasjon, kompetanse og kunnskap om trusler og mottiltak til virksomhetenes IT-driftsansvarlige

For å kunne ivareta dette behovet må det ifølge Moderniseringsdepartementet bygges opp operative funksjoner som senteret ikke har i dag.[260]

I møte med Riksrevisjonen har Senter for informasjonssikring poengtert at brukerne har etterspurt praktiske veiledninger for bedre sikkerhet. Senteret har også registrert ønsker om eksempler på god praksis og sjekklister for sentrale områder, og har derfor ønsket å benytte mer ressurser på denne oppgaven.[261] Veiledningene formidles i hovedsak gjennom senterets nettsider.[262] De kan også formidles via andre kanaler, for eksempel gjennom forelesninger som holdes av senterets ansatte, eller via referansegruppene som senteret har opprettet innen visse sektorer.

Vurderinger av Senter for informasjonssikring

I vår spørreundersøkelse til virksomhetene og organisasjonene som har gjennomføringsansvar i den nasjonale strategien, ba vi også om vurderinger av hvordan Senter for informasjonssikring (SIS) løser sine oppgaver.

De fleste virksomhetene påpeker at senteret er lite kjent blant brukerne. IKT-Norge hevder for eksempel at SIS burde ha vært langt mer utadrettet, og at senterets informasjonsoppgaver ikke har blitt ivaretatt. At senteret er lite kjent i næringslivet, ble i stor grad bekreftet av en brukerundersøkelse som ble gjennomført på oppdrag fra

259) Tiltak og ansvar hentet fra Nasjonal strategi for informasjonssikkerhet, side 20–24. Moderniseringsdepartementet har senere overtatt ansvaret for de fleste av tiltakene fra Nærings- og handelsdepartementet.

260) Notat fra Nærings- og handelsdepartementet til Forsvarsdepartementet, Justis- og politidepartementet, Samferdselsdepartementet og Finansdepartementet av 24. september 2004 om permanent organisering av Senter for informasjonssikring

261) Referat fra møte mellom Senter for informasjonssikring og Riksrevisjonen 18. september 2003

262) Se www.norsis.no.

Nærings- og handelsdepartementet i april 2004. Den konkluderer med at SIS oppleves som lite synlig av brukerne: 67 % av brukerne i undersøkelsen benytter seg sjelden eller aldri av tjenester fra SIS. Undersøkelsen viste også at brukerne i liten grad opplever at tjenestene/produktene fra senteret er nyttige.

Abelia mener at dårlig distribusjon kan synes som et hovedproblem for Senter for informasjonssikring. Organisasjonen ser det som et generelt problem at alle myndighetsetater som jobber innen området, ser ut til å mene at det viktigste de kan gjøre, er å lage en nettside/portal med informasjon de mener er relevant. Abelias erfaring er at dette sjelden skjer i samspill med næringslivet selv og sjelden i form av noen avansert strategi for å distribuere relevant informasjon ut til potensielle brukere. Resultatet er dermed hjemmesider/portaler som ingen har hørt om.

Moderniseringsdepartementet er ikke enig i påstanden om at SIS er lite kjent, og henviser til antall treff på senterets nettsider. Departementet mener videre at man har fått gode tilbakemeldinger fra de fokusgruppene som senteret bruker, bl.a. når det gjelder de aktivitetene SIS har generert. (Senterets årsrapport for 2004 viser at nettsidene hadde mellom 600 og 800 besøk per måned fram til og med oktober 2004, og at besøket har steget en del etter dette.[263])

263) Etter presseoppslag i slutten av november var månedstallene noe høyere for november og desember 2004.

6 Fakta: Telesikkerhet og -beredskap

6.1 Bakgrunn

I behandlingen av St. meld. nr. 47 (2000–2001) *Telesikkerhet og -beredskap i et telemarked med fri konkurranse* viser samferdselskomiteen til at telenettets betydning for flere vitale samfunnsfunksjoner er stor, og at det derfor er av overordnet betydning å sikre operativitet i telenettet under alle forhold.[264]

Forsvarets forskningsinstitutt (FFI) peker på at telekommunikasjon, sammen med kraftforsyning og ledelse/informasjon, skiller seg ut som vesentlig for all samfunnsvirksomhet.[265] Svikt i én av disse funksjonene vil kunne medføre svikt i mange andre samfunnsfunksjoner, og de kan således betraktes som bærebjelker som må være intakte for at samfunnet skal kunne fungere. De sterke gjensidige avhengighetene i samfunnet er forhold som bidrar sterkt til det moderne samfunnets sårbarhet. Samtidig med at samfunnet i økende grad er blitt avhengig av telesektoren, har telesektoren i løpet av få år gjennomgått store endringer. Utviklingen har gått fra et statlig televerk med enerett til et konkurransemarked med mange aktører. Dette er en utvikling man også finner i de fleste andre land i den vestlige verden. En rask teknologisk utvikling har gitt sterk vekst i teletjenestenes funksjonalitet og kapasitet, og det har også skjedd en globalisering av eierstrukturene og telenettenes utbredelse. Trusselbildet har også endret seg i retning av mer høyteknologiske trusler. Samlet sett fører denne utviklingen til et mye mer komplekst og uoversiktlig bilde enn tidligere. Myndighetene må derfor ta i bruk andre virkemidler enn tidligere for å oppnå et sikkert samfunn.[266]

Dette er noe av bakgrunnen for at regjeringen gjennom St.meld. nr. 47 (2000–2001) *Telesikkerhet og -beredskap i et telemarked med fri konkurranse* utformet en ny strategi for telesikkerhet og -beredskap, med en rekke tiltak som skulle bidra til å fremme sikkerheten på dette området. I dette kapitlet presenterer vi først kort etableringen av en ansvarlig enhet for området i Post- og teletilsynet, og grunnlaget for tilsynets arbeid. Deretter følger en gjennomgang av status i de tiltakene som ble beskrevet i meldingen. Så langt som mulig blir det presentert forklaringer på hvorfor tiltak eventuelt ikke er gjennomført som planlagt. Til slutt i kapitlet er det en gjennomgang av finansieringsløsninger for tiltakene og av Samferdselsdepartementets styring og oppfølging av området.

6.2 Delegering av oppgaver til Post- og teletilsynet

På bakgrunn av strategien som er omtalt i St.meld. nr. 47 (2000–2001) besluttet Samferdselsdepartementet å delegere et særskilt myndighetsansvar for telesikkerhet og -beredskap til Post- og teletilsynet. Tilsynet skal:

- sette krav til telesikkerhet og teleberedskap og vurdere investeringer i tiltak for å øke robustheten i telenettene
- føre tilsyn med at pålagte tiltak blir iverksatt
- bevisstgjøre, veilede og øke kompetansen til operatører, brukere og andre aktører
- arrangere samøvelser og utvikle samarbeid mellom teleoperatørene[267]

I mai 2001 ble det opprettet en egen enhet i Post- og teletilsynet med ansvar for telesikkerhet og -beredskap: Seksjon for sikkerhet og beredskap i nett.

Grunnlag for Post- og teletilsynets arbeid på området
Lov om elektronisk kommunikasjon (ekomloven) av 4. juli 2003 gir myndighetene hjemmel til å sette krav til sikkerhet og beredskap overfor teleoperatørene. I lovens § 2-10 heter det at tilbyder skal tilby elektronisk kommunikasjonsnett og -tjeneste med nødvendig sikkerhet for brukerne i fred, krise og krig, samt opprettholde nødvendig beredskap. Det er spesifisert at viktige samfunnsaktører skal prioriteres ved behov. Forvaltningen kan fastsette forskrift, treffe enkeltvedtak eller inngå avtale for å nå disse målene.

Lovens krav til sikkerhet er utdypet noe i kapittel 8 i ekomforskriften, som trådte i kraft 1. mars 2004. Forskriften stiller krav om at teletilbydere skal ha oversikt over hvilke brukere som innehar samfunnsviktige funksjoner, at det skal foreligge beredskapsplaner, at tilbyderen skal delta i øvelser arrangert av tilsynet, at brukere med samfunnsviktige funksjoner skal prioriteres i krise- og beredskapssituasjoner, og at Post- og teletilsynet skal varsles om vesentlige driftsmessige og tekniske problemer. Kravet om oversikt over brukere med samfunnsviktige funksjoner er gitt selv om det foreløpig ikke er klarlagt hvilke grupper dette inkluderer. Ifølge departementet skal kravene i forskriften likevel oppfylles overfor samfunnsviktige kunder, og de aktuelle tilbyderne må ta hensyn til dette.[268] Lovens

264) Innst. S. nr. 329 (2000–2001)

265) Hagen, J.M. et al.: Analyse av sårbarhetsreduserende tiltak innen telekommunikasjon, FFI/Rapport-99/00241, Forsvarets forskningsinstitutt, 1999

266) St.meld. nr. 47 (2000–2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse

267) St.meld. nr. 47 (2000–2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse

268) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

krav om nødvendig sikkerhet for brukerne defineres ikke nærmere i forskriften, som ikke setter krav til et helhetlig sikkerhetsstyringssystem. Post- og teletilsynet har ikke gitt nærmere retningslinjer eller anbefalinger overfor teletilbydere om sikkerhet og beredskap.

Før ekomloven ble vedtatt, var det teleloven som ga rettsgrunnlaget for sikring av telenett, jf. spesielt lovens § 7-7, som ga Samferdselsdepartementet mulighet til å gi pålegg om at private aktører skulle utføre særlige oppgaver knyttet til teleberedskap og telesikkerhet.

Post- og teletilsynet skal føre tilsyn med at pålagte sikkerhets- og beredskapstiltak blir iverksatt. Tiltak kan pålegges som generelle krav f.eks. i forskrifter eller som enkeltvedtak, men tilsynet har ennå ikke benyttet muligheten til å fatte enkeltvedtak på dette området. På spørsmål om hvordan det blir ført tilsyn med at pålagte tiltak følges opp av operatørene, svarer Post- og teletilsynet at det f.eks. henter inn rapporter om større hendelser i nettet, har løpende oppfølgings- og orienteringsmøter med operatørene, og deltar i vernekontroll og inspeksjon av fjellanlegg og andre viktige installasjoner. Post- og teletilsynet foretar ikke tradisjonelle tilsyn med at formelle krav følges, og utarbeider ikke tilsynsrapporter på dette området.[269] Samferdselsdepartementet er opptatt av at nødvendig tilsyn tilpasses ressursene til Post- og teletilsynet, og at for eksempel sikkerhetsbrudd indikerer hva tilsynet bør se nærmere på.[270]

6.3 Gjennomføring av tiltak fra St.meld. nr. 47

St.meld. nr. 47 (2000–2001) *Telesikkerhet og -beredskap i et telemarked med fri konkurranse* peker på en rekke tiltak for å bedre telesikkerheten og -beredskapen i Norge. Beskrivelse og tiltak i meldingen baserer seg på utredninger som Forsvarets forskningsinstitutt har gjennomført tidligere (1999), og på en rapport fra det såkalte TIFKOM-prosjektet (2000)[271]. I et brev av 12. desember 2001 fra Samferdselsdeparte-mentet til Post- og teletilsynet om oppfølging av meldingen, peker departementet på hvilke tiltak tilsynet skal prioritere i første omgang.

Nedenfor følger en gjennomgang av de prioriterte tiltakene og status for gjennomføringen av disse per mars 2005 (punkt 6.3.1–6.3.7). I tillegg er status for andre tiltak i meldingen kort omtalt (punkt 6.3.8). Beskrivelsen av bakgrunnen for tiltakene er for en stor del basert på forklaringer gitt i St.meld. nr. 47.

6.3.1 Spesielle samfunnspålagte oppgaver (SSO)

Telenor har i kraft av selskapets ledende posisjon på det norske telemarkedet vært pålagt av Samferdselsdepartementet å levere spesielle samfunnspålagte oppgaver (SSO). Dette omfatter bl.a. beredskapsforberedelser for Totalforsvaret og nød- og sikkerhetstjenester knyttet til kystradioen. Etter at Telenors resterende eneretter ble opphevet i 1998, har selskapets merkostnader i forbindelse med disse oppgavene blitt kompensert ved offentlig kjøp av tjenester gjennom avtaler, først med Justis- og politidepartementet og siden med Samferdselsdepartementet.[272]

Ifølge St.meld. nr. 47 er det ikke lenger tilstrekkelig at bare én operatør er pålagt å levere teleberedskapstjenester, siden andre operatører de senere årene har overtatt stadig større markedsandeler. Meldingen påpeker risikoen som er forbundet med at ikke alle viktige brukere i Totalforsvaret har fasttelefonabonnement hos Telenor med tilhørende beredskapsforpliktelser. Departementet understreker i meldingen at SSO-ordningen ikke sikrer en tilfredsstillende beredskap i telesektoren, og at det må etableres et nytt SSO-konsept som setter krav som omfatter alle samfunnsviktige teleoperatører. Departementet peker videre på at framtidige teleberedskapstiltak også vil innbefatte tiltak rettet mot mobiltelefoni. Mobiltelefoni var ikke dekket av SSO-ordningen på dette tidspunktet.

