Informationssäkerhetspolitik

Organisatoriska konsekvenser

Slutbetänkande av InfoSäkutredningen

Stockholm 2005

STATENS OFFENTLIGA UTREDNINGAR

SOU 2005:71

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer på uppdrag av Regeringskansliets förvaltningsavdelning.

Beställningsadress:
Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-690 91 91
Ordertel: 08-690 91 90
E-post: order.fritzes@nj.se
Internet: www.fritzes.se

Svara på remiss. Hur och varför. Statsrådsberedningen, 2003.
– En liten broschyr som underlättar arbetet för den som skall svara på remiss.

Broschyren är gratis och kan laddas ner eller beställas på
http://www.regeringen.se/remiss

Tryckt av Edita Västra Aros AB
Stockholm 2005

ISBN 91-38-22412-7
ISSN 0375-250X

Missiv

Till statsrådet och chefen för Försvarsdepartementet

Genom beslut den 11 juli 2002 (dir. 2002:103) bemyndigade regeringen chefen för Försvarsdepartementet att tillkalla en särskild utredare med uppdrag att bedöma behovet av signalskydd i samhällsviktig verksamhet samt att lämna förslag till organisatorisk placering, lokalisering, uppgifter, ledning och samordning av signalskyddstjänsten. Med stöd av regeringens bemyndigande kallade chefen för Försvarsdepartementet f.d. riksdagsledamoten Anders Svärd till särskild utredare (regeringsbeslut 2002:1743/CIV, protokoll Fö 2002:1744/EPS).

Utredningen antog namnet InfoSäkutredningen.

En delrapport om signalskydd lämnades till regeringen den 28 februari 2003 (SOU 2003:27).

Utredningens uppdrag utökades genom tilläggsdirektiv beslutade den 20 februari 2003 (2003:29). Den särskilde utredaren fick utöver det ursprungliga uppdraget i uppgift att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas, hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden samt hur OECD:s riktlinjer om nät- och informationssäkerhet kan genomföras i Sverige. Utredaren fick dessutom i uppdrag att följa myndigheternas uppbyggnad av de verksamheter som regeringen aviserade i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158), angående informationssäkerheten i samhället.

Delrapporten Informationssäkerhet i Sverige och internationellt – en översikt, lämnades till regeringen den 1 april 2004 (SOU 2004:32).

Enligt tilläggsdirektiv beslutade den 7 april 2004 (2004:46) skall utredningen genomföra den utvärdering som regeringen anmälde till riksdagen i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s.105) avseende de bedömningar när det gäller uppgiftsfördelningen som regeringen gjorde inom informationssäkerhetsområdet.

Delrapporten Säker information – Förslag till informationssäkerhetspolitik SOU 2005:42, överlämnades till regeringen den 13 maj 2005.

Genom tilläggsdirektiv 2005:53, beslutat den 28 april, förlängs utredningens arbete. De organisatoriska aspekterna av utredningens förslag, skall lämnas till regeringen den 9 september 2005. I detta slutbetänkande återkommer utredningen även till ekonomiska konsekvenser av de förslag som läggs.

Kansliråd Ulf Johansson, departementssekreterare Julia Mikaelsson (entledigad den 9 augusti 2005), ämnessakkunnig Richard Oehme (entledigad 9 augusti 2005) samt kansliråd Fredrik Sand har varit sakkunniga i utredningen. Experter har varit avdelningschef John Daniels (entledigad den 9 augusti 2005), överstelöjtnant Håkan Gustafsson, verksamhetscontroller Torbjörn Gustavsson (förordnad den 9 augusti 2005), kriminalkommissarie Patrik Håkansson, avdelningschef Anders Johanson, säkerhetschef Bo Karlsson, enhetschef Staffan Karlsson, Brigadgeneral Stefan Kristiansson (förordnad den 9 augusti 2005), chefsjurist Elisabeth Lager, avdelningsdirektör Anna Larsson (entledigad den 9 augusti 2005), IT-strateg Anders Nordh, överingenjör Mats Ohlin, avdelningsdirektör Anna-Karin Waldton samt avdelningsdirektör Wiggo Öberg. Nils-Gunnar Forsberg var adjungerad till utredningen.

I det fortsatta arbetet har analytiker Josefin Grennert, departementsråd Michael Mohr (entledigad den 9 augusti 2005) och Jur. kand. Katinka Persson (förordnad den 15 maj 2005) fungerat som sekreterare. Konsult Bo Riddarström på BRi Konsult AB, har fungerat som resursperson för utredningen.

Arbetssätt och förankring

Utredningen har haft fortsatt god kontakt med berörda aktörer genom sin stora expertgrupp. Utredningen har också sammanträffat med representanter för näringslivet vid flera tillfällen. För utredningens organisatoriska överväganden samt

olika typer av konsekvenser härav, har f.d. statssekreterare Åke Pettersson varit utredningen behjälplig.

Avgränsning och ambition med slutbetänkandet

I utredningens tredje delbetänkande, SOU 2005:42 lades grunden för organisatoriska förslag. Betänkandet utgjordes av utredningens förslag till principer för utveckling av informationssäkerheten. Förslagen baserades på identifierade behov på området, till exempel av författningsstöd, kompetensutveckling och samordning.

I slutbetänkandet avger utredningen förslag till organisatoriska förändringar i enlighet med den i SOU 2005:42 formulerade målstrukturen.

Utredningens experter Stefan Kristiansson och Håkan Gustafsson har tillsammans avgett ett särskilt yttrande.

Stockholm i september, 2005

Anders Svärd

/Josefin Grennert

Katinka Persson

Innehåll

Sammanfattning

Säker information vid rätt tillfälle är en förutsättning för tillväxt, konkurrens, utveckling, välfärd och trygghet i samhället. Det gäller alla – medborgare, företag och offentlig verksamhet.

Sverige innehar en framstående ställning internationellt i fråga om användning av ny teknik och redan genomförda investeringar i människor, kompetens och teknik utgör en stor potential för framtiden.

Informations- och kommunikationstekniken har möjliggjort en explosionsartad utveckling inom informationsförsörjningen. Med ny teknik, där uppgifter och information bearbetas, lagras och förmedlas elektroniskt, följer dock inte bara ökade möjligheter, utan också problem i form av nya sårbarheter och beroenden. IT-utvecklingen har visat sig vara snabbare än förmågan att utveckla adekvat säkerhetstänkande.

Frågor kring sårbarheten berör ett mycket stort antal aktörer och intressen, och området präglas av stor dynamik. Det är svårare att värna säkerheten i moderna informationssystem, där informationen lagras, bearbetas och förmedlas elektroniskt än när informationen föreligger i fysisk form. Till detta måste läggas att bilden av dagens brister och hot är mycket komplex och därmed även behovsbilden.

Enligt utredningen är det viktigt att inse att det inte finns någon definitiv lösning på problemet med informationssäkerhet. Utredningen framhåller i Säker information – förslag till informationssäkerhetspolitik (2005:42) att en gemensam, nationell strategi och en samverkansprocess skulle kunna lära oss att leva med problem som rör informationssäkerhet. Detta förutsätter ett långsiktigt arbete mot övergripande, långsiktiga mål. Med det finns också behov av beslutskraft i ett kort perspektiv och en operativ förmåga för att kunna hantera incidenter i realtid. Därför behövs,

enligt utredningen, en sammanhållen politik inom informationssäkerhetsområdet och en gemensam målstruktur.

I informationssäkerhet i Sverige och internationellt – en översikt (2004:32) redovisade utredningen en översikt av informationssäkerhetsarbetet i Sverige och internationellt. Utredningen kunde bland annat konstatera att även om problembilden i allt väsentligt sammanfaller, så har länderna valt att organisera informationssäkerhetsarbetet på olika sätt. Det är således svårt att direkt överföra organisationsmodeller från ett land till ett annat.

I detta slutbetänkande redovisar utredningen sina slutsatser och förslag till organisation av informationssäkerhetsarbetet i Sverige. De viktigaste utgångspunkterna återfinns i utredningens förslag till nationell strategi för ökad informationssäkerhet och i synen på omfattningen av det statliga åtagandet.

Den nationella strategin förutsätter organisatoriska grepp

Några av de förslag som redovisas i strategin förutsätter att staten utvecklar den egna organisationen och att samverkan mellan privat och offentlig sektor fördjupas. Behovet att förstärka informationssäkerhetsarbetet inom underrättelse- och säkerhetstjänsternas område liksom att förstärka förmågan inom området nationell säkerhet motiverar bland annat organisatoriska åtgärder. Inom båda dessa områden krävs, enligt utredningens mening, både tydligare ansvarsfördelning och säkerställande av kompetens och resurser.

Regeringen genomförde med början år 2002 organisatoriska förändringar för att etablera funktionerna omvärldsanalys, incidenthantering, teknikkompetens samt evaluering och certifiering. Den utvärdering som utredningen nu har gjort leder också till organisatoriska konsekvenser för berörda myndigheter.

Slutligen bör den av utredningen föreslagna strategin att förebygga, förbereda inför, förhindra, upptäcka, hantera och ingripa vid störningar i några fall leda till justeringar inom vissa myndigheter, utan att dessa behöver omorganiseras. Dessutom kan förutses att uppgifter i några fall bör preciseras och införas i berörda myndigheters instruktioner.

Det statliga åtagandet blir styrande

Statens åtagande, ansvar och intresse har av utredningen sammanfattats enligt följande:
1. Staten har ett övergripande ansvar för att en helhetssyn etableras och appliceras på informationssäkerheten och att nationella intressen bevakas genom EU och i internationella sammanhang.
2. Staten har ansvaret för samhällets regelverk på informationssäkerhetsområdet.
3. Staten har ett särskilt ansvar för informationssäkerheten inom ett antal politikområden. Det gäller statens kärnverksamhet, som till exempel rättsväsendet. Det gäller även ansvaret för att olika samhällsviktiga verksamheter bedrivs med tillräcklig säkerhet oavsett vem som äger dem (till exempel inom elförsörjning och telekommunikation).
4. Staten har slutligen ett eget intresse för informationssäkerheten inom sitt verksamhets- och ansvarsområde, i sina olika roller som till exempel ansvarig för myndighetsutövning och i sin ägarroll.

Det statliga åtagandets omfattning leder till krav på att bygga upp förmåga inom flera viktiga områden och att lösa ett antal uppgifter i den statliga verksamheten. Informationssäkerhetsarbetet måste, som utredningen påpekar, utgöra en integrerad del av alla aktörers verksamheter, så också inom staten. Det följer av ansvarsprincipens tillämpning.

Utredningen redovisade även vad som bör falla inom det privata åtagandet och vad som skulle kunna betraktas som det statliga åtagandet, även om gränsdragningen är svår.

Enligt utredningens uppfattning bör även dessa åtaganden leda till organisatoriska konsekvenser. Utöver detta återstår att formulera nya uppdrag och uppgifter till myndigheter i den befintliga organisationsstrukturen, i syfte att öka informationssäkerheten.

Flera utgångspunkter för val av organisation

Utredningen har konstaterat att informationssäkerheten inte bara inrymmer frågeställningar för respektive verksamhetsansvarig, utan att det också finns problem av gemensam natur, där stora krav ställs på samordning. Vidare finns flera problem och frågeställningar av tvärsektoriell karaktär, som ofta kräver tillgång till specialistkompetens. Dessa problemområden förutsätter ett

annat angreppssätt på styrning och organisation. Det är också viktigt att gränsdragningen mellan det privata och det offentliga åtagandet tydliggörs.

Vidare finns det, som utredningen redovisar under avsnittet om samverkan mellan privat och offentlig sektor, sannolikt frågeställningar som inte kan lösas av en aktör ensam, inte ens av staten. En fördjupad samverkan inom offentlig sektor och mellan privata och offentliga aktörer förutsätter en tydlig ansvarsfördelning inom staten och en organisation som kan hantera frågor av gemensam, tvärsektoriell natur i en vardag präglad av sektorstänkande och sektorsansvar.

Till dessa resonemang kan slutligen läggas att informationssäkerheten kräver tillgång till hög kompetens och resurser, såväl administrativt som tekniskt. I egenskap av liten nation är det av synnerlig vikt att regeringen fokuserar de resurser som finns tillgängliga och utnyttjar samhällets samlade kapacitet på ett bättre sätt.

I tidigare betänkanden har utredningen pekat på ett antal förhållanden och synsätt som kan vara vägledande för informationssäkerhetsarbetet. Några av dessa är särskilt viktiga för val av organisation inom staten:

1. Informationssäkerhet omfattar hela samhället och frågeställningen är därför vidare än totalförsvarets behov.
2. Det finns ett behov att kraftsamla och att tydligare fokusera den statliga verksamheten nationellt, inom EU och internationellt.
3. Alla statliga aktörer måste, inom ramen för sitt respektive sektorsansvar, medverka till förmågan att förebygga, förbereda inför, förhindra, upptäcka, hantera och ingripa vid störningar.
4. Ansvaret för förmågan i den statliga kärnverksamheten, liksom för säkerheten i samhällsviktiga verksamheter, måste tydliggöras. Vissa gemensamma behov förutsätter bättre samordning inom staten och i samverkan med andra, icke-statliga aktörer.
5. Kompetensen och förmågan att hantera tvärsektoriella frågor måste säkerställas inom informationssäkerhetsområdet.

Tre grundläggande organisationsprinciper

Med de olika utgångspunkter som utredningen redovisar kan tre principer för organisation inom staten urskiljas.

Den första organisationsprincipen följer av ansvarsprincipen. Detta innebär att varje sektorsmyndighet har ansvaret för utvecklingen av informationssäkerheten inom sitt ansvarsområde och för de aktörer som berörs av myndighetens verksamhet. I syfte att tydliggöra omfattningen av detta ökade ansvar har utredningen i det tredje delbetänkandet lämnat ett förslag till förordning om vissa åtgärder för informationssäkerhet i den statliga verksamheten.[1] Inom några områden finns det enligt utredningens mening anledning att ytterligare tydliggöra detta ansvar och uppdrag. PTS utökade ansvar och befogenheter inom området elektronisk kommunikation är ett sådant exempel. Finansinspektionens samverkan med aktörer inom finansmarknaden är ett annat. I andra fall kan det handla om att ge ökad prioritet och lyfta upp säkerhetsfrågorna i berörda myndigheters verksamhet och förstärka insatserna, som exempelvis inom energi och transportsektorn.

Den andra organisationsprincipen syftar till att tillgodose sådana behov som är gemensamma i den statliga verksamheten. Detta syftar framför allt till att uppnå en bättre samordning inom staten i administrativa och tekniska sammanhang

Den tredje organisationsprincipen syftar till att säkerställa kompetens och förmåga att hantera tvärsektoriella frågeställningar i hela samhället, vare sig det handlar om att kunna hantera och ingripa vid störningar eller att ge underlag för förebyggande arbete hos alla aktörer.

Samverkan mellan privat och offentlig sektor

Genom tidigare betänkanden har utredningen visat att det finns sammanfallande problem och behov inom privat och offentlig sektor och att det finns anledning att samverka kring dessa, inte minst av praktiska skäl. Utredningen har vidare i sitt senaste delbetänkande Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42), konstaterat att det inte finns någon definitiv lösning på problemet med informationssäkerhet. En väl förankrad samverkansprocess skulle dock kunna lära oss leva med problemen.

Utredningen har därutöver funnit att det finns problemställningar som är av sådan art att ingen av aktörerna ensam kan

[1] Förslag till förordning om vissa åtgärder för informationssäkerhet hos staten. Se Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42,) s. 31 ff.

klara av problemen. Följaktligen finns ett behov av att samverka för att identifiera och komma närmare lösningar på dessa. Det finns dessutom skäl att söka samverkan kring de prioriteringar som måste göras mellan olika problem och sektorer, i syfte att utnyttja tillgänglig kompetens och resurser på ett optimalt sätt.

Utredningens slutsats är att det i dagsläget finns en vilja till samverkan mellan aktörer i privat och offentlig sektor. Det är också utredningens uppfattning att näringslivet har ett intresse av att det finns adekvat utbildning, forskning och regelverk på informationssäkerhetsområdet. Den privata sidan kan bidra med tekniska lösningar och samhällets behov utgör en marknad för näringslivets aktörer. Det finns således en ömsesidig nytta i detta gemensamma intresse.

