Innst. S. nr. 85

(2005-2006)

Innstilling til Stortinget fra kontroll- og konstitusjonskomiteen

Dokument nr. 3:4 (2005-2006)

Innstilling fra kontroll- og konstitusjonskomiteen om Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur

Til Stortinget

1. SAMMENDRAG

1.1 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 pst. av norske virksomheter rammet av datakriminalitet eller andre uønskede hendelser, og at dette kostet norske virksomheter mer enn fem milliarder kroner.

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.

1.2 Oppsummering av undersøkelsen

Undersøkelsen er gjennomført ved analyse av sentrale dokumenter i arbeidet med informasjonssikkerhet innen statsforvaltningen, ved intervjuer og ved en spørreundersøkelse. 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.

1.2.1 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.

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. Departementet har samtidig en pådriverrolle overfor fagdepartementene.

Justis- og politidepartementet har et samordnings- og tilsynsansvar for samfunnets sivile sikkerhet og for beredskap i kritisk infrastruktur. Departementet har overordnet ansvar for Direktoratet for samfunnssikkerhet og beredskap (DSB), som ble opprettet 1. september 2003.

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. Nasjonal sikkerhetsmyndighet ble opprettet 1. januar 2003 som et eget direktorat administrativt underlagt Forsvarsdepartementet i militær sektor og Justis- og politidepartementet i sivil sektor.

Samferdselsdepartementet har et sektoransvar for telesikkerhet og -beredskap, og er regelverksforvalter av lov om elektronisk kommunikasjon, 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 Samferdselsdepartementets 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 Moderniseringsdepartementet 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.

Mange fagorganer 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.

1.2.2 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. 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

Forsvarskomiteen og justiskomiteen har presisert at den grunnleggende kunnskapen om hva som skaper sårbarhet, bør prioriteres i sikkerhetsarbeidet, jf. Innst. S. nr. 9 (2002-2003). 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. 5 200 datainnbrudd og 2,7 millioner forsøk på datainnbrudd i 2003. 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.

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. 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 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.

Forsvarskomiteen og justiskomiteen har påpekt at det er viktig å gjennomføre øvelser for å få et ledelsesapparat som kan håndtere kriser, jf. Innst. S. nr. 9 (2002-2003). 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. 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.

1.2.3 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.

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.

1.2.4 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. 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.

1.2.5 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 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.

Samferdselskomiteen har vist 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, jf. Innst. S. nr. 329 (2000-2001). I undersøkelsen stilles det spørsmål om hvilke konsekvenser manglende gjennomføring av tiltakene i St.meld. nr. 47 (2000-2001) har for operativiteten i telenettene.

1.3 Departementenes kommentarer

1.3.1 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.

1.3.2 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.

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.

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. 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.

1.3.3 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.

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 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 departementsstrukturen høsten 2004 medførte at framdriften for en del av tiltakene mot næringslivet ble forsinket.

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.

1.3.4 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.

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.

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.

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.

1.4 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.

1.4.1 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.

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.

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 understreker derfor 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.

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 krisehåndterings-

planer 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.

1.4.2 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. 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 Budsjett-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.

1.4.3 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.

1.4.4 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).

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.

1.5 Departementenes svar

1.5.1 Forsvarsdepartementet

Saken har vært forelagt Forsvarsdepartementet. Det følger av statsrådens svarbrev til Riksrevisjonen av 3. november 2005:

"…

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.

…

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."

1.5.2 Justis- og politidepartementet

Saken har vært forelagt Justis- og politidepartementet. Det følger av statsrådens svarbrev til Riksrevisjonen av 20. oktober 2005:

"…

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."

1.5.3 Moderniseringsdepartementet

Saken har vært forelagt Moderniseringsdepartementet. Det følger av statsrådens svarbrev til Riksrevisjonen av 24. oktober 2005:

"…

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) mv.

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."

1.5.4 Samferdselsdepartementet

Saken har vært forelagt Samferdselsdepartementet. Det følger av statsrådens svarbrev til Riksrevisjonen av 28. oktober 2005:

"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."

1.6 Riksrevisjonens uttalelse

Riksrevisjonens undersøkelse viser at myndighetenes arbeid med IT-sikkerhet preges av mange aktører og uklare ansvarsforhold. Riksrevisjonen understreker 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.

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 understreker 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.