Det har ifølge departementet tatt noe tid å få på plass et nytt SSO-konsept. En viktig årsak er at staten måtte kjøpe seg ut av tidligere forpliktelser overfor Telenor, og dette måtte finansieres over statsbudsjettet.[273] SSO-avtalen mellom departementet og Telenor ble avviklet i en sluttoverenskomst som skulle dekke beredskapstiltak for 2003 og 2004 samt gi kompensasjon i forhold til statens forpliktelser ved avviklingen. Bevilgninger på henholdsvis 48,1 millioner kroner for 2003 og 55 millioner kroner for 2004 ble benyttet til å avvikle den daværende SSO-ordningen.[274]

Fra og med 2005 overtok Post- og teletilsynet ansvaret for bevilgninger til telesikkerhet og -beredskap og tilhørende avtaler. Da avtalen for 2005 skulle inngås, hadde ikke tilsynet tilstrekkelig grunnlag til å foreta større endringer i innholdet i avtalen. Tilsynet inngikk derfor en avtale med Telenor for 2005 som i hovedsak innebar en videreføring av tiltak i den tidligere SSO-ordningen. Samtidig startet tilsynet opp et internt prosjekt bl.a. for å gi grunnlag for etablering av et nytt konsept som kunne erstatte SSO-ordningen, jf. nærmere omtale nedenfor. For 2006 ønsker Samferdselsdeparte-

269) Post- og teletilsynets svar på spørreliste fra Riksrevisjonen av 23. februar 2005

270) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

271) Prosjekt TIFKOM (Teleberedskap i fritt konkurransemarked) ble etablert av Samferdselsdepartementet etter råd fra Totalforsvarets råd for sikring av tele- og informasjonssystemer. Post- og teletilsynet var prosjektansvarlig.

272) Jf. St.prp. nr. 1, Tillegg nr. 1 (1997–98) for Justis- og politidepartementet, samt bevilgninger på kap. 1360 i St.prp. nr. 1 for Samferdselsdepartementet i senere år

273) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

274) Se St.prp. nr. 1 for Samferdselsdepartementet for periodene 2002–2003 og 2003–2004, kapittel 1360 Samferdselsberedskap.

mentet at det nye konseptet skal ha erstattet SSO-ordningen, og at tilsynet således inngår avtaler med Telenor og eventuelt andre operatører som har kunder som ivaretar samfunnskritiske funksjoner.

Post- og teletilsynet mener det ikke har vært noen svakhet at avtaler om tiltak for telesikkerhet og -beredskap hittil bare har omfattet Telenor, siden avtalen først og fremst dekker kritisk infrastruktur i transportnettet,[275] samt administrative tiltak hos Telenor. Post- og teletilsynet mener at dette også øker sikkerheten og beredskapen hos samtlige av de andre aktørene, siden de i stor grad leier eller er avhengige av infrastruktur fra Telenor. Samtidig vurderer tilsynet mulighetene for å inngå avtaler med flere større operatører i framtiden.[276]

Samferdselsdepartementet mener også at det fram til de senere årene ikke har vært noen svakhet at SSO-overenskomsten ikke har omfattet flere aktører, siden det i realiteten fortsatt er Telenor som har de fleste kundene som ivaretar samfunnskritiske funksjoner. Når det gjelder mobilnettene, mener Samferdselsdepartementet at markedet sørger for tilstrekkelig sikkerhet, bl.a. på grunn av selskapenes egeninteresse i å unngå inntektstap hvis nettene er ute av funksjon.[277]

Samferdselsdepartementet legger til grunn at telesikkerheten i Norge er god. Departementet viste i møte med Riksrevisjonen til et eksempel der strømtilførselen i Nord-Norge hadde falt ut etter en storm, mens telefonsystemet ikke ble direkte påvirket av stormen. Riktig nok falt telefonforbindelsen delvis ut etter hvert pga. manglende strømforsyning og aggregater som gikk tomme. Avtalen om telesikkerhet og -beredskap mellom Post- og teletilsynet og Telenor omfatter ikke krav om strømforsyning.

Post- og teletilsynet startet høsten 2004 et internt prosjekt for å vurdere behovet for sikring av kritisk infrastruktur. Prosjektet vil gjennomgå hva som er kritiske elementer i dagens IKT-infrastruktur, som et grunnlag for å bestemme videre satsing på sårbarhetsreduserende tiltak for offentlig IKT-infrastruktur. Hovedhensikten med prosjektet er å skape et beslutningsgrunnlag for etablering av et nytt konsept som kan erstatte SSO-ordningen. Ifølge Post- og teletilsynet vil prosjektet ha betydning for flere andre tiltak, også flere av tiltakene som er omtalt nedenfor.[278]

6.3.2 Prioritet i fast- og mobilnett

Kapasiteten i telenettene er dimensjonert med mindre sambandsressurser tilgjengelig enn det som må til for at alle skal kunne benytte disse samtidig, noe som heller ikke er nødvendig ut fra et bruksmønster som fordeler seg over hele døgnet. Ved alvorlige hendelser, som større ulykker i et område, er det derimot sannsynlig at mange vil ringe samtidig, og behovet for tjenestenettene vil øke sterkt. Dette kan medføre at ikke alle som ønsker det, får tilgang til å bruke telenettene. Et felles behov for de prioriterte brukerne i Totalforsvaret er å bli sikret framkommelighet i telenettene også i situasjoner der nettene blir overbelastet og ikke kan håndtere trafikkavvikling. For å sikre prioriterte brukere i Totalforsvaret tilgang til nettene også i kritiske situasjoner der mange ønsker å benytte telefon, må det implementeres spesielle prioriteringsmekanismer i telenettene.

Tekstboks 12

To eksempler på at manglende prioritetsordning i telenettene kan skape problemer, er flommen på Østlandet i 1995 og Åsta-ulykken i 2000. Felles for begge disse hendelsene var at behovet for kommunikasjon i og ut fra de berørte stedene ble større enn normalt. Under Åsta-ulykken ble mobilnettet overbelastet av passasjerene på ulykkestoget og av pressefolk som holdt linjene når de kom gjennom til sine redaksjoner. Dette resulterte i at mobilnettene ble overbelastet, og at viktige brukere i forbindelse med redningsaksjonen ikke fikk den nødvendige tilgjengeligheten til kommunikasjonssystemene.

Kilde: Se vedlegg 1.

Ekomforskriften som ble gjort gjeldende i mars 2004, pålegger tilbyder (§ 8-4) å gi prioritet til viktige brukere (bruker med samfunnskritisk funksjon) i krise- og beredskapssituasjoner.

Prioritet i telenettet ble tidligere ivaretatt gjennom en ordning kalt *viktig prioritert telefon* (VPT). Ordningen omfattet kun Telenor, og ble nedlagt med virkning fra årsskiftet 2000/2001. I St.meld. nr. 47 uttaler Samferdselsdepartementet at det raskt må innføres en ny prioritetsordning, både i faste nett og i mobilnettene, til erstatning for VPT-ordningen. En slik ordning trengs for å sikre at forhåndsdefinerte viktige abonnenter får prioritet i situasjoner der nettene eller deler av nettene er overbelastet.

Post- og teletilsynet gjennomførte i 2003 en risiko- og sårbarhetsanalyse av mobilnettene i Norge. Analysen var delt inn i to deler: første del var en simulering av feil i nettet ved normal drift, og andre del var en scenariobeskrivelse for å vise effekten av at GSM-nettet blir utilgjengelig når kapasiteten er for liten. Undersøkelsen viste generelt god tilgjengelighet i det norske mobilnettet. Derimot viste scenarioanalysene at mobilnettene kan være sårbare i krisesituasjoner, på grunn av mangel på kapasitet. På bakgrunn av denne sårbarhetsanalysen vur-

275) Transportnettet er stamnettet som kobler landet som helhet sammen, mens aksessnettet knytter den enkelte brukeren til transportnettet.

276) Post- og teletilsynets svar på spørreliste fra Riksrevisjonen av 23. februar 2005

277) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

278) Internt notat av 3. september 2004, Post- og teletilsynet

derte Post- og teletilsynet det slik at mobilnettene er det området der en ny prioritetsordning vil ha størst effekt.

Post- og teletilsynet startet derfor våren 2004 et prosjekt for å prøve ut en prioritetsordning i mobilnettene. I arbeidet inngår et teknisk delprosjekt med uttesting av en prioritetsordning i nettene til Telenor og NetCom. Arbeidet har ifølge Post- og teletilsynet gått saktere enn planlagt. Én grunn til det er at man har ventet på nye versjoner av software i GSM-sentralene, en annen grunn er en viss uvilje mot å prioritere arbeidet fra Telenors og NetComs side.[279] Prosjektet var opprinnelig planlagt ferdigstilt i 2004. Aktiviteten forventes nå ferdigstilt i løpet av 2005. Ifølge Samferdselsdepartementet har Post- og teletilsynet vært tydelige på at operatørene må følge opp prosjektet bedre, og departementet har derfor ikke involvert seg i dette foreløpig.[280]

Når det gjelder de administrative rutinene for prioritetsordningen, heter det i St.meld. nr. 47 at Direktoratet for samfunnssikkerhet og beredskap (DSB) allerede er bedt om å utarbeide forslag til klare retningslinjer og rutiner for å velge ut personer som bør ha prioritet, og til hvordan ordningen bør administreres. Ifølge meldingen startet DSB dette arbeidet i begynnelsen av 2001.[281] Arbeidet ble tatt opp igjen i mars 2004 da et felles prosjekt mellom Post- og teletilsynet og DSB ble igangsatt. Prosjektet var planlagt avsluttet innen utgangen av oktober 2004. Prosjektet er forsinket i forhold til denne planen. Det forventes at arbeidet vil være klart i løpet av sommeren 2005.[282]

Når det gjelder finansiering av ordningen, opplyser Samferdselsdepartementet at departementene diskuterer om prioritetsordningen bør være kundefinansiert (ved brukerbetaling), men dette er ikke avklart. Samferdselsdepartementet legger til grunn at ordningen må etableres teknisk før finansieringen avklares. Post- og teletilsynet har ansvar for å utvikle ordningen teknisk, men det er Justis- og politidepartementet og DSB som har ansvaret for å administrere den. Ifølge Samferdselsdepartementet forventer Post- og teletilsynet at prioritetsordningen for mobilnettet vil kunne være etablert teknisk i løpet av 2006, forutsatt at Telenor og NetCom er samarbeidsvillige.
Samferdselsdepartementet kan foreløpig ikke angi når spørsmålet om finansiering av ordningen vil være avklart. I møte med Riksrevisjonen 16. mars 2005 presiserer Samferdselsdepartementet at St.meld. nr. 47 hadde et fem-årsperspektiv, og departementet mener det er en akseptabel realisering/framdrift hvis prioritetsordningen blir implementert i 2006.[283]

Det foreligger ingen konkrete planer for analyse eller innføring av prioritert tjenestetilgang i fastnett. Post- og teletilsynet mener at på grunn av stor kapasitet er risikoen liten for at viktige personer eller virksomheter ikke blir tilgjengelige i fastnettet i en krisesituasjon, og hevder det ikke har vært noe problem i nyere tid. Post- og teletilsynet viser også til at dette ikke er en funksjon som uten videre kan innføres på nasjonal basis, og at man i så fall må vente til den internasjonale standardiseringen i Den internasjonale teleunion (ITU), Det europeiske standardiseringsinstitutt for telekommunikasjoner (ETSI) og NATO er klar. Flere konkrete saker har vist at tilgjengelighet kan være et problem i mobilnettene, og tilsynet har derfor valgt å prioritere arbeidet med tiltak i mobilnettene.[284]

6.3.3 Samlokalisering i fjellanlegg

Telenettene inneholder en del vitalt utstyr som er avgjørende for at nettene skal fungere tilfredsstillende. Dette er utstyr av høy verdi som det er vanskelig å gjenanskaffe raskt ved ødeleggelse. Slikt utstyr kan beskyttes mot ytre fysiske og elektromagnetiske påkjenninger ved at utstyret blir plassert i fjellanlegg.

Ifølge St.meld. nr. 47 skal Post- og teletilsynet legge til rette for at det for *framtidige* installasjoner skal finnes en mulighet for samlokalisering i fjellanlegg for de operatørene som leverer tjenester til Totalforsvaret. Man skal videre kartlegge nærmere hvilke fjellanlegg som er mest aktuelle som samlokaliseringssentra, anbefale eierform og undersøke hvilke investeringer som er nødvendige for å klargjøre anlegg for samlokalisering.

Post- og teletilsynet vurderer det slik at samlokalisering i fjellanlegg ikke spiller en like sentral rolle i sikkerhets- og beredskapsarbeidet nå som tidligere, på grunn av den teknologiske utviklingen. Tilsynet mener likevel at det er av betydning å få utnyttet de eksisterende anleggene på best mulig måte.[285] Post- og teletilsynet har vært i dialog med Telenor om forbedring av Telenors system for samlokalisering. I samsvar med kravet om at Telenor skal tilrettelegge for samlokalisering av utstyr fra andre teleoperatører, har Telenor etablert produktet "Telelosji" og utarbeidet en standardavtale som benyttes ved innplassering av utstyr fra andre operatører. Telenor tilbyr samlokalisering i felles teknisk rom eller i eget telelosji-rom. Ifølge Post- og teletilsynet har ikke ordningen resultert i noen større økning i andelen utstyr fra

279) Post- og teletilsynets svar på spørreliste fra Riksrevisjonen av 23. februar 2005

280) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

281) St.meld. nr. 47 (2000–2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse

282) Status i oppfølgingen og koordinering av Nasjonal strategi for informasjonssikkerhet per 4. mai 2005, utarbeidet for møte i Koordineringsutvalget for informasjonssikkerhet i mai 2005

283) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

284) Post- og teletilsynets svar på spørreliste fra Riksrevisjonen av 23. februar 2005

285) Post- og teletilsynets svar på spørreliste fra Riksrevisjonen av 23. februar 2005

Scanpix Creative/Corbis

Tekstboks 13

To graveuhell i 2000 som rammet Telenors telenett, viser betydningen av redundans. I det ene tilfellet ble en kabel utenfor Bergen skadet slik at flyplassen på Flesland mistet teleforbindelsene, med det resultat at flytrafikken ble lammet. Et kabelbrudd i Kristiansand førte til at Telenors teletrafikk i regionen, inkludert nødmeldingstjenesten, ble lammet. Flyplassen på Kjevik mistet teleforbindelsen, og tusener av ferierende fikk opp "Intet nett" på mobilen. Fordi mobiloperatøren NetCom brukte BaneTele, transportnettet til Jernbaneverket, for kommunikasjon mellom mobilsentral og basestasjoner, kunne likevel NetComs kunder bruke mobiltelefon i Kristiansand-området. Telenors kunder kunne ikke ringe, i verken fastnett eller mobilnett.