Företrädare för näringslivet har nu tagit ett initiativ till att bilda ett självständigt samverkansorgan. Detta bör därför tas tillvara av staten, kommuner och landsting. Ett sådant organ bör, enligt utredningens mening, ha till uppgift att dels medverka till att öka medvetenheten i informationssäkerhetsfrågor, dels ge underlag för en lönsam och optimal riskhantering hos alla aktörer.

Utredningen föreslår att det redovisade samverkansinitiativet tas tillvara och att staten omgående utser en utredare eller förhandlare. I avvaktan på regeringens ställningstagande till utredningens övriga förslag, kan utredaren eller förhandlaren skapa underlag för ställningstagande till statens samverkan med andra aktörer inom informationssäkerhetsområdet samt klarlägga intresse och möjligheter för samverkan med kommuner och landsting i dessa frågor.

Regeringens ledande och samordnande roll

Regeringen har en ledande och samordnade roll inom informationssäkerhetspolitiken. Det sätt som regeringen väljer att sätta mål för verksamheter, styra och följa upp resultat är avgörande för myndigheternas arbete. Inom informationssäkerhetsområdet är det av särskilt vikt med hänsyn till frågornas komplexitet, dynamik och internationella dimension. Utredningen återkommer därför till sitt förslag att utarbeta en sammanhållande målstruktur för informationssäkerhetsarbetet.

Utredningens slutsatser

Flera av de utgångspunkter som utredningen lyfter fram kan var och en för sig läggas till grund för val av organisation, med olika resultat beroende på vilka prioriteringar eller särintressen som styr valet. Den helhetssyn som enligt utredningen bör styra även valet av organisationslösning (och fördelningen av ansvar, befogenheter och skyldigheter inom staten) måste med nödvändighet bygga på en sammanjämkning av flera av de grundläggande frågeställningar som utredningen lyfter fram.

Tre grundläggande principer för organisation av informationssäkerhetsarbetet redovisas ovan. Den första följer ansvarsprincipen. Den andra syftar till att tillgodose gemensamma behov inom staten. Den tredje organisationsprincipen syftar till att säkerställa kompetens och förmåga att hantera tvärsektoriella frågeställningar i hela samhället.

Mot denna bakgrund är utredningens första slutsats att det måste ligga inom varje myndighets ansvar att svara för informationssäkerheten i den egna verksamheten och i kontakt med de aktörer som berörs av myndighetens verksamhet. Detta följer av ansvarsprincipen. Ansvar, befogenheter och skyldigheter bör förtydligas i berörda myndigheters instruktioner och i regleringsbrev. Föreskrifter samt råd och anvisningar bör utarbetas till den av utredningen föreslagna förordningen om vissa åtgärder för informationssäkerhet hos staten.

Utredningen föreslår att informationssäkerhetsarbetet bör organiseras så att kraftsamling kan ske till administrativa respektive tekniska frågeställningar. Utredningens andra slutsats är därför att gemensamma behov inom staten och tvärsektoriella frågeställningar i hela samhället bör samlas under en myndighet för administrativa funktioner respektive en myndighet för tekniska funktioner. Därmed förbättras även förutsättningarna för en sammanhållen informationssäkerhetspolitik.

Utredningens tredje slutsats är att några myndigheter, inom ramen för sina nuvarande ansvarsområden, bör ges utökade uppgifter och resurser för förebyggande arbete, rådgivning med mera.

Utredningen har visat att det finns problemställningar, som är av sådan art, att ingen av samhällets aktörer ensam kan lösa dem. En fjärde slutsats är därför att samverkan mellan privat och offentlig sektor bör utvecklas på informationssäkerhetsområdet.

Slutligen framhåller utredningen regeringens ledande och samordnande roll. Utredningens femte slutsats är att denna roll i informationssäkerhetsarbetet förutsätter en sammanhållande målstruktur som även fångar in frågeställningar som rör gemensamma och tvärsektoriella problem.

En ny organisationsstruktur för informationssäkerhetsarbetet

Ansvaret för policyfrågor och den administrativa funktionen, liksom ansvaret för den tekniska funktionen skulle kunna samlas i en central myndighet för informationssäkerhet. Utredningen har dock stannat för att föreslå att Krisberedskapsmyndigheten (KBM) förstärks och ges samordningsansvaret för policy och administrativ informationssäkerhet. Samordningsansvaret för den tekniska informationssäkerheten föreslås läggas på en nybildad myndighet med ansvar för signalunderrättelser, signalskydd och hög teknikkompetens. Denna nya myndighet föreslås huvudsakligen bygga på den kompetens som i dag finns inom Försvarets radioanstalt (FRA) men med utökat ansvarsområde och förstärkta resurser. Den föreslagna förändringen motiverar också ett nytt namn som bättre återspeglar dess uppgifter än vad namnet Försvarets radioanstalt gör. Utredningen föreslår namnet Institutet för signalunderrättelsetjänst och teknisk informationssäkerhet (IST).

Motivet för två myndigheter med samordningsansvar för olika delar av informationssäkerheten är framför allt att det är rationellt och ger utrymme för synergieffekter med dessa myndigheters övriga ansvarsområden. Det bör ge underlag för en bättre sammanhållen informationssäkerhetspolitik. Detta förutsätter dock ett välutvecklat löpande samarbete mellan de båda huvudansvariga myndigheterna, liksom mellan dessa och andra myndigheter, näringslivet och andra aktörer som har uppgifter och behov på informationssäkerhetsområdet.

Utredningens förslag kommer att få vissa konsekvenser för berörda myndigheters personal. I flera fall föreslår utredningen en förstärkning av kompetens och bemanning. De medel som hittills anslagits som projektmedel för informationssäkerhet via den så kallade civila ramen föreslås omvandlas till ordinarie anslagsmedel. Det innebär samtidigt en markering av att myndighetsorganisationen för informationssäkerhet får en permanent karaktär, efter de inledande årens mera projektinriktade uppbyggnadsperiod.

Det utökade ansvaret för informationssäkerhet som utredningen föreslår bör också återspeglas på ledningsnivå i de båda myndigheter som föreslås få samordningsansvar.

Policyansvar och administrativt samordningsansvar

I policyansvaret ligger att förvalta och utveckla den nationella informationssäkerhetsstrategin, att samordna informationssäkerhetsarbetet mellan samhällets aktörer, att under regeringen inrikta samhällets informationssäkerhetsarbete, att utgöra samhällets kontaktpunkt för informationssäkerhet och att under regeringen utgöra internationell kontaktpunkt genom att samordna och, där så bedöms lämpligt, företräda Sverige i internationell samverkan, där inte andra myndigheter är utpekade.

Också nationellt har utpekandet av en samordnande myndighet betydelse för allmänhet, näringsliv, kommuner etc. Det underlättar för samtliga aktörer i samhället om de i policyfrågor kan vända sig till en myndighet med frågor som rör informationssäkerhet eller skyddet av samhällsviktig IT-infrastruktur. Detta innebär i sig inget avsteg från ansvarsprincipen eftersom genomförandet av specifika uppgifter även fortsättningsvis bör ligga hos direkt ansvariga myndigheter.

KBM bör i sin roll som policymyndighet ges möjlighet att ge ut föreskrifter om en grundläggande säkerhetsnivå med stöd av den av utredningen föreslagna förordningen om informationssäkerhetssäkerhet hos staten.[2] Nära samverkan måste härvidlag etableras med sektorsansvariga myndigheter med egen föreskriftsrätt, exempelvis Post- och telestyrelsen, Finansinspektionen samt Säkerhetspolisen.

Även revision och tillsyn av föreskrifterna måste utvecklas. Detta bör dock genomföras av annan aktör än KBM, exempelvis av Statskontoret i en ny roll.

KBM sammanställer en helhetsbild genom sitt utpekade ansvar för omvärldsanalys. Denna kan i en förändrad organisation utvecklas ytterligare, bland annat genom att KBM får en förbättrad tillgång till underrättelserapporter.

Det finns behov av en formaliserad samverkan med KBM som samordnande myndighet mellan aktörer i samhället som äger, driver, eller på annat sätt har ansvar för samhällsviktig verksamhet

[2] Förslag till förordning om vissa åtgärder för informationssäkerhet hos staten. Se Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42), sid. 31ff.

eller infrastruktur. Informationsutbytet kan avse incidenter, bästa metod, hotbilder, risker och sårbarheter. Informationen måste fungera både inom, respektive mellan, stat, kommuner, näringsliv och andra organisationer.

Samverkan ger ett viktigt underlag till helhetsbilden liksom den till ömsesidig nytta förmedlar känslig eller förtrolig information, frågeställningar och påverkan. Det innefattar också till exempel att delta i och analysera utvecklingen inom EU och i övriga internationella sammanhang och att delta i relevanta arbetsgrupper för att strategiskt påverka de processer inom EU och internationellt som berör Sverige. Samverkan bidrar också till att stärka Sveriges position i dessa aktiviteter.

KBM bör i extraordinära situationer ha ett delegerat ansvar att inom givna ramar samordna informationssäkerhetsarbetet.

Utifrån helhetsbilden och policyansvaret på informationssäkerhetsområdet samt utifrån KBM:s befintliga kompetens på övningar på krishanteringsområdet är det naturligt att KBM har det samordnande myndighetsansvaret för övningar på informationssäkerhetsområdet. Liksom i det förebyggande arbetet kan övningsverksamheten till stor del hanteras av näringslivet. KBM:s roll bör främst vara att identifiera, uppmärksamma och formulera behov och mål för insatserna.

Det förefaller naturligt att samordning av kontakter mellan privat och offentlig sektor faller på KBM inom ramen för myndighetens samordningsansvar.

Utredningen förordar en signalskyddstjänst som omfattar hela samhällets behov, inte bara totalförsvarets. För att skapa möjlighet till helhetssyn för den utbildning som erfordras inom informationssäkerhetsområdet samt för att uppnå synergieffekter bör signalskyddsutbildningen utvecklas så att utbildning kan ges inom hela informationssäkerhetsområdet. Utredningen föreslår därför att huvudmannaskapet för signalskyddsutbildningen överförs från Försvarsmakten till KBM.

Tekniskt samordningsansvar

Utredningen föreslår att ansvaret för signalskydd överförs från Försvarsmakten, MUST Säkerhetskontor, till den nybildade myndighet, IST, som övertar Försvarets radioanstalts nuvarande uppgifter. Även KBM:s ansvar för nyckeldistribution föreslås överföras till IST. Det administrativa godkännandet av

signalskyddssystem liksom även föreskriftsrätten för samhällsviktiga system föreslås dock placeras vid KBM.

KBM:s signalskyddsverksamhet bedrivs i huvudsak i Sollefteå. Överföringen bör leda till en utökad verksamhet i Sollefteå.

Utöver det nuvarande signalspaningsuppdraget har FRA uppgifter inom svensk informationssäkerhet. Det gäller kompetens inom kryptologi, där FRA sedan 1980-talet svarar för att bemanna de kryptologiska funktionerna vid MUST.

FRA har också sedan 2003 en särskild teknikkompetens-funktion, TKF, till stöd för statliga myndigheter och bolag, som bland annat medverkar i tester av säkerheten i myndigheters IT-system tillsammans med berörda myndigheter. Informations-säkerhetsuppgifterna har tillförts FRA för att nyttiggöra FRA:s unika signalspaningskompetens och allmänt höga tekniska kompetens. FRA har färdiga krisberedskapsprocesser som har testats och används i verkliga fall för att stödja insatser vid myndighetskriser. Dessa kommer att vara värdefulla om det skulle uppstå en nationell kris med IT-inslag.

Signalskydd och signalspaning kan ses som två sidor av samma mynt. Det finns fördelar med ett nära samarbete mellan dessa båda områden. Länder med brister i signalskyddet har ofta dålig kontakt mellan signalskydd och signalspaning. Det behövs kompetens i att forcera bristfälligt signalskydd för att kunna skapa ett eget bra signalskydd. Kompetensen härför finns för närvarande i första hand inom FRA.

Svensk kryptoindustri har idag svårt att konkurrera med utländsk, då det inte finns en inhemsk organisation som kan godkänna kryptosystem utanför totalförsvaret. Det visar på ytterligare ett behov av att bredda omfattningen av samhällets signalskydd, vilket kan ske genom en flyttning av signal-skyddsfunktionen, från Försvarsmakten till den nybildade myndigheten för teknisk informationssäkerhet, IST. Verksam-heterna för nyckelproduktion och signalkontroll skulle därmed kunna integreras, eftersom dessa redan finns inom nuvarande FRA.

En effekt som uppstår vid samordning av alla teknikdelar hos en myndighet är snabbare beslutsvägar. Det är av stor vikt att snabbt kunna sätta ihop en insatsgrupp för att stödja insatser vid nationella kriser med IT-inslag och för att kunna medverka till identifiering av inblandade aktörer i IT-relaterade hot mot samhällsviktiga system. Med en delad organisationsbild är det svårare att upprätthålla en kritisk kompetensmassa.

Om uppgiften att leda och samordna signalskyddstjänsten inom totalförsvaret överförs från Försvarsmakten, erfordras att de medel som finns avsatta i materialplanen för utveckling också förs över. Försvarsmakten kommer oavsett vem som har det samordnande ansvaret för signalskyddstjänsten att vara en av de största avnämarna.

Sverige har på senare år deltagit alltmer aktivt i internationella signalskyddssammanhang. För att det internationella arbetet skall vara väl koordinerat behövs en utpekad National Communications Security Agency (NCSA), det vill säga en organisation i landet som ansvarar för signalskyddsfrågor, och en National Distribution Agency (NDA), en organisation som är behörig att distribuera kryptonycklar. Utredningen föreslår att den nybildade myndigheten för teknisk informationssäkerhet, IST, ges uppgifterna som NCSA och NDA.

Incidentrapporteringsfunktion

Sveriges IT-incidentcentrum, Sitic vid Post- och telestyrelsen ansvarar för systemet för informationsutbyte om IT-incidenter mellan samhällets alla aktörer. Uppgiften är bland annat att snabbt sprida information om IT-incidenter, att lämna information och råd om förebyggande åtgärder, att sammanställa och ge ut statistik som underlag för kontinuerliga förbättringar i det förebyggande arbetet.

Om Sitic skall fungera väl krävs ett nära och förtroendefullt samarbete med andra aktörer inom informationssäkerhetsområdet, inte minst med KBM och FRA som föreslås få särskilt samordnande uppgifter för den nationella informationssäkerheten. Det är angeläget att sådana väl fungerande samarbetskanaler finns såväl på ledningsnivå i myndigheterna, som på handläggarnivå.

Certifiering och evaluering

Det nationella systemet för evaluering och certifiering av IT-säkerhet i produkter och system i enlighet med IS 15408 Evalueringskriterier för IT-säkerhet i produkter och system (Common Criteria) tillkom efter riksdagens beslut under 2002. Certifieringsorganet är nu etablerat som en oberoende funktion

inom FMV med namnet Sveriges Certifieringsorgan för IT-säkerhet, CSEC.

Arbetet med att etablera certifieringsordningen är genomfört. Detta arbete omfattar bland annat utarbetande av kvalitetsmanual, ansvarsbeskrivningar, beskrivningar av processer för licensiering av evalueringslaboratorier, regler för genomförande av certifieringar samt utbildning av certifierare och evalueringsföretag.

Utredningen finner att de motiv som anfördes inför riksdagsbeslutet om etableringen av ett svenskt system för evaluering och certifiering alltjämt är giltiga. Utredningen har också i tidigare betänkanden betonat vikten av att tillämpa existerande internationella standarder inom IT-säkerhetsområdet. Common Criteria syftar till att sammankoppla ledningsfunktioner, inklusive riskhantering, och mer detaljerade tekniska specialstandarder med hur krav på säkerhets- och skyddsfunktioner ska kunna härledas, uttryckas och verifieras i de tekniska lösningarna i IT-produkter och program.