2. KOMITEENS MERKNADER

Komiteen, medlemmene fra Arbeiderpartiet, Berit Brørby, Svein Roald Hansen og Ivar Skulstad, fra Fremskrittspartiet, Carl I. Hagen og lederen Lodve Solholm, fra Høyre, Per-Kristian Foss, fra Sosialistisk Venstreparti, Inge Ryan, fra Kristelig Folkeparti, Dagfinn Høybråten, og fra Senterpartiet, Magnhild Meltveit Kleppa, viser til at tekniske framskritt knyttet til datateknikk og elektronikk, har gitt menneskene muligheter både for å utforske verdensrommet og å skape et helt nytt materielt grunnlag for tilværelsen. Men ved å ta i bruk de mulighetene den teknologiske utvikling gir, utvikles samfunns- og leveforhold som er langt mer sårbare enn før. Dette fordi bruk av høyteknologi er avhengig av mange ulike faktorer og konsekvensene kan bli svært vidtrekkende om noe ikke fungerer.

Komiteen har merket seg Sårbarhetsutvalgets påpeking av at stater og terrorgrupper med forholdsvis enkle midler kan lamme viktige virksomheter og samfunnsfunksjoner. Mulighet for sabotasje, internasjonal kriminalitet og spionasje, eller brudd i telesamband, elektrisitetsforsyning eller betalingssystemer, stiller oss overfor utfordringer ethvert samfunn må ta på alvor.

På denne bakgrunn vil komiteen uttrykke tilfredshet med at Riksrevisjonen har iverksatt undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur, både i forhold til å bedre IT-sikkerheten og til tiltak for bedre telesikkerhet.

Komiteen konstaterer at formålet med undersøkelsen har vært å vurdere dette arbeidet opp mot Stortingets vedtak og forutsetninger. Det har følgelig vært naturlig å se på organiseringen av arbeidet, plan og gjennomføringsprosessene og de tiltak som er iverksatt.

Komiteen viser til St.meld. nr. 17 (2001-2002) Samfunnssikkerhet hvor det ble slått fast at ansvaret for IT-sikkerheten skal være et virksomhetsansvar, og har merket seg at dette er fulgt opp gjennom organiseringen av arbeidet.

Når det gjelder ansvarsfordelingen for koordinering og tverrgående tilsynsoppgaver innen IT-sikkerhet, konstaterer komiteen derimot at det fortsatt mangler grunnleggende avklaringer.

Riksrevisjonens undersøkelse viser at Justisdepartementet ikke har avklart betydningen av hva ansvaret for kritisk infrastruktur innebærer og hvilket ansvar departementet vil ha i en krisesituasjon. Selv om det ifølge undersøkelsen er satt i gang noe arbeid for å definere hva som er samfunnskritisk infrastruktur, synes dette arbeidet ikke å ha hatt tilstrekkelig prioritet.

Komiteen har registrert departementets tilsvar til Riksrevisjonen og kan vanskelig se at dette tilfredsstiller de krav til klarhet om ansvarsfordeling som Stortinget burde kunne forvente.

Komiteen vil understreke betydningen av klare prosedyrer i krisesituasjoner og peker på behovet for at Justisdepartementets rolle i en slik sammenheng utdypes og klargjøres ytterligere.

Komiteen har videre merket seg Riksrevisjonens påpeking av ulik oppfatning mellom Samferdselsdepartementet og Moderniseringsdepartementet (Fornyings- og administrasjonsdepartementet fra 1. januar 2006) når det gjelder SDs ansvar for sikkerhet for Internett-relaterte tjenester sett i forhold til MODs ansvar for sikkerheten i IT-sikkerhetsarbeidet. Basert på MODs svar synes avgrensningen av Samferdselsdepartementets ansvar noe uklart.

Komiteen har registrert at MOD har ansett det hensiktsmessig å nedsette en interdepartemental arbeidsgruppe for å avklare de ulike departementenes rolle.

Komiteen deler Riksrevisjonens bekymring for hvilke konsekvenser manglende ansvarsavklaring for IT-sikkerheten i samfunnet vil kunne få i en krisesituasjon.

Komiteen har merket seg Riksrevisjonens påpeking av at utarbeidelse av veiledninger for risiko- og sårbarhetsanalyser ikke automatisk fører til at slike blir benyttet verken ved valg av metoder eller når sikkerhetstiltak skal prioriteres. Etter komiteens syn understreker dette behovet for klar ansvarsplassering

og en helhetlig tilnærming til sikkerhetsproblematikken.

Komiteen har videre notert Riksrevisjonens understreking av behovet for å fange opp informasjon om trusler og sårbarhet i IT-infrastrukturen og henvisningene til Varslingssystem for digital infrastruktur (VDI) og Senter for informasjonssikring (SIS).

Komiteen konstaterer at ingen av de to organene så langt synes å ha nådd vesentlige mål for virksomheten. Forsvarsdepartementets så vel som Moderniseringsdepartementets kommentarer til Riksrevisjonen, styrker antagelsen om et stort forbedringspotensial for begge virksomheter.