Kilde: Se vedlegg 1.

andre operatører i fjellanleggene, og tilsynet har ingen konkret plan for å øke graden av samlokalisering i fjellanlegg. Tilsynet viser til at de fleste operatører ikke finner det kostnadseffektivt å benytte tilbudet, og mener at dersom ordningen skal bli mer utbredt, må den stimuleres bl.a. gjennom sterkere økonomiske virkemidler. Tilsynet viser til at dersom prosjekt for vurdering av behovet for sikring av kritisk infrastruktur (jf. punkt 6.3.1) skulle komme fram til at effektiv bruk av fjellanlegg bør prioriteres høyere, vil Post- og teletilsynet se nærmere på om dagens ordning er tilfredsstillende.[286]

Ifølge Samferdselsdepartementet har Post- og teletilsynet ingen plikt til å få tilbyderne inn i fjellanleggene. Operatørene har vist liten interesse for samlokalisering, med unntak av enkelte anlegg. Dette kan ifølge departementet bl.a. ha sammenheng med at kostnadene fra Telenor for lokalisering i anleggene kan være relativt høye, selv om disse er beregnet til selvkost. Departementet mener at tilsynet har lagt til rette for samlokalisering i fjellanlegg.[287]

6.3.4 Redundans i telenettene

Med redundans menes omrutingsalternativer eller reserveløsninger i den enkelte operatørs nett eller mellom ulike operatørers nett. Alternativene skal sikre normal drift dersom deler av nettet er ute av drift eller overbelastes av ulike årsaker.

Ifølge St.meld. nr. 47 har problemet vært at de enkelte operatørene bygger ut nett og sammenkoblingspunkter mellom nettene til de ulike operatørene bare dersom det er kommersielt interessant. Disse nettløsningene anses ikke å være tilstrekkelige i krisesituasjoner, og Samferdselsdepartementet påpeker at det bør iverksettes tiltak som kan øke antallet omrutingsmuligheter i telenettene, dvs. at redundansen i telenettene må økes.[288]

For å sikre tilstrekkelig prioritet til arbeidet med driftssikkerhet og sikring mot skader i normale og unormale situasjoner, påpeker St.meld. nr. 47 at Post- og teletilsynet bør følge opp utviklingen i utbygging av teleinfrastrukturen. Videre viser meldingen til at Post- og teletilsynet gjennom pålegg med hjemmel i regelverket skal bidra til samarbeid om tiltak for å øke redundansen i telenettene. Meldingen understreker at det vil bli spesielt viktig å få til et samarbeid mellom operatører med landsdekkende transportnett, med tanke på å etablere flere sammenkoblingspunkter mellom disse nettene.

Post- og teletilsynet viser til at det har holdt en viss oversikt over utviklingen når det gjelder redundans i telenettet, gjennom dialog med de store netteierne (Telenor og BaneTele). Samøvelsen i 2003 fokuserte ifølge tilsynet bl.a. på redundans og utnyttelse av nettressurser på tvers av operatørene. Tilsynet mener at en rekke tiltak fra operatørenes side de senere årene har ført til bedre redundans i nettet. Eksempelvis har etableringen av MIGTRAN-noder[289] i Telenors nett gjort at man kan håndtere en situasjon med økt trafikk som

286) Oversikt over status for tiltakene i St.meld. nr. 47 (2000–2001) per desember 2004. Fra Post- og teletilsynet til Samferdselsdepartementet januar 2005

287) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

288) St.meld. nr. 47 (2000–2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse

289) MIGTRAN står for migrering av transittnettet og er en pakkebasert teknologi som deler opp og sender telefonsamtalene som pakker. Dermed blir det også mulig å integrere ulike typer tale- og datatrafikk i ett og samme nett. Kilde: Telenors nettsider. Tradisjonell telefoni er linjesvitsjet – man etablerer en forbindelse mellom to samtalepartnere som skal ha en gitt kapasitet.

følge av linjebrudd bedre, fordi nodene kan fungere som back-up for hverandre.[290] Videre viser tilsynet til at de nordligste landsdelene er mindre sårbare gjennom at det er etablert alternative sambandsføringer mellom Sør- og Nord-Norge.

Post- og teletilsynet viser også til at det å vurdere behovet for økt redundans inngår som et viktig område i det pågående analysearbeidet i prosjekt for vurdering av behovet for sikring av kritisk infrastruktur (jf. punkt 6.3.1). Tilsynet har for øvrig ingen konkrete planer om tiltak for å øke redundansen i telenettene.

Samferdselsdepartementet mener også at nettene for elektronisk kommunikasjon har blitt mer robuste siden framleggelsen av St.meld. nr. 47. Operatørene har selv tatt ansvar for dette, jf. den teknologiske utviklingen, samtidig som Post- og teletilsynet har søkt å påvirke operatørene.[291]

6.3.5 Sikkerhetsevaluering av offentlige telenett

Ifølge St.meld. nr. 47 skal Post- og teletilsynet foreta en samlet sikkerhetsevaluering av offentlige telenett i samarbeid med operatørene. Evalueringen skal avdekke hvor det finnes sikkerhetsgradert informasjon og behov for sikkerhetsklarering for de personene som skal ha tilgang til informasjonen. Teleanlegg av særlig vesentlig betydning for landsdekkende og internasjonal telekommunikasjon, som ikke kan erstattes av andre anlegg innenfor samme telenett eller teletjeneste, vil være skjermingsverdige objekter.[292] Det vil de være fordi tilgjengeligheten til telekommunikasjon har betydning for rikets sikkerhet.

Post- og teletilsynet viser i denne forbindelse til prosjekt for vurdering av behovet for sikring av kritisk infrastruktur som er beskrevet i punkt 6.3.1. Prosjektet analyserer hva som er mest kritisk i fysisk og logisk infrastruktur i dag, og analysen skal benyttes som et grunnlag for å definere konkrete sikkerhetskrav til ulike deler av nettet.

6.3.6 Fastsettelse av forskrift om sikring av telekommunikasjonsanlegg mot elektromagnetisk puls (EMP)

Elektromagnetisk stråling er en fysisk trussel mot telenettene. Elektromagnetisk puls (EMP) kan forårsake stor skade i elektronisk utstyr dersom den er kraftig nok. Eksempler på naturlig generert EMP er lynnedslag, radiosendere, termostater og koblinger i det elektriske nettet. Alle disse typene EMP er det mulig å sikre seg mot. Menneskeskapt EMP kan genereres ved bruk av spesielle EMP-våpen og ved detonasjon av kjernevåpen over atmosfæren. Kjernefysisk EMP vil kunne bli så kraftig at elektronisk utstyr vil bli ødelagt i stort omfang, og mot denne typen EMP er det kostnadskrevende å foreta effektive beskyttelsestiltak.

I Norge har det i hovedsak vært Forsvarets mest kritiske systemer som er gitt effektiv EMP-beskyttelse. Også innenfor sivile infrastrukturer med stor viktighet for Totalforsvaret, har det vært foretatt en viss grad av sikring, bl.a. i systemer innenfor kraftforsyningen og i Telenors telenett. Det er utarbeidet retningslinjer for å sikre viktige IT-installasjoner i Totalforsvaret mot EMP.[293]

St.meld. nr. 47 forutsetter at Post- og teletilsynet skal fastsette en forskrift om beskyttelse av telekommunikasjonsanlegg mot elektromagnetisk puls, når tilsynets arbeid med telesikkerhet og -beredskap er kommet i gang. Det framgår av meldingen at et utkast til forskrift allerede var utarbeidet og hadde vært på høring. Det ble imidlertid besluttet at det videre arbeidet med bearbeiding av høringssvarene skulle avvente Forsvarsdepartementets fastsetting av objektsikkerhetsforskriften, jf. omtale av denne under punkt 5.1.1. Post- og teletilsynet opplyser at arbeidet med EMP-forskriften vil bli gjenopptatt når objektsikkerhetsforskriften blir fastsatt. Forskriften er ennå ikke fastsatt per mai 2005.

Ut fra det eksisterende trusselbildet mener Post- og teletilsynet at teleinfrastrukturen i Norge i dag er tilstrekkelig sikret mot elektromagnetisk puls. Tilsynet påpeker imidlertid at det bare er sentrale, viktige punkter i nettet som er sikret mot EMP ved plassering i fjell- og bunkersanlegg. Store deler av infrastrukturen, de fleste telefonsentralene, alle basestasjoner i mobilnettene og lignende er ikke plassert i EMP-beskyttede anlegg.[294]

6.3.7 Sårbarhetsreduserende tiltak i Internett

I løpet av forholdsvis kort tid har Internett blitt en dominerende formidlingskanal for store deler av den digitale informasjonsoverføringen. St.meld. nr. 47 legger til grunn at Internett framover vil tilby stadig flere av de samfunnskritiske tjenestene som de tradisjonelle teletjenestene har utført. Meldingen understreker at det vil være behov for å iverksette særskilte sikringstiltak for Internett tilsvarende det man i dag gjør i telesektoren for øvrig. Departementet påpeker at Post- og teletilsynet må overvåke utviklingen i bruken av Internett, og fortløpende vurdere behovet for å iverksette sikkerhets- og beredskapstiltak.

St.meld. nr. 47 framhever at «Norwegian Internet eXchange» (NIX) hadde vært et sårbart punkt fordi det fram til 2000 var det eneste sammenkoblingspunktet

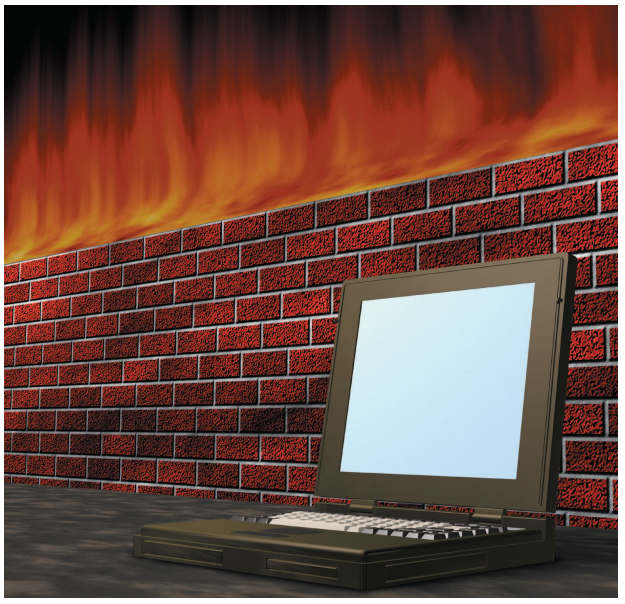
290) Post- og teletilsynets svar på spørreliste fra Riksrevisjonen av 23. februar 2005

291) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

292) Begrepet skjermingsverdige objekter blir nærmere forklart i punkt 5.1.1.

293) Retningslinjer for beskyttelse av elektroniske installasjoner i Totalforsvaret mot elektromagnetisk puls (EMP). Utgitt av Samferdselsdepartementet 24. mars 1998.

294) Post- og teletilsynets svar på spørreliste fra Riksrevisjonen av 23. februar 2005



Scanpix Creative/Masterfile

mellom de ulike Internett-operatørene. NIX ble drevet av Universitetet i Oslos sentrale IT-avdeling. Universitetet etablerte et annet sammenkoblingspunkt i 2000 (NIX2). Ifølge meldingen økte dette tilgjengeligheten og gjorde det totale norske Internett mindre sårbart for kabelbrudd og lignende. De to sammenkoblingspunktene framheves allikevel i St.meld. nr. 47 som svært sårbare punkter, og meldingen legger til grunn at sikring av disse vil være en viktig faktor i en nasjonal sårbarhetsstrategi for Internett.[295]

Ifølge Post- og teletilsynet vil tilsynet definere sikkerhetskrav til NIX1 og NIX2, men dette er ennå ikke gjort. Årsaken er ifølge tilsynet at sammenkoblingspunktene er eid og drevet av Universitetet i Oslo, og således ikke er en del av tilsynets ansvarsområde. Tilsynet har fått utarbeidet en rapport om sammenkoblingspunktene, og det mener at mange av tiltakene som er foreslått i denne, er fulgt opp av universitetet. Tilsynet viser til at det jevnlig er i dialog med dem som er ansvarlige for driften av NIX-ene.

Nasjonal sikkerhetsmyndighets risikovurdering for 2005 understreker betydningen av å sikre sentrale enkeltpunkter i Internett-systemet, som for eksempel NIX. Direktoratet antyder også at andre enkeltpunkter fra kommersielle aktører har fått større betydning enn tidligere, fordi disse aktørene betjener en rekke tjenestetilbydere på Internett som kjøper sine sambandstjenester hos dem. Ifølge Nasjonal sikkerhetsmyndighet blir dermed Internett mer sårbart enn tidligere både overfor logiske angrep i form av for eksempel tjenestenektangrep, og overfor klassiske angrep som sabotasje mot nøkkelpunkter.