Utredningen föreslår att uppgiften som signatär inom ramen för CCRA överförs från Swedac till KBM. Swedacs uppgifter och roll för ackreditering och teknisk kontroll för andra, öppna system inom till exempel EU föreslås oförändrad.

Frivillig krisresurs

Ett sätt att bidra till att kunna hantera en allvarlig eller extraordinär situation vore att mobilisera kompetens dit den behövs, för att begränsa en skada eller att arbeta förebyggande mot nya attacker eller angrepp. Ett sådant nationellt säkerhetsinitiativ skulle vara att upprätta en kompetensbank. Det samordnande ansvaret för att ta tillvara sådana frivilligresurser bör läggas på KBM som ges uppgiften att hantera kontakterna och upprätta erforderliga avtal med enskilda och berörda företag samt tillse att övningsverksamhet genomförs.

Rikspolisstyrelsen och Statens Kriminaltekniska laboratorium

Allvarliga IT-incidenter utgör i grunden ofta brott. Inom informationssäkerhetsområdet har det visat sig att en rad myndigheter och andra organisationer har behov av polisens medverkan i olika arbets- och samverkansgrupper. Polisen och

Säkerhetspolisen kan genom sina operativa uppdrag tillföra erfarenheter inom området.

Rikskriminalpolisen är Sveriges kontaktpunkt inom ramen för G8:s 24/7 High Tech Crime arrangemang och Interpols National Central Reference Point System , NCRP, vilket understryker att polisen är en viktig aktör i samhällets informationssäkerhetsarbete.

För att möta dessa omvärldskrav och ett önskemål om samordning internt inom polisen, har en för Rikskriminalpolisen och Säpo gemensam funktion S-BIT etablerats. Då verksamheten inte fått öronmärkta medel för området har funktionen endast ett begränsat antal tjänster, mot planerade 12. För att leva upp till de beskrivna målen och de krav och önskemål som ställs på polisen inom området informationssäkerhet är det önskvärt att särskilda medel kan avsättas för ändamålet. S-BIT:s verksamhet bör därför delvis finansieras med medel ur KBM:s så kallade civila ram eller genom anslagstilldelning.

Allt större del av den brottsutredande verksamheten kommer i kontakt med IT och kräver kunskaper om bevissäkring och undersökning i IT-miljö, så kallad IT-forensisk verksamhet. Inom det IT-forensiska området och vid vissa tekniska problem, lämnar FRA i vissa fall stöd till polisen. Det är av vikt att metodutvecklingen vad gäller IT-forensisk verksamhet sker inom polisen, i första hand vid Statens Kriminaltekniska Laboratorium. FRA bör dock kunna vara en stödjande resurs, särskilt ifråga om kryptologisk kompetens.

Ekonomiska konsekvenser

Utredningens förslag innebär en höjd ambitionsnivå för samhällets informationssäkerhet. Vissa av förslagen medför ökade kostnader. Det gäller dels ökade resursbehov vid Krisberedskapsmyndigheten, dels vid den nybildade myndigheten, IST, som föreslås få policyansvar och administrativt samordnande ansvar respektive tekniskt samordnande ansvar för samhällets informationssäkerhet.

Vidare föreslås att finansieringen av Sitic – Sveriges incidenthanteringscentrum vid Post och telestyrelsen och CSEC – Sveriges Certifieringsorgan för IT-säkerhet skall ske via ordinarie anslag.

Finansiering föreslås ske genom avräkning från KBM:s så kallade civila ram, 7:5 Krisberedskap. Efter avräkning kvarstår ett ökat anslagsbehov med 43 miljoner kronor per år för att kunna

genomföra utredningens förslag till förbättrad informationssäkerhet.

Utredningen föreslår vidare överflyttning av ansvar och verksamhet för signalskydd från Försvarsmakten, MUST Säkerhetskontor, till den nybildade myndigheten för teknisk informationssäkerhet, IST. Även KBM:s ansvar och verksamhet för signalskydd föreslås överflyttat till IST. Det administrativa godkännandet av signalskyddssystem föreslås dock placeras vid KBM. Utredningen föreslår också en överföring av huvudmannaskapet för signalskyddsutbildningen från Försvarsmakten till KBM. Förslagen avses ej få kostnadseffekter för statsbudgeten.

Utredningen har också i sitt tidigare betänkande Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42) föreslagit att KBM genom sin roll i forskningshänseende bör utveckla ett tematiskt forskningsområde kring Informationssäkerhet. För att en satsning skall uppfattas som meningsfull inom forskarsamhället bör den årliga ramen vara 10-15 miljoner kronor, beroende på medfinansiering. Finansieringen av KBM:s insats i en sådan satsning föreslås ske via projektmedel ur den civila ramen.

1 Underlag för utredningens överväganden

1.1 Regeringens strategi för informationssäkerhet i samhället och skydd av samhällsviktiga IT-beroende system

Enligt den bedömning regeringen gjorde i propositionen Samhällets säkerhet och beredskap (2001/02:158), bör den övergripande målsättningen vara att upprätthålla en hög informationssäkerhet i hela samhället som innebär att man skall kunna förhindra eller hantera störningar i samhällsviktig verksamhet. I propositionen anfördes att strategin för att uppnå detta mål, liksom övrig krishantering i samhället, bör utgå från ansvarsprincipen, likhetsprincipen och närhetsprincipen – det vill säga att den som ansvarar för informationsbehandlingssystem även ansvarar för att systemet har den säkerhet som krävs för att systemet skall fungera tillfredsställande. Ansvarsprincipen innebär att den som har ansvar för en verksamhet under normala omständigheter även skall ha ansvaret under extraordinära situationer eller vid svåra påfrestningar på samhället. Likhetsprincipen innebär att en verksamhets organisation och lokalisering i så stor utsträckning som möjligt skall vara likadan i fred, kris och vid höjd beredskap. Närhetsprincipen, slutligen, innebär att kriser skall hanteras på lägsta möjliga nivå i samhället.

Regeringen aviserade vidare sin avsikt att inrätta fyra funktioner i syfte att förbättra informationssäkerheten. Dessa var omvärldsanalys, IT-incidenthantering, teknikkompetens samt ett system för evaluering och certifiering. Avsikten var att uppgifterna skulle läggas på de myndigheter som redan hade näraliggande uppgifter. Den organisatoriska lösningen skulle prövas i två år, varefter den skulle utvärderas och eventuell förändring genomföras.

Vidare framhölls det internationella engagemanget inom informationssäkerhetsområdet som viktigt, inte minst på grund av områdets globala natur. Regeringen visade sitt stöd för ambitionen att stärka nät- och informationssäkerheten på europeisk nivå.

Utredningen delar regeringens bedömning, men har funnit anledning att konkretisera och fördjupa den. Utredningen har tagit fram underlag för utvärdering av de organisatoriska åtgärderna, vilka läggs fram i detta slutbetänkande av

Informationssäkerhetsutredningen.

1.2 Utredningens direktiv

Utredningen angående vissa frågor om informationssäkerheten i samhället (InfoSäkutredningen, Fö 2002:6) har av regeringen fått i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas samt hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet skall utformas. Utredaren fick även på sin lott att följa myndigheternas uppbyggnad av den informationssäkerhetsverksamhet som regeringen gav myndigheterna i uppgift enligt propositionen 2001/02:158. I uppdraget ingick även att lämna förslag till hur OECD:s riktlinjer om säkerheten i nät- och informationssystem kan genomföras i Sverige.

Det ursprungliga direktivet (dir. 2002:103) samt tilläggsdirektiven (dir. 2003:29 och 2004:46) tillsammans med direktivet om förlängd tid för uppdraget (dir. 2005:53) återges i sin helhet i bilaga 1-4.

1.3 Definitioner

Utredningen ser det inte som sin uppgift att skapa en ny terminologi för informationssäkerhetsområdet. Däremot är det befogat att slå fast vilka begrepp utredningen utgår ifrån i sitt arbete, och motiven till detta. Ett övergripande skäl till att vissa begrepp används är att de i stor utsträckning är vedertagna bland aktörer i såväl privat som offentlig sektor. Det tidigare förhållandet att språkbruket skilde sig åt mellan privat och offentlig sektor har med tiden blivit mindre påtagligt. Det divergerande språkbruket utgjorde ett problem såväl ur samverkans- som författningshänseende. Det är nu snarare så, som utredningen redogjorde för i sitt andra delbetänkande, Informationssäkerhet i Sverige och internationellt – en översikt (SOU 2004:32), att de begrepp som formulerats av inblandade aktörer efter deras specifika behov inte överensstämmer med de av statsmakterna formulerade definitioner som återfinns i rättsliga, administrativa eller finansiella regler.

Utredningen använder det språkbruk som anges i SIS (Swedish Standards Institute) Handbok 550: Terminologi för informationssäkerhet (utgåva 2, 2004).

Terminologin inom EU på informationssäkerhetsområdet ger stöd för den bredare definition av informationssäkerhet som utredningen använder sig av. Kommissionen definierar i sitt meddelande från 2001 Nät- och informationssäkerhet: förslag till en europeisk strategi (KOM[2001]298) informationssäkerhet som ”förmågan hos ett nät att tåla, vid en viss tillförlitlighetsnivå, olyckshändelser eller illvilligt uppträdande som äventyrar tillgängligheten, äktheten, integriteten och konfidentialiteten hos lagrade eller vidarebefordrade data och besläktade tjänster som tillhandahålls av, eller är tillgängliga, via dessa nät”. I rådets säkerhetsbestämmelser slås fast att informationssäkerhet rör skyddandet av uppgifter mot oavsiktligt eller avsiktligt sekretessbrott, förlust av okränkbarheten eller tillgängligheten (det vill säga att förebygga förvanskning, obehörig ändring eller radering samt att åtkomst inte skall hindras den som är behörig). Båda dessa skrivningar överensstämmer i hög grad med utredningens definition.

Ett annat begrepp som har visat sig ha grundläggande betydelse för utredningsarbetet är samhällsviktig verksamhet. I diskussionen om vad som utgör det offentliga åtagandet är begreppet återkommande. Enligt utredningens erfarenhet finns dock inte någon generellt vedertagen definition av begreppet. Sannolikt är det så att det finns en mängd olika verksamheter som vid ett givet tillfälle kan vara mer eller mindre viktiga för samhället. Staten kan således ha ett ökat intresse av att säkerheten upprätthålls i sådana verksamheter. Det finns därmed ett behov av att vidare definiera vilka kriterier som skall uppfyllas för att en verksamhet eller ett system skall definieras som samhällsviktigt.

1.4 Tidigare betänkanden

Nedan följer korta beskrivningar av utredningens tre tidigare delbetänkanden.

1.4.1 SOU 2003:27 Signalskydd

Utredningens första delbetänkande behandlade signalskydd. Utredningen konstaterade i betänkandet att det finns ett behov av signalskydd även utanför det som lagstiftningsmässigt definieras som totalförsvaret. Möjligheterna att finansiera resurser och

kompetens inom totalförsvaret måste vägas mot möjligheterna att tillgodose behoven med kommersiellt tillgängliga system. Utredningen pekade på behov och intresse av samarbete mellan den verksamhet som bedrivs inom totalförsvaret och den inom privat eller kommersiell verksamhet, som motiverar vidare utredning av samverkansmöjligheter. Det har därför också funnits ett behov av att se över gränsdragningar i lagstiftningen, ansvarsförhållanden, organisation etcetera.

Utredningen utgick från att en svensk anpassning till internationella normer (till exempel de gällande inom EU) avseende signalskydd och hantering av skyddsvärd information, är eftersträvansvärd. En möjlighet syntes vara att utvidga säkerhetsskyddslagens tillämpningsområde till att omfatta även annan skyddsvärd information än den som är hemlig med hänsyn till rikets säkerhet. Med en sådan ordning skulle en större krets av de organ som hanterar skyddsvärd information kunna omfattas av tillämpningsföreskrifter eftersom lagens tillämpningsområde även omfattar kommuner, landsting och vissa andra enskilda rättsubjekt.

Ett mindre långtgående alternativ ansågs kunna vara att regeringen föreskriver att särskilda signalskyddsrutiner med mera skall tillämpas hos de statliga myndigheterna.

De frågor som utredningen beslutade att vidare utreda i det fortsatta arbetet rör organisation, lokalisering och författningsändringar. Då signalskydd av utredningen definieras som en integrerad del av informationssäkerhet i stort, omfattas området i övrigt av de förslag gällande informationssäkerhet som utredningen presenterar.

1.4.2 SOU 2004:32 Informationssäkerhet i Sverige och internationellt – en översikt

Utredningens andra delbetänkande gjorde en översikt av informationssäkerhetsläget nationellt och internationellt.

Det offentliga åtagandet

Utredningen slog i sitt andra delbetänkande fast att det är nödvändigt att det offentliga engagerar sig i informationssäkerhetsfrågorna, eftersom satsningarna annars kan förväntas bli otillräckliga. Det är också enbart staten som kan ha den överblick

som är nödvändig för att kunna göra adekvata riskbedömningar. Det är dock viktigt att det offentligas engagemang begränsas till de områden eller åtgärder där dess roll är avgörande eller nyttan är så stor att det motiverar ingrepp. I vissa fall kan det vara befogat att offentliga organ tar ansvar för finansiering och genomförande av säkerhetsåtgärder.

Utredningen redovisade mot denna bakgrund de huvudsakliga funktioner och kontinuerliga arbetsuppgifter för offentliga organ som, utöver det ansvar som följer av ansvarsprincipen och oberoende av dagens organisationsstruktur och funktioner, kunde identifieras inom informationssäkerhetsområdet. Dessa berörde bland annat tydliggörandet av en nationell strategi, att föreslå och förmedla grundläggande regelverk, signalskyddstjänst, att ge råd och information till allmänheten och stöd till myndigheter, särskilda råd och stöd till särskilt viktiga myndigheter eller avseende särskilt viktiga system samt att förebygga, upptäcka, utreda och lagföra IT-relaterad brottslighet.

Utredningen ansåg att det finns flera tänkbara målgrupper för informationssäkerhetsarbetet. De som särskilt nämndes var statlig förvaltning, kommuner och landsting, näringsliv och allmänhet.

Utredningen konstaterade att det under 2003 förekommit diskussioner rörande gränsdragningsfrågor, dels om relationen mellan de fyra på informationssäkerhetsområdet särskilt utpekade myndigheterna Försvarets Materielverk (FMV), Försvarets radioanstalt (FRA), Krisberedskapsmyndigheten (KBM) och Post- och Telestyrelsen (PTS), dels om dessa myndigheters relation till andra myndigheter verksamma inom informationssäkerhets-området – till exempel Statskontoret, Styrelsen för ackreditering och teknisk kontroll (Swedac), Säkerhetspolisen och Försvarsmakten. Oklarheterna om gränsdragning gäller i vissa fall instruktioner för myndigheterna, men framför allt den praktiska uppdelningen av arbetet. Vidare befanns den operativa ansvarsfördelningen och samordningen vid krishantering vara oklar. Det framkom också farhågor om att utpekandet av särskilt ansvar för vissa myndigheter riskerar att överskugga det ansvar som varje myndighet redan har inom sitt område. Vissa lagtekniska hinder för verksamheten konstaterades också.

Utredningen slog fast att informationssäkerhet är, och kommer att vara, en angelägenhet för var och en som hanterar information i någon form. Samtidigt måste arbetet med denna typ av frågor samordnas. Arbetet måste också bedrivas med såväl långsiktighet som beredskap i det korta perspektivet.

En analys av kriterier för vad som är samhällsviktig infrastruktur är nödvändig för att myndigheternas roller och ansvar skall kunna fastställas.

Utredningen argumenterade för att utgångspunkten för fastställande av ansvar, åtgärder, finansiering med mera bör vara funktionsorienterad. Tidigare har utgångspunkten för informationssäkerhetsarbetet varit situationsberoende i den meningen att ansvar varit beroende av i vilken situation som informationssäkerheten varit viktig. I första hand har uppdelning skett i termer av informationssäkerhet i fred respektive under höjd beredskap och krig. Utredningen menade att upprätthållande av samhällsviktig infrastruktur bör vara utgångspunkten för vilket ansvar staten har för informationssäkerheten.