Komiteen imøteser avklaring både på SIS' ansvar og oppgaver i forhold til relevante faginstanser og VDIs organisering for å sikre fastsatte mål.

Komiteen viser til Riksrevisjonens vurdering av mulige årsaker til manglende fremdrift av IT-sikkerhetsarbeidet og konstaterer at departementene fram til mai 2005 ikke hadde hatt kontakt med de utvalgte bransjeorganisasjonene som i henhold til Nasjonal strategi for informasjonssikkerhet, er gitt et medansvar for å ivareta viktige funksjoner. Komiteen finner det kritikkverdig at denne kontakten ikke er fulgt opp i tråd med forutsetningene.

Videre synes uenighet rundt plasseringen av CERT (Computer Emergency Response Team) å være av betydning for manglende fremdrift. Komiteen forutsetter at spørsmålet om plassering, ansvar og forhold til andre aktører snarest blir avklart.

Komiteen finner grunn til alvorlig bekymring når Riksrevisjonen viser at plandokumentene for oppfølgingen av Nasjonal strategi for informasjonssikkerhet har vært utilstrekkelige, at de som har hatt ansvaret for samordning er gitt få virkemidler, at finansieringen av tverrsektorielle tiltak har vært undervurdert og at regelverket ikke i tilstrekkelig grad har vært samordnet.

Riksrevisjonen retter særskilt søkelyset på telesikkerhet og -beredskap. At bare et fåtall av de vedtatte tiltak i St.meld. nr. 47 (2000-2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse er satt ut i livet, er etter komiteens syn sterkt å beklage og avdekker en manglende respekt for Stortingets vedtak.

Komiteen har notert at de respektive departementer ved flere anledninger understreker at arbeid er i gang. Basert på Riksrevisjonens rapport og de svar departementene har gitt, fremstår innsatsen for å bedre sikkerheten som lite helhetlig og strukturert.

Komiteen deler Riksrevisjonens vurdering av at avhengighet mellom sektorer kan bety at vurderingen av sikkerheten i den enkelte sektor ikke nødvendigvis gir et korrekt bilde av sikkerhetstilstanden for samfunnet som helhet.

Oppsummert anser komiteen at arbeidet med å sikre IT-sikkerhet synes å lide under manglende koordinering og avklaring av funksjoner, og vil uttrykke bekymring for situasjonen.

Komiteen vil understreke at helt avgjørende funksjoner som elektrisitetsforsyning og kommunikasjoner, teletjenester og informasjonstjeneste, betalingsoverføringer, helsetjenester og sykehusdrift mv., er avhengige av informasjonsteknologi. Bare i begrenset grad kan de enkelte institusjoner avbøte risiko ved for eksempel å skaffe seg nødvendige strømaggregater eller doble anlegg. Det er også grunn til å peke på at Norge er betydelig avhengig av utlandet i forbindelse med forsyninger av elektronisk utstyr og reservedeler. Dette reiser spørsmål om behov for reservelagre i Norge, om en helhetlig strategi for back-up-sentraler osv.

Komiteen viser i tillegg til Sårbarhetsutvalgets understreking av behovene for en styrking av beredskapen på personellsiden med sterkere vekt på opplæring og ajourføring av kunnskaper, med skjerpede sikkerhetsrutiner og muligheter for personellkontroll i forbindelse med samfunnsviktig virksomhet. Komiteen slutter seg til disse vurderingene.

Komiteen anser de problemstillinger som er reist i Riksrevisjonens rapport, for å være av stor viktighet og forutsetter at Regjeringen i løpet av 2006 kommer tilbake med en redegjørelse til Stortinget for arbeidet med å avklare de overordnede ansvarsforholdene mellom departementene når det gjelder IT-sikkerhet. Redegjørelsen forutsettes også å inneholde en vurdering av krisehåndtering, plassering av CERT samt status for arbeidet med å fange opp trusler og avdekke sårbarhet.

Komiteen understreker viktigheten av at det stilles tilstrekkelige ressurser til rådighet slik at arbeidet med å sikre en tilfredsstillende kriseberedskap og IT-infrastruktur kan gis nødvendig prioritet.

3. KOMITEENS TILRÅDING

Komiteen har ellers ingen merknader, viser til dokumentet og rår Stortinget til å gjøre slikt

vedtak:

Dokument nr. 3:4 (2005-2006) - om Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur - vedlegges protokollen.

Oslo, i kontroll- og konstitusjonskomiteen, den 7. februar 2006

Lodve Solholm
leder

Berit Brørby
ordfører