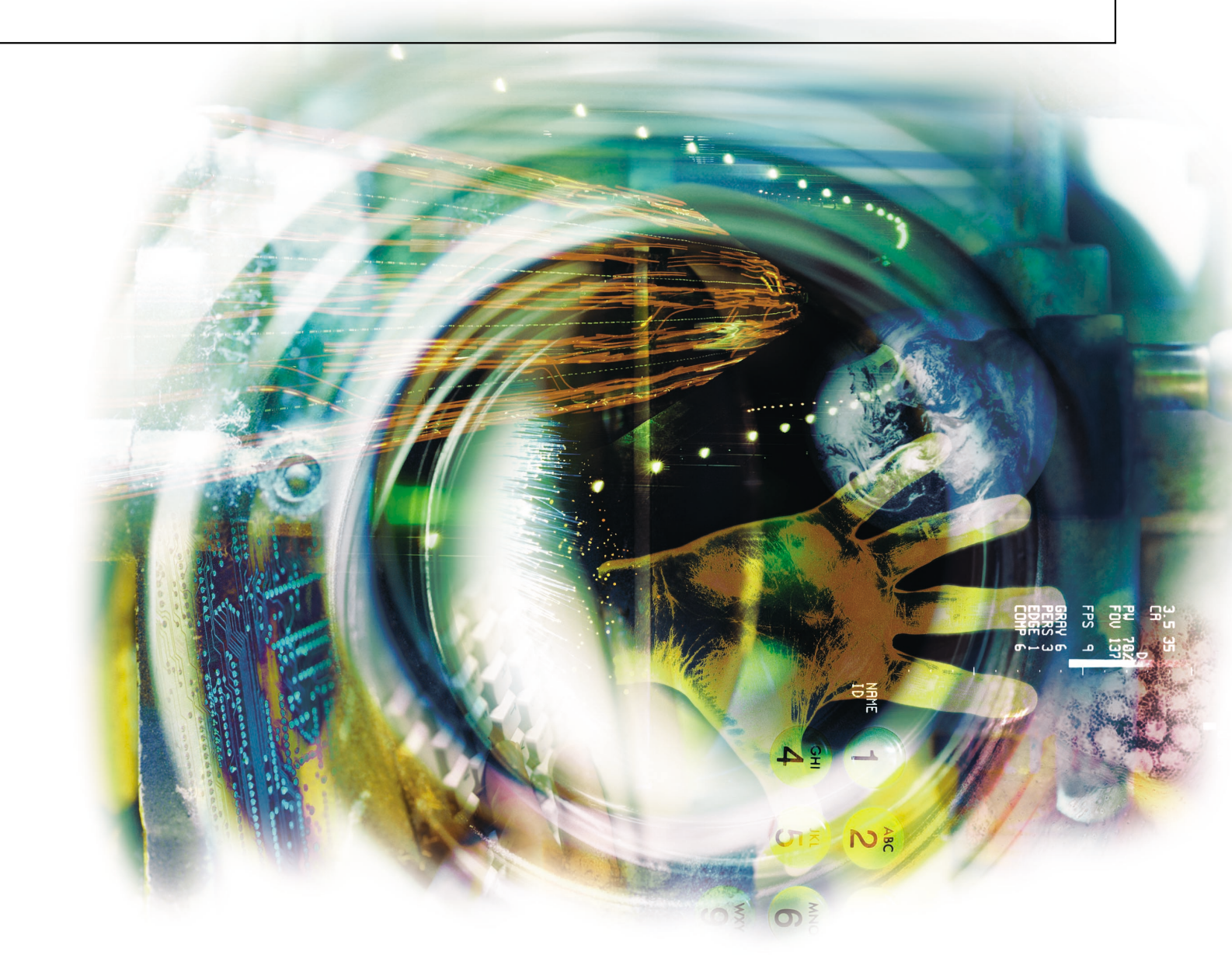
FORSVARSDEPARTEMENTET
NÆRINGS- OG HANDELSDEPARTEMENTET
JUSTIS- OG POLITIDEPARTEMENTET

Juni 2003

e-norge

Nasjonal strategi for informasjonssikkerhet

Utfordringer, prioriteringer og tiltak



Innholdsfortegnelse

Innledning

Regjeringens nasjonale strategi for informasjonssikkerhet er utviklet på felles initiativ fra Nærings- og handelsdepartementet, Justisdepartementet og Forsvarsdepartement. Strategien har et perspektiv på 2-3 år.

Strategiens formål er:
1. Å sikre en helhetlig tilnærming til arbeidet med informasjonssikkerhet som grunnlag for politiske beslutninger og prioriteringer.
2. Å legge til rette for bedre koordinering av myndigheter som arbeider med informasjonssikkerhet.

Strategien skal bidra til:
- å redusere sårbarheten ved alminnelig bruk av IT og i kritisk IT-infrastruktur
- å legge til rette for trygg elektronisk forretningsdrift i privat og offentlig sektor samt sikre og pålitelige nettjenester fra det offentlige.

Strategien henvender seg i første rekke til myndigheter, næringslivet og organisasjoner. Den er imidlertid viktig for alle brukere av informasjonsteknologi - også enkeltindivider - fordi de fleste av dem er knyttet til lokale, nasjonale og internasjonale datanett.

Regjeringen har fire overordnede mål for informasjonssikkerhet:

1. 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.

2. 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.

3. Norge skal ha en allment tilgjengelig samfunnsinfrastruktur for elektronisk signatur, autentisering av kommunikasjonspartere samt sikker overføring av sensitiv informasjon.

4. Regelverk som berører informasjonssikkerhet skal håndheves og videreutvikles på en samordnet, og for brukere enkel og oversiktlig måte.

Økt bevissthet om informasjonssikkerhet hos alle vil bidra til økt og tryggere bruk av nettbaserte tjenester. Det vil også styrke arbeidet med å utvikle tiltak for å sikre samfunnskritisk IT-infrastruktur.

I 2002 publiserte OECD *Retningslinjer for sikkerhet i informasjonssystemer og nettverk* og lanserte begrepet "sikkerhetskultur" i forbindelse med bruk av IT og Internett. Strategien bygger på disse retningslinjene.

Strategi

Myndighetene vil ha ulike roller for å ivareta nasjonale og samfunnsinteresser innen informasjonssikkerhet, men også andre aktører som utvikler, eier, leverer, forvalter og bruker informasjonssystemer og –nettverk vil spille en viktig rolle. Alle har et felles ansvar for øket bevissthet om og forståelse av IT-sikkerhetsspørsmål, og for å bidra til å utvikle en "sikkerhetskultur" i samfunnet.

I Beskytte kritisk IT-infrastruktur

Samfunnskritisk IT-infrastruktur skal beskyttes i forhold til tilgjengelighet, integritet og konfidensialitet. I de fleste tilfeller vil sikring av tilgjengelighet og integritet være viktigst. Sikringstiltak må ta tilstrekkelig hensyn til opprettholdelse av systemenes fulle funksjonalitet. Virksomheter må selv sørge for planer og tiltak ved svikt i egen kritisk IT-infrastruktur.

II Samordne regelverk for IT-sikkerhet bedre

Håndheving og utvikling av regelverket skal samordnes bedre. Det må bli enklere for brukerne å etterleve reglene samtidig som den tilsiktede virkningen skal sikres. Myndigheter og regelforvaltere må utveksle erfaringer og samarbeide om felles metoder og verktøy slik at ressursene utnyttes bedre, brukernes myndighetskontakt forenkles og næringslivets byrder reduseres.

III Koordinere arbeidet med IT-sikkerhet

Det skal etableres et permanent utvalg for nasjonal koordinering av arbeidet med IT-sikkerhet, sammensatt av sentrale myndigheter og regelverksforvaltere. Utvalgets primære arbeidsfelt skal være alminnelig IT-sikkerhet, men også spørsmål knyttet til rikets sikkerhet, vitale nasjonale sikkerhetsinteresser og kritiske samfunnsfunksjoner skal vurderes. Utvalget skal ikke bryte med det etablerte linjeansvaret for IT-sikkerhetstiltak i sektorene.

IV Gjennomføre risiko- og sårbarhetsanalyser

Risiko- og sårbarhetsanalyser skal ligge til grunn for alle tiltak myntet på informasjonssikkerhet. Strategier og tiltak skal utarbeides, gjennomgås og revideres på basis av regelmessig gjennomførte analyser. Det er i virksomhetenes egen interesse at det blir gjennomført analyser og utarbeidet strategier.

Slike strategier må ivareta sikkerhetsbehovene knyttet til den aktuelle informasjonsbehandlingen eller det aktuelle systemet. Det bør alltid være klarlagt hva som er akseptabel risiko ved informasjonsbehandlingen eller -systemet og hvilke egenskaper som skal prioriteres - tilgjengelighet, integritet eller konfidensialitet - samt hvilke kostnader som sikring av dette innebærer og som må bæres av virksomheten.

V Klassifisere informasjon og informasjonssystemer

Systemer og informasjon bør klassifiseres i forhold til hvor kritisk systemet/informasjonen er for virksomheten eller samfunnet og hvilke trusler de kan utsettes for. Hensikten er å forenkle arbeidet med og redusere kostnader knyttet til IT-sikkerhet. Aktuelle sikringstiltak kan på en enkel måte knyttes til de ulike klassene. Hvor mange klasser som skal defineres avhenger av virksomheten selv og hva slags informasjonsbehandling eller hvilke systemer som håndteres.