Utredningen fokuserade på legaldefinitioner som skulle kunna koppla samman de övergripande begreppen och definitionerna med de tekniska och administrativa som redan finns etablerade. Utredningen ansåg det viktigt att skapa en grund för tydligare författningar samt att öka spårbarheten inom informationssäkerhetsområdet och därmed möjligheterna att förankra begrepp och definitioner hos alla aktörer och användare.

Ett problem som utredningen pekade på var att de begrepp som skapas för att fungera i rättsliga sammanhang inte alltid harmonierar med de begrepp som utvecklas och används av ansvariga för forskning och utveckling, producenter, leverantörer, systemkunniga, tekniker med flera. Nuvarande regelverk på informationssäkerhetsområdet är endast allmänt hållet och speglar knappast det faktum att en mycket stor del av informationshanteringen i samhället inte längre sker i traditionell fysisk form. Utredningen menade att begrepp och definitioner som rör informationssäkerhet måste konkretiseras ytterligare för att kunna tjänstgöra som verktyg och att regelverket i högre grad bör anpassas till hantering av handlingar i IT-system.

Internationell koppling

Enligt utredningen föreföll det som att EU (och OECD) har bättre anpassade bestämmelser och tydligare visioner för informationssäkerhetsarbetet än Sverige. Några undantag från EU:s säkerhetsbestämmelser har inte gjorts från svensk sida. Bestämmelserna reglerar hantering av sekretessbelagda EU-uppgifter. Medlemsstaterna skall vidta lämpliga åtgärder så att det

vid hantering av sekretessbelagda EU-uppgifter säkerställs att bestämmelserna respekteras av medlemsstaternas myndigheter. Även om bestämmelserna bara omfattar sekretessbelagda EU-uppgifter skulle de kunna utgöra en utgångspunkt för utredningens fortsatta överväganden. Med den grundläggande definitionen av informationssäkerhet inom EU (”uppgifter som lagras, bearbetas eller överförs i elektronisk form”) som utgångspunkt skulle bestämmelser kunna konkretiseras utifrån den administrativa och tekniska hierarki som utarbetats inom SIS-projektet.

Utredningen pekade på regeringens möjligheter att genom den delegerade normgivningskompetensen utfärda förordningar för att styra statlig verksamhet. Det skulle således vara möjligt att samla bestämmelser om informationssäkerhet på motsvarande sätt som redan görs för krig och krigsfara genom BITS (KBM:s rekommendationer för basnivå för IT-säkerhet). I detta sammanhang skulle begrepp och definitioner utvecklas.

Författningar

Utredningen erfor att flera myndigheter upplevde att begreppet rikets säkerhet i 2 kap. Sekretesslagen (1980:100) har ett för snävt tillämpningsområde. Vidare faller mycket av för samhället viktig verksamhet utanför säkerhetsskyddslagen (1996:627), eftersom den inte rör rikets säkerhet enligt dagens tolkning av begreppet. Till exempel borde begreppet inkludera ekonomisk säkerhet och attraktionskraft samt handelsstatus. Sverige bör dock inte gå längre i sin tolkning av när inskränkningar är tillåtna än vad som accepteras av den Europeiska domstolen för de mänskliga rättigheterna.[3]

Utredningen konstaterade att det kunde finnas anledning att analysera säkerhetsskyddslagen (1996:627) närmare i det fortsatta arbetet. Med hänsyn till den teknikutveckling som skett och särskilt med hänsyn till den omfattande användningen av Internet och e-post, ansåg utredningen att det fanns anledning att i det fortsatta utredningsarbetet ta ställning till om det behövs en mer genomgripande översyn av lagar och förordningar som har relevans

[3] Konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) av den 4 november 1950. Genom lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna gäller Europakonventionen jämte tilläggsprotokoll som svensk lag sedan den 1 januari 1995.

för dessa frågor. I lagen om elektronisk kommunikation (2003:389) regleras frågor om säkerhet vid elektronisk kommunikation. Genom en lagändring som trädde i kraft den 1 juli 2005 har säkerhetsfrågorna stärkts. Den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster skall se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet samt på uthållighet och tillgänglighet vid extraordinära händelser i fredstid.

Det internationella perspektivet konstaterades vara av stor betydelse både vad gäller säkerhetsskyddsklassning och brottsförebyggande och lagförande av IT-relaterad brottslighet.

Kompetensförsörjning

Utredningen slog fast att det föreligger ett generellt behov av att öka medvetenheten om sårbarheter och risker på alla nivåer i samhället. Dessutom finns det ett behov av att stärka beställarkompetensen bland annat hos ägare av samhällsviktig infrastruktur. Företeelsen *outsourcing* – att lägga verksamhet på entreprenad – ökar ytterligare behovet av beställarkompetens.

Behov av kryptologisk kompetens i samhället är stort och växande. Kompetenskraven har höjts kraftigt under senare år. Utredningen avsåg att återkomma med förslag till åtgärder för hur detta behov skall kunna tillgodoses.

För att täcka behov av utbildning och medvetandegörande som ansågs finnas, föreslog utredningen en rad åtgärder redan på grundskolenivå, som ett sätt att på bred front öka medvetandet. Beträffande högskolenivå angav utredningen sin avsikt att vidare belysa tillgången till säkerhetsinriktade ämnen inom bland annat tekniska och ekonomiska utbildningar. Som en del i samhällets säkerhetsförebyggande arbete finns skäl att överväga att bygga in rekommendationer om inslag av utbildning om sårbarhet och säkerhet som en normal del i grundutbildningarna i ett antal akademiska examina.

En metod för att ytterligare utveckla beställarkompetens kan vara att använda gemensamma standarder för informationssäkerhet. Utredningen angav att man avsåg att värdera huruvida en mera generell användning av informationssäkerhetsstandard är en bra och resurseffektiv metod för att utveckla beställarkompetens samt en gemensam nivå vad gäller informationssäkerhet.

Den offentliga verksamheten måste på ett aktivt sätt ta tillvara den säkerhetskompetens och den snabba utveckling som finns inom den privata sektorn. Det är inte en uppgift för den offentliga sektorn att tillgodose behovet av leverantörskompetens, utan detta bör främst ske genom det utbud som utvecklas på den privata marknaden.

Utredningen konstaterade dock att i den mån marknaden inte är tillräckligt stor, eller om det av någon annan anledning befinnes olämpligt, måste staten kunna träda in. När det gäller infrastruktur och informationssystem som är samhällskritiska, har staten ett särskilt ansvar. Det är därför av nationellt intresse att tillgodose samhällets behov av leverantörskompetens inom området.

Utredningen redovisade sin avsikt att särskilt belysa möjligheterna till kompetensutveckling genom en mera generell användning av revisionsinstrumentet inom områdena informationssäkerhet och IT-säkerhet.

Integrering av informationssäkerhet och signalskydd

Utredningen kunde konstatera att centrala förvaltningsmyndigheter med flera i allt större omfattning begär stöd i signalskyddsfrågor även för hantering av skyddsvärd information som inte omfattas av sekretess enligt sekretesslagen (1980:100).

Inom det internationella samarbetet har Sverige hävdat sig väl inom signalskyddsområdet och ofta uppskattats för sin kompetens. Utredningen konstaterade att en kvalificerad resurs för granskning och i tillämpliga fall kryptogodkännande av svensktillverkade produkter för internationella organisationers behov dock är nödvändig för att upprätthålla Sveriges goda internationella anseende på området.

Försvarsmakten utövar idag rollen som National Communications Security Agency (NCSA) genom Totalförsvarets signalskyddssamordning, TSA.[4] Något formellt beslut har dock inte tagits i denna fråga. Utredningen ansåg att det finns ett behov av att tydliggöra denna roll på ett bättre sätt.

[4] TSA organiseras i dag av Försvarsmakten/MUST Säkerhetskontor.

Samordning av det internationella agerandet

Målet för det svenska agerandet på den internationella arenan är att få genomslag för svenska intressen. Detta gäller på alla nivåer – regeringen, Regeringskansliet och myndigheterna.

Utredningen konstaterade att det finns ett stort behov av samordning mellan olika aktörer. Med en väl genomarbetad och förankrad nationell strategi och en tydlig arbetsfördelning, såväl inom Regeringskansliet som mellan myndigheterna, bör de befintliga verktygen – det vill säga gemensam beredning, regleringsbrev och myndighetsinstruktioner – vara tillräckliga för att hantera såväl förutsedda som snabbt uppkomna frågor. Utredningen menade däremot att det kan finnas skäl att lägga större vikt vid de internationella frågorna när myndigheternas instruktioner och regleringsbrev ses över.

Finansieringsaspekter

Säkerhet måste ses som intäktsskapande eller kostnadsbesparande. Till exempel är visionen 24-timmarsmyndighet[5] baserad på flera kvalitativa tjänster till medborgarna till lägre kostnader. Informationssäkerheten berör alla verksamheter och ligger inom varje enskild organisations ansvar. Informationssäkerheten måste lösas i det dagliga arbetet och i den ordinarie organisationen. Därför bör också säkerhetslösningarna finansieras inom de normala finansieringsramarna för verksamheten. Utredningen gjorde bedömningen att kostnaderna, alternativt de negativa effekterna, riskerar att bli avsevärt större om inga åtgärder vidtas.

I den offentliga förvaltningen skall kostnaderna med anledning av de föreslagna åtgärderna redovisas i samband med årsredovisningen. Åtgärderna skall genomföras och finansieras inom tilldelade budgetramar inom respektive myndighetsansvar. När så är tillämpligt kan åtgärder samfinansieras mellan offentlig och privat sektor.

Inom Utgiftsområde 6 Försvar samt beredskap mot sårbarhet sker för närvarande en översyn av finansieringsprinciperna för anslaget 6:5 Civilt försvar. Utredningen avsåg att följa översynen av dessa principer.

[5] Strategiskt arbete med att utveckla en sammanhållen elektronisk förvaltning.

Utgångspunkter för en nationell informationssäkerhetsstrategi

Utredningen konstaterade att en nationell informationssäkerhetsstrategi bör ha ett långsiktigt, framåtblickande perspektiv, som kan ligga till grund för handlingsplan och åtgärder på två till tre års sikt. Strategin bör vända sig till myndigheter, näringsliv och organisationer, men även till enskilda användare, då de flesta i dag är anslutna till olika lokala, nationella eller internationella informationstjänster.

1.4.3 SOU 2005:42 Säker information - förslag till informationssäkerhetspolitik

I det tredje och senaste delbetänkandet presenterade utredningen sitt förslag till ramverk för organisering av informationssäkerhet. Utredningen redogjorde för de behov som har identifierats på informationssäkerhetsområdet och lade ett antal förslag.

Principer för ansvarsfördelning och åtgärder

Två principer har utkristalliserats: den första handlar om hotets ursprung och den andra om hotets möjliga konsekvenser.

Enligt utredningens mening innebär den första principen att ansvaret för hantering av administrativa och tekniska säkerhetsbrister faller på den som är ansvarig för verksamheten. Detta följer även av ansvarsprincipen. Det utesluter dock inte att staten har ett ansvar, till exempel för vissa förebyggande åtgärder inom det privata området. Det kan vara svårt för enskilda och företag att skydda sig mot aktörsberoende, antagonistiska hot. Dessa hot kan mycket snabbt komma att kräva statliga insatser, särskilt när det gäller samhällsviktig verksamhet.

Den andra principen innebär att ju svårare konsekvenser ett hot eller en brist kan leda till, desto mer sannolikt är det att staten kommer att involveras i någon form. I det statliga åtagandet bör därför ingå frågor om till exempel krishantering, brottsbekämpning eller totalförsvar.

Med dessa starkt förenklade principer för arbets- och ansvarsfördelning inom informationssäkerhetsområdet som utgångspunkt kan fyra uppgifter eller handlingslinjer urskiljas: att förebygga, förbereda inför, förhindra respektive hantera allvarliga störningar. Dessa är uppgifter som flertalet aktörer måste axla i en

eller annan form. Två av dessa mål eller uppgifter ingår redan i regeringens strategi; förhindra och hantera.

Det finns ingen definitiv lösning på problemet med informationssäkerhet. Därtill är problemet alldeles för komplext och området dessutom under ständig utveckling. Däremot finns det ett stort behov av att samordna informationssäkerhetsarbetet. En av utredningens huvuduppgifter är därför att se utvecklingsmöjligheter i den av regeringen angivna strategin för informationssäkerhet.

En samlad bedömning av hotbild, risker och sårbarheter bör ligga till grund för verksamhetsansvarigas planering och arbete. Utredningen anser att en gemensam, nationell strategi och en samverkansprocess skulle kunna lära oss att leva med de problem som rör informationssäkerhet som inte går att undvika.

Gränsen för vad som är den verksamhetsansvariges ansvar och sådana situationer som motiverar ingripande från staten kan inte dras med säkerhet. Utredningen menar att utgångspunkten här bör vara att staten är den aktör som har det övergripande ansvaret för helhetsbilden. Staten bör dessutom upprätthålla tillräcklig förmåga att hantera oförutsedda eller nya typer av allvarliga störningar och kriser. Det finns enligt utredningen skäl att införa informationssäkerhetspolitik som begrepp för att sammanföra de horisontella aspekterna (gemensamma eller liknande informationssäkerhetsproblem) av informationssäkerhet med de vertikala (informationssäkerhet i verksamheten).

Att öka förtroendet för IT är en förutsättning för att utfallet av andra åtgärder på informationssäkerhetsområdet skall falla väl ut. Detta kan ske genom att öka kunskaperna om de risker och hot som finns, samt vilka åtgärder som kan vidtas. Utredningen anser att dessa åtgärder måste ske på en bred front. Det gäller att öka kompetensen i alla delar av samhället.

Utredningen konstaterar att staten dessutom behöver egen och unik kompetens. Dels har staten krav på sig att ta ansvar för samhället, oavsett konjunkturer, och dels har staten det yttersta ansvaret för den nationella säkerheten – vilket ställer särskilda krav.

Det krävs även ömsesidigt informationsutbyte och samarbete mellan den offentliga sektorn och näringslivet. Utredningen konstaterar att Sverige i dag inte har tillräckliga resurser för att bygga dubbla strukturer.

Utredningen konstaterar vidare att det behövs bättre rutiner för att tillvarata den information som i dag finns i underrättelse-organen. Dessa myndigheter har en unik kompetens och använder

sig av unika metoder, men det måste säkerställas att den information de inhämtar inte stannar hos dem. Metoder för delgivning bör utvecklas för att kunna ge en helhetsbild av de risker och hot som finns inom IT-världen.

Utredningen anser att det bör finnas en funktion för analys av de incidenter som inträffar, för att vi skall kunna dra slutsatser av dessa.

Styrmedel

Staten förfogar över en rad administrativa, ekonomiska och informativa styrmedel. I praktiken är dessa relativt svagt utvecklade på informationssäkerhetsområdet och utredningen lämnade därför förslag till inriktning av fortsatt författningsarbete och tillämpning av standard. Utredningen menar att en målstruktur för informationssäkerhet skulle kunna medverka till en sammanhållen politik på området.

Strategi för informationssäkerhet

Utredningen framhåller att en strategi för informationssäkerhet måste kunna inrymma många aspekter, tidsperspektiv, mål och medel eftersom den syftar till att sammanfatta en handlingslinje på lång sikt. Strategin skall kunna ligga till grund både för privata och offentliga aktörer. En ökad informationssäkerhet måste därför bygga på att regeringen i en nationell strategi lyckas fånga in frågeställningar som kan omfattas av flertalet aktörer och intressenter. Strategin förutsätter därför att formerna för samverkan utvecklas. Dessutom krävs ett modernt regelverk som stödjer, framtvingar eller tydliggör krav på aktörerna och som säkerställer att säkerheten efterlevs.