295) St.meld. nr. 47 (2000–2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse

Tekstboks 14

Tjenestenektangrep innebærer at angripere sender store mengder forespørsler mot den datamaskinen og de tjenestene de ønsker å angripe, med det formål å hindre denne maskinen i å yte de tjenestene den skal, og eventuelt få den til å bryte sammen.

De siste par årene har det vært flere utpressingstilfeller basert på tjenestenektangrep mot bedrifter som er avhengige av Internett i sin virksomhet. Britiske selskaper som tilbyr veddemål, har bl.a. blitt utsatt for utpressingsforsøk flere ganger ved at kriminelle truer med å starte tjenestenektangrep som vil gjøre det umulig for kunder å nå selskapets nettsted. Russisk politi arresterte i juli 2004 flere personer for angrep på tippeselskapene, og det antas at selskapene har tapt nærmere 500 millioner kroner på denne typen angrep.

Kilde: Se vedlegg 1.

Ifølge Nasjonal strategi for informasjonssikkerhet bør leverandører av Internett-tilgang følge anerkjente sikkerhetsnormer og standarder og synliggjøre hvilken grad av tilgjengelighet, kapasitet og driftsstabilitet som tilbys, samt hvilken brukerhjelp som kan ytes ved feilsituasjoner. Post- og teletilsynet er gitt delansvar for dette, og har tatt initiativ til å etablere et eget internettforum for leverandører av tilgang til Internett (ISP), for å følge utviklingen og ta opp aktuelle problemstillinger.[296]

Tilsynet har dessuten foreslått at det etableres en CERT-funksjon[297] i Post- og teletilsynet (jf. omtale i punkt 5.1.4), men avventer her politisk behandling av hvordan denne funksjonen skal organiseres i Norge. Ifølge tilsynet har det hittil ikke vært iverksatt spesielle tiltak for å redusere sårbarheten i Internett, men tilsynet overvåker situasjonen.[298]

6.3.8 Øvrige tiltak

I utgangspunktet vurderte Samferdselsdepartementet alle tiltakene i St.meld. nr. 47 som viktige for å sikre telesikkerheten og -beredskapen i Norge. Departementet ønsket at Post- og teletilsynet i første omgang skulle prioritere de ovennevnte tiltakene.[299] I det følgende gjør vi rede for de tiltakene i stortingsmeldingen som ikke var av de høyest prioriterte innledningsvis i arbeidet, men som likevel er viktige elementer for å sikre telesikkerheten og -beredskapen i Norge.

296) Post- og teletilsynets oversikt over tiltaksstatus per desember 2004

297) Computer Emergency Response Team

298) Post- og teletilsynets oversikt over tiltaksstatus per desember 2004, og Post- og teletilsynets svar av 23. februar 2005 på spørreliste fra Riksrevisjonen

299) Brev av 12. desember 2001 fra Samferdselsdepartementet til Post- og teletilsynet vedrørende St.meld. nr. 47 (2000–2001) Implementering av strategi for telesikkerhet og -beredskap

Tekstboks 15

Den svenske Post- och telestyrelsen fikk i september 2004 i oppdrag fra regjeringen å utarbeide en strategi for et sikrere Internett. Strategien ble lagt fram i februar 2005. Målet for strategien er å skape et mer robust Internett, noe som innebærer å sikre kritiske funksjoner i Internetts infrastruktur som kan medføre alvorlige forstyrrelser eller avbrudd. Strategien legger vekt på at det må etableres et regelverk som gjør det mulig for staten å sette krav til, få innsyn i og gjennomføre tilsyn med de virksomhetene som ivaretar funksjoner som er sentrale for Internett. Beskyttelse av kritiske logiske funksjoner prioriteres også høyt. Strategien foreslår dessuten tiltak for å bedre kunnskapsnivået blant brukere og peker på viktigheten av internasjonalt samarbeid.

Kilde: Se vedlegg 1.

Beredskapsutstyr

Ifølge St.meld. nr. 47 bør det etableres lagre med transportabelt beredskapsutstyr. Dette utstyret skal kunne settes inn i telenettene ved trafikkbrudd som kan medføre alvorlige konsekvenser for samfunnet. Samferdselsdepartementet mener dette er et tiltak som må videreføres i konseptet som skal erstatte SSO-ordningen. Post- og teletilsynets avtale med Telenor om telesikkerhet og -beredskap inneholder bestemmelser om beredskapsutstyr. Ingen av de andre teleoperatørene er pålagt å ha slikt utstyr, men dette vil ifølge Post- og teletilsynet bli vurdert i tilknytning til utformingen av et nytt avtalekonsept som skal erstatte SSO-ordningen.

Tekstboks 16

Betydningen av telenettenes driftssystemer ble illustrert da NetComs mobilnett var utilgjengelig for selskapets kunder store deler av søndag 12. og mandag 13. juni 2005. I tillegg til selskapets 1,2 millioner egne kunder ble også kunder av andre mobilselskaper som benytter NetComs mobilnett, berørt av problemene. Problemene kom av en feil i en nummerdatabase, der søkeindeksen ikke fungerte tilfredsstillende etter en oppgradering.

Post- og teletilsynet fikk rapport fra NetCom i etterkant av hendelsen. På bakgrunn av dette fant ikke tilsynet noe grunnlag for kritikk mot NetCom for verken forekomsten eller håndteringen av hendelsen. Ifølge tilsynet hadde ingen samfunnskritiske brukere problemer som følge av hendelsen. Tilsynet bemerker i brev til Samferdselsdepartementet om hendelsen at mobiltjenester teknisk sett er mer sårbare enn tradisjonell fasttelefon, og at virksomheter med kritiske funksjoner bør ha reserveløsninger.

Kilde: Se vedlegg 1.

Sikkerhet i telenettenes IKT-baserte produksjonssystemer

Utviklingen har ført til at det er blitt stadig viktigere å beskytte driftssystemene som teleoperatørene benytter, ikke minst i forhold til logiske trusler. En sentralisering i telenettene og økt bruk av kommersielt, lett tilgjengelig IT-utstyr er blant trendene som øker betydningen av disse systemene. Samtidig understreker St.meld. nr. 47 at logiske angrep ved forsøk på inntrenging i telenettenes IT-baserte produksjonssystemer, i dag anses som en større reell trussel enn fysiske angrep, og at konsekvensene av slike angrep kan være alvorlige for større eller mindre deler av samfunnet.

Meldingen påpeker at Post- og teletilsynet bør stille krav til operatørene om at de skal utarbeide en oversikt over hvordan viktige systemer, f.eks. driftssystemer, er koblet mot det øvrige nettverket. Tilsynet bør også sette krav om bedre beskyttelse av viktige delsystemer. Post- og teletilsynet understreker at driftssystemene er blant de viktigste elementene i moderne kommunikasjonssystemer. Tilsynet mener at dette området burde vært mer i fokus, og viser til at tidligere analyser, nye tjenester og bruksmønstre understreker dette.[300] Tilsynet nevner at man i forbindelse med det pågående analysearbeidet i tilsynets prosjekt for økt sikkerhet og beredskap innhenter informasjon om dagens løsninger, og at behovet for videre tiltak blir vurdert.[301] Det er ikke fullført noen evaluering av dagens driftssystemer, og ingen tiltak er så langt iverksatt.

Samferdselsdepartementet mener Post- og teletilsynet jobber med flere tiltak som er knyttet til denne typen risiko. Departementet viser til arbeidet med å utvikle en CERT-funksjon, til case-studien i forskningsprosjektet BAS-5 og til prosjektet for evaluering av teleinfrastruktur, og mener at Post- og teletilsynet har tilstrekkelig søkelys på logiske trusler.[302]

Klassifisering av teleinfrastrukturen

Meldingen legger til grunn at det bør innføres en klasseinndeling av telekommunikasjonsinfrastrukturen etter hvilken betydning infrastrukturen har for telenettenes funksjon. For teleinfrastruktur som vurderes å ha vesentlig betydning for at telekommunikasjonen skal fungere, ble det f.eks. lagt til grunn at det burde stilles en rekke krav knyttet til telesikkerhet og -beredskap, mens teleinfrastruktur som ikke er av avgjørende betydning, burde få færre sikringskrav. Post- og teletilsynet har opplyst at tiltaket inngår i prosjekt for vurdering av behovet for sikring av kritisk infrastruktur som er omtalt i punkt 6.3.1. Tilsynet mener at en klassifisering vil gjøre det mulig på en enklere måte å vurdere om forhold

300) Post- og teletilsynets svar på spørreliste fra Riksrevisjonen av 23. februar 2005

301) Post- og teletilsynets oversikt over tiltaksstatus per desember 2004

302) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

rundt ulike anlegg og nett tilfredsstiller de kravene tilsynsmyndigheten har definert.[303]

Red teams
Ett tiltak for å sikre informasjonen i telenettets IKT-baserte produksjonssystemer kan være å ta i bruk såkalte red teams. Et *red team* er en gruppe mennesker som har fått i oppdrag å trenge inn i datasystemene til en bedrift for å avdekke mulige svakheter i systemenes sikkerhet. Dette har vært gjennomført i Sverige, og Samferdselsdepartementet mener at slike red teams bør tas i bruk også i norske telenett for å avdekke svakheter. Departementet har gitt Post- og teletilsynet i oppgave å utarbeide et opplegg basert på den svenske modellen.

Post- og teletilsynet opplyser at det så langt ikke har gjort noe på dette området, og det foreligger ingen umiddelbare konkrete planer om å starte denne aktiviteten. Tilsynet uttaler at det ikke har etablert den nødvendige kompetansen, og at det i tilknytning til dette også er juridiske fallgruver som må utredes.[304]

Samøvelser
Post- og teletilsynet har fått i oppgave å planlegge og arrangere samøvelser for alle aktørene i telesektoren som anses som viktige i beredskapssammenheng.[305] Post- og teletilsynet har lagt opp til å arrangere samøvelser annethvert år. Første øvelse ble avviklet i 2003, og det er planlagt en ny øvelse i første halvår 2005.

Bevisstgjøring, kompetanseheving og veiledning
Ifølge St.meld. nr. 47 skal Post- og teletilsynet bevisstgjøre brukere når det gjelder robusthet, samt tilrettelegge for enklere gjennomføring av sårbarhetsreduserende tiltak. Ifølge Post- og teletilsynet holder *Seksjon for sikkerhet og beredskap i nett* jevnlig innlegg om sikkerhet og beredskap på seminarer og i andre aktuelle fora. Fram til og med 2004 hadde tilsynet ikke kapasitet til å prioritere andre tiltak for kompetanseheving.[306] I 2005 har tilsynet påpekt de sikkerhetsmessige aspektene knyttet til bruk av bredbåndstelefoni overfor tilbydere og brukere. (Se for øvrig omtale av portalen nettvett.no i punkt 5.2.2.)

Nasjonal autonomi
Nye telenett blir i dag ofte etablert på tvers av landegrensene. Nasjonal autonomi innebærer at det skal være mulig å kommunisere innenfor nasjonens grenser uten å være avhengig av driftsstøtte fra utlandet. St.meld. nr. 47 gir Post- og teletilsynet i oppgave å utrede nærmere forutsetningene for og konsekvensene av å innføre et krav om nasjonal autonomi for alle samfunnsviktige teleoperatører. Post- og teletilsynet opplyser at de med assistanse fra Forsvarets forskningsinstitutt har gjennomført en utredning om nasjonal autonomi. Denne ble ferdigstilt 17. januar 2005.

303) Post- og teletilsynets oversikt over status i tiltakene fra St.meld. nr. 47 (2000–2001), per desember 2004

304) Post- og teletilsynets oversikt over status i tiltakene fra St.meld. nr. 47 (2000–2001), per desember 2004

305) St.meld. nr. 47 (2000–2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse

306) Post- og teletilsynets oversikt over status i tiltakene fra St.meld. nr. 47 (2000–2001), per desember 2004

6.4 Finansiering av tiltakene

St.meld. nr. 47 (2000–2001) omtaler forskjellige modeller for finansiering av tiltakene som skal gjennomføres på området. Ifølge meldingen vil finansiering av telesikkerhets- og beredskapstiltakene avhenge av type tiltak, og avgjøres konkret i forbindelse med at man beslutter å sette i verk de enkelte tiltakene. Meldingen understreker at det er viktig at de finansieringsløsningene som velges, bidrar til klare ansvarsforhold, og at Post- og teletilsynet gis nødvendig handlekraft slik at arbeidet med telesikkerhet og -beredskap ikke blir forsinket eller at målene ikke nås.[307]

Det framgår av policydokumentet som Post- og teletilsynet har utarbeidet, at det å etablere et juridisk og økonomisk hjemmelsgrunnlag for å sette i verk tiltak ble ansett som en hovedutfordring for tilsynet da det fikk ansvar for telesikkerhets- og beredskapsarbeidet.[308] Å utarbeide et forslag til policy for finansiering av tiltakene var et prioritert tiltak for tilsynet i 2003. Det er ikke etablert noen policy for finansiering.

Ekomloven trådte i kraft i juli 2003. I lovens § 2-10 heter det at tilbyder skal tilby elektronisk kommunikasjonsnett og -tjeneste med nødvendig sikkerhet for brukerne i fred, krise og krig, samt opprettholde nødvendig beredskap. Loven slår fast at tilbyder i utgangspunktet skal dekke kostnadene ved sikkerhets- og beredskapstiltak, men at reelle merkostnader forbundet med levering av tiltakene skal kompenseres av staten.