VI Bevisstgjøre alle aktører

Alle aktører skal bevisstgjøres når det gjelder trusselbilde, muligheter, begrensninger og nødvendige tiltak for å bidra til etablering av en kultur for IT-sikkerhet. Dette er en oppgave for myndighetene, men alle har et selvstendig ansvar for å skaffe nødvendig kunnskap, slik at man ikke bryter norsk lov eller ignorerer alminnelige etiske og demokratiske prinsipper. Unnlatelse å skaffe seg nødvendig kunnskap kan føre til skade hos andre, som man kan bli stilt ansvarlig for.

VII Varsle og gi råd

Det skal etableres varslingsordninger som samfunnsaktørene kan benytte for å beskytte systemer og nettverk mot IT-angrep, og som muliggjør rask iverksettelse av forebyggende og skadebegrensende tiltak. Ordningene bør primært være tilgjengelig for eiere av samfunnskritiske systemer og –infrastruktur, men alminnelige bedrifter og offentlige etater bør også ha tilgang på slik informasjon. Myndighetene har ansvar for å etablere slike varslingsmekanismer. Næringslivets organisasjoner og myndighetene må i fellesskap ta ansvaret for aktuelle ordninger i næringslivet. Forvaltningen må sørge for tilsvarende ordninger innen egen sektor.

VIII Ansvarliggjøre bransjen og leverandørene

IT-bransjen har ansvar for å legge inn sikkerhet i produkter, systemer og nett og for å informere brukerne om hvordan de kan beskytte seg.
For å styrke samfunnets IT-sikkerhet bør bransjen utarbeide normer for produktutvikling, satse på å implementere brukervennlig IT-sikkerhet og ta ansvar overfor egne kunder og samarbeidspartnere. Dersom bransjen ikke tar dette ansvaret, vil myndighetene vurdere særskilte reguleringstiltak eller stille krav knyttet til egen innkjøpsvirksomhet.

1

IX Sertifisere kritiske systemer

Kritiske IT-systemer og –infrastruktur bør beskyttes gjennom sertifiserte sikkerhetsløsninger.
Virksomheter bør strukturere arbeidet med informasjonssikkerhet etter tilgjengelige standarder. Organisasjoner som ønsker å kvalitetssikre arbeidet bør ta i bruk sertifiseringsordninger for IT-sikkerhet som er tilgjengelige i Norge. Kostnadene ved dette bør avveies mot gevinster med økt sikkerhet og redusert sårbarhet.

X Styrke sikkerhetskompetansen

Kompetanse innen IT-sikkerhet skal styrkes i hele samfunnet, befolkningen, i virksomhetene og i forvaltningen. Det skal etableres utdanningstilbud innen IT-sikkerhet som gir kompetanse på master-nivå og fokus på IT-sikkerhet skal styrkes innen andre kompetanseområder. Forskning og utvikling innen IT-sikkerhet skal også styrkes.

XI Legge til rette for allmenn bruk av elektronisk signatur/PKI (Public Key Infrastructure)

Norge skal ha en godt tilgjengelig samfunnsinfrastruktur for elektronisk identifisering og –signatur, basert på PKI-teknologi, som muliggjør autentisering, digital signering og konfidensialitet av elektronisk kommunikasjon. Infrastrukturen skal baseres på internasjonale standarder, men tilpasses norske forhold, med klart definerte roller, forpliktende avtaler og andre tiltak som sikrer teknisk samspill og samtrafikk. Infrastrukturen som skal utvikles i samarbeid mellom offentlig og privat sektor, skal være tatt i bruk av tilstrekkelig mange tjenestetilbydere og brukere innen utgangen av 2005.

XII Delta i internasjonalt samarbeid

Norge skal delta aktivt i internasjonale organer der IT-sikkerhet drøftes og internasjonale tiltak vedtas. Informasjonssikkerhet krever en internasjonal tilnærming og –koordinering. Norge skal delta i relevante organer innen OECD og NATO. Norge tar sikte på å delta i det foreslåtte Nettverks- og informasjonssikkerhetsbyrået i EU. I tillegg vil nærmere samarbeid med land som er kommet langt i å gjennomføre en sikkerhetskultur vurderes.

Informasjonssikkerhet koster

2

Informasjonssikkerhet ligger innenfor ledelsens linjeansvar. Den må ivaretas i daglig oppgaveløsning og finansieres innenfor rammene for finansiering av den ordinære virksomheten. Kostnader som gjennomføringen av strategien vil medføre vil berøre både offentlige og private virksomheter.

I offentlig forvaltning vil de administrative og økonomiske konsekvenser av de foreslåtte tiltakene måtte konkretiseres i forbindelse med planlegging av gjennomføringen. Tiltakene må gjennomføres og finansieres innenfor de til enhver tid gjeldende budsjettrammer for hver enkelt offentlig virksomhet. I private virksomheter vil ev. kostnader måtte tas under ordinære driftsrammer for virksomheten. Det vil måtte foretas en avveining mellom kostnader økt sikkerhet medfører og de gevinster (reduksjon i sårbarhet, sikring av kritiske data osv., reduksjon av kostnader i primærvirksomhet) som planlegges oppnådd. I privat virksomhet bør en beregning av mulige tap ved sikkerhetsbrudd inngå i en slik avveining. Det tas sikte på å innlede en dialog med privat sektor med tanke på samfinansiering av enkelte av tiltakene.

Tiltak under de enkelte strategipunktene skal finansieres av de ansvarlige departementer, ev. i samarbeid med privat sektor. Enkelte av tiltakene under strategipunkt I er allerede iverksatt . Andre tiltak må utredes og planlegges nærmere. Spørsmålet om iverksettelse og dimensjonering vil måtte avveies mot kostnader gjennomføringen vil medføre.

Tiltak under punkt II og III vil medføre kun begrensede kostnader, men medføre administrative konsekvenser ved at det tillegges noen nye oppgaver til eksisterende myndighetsorganer.

Tiltak under punkt IV og V kan medføre kostnader for næringslivet og for offentlige virksomheter. Kostnadene vil uansett måtte tas dersom virksomheten faller under regelverk som krever slike tiltak (som f.eks. personopplysningsloven eller sikkerhetsloven). Private virksomheter vil måtte foreta en kost-nytte vurdering før ev. iverksettelse av tiltakene.

Tiltak under punkt VI vil medføre kostnader der størrelse vil avhenge av ambisjonsnivå, fra ubetydelige kostnader ved enkle informasjonstiltak til større kampanjer. Samarbeid med næringslivets bransjeorganisasjoner vil kunne bidra til jevnere fordeling av kostnader mellom myndigheter og privat sektor.

Tiltak under punkt VII er allerede iverksatt og nødvendig budsjettmessig dekning sikret til utgangen av 2004.

Tiltak under punkt VIII er delvis iverksatt i IKT-bransjen, som tar kostnadene som en del av deres forretningsutviklingskostnader. Her kan det også være tale om omstillingskostnader i IKT-bransjen.

Tiltak under punkt IX kan medføre kostnader for private eller offentlige virksomheter. Iverksettelse av tiltakene bør være gjenstand for kost-nytte vurdering i hver enkel virksomhet. Virksomheter som vil bli pålagt tiltak gjennom myndighetsregulering vil måtte bære kostnadene innenfor sine ordinære driftsrammer.

Tiltak under punkt X er delvis iverksatt og budsjettmessig dekning sikret gjennom ordinære tildelinger og delvis samfinansiering med privat sektor. Private virksomheter har selvstendig ansvar for å vurdere nytten ved oppgradering av egen sikkerhetskompetanse mot de kostnader slik oppgradering vil medføre.

Tiltak under XI er delvis under iverksetting. Kostnader vil fordeles mellom offentlig og privat sektor. Tiltak knyttet til koordineringsoppgaver vil medføre administrative konsekvenser ved at det vil opprettes et nytt organ under AAD. Kostnader knyttet til implementeringsrettede tiltak vil måtte dekkes innenfor ordinære driftsrammer for både offentlige og private virksomheter.

Tiltak under punkt XII er under gjennomføring og kostnader dekkes under ordinære driftsrammer for angjeldende myndigheter. Kostnader knyttet til ev. deltagelse i et nytt EU organ vil være ubetydelige.

Om informasjons-sikkerhet

Informasjon er et aktivum som kan ha stor verdi for en virksomhet eller for et individ. Informasjon, informasjonssystemer (dvs. systemer der informasjonen produseres, lagres og behandles) og nett der informasjonen utveksles kan utsettes for trusler og anslag, og må derfor beskyttes forsvarlig.

Beskyttelse av informasjon innebærer sikring av informasjonens:

- tilgjengelighet (for rett person, til rett tid og i rett form)
- integritet (at informasjonen er korrekt og ikke forfalsket/ødelagt)
- konfidensialitet (at informasjonen sikres mot uvedkommende innsyn).

Informasjonssikkerhet kan derfor defineres som tiltak for å beskytte *informasjonen* 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 informasjonen utveksles.

Informasjon lagres, behandles og kommuniseres i stor grad ved hjelp av IT-systemer, selv om vi fremdeles bruker papir for å tilegne oss den. Med IT menes teknologier *både* for behandling *og* kommunikasjon av elektronisk informasjon.