Strategin innefattar att:

1. utveckla Sveriges position inom EU och i internationella sammanhang
2. skapa förtroende, trygghet, säkerhet och öka integritetsskyddet
3. främja ökad användning av IT
4. förebygga och kunna hantera störningar i informations- och kommunikationssystem
5. förstärka underrättelse- och säkerhetstjänstens arbete samt utveckla delgivningen

6. förstärka förmågan inom området nationell säkerhet

I strategin bör även ingå att:

7. utnyttja samhällets samlade kapacitet
8. fokusera på samhällsviktig verksamhet
9. öka medvetenheten om säkerhetsrisker och möjligheter till skydd
10. säkerställa kompetensförsörjningen

2 Nuvarande hantering av informationssäkerhet

2.1 Inledning

I Säkerhet i en ny tid (SOU 2001:41), från Sårbarhets- och säkerhetsutredningen betonades vikten av att säkerställa att viktiga IT-system skyddas från angrepp. Teknisk infrastruktur omfattar under fredstid bland annat elförsörjning, telekommunikationer samt informationsteknik som system. Staten har ett ansvar för den kritiska infrastrukturen. För att förbättra den svenska informationssäkerheten genomfördes en del förändringar i enlighet med propositionen Samhällets säkerhet och beredskap (2001/02:158). Fyra myndigheter fick särskilda uppgifter inom verksamhetsområdena teknikkompetens, omvärldsanalys, IT-incidenthantering samt evaluerings- och certifieringsfunktion: Försvarets materielverk (FMV), Försvarets radioanstalt (FRA), Post- och telestyrelsen (PTS) samt Krisberedskapsmyndigheten (KBM). Även Försvarsmakten med MUST (Militära underrättelse- och säkerhetstjänsten), Rikspolisstyrelsen (RPS) med Rikskriminalpolisen (RKP) och Säkerhetspolisen samt Statskontoret är viktiga aktörer på informationssäkerhetsområdet. Så är även Datainspektionen, Finansinspektionen och Konsumentverket, som kommer i kontakt med allmänheten i anledning av informationssäkerhetsfrågor.

I detta kapitel kommer det att redogöras för resultaten efter förändringarna efter proposition 2001/02:158, en presentation av hur det ser ut i dag på informationssäkerhetsområdet.

Utredningen har funnit att en indelning med fördel kan göras av funktionerna som har att göra med informationssäkerhet; i administrativa respektive tekniska funktioner. Nedan följer därför en beskrivning av funktionerna utifrån denna indelning.

Därefter vidtar en beskrivning av myndigheternas arbete i dag på informationssäkerhetsområdet. Detta sker med utgångspunkt i varje enskild myndighet och dess verksamhetsområde.

2.2 Administrativa funktioner

På den administrativa sidan har utredningen identifierat följande funktioner: samordning, kompetensförsörjning, tillsyn, informationsspridning, brottsförebyggande verksamhet samt internationell samverkan. En annan viktig funktion är samverkan mellan stat, kommuner, landsting och näringsliv – som utredningen framhållit i det tredje delbetänkandet, Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42).

Funktionerna har ofta någon form av underfunktioner, vilka kan falla inom skilda myndigheters ansvarsområden.

2.2.1 Samordning

Inom funktionen samordning finner vi ledning, sårbarhetsanalys, planering, inriktning, analys av omvärldsutvecklingen och omvärldsbevakning.

KBM är i dag den myndighet som har samordningsuppgifter. Samverkan sker i dag genom formaliserade samverkansorgan i KBM:s regi, till exempel informationssäkerhetsrådet och Samverkansgruppen för informationssäkerhet (Samfi) – där FMV, FRA, KBM, PTS, FM, Statskontoret samt RKP:s och Säkerhetspolisens S-BIT (samordningsfunktionen för brottsrelaterade IT-incidenter) ingår. S-BIT drivs av RKP och Säkerhetspolisen gemensamt och vid Samfis möten representeras S-BIT av en representant från RKP och en från Säkerhetspolisen. RKP är även svensk kontaktpunkt i internationell samverkan inom området IT-relaterad brottslighet.

Ledning

I dag finns ingen som har ett utpekat ansvar för ledning av samordningen av informationssäkerhetsfrågorna. Det framgår emellertid av instruktionen för KBM att myndigheten skall ha ett sammanhållande myndighetsansvar för samhällets

informationssäkerhet genom att sammanställa en helhetsbild av informationssäkerheten.[6]

Sårbarhetsanalys

Sårbarhetsanalys sker i dag inom KBM:s verksamhet. I instruktionen för KBM framgår att KBM inom sitt område skall sammanställa risk- och sårbarhetsanalyser.[7]

Planering

Även planering inryms i KBM:s verksamhet. KBM skall samordna planeringen av åtgärder som stärker beredskapen när det gäller krishantering och civilt försvar.[8] Även om KBM:s uppgifter inom informationssäkerhetsområdet framgår av 5 § i instruktionen för KBM, så har många av de uppgifter som beskrivs i övriga paragrafer en direkt eller indirekt relevans för informationssäkerhetsområdet.

Inriktning

I dag sker ingen övergripande inriktning av informationssäkerhetsarbetet, även om varje myndighet enligt ansvarsprincipen har ett ansvar för sitt utnyttjande av informationstekniken – varje generaldirektör har ansvar för sin myndighet, varje chef har ansvar för sin verksamhet.

Omvärldsbevakning och omvärldsanalys

KBM bedriver strukturerad och kontinuerlig omvärldsbevakning genom inhämtning och bearbetning av material från öppna källor, teknisk inhämtning, nationella kontakter med samhällets aktörer genom formella och informella nätverk samt internationella kontakter. Beträffande de nationella kontakterna finns en önskan om att i högre utsträckning få del av information från underrättelse- och säkerhetsorganisationer, dock inte på annat sätt än vad uppgiftslämnaren avsett, eftersom det utgör

[6] Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten, 5 §.
[7] Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten, 2 § p. 3.
[8] Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten, 3 §.

grundförutsättningarna för att informationsdelning skall fungera. KBM skall i sitt arbete med informationssäkerhetsfrågor analysera omvärldsutvecklingen inom området mot bakgrund av erhållet underrättelseunderlag och årligen lämna en samlad bedömning till regeringen.[9]

PTS utför omvärldsanalys vad gäller elektroniska kommunikationer och redovisar årligen till regeringen läget i sektorn. Utöver denna årliga rapport resulterar arbetet i rapporter om angelägna säkerhetsproblem inom sektorn, till exempel avseende skräppost, spionprogram, phishing, och säkerhetsproblem i samband med IP-telefoni.

2.2.2 Kompetensförsörjning

Under kompetensförsörjning kan insorteras utbildning, forskning, beställarkompetens samt folkbildning. Det är viktigt att kompetens bibehålls och utvecklas även inom kryptologi och signalskydd, vilket behandlas längre fram under teknikkompetens och signalskydd.

Utbildning

Internet är lätt att använda, och dessutom lättillgängligt för många i dagens samhälle. Men användandet medför risker. Därför är det av synnerlig vikt att kunskapen om informationssäkerhetsfrågor höjs på alla nivåer och i alla åldrar. Det gäller från grundskolan över gymnasieskolan och vidare till universitetsnivå och framför allt i lärarutbildningen. I dag är det ingen som har ett övergripande ansvar för utbildning inom informationssäkerhetsområdet.

Forskning

Forskning är en grundförutsättning för att vara förberedd och ligga långt fram inom informationssäkerhetsområdet. Därför är det viktigt att forskning inom området främjas på alla nivåer. Det finns i dag ingen med ett övergripande ansvar för forskning inom informationssäkerhet.

[9] Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten, 5 § p. 1.

Beställarkompetens

Statskontoret har bland annat till uppgift att bistå departement och myndigheter med beställarkompetens, genom sin uppgift att se till att reglerna för den offentliga förvaltningens inköp och användning följs, och att villkoren är så bra som möjligt. På IT-området genomför Statskontoret ramavtalsupphandlingar för den offentliga sektorn. FMV upphandlar IT-komponenter och –system för totalförsvarets räkning. I upphandlingsverksamheten ingår som en väsentlig del att ställa relevanta krav på säkerhet i de produkter och tjänster som upphandlas.

Folkbildning

Det närmaste man kan komma ett ansvar för folkbildning inom informationssäkerhetsfrågor i dag är uppgiften som finns i KBM:s instruktion: att arbeta förebyggande med utbildning och information i informationssäkerhetsfrågor.[10] Folkbildning kan vara ett medel för att uppnå högre informationssäkerhetstänkande hos allmänheten.

PTS har regeringens uppdrag att informera konsumenter, myndigheter och företag om Internetsäkerhet. Myndigheten har utvecklat webbplatser, en interaktiv utbildning och ett verktyg där användarna kan testa sin dator. PTS, KBM, Datainspektionen med flera deltar aktivt i folkbildningskampanjen Surfa lugnt för att få folk att använda Internet på ett säkrare sätt.

Enligt sitt uppdrag skall Sitic samla och sprida information till organisationer och samhället som berör området IT-säkerhet. Sitics råd möjliggör för användarna att minska riskerna för, och konsekvenserna av, IT-incidenter. Detta informationsarbete sker bland annat genom publicering av förebyggande råd på en webbplats, seminarieverksamhet och föreläsningar.

2.2.3 Tillsyn

Tillsyn sker inom områdena säkra nät, integritetsskydd, betalningsväsendet, kvalificerade elektroniska signaturer samt säkerhetsskyddslagen.

[10] Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten, 5 § p. 3.

Säkra nät

PTS har genom lagen (2003:389) och förordningen (2003:396) om elektronisk kommunikation föreskriftsrätt och tillsynsansvar.[11] Lagen föreskriver att de som tillhandahåller allmänt tillgänglig kommunikationstjänst skall vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas, och vidta nödvändiga åtgärder för att upprätthålla detta skydd på nätet.[12] Genom en lagändring som trädde i kraft den 1 juli 2005 har också kraven på god funktion och teknisk säkerhet, samt på uthållighet och tillgänglighet vid extraordinära händelser i fredstid, utvidgats till att gälla all sorts elektronisk kommunikation.

Etablering pågår av ett svenskt säkert nät, SGSI (Svenska statens säkra intranät). Det primära syftet är att åstadkomma en länk mot EU:s säkra nät, TESTA, men också för att kunna användas för kommunikation mellan alla anslutna myndigheter i Sverige för överföring av sekretessklassad information enligt EU:s lägsta sekretessklass (Restreint UE). Statskontoret är produktägare till SGSI och produktion och förvaltning sker i samverkan med de myndigheter som anslutit sig till tjänsten.

Integritetsskydd

Datainspektionen är en förvaltningsmyndighet som har till uppgift att skydda människors privatliv i IT-samhället. Datainspektionen skall följa och beskriva utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik.[13] Datainspektionen ger ut allmänna råd som gäller behandlingen av personuppgifter. Reglerna om personlig integritet i dessa frågor finns i personuppgiftslagen (1998:204).[14] Den som behandlar personuppgifter med hjälp av informationsteknik måste skydda uppgifterna extra noggrant, så att människors personliga integritet inte kränks. Informationstekniken kan leda till att skadan snabbt blir mycket omfattande. Särskilda bestämmelser om integritetsskydd vid elektronisk kommunikation finns i 6 kap. lagen (2003:389) om elektronisk kommunikation. PTS utövar tillsyn i enlighet med lagen.

[11] Lagen (2003:389) om elektronisk kommunikation, 7 kap., förordning (2003:396) om elektronisk kommunikation, 2 § samt förordning (1997:401) med instruktion för Post- och telestyrelsen, 3 § p. 1.
[12] Lag (2003:389) om elektronisk kommunikation, 6 kap. 3 §.
[13] Förordning (1998:1192) med instruktion för Datainspektionen, 1 § 3 st.
[14] Samt i lagen (2003:389) om elektronisk kommunikation, 6 kap., där även förhållandet till PUL klargörs.

Betalningsväsendet

Finansinspektionen övervakar företagen på finansmarknaden och har i uppdrag att bidra till att finanssystemet fungerar effektivt och uppfyller kravet på stabilitet.[15] Finansinspektionen verkar även för gott konsumentskydd i finanssektorn.[16]

Kvalificerade elektroniska signaturer

PTS utövar tillsyn enligt lagen (2000:832) om kvalificerade elektroniska signaturer, samt meddelar föreskrifter enligt förordningen (2000:833) om kvalificerade elektroniska signaturer.[17]

Säkerhetsskyddslagen

Bestämmelser om informationssäkerhet finns i dag i säkerhetsskyddslagen (1996:627). I säkerhetsskyddsförordningen (1996:633) finns närmare bestämmelser om säkerhetsskydd. Av säkerhetsskyddslagens 31 § och säkerhetsskyddsförordningens 39-42 §§ framgår att tillsynsansvaret i dag främst åvilar RPS och Försvarsmakten. FRA bistår i dag RPS och Säkerhetspolisen i arbetet med tillsyn enligt säkerhetsskyddslagstiftningen. Finansieringsfrågan för detta arbete är ej tillräckligt klarlagd i dagens läge.

Regelverk för 24-timmarsmyndigheten

Nämnden för elektronisk förvaltning är den myndighet som har till uppgift att stödja utvecklingen av ett säkert och effektivt elektroniskt informationsutbyte mellan myndigheter samt mellan myndigheter och enskilda. Enligt förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte får nämnden för elektronisk förvaltning meddela föreskrifter i fråga om standarder eller liknande krav som skall vara gemensamma för elektroniskt informationsutbyte för myndigheter under regeringen. Nämnden skall när den meddelar föreskrifter beakta nationell och internationell standard.

[15] Förordning (1996:596) med instruktion för Finansinspektionen, 1 §.
[16] Förordning (1996:596) med instruktion för Finansinspektionen, 2 §.
[17] Förordning (1997:401) med instruktion för Post- och telestyrelsen, 3 § p. 11.

Standarder

I dag finns ingen med övergripande ansvar för statens medverkan i standardiseringsarbetet på informationssäkerhetsområdet. Standarder gäller både administrativa och tekniska rutiner, men ligger i båda fallen till grund för möjligheten att utföra revision av arbetet. Utredningen anser att skapandet av standarder inte är ämnat att likrikta. Det handlar istället om att tillämpa och utveckla standarder som även går att revidera mot.

2.2.4 Informationsspridning

En del av informationsspridningen är att medvetandegöra samhället så att informationssäkerhetsfrågorna finns närvarande som en naturlig komponent i användandet av informationsteknik. Denna verksamhet bedrivs i dag av ett flertal aktörer; RPS genom Säkerhetspolisen, KBM, Konsumentverket och PTS (bland annat genom Sitic) samt FM.

2.2.5 Brottsförebyggande

Den brottsförebyggande verksamheten inom informationssäkerhetsområdet bedrivs av RPS, och då främst av Säkerhetspolisens säkerhetsskyddsenhet och vid den med RKP gemensamma samordningsfunktionen för brottsrelaterade IT-incidenter (S-BIT). Brottsförebyggande verksamhet inom informationssäkerhetsområdet bedrivs även vid RKP:s IT-brottsrotel samt vid Säkerhetspolisen och även i viss omfattning vid landets övriga polismyndigheter.

2.2.6 Internationell samverkan

Utredningen har tidigare slagit fast vikten av internationell samverkan. En hel del arbete bedrivs inom EU för att öka nät- och informationssäkerheten, stärka integriteten samt öka tillgängligheten. En annan del är den samverkan som sker inom ramen för internationell polis- och säkerhetstjänstsamverkan. Problemen med hoten mot informationssystem är i allra högsta grad internationella och därmed en global angelägenhet.

Utredningen har funnit att det svenska deltagandet i internationellt utbyte varit splittrat och inte samordnat i tillräcklig utsträckning. Sverige har ett rykte om hög nivå på informationssäkerhetsområdet. För att Sverige skall ha fortsatt gott genomslag inom området måste den internationella samverkan samordnas.

Utredningen konstaterade i sitt tredje delbetänkande, Säker information - förslag till informationssäkerhetspolitik (SOU 2005:42), att de olika utredningsförslagen innebär att OECD:s riktlinjer implementeras i Sverige.

2.2.7 Samverkan offentligt – privat

Utredningen har tidigare påtalat vikten av samverkan mellan det offentliga och det privata.

2.3 Tekniska funktioner

På den tekniska sidan har utredningen identifierat behov av handhavande av följande funktioner: incidentrapporter, certifiering och evaluering samt teknikkompetens.