Post- og teletilsynet mener finansiering definitivt har hatt betydning for framdriften i gjennomføringen av tiltakene i St.meld. nr. 47. Tilsynet viser til at ekomloven legger opp til at staten skal betale operatørene for reelle merkostnader for pålagte tiltak, med visse reservasjoner. Dette betyr at tilsynet må ta nødvendig finansiering overfor teleoperatørene i betraktning før det kan sette krav til eller gi pålegg om bedre sikkerhet. Post- og teletilsynet har ikke sett behov for å bruke hjemlene om pålegg eller enkeltvedtak overfor opera-tørene ennå.[309] Ekomforskriften setter noen krav til enkelte tilbydere, men det har hittil ikke vært aktuelt å kompensere tilbyderne for disse kravene. Staten har derfor hittil ikke

307) St.meld. nr. 47 (2000–2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse, kap. 12

308) Post- og teletilsynet, Seksjon for sikkerhet og beredskap i nett: Policydokument, desember 2002

309) Post- og teletilsynets svar på spørreliste fra Riksrevisjonen av 23. februar 2005

kompensert for andre tiltak enn dem som har fulgt av SSO-avtalen. Samferdselsdepartementet er enig i at det hittil ikke har vært behov for å sette konkrete sikkerhetskrav til operatørene.[310]

Ifølge Post- og teletilsynet har finansielle insentiver overfor operatørene for å få gjennomført tiltak ikke vært vurdert hittil i arbeidet med telesikkerhet og -beredskap. Tilsynet har imidlertid inngått avtaler med de største mobiloperatørene om å teste ut tekniske muligheter for å innføre en løsning for prioritering av gitte brukere i mobilnettene. Staten dekker utgiftene i forbindelse med uttestingen.[311]

Samferdselsdepartementet mener at ordinært budsjett gir Post- og teletilsynet et tilstrekkelig finansielt grunnlag til å administrere sikkerhetsarbeidet. I tillegg viser departementet til midler som bevilges over eget kapittel i statsbudsjettet, for å kompensere private aktører for gjennomførte sikkerhetstiltak.[312] Fra 2005 forvalter Post- og teletilsynet disse midlene.[313] Tidligere år har Samferdselsdepartementet forvaltet tilskuddsmidlene til telesikkerhet og -beredskap, og departementet har utbetalt midlene direkte til Telenor i samsvar med SSO-overenskomsten.

6.5 Samferdselsdepartementets styring og oppfølging

Styringsdokumenter og -dialog

Samferdselsdepartementet ga retningslinjer for Post- og teletilsynets planlegging og oppfølging av St.meld. nr. 47 i brev av 20. desember 2001, og trakk der fram de tiltakene som departementet ønsket at tilsynet skulle prioritere. I brevet påpekte departementet at det var avgjørende at Post- og teletilsynet så raskt som mulig kom i gang med å implementere tiltakene i meldingen.

Som grunnlag for oppfølgingen hadde Samferdselsdepartementet utarbeidet en oversikt over tiltakene, med angivelse av om det var departementet eller tilsynet som var ansvarlig for å følge opp de enkelte tiltakene. Departementet la i brevet til grunn at Post- og teletilsynet skulle gi innspill til hvordan oppfølgingen skulle skje, og hva som ville være realistiske tidsfrister for de enkelte tiltakene. Departementet tok sikte på at Post- og teletilsynet i februar/mars 2002 skulle presentere forslag til oppfølging av tiltakene.[314]

Post- og teletilsynet la i 3. kvartal 2002 fram et diagram som viste tilsynets arbeidsplan på området.[315] Diagrammet plasserte de enkelte aktivitetene som fulgte av meldingen til Stortinget, på en tidsakse. Det ble ikke utarbeidet noen beskrivelser av de enkelte tiltakene i diagrammet. Tilsynet har senere gått bort fra å bruke dette plandokumentet.

Mot slutten av 2002 utarbeidet Post- og teletilsynet et policydokument for sikkerhet og beredskap i nett, der det definerer en overordnet policy for sitt ansvar innen telesikkerhet og -beredskap. Tilsynet har i tillegg utarbeidet plandokumenter knyttet til noen enkelttiltak i forbindelse med oppstart av gjennomføring av disse tiltakene. Det foreligger ikke noe samlet plandokument for aktivitetene.

I starten av oppfølgingsarbeidet gjennomførte Samferdselsdepartementet særskilte kvartalsvise møter om telesikkerhet og -beredskap med Post- og teletilsynet. Det var forutsatt at tilsynet i forkant av møtene skulle utarbeide kvartalsrapporter på dette området. Det ble ikke stilt innholdsmessige krav til disse rapportene. Det var også lagt opp til at Samferdselsdepartementet kontinuerlig skulle vurdere egnet oppfølging av Post- og teletilsynets gjennomføring av oppgavene.[316] Fra og med 2004 opphørte den egne kvartalsvise rapporteringen på området, og telesikkerhet og -beredskap gikk inn i den ordinære tertialrapporteringen mellom tilsynet og departementet. Samtidig opphørte de særskilte kvartalsvise møtene.

Samferdselsdepartementet opplyser at det fortsatt styrer med utgangspunkt i St.meld. nr. 47. Departementet ser at meldingen på enkelte punkter begynner å bli utdatert teknologisk, men målene i meldingen er fortsatt styrende. Det foreligger ikke noe annet styringsdokument på området.[317]

Det har ikke blitt formulert mål og resultatkrav for arbeidet med telesikkerhet i de årlige tildelingsbrevene til Post- og teletilsynet. Samferdselsdepartementet mener at målsettingene formulert i St.meld. nr. 47 er

310) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

311) Post- og teletilsynets svar på spørreliste fra Riksrevisjonen av 23. februar 2005

312) Bevilget over kap. 1360 Samferdselsberedskap, post 71 Tilskudd til samfunnspålagte oppgaver vedr. Totalforsvaret

313) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

314) Brev av 12. desember 2001 fra Samferdselsdepartementet til Post- og teletilsynet om St.meld. nr. 47 (2000–2001) Implementering av strategi for telesikkerhet og -beredskap

315) Post- og teletilsynets kvartalsrapport nr. 3/2002 om telesikkerhet og -beredskap

316) Referat fra møte 20. mars 2003 mellom Samferdselsdepartementet og Riksrevisjonen

317) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

klare, og at tiltakene i meldingen gir klare føringer for hva Post- og teletilsynet skal arbeide med. Departementet mener at det derfor ikke har vært behov for å sette spesifikke resultatkrav for telesikkerhetsarbeidet hvert år. Det foreligger ingen spesifikke skriftlige rapporter om resultater av arbeidet hittil.[318]

Post- og teletilsynet mener departementets prioriteringer i innledningsfasen var klare nok, men påpeker at det på bakgrunn av tilgjengelige ressurser har vært nødvendig med ytterligere strenge prioriteringer fra tilsynets side. Det har vært dialog på de kvartalsvise møtene rundt endringer i prioriteringer, og Post- og teletilsynet viser til at det har vært enighet om de prioriteringene som har vært gjort.[319]

Bemanningssituasjonen
Ifølge St.meld. nr. 47 bør Post- og teletilsynet ha en bemanning på minimum 4–7 personer i en enhet som skal arbeide for telesikkerhet og -beredskap, for å få et kompetent sikkerhets- og beredskapsmiljø. På det meste har tilsynet hatt tre stillinger på fulltid på området. Post- og teletilsynet mener at utviklingen i ressurser og antall ansatte ikke har stått i forhold til ambisjonsnivået i St.meld. nr. 47 og oppgavene departementet har bedt tilsynet om å prioritere. Tilsynet peker også på at det har vært nødvendig med en oppbemanning i perioden, noe som er ressurskrevende i seg selv. Vedtaket om å flytte tilsynet til Lillesand har ifølge tilsynet forsterket bemanningsproblemet i og med at flere folk slutter og må erstattes. Prosjektledere har også vært skiftet ut, slik at tilsynet i lengre perioder har vært uten prosjektleder. Dette har ifølge tilsynet hatt innvirkning på framdriften av tiltakene.[320]

Samferdselsdepartementet er klar over at flyttevedtaket har ført til at enkelte har sluttet i tilsynet, og viser også til at Post- og teletilsynet har tatt opp med departementet problemet med bemanning og det at prosjektledere har sluttet. Departementet peker likevel på at Post- og teletilsynet har stor frihet til å prioritere ressursfordelingen internt, og at tilsynet har mulighet til å prioritere ressurser mellom ulike områder. Dimensjoneringen av telesikkerhetsarbeidet (antall ansatte o.a.) er ifølge departementet også avhengig av den interne prioriteringen i Post- og teletilsynet.[321]

Framdrift
Når det gjelder framdriften for tiltakene fra St.meld. nr. 47, opplyser Post- og teletilsynet at Samferdselsdepartementet bare har etterspurt begrunnelse i de tilfellene der prosjektene har tatt mer tid enn planlagt.

På spørsmål om departementet er fornøyd med framdriften i tiltakene, uttaler departementet at det var behov for å konkretisere og utrede tiltakene i stortingsmeldingen ytterligere. Departementet viser til at enkelte av tiltakene i meldingen var formulert slik: ”Post- og teletilsynet skal vurdere […]” Utredningene fra Post- og teletilsynet har vært på snevrere områder enn de utredningene som lå til grunn for meldingen. Behovet for å utrede flere forhold nærmere har ført til at implementeringen av tiltakene har tatt tid. Samtidig har fokus blitt flyttet over tid: Både brukerne og teknologien har endret seg, og det har ført til et behov for å revurdere innrettingen på tiltakene. Samferdselsdepartementet viser til at det for eksempel i forbindelse med innføringen av en prioritetsordning er brukt noe tid på å vurdere utviklingen i internasjonale standarder på området. Departementet viser i tillegg til at Post- og teletilsynet har fått arbeidsoppgaver som ikke var omtalt i meldingen, bl.a. bredbåndsområdet som tilsynet må jobbe med framover.[322]

318) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

319) Post- og teletilsynets svar på Riksrevisjonens spørreliste av 23. februar 2005

320) Post- og teletilsynets svar på Riksrevisjonens spørreliste av 23. februar 2005

321) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

322) Referat fra møte mellom Samferdselsdepartementet og Riksrevisjonen 16. mars 2005

7 Vurderinger

7.1 Organisering av arbeidet med IT-sikkerhet[323]

I St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* er det forutsatt at ansvaret for IT-sikkerhet skal være et virksomhetsansvar. Dette er fulgt opp gjennom organiseringen av arbeidet i staten. I tillegg påpeker St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* og Innst. S. nr. 9 (2002–2003) betydningen av koordinering og ansvarsklargjøring på området. Undersøkelsen viser at de fleste fagorganene og bransjeorganisasjonene mener at ansvaret for informasjonssikkerhet i forvaltningen er spredt på en rekke forskjellige aktører, hvorav flere har relativt begrensede ressurser på området. Flere har påpekt manglende avklaringer, fragmentering og at begrensede ressurser brukes til overlappende oppgaver. Bransjeorganisasjonene mener det er vanskelig å finne ut hvilken etat som har ansvar for de enkelte problemstillingene.

Undersøkelsen viser at det fortsatt mangler avklaringer på viktige områder på departementsnivå:

- *Ansvaret for kritisk infrastruktur*: Undersøkelsen viser at det er uklart hva Justis- og politidepartementets ansvar for kritisk infrastruktur innebærer, hva ansvaret for IT-sikkerheten i denne strukturen omfatter, og hvilket overordnet ansvar Justis- og politidepartementet har for IT-sikkerheten i en krisesituasjon.
- *Ansvaret for Internett*: Samferdselsdepartementet har ansvar for forhold underlagt ekomloven, herunder Internett. Det synes imidlertid å være ulike oppfatninger mellom departementene når det gjelder Samferdselsdepartements ansvar for sikkerhet for Internett-relaterte tjenester sett i forhold til Moderniseringsdepartementets ansvar for helheten i IT-sikkerhetsarbeidet.
- *Kontakten med næringslivet*: Undersøkelsen viser at det har tatt tid å få avklart hvilket departement som skal følge opp bruken av IT i næringslivet etter omorganiseringen på departementsnivå i 2004. Nærings- og handelsdepartementet har nå opprettet en seksjon som bl.a. har ansvar for å følge opp bruken av IT i næringslivet. Samtidig skal Moderniseringsdepartementet ha pådriveransvar for alle tiltak i Nasjonal strategi for informasjonssikkerhet som retter seg mot eller inkluderer næringslivet.

For å sikre koordinering av arbeidet ble Koordineringsutvalget for informasjonssikkerhet etablert i 2004. Det er for tidlig å vurdere om utvalget har bidratt til økt koordinering på departementsnivå.