Tiltak og virkemidler som benyttes for å beskytte informasjon som lagres, behandles og kommuniseres i IT-systemer kalles *IT-sikkerhet*. I dette dokument benytter vi derfor begrepet *IT-sikkerhet* synonymt med *informasjonssikkerhet.*

I mange sammenhenger benyttes også begrepet *IT-sårbarhet*. IT-sårbarhet er en egenskap ved IT-systemer og andre former for IT-bruk som gjør dem utsatt (følsomme) for ødeleggelse eller lammelse av en trussel.[1]

Se Vedlegg 1 for de mest brukte ord og uttrykk innen informasjonssikkerhet.

I et marked med krav om effektiv drift og god service til kundene åpner stadig flere virksomheter datasystemene sine for eksterne brukere. En slik økt tilgjengelighet øker også muligheten for kriminelle aktiviteter eller annen type anslag.

[1] Med en trussel menes f.eks. en hacker, en terrorist, en uoppdaget konstruksjonsfeil, feilaktig bruk, overbelastning, naturkatastrofe el.l.

Betydningen av god informasjonssikkerhet kan best belyses ved noen eksempler.

Eksempel 1

En liten, høyteknologisk bedrift som utvikler programvare for styring av industriprosesser vil ha mye av sine verdier lagret i form av programkode (informasjon). Dersom bedriften ikke har iverksatt nødvendige IT-sikkerhetstiltak kan disse verdiene lett gå tapt, f.eks. ved at en hacker bryter seg inn i bedriftens datasystemer og ødelegger koden, uten at tilstrekkelige sikkerhetskopier foreligger. På samme måte kan en ansatt volde stor skade om han tar med seg koden når han slutter og benytter den når han selv starter en konkurrerende bedrift eller blir ansatt i en slik. Skjer noe av dette må bedriften benytte store ressurser og bære tunge kostnader for å gjenskape den ødelagte informasjonen, ev. bekoste rettslige skritt for å stanse urettmessig bruk hos konkurrentene.

Eksempel 2

Avbrudd i kraftforsyningen kan være svært kritisk for de fleste virksomheter. Med bakgrunn i en strømforsyning som vanligvis er pålitelig vurderes anskaffelse av et reserveaggregat ofte som for dyrt i forhold til nytten. Driftskontrollsystemer i dagens kraftforsyning er i stor grad basert på fjernstyring, der IT-systemer har en sentral rolle. Slike systemer baseres gjerne på åpent tilgjengelige standarder og det er enkelt å integrere dem med administrative systemer hos kraftleverandørene. Dette gir utvidet funksjonalitet og effektivitet. Administrative systemer knyttes gjerne opp mot offentlige nett, noe som kan eksponere driftskontrollsystemene, og dermed driften av kraftforsyningen, for risiko en slik nettilknytning kan føre med seg. Manglende sikkerhetstiltak og tilstrekkelig kompetanse hos en ondsinnet aktør kan derfor ramme driftskontrollsystemet til kraftproduksjonen via det administrative systemet. Som en konsekvens av dette kan virksomheter som er avhengig av kraftforsyningen også rammes av omfattende strømutfall. Slike avbrudd i kraftforsyning kan få alvorlige samfunnsmessige konsekvenser.

Eksempel 3

Overføring av lyd, tekst, bilder og andre data ved hjelp av elektromagnetiske signaler krever tilgjengelige og sikre kommunikasjonsnett. Brudd i kabler, radioutstyr, og lignende kan få store konsekvenser både for leverandører og brukere av elektroniske kommunikasjonstjenester. I det offentlige telenettet er det særlig de IT-baserte driftsstyringssystemene som er sårbare – det er disse som sørger for den daglige driften. Angrep rettet mot disse systemene kan derfor få alvorlige samfunnsmessige konsekvenser.

Våre offentlige nett, som for eksempel mobilnett, er ikke dimensjonert slik at alle kan benytte disse samtidig. Manglende sikring av driftssystemer for mobilnett kan gi en ondsinnet aktør mulighet til enten å modifisere styringsparametre eller generere falsk trafikk. I en situasjon med unormal stor trafikk kan mobilnettene dermed bli overbelastet og brukerne vil ikke kunne benytte tjenesten. Ved å ramme mobilnettet som mange har gjort seg avhengig av, kan liv og helse gå tapt, for ikke å nevne de økonomiske konsekvenser av langvarig bortfall av kommunikasjon.

Eksempel 4

En lege som skal sende en elektronisk sykemelding til Rikstrygdeverket må ha en løsning på sitt legekontor som ivaretar informasjonssikkerheten. Rikstrygdeverket må være sikker på at det er en autorisert lege og at det er den riktige legen som sender sykemeldingen. Man må også være sikker på at informasjonen i meldingen er korrekt og ikke vært manipulert underveis. Sist, men ikke minst, må informasjonen være sikret konfidensialitet. Uten slike sikringstiltak vil elektronisk formidling av sykemeldinger verken være forsvarlig eller mulig.

Eksempel 5

En privatperson som skal sende e-post til sin advokat vedrørende en sak som behandles i rettsapparatet må sikre seg mot at uvedkommende kan oppfange informasjonen. Konfidensialiteten i det man sender via e-post må være godt nok ivaretatt. Mulighetene for å fange opp åpne (dvs. ikke kryptert) e-postmeldinger er ganske store, forutsatt at man vet hvor man skal lete. Kryptering av e-postmeldingene fra privatpersoner kan motvirke dette.

Når vi mottar et elektronisk dokument tilsendt fra et offentlig organ, ønsker vi å være sikker på at dokumentet kommer fra den rette instans og at det ikke er tuklet med underveis. Dette kan ivaretas ved at det offentlige organet bruker elektronisk signatur. Det må være enkelt for privatpersoner å sjekke at slik signatur er påført dokumentet og at den er korrekt.

Eksempel 6

Når man benytter nettbank på en hjemme-PC som f.eks. tenåringer bruker til å kommunisere på nettet, bør man være klar over hvilke trusler informasjonen lagret i PCen kan utsettes for. Har PCen bredbåndstilknytning til Internett kan den stå "vidåpen" for angrep utenfra dersom man ikke abonnerer på en brannmurtjeneste. Samme PC vil også kunne brukes til å angripe andre brukere av nettet, uten at eieren er klar over det. Slike angrep kan i verste fall føre til at hele nettet blir ustabilt og utilgjengelig i perioder. Virus fra disketter eller andre lagringsmedier kan også skade informasjonen som er lagret på PCen og skade dens evne til å fungere. Derfor er det viktig også for privatbrukere å ha gode rutiner for adgang til PCen, det vil si adskilte brukerområder, kontroll av lagringsmedier, kontroll av nettilgang osv.

4 Informasjonssikkerhet - et samfunnsanliggende

Informasjonssamfunnet

Informasjonssamfunnet kjennetegnes ved at alle nå har mulighet til å formidle store mengder informasjon hurtig, over store avstander og til en lav kostnad. Samtidig er tilgangen til opplysninger, fakta og viten blitt enorm. Informasjonssystemer, nettverk og tjenester smelter sammen. Omfanget av elektronisk forretningsdrift og tilbudet av elektroniske tjenester øker raskt og til nå har vi bare sett starten på denne utviklingen. Likevel kan det slås fast at bruk av informasjonsteknologien alt nå gjennomsyrer de fleste samfunnsaktiviteter.

Et utvidet risikobilde

Informasjonsteknologien har gjort samfunnet sårbart på nye områder. Bevisste angrep på informasjonssystemene kan ha ulike former, som ulovlig adgang, spredning av virus og tjenestenekting. Angrepene kan gjennomføres når som helst, mot hvem som helst og fra hvor som helst. Samfunnet står med andre ord overfor nye sikkerhetspolitiske utfordringer bl.a. ved at enkeltstater eller grupper kan gjennomføre koordinerte IT-angrep og lamme samfunnskritiske funksjoner. I tillegg til bevisste angrep kan sårbarheten knyttes til hendelige uhell – som følge av slurv eller uvitenhet. Sårbarhet i forhold til naturpåkjenninger, som f.eks. flom og lynnedslag, påvirker også det totale risikobildet.

Ustabilitet i informasjonssystemene kan forstyrre oppnåelsen av viktige samfunnsmål og ivaretakelsen av personlig frihet. Dette kan også svekke tillit og tiltro til IT som grunnlag for ny forretningsvirksomhet.

Informasjonssamfunnets særskilte utfordringer innen informasjonssikkerhet er:

Identifisering av kritisk IT-infrastruktur

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. En særlig utfordring vil være å identifisere og sikre samfunnskritisk IT-infrastruktur.

Sikring av kritisk IT-infrastruktur

Virksomheters sikkerhetstiltak bør være dimensjonert etter en vurdering av den aktuelle risiko. Det er imidlertid en utfordring å komme frem til felles og helhetlige kriterier for sikring av samfunnskritiske funksjoner bl. a. fordi de er så forskjellige. En grunnleggende fellessikring vil gi mulighet for å styrke nasjonale, regionale eller lokale tiltak i situasjoner hvor risikoen bedømmes å være særlig høy. Sikringen bør omfatte fysiske, logiske, elektroniske og administrative tiltak som utgjør nødvendige barrierer og samtidig fungerer som deteksjons- og reaksjonstiltak. Det vil være utfordrende å utvikle passende standarder for å skape tilstrekkelig sikkerhet og robusthet. Slike standarder bør imidlertid tas i bruk hvis målet om robusthet skal oppnås.