2.3.1 IT-incidentrapporter

IT-incidentrapporter hanteras i dag av PTS. IT-incidenter med brottskoppling hanteras inom Polisen och Säkerhetspolisen. PTS fick 2002 i uppdrag av regeringen att inrätta en rikscentral för IT-incidentrapportering, Sitic.[18] Funktionen skall fungera som en rikscentral för IT-incidentrapportering och ha som främsta uppgift att stödja samhället med skydd mot IT-incidenter.

För att förbättra samhällets skydd mot IT-incidenter är omvärldsbevakning och reaktioner på den centralt. I början förelåg problem med att rapporter inte kunde sekretessbeläggas. Efter en lagändring kan emellertid Sitic nu sekretessbelägga incident-rapporter från alla samhällets organisationer. Mörkertalsstudien[19], som genomfördes av Sitic och RKP, indikerar att det huvudsakliga

[18] Regeringsbeslut 2002-05-30, dnr N2002/5443/ITFoU.
[19] Mörkertalsundersökningen 2005 – Svenska organisationer om IT-säkerhetsincidenter, PTS, dnr 05-9152/59.

skälet till att organisationer väljer att inte rapportera till Sitic är att man inte känner till Sitics arbete.

2.3.2 Certifiering och evaluering

Certifiering av granskningsresultat (evalueringsresultat) bedrivs av certifieringsorgan, CB (*Certification Body*).

Certifiering av IT-säkerhet i produkter och system

FMV har fått i uppdrag att upprätta en svensk funktion för certifiering av produkter mot standarden ISO/IEC 15408, evalueringskriterier för IT-säkerhet, även kallad *Common Criteria for Information Security Evaluation*. Denna standard anger hur man kan formulera krav på, deklarera respektive utvärdera realiseringen av erforderliga säkerhetsfunktioner. Enligt uppdraget skall FMV:s funktion ackrediteras av Swedac i enlighet med lagen (1992:1119) om teknisk kontroll.

Certifiering av ledningssystem

Swedac har i enlighet med ovan nämnda lag ackrediterat två privata organ, DNV och SEMKO-DEKRA för certifiering av ledningssystem för informationssäkerhet, LIS. Certifiering sker mot kraven i standarden SS 627799-2. Denna standard håller på att antas som internationell standard, ISO/IEC 27001, *Information Security Management Systems Requirements.*

2.3.3 Teknikkompetens

I funktionen teknikkompetens finner vi signalskydd, teknisk analys och aktiv IT-kontroll.

Signalskydd

Signalskydd är ett av de viktigaste medlen för att uppnå erforderlig informationssäkerhet i känsliga system, och kryptografi är en viktig metod för att erhålla sekretess i ett system.

Försvarsmakten, genom MUST, leder och samordnar i dag signalskyddet inom totalförsvaret. KBM samordnar signalskyddstjänsten inom sitt verksamhetsområde, och FMV har ansvar för att samordna försvarsindustrins behov av signalskydd.

Försvarsmakten ansvarar också för upphandlingen av kryptosystem, inklusive upphandling av utveckling av kryptosystem. Detta arbete sker i samarbete med FRA och FMV. Upphandling av kryptosystem sker av FMV på uppdrag av Försvarsmakten och KBM.

Utredningen har konstaterat att behovet av signalskydd har ökat i samhället, främst beroende av att allt mer information överförs i oskyddade nät. Försvarsmaktens ansvar för signalskyddstjänsten begränsar sig till att tillgodose totalförsvarets krav på att skydda försvarssekretess, enligt Sekretesslagen (1980:100) 2 kap. 2 §. Detta får till följd att viktiga samhällssektorer inte per automatik får tillgång till dessa signalskyddssystem.

I takt med det ökande samarbetet med andra stater och internationella organisationer, främst inom EU, har det uppkommit krav från svenska företag, som vill exportera signalskyddssystem till andra länder, att få dessa signalskyddssystem godkända för användning i Sverige. Ett sådant godkännande är en förutsättning för att företag skall kunna exportera inom EU. Då Försvarsmakten i dag inte har denna roll, utan bara kan godkänna signalskyddssystem för totalförsvaret, kan inte företagen vara med och konkurrera på den europeiska marknaden.

Försvarsmakten har också ansvaret för att bedriva signalskyddsutbildning inom totalförsvaret. Det sker i dag vid Totalförsvarets signalskyddsskola (TSS), som är en del av Försvarsmakten Upplands Regemente, S1. KBM köper utbildning av Försvarsmakten för det behov som de civila myndigheterna har.

I dag finns ingen organisation formellt utpekad som ansvarig för signalskyddsfrågor, så kallad National Communications Security Authority (NCSA). Det finns inte heller någon formellt utpekad som behörig att distribuera kryptonycklar, så kallad National Distribution Authority (NDA). För närvarande utförs detta arbete i praktiken av Försvarsmakten.

Aktiv IT-kontroll

Aktiv IT-kontroll med sanktionerade intrångsförsök utförs av FRA. Aktiv IT-kontroll är ett effektivt medel för en organisation att få behovet av informationssäkerhet tydliggjort.

Teknisk analys

Teknisk analys omfattar, utöver aktiv IT-kontroll, även bland annat tekniskt stöd vid kriminalteknisk analys, kodgranskning, teknisk rådgivning, evalueringsarbete, tekniskt arbete med standarder, internationellt tekniksamarbete med mera, samt den administrativa analys som krävs för fullgörandet av andra delar av teknisk analys.

I dag har FRA i uppdrag att utföra teknisk analys, enligt sin instruktion.[20] Dessutom tillhandahåller en del privata aktörer tjänster på området.

2.4 Myndigheterna

Enligt ansvarsprincipen är alla myndigheter ansvariga att tillse att de har en tillräcklig informationssäkerhet inom sin verksamhet. Vissa myndigheter arbetar mer direkt med informationssäkerhetsfrågor än andra. I Samhällets säkerhet och beredskap (prop. 2001/02:158) fördelade regeringen nya uppgifter inom informationssäkerhetsområdet på främst fyra utpekade myndigheter. FMV, FRA, KBM samt PTS tilldelades ansvar inom verksamhetsområdena system för evaluering och certifiering, teknikkompetens, omvärldsanalys samt IT-incidenthantering. Regeringen anmälde i samma proposition att en utvärdering skulle ske efter två år. I ett tilläggsdirektiv (dir. 2004:46) fick InfoSäkutredningen (Fö 2002:6) i uppdrag att genomföra denna utvärdering.

Bland övriga myndigheter inom informationssäkerhetsområdet finns RPS, Försvarsmakten, FHS och Statskontoret. Datainspektionen och Finansinspektionen har ett visst tillsynsansvar på området. Även Konsumentverket kommer i kontakt med informationssäkerhetsfrågor, i sitt arbete med att tillvarata konsumenternas intressen. Liknande uppgifter har Finansinspektionen.

Nedan följer en genomgång av deras arbete på området i dag.

[20] Förordning (1994:714) med instruktion för Försvarets radioanstalt, 3 a §.

2.4.1 Rikspolisstyrelsen

Inom RPS är det främst Säkerhetspolisen som arbetar med informationssäkerhetsfrågor. En del arbete bedrivs även av RKP genom S-BIT som är RKP:s och Säkerhetspolisens samordningsfunktion för brottsrelaterade IT-incidenter.

Eftersom Polisen har en rättsvårdande funktion är det av vikt att skilja de rättsvårdande uppgifterna från informationssäkerhetsfrågorna.

RKP utgör även Sveriges kontaktpunkt inom G8:s 24/7-kontaktnät. Det innebär att när någon inom G8-nätverket vill komma i kontakt med Sveriges rättsvårdande myndigheter i samband med IT-relaterade incidenter kan de göra det under veckans alla dagar och dygnets alla timmar. RKP utgör även Sveriges kontaktpunkt för Interpols kontaktnät NCRP (National Central Reference Point). Skillnaden mellan G8:s 24/7-nätverk och NCRP är att Interpol inte har krav på beredskap dygnet runt.

RPS utövar tillsyn enligt säkerhetsskyddsförordningen (1996:633) och kontrollerar då säkerhetsskyddet när det gäller Kustbevakningen (KBV), KBM, Statens räddningsverk (SRV), Styrelsen för psykologiskt försvar (SPF) och övriga myndigheter, utom Justitiekanslern (JK) och de som Försvarsmakten utövar tillsyn över enligt samma förordning.[21]

2.4.2 Försvarsmakten

Försvarsmakten leder och samordnar signalskyddstjänsten inom totalförsvaret.[22] I det arbetet ansvarar Försvarsmakten för utveckling och godkännande av signalskyddssystem, produkter och distribution av signalskyddsnycklar samt kontroll och uppföljning av verksamheten. Försvarsmaktens ansvars- och tillsynsområde enligt säkerhetsskyddsförordningen (1996:633) omfattar FHS, FMV, FOI, FRA, Fortifikationsverket samt Pliktverket.[23] Dessutom utövar Försvarsmakten Totalförsvarets CA (Certificate Authority) för PKI-funktioner (Public Key Infrastructure).

Övervakning av Försvarsmaktens egna nät sker genom FM CERT. Övervakningen inriktas på att säkerställa sekretess, tillgänglighet, riktighet och spårbarhet.

[21] Säkerhetsskyddsförordning (1996:633), 39 §.
[22] Förordning (2000:555) med instruktion för Försvarsmakten, 4 § p. 3.
[23] Säkerhetsskyddsförordning (1996:633), 39 §.

Enligt sin instruktion lämnar Försvarsmakten även stöd till Regeringskansliet avseende signalskyddstjänst.[24]

Inom signalskyddsområdet och IT-säkerhetsområdet tillhandahåller Försvarsmakten även signalskydds- och säkerhetslösningar för EU:s rådssekretariat, samt utbyter information bilateralt.

Försvarsmakten utövar i praktiken rollen som NCSA (National Communications Security Authority) genom MUST Säkerhetskontor, men något formellt beslut i frågan har inte tagits.

Försvarsmakten är en myndighet som hanterar stor mängd sekretessbelagt material på totalförsvarets område, och således har stora behov av kvalificerade informationssäkerhetslösningar. En del av hotbilden mot Försvarsmakten och dess tillsynsmyndigheter på informationssäkerhetsområdet utgörs av främmande länders underrättelse- och signalspaningstjänst. Detta hot har medfört att Försvarsmakten under lång tid har utvecklat en god kompetens avseende informationssäkerhet. Utvecklingen med att ta fram kvalificerade IT-säkerhets och –kryptolösningar har bland annat skett med stöd av FRA och FMV. Försvarsmakten utvärderar också IT-säkerhets- och kryptolösningar för att kunna använda resultatet såväl internt som hos tillsynsmyndigheterna.

Vidare har Försvarsmakten ansvar för att bedriva signalskyddsutbildning inom totalförsvaret vid Totalförsvarets signalskyddsskola (TSS), som är en del av Upplands regemente, S1, i Enköping.

För att möta en helhetssyn inom informationssäkerhetsområdet omorganiserades de delar av MUST som hanterar såväl administrativa som tekniska informationssäkerhetsfrågor till MUST Säkerhetskontor den 1 februari 2005. Detta för att erhålla synergi i hur IT-säkerhet inklusive signalskydd tillsammans med administrativa regler, kontrollinstrument och hotbildsanalys samverkar för att kunna möta varierande hotbilder och förutsättningar.

Inom Försvarsmakten är det chefen för MUST som är ansvarig för informationssäkerhetsfrågor.

2.4.3 Försvarets materielverk

FMV fick i uppdrag att bygga upp ett system för certifiering av IT-säkerhetsprodukter inom ramen för Common Criteria Recognition Agreement (CCRA) i enlighet med proposition 2001/02:158

[24] Förordning (2000:555) med instruktion till Försvarsmakten, 4 §.

Samhällets säkerhets och beredskap. CCRA är en samverkan mellan för närvarande tjugo nationer där det övergripande målet är att höja den nationella säkerheten genom att använda Common Criteria som ett verktyg för kravställning och granskning.

FMV leder sedan fem år arbetet inom den internationella standardiseringsgrupp som ansvarar för bland annat *Common Criteria.*

FMV:s certifieringar, liksom de som utförs av eventuella andra svenska certifieringsorgan, skall med hjälp av detta system kunna erkännas internationellt. En av huvuduppgifterna är att utfärda certifikat för IT-produkter baserade på Common Criteria, den internationella standarden Kriterier för utvärdering av IT-säkerhet (IS 15408). FMV kommer inom kort att söka ackreditering som certifieringsorgan, CB (Certification Body). Ackrediteringen sker genom Swedac.

Att bygga upp ett system för certifiering och evaluering är en krävande process. Även om man tar det i beaktande, konstaterar utredningen att arbetet dragit ut på tiden. FMV hade inledningsvis en del problem som påverkat möjligheterna att genomföra uppdraget. Ansvars- och rollfördelningen mellan Swedac och FMV har varit föremål för långa diskussioner. Myndigheterna har olika syn på vem som skall göra vad i förhållande till CCRA. Detta har inneburit att de andra medlemsländerna har ställt sig undrande till vem som är ansvarig och vem som utgör certifieringsorgan i Sverige.

2.4.4 Försvarets radioanstalt

FRA har i uppdrag att genomföra IT-säkerhetsanalyser.[25] FRA skall ha hög teknisk kompetens inom informationssäkerhetsområdet och får efter begäran stödja sådana statliga myndigheter och statlig ägda bolag som hanterar information som bedöms vara känslig ur sårbarhetssynpunkt eller ur ett säkerhets- eller försvarspolitiskt avseende.[26] Detta mandat gäller endast myndigheter och statligt ägda bolag som bedriver samhällsviktig verksamhet. Det innebär att samhällsviktig verksamhet som bedrivs av privata företag inte kan omfattas. Till exempel kan FRA stödja Vattenfall men inte Sydkraft.

[25] Förordning (1994:714) med instruktion för Försvarets radioanstalt, 3 a § p. 3.
[26] Förordning (1994:714) med instruktion för Försvarets radioanstalt, 3 a § st. 1.

FRA har ett ansvar att tillgodose signalskyddsverksamheten med kryptologisk kompetens.

FRA:s uppdrag att skapa en teknikkompetensfunktion inom informationssäkerhetsområdet har lett till att FRA i dag har en enhet för Teknisk Informationssäkerhet och en grupp för forskning och utveckling inom informationssäkerhetsområdet.

Statens behov av en resurs med hög teknisk kompetens inom IT-säkerheten slogs fast av Sårbarhets- och säkerhetsutredningen.[27] Regeringen angav i Samhällets säkerhet och beredskap (prop. 2001/02:158) att teknikfunktionen vid FRA inte bör uppträda på konkurrensutsatta marknader, men att staten har ett ansvar för att säkerställa att denna sorts kompetens finns att tillgå på nationell nivå. Den ökade efterfrågan på FRA:s tjänster, tillsammans med dess uppbyggda kompetens, har aktualiserat konkurrensfrågor på senare tid. FRA har kompletterat sin verksamhet med säkerhetsanalyser och förmåga att även leverera tjänster inom administrativ informationssäkerhet. Det föreligger oklarhet kring vad som kan anses innefattas i uppdraget till FRA.

FRA bistår Säkerhetspolisen i tillsynen enligt säkerhetsskyddslagstiftningen.[28] Finansieringsfrågan är i dag inte tillfredsställande löst.

2.4.5 Krisberedskapsmyndigheten

Enligt förordning (2002:528) med instruktion för Krisberedskapsmyndigheten har KBM givits en form av sammanhållande ansvar för frågor på informationssäkerhetsområdet.[29] KBM har inrättat en samverkansgrupp för informationssäkerhet (Samfi), där förutom KBM även FRA, FMV och PTS deltar tillsammans med Försvarsmakten, Statskontoret samt RPS och Säkerhetspolisen genom S-BIT. KBM samverkar även med liknande myndigheter i andra länder och utgör Sveriges internationella kontaktpunkt för informationssäkerhetsfrågor inom myndighetens ansvarsområde.[30]

Myndigheten KBM inrättades i juli 2002. En särskild enhet för informationssäkerhetsfrågor inrättades emellertid först i maj 2003. KBM verkar endast i begränsad utsträckning ha påbörjat

[27] SOU 2001:41 Säkerhet i en ny tid, s. 205.
[28] Säkerhetsskyddslagen (1996:627) och Säkerhetsskyddsförordningen (1996:633).
[29] Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten, 5 §.
[30] Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten, 9 §.

verksamheter som syftar till att tillgodose de förändringsbehov som identifierats. Informationssäkerhetsfrågorna är synnerligen viktiga men har inte alltid fått den prioritet som är motiverat av frågans allvar. Varken KBM eller någon annan myndighet har emellertid fått något utpekat ansvar för ledning av samordningen av informationssäkerhetsfrågorna, vilket i vissa sammanhang utgör ett problem.

KBM bedriver omvärldsbevakning samt analys av omvärldsutvecklingen. Genom att sammanställa risk- och sårbarhetsanalyser samt inhämtning från andra öppna källor lämnar myndigheten en årlig lägesbedömning på informationssäkerhetsområdet till regeringen.[31]

Ytterligare en uppgift för myndigheten är att utveckla samarbetet mellan stat och näringsliv.

KBM har utvecklat en teknisk rekommendation med enkla råd – BITS (basnivå för IT-säkerhet). BITS används bland annat av länsstyrelser, kommuner och landsting i arbetet med att vidareutveckla IT-säkerheten.

2.4.6 Post- och telestyrelsen och Sitic

Inom informationssäkerhetsområdet har PTS ett ansvar som bland annat följer av lagen (2003:389) om elektronisk kommunikation. Det gäller till exempel krav på god funktion och teknisk säkerhet samt integritetsskydd i elektronisk kommunikation (till exempel telefoni, mobiltelefoni och Internet). Myndigheten arbetar för att göra näten mer robusta och för att förhindra att system slås ut vid störningar. PTS utreder och informerar även om säkerhet på Internet och andra säkerhetsproblem.

PTS fick av regeringen i uppdrag att bilda en rikscentral för IT-incidentrapportering. Sitic (Sveriges IT-incidentcentrum) har som främsta uppgift att stödja samhället i arbetet med skydd mot IT-incidenter. Arbetet sker genom ett system för informationsutbyte om IT-incidenter mellan samhällets organisationer och Sitic. Sitic sprider information om nya problem som kan störa IT-system. Centrumet ger råd om förebyggande åtgärder och sammanställer statistik.

Sitic har en omfattande omvärldsbevakning och en övervägande del av den är operativ. Utifrån hitintills insamlad erfarenhet har ett informationsinsamlingssystem skapats. Uppbyggda relationer med

[31] Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten, 2 §.

individer, organisationer och samlingsorganisationer – nationellt och internationellt – har varit av stor vikt för att få tillgång till förstahandsinformation. Det väsentliga från omvärldsbevakningen publiceras i första hand på Sitics webbplats och via e-post till anmälda prenumeranter.

Utredningen kan konstatera att inrapporteringen av incidenter till Sitic hittills har varit låg. Företag och organisationer känner inte till Sitic och har inte mekanismer för intern rapportering av IT-incidenter. Kunskapen om möjligheten att sekretessbelägga information om incidenter är inte spridd.

En erfarenhet från Sitics arbete visar dock att tidig identifiering av risker, via omvärldsbevakning, ofta är viktigare än efterhandsanalyser av incidenter för att förebygga IT-incidenter.

2.4.7 Statskontoret

Statskontoret har hittills haft flera uppgifter som har betydelse för utredningens överväganden och förslag. Myndigheten skall enligt sin instruktion samordna arbetet med den fredstida informationssäkerheten för den civila statsförvaltningen under regeringen.[32] I praktiken har informationssäkerhetsarbetet i första hand inriktats på förändringsarbetet i offentlig sektor samt att åstadkomma tillgång till produkter och tjänster, genom uppgiften inom ramen för IT-upphandling. Detta har också omfattat upphandling av säkerhetsprodukter som möjliggjort utvecklingen av myndigheternas e-tjänster, till exempel e-legitimation och spridning och hämtningssystem (SHS).

Statskontoret har möjlighet att påverka upphandlingen av till exempel utrustning och program genom sin uppgift att se till att villkoren för den offentliga förvaltningens inköp och användning av utrustning och tjänster på informationsområdet är så bra som möjligt. På IT-området genomför Statskontoret ramavtalsupphandlingar för den offentliga sektorn. I upphandlingsverksamheten ingår som en väsentlig del att ställa relevanta krav på säkerhet i de produkter och tjänster som upphandlas.

Statskontoret har i sitt arbete med vägledning för bland annat 24-timmarsmyndigheterna också utarbetat rekommendationer för styrning av informationssäkerhet i enlighet med LIS, och med det

[32] Förordning (1992:877) med instruktion för Statskontoret, 2 § p. 2.

som grund även deltagit i det nationella och internationella standardiseringsarbetet med inriktning på LIS.

Vidare skall myndigheten stödja övriga myndigheters arbete med bland annat sekretessen i allmänna handlingar som hanteras i IT-system enligt sekretesslagen (1980:100) 15 kap. 9 §. Statskontoret ansvarar också för kansliet för Nämnden för elektronisk förvaltning.

2.4.8 Datainspektionen

Datainspektionen är en förvaltningsmyndighet som har till uppgift att skydda människors privatliv i IT-samhället.[33] Myndigheten har även uppgifter med anledning av personuppgiftslagen (1998:204),[34] för att säkerställa att den personliga integriteten skyddas i sammanhang där informationsteknik används för att behandla personuppgifter.

2.4.9 Finansinspektionen

Finansinspektionen har fått skarpare resurser och förstärkt mandat att utöva tillsyn både vad gäller finansmarknaden, värdepapper och försäkringsmarknaden. Finansinspektionen övervakar företagen på finansmarknaden och har uppdrag att bidra till att finanssystemet fungerar effektivt och uppfyller kravet på stabilitet.[35] De skall även verka för gott konsumentskydd i finanssektorn.

2.4.10 Konsumentverket

Konsumentverket arbetar bland annat med att ta tillvara konsumenters intressen i förhållande till IT-marknaden. De ger bland annat råd om e-handel, modemkapning och bredband, tar emot anmälningar om oönskad e-postreklam och ger tips om att använda Internet på ett säkert sätt samt ger råd och bistår de som blivit lurade på nätet.

[33] Förordning (1998:1192) med instruktion för Datainspektionen, 1 §.
[34] Personuppgiftsförordningen (1998:1191).
[35] Förordning (1996:596) med instruktion för Finansinspektionen.

2.4.11 Swedac

Styrelsen för ackreditering och teknisk kontroll (Swedac) ackrediterar laboratorier och certifierings- och kontrollorgan enligt lagen (1992:1119) om teknisk kontroll. Ackreditering föregås av insyning av organet mot kraven i tillämplig internationell standard. Swedac har i regel inte ansvar för de regelverk som organen certifierar eller kontrollerar mot.

3 Utgångspunkter för organisation av informationssäkerhetsarbetet

Såväl offentliga organ, företag som privatpersoner är beroende av fungerande IT och säker information. Att det är olika typer av aktörer som berörs gör informationssäkerhetsarbetet komplicerat, men ger också möjligheter till fruktbärande samverkan.

Utredningen har i tidigare betänkanden pekat på de stora samberoenden som finns och den stora dynamik som bestämmer utvecklingen inom informationssäkerhetsområdet.

I det tredje delbetänkandet Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42), redovisade utredningen ett antal förslag till åtgärder som på kort och lång sikt skulle förbättra informationssäkerheten i Sverige och därigenom bidra till bland annat tillväxt, konkurrens och ge förutsättningar för ökad delaktighet och utvecklad demokrati. Utredningen redovisade förslag till hur regeringens strategi för informationssäkerhet kan utvecklas. Vidare lämnades förslag till vad som bör falla inom det privata åtagandet och vad som skulle kunna betraktas som det statliga åtagandet, även om gränsdragningen är svår.

Utvecklingen av den övergripande strategin sammanfattas i tio punkter som innefattar att:

1. utveckla Sveriges position inom EU och i internationella sammanhang
2. skapa förtroende, trygghet, säkerhet, och öka integritetsskyddet
3. främja ökad användning av IT
4. förebygga och kunna hantera störningar i informations- och kommunikationssystem
5. förstärka underrättelse- och säkerhetstjänstens arbete samt utveckla delgivningen
6. förstärka förmågan inom området nationell säkerhet

I strategin bör även ingå att:

7. utnyttja samhällets samlade kapacitet
8. fokusera på samhällsviktig verksamhet

9. öka medvetenheten om säkerhetsrisker och möjligheter till skydd
10. säkerställa kompetensförsörjningen

Den av utredningen föreslagna utvecklingen av regeringens strategi bör leda till organisatoriska konsekvenser. Detta följer av behovet att förstärka underrättelse- och säkerhetstjänsternas informationssäkerhetsarbete respektive att förstärka förmågan inom området nationell säkerhet med avseende på informationssäkerhet. Båda dessa områden förutsätter tydlig ansvarsfördelning och säkerställande av kompetens och resurser. Vidare bör den utvärdering som utredningen har gjort av de av regeringen beslutade organisatoriska förändringarna för att etablera funktionerna omvärldsanalys, incidenthantering, teknikkompetens samt evaluering och certifiering få organisatoriska konsekvenser. Slutligen bör den av utredningen föreslagna strategin att förebygga, förbereda inför, förhindra, upptäcka, hantera och ingripa vid störningar i några fall leda till justeringar inom nuvarande organisationer. Dessutom kan förutses att dessa uppgifter i några fall bör preciseras och införas i berörda myndigheters instruktioner.

Det statliga åtagandets omfattning leder till krav på att bygga upp förmåga inom flera viktiga områden och att lösa ett antal uppgifter i den statliga verksamheten. Långt ifrån alla krav eller uppgifter är dock direkt beroende av hur staten organiserar sin verksamhet. Informationssäkerhetsarbetet måste, som utredningen påpekar, utgöra en integrerad del av alla aktörers verksamheter, så också inom staten. Detta följer av ansvarsprincipens tillämpning. Det återstår därför att formulera uppdrag och uppgifter till myndigheter i den befintliga organisationsstrukturen i syfte att öka säkerheten. Utredningen har därför i delbetänkande 3, Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42) redovisat förslag till handlingsprogram.

Samtidigt har utredningen konstaterat att informationssäkerheten inte bara inrymmer frågeställningar för respektive verksamhetsansvarig utan att det också finns gemensamma behov och problem av tvärsektoriell natur. Dessa båda frågeställningar förutsätter ett annat angreppssätt på styrning och organisation och att gränsdragningen mellan det offentliga och privata åtagandet måste tydliggöras.

Dessutom finns det, som utredningen redovisar under avsnittet offentlig-privat samverkan, sannolikt frågeställningar som inte kan lösas av en aktör ensam, inte ens av staten. En fördjupad samverkan

inom offentlig sektor och mellan offentliga och privata aktörer förutsätter därför en tydlig ansvarsfördelning inom staten och en organisation som kan hantera frågor av gemensam respektive tvärsektoriell natur, i en vardag präglad av sektorstänkande och sektorsansvar.

Statens åtagande, ansvar och intresse har av utredningen sammanfattats enligt följande:

1. Staten har ett övergripande ansvar för att en helhetssyn etableras och appliceras på informationssäkerheten och att nationella intressen bevakas genom EU och i internationella sammanhang.
2. Staten har ansvaret för samhällets regelverk på informationssäkerhetsområdet.
3. Staten har ett särskilt ansvar för informationssäkerheten inom ett antal politikområden. Det gäller statens kärnverksamhet, som till exempel rättsväsendet. Det gäller även ansvaret för att olika samhällsviktiga verksamheter bedrivs med tillräcklig säkerhet oavsett vem som äger dem (till exempel elförsörjning och telekommunikation).
4. Staten har slutligen ett eget intresse för informationssäkerheten inom sitt verksamhets- och ansvarsområde, i sina olika roller som till exempel ansvarig för myndighetsutövning och i sin ägarroll.

Enligt utredningens uppfattning bör samtliga dessa åtaganden leda till organisatoriska konsekvenser.

Till detta skall fogas de organisatoriska konsekvenser som följer av den av utredningen föreslagna utvecklingen av regeringens strategi.

Utredningen har i sina direktiv fått i uppgift att genomföra en utvärdering av de fyra myndigheter som gavs uppgifter inom informationssäkerhetsområdet i enlighet med det som regeringen anmälde i Samhällets säkerhet och beredskap (prop. 2001/02:158). Den rapport som FOI redovisade på uppdrag av utredningen,[36] samt de egna kontakter som utredningen har haft med berörda myndigheter utgör en viktig grund för de ställningstaganden som utredningen gör.

En organisatorisk fördelning av uppgifter på området måste vara tillräckligt flexibel och långsiktig för att kunna klara den utmaning som teknisk utveckling innebär samt fluktuerande belastning av funktionerna.

I tidigare betänkanden har utredningen pekat på ett antal förhållanden och synsätt som kan vara vägledande för

[36] Underlag för utvärdering av uppgiftsfördelning inom informationssäkerhetsområdet, Barck-Holst, Fischer och Lewerentz, FOI-R-1369-SE, November 2004, ISSN 1650-1942.

informationssäkerhetsarbetet. I föreliggande kapitel presenterar utredningen de utgångspunkter som ligger till grund för hur detta arbete bör organiseras.

Olika utgångspunkter för val av organisation

Den organisatoriska modell som gäller i dag formulerades som svar på ett starkt behov av ett samordnat statligt informationssäkerhetsarbete (prop. 2001/02:158 Samhällets säkerhet och beredskap). Flera funktioner saknades helt och fick byggas upp från grunden. Samtidigt behövde ett fungerande informationssäkerhetsarbete snabbt komma igång. Fyra funktioner skapades för att fungera under de förutsättningar som rådde då, såväl organisatoriska som tekniska. I dag har utvecklingen gått framåt och regeringen har gett utredningen i uppdrag att genomföra en utvärdering och vid behov komma med förslag till alternativ organisering. Utredningen har därvid funnit att nuvarande organisatoriska modell behöver modifieras i vissa avseenden för att bättre möta dagens krav på informationssäkerhet. Samverkan mellan de olika funktionerna måste bli bättre då de är delar av en helhet och till del beroende av varandra. Uppgifterna måste vara tydliga och väl avgränsade för att undvika kraftsplittring och överlappande arbete. Oklarheter måste undanröjas och genomförandefrågor hamna i fokus så att avsett resultat kan uppnås. Om nuvarande organisationsstruktur i stort bevaras, med marginella eller inga förändringar, tas arbete och erfarenhet till vara. Å andra sidan cementeras även de aspekter av arbetet som fungerar mindre bra.

Ett alternativt sätt att hantera informationssäkerhetsfrågorna är att samla alla funktioner som behövs under en och samma myndighet. Detta skulle kunna medföra korta beslutsvägar och goda möjligheter till korsbefruktning mellan funktioner som är avhängiga varandra. En sådan lösning skulle även skapa en självklar arena för olika typer av informationssäkerhetsfrågor och på så sätt minska risken för att ärenden inte behandlas bara för att de inte har någon naturlig organisatorisk hemvist. Att samla alla aspekter av informationssäkerhet under ett tak skulle innebära ett mycket stort organisatoriskt ingrepp då informationssäkerhetsrelaterade funktioner i dag är spridda på ett antal aktörer. Förväntade gynnsamma effekter skulle inte uppstå omedelbart. Det är till och

med sannolikt att en temporär minskning av effektiviteten i arbetet skulle uppstå.

Om däremot varje sektorsmyndighet ansvarade för informationssäkerheten inom sitt ansvarsområde, utan en gemensam, sammanhållande stödfunktion, skulle överlappande och sammanfallande uppgifter bli en nödvändig konsekvens. Denna lösning är enligt utredningens mening inte att föredra. Ansvarsprincipen innebär förvisso att varje aktör har ansvar för sin informationssäkerhet och utredningen har vid flertalet tillfällen förordat att så även fortsättningsvis skall vara fallet. Dock har staten det övergripande ansvaret, för till exempel sådana funktioner som rimligen inte kan lastas den enskilde, oavsett om det gäller ett företag eller en myndighet.

Utredningen presenterade i sitt tredje betänkande Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42), i anslutning till strategi för informationssäkerhet, ett handlingsprogram. De förslag till åtgärder som där läggs fram kan till del uppfyllas i en uppsättning funktioner. Utredningen har konstaterat att de funktioner som är viktiga eller till och med nödvändiga för ett gott informationssäkerhetsarbete i stor utsträckning redan finns. Däremot kan funktionerna i vissa fall behöva utvecklas, förstärkas och/eller sammanföras.

Utredningen har konstaterat att informationssäkerheten inte bara inrymmer frågeställningar för respektive verksamhetsansvarig utan att det också finns behov av gemensam natur, där stora krav ställs på samordning. Vidare finns flera frågeställningar av tvärsektoriell karaktär, som ofta kräver tillgång på specialistkompetens. Dessa frågeställningar förutsätter ett annat angreppssätt på styrning och organisation än det traditionella sektorstänkandet. Det förutsätter vidare att gränsdragningen mellan det offentliga och privata åtagandet måste tydliggöras.

Till dessa resonemang kan läggas att informationssäkerheten kräver tillgång till hög kompetens och resurser, såväl administrativt som tekniskt. Som liten nation är det av synnerlig vikt för Sverige att regeringen fokuserar de resurser som finns tillgängliga och utnyttjar samhällets samlade kapacitet på ett bättre sätt.

I tidigare betänkanden har utredningen pekat på ett antal förhållanden och synsätt som kan vara vägledande för informationssäkerhetsarbetet. Några av dessa är särskilt viktiga för val av organisation inom staten:

1. Informationssäkerhet omfattar hela samhället och frågeställningen är därför vidare än totalförsvarets behov.

2. Det finns ett behov att kraftsamla och att tydligare fokusera den statliga verksamheten nationellt, inom EU och internationellt.
3. Alla statliga aktörer måste, inom ramen för sitt respektive sektorsansvar, medverka till förmågan att förebygga, förbereda inför, förhindra, upptäcka, hantera och ingripa vid störningar.
4. Ansvaret för förmågan i den statliga kärnverksamheten, liksom för säkerheten i samhällsviktiga verksamheter, måste tydliggöras. Vissa gemensamma behov förutsätter bättre samordning inom staten och i samverkan med andra, icke-statliga aktörer.
5. Kompetensen och förmågan att hantera tvärsektoriella frågor måste säkerställas inom informationssäkerhetsområdet.

Den första organisationsprincipen följer av ansvarsprincipen. Detta innebär att varje sektorsmyndighet har ansvaret för utvecklingen av informationssäkerheten inom sitt ansvarsområde och i relation till de aktörer som berörs av myndighetens verksamhet. I syfte att tydliggöra omfattningen av detta ökade ansvar har utredningen i det tredje delbetänkandet lämnat ett förslag till förordning om vissa åtgärder för informationssäkerhet i den statliga verksamheten.[37] Inom några områden finns det enligt utredningens mening anledning att ytterligare tydliggöra och förstärka detta ansvar och uppdrag. PTS utökade ansvar och befogenheter inom området elektronisk kommunikation är ett sådant exempel. Finansinspektionens samverkan med aktörer inom finansmarknaden är ett annat. I andra fall kan det handla om att ge ökad prioritet och lyfta upp säkerhetsfrågorna i berörda myndigheters verksamhet och förstärka insatserna, till exempel inom energi- och transportsektorerna.

Den andra organisationsprincipen syftar till att tillgodose sådana behov som är gemensamma i den statliga verksamheten. Detta syftar framförallt till att uppnå en bättre samordning inom staten i administrativa och tekniska sammanhang.

Den tredje organisationsprincipen syftar till att säkerställa kompetens och förmåga att hantera tvärsektoriella frågeställningar i hela samhället, vare sig det handlar om att kunna hantera och ingripa vid störningar eller att ge underlag för förebyggande arbete hos alla aktörer.

[37] SOU 2005:42 Säker information – Förslag till informationssäkerhetspolitik, s. 31 ff.

Administrativa respektive tekniska frågeställningar

Det finns flera olika aspekter av och sätt att se på åtgärder inom informationssäkerhetsområdet. Utredningen har i tidigare betänkande pekat på en vanligt förekommande indelning i administrativa respektive tekniska frågeställningar. Denna indelning återfinns också i de grundläggande definitioner som finns inom informationssäkerhetsområdet och som utredningen tidigare har anslutit sig till. Utredningen är medveten om att begreppet ”administrativ” i vissa sammanhang kan uppfattas som liktydigt med byråkratiska, förvaltningsmässiga åtgärder. Som framgår av de definitioner som återfinns i SIS-handboken inryms dock många aspekter av informationssäkerhetsarbete i begreppet administrativ. Då det har visat sig svårt att finna ett bättre begrepp har utredningen valt att använda denna indelning i resonemangen om vilka principer som bör ligga till grund för organisation av informationssäkerhetsarbetet i den statliga verksamheten.

Utredningens syn på vad som bör ingå i den administrativa respektive tekniska funktionen utvecklas närmare i avsnitten 3.1 och 3.2.

Utredningen har även övervägt och prövat möjligheten att använda indelningen i administrativa respektive tekniska frågeställningar som grundläggande organisatoriskt angreppssätt för att fokusera och kraftsamla den statliga organisationen. Tillsammans med förslaget till en mer utvecklad samverkan mellan privat och offentlig sektor skulle således en kraftsamling till en administrativ respektive en teknisk organisation (eller funktion) lägga grunden för en bättre ansvars- och arbetsfördelning inom staten.

Behov av förändringar inom befintliga organisationer

Som utredningen tidigare framhållit leder det statliga åtagandet till krav på att bygga upp förmåga inom flera viktiga områden och att lösa ett antal uppgifter i den statliga verksamheten. Långt ifrån alla krav eller uppgifter är dock direkt beroende av hur staten organiserar sin verksamhet. Inom några områden kan det som utredningen redan påpekat finnas anledning att ytterligare tydliggöra vissa myndigheters ansvar och uppdrag. I andra fall kan det handla om att ge ökad prioritet och lyfta upp informationssäkerhetsfrågorna i berörda myndigheters verksamhet

och förstärka insatserna. Utredningen redovisar detta under kapitel 4.

Samverkan mellan privat och offentlig sektor

Enligt utredningen finns det problemställningar som är av sådan art att ingen av aktörerna ensam kan leverera lösningar. Följaktligen finns behov av att samverka för att identifiera och komma närmare lösningar på dessa. Det finns dessutom skäl att söka samverkan kring de prioriteringar som måste göras mellan olika problem och sektorer, i syfte att utnyttja tillgänglig kompetens och resurser på ett optimalt sätt. Under avsnitt 3.3 redovisar utredningen förslag till fortsatt arbete. Vidare bör staten samordna sina egna intressen inför en sådan fördjupad samverkan. Detta bör enligt utredningen ske genom att en myndighet ges uppgiften att initiera samverkan mellan statliga myndigheter och privat sektor samt svara för den nödvändiga samordningen mot övriga aktörer.

Regeringens ledande och samordnande roll

Regeringen har en ledande och samordnade roll inom informationssäkerhetspolitiken. Det sätt som regeringen väljer att sätta mål, styra och följa upp resultat är avgörande för myndigheternas arbete. Inom informationssäkerhetsområdet är det av särskild vikt med hänsyn till frågornas komplexitet, dynamik och internationella dimension. Utredningen har därför i det tredje delbetänkandet pekat på vikten av en sammanhållande målstruktur för informationssäkerhetsarbetet.

3.1 Administrativa funktioner

Utredningen kan konstatera att regeringens strategi bör ligga fast i fråga om en funktion för omvärldsanalys. Den bör dock utvidgas i vissa avseenden, som utvecklas närmare under avsnitt 3.3.1.

Utredningen har funnit aspekter av informationssäkerhet som behöver förstärkas och inordnas under de funktioner som finns idag. Detta gäller behovet av samordning av informationssäkerhetsarbetet nationellt och internationellt (avsnitt 3.1.3), liksom ett sammanhållande ansvar för kompetensfrågorna

(avsnitt 3.1.4) och frågor som rör standarder och revision (avsnitt 3.1.5).

3.1.1 Omvärldsbevakning och omvärldsanalys

Staten har, som utredningen har påpekat vid ett flertal tillfällen i tidigare betänkanden, Informationssäkerhet i Sverige och internationellt – en översikt (SOU 2004:32), och Säker information – förslag till informationssäkerhetspolitik (SOU2005:42), det sammanhållande ansvaret för informationssäkerhetsarbetet i samhället. För detta krävs att en bild av informationssäkerhetsläget, med hjälp av statistik och annan information, löpande tas fram och hålls uppdaterad. Omvärldsbevakning innebär insamlandet av information på området och analys är en bearbetning av detta underlag. Omvärldsanalys kan i stor utsträckning grundas på öppet material som sammanställs för att kontinuerligt kunna göra bedömningar och jämförelser. Huvuddelen av omvärlds-bevakningen tillhör det vardagliga informationssäkerhetsarbetet, som att hålla systemen uppdaterade mot nya risker, underlag för underhåll och investeringar samt att följa utvecklingen inom informationssäkerhet.

Inom området finns det dessutom information som inte är allmänt åtkomlig, till exempel den information som underrättelseorganisationerna tar fram samt incidentrapporter. För att omvärldsanalysen skall vara heltäckande och fylla sin funktion som underlag för inriktning av informationssäkerhetsarbetet bör den vara en sammanställning av såväl öppen som hemlig information. Det är, som utredningen tidigare har konstaterat i Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42), viktigt att den myndighet som för sin uppgift måste få tillgång till vissa underrättelser har erforderlig kompetens och tillräckliga resurser men också bereds möjlighet att påverka inriktningen av underrättelseorganisationernas arbete och att myndigheten delges information.

3.1.2 Samordning

Informationssäkerhetsarbete bedrivs, som huvuduppgift eller som en naturlig följd av verksamheten, av många aktörer. Det finns ett stort behov av ledning på informationssäkerhetsområdet. Detta

gäller såväl samordning av myndigheter som styrning av informationssäkerhetsarbetet.

Staten har rimligen ett övergripande ansvar för informationssäkerhet i samhället som omfattar både statsförvaltningens eget behov av informationssäkerhet och de aspekter av övriga samhällets informationssäkerhet som inte naturligen åvilar kommuner och landsting eller enskilda. Staten har därmed ett ansvar för att ha beredskap för vardagliga informationssäkerhetsproblem, men också en operativ förmåga att hantera allvarligare incidenter med mer omfattande konsekvenser för en eller flera sektorer. Utvärdering av informationssäkerhetsarbetet har visat att vissa delar av uppgiftsfördelningen inom offentlig sektor fungerar relativt friktionsfritt medan det i andra funktioner förekommer överlappande arbete och oklarheter om vem som skall göra vad. De olika uppgifter som åvilar staten, som till exempel statens egen informationssäkerhet, skydd av vitala funktioner, förtroendehöjande åtgärder som grund för tillväxt samt internationellt harmoniseringsarbete, utförs av olika aktörer och måste samordnas.

Det samordnande ansvaret bör tillfalla en statlig aktör som samtidigt har befogenheter som står i paritet med uppgiften. I ett krisläge bör någon aktör dessutom få ett utökat ansvar och därtill utökade befogenheter. Denna myndighet bör i extraordinära situationer ha möjlighet att förelägga andra aktörer uppgifter och därmed ha ett delegerat ansvar att inom givna ramar och under specificerade omständigheter styra informationssäkerhetsarbetet. Utredningen anser att ett samordningsansvar för policy och administrativa funktioner bör ligga på en enskild myndighet.

En fördjupad samverkan mellan offentliga och privata aktörer förutsätter att arbetet samordnas inom staten, även om varje sektorsmyndighet måste ta ansvar för samverkan inom sina respektive sektorer. Denna samverkan redovisas under avsnitt 3.3.

3.1.3 Internationell samordning

Informationssäkerhet är ett globalt behov, vilket utredningen och andra har konstaterat vid ett flertal tillfällen. Sverige kan inte lösa sin informationssäkerhet i isolering och kan inte heller upprätthålla kontakt med andra länder om informationssäkerheten inte är någorlunda harmoniserad. Dessutom ökar god informationssäkerhet möjligheterna att hävda svenska intressen inom EU och verkar produktivitetshöjande. För att Sveriges agerande på den

internationella arenan skall optimeras och för att öka genomslaget i EU måste en gemensam och konsekvent bild av det svenska informationssäkerhetsarbetet, till exempel avseende prioriteringar, föras fram. Den nationella strategin, olika typer av nationellt utbyte och samarbete är instrument för att skapa en gemensam bild och underlätta att arbeta mot gemensamma mål för organisationer med skilda uppdrag. Utredningen är dock medveten om att informationssäkerhetsfrågor uppkommer inom en mängd olika områden och vid olika tidpunkter. Det ställer stora krav på informationsutbyte och samarbete för att uppnå en god samordning. Sverige bör ta tillvara möjligheten att bidra till harmonisering av informationssäkerhetsarbetet mellan EU:s medlemmar och spela en aktiv roll i det internationella arbetet. Det ställer höga krav på en helhetsbild av informationssäkerhetsarbetet.

Många aktörer, såväl myndigheter som företag, har inom ramen för sin informationssäkerhetsrelaterade verksamhet behov av kontakt med sina motsvarigheter i andra länder. Strategin och de andra verktygen som används för att skapa en gemensam syn på informationssäkerhetsarbetet förstärker ett samfällt svenskt agerande. De organisationer som har den här typen av utbyten bör regelbundet uppdatera varandra genom en sammanhållen funktion genom en utpekad aktör.

3.1.4 Sammanhållande ansvar för utbildning och medvetandehöjande åtgärder

Utredningen har betonat att medvetandehöjande åtgärder, främst genom kompetensutveckling, är nödvändiga för ett gott informationssäkerhetsarbete. Utredningen lade i sitt tredje delbetänkande, Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42) en rad förslag syftandes till en långsiktig förstärkning av kompetensförsörjningen. Dessa omfattade åtgärder inom grundskolan, gymnasiet, högskolan samt forskning. I en sådan strävan är kontinuitet och stringens viktigt.

Utredningen har konstaterat att det i dag saknas en sammanhållande organisation för kompetensförsörjning. Enligt utredningens mening bör en enskild myndighet ges ett sammanhållande ansvar för att kompetensutvecklingen inom informationssäkerhetsområdet sker medvetet och framåtsyftande. En sådan aktör bör förfoga över medel att fördela bland annat för forskningsinsatser. Dessutom är det av vikt att denna aktör har

tillräcklig egen kompetens för att leda och inrikta kompetensutveckling på informationssäkerhetsområdet. Många aktörer bidrar till detta arbete: leverantörer, branschorganisationer, intresseorganisationer, massmedier, innehålls- och tjänsteförmedlare med flera. Till en viss del är detta arbete en naturlig följd av organisationernas uppdrag eller intressen. Till exempel har modemkapning uppmärksammats av Konsumentverket och tidningar har skrivit om datavirusspridning. IT-utvecklingen och ökat användande av IT leder till ett stort behov av att höja kompetensen inom säkerhets- och handhavandefrågor. Det blir då viktigt att försöka hitta de områden där informationen inte kan anses tillräcklig för användarna eller där den saknas helt. Behovet finns redan i dag och informationsutbudet måste anpassas till detta. Möjligen kan man komma långt med en kraftig punktinsats. Med tiden, om informationssäkerhet blir en självklarhet, kommer inte lika stora insatser att behövas.

En viktig del i kompetenshöjning är informationsspridning. Detta bör vara varje sektorsmyndighets ansvar.

De allra flesta som använder datorer privat har liten kunskap om hoten och framför allt om vilka möjligheter som finns till skydd. Genom att använda folkrörelser och frivilliga försvarsorganisationer skulle kunskapsnivån kunna höjas på bred front. Inom dessa organisationer finns redan etablerade strukturer för utbildning. Det bör dock påpekas att denna folkbildning skall vända sig till allmänheten, och inte bara till organisationernas medlemmar