323) Jf. problemstilling A

I St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet,* Innst. S. nr. 9 (2002–2003) og St.prp. nr. 1 (2002–2003) for Justis- og politidepartementet og Nærings- og handelsdepartementet er det lagt opp til at ansvarsforholdet skal klargjøres også mellom ulike fagorganer. Gjennomgangen viser at det er etablert skriftlige samarbeidsavtaler mellom de fleste organene, i tillegg til at det gjennomføres jevnlige kontaktmøter. Det er imidlertid liten grad av formalisert samarbeid mellom Post- og teletilsynet og henholdsvis Nasjonal sikkerhetsmyndighet og Senter for informasjonssikring. Alle disse tre organene arbeider med å framskaffe oversikt over trusler mot IT-systemer og sårbarhet i systemene. En avgjørelse rundt organisasjonsmessig plassering av en nasjonal CERT vil kunne påvirke forholdet mellom de tre virksomhetene og kreve nye avklaringer av det enkelte organs ansvar.[324]

I behandlingen av St.meld. nr. 39 (2003–2004) *Samfunnssikkerhet og sivilt-militært samarbeid* uttaler forsvarskomiteens flertall at meldingen "ikke på en tilstrekkelig måte tar inn over seg at det offentlige Norges vern mot IT-angrep synes for lite koordinert. Flertallet mener at ansvaret for det offentliges IT-sikkerhet synes for dårlig, og at dette sakskomplekset lider under det faktum at for mange aktører er tildelt ansvar. Dette gjelder ikke bare på underordnet nivå, men det kan også synes som om det på departementalt nivå er for mange som har en rolle i utformingen av den statlige IT-sikkerheten."[325]

Ut fra disse påpekningene og de faktaene som er presentert i denne undersøkelsen, kan det stilles spørsmål ved om sentrale departementer[326] har gjort tilstrekkelig for å avklare ansvarsforholdene, særlig på departementsnivå. Det kan også stilles spørsmål om hvilke konsekvenser manglende avklaringer kan få i en eventuell krisesituasjon, særlig for samfunnskritisk IT-infrastruktur.

7.2 Samfunnskritisk IT-infrastruktur

7.2.1 Manglende avgrensning[327]

Stortinget mener i Innst. S. nr. 9 (2002–2003) at det er avgjørende at det utvikles robust infrastruktur i alle samfunnsviktige institusjoner. Dette følges opp i

324) CERT står for Computer Emergency Response Team: et ekspertteam som håndterer IT-sikkerhetshendelser.

325) Innst. S. nr. 49 (2004–2005)

326) Moderniseringsdepartementet, Justis- og politidepartementet og Samferdselsdepartementet

327) Jf. problemstilling C.1

Nasjonal strategi for informasjonssikkerhet, der beskyttelse av kritisk infrastruktur er ett av fire hovedmål. Ifølge strategien er en identifisering av kritisk IT-infrastruktur en forutsetning for å gjennomføre risikovurderinger og implementere nødvendige tiltak. Undersøkelsen viser at det er satt i gang en del arbeid med å definere hva som er samfunnskritisk infrastruktur, men at myndighetene per i dag ikke har en klar oversikt over hva som er kritisk IT-infrastruktur, og hvilke systemer denne består av. Gjennomgangen viser også at det fortsatt ikke er klart hva som skal defineres som skjermingsverdige objekter i henhold til sikkerhetsloven, og hva som skal gjøres for å beskytte disse. Man kan derfor spørre om denne mangelen på avgrensning og definering innebærer en risiko for at kritiske systemer ikke er godt nok beskyttet, og at det settes inn kostbare tiltak der dette ikke er nødvendig.

7.2.2 Tiltak for å redusere sårbarhet[328]

I Innst. S. nr. 9 (2002–2003) presiserer forsvarskomiteen og justiskomiteen at den grunnleggende kunnskapen om hva som skaper sårbarhet, bør prioriteres i sikkerhetsarbeidet. Det pågående forskningsprosjektet BAS-5 er et av de viktigste tiltakene for å framskaffe mer kunnskap om sårbarhet i nasjonalt viktige IT-systemer. Undersøkelsen viser imidlertid at det har tatt tid å etablere og finansiere prosjektet, som omtales som viktig av både departementene og fagetatene.

Ifølge Nasjonal strategi for informasjonssikkerhet skal det utarbeides sektorvise normer for å beskytte kritisk IT-infrastruktur. Gjennomgangen viser at det ikke er planlagt eller gjennomført aktiviteter på området.

Undersøkelsen viser at de fleste offentlige organer som arbeider med IT-sikkerhet, har utarbeidet veiledninger for risiko- og sårbarhetsanalyser, og det pågår mange aktiviteter for å videreutvikle metoder og verktøy. Det synes som om myndighetene i mindre grad har lagt vekt på å legge til rette for at metodene faktisk blir brukt. Det er heller ikke lagt opp til at kunnskap fra analysene skal kunne benyttes i prioriteringen av sikkerhetstiltak uavhengig av sektor.

7.2.3 Systemer for å fange opp trusler[329]

Informasjon om sikkerhetshendelser er nødvendig for å få et bilde av foreliggende trusler og sårbarhet i IT-infrastrukturen, og for å kunne gi råd om konkrete trusler eller assistanse ved gjenoppretting av tjenester. Varslingssystem for digital infrastruktur (VDI) er etablert for å styrke informasjonen om sikkerhetshendelser. VDI har lyktes med å få tilgang til informasjon om logiske trusler via Internett og har således oppnådd en av hensiktene med systemet. St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* peker på at VDI skal være mest mulig åpent, både når det gjelder hvem som skal kunne være deltakere og brukere, og når det gjelder det at informasjonen skal være mest mulig tilgjengelig. Undersøkelsen viser at antallet deltakere i varslingssystemet fortsatt er relativt begrenset, og at systemet gir lite informasjon til allmennheten.

Ifølge St.prp. nr. 1 (2001–2002) for Nærings- og handelsdepartementet skal Senter for informasjonssikkerhet bidra til en mer robust IT-infrastruktur ved bl.a. å framskaffe et helhetlig bilde av truslene mot norske IT-systemer. Som et grunnlag for dette er det forutsatt at offentlige og private virksomheter raskt skal melde inn sikkerhetsbrudd og hendelser til senteret. Gjennomgangen viser at få sikkerhetshendelser faktisk innrapporteres til senteret. I løpet av 2004 mottok senteret mindre enn fem rapporter om sikkerhetshendelser.

Undersøkelsen viser at myndighetene gjennom etableringen av Varslingssystem for digital infrastruktur og Senter for informasjonssikkerhet har etablert organer som kan fange opp trusler mot IT-systemer, men at disse organene foreløpig ikke har nådd vesentlige mål for sin virksomhet. Det kan derfor stilles spørsmål ved om departementene har iverksatt tilstrekkelige tiltak for å sikre måloppnåelse på dette området.

7.2.4 Evne til å håndtere sikkerhetshendelser[330]

Ved behandlingen av St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet* uttaler forsvarskomiteen og justiskomiteen at klargjøring av beredskapsplaner og krisehåndteringsplaner for bl.a. IT-sikkerhet er viktig. I meldingen heter det at Justisdepartementet vil ta initiativ for å sikre at tiltak ved bortfall av IKT, herunder tiltak i forhold til situasjoner der det pågår eller er mistanke om angrep via informasjonssystemer, blir reflektert i kriseplaner. På nasjonalt plan arbeider Justis- og politidepartementet og Direktoratet for samfunnssikkerhet og beredskap (DSB) med å utvikle et nytt nasjonalt beredskapssystem. Gjennomgangen viser at det ennå ikke er klart i hvilken grad risiko for alvorlig svikt i IT-systemer vil bli reflektert i det nye beredskapssystemet.

På virksomhetsnivå viser statistikk fra Statistisk sentralbyrå at oppdaterte beredskapsplaner bare foreligger i et mindretall av virksomhetene i statlig, kommunal og privat sektor. Nasjonal strategi for informasjonssikkerhet inneholder ikke tiltak direkte rettet mot å fremme utviklingen av gode beredskaps- og krisehåndteringsplaner i virksomhetene.

Når det gjelder betydningen av øvelser, påpeker Innst. S. nr. 9 (2002–2003) viktigheten av å ha et ledelsesapparat som kan håndtere kriser. Komiteen uttaler videre at saksbehandlere innen sikkerhet, beredskap og krisehåndtering bør være sidestilt med ledelsesnivået som målgruppe for øvelser. Ett av formålene med øvelser er å identifisere konkrete forebyggende tiltak. Undersøkelsen viser at øvelser initiert av DSB i stor grad har vært konsentrert om ledelsesapparatet, mens saksbehandlernivået

328) Jf. problemstilling C.2

329) Jf. problemstilling C.3

330) Jf. problemstilling C.4

synes å ha vært lavere prioritert. Videre ser det ut til at øvelser gjennomført på initiativ fra DSB ikke har vært tilstrekkelig til å identifisere forebyggende tiltak.

OECDs retningslinjer for sikkerhet i informasjonssystemer og nettverk vektlegger betydningen av å ha systemer som kan forebygge, oppdage og reagere på sikkerhetshendelser, og mange land har etablert en statsfinansiert CERT (*Computer Emergency Response Team*). St.meld. nr. 39 (2003–2004) *Samfunnssikkerhet og sivilt-militært samarbeid* viser til at flere instanser har påpekt behovet for en slik enhet (CERT) for å sikre effektiv håndtering av en krise der flere samfunnskritiske funksjoner blir angrepet samtidig. Ifølge meldingen vil en slik enhet kunne styrke den nasjonale beredskapen mot IT-angrep gjennom å utvikle et system for koordinert respons og gjenoppretting, først og fremst innenfor virksomheter med samfunnskritiske funksjoner. Undersøkelsen tyder på at det er enighet om at en CERT bør etableres, men at det er uenighet om hvilket fagmiljø som skal ha oppgaven. Det er fortsatt ikke etablert et system som effektivt kan håndtere IT-sikkerhetshendelser.

Gjennomgangen gir grunn til å stille spørsmål ved om:
- dagens nasjonale beredskapssystem i tilstrekkelig grad håndterer alvorlig svikt i IT-systemer, og om øvelsesvirksomheten har vært i samsvar med Stortingets forutsetninger
- manglende beredskapsplaner i virksomheter er en samfunnsmessig risikofaktor
- manglende systemer for koordinert respons og gjenoppretting kan få alvorlige samfunnsmessige konsekvenser ved et eventuelt angrep på kritisk infrastruktur

7.3 Tilrettelegging for utvikling av god sikkerhetskultur[331]

Ett av de overordnede målene for IT-sikkerhet er ifølge St.prp. nr. 1 (2003–2004) for Justis- og politidepartementet og Nærings- og handelsdepartementet å bygge opp en sikkerhetskultur. Nasjonal strategi for informasjonssikkerhet inneholder en rekke tiltak som skal bidra til en bedre sikkerhetskultur. Dette er i samsvar med OECDs anbefalinger på området. Undersøkelsen viser imidlertid at svært få tiltak for utvikling av en sikkerhetskultur er igangsatt eller gjennomført:

- Ifølge OECDs anbefalinger bør offentlig sektor søke å være en drivkraft i utviklingen av en sikkerhetskultur ved bl.a. å framstå som et godt eksempel og ved å anvende sin betydelige innkjøpsmakt. Undersøkelsen viser at tiltakene i strategien som følger av dette målet, ikke er gjennomført. Videre viser den at næringslivet ikke vurderer offentlig sektor som en drivkraft og som et godt eksempel for privates arbeid med IT-sikkerhet.
- Strategien inneholder en del tiltak for å bevisstgjøre allmennheten om IT-sikkerhet. Internettportalen nettvett.no er etablert, men øvrige tiltak på dette området er ikke igangsatt, og det foreligger ikke konkrete planer for gjennomføring.
- Enkelte tiltak for å bedre kompetansen i IT-sikkerhet ble gjennomført kort tid etter at Sårbarhetsutvalget la fram sin utredning, bl.a. ble det etablert et femårig forskningsprogram i regi av Norges forskningsråd. Nasjonal strategi for informasjonssikkerhet inneholder enkelte nye kompetansetiltak, men det foreligger ikke konkrete planer for å gjennomføre disse.
- Stortinget ba allerede i B.innst. S. nr. 1 (1996–1997) regjeringen om å legge fram forslag om etablering av en sertifiseringsordning for IT-sikkerhet. Regjeringen kom i 1998 tilbake med forslag om å etablere to ordninger for sertifisering av henholdsvis produkter og organisasjoner, begge basert på internasjonale standarder. Nasjonal strategi for informasjonssikkerhet inneholder tiltak for å fremme bruken av de nevnte standardene og sertifiseringsordningene. Det er imidlertid ikke gjennomført signifikante tiltak mot dette målet, og planlagte tiltak på området er uklare. Undersøkelsen viser at standardene er lite kjent i næringsliv og forvaltning, og at svært få virksomheter/produkter er sertifisert. For eksempel skjedde den første sertifiseringen av et produkt med basis i den ene ordningen først i 2004.
- En av oppgavene til Senter for informasjonssikring er å veilede virksomheter i arbeidet med IT-sikkerhet. Undersøkelsen tyder imidlertid på at senteret er lite kjent utover et begrenset, profesjonelt sikkerhetsmiljø, og at det for eksempel har problemer med å nå små og mellomstore bedrifter.
- Andre veiledningstiltak som er planlagt gjennomført i samarbeid med næringslivet, er i hovedsak ikke igangsatt.

Undersøkelsen viser også at planene for hvordan og når tiltak skal gjennomføres, i mange tilfeller er uklare. Tilbakemeldinger fra bransjeorganisasjoner tyder videre på at myndighetenes arbeid med å utvikle en sikkerhetskultur i liten grad er gjennomført i privat sektor. Mangelfull sikkerhetskultur kan få alvorlige samfunnsmessige og økonomiske konsekvenser. På denne bakgrunn kan det stilles spørsmål ved om myndighetenes oppfølging har vært tilstrekkelig.

7.4 Mulige årsaker til manglende framdrift i arbeidet

Manglende avklaringer av ansvarsforhold som nevnt innledningsvis, kan være en av årsakene til lav framdrift i arbeidet og til andre problemer omtalt over. I tillegg kan forhold ved plan- og gjennomføringsprosessen, finansieringen og manglende samordning av regelverk være mulige årsaker til de omtalte problemene.