Sikker overføring av informasjon

For å bidra til større tillit og trygghet i forbindelse med elektronisk samhandling anbefales utstrakt bruk av krypto, bl. a. til sikring av forretningstransaksjoner og personlig kommunikasjon. Når enkeltindivider og virksomheter sikrer informasjon mot innsyn kan dette imidlertid skape problemer for politiets etterforskning av alvorlig kriminalitet og terrorisme. Slike hensyn må balanseres mot hverandre.

Utvikling av regelverket

Lover, forskrifter og instrukser for informasjonssikkerhet er utviklet over tid og med utgangspunkt i forskjellige behov. Mange virksomheter må forholde seg til flere regelverk, gitt at virksomhetens systemer behandler forskjellige typer informasjon. Det er viktig å utvikle regelverk som ivaretar variasjonen i de sikkerhetsmessige behov, hensynet til personlig frihet og hensynet til enklest mulig etterlevelse og revisjon.

Virksomhetenes fokus på sikkerhet

Det er ledelsen som har hovedansvaret for å sikre virksomheters verdier, enten det er på vegne av samfunnet eller på vegne av virksomheten selv. De ansatte må gjøres oppmerksom på at sikkerhetsbrudd kan påføre vesentlig økonomisk skade. I større virksomheter vil det være formålstjenlig med en egen sikkerhetsorganisasjon og det er en ledelsesoppgave å sette av nødvendige ressurser til sikkerhetsarbeid. I virksomheter uten egen sikkerhetsorganisasjon må ledelsen sørge for å ha nødvendige forutsetninger for å kjøpe ekstern kompetanse, og for å vurdere konsekvensen av å sette bort IT-baserte tjenester. For å få et realistisk bilde av sikkerhetstilstanden er det viktig med en god rolleavklaring mellom dem som utøver sikkerhet og dem som reviderer utøvelsen. Gjennomføring av tiltak i næringslivet vil baseres på en dialog med myndighetene og bransjeorganisasjonene. God IT-sikkerhet er også en forsikring mot mulige store tap.

Skillet mellom arbeid og private aktiviteter

Økt bruk av bærbare PC'er, mobiltelefoner og PDA'er som er oppkoblet til Internett er med på å utviske skillet mellom arbeidsrelatert og privat bruk av IT. Bredbåndsteknologien gjør at utstyr er oppkoblet til nettet konstant. Det blir stadig enklere å utveksle og synkronisere data mellom bærbare og stasjonære enheter. Dette stiller oss overfor utfordringer knyttet til ukontrollert overføring av informasjon, og sårbarhet i forhold til angrep.

Sikkerhetskultur i samfunnet

Det må etableres en sikkerhetskultur knyttet til bruk av IT hos viktige samfunnsaktører, i virksomhetene og blant folk flest. Mange brukere er uvitende om hvilken risiko man utsetter seg for ved bruk av informasjonsnettverk, eller hvilke løsninger som allerede tilbys for å unngå mulige trusler. Dermed blir det vanskelig for den enkelte å vurdere risikoen. Det er derfor behov for både økt bevissthet og kompetanse hos brukere. Etisk fremferd har også betydning for en god og trygg utnyttelse av

teknologien. Bruk av Internett stiller nye krav til etisk forsvarlig adferd, både hos tjenestetilbyderne og brukerne.

Elektronisk signatur og autentisering av kommunikasjonspartnere

For å oppnå store effektiviseringsgevinster ved bruk av IT er det viktig at elektronisk dokumentbehandling og kommunikasjon gjøres like sikker som samhandling ved hjelp av papirdokumenter. Det er nødvendig med en effektiv og pålitelig infrastruktur som gir elektronisk samhandling samme faktiske, kulturelle og juridiske trygghet som den papirbaserte. Infrastrukturen må være tilrettelagt slik at det er mulig å skape tillit mellom to parter som ikke kjenner hverandre, og slik at informasjonen kan beskyttes mot forfalskning eller andre angrep.

Kost-nytte vurderinger av IT-sikkerhet

Skjerpet myndighetsfokus på IT-sikkerhet kan bety økte kostnader for ulike aktører i samfunnet. Implementering av sikkerhetstiltak må baseres på en avveining mellom risiko og kostnader knyttet til gjennomføring. Konsekvenser og skadevirkninger ved ikke å foreta seg noe bør bli vurdert. Før evt. tiltak blir pålagt skal konsekvenser for næringslivet utredes.

Alle virksomheter bør frivillig gjøre egne avveininger mellom risikobildet, sikkerhetstiltak, kostnader og eventuelle ulemper slike tiltak kan medføre. Risikoeksponering ved manglende sikring bør være klarlagt og inkludert i virksomhetens budsjetter og regnskap.

Myndigheter og regelverk for IT-sikkerhet

Dette kapitlet gir en oversikt over sentrale myndigheter med ansvar for regelverk som berører IT-sikkerhet. Fremstillingen tar utgangspunkt i følgende viktige forhold som må ses i sammenheng:
rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser,
sikkerhet for kritiske samfunnsfunksjoner,
alminnelig IT-sikkerhet, som ikke dekkes av punktene overfor.

Når det gjelder rikets sikkerhet skal informasjonen beskyttes mot uvedkommendes innsyn gjennom sikkerhetsgradering og tilhørende tiltak. Selv om dette sannsynligvis bare omfatter noen ganske få prosent av den totale informasjonsmengden, er verdien av slik informasjon svært stor. Kritiske samfunnsfunksjoner omfatter sannsynligvis også en begrenset andel av den totale informasjonsmengden. Alminnelig sikkerhet som gjelder offentlige og private virksomheter samt alle husstander, omfatter en svært betydelig andel av all informasjon, informasjonsbehandling, og IT-utstyr som finnes i samfunnet.

Når det gjelder rikets sikkerhet er ansvaret klart fordelt på myndigheter, og er nedfelt i et regelverk med klar tilnærming for å møte antatt store trusler. Når det gjelder kritiske samfunnsfunksjoner er bildet noe mindre klart, med flere enkeltsektorers myndigheter og regelverk involvert. Innen området alminnelig sikkerhet finnes ingen helhetlig regulering når det gjelder IT-sikkerhet. Trusselbildet, konsekvenser av sikkerhetsbrudd og oppfatninger av akseptabel risiko er ulike på de tre områdene.

Rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser

Sikkerhetsloven med tilhørende forskrifter gir regler for håndtering av sikkerhetsgradert informasjon og –objekter. Loven retter seg mot trusler i form av spionasje, sabotasje og terrorhandlinger, som kan true rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Loven foreskriver sikkerhetstiltak som skal fjerne eller redusere sårbarhet i forhold til de nevnte truslene. Forsvardepartementet har forvaltningsansvaret for sikkerhetsloven. Loven gjelder for stat og kommune, og andre definerte virksomheter. Den enkelte sektormyndighet har det løpende ansvaret for forebyggende sikkerhet.

Direktoratet Nasjonal sikkerhetsmyndighet (NSM) ble opprettet 1.1. 2003, med fag- og tilsynsoppgaver hovedsakelig forankret i sikkerhetsloven med forskrifter. NSM er administrativt underlagt Forsvarsdepartementet, med faglig rapportering til Justisdepartementet når det gjelder sivil sektor og til Forsvarsdepartementet når det gjelder militær sektor.

Sikkerhet for kritiske samfunnsfunksjoner

Samfunnssikkerhet er den evnen samfunnet har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og andre grunnleggende behov under ulike former for påkjenninger. Tabellen gir en

oversikt over noen av de kritiske samfunnsfunksjoner der sikkerhet i underliggende IT-systemer vil ha betydning for samfunnssikkerhet.

Justisdepartementet har samordnings- og oppfølgingsansvaret når det gjelder samfunnssikkerhet og beredskap i sivil sektor. Formålet er å sikre god kvalitet på planleggingen og en effektiv bruk av ressursene. Alvorlige beredskaps- og sikkerhetsutfordringer skal gjenspeiles i tiltak som planlegges iverksatt ved kriser. Dette gjelder også tiltak som iverksettes ved svikt i samfunnskritiske IT-systemer og —infrastruktur.

Tabell 1
Ansvar for kritisk infrastruktur

Samfunnsmessig funksjon	*Koordinere oppfølgingen av krav til IT-systemet*	*Definere krav til IT-systemer, følge opp*	*Implementere krav i aktuelle IT-systemet*
Telenettet	Samferdselsdep.	Post- og teletilsynet	teleselskapene
Finans	Finansdepartementet	Norges Bank, Kredittilsynet	Norges Bank, driftssentraler
Energi og vassdrag	Olje- og enrgidep.	Norges vassdrag- og energidirektorat	energiselskapene
Vannforsyning og avløp	Kommunal- og regiondep. Helsedep.	Kommunale vann- og avløpsverk	kommuner, vannverk
Olje- og gass	Olje- og enrgidep. Arbeids- og admin. departementet	Oljedirektoratet/ Petroleumstilsynet	oljeselskaper
Flytransport	Samferdselsdep.	Luftfartstilsynet	Avinor AS, flyplasser
Jernbanetransport	Samferdselsdep.	Jernbanetilsynet	NSB/Jernbaneverket
Sjøtransport	Fiskeridep. Nærings- og handelsdep.	Kystdirektoratet Sjøfartsdirektoratet	Kystdirektoratet Sjøfartsdirektoratet
Vegtransport	Samferdselsdep.	Vegdirektoratet	Vegvesenet (regionalt)
Helse og liv	Helsedep., Sosialdep.	Sosial- og helsedir.	Helseforetak, private helseinstitusjoner
Sentraladministrasjonen[2]	Arbeids- og administrasjonsdep.	Departementene, Forvaltningstjenesten,	Forvaltningstjenesten departementer
Nødtjenester	Justisdepartementet (samordner) Helsedep, Arbeids- og administrasjonsdep.	Politidirektoratet, Sosial- og helsedir. Dir. for samfunnssikkerhet og beredskap	Kommuner, mfl
Forsvaret	Forsvarsdepartem.	Forsvarsdepartem. Forsvarets sikkerhetsavdeling	Forsvarets militære organisasjon, Forsvarsbygg, FFI

Direktoratet for samfunnssikkerhet og beredskap (DSB) skal bistå Justisdepartementet og er fagmyndighet innen kriseberedskap på nasjonalt, regionalt og lokalt nivå. DSB arbeider med samfunnssikkerhet og beredskap i offentlig sektor, og er Sivilforsvarets sentrale ledelse.

Sivilforsvarsloven gir bestemmelser om tiltak som bedrifter må gjennomføre for å beskytte seg selv (industrivern). Tiltakene omfatter beskyttelse av personer, eiendom og produksjon, gjennom forebygging, beredskap, evne til å håndtere nødsituasjoner og evne til å komme tilbake til en normal situasjon.

Regjeringen har gått inn for å etablere et nytt direktorat for samfunnssikkerhet og beredskap fra 1.7.2003. Det skal bestå av Direktoratet for sivilt beredskap og hoveddelen av Direktoratet for brann- og elsikkerhet. Sivilforsvaret skal etableres som egen etat under det nye direktoratet.

Alminnelig IT-sikkerhet

Nærings- og handelsdepartementet har ansvaret for å koordinere nasjonal IT-politikk, herunder IT-sikkerhet. Departementets ansvar omfatter også for lov om elektronisk signatur med egen forskrift. Post- og teletilsynet har fått delegert oppgaven å håndheve forskriften.

Nærings- og handelsdepartementets koordinering av arbeidet med IT-sikkerhet omfatter:
- å identifisere og følge opp sektorovergripende spørsmål – gjennomføre eller koordinere tverrgående tiltak
- å være pådriver overfor fagdepartementene
- å delta i internasjonale organer og ivareta norske interesser der.

Nærings- og handelsdepartementet har også ansvaret for å koordinere arbeidet med IT-sikkerhet i næringslivet.

Justisdepartementet har ansvaret for forvaltningsloven, offentlighetsloven og personopplysningsloven, som bla. gir regler om taushetsplikt for visse opplysninger. Reglene om personopplysninger gjelder både i offentlig og privat sektor. IT-sikkerhet er direkte regulert for personvernet. IT-sikkerhet er ikke direkte regulert i de to andre lovene, men de omfatter regler om saksbehandling som må tas hensyn til også i forbindelse med IT-sikkerhet.

Arbeids- og administrasjonsdepartementet forvalter forskriften til personopplysningsloven og forskriften om elektronisk kommunikasjon med og i forvaltningen. Arbeids- og administrasjonsdepartementets ansvarsområde er også knyttet til tverrgående spørsmål vedrørende IT i offentlig sektor, samt IT for alle departementene. Departementet har også ansvaret for Datatilsynet og Personvernnemnda. Sammen med Helsedepartementet og Miljøverndepartementet er AAD fagmyndighet for helse- miljø- og sikkerhetsregelverket. I dette regelverket stilles det krav til sikkerhet i tilknytning til olje- og energisektoren. Spesifikke krav til IT-sikkerhet må utledes av disse generelle kravene.

Statsministerens kontor har ansvaret for statsforvaltningens beskyttelsesinstruks. Den gir regler for håndtering av opplysninger som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter. Når informasjon er beskyttelsesgradert og skal behandles elektronisk, gjelder enkelte av reglene under sikkerhetsloven med forskrifter og Nasjonal sikkerhetsmyndighet (NSM) har et tilsynsansvar for dette.

Lov om elektronisk kommunikasjon, som skal erstatte teleloven, gir hjemmel for å definere nærmere krav til IT-sikkerhet hos leverandører av kommunikasjonstjenester. Loven forvaltes av Samferdselsdepartementet. Post- og teletilsynet vil i forskrift kunne gi nærmere bestemmelser om IT-sikkerhet.

Under Nærings- og handelsdepartementet er det etablert en norsk sertifiseringsordning for IT-sikkerhet i organisasjoner, administrert av Norsk Akkreditering. Denne frivillige ordningen er basert på den britiske standarden BS 7799.

I tillegg til tverrgående lover finnes det også sektorlovgivning med relevans for IT-sikkerhet. F. eks. forvalter Finansdepartementet kredittilsynsloven. Kredittilsynet har fastsatt en forskrift om bruk av informasjonsteknologi for bank- og finanssektoren, med regler om IT-sikkerhet. På Helsedepartementets område gir helsepersonelloven omfattende regler om bl.a. taushetsplikt, elektronisk journal, mv. Reglene stiller også krav til IT-sikkerhet. Se ellers tabell 1 og vedlegg 2.

5

Både personopplysningsforskriften og forskriften om elektronisk kommunikasjon med forvaltningen legger til grunn at man skal følge anerkjente standarder eller metoder. I praksis betyr dette den nevnte standarden og dens norske motstykke.

Nasjonal sikkerhetsmyndighet er tildelt en rolle som nasjonal sertifiseringsmyndighet for frivillig sertifisering av IT-sikkerhet i produkter og systemer, gjennom en ordning som kalles SERTIT. Den er basert på en internasjonal standard, s.k. Common Criteria, og en internasjonal avtale for gjensidig aksept over landegrensene. Det er en ordning, der NSM skal betjene de behov i samfunnet som faller utenom sikkerhetslovens regulering.

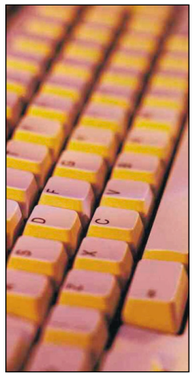
Se Vedlegg 2 for kortfattet oversikt over sentrale myndigheter og regelverk.

Tiltak

6

Hver sektor skal lage en handlingsplan for gjennomføring av tiltak for å realisere denne strategien. Gjennomføringsansvar innebærer at den oppgitte myndighet eller organisasjon vil ha en rolle i gjennomføringen av de deler av tiltaket som faller naturlig i deres fagområde. Prioriterte tiltak er:

I Kritisk IT-infrastruktur



Risiko- og sårbarhetsvurdering av samfunnskritisk IT-infrastruktur
Det skal lages et felles sett med kriterier som gjør det mulig å identifisere samfunnskritisk IT-infrastruktur og systemer og det skal utarbeides en metode for risiko- og sårbarhetsvurdering samt å gjennomføre en risiko- og sårbarhetsvurdering av slike. Sektorene skal utarbeide normer for sikring både mht. konfidensialitet, integritet og tilgjengelighet.

Gjennomføringsansvar: Justisdepartementet , Forsvarsdepartementet, Direktorat for samfunnssikkerhet og beredskap og Nasjonal sikkerhetsmyndighet når det gjelder felles metode, sektordepartementene når det gjelder sektornormer.

Prioritetsordning i telenettene
Det skal vurderes hvordan innføring av en ny prioritetsordning i telenettene skal gjennomføres. En ny prioritetsordning må omfatte alle tilbydere av offentlig telefontjeneste både i fastnett og mobilnett, og skal sikre at forhåndsdefinerte viktige abonnenter, som for eksempel nøkkelpersoner og nøkkeletater får prioritet i situasjoner der nettene eller deler av nettene er overbelastet. Det skal utarbeides krav til den nye ordningen.

Gjennomføringsansvar: Post- og teletilsynet.

Sikkerhet i offentlige telenett
Det skal foretas en samlet sikkerhetsevaluering av offentlige telenett. En slik evaluering må gjøres i samarbeid med operatørene og gjøres tilgjengelig for brukerne slik at de kan forholde seg til sikkerhetsegenskapene.

Gjennomføringsansvar: Post- og teletilsynet.

Robusthet mot feil og angrep i Internett
Utredningen om det norske Internetts robusthet mot alvorlige tekniske feil og sabotasje samt andre fysiske eller logiske anslag skal følges opp. Det bør vurderes etablering av flere nasjonale svitsjingspunkter (NIX-er) i tillegg til god sikring av de eksisterende. Eventuelle tiltak bør samordnes med europeiske og internasjonale initiativ for sikkerhet i Internett.

Gjennomføringsansvar: Samferdselsdepartementet i samarbeid med Nærings- og handelsdepartementet og NSM.

II Regelverk for IT-sikkerhet

Regelverksgjennomgang og samordnet håndheving
Det bør settes i gang et arbeid i forhold til regelverk for informasjonssikkerhet, for å få de eksisterende reglene i bedre praktisk bruk, og gi bedre grunnlag for fornyelse og forenkling av dem, inklusive spørsmålet om samordnet/enklere håndheving.
Arbeidet skal omfatte å lage en oversikt over reglene for informasjonssikkerhet, lage praktiske veiledninger, samt kurs og opplæringstiltak.

Gjennomføringsansvar: Justisdepartementet og berørte departementer.

Utvikling av regelverk som berører IT-sikkerhet
Den enkelte regelverksforvalter bør systematisk innhente opplysninger om hvordan regelverkene faktisk virker i praksis, og periodevis vurdere behovet for endringer i regelverket.

Det skal arbeides for at regelverk som berører IT-sikkerhet utvikles på en mest mulig koordinert måte, at det gis klare og konsise regler, og at det gjøres klare avgrensinger mot andre regelverk, slik at det ikke oppstår tvil om tolkningen eller om hvilke regler som gjelder i et gitt tilfelle.

Gjennomføringsansvar: aktuelle regelverksforvaltere, Justisdepartementet

Generelle offentlige IT-sikkerhetsnormer
Det skal utarbeides en generell mal for policy for IT-sikkerhet i offentlige virksomheter. I tillegg til en generell del bør malen inneholde spesifikke deler tilpasset anvendelsesområder som økonomiforvaltning, arkiv og saksbehandling, personalforvaltning samt forvaltning av systemer og infrastrukturer. Malen skal ta hensyn til relevant IT-sikkerhetsregelverk for de ulike områdene.

Gjennomføringsansvar: Arbeids- og administrasjonsdepartementet i samarbeid med relevante departementer og kommunesektoren.

Implementering av IT-sikkerhet i private virksomheter
Det skal utvikles veiledninger for hvordan IT-sikkerhet skal implementeres i systemer og iverksettes i organisasjonen.

Gjennomføringsansvar: relevante bransjeorganisasjoner og sektormyndigheter i samarbeid med Næringslivets Sikkerhetsorganisasjon

Felles IT-sikkerhetsnormer for helsesektoren
Det opprettes en sentral sikkerhet – og driftsgruppe for nasjonalt helsenett. Gruppen skal utarbeide en sikkerhetspolicy for helsenett, som innbefatter døgnkontinuerlig overvåking av nettet herunder tiltak for kriser og hurtig feilretting. Gruppen skal også delta i utarbeidelse av bransjenormer som sikrer at helsesektoren får felles forståelse for sikkerhetsmessige tiltak ifm tilknytning til helsenettet. Bransjenormen skal bidra til å sikre en omforent sikkerhetspolicy for sektoren.

Gjennomføringsansvar: Sosial – og helsedirektoratet

III Nasjonal koordinering av IT-sikkerhet

Koordinerings- og rådgivningsutvalg for IT-sikkerhet
Det skal etableres et koordineringsutvalg for IT-sikkerhet, som vil inkludere sentrale myndigheter og regelverksforvaltere på området. Utvalgets oppgave vil være å arbeide for samordnet utøvelse av tilsynsvirksomhet, hensiktsmessig samordning av videreutviklingen av IT-sikkerhetsregelverket og samordnet håndheving av IT-sikkerhetsbestemmelser for å forenkle etterlevelse hos brukere. Utvalget skal også gi råd om hensiktsmessig koordinering av IT-sikkerhet og -beredskap i samfunnet, herunder hensiktsmessige ordninger for sikring av kritisk IT-infrastruktur.
Utvalgets sekretariat bør forankres permanent i egnet departement eller direktorat.

Gjennomføringsansvar: Justisdepartementet, Forsvarsdepartementet, Nærings- og handelsdepartementet, Arbeids- og administrasjonsdepartementet.

Senter for informasjonssikring (SIS)
Forsøkprosjektet Senter for informasjonssikring skal evalueres innen utgangen av 2004 og et forslag til en evt. permanent ordning fremmes. Senterets hovedoppgaver er å fremskaffe et helhetlig bilde av truslene mot norske IKT-systemer, formidle informasjon, kompetanse og kunnskap om trusler og mottiltak samt ivareta kontakt og samarbeid med tilsvarende organisasjoner i andre land. Det skal stimuleres til at flest mulig virksomheter, offentlige som private, innrapporterer sikkerhetshendelser til senteret i forsøkperioden.

Gjennomføringsansvar: Nærings- og handelsdepartementet i samarbeid med Justisdepartementet og Forsvarsdepartementet.

Beredskap og IT-sikkerhet
Det skal vurderes om Direktoratet for samfunnssikkerhet og beredskap skal få et ansvar for å veilede og føre tilsyn med kommuner, fylkesmenn og annen virksomhet, vedrørende krav til IT-sikkerhet i forbindelse med sivil beredskap. Direktoratet skal utrede spørsmålet om hvordan IT-sikkerhet kan integreres i gjeldende planverk.

Forsvaret skal samtidig utrede hvordan IT-sikkerhet skal integreres i det militære planverket.

Gjennomføringsansvar: Justisdepartementet og Forsvarsdepartementet.

IV Risiko og sårbarhetsanalyser

Utvikling av verktøy og metoder for risiko- og sårbarhetsvurdering
Det skal stimuleres til utvikling av sikkerhetsmodeller, metoder, verktøy og mekanismer for å gjøre det mer kosteffektivt og brukervennlig å håndtere

IT-sikkerhet på en betryggende måte. Små- og mellomstore virksomheters behov bør stå særlig i fokus ved utvikling/tilpasning av aktuelle metoder.

Gjennomføringsansvar: Nærings- og handelsdepartementet i samarbeid med bransjeorganisasjoner, regelverksforvaltere og internasjonale organisasjoner.

V Klassifisering av informasjon og informasjonssystemer

Klassifisering av informasjon og systemer, sikkerhetsnormer i private virksomheter
Det bør utvikles klassifikasjonsordninger og sikkerhetsnormer for private virksomheters informasjonsbehandling med utgangspunkt i anerkjente nasjonale og internasjonale standarder.

Gjennomføringsansvar: relevante bransjeorganisasjoner og sektormyndigheter i samarbeid med Næringslivets Sikkerhetsorganisasjon.

VI Bevisstgjøring av alle aktører

Trygg informasjonstrafikk
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 og nyttige lenker til relevant tilleggsinformasjon. Tjenesten skal gi mulighet for å kunne besvare spørsmål fra publikum.

Gjennomføringsansvar: Nærings- og handelsdepartementet i samarbeid med Justisdepartementet.

Det bør gjennomføres en informasjonskampanje for å spre kjennskap til god praksis og utbre god praksis vedrørende sikkerhet for husstandenes PC-er.

Gjennomføringsansvar: Nærings- og handelsdepartementet i samarbeid med Justisdepartementet.

Undervisning i IT-sikkerhet i skoleverket
Det skal utarbeides en "undervisningspakke" for grunn- og videregående skole med vekt på IT-sikkerhet. Materialet skal kunne brukes ved undervisning i bruk av IT i skolene. På sikt bør læreplanene eksplisitt omfatte IT-sikkerhet som emne innen IT-relaterte fag.

Gjennomføringsansvar: Nærings- og handelsdepartementet i samarbeid med Utdannings- og forskningsdepartementet og Nasjonalt Læringssenter.

Kompetanse om IT-sikkerhet i virksomhetene
Det skal arbeides for at ledere i private og offentlige virksomheter tar ansvar for å sikre at virksomheten har tilstrekkelig kompetanse innen IT-sikkerhet ut fra definerte behov og at virksomheten satser på kompetansefremmende tiltak for personer i de ulike sikkerhetsrollene.

Gjennomføringsansvar: Nærings- og handelsdepartementet, Arbeids- og administrasjonsdepartementet, i samarbeid med bransjeorganisasjoner.

VII Varsling og rådgivning

Kriseteam for telesektoren
Det skal vurderes etablering av et kriseteam for teleoperatører (TERT - *Teleoperatørenes "emergency response team"*) for at disse raskt skal kunne utveksle informasjon og håndtere feilsituasjoner. Det vil i den forbindelse være viktig å få etablert et opplegg for hvem som skal kalles inn, når det skal skje og hvordan man skal håndtere kriser.

Gjennomføringsansvar: Post- og teletilsynet.

Varslingssystem for digital infrastruktur (VDI)
Prosjektet Varslingssystem for digital infrastruktur (VDI) er etablert som en permanent ordning hos Nasjonal sikkerhetsmyndighet. Ordningen omfatter analyse av trafikkmønstre på nettet for å fange opp mulige angrep og hendelser. Erfaringene fra analysene bør gjøres tilgjengelig for aktuelle samarbeidspartnere og ev. andre parter etter behov. Det skal arbeides for at gode samarbeidsformer mellom Senter for informasjonssikring, Politiets datakrimsenter og VDI etableres.

Gjennomføringsansvar: Nasjonal sikkerhetsmyndighet.

VIII Tiltak hos leverandører av IT-produkter og –tjenester

Sikker Internett-aksess
Aktørene bør følge anerkjente sikkerhetsnormer og standarder, og må synliggjøre hvilken grad av tilgjengelighet, kapasitet og driftsstabilitet som kan forventes, samt hvilken brukerhjelp som kan ytes ved feilsituasjoner. Aktørene bør kunne tilby sikkerhetstjenester av typen virusskanning, e-postfiltrering og brannmur-oppsett.

Sikkerhet i IT-tjenester
Tjenesteleverandører (ISP, ASP osv.) bør følge anerkjente sikkerhetsnormer og standarder og gjøre kjent hvilket sikkerhetsnivå tjenesten tilbyr. Der leverandørene har sertifiseringer av IT-sikkerhet, bør disse gjøres kjent for brukere.

Sikkerhet i IT-produkter
Leverandørene av IT-systemer skal opplyse hvilken sikkerhet som oppnås ved anvendelse av produktet, under gitte forutsetninger. Leverandører bør følge anerkjente sikkerhetsnormer og standarder, og tilrettelegge for enklest mulig bruk av sikkerhetsfunksjonalitet i sine systemer.

Gjennomføringsansvar: bransjeorganisasjoner (Abelia, IKT-Norge), Post- og teletilsynet, Nærings- og handelsdepartementet.

Klargjøring av ansvar for IT-sikkerhet ved bruk av utstyr som stilles til rådighet av tjenesteleverandør for andre
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. Kundene til ASP bør stimuleres til å stille krav om etterlevelse/dokumentasjon av visse minimumsstandarder, som f.eks. ISO sertifisering.

Gjennomføringsansvar: bransjeorganisasjoner (Abelia, IKT-Norge), Nærings- og handelsdepartementet.

IT-sikkerhet ved bruk av massemarked-produkter
Det skal arbeides for at produkter og systemer rettet mot massemarkedet skal ledsages av lettfattelig opplysnings- og opplæringsmateriale innen IT-sikkerhet rettet mot relevante målgrupper (bruk, drift, sikkerhetsadministrasjon).

Gjennomføringsansvar: Nærings- og handelsdepartementet, bransjeorganisasjoner (Abelia, IKT-Norge).

IX Sertifisering og standarder

Sertifisering av IT-sikkerhet
Etablerte sertifiseringsordninger for IT-sikkerhets implementering i organisasjoner (BS7799-ordningen under Norsk Akkreditering) og for IT-sikkerhet i produkter og systemer (SERTIT i Nasjonal sikkerhetsmyndighet) bør tas bredere i bruk av norske virksomheter.

Gjennomføringsansvar: Norsk Akkredittering, Nasjonal sikkerhetsmyndighet, Nærings- og handelsdepartementet.

Bruk og utvikling av standarder for IT-sikkerhet
Etablerte standarder for IT-sikkerhet bør tas i bruk i offentlige og private IT-anskaffelser, både når det gjelder kjøp av produkter, tjenester og utviklingsoppdrag.

Norsk deltakelse i standardiseringsarbeid innen IT-sikkerhet bør styrkes. Informasjon om standarder og deres anvendelsesområder skal styrkes.

Gjennomføringsansvar: Nærings- og handelsdepartementet og Arbeids- og administrasjonsdepartementet, i samarbeid med Norsk Teknologisenter, bransjeorganisasjoner og aktører i markedet.

X Forskning, kompetanse og utdanning

Forskning og utvikling innen IT-sikkerhet
Det er iverksatt et flerårig forskningsprogram innen IT-sikkerhet. Et slikt strategisk program skal dekke både de organisatoriske, bruksmessige og –tekniske sider ved IT-sikkerhet. Det er viktig at privat næringsliv deltar i forskningsinnsatsen. Det skal utdannes doktorgradskandidater i programmet.

Gjennomføringsansvar: Norges Forskningsråd, Nærings- og handelsdepartementet, Justisdepartementet, Forsvarsdepartementet.

Det skal igangsettes et forskningsprosjekt som skal gi anbefalinger om tiltak for å sikre samfunnskritiske IT-infrastruktur og –systemer. Dette prosjektet vil igangsettes som et ledd i videreføringen av forskningsserien "Beskyttelse av samfunnet" (BAS).

Gjennomføringsansvar: Direktorat for samfunnssikkerhet og beredskap, Nasjonal sikkerhetsmyndighet, Justisdepartementet, Forsvarsdepartementet, Nærings- og handelsdepartementet.

Undervisning i IT-sikkerhet ved universiteter og høgskoler
Utdanninger der bruk av IT er en integrert del bør styrkes ved å utvide denne delen med undervisning i IT-sikkerhet. Dette gjelder særlig utdanninger der sikkerhet er et vesentlig emne. Det bør utarbeides læreplaner og materiell til støtte for slik undervisning.

Gjennomføringsansvar: Utdannings- og forskningsdepartementet, Nærings- og handelsdepartementet.

Nasjonale studier i IT-sikkerhet på mastergradsnivå
Det skal etableres flere høyere utdanninger innen IT-sikkerhet på mastergradsnivå med godkjenning i norske institusjoner for høyere utdanning.

Gjennomføringsansvar: Utdannings- og forskningsdepartementet, i samarbeid med Forsvarsdepartementet, Justisdepartementet, Nærings- og handelsdepartementet, Samferdselsdepartementet, Finansdepartementet.

XI Elektronisk signatur/PKI

Samordning av PKI i offentlig sektor
Det er besluttet opprettet et organ under Arbeids- og administrasjonsdepartementet, med hjemmel i forskrift om elektronisk kommunikasjon med og i forvaltningen (§ 28), for å samordne innføring og bruk av elektronisk signatur og PKI i offentlig sektor for behandling av ikke-gradert informasjon. Organet skal:

a. *Systematisere erfaringer*, støtte etater som går foran i utviklingen og iverksette nødvendige konsekvensanalyser
b. *Kategorisere IKT-løsninger i forvaltningen etter deres behov for elektronisk signatur*, og ut fra det *fastslå noen få, felles sikkerhetsnivåer* for slike løsninger. Arbeidet innebærer å vurdere de ulike tjenestenes krav og forutsetninger og å foreslå felles løsninger som favner om flest mulig tjenester.
c. *Utvikle felles krav og retningslinjer for bruk av PKI i offentlig sektor*. Kravene skal baseres på etablerte markedsstandarder og ta hensyn til gjeldende reguleringer på området. Videre skal kravene ivareta nødvendig hensyn til samhandling med andre land. Organet skal også vurdere løsninger som er tilgjengelige i markedet opp mot felleskravene, for å fastlå egnethet til bruk i offentlig sektor.
d. *Etablere nødvendige samarbeidsfora* for offentlige etater både i stat og kommunesektoren, og stimulere til samordning av forskjellige prosjekter som pågår i offentlig sektor.
e. *Etablere eller delta i egnet arena for dialog med markedsaktørene* som tilbyr løsninger for autentisering og elektronisk signatur, jf bl.a. PKI-forum organisert av Nærings- og handelsdepartementet.

f. Vurdere bruk av felles kravspesifikasjoner, for eksempel i standardavtaler, for å fremme den ønskede utvikling på området, særlig når det gjelder behovet for åpne løsninger, gjenbruk og effektiv implementering av PKI.

Gjennomføringsansvar: Arbeids- og administrasjonsdepartementet i samarbeid med departementene som er representert i samordningsorganet.

Utvikling og gjenbruk av PKI-løsninger
Det bør prioriteres prosjekter som vil ta i bruk PKI-løsninger basert på felles krav, eller som vil gjenbruke eksisterende løsninger.
Samarbeidsprosjekter bør også vurderes mellom offentlige og private leverandører av elektroniske tjenester der deltakerne kan utvikle flere typer tjenester basert på felles PKI-løsninger, eksempelvis ved FoU-kontrakter eller OPS (offentlig- privat samarbeid).

Gjennomføringsansvar: Arbeids- og administrasjonsdepartementet i samarbeid med Nærings- og handelsdepartementet.

Funksjonelle krav til en samfunnsinfrastruktur for elektronisk signatur
Leverandører av PKI-tjenester bør i felleskap utforme funksjonelle krav til samfunnsinfrastrukturen, med utgangspunkt i behovene identifisert hos leverandører av elektroniske tjenester og hos forbrukerne.

Gjennomføringsansvar: aktuelle leverandører av PKI-tjenester, Nærings- og handelsdepartementet.

Sikkerhetsnivåene for kvalifisert sertifikat og kvalifisert signatur
Sikkerhetsnivåene for kvalifisert sertifikat og kvalifisert signatur skal spesifiseres, nødvendige tekniske forutsetninger skal defineres, standarder og profiler som grunnlag for felles fremstøt mot leverandører av lokale PKI-systemer og bruker utstyr skal avklares.

Gjennomføringsansvar: Nærings- og handelsdepartementet i samarbeid med aktuelle leverandører av PKI-tjenester.

Krav til testmiljø for samtrafikk
Leverandører av PKI-tjenester skal i felleskap utforme krav til testmiljø for samtrafikk dem imellom.

Gjennomføringsansvar: aktuelle leverandører av PKI-tjenester, Nærings- og handelsdepartementet.

Informasjons- og bevisstgjøringskampanjer
Det bør gjennomføres informasjons- og bevisstgjøringskampanjer mot forbrukerne og mot eksisterende/potensielle leverandører av elektroniske tjenester mhp å ta i bruk samfunnsinfrastrukturen.

Gjennomføringsansvar: aktuelle leverandører av PKI-tjenester, Nærings- og handelsdepartementet.

XII Internasjonalt samarbeid

Internasjonale møter om IT-sikkerhet til Norge og norsk deltakelse internasjonalt.
Det skal arbeides for at internasjonale fora som arbeider med IT-sikkerhet legger sine møter til Norge, slik at flest mulig norske aktører kan dra nytte av internasjonale samarbeidsarenaer. Norsk deltakelse i relevante standardiserings- og erfaringsutvekslingsfora bør prioriteres.

Gjennomføringsansvar: alle departementer, næringslivets organisasjoner, standardiseringsorganisasjoner.

Deltagelse i EUs organ for nettverks- og informasjonssikkerhet
Norge vil arbeide for å delta i organet for nettverks- og informasjonssikkerhet som planlegges etablert i EU.

Gjennomføringsansvar: Nærings- og handelsdepartementet, Samferdselsdepartementet, Utenriksdepartementet.

Vedlegg 1
Aktuelle begreper

Infrastruktur
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 en strategi for IT-sikkerhet vil en infrastruktur omfatte datamaskiner, programvare, nettverk, lokaler, omgivelser og spesielle forhold som inngår i utvikling, forvaltning og drift av IT-systemene.

Samfunnskritisk
Et informasjonssystem eller en infrastruktur er samfunnskritisk hvis samfunnets funksjonsevne i stor grad påvirkes av at systemet eller infrastrukturen ikke fungerer.

Virksomhetskritisk
Et informasjonssystem eller en infrastruktur er virksomhetskritisk hvis virksomhetens funksjonsevne i stor grad påvirkes av at systemet eller infrastrukturen ikke fungerer.

Kritisk for individet
Et informasjonssystem eller en infrastruktur kan også være kritisk for det enkelte individ.

Kritikalitet
Kritikalitet kan beskrives ved en skala som indikerer relativ viktighet av informasjonen eller informasjonssystemet i en virksomhet, basert på hvor stor skade som kan oppstå ved brudd på konfidensialitet, integritet eller tilgjengelighet.

Risiko og risikonivå
Risiko beskriver fare for tap og usikkert eller uberegnelig utfall av at en trussel materialiseres. I forbindelse med IT-sikkerhet er risiko en funksjon av sannsynligheten for at en sikkerhetshendelse vil inntreffe og den forventede skadevirkningen hendelsen kan medføre.

Akseptabel risiko
Akseptabel risiko er det risikonivået som er akseptabelt for samfunnet, en virksomhet eller et individ. Akseptabel risiko kan uttrykkes kvantitativt ved å sette en målestokk på de elementer som inngår i en risikovurdering, eller det kan uttykkes kvalitativt.

Sårbarhet
Sårbarheten til et system er et uttrykk for de svakheter og mangler som finnes i systemet og spesielle omstendigheter som øker sannsynligheten for at trusler vil materialisere seg i en sikkerhetshendelse (eksempler på spesielle omstendigheter kan være størrelse, kompleksitet, at mange aktører er involvert, geografisk spredning, hyppige endringer og utsatt beliggenhet).

Robusthet
Robustheten til et system er dets evne til å tåle påkjenninger (mestre trusler og sikkerhetshendelser).

Trussel og trusselnivå
En trussel er en handling eller hendelse som kan fremkalle frykt, føre til tap eller skade. I forbindelse med IT-sikkerhet er trusler ulike situasjoner som kan føre til at konfidensialitet, integritet og tilgjengelighet blir kompromittert.

Trusselnivå indikerer sannsynligheten for at trusler skal materialisere seg, og kan anslås på bakgrunn av historikk om hendelser eller vurdering av risikobildet.

Skadeomfang/skadevirkning
Skadevirkning er et verdianslag eller en målestokk som indikerer hvilken betydning eller hvilke tap som oppstår ved brudd på konfidensialitet, integritet eller tilgjengelighet.

IT-sikkerhetshendelse
En IT-sikkerhetshendelse, eller en serie av hendelser, beskriver at det har oppstått en situasjon hvor konfidensialitet, integritet eller tilgjengelighet er kompromittert.

Reviderbarhet og sporbarhet.
Reviderbarhet angår evnen til å avdekke hendelser og handlinger og knytte disse til bestemte subjekter. Sporbarhet oppnås for eksempel ved å anvende logging, som dokumenterer handlinger og hendelser og bidrar til at handlinger og hendelser lar seg rekonstruere i ettertid. For å sikre *integritet*, må reviderbarhet og sporbarhet ivaretas.

Ikke-benekting (vedkjenning)
Sikkerhet for at den som har sendt eller mottatt informasjon gjennom elektronisk meldingsformidling ikke kan nekte for dette i ettertid.

Sikkerhetsstandarder
En standard spesifikasjon (dokument) som er vedtatt av et anerkjent standardiseringsorgan eller offentlig publisert av en sammenslutning av markedsaktører, til gjentatt eller permanent bruk, herunder:

BS 7799 British Standard for Information Security Management
Består av to deler. Del 1 omhandler generell sikkerhetspraksis. Del 2 omhandler konkrete sikkerhetsprosedyrer. Den norske sertifiseringsordningen av IT-sikkerhet i organisasjoner utsteder sertifikater etter evaluering gjennomført etter BS7799 Del 2.

ISO/IEC 17799:2000 (Internasjonal versjon av BS 7799 del 1)
Standard (beste praksis) for håndtering av informasjonssikkerhet i virksomheter. I 2001 ble standarden "NS-ISO/IEC 17799 Informasjonsteknologi. Administrasjon av informasjonssikkerhet" utgitt på norsk. Denne bygger på den britiske standarden BS 7799-1. BS 7799-2 er ennå ikke utgitt som norsk eller internasjonal standard.

[1] Med en trussel menes f. eks. en hacker, en terrorist, en uoppdaget konstruksjonsfeil, feilaktig bruk, overbelastning, naturkatastrofe el.l.
[2] Departementene

v1

Common Criteria
Common Criteria for Information Technology Security Evaluation (CC), nedfelt i
ISO/IEC 15408:1999 del 1-3 for evaluering av IT-sikkerhet i systemer og produkter.

Skadelige koder (virus)
En type logisk angrep på komponenter som utgjør IT-systemer og som kan skape store problemer for systemeier. Virus er kodesegmenter som duplis-erer seg selv ved å knytte seg opp mot datafiler. Angrepet materialiserer seg når man benytter seg av den infiserte filen.

Tjenestenekting ("denial of service")
Angrep mot et nettsted i form av forespørsler for å gjøre det vanskelig for andre brukere å oppnå kontakt med tjenesten som ønskes rammet. I ver-ste fall kan dette føre til at det angrepne nettstedets servere vil bryte sam-men. Slike angrep kan innebære bruk av flere kraftige datamaskiner sam-tidig.

CERT
CERT - Computer Emergency Response Team. Ekspertteam som håndterer IT-sikkerhetshendelser. CERT er et registrert varemerke for Carnegie Mellon University. Mange benytter derfor forkortelsen C(S)IRT - Computer (Security) Incident Response Team.

Vedlegg 2

Oversikt over noen sentrale regelverksfor-valtere innen informasjonssikkerhet

v2

Myndighet	Aktuelt lov-/regelverk
Forsvarsdepartementet/Nasjonal sikkerhetsmyndighet	Sikkerhetsloven med forskrifter, beskyttelsesinstruksen (IT-delen)
Samferdselsdepartementet / Post og teletilsynet	Teleloven (Lov om elektronisk kommunikasjon) med forskrifter
Nærings- og handelsdepartementet	Lov om elektronisk signatur, forskrift om krav til utsteder av kvalifiserte sertifikater mv
Datatilsynet	Tilsyn i forhold til person-opplysningsloven med forskrifter
Arbeids- og administrasjonsdepartementet	Forskrift til personopplysnings loven, forskrift om elektronisk kom-munikasjon med og i forvaltningen
Statsministerens kontor	Beskyttelsesinstruksen (kgl. res. av 17.3.72, endret 29.6.01)
Justisdepartementet	Personopplysningsloven, forvaltningsloven og offentlighets-loven, flere kongelige resolusjoner
Direktoratet for samfunnssikkerhet og beredskap	Sivilforsvarsloven, kgl. res. av 24.3.73, av 16.9.94, og av 3.11.00, flere andre lover
Kredittilsynet	Kredittilsynsloven/IT-forskriften
Norges Bank	Sentralbankloven
Økokrim (Politiets datakrimsenter)	Straffeloven, Straffeprosessloven
Politiets sikkerhetstjeneste	Politiloven (§17a,b,c)
Forsvarets Overkommando / Etterretningsstaben	Lov om Etterretningstjenesten
Næringslivets sikkerhetsorganisasjon	Sivilforsvarsloven, HMS-forskrifter
Sosial- og helsedirektoratet	Helsepersonelloven
Rikstrygdeverket	Folketrygdloven (§25)

Utgitt av:
Nærings- og handelsdepartementet
Postboks 8014 Dep
0030 Oslo
www.enorge.org

Flere eksemplarer kan bestilles fra Nærings-
og handelsdepartementet
Telefon: 22 24 03 01
Telefaks: 22 24 03 15
E-post: enorge@enorge.org

Publikasjonsnummer K-0668 B

Trykk og design: Konsis Grafisk AS