7.4.1 Begrenset deltakelse i gjennomføringsfasen[332]

I samsvar med anbefalingene fra OECD er det utviklet

331) Jf. problemstilling D

332) Jf. problemstilling B

en Nasjonal strategi for informasjonssikkerhet. OECD anbefaler også at det legges opp til systematisk samarbeid med privat sektor for å utvikle en sikkerhetskultur. Gjennomgangen viser at departementene la opp til en relativt bred deltakelse i utviklingen av strategien, men at det har vært mindre deltakelse i gjennomføringsfasen.

Det har ikke har vært kontakt mellom Nærings- og handelsdepartementet/Moderniserings-departementet og aktuelle bransjeorganisasjoner om oppfølging av strategien. Etter omorganiseringen av departementene sommeren 2004 har det tatt tid å avklare hvilket departement som skal ha ansvaret for kontakten med næringslivet. Manglende kontakt med næringslivet kan redusere mulighetene for å utvikle en god sikkerhetskultur i samfunnet. Også tiltakene i skole- og universitetssektoren er forsinket, noe som kan skyldes at det ikke er etablert et tilstrekkelig samarbeid mellom Moderniseringsdepartementet og Utdannings- og forskningsdepartementet.

7.4.2. Utilstrekkelige plandokumenter[333]

Undersøkelsen viser at de mest berørte departementene har utarbeidet handlingsplaner for oppfølging av Nasjonal strategi for informasjonssikkerhet. Handlingsplanene er imidlertid i stor grad oppsummeringer av hva som gjøres innenfor hvert departementsområde, og er på mange måter ikke mer detaljerte enn Nasjonal strategi for informasjonssikkerhet. Handlingsplanene inneholder i liten grad prioritering av tiltak eller informasjon om hvordan tiltakene skal realiseres, dvs. kobling til ressursanslag og budsjetter. Gjennomgangen viser videre at handlingsplanene i noen grad gir informasjon om når tiltak forventes ferdigstilt, men en god del tiltak er fortsatt ikke igangsatt eller vurderes som "løpende" tiltak. Undersøkelsen viser at det ikke foreligger godt planlagte, samordnede og effektive handlingsprogrammer etter OECDs anbefalinger.

Verken i strategien eller i handlingsplanene er det satt opp resultatkriterier som gjør det mulig å måle effekten av de enkelte tiltakene eller av flere tiltak samlet, jf. krav i økonomireglementet. Dette tilsier økt vekt på å gjennomføre evalueringer for å få informasjon om resultater og måloppnåelse. Det er ikke dokumentert at det skal gjennomføres slike evalueringer som et hjelpemiddel i styringen av den videre aktiviteten på området.

7.4.3 Krevende samordningsoppgaver[334]

Moderniseringsdepartementet skal stå for koordineringen av arbeidet med oppfølging av strategien. I dette arbeidet benytter departementet Koordineringsutvalget for informasjonssikkerhet, som skal holde oversikt over status i arbeidet. Organiseringen av det offentlige IT-sikkerhetsarbeidet og utformingen av den nasjonale strategien innebærer ingen plikt for den enkelte virksomhet til å gjennomføre tiltak i strategien. Med dette utgangspunktet og med så mange virksomheter involvert i gjennomføringen av strategiens tiltak er det en vanskelig oppgave å følge opp at strategien blir realisert på en effektiv måte. Undersøkelsen viser at Moderniseringsdepartementet har få virkemidler knyttet til IT-sikkerhet, og at det har avsatt relativt begrenset med ressurser til denne aktiviteten.

7.4.4 Problemer med å finansiere tverrsektorielle tiltak[335]

Innenfor IT-sikkerhetsarbeidet er det en rekke tiltak som krever samarbeid og finansiering på tvers av etatsgrenser. Flere etater har påpekt problemer med å få finansiert tverrsektorielle IT-tiltak som mange departementer og etater ser nytten av. Det kan derfor stilles spørsmål ved om de koordinerende departementene har lagt tilstrekkelig vekt på det økonomiske aspektet ved planlegging av tiltak på området.

7.4.5 Manglende samordning av regelverk[336]

Nasjonal strategi for informasjonssikkerhet legger vekt på at regelverket for IT-sikkerhet skal samordnes bedre. I undersøkelsen peker flere etater og bransjeorganisasjonene på forhold ved regelverket som kan gjøre samordning av sikkerhetsarbeidet vanskelig, og på at mange av de administrative problemene rundt ansvarsforhold bunner i et til dels sprikende regelverk. Kompleksitet og fragmentering av regelverket blir trukket fram som et problem for næringslivet/brukerne. Undersøkelsen viser at det har tatt tid å få nedsatt en arbeidsgruppe for regelverksgjennomgang. Arbeidet er fortsatt i en innledende fase. Det er tidligere gjort flere forsøk på slik samordning uten at det har hatt ønsket effekt.

7.5 Særskilt om telesikkerhet og -beredskap[337]

I samsvar med St.meld. nr. 47 (2000–2001) *Om telesikkerhet og -beredskap i et telemarked med fri konkurranse* ble det i 2001 opprettet en enhet i Post- og teletilsynet som har ansvar for telesikkerhet og -beredskap. Post- og teletilsynet fikk ansvaret for å gjennomføre eller utrede en rekke av tiltakene i meldingen. Undersøkelsen viser at hoveddelen av de prioriterte tiltakene fire år senere fremdeles er under utredning, og at få tiltak er gjennomført:

- Meldingen peker på at det ikke lenger er tilstrekkelig at bare én operatør (Telenor) er pålagt å levere teleberedskapstjenester, og at det må etableres et nytt konsept med krav til alle teleoperatører med samfunnsviktige kunder. Undersøkelsen viser at det fortsatt er bare én operatør som leverer teleberedskapstjenester.
- Ifølge meldingen må det raskt innføres en ny ordning som sikrer prioriterte brukere telefonforbindelse i kritiske situasjoner der telenettene overbelastes.

333) Jf. problemstilling B

334) Jf. problemstilling B

335) Jf. problemstilling B

336) Jf. problemstilling A

337) Jf. problemstilling E

Undersøkelsen viser at det ikke foreligger noen ny prioritetsordning, verken i mobilnettene eller i fastnettet. Innføring av en prioritetsordning i mobilnettene har blitt prioritert og er teknisk sett under utprøving, men finansieringen av ordningen er ikke avklart.

- Post- og teletilsynet skal arbeide for økt redundans[338] i telenettene gjennom pålegg og ulike samarbeidstiltak. Det er ikke gjennomført noen samlet vurdering av redundans i telenettene, og det er heller ikke planlagt eller gjennomført tiltak for økt redundans.
- Post- og teletilsynet skal videre legge til rette for at det for framtidige installasjoner finnes en mulighet for samlokalisering i fjellanlegg for de operatørene som leverer tjenester til Totalforsvaret. Tilsynet har lagt vekt på at et tilbud om samlokalisering skal foreligge, men har ikke prioritert tiltak som kan bidra til en faktisk høyere grad av samlokalisering i fjellanleggene.
- Post- og teletilsynet skal stille krav til operatørene om at det utarbeides en oversikt over hvordan viktige produksjons- og driftssystemer er koblet mot det øvrige nettverket. Tilsynet har ikke stilt slike krav, og har heller ikke satt krav til beskyttelse av disse systemene.
- Post- og teletilsynet skal også utvikle en klassifiseringsordning for teleinfrastrukturen. Det er ikke foretatt en klassifisering av teleinfrastrukturen i sikringsklasser, og heller ikke definert konkrete sikkerhetskrav til de enkelte klassene.
- Post- og teletilsynet skal i samarbeid med teleoperatørene gjennomføre en sikkerhetsevaluering av teleinfrastrukturen. Det er ikke gjennomført en sikkerhetsevaluering av telenettene ut fra sikkerhetslovens krav og sett i sammenheng med klassifiseringen som er nevnt i forrige punkt.
- Post- og teletilsynet skal videre fastsette forskrift om beskyttelse av telekommunikasjonsanlegg mot elektromagnetisk puls (EMP). En slik forskrift er fortsatt ikke fastsatt, og det foreligger ingen konkrete planer for å vurdere EMP-sikring av telekommunikasjonsanlegg.
- Post- og teletilsynet skal endelig overvåke utviklingen i bruken av Internett og fortløpende vurdere behovet for å implementere sikkerhets- og beredskapstiltak. Tilsynet har hittil ikke iverksatt spesielle tiltak for å redusere sårbarheten i Internett.

Samferdselsdepartementet mener det var behov for ytterligere konkretisering og utredning av tiltakene i stortingsmeldingen, og at dette har ført til at iverksettingen har tatt tid. Departementet peker også på at både brukerne og teknologien har endret seg, noe som har medført behov for å revurdere innrettingen på tiltakene.

Undersøkelsen viser at det finnes få plan- og styringsdokumenter for arbeidet med tiltakene i meldingen, og at departementet ikke har formulert konkrete mål og resultatkrav overfor tilsynet i henhold til bevilgningsreglementet og økonomireglementet. Post- og teletilsynet har heller ikke utarbeidet noe samlet plandokument for sine aktiviteter. Samferdselsdepartementet har ikke fulgt opp endrede forutsetninger med nye skriftlige styringssignaler til Post- og teletilsynet, og det er derfor grunn til å stille spørsmål ved om departementet har vært tilstrekkelig aktivt i oppfølgingen av tiltakene. St.meld. nr. 47 (2000–2001) legger til grunn at Post- og teletilsynet bør ha en bemanning på minimum 4–7 personer for å få et kompetent sikkerhetsmiljø. Gjennomgangen viser at tilsynet på det meste har hatt tre stillinger på fulltid innen området, og at det i perioden har vært en del utskiftninger av personell, også prosjektledere.

St.meld. nr. 47 (2000–2001) understreker viktigheten av at de finansieringsløsningene som velges, bidrar til klare ansvarsforhold, og at Post- og teletilsynet gis nødvendig handlekraft slik at arbeidet med telesikkerhet og -beredskap ikke blir forsinket eller at de mål som settes ikke nås. Et gjennomgående trekk når det gjelder gjennomføringen av tiltakene fra meldingen, er at finansiering av enkelttiltak ikke er avklart. Forutsetningen i ekomloven om at merkostnader som teleoperatører har for å tilfredsstille krav til sikkerhet og beredskap, skal kompenseres av staten, gjør det enda viktigere å avklare finansiering i en tidlig fase.

St.meld. nr. 47 (2000–2001), som er basert på tidligere utredninger av Forsvarets forskningsinstitutt og et prosjekt ledet av Post- og teletilsynet, ble lagt fram i mai 2001. Fire år senere er hoveddelen av tiltakene fremdeles under utredning, få tiltak er gjennomført, og man har i liten grad avklart hvordan tiltakene på området skal finansieres. Det kan derfor stilles spørsmål ved om Samferdselsdepartementet i tilstrekkelig grad har vektlagt arbeidet med å finne finansieringsløsninger for å sikre framdrift i tiltakene. Tydelige resultatkrav og styringsdokumenter antas å være viktige i en situasjon der Post- og teletilsynet hadde fått nye oppgaver og hadde visse bemanningsproblemer. Det kan stilles spørsmål om hvorvidt mangelfull styring og oppfølging fra Samferdselsdepartementet kan ha medført manglende framdrift i arbeidet.

Post- og teletilsynet skal føre tilsyn med at regelverk for telesikkerhet og -beredskap overholdes, og at pålagte tiltak blir gjennomført. Hittil har tilsynsvirksomheten i overveiende grad hatt karakter av områdeovervåking, og det gjennomføres ikke tradisjonell tilsynsvirksomhet med kontroll av overholdelse av regler og oppfølging av funn. Det kan stilles spørsmål ved om dette gir tilsynet tilstrekkelig effektiv kontroll med den reelle sikkerhetstilstanden for telenettene.

I Innst. S. nr. 329 (2000–2001) viser samferdselskomiteen til at telenettets betydning for flere vitale samfunnsfunksjoner er stor, og at det derfor er av overordnet betydning å sikre operativitet i telenettet under alle forhold. Undersøkelsen viser at en rekke prioriterte tiltak innenfor telesikkerhet og -beredskap fortsatt ikke er gjennomført, og det kan derfor stilles spørsmål ved om operativiteten i telenettene er tilstrekkelig sikret.

338) Med redundans menes omrutingsalternativer eller reserveløsninger i den enkelte operatørs nett eller mellom ulike operatørers nett.

Vedlegg 1: Kildehenvisninger til rapportens tekstbokser

Tekstboks 1

- *Mørketallsundersøkelsen 2003 – Om datakriminalitet og IT-sikkerhet*, Økokrim/Næringslivets Sikkerhetsråd/
- Senter for informasjonssikring, kortversjon, juni 2004, side 12
- Statistikk fra Internet Storm Centre, jf. http://isc.sans.org/survivalhistory.php

Tekstboks 2:

- St.meld. nr. 47 (2000–2001) *Om telesikkerhet og -beredskap i et telemarked med fri konkurranse*
- Radha Gulati: *The Threat of Social Engineering and Your Defense Against It*, SANS Reading room, 31. oktober 2003, jf. http://www.sans.org/rr/whitepapers/engineering

Tekstboks 3:

- Forsvarets forskningsinstitutt; *Sårbarhetsreduserende tiltak innen telekommunikasjon*. FFI/Rapport-99/00242, pkt. 5.2.1
- *Mørketallsundersøkelsen 2003 – Om datakriminalitet og IT-sikkerhet*, Økokrim/Næringslivets Sikkerhetsråd/ Senter for informasjonssikring, kortversjon, juni 2004, side 12

Tekstboks 4:

- *Samhällets informationssäkerhet – Lägesbedömning 2005*, Krisberedskapsmyndigheten i Sverige
- United States Government Accountability Office: *Critical Infrastructure Protection – Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems (GAO-02-474),* juli 2002
- United States Government Accountability Office: *Critical Infrastructure Protection – Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities (GAO-05-434)*, mai 2005

Tekstboks 5:

- National Infrastructure Security Co-ordination Centre: *Briefing 08/2005, Targeted Trojan Email Attacks*, 16. juni 2005
- "Lurer nøkkelfolk med tilpassede trojanere", digi.no, 21. juni 2005
- "Targeted Trojan-horse attacks hitting U.S., worldwide", SecurityFocus, 22. juni 2005
- St.meld. nr. 39 (2003–2004) *Samfunnssikkerhet og sivilt-militært samarbeid*
- Direktoratet for samfunnssikkerhet og beredskap: *Strømbrudd i Europa og Nord-Amerika august–september 2003* (DSB-rapport 2003-10-14)

Tekstboks 6:

- "Försäkringskassan nästan på banan igjen", IDG.se, 28. juni 2004
- "Försäkringskassan väntade med patch till Windows XP", IDG.se, 24. juni 2004
- "Worm Disruptions Shake Preconceptions", Washington Post, 28. januar 2003
- "Slammer worm crashed Ohio nuke plant network", SecurityFocus, 19. august, 2003
- "Hacker jailed for revenge sewer attacks", The Register, 31. oktober 2001
- "Bankproblemene varer til onsdag", Computerworld, 6. august 2001
- "Fem ganger fy", Computerworld, 8. august 2001
- "Med ryggen mot veggen", Computerworld, 10. august 2001

Tekstboks 7:

- United States Government Accountability Office: *Critical infrastructure protection – Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities (GAO-05-434)*, mai 2005

Tekstboks 8:

- Oversikten over CERT-organisasjonene har tatt utgangspunkt i opplysninger hentet fra systemet "Trusted Introducer for CSIRTs in Europe", som er drevet av S-CURE i Nederland på oppdrag fra TERENA (Trans-European Research and Education Networking Association), jf. http://www.ti.terena.nl

Tekstboks 9:

- *Mørketallsundersøkelsen 2003 – om datakriminalitet og IT-sikkerhet*, Næringslivets Sikkerhetsråd/ Senter for informasjonssikring/Økokrim, juni 2004
- "Phishing-forsøk mot en norsk bank", Senter for informasjonssikring, 18. mars 2005, jf. http://www.norsis.no
- Eksempler på phishing i utlandet hentet fra Anti-phishing Working Group, jf. http://www.antiphishing.org/phishing_archive.html
- "Data-hacker skreiv ut falske billettar", Bergens Tidende, 21. september 2004
- "Lost Credit Data Improperly Kept, Company Admits", New York Times, 20. juni 2005

Tekstboks 10:

- *The Federal Information Security Management Act (FISMA)*, vedtatt som en del av *E-Government Act of 2002*
- Committee on Government Reform – US House of Representatives: *2004 Federal Computer Security Report Card Grades*, 16. februar 2005
- Videnskabsministeriet: *It-sikkerhed overalt og for alle – Videnskabsministeriets arbejdsprogram for it-sikkerhed 2005*, jf. også tilgjengelig informasjon på http://www.it-sikkerhedsportalen.dk
- Office of the e-Envoy: *Security – e-Government Strategy Framework Policy and Guidelines (versjon 4.0)*, september 2002
- Bundesamt für Sicherheit in der Informationtechnik: *E-Government-Handbuch*,

nettversjon tilgjengelig på nettsiden http://www.bsi.bund.de/fachthem/egov/6.htm

Tekstboks 11:

- ISMS International User Group: *International Register of ISMS Accredited Certificates*, jf. http://www.xisec.com
- Department of Trade and Industry / PriceWaterhouseCoopers: *Information Security Breaches Survey 2004 – technical report*, side 10
- Videnskabsministeriet: *It-sikkerhed overalt og for alle – Videnskabsministeriets arbejdsprogram for it-sikkerhed 2005*, jf. også tilgjengelig informasjon på http://www.it-sikkerhedsportalen.dk

Tekstboks 12:

- St.meld. nr. 47 (2000–2001) *Om telesikkerhet og -beredskap i et telemarked med fri konkurranse*

Tekstboks 13:

- St.meld. nr. 47 (2000–2001) *Om telesikkerhet og -beredskap i et telemarked med fri konkurranse*

Tekstboks 14:

- St.meld. nr. 47 (2000–2001) *Om telesikkerhet og -beredskap i et telemarked med fri konkurranse*
- "Russian extortion gang faces 15 years", The Register, 29. juli 2004

Tekstboks 15:

- Post- och telestyrelsen: *Strategi för att säkra Internets infrastruktur*, 15. februar 2005

Tekstboks 16:

- "Sånn som dette kan vi ikke ha det", Aftenposten, 14. juni 2005
- "NetCom-fadesen kan få etterspill", Aftenposten, 27. juni 2005
- "Nye problemer for NetComs mobilnett", digi.no, 13. juni 2005
- Post- og teletilsynet: brev til Samferdselsdepartementet av 4. juli 2005 med tittelen *Oversendelse av PTs vurdering av NetComs utfall 12. og 13. juni*

Vedlegg 2: Referanseliste

Referanselisten gir ikke en fullstendig oversikt over kildene som ble brukt i rapporten.
Listen gir en oversikt over kilder som er benyttet i undersøkelsen, men ikke er nevnt i fotnotene i rapporten.

Norske kilder

- Arbeids- og administrasjonsdepartementet: *Strategi for IKT i offentlig sektor – Sentrale fokusområder for å fremme brukerrettede tjenester, effektivitet og forenkling på lokalt nivå,* 18. februar 2003
- Direktoratet for sivilt beredskap: *Systematisk samfunnssikkerhet og beredskap, En veileder i internkontroll for beredskapsarbeid i departementene,* desember 2001
- Direktoratet for sivilt beredskap: *Systematisk samfunnssikkerhets- og beredskapsarbeid i kommunene - en veileder fra Direktoratet for sivilt beredskap,* mai 2001
- Forskningsrådet: *IKT sikkerhet og sårbarhet (IKT SoS), Programbeskrivelse* , revidert februar 2004
- Forsvarsdepartementet: *Iverksettingsbrev for forsvarssektoren - Den videre moderniseringen av Forsvaret i perioden 2005-2008,* 14. september 2004
- Forsvarets Forskningsinstitutt: *Strategier for informasjonssikkerhet – En komparativ studie av strategiarbeidet i Norge, USA, Australia og EU, FFI/Rapport-2003/00271,* 21. januar 2004
- Kredittilsynet: *Den finansielle infrastruktur og bruk av informasjonsteknologi – Risiko- og Sårbarhetsanalyse,* 10. mars 2002
- Moderniseringsdepartementet: *eNorge 2009 – Det digitale spranget,* juni 2005
- Nasjonal Sikkerhetsmyndighet: *Risikovurdering 2003* (Ugradert versjon)
- Nasjonal Sikkerhetsmyndighet: N*asjonal sikkerhetsmyndighets risikovurdering 2004,* ugradert versjon
- Nasjonal Sikkerhetsmyndighet: *NSMs risikovurdering 2005,* ugradert versjon
- Nasjonal Sikkerhetsmyndighet: *Månedsrapporter fra VDI-sentralen fra 2004 og 2005*
- Næringslivets Sikkerhetsråd: *Veiledning til bedre IT-sikkerhet!,* mars 2003
- Nærings- og handelsdepartementet: *eNorge 2005,* 14. mai 2002
- Nærings- og handelsdepartementet: *eNorge 2.0,* 11. desember 2000
- Nærings- og handelsdepartementet: *eNorge – Tilstandsrapport 2004,* 25. mai 2004
- Nærings- og handelsdepartementet: *eNorge – Tilstandsrapport juni 2003, 23.* juni 2003
- Nærings- og handelsdepartementet: *Forslag til etablering av koordineringsutvalg for informasjonssikkerhet, notat fra Ad-hoc arbeidsgruppe vedr. koordineringsutvalg for informasjonssikkerhet,* 18. desember 2003
- Scandpower: *Sårbarhet og beredskap relatert til Internett,* 28. september 2000
- Senter for informasjonssikring: *IKT trusselbilde for Norge,* rapporter fra juni 2003, oktober 2003, mars 2004, oktober 2004 og april 2005
- Teknologirådet: *Fra rådet til tinget - Når nettene blir mange: Digital infrastruktur i Norge,* Nyhetsbrev nr .4, oktober 2002

Faglitteratur

- Anderson, Ross: *Security Engineering – A Guide to Building Dependable Distributed Systems,* John Wiley & Sons, 2001
- Anderson, Ross: *Why Information Security is Hard - An Economic Perspective*
- Denning, Dorothy E.: *Information Warfare and Security,* Addison-Wesley, 1998
- Dunn, Myriam og Wigert, Isabelle: *International Critical Information Infrastructure Protection Handbook 2004,* ETH Zürich, januar 2004
- Schneier, Bruce: Beyond *Fear – Thinking sensibly about security in an uncertain world*, Copernicus Books, 2003

Internasjonale dokumenter

Den europeiske union (EU):

- Dependability Development Support Initiative: *Securing the information Society: A European Policy Agenda – Summary of DDSI findings* (IST-2000-29202), november 2002
- Europaparlamentets og Rådet for Den europeiske union: F*oordning (EF) nr. 460/2004 av 10. mars 2004 om opprettelse av en europeisk etat for nett- og informasjonssikkerhet*
- Rådet for Den europeiske union: *resolusjon av 28. januar 2002 om en felles strategi og særlige foranstaltninger innenfor nett- og informasjonssikkerhet* (2002/C 43/02)
- Rådet for Den europeiske union: *resolusjon av 18. februar 2003 om en europeisk strategi for utvikling av en kultur for nett- og informasjonssikkerhet* (2003/C 48/01)

Forenede Nasjoner (FN):

- Resolusjon 55/63: *Combating the criminal misuse of information technologies,* 22. januar 2001
- Resolusjon 57/239: *Creation of a global culture of cybersecurity,* 31. januar 2003
- Resolusjon 58/199: *Creation of a global culture of cybersecurity and the protection of critical information infrastructures,* 30. januar 2004

Organisasjonen for økonomisk samarbeid og utvikling (OECD):

- Directorate For Science, Technology And Industry, Committee For Information, Computer And Communications Policy, Working Party on Information Security and Privacy: *Summary of responses to the survey on the implementation of the OECD guidelines for the security of information systems and networks: towards a culture of security,* 24. september 2004

Sverige:

- Krisberedskapsmyndigheten: *Basnivå för IT-säkerhet* (2003:2)
- Krisberedskapsmyndigheten: *Samhällets informationssäkerhet - Lägesbedömning 2005*
- Post & Telestyrelsen: *Robusta elektroniska kommunikationer - Strategi för åren 2003-2005,* 31. mars 2003
- Regeringens proposition 2001/02:158: *Samhällets säkerhet och beredskap,* 14. mars 2002
- SOU2004:32 *Informationssäkerhet i Sverige och internationellt – en översikt* (Delrapport 2 från InfoSäkutredningen)

Danmark:

- Ministeriet for Videnskab, Teknologi og udvikling: *It-sikkerhed overalt og for alle - Videnskabsministeriets arbejdsprogram for it-sikkerhed 2005*
- Ministeriet for Videnskab, Teknologi og udvikling: *Rapport om standard for it-sikkerhedsprocesser i staten,* juni 2003

Finland:

- The Ministry of Transport and Communications: *Government Resolution On National Information Security Strategy,* 4. september 2003

Nederland:

- Ministerie van Verkeer en Waterstaat/ Ministerie van Economische Zaken: *Internet vulnerability - Working together towards better security and dependability*, juli 2001
- Luiijf, Ir. H.A.M. og Klaver, Dr. M.H.A.: *In bits and pieces - Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society*, mars 2000

Storbritannia:

- Cabinet Office/Central Sponsor for Information Assurance: *Protecting our information systems - Working in partnership for a secure and resilient UK information infrastructure*, 2004
- Information Assurance Advisory Council: *Protecting the digital society - a manifesto for the UK*, mars 2002
- National Infrastructure Security Co-ordination Centre: *International CIIP Directory,* januar 2005
- Office of Telecommunications: *Guidelines on the essential requirements for network security and integrity,* 9. oktober 2002

USA:

- The White *House: The National Strategy To Secure Cyberspace*, februar 2003
- U.S. House of Representatives, Committee On Government Reform: *Davis Statement on 2004 Federal Computer Security Report Card Grades,* 16. februar 2005
- U.S. Government Accountability Office: *Combating terrorism - Evaluation of Selected Characteristics in National Strategies Related to Terrorism,* 3. februar 2004
- U.S. Government Accountability Office, Testimony Before the House Committee on Government Reform: *Information Security - Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements*, 7. april, 2005
- National Security Telecommunications Advisory Council: *Network security/vulnerability assessments – Task force report,* mars 2002

Riksrevisjonen
Pilestredet 42
Postboks 8130 Dep
0032 Oslo

sentralbord 22 24 10 00
telefaks 22 24 10 01
riksrevisjonen@riksrevisjonen.no

www.riksrevisjonen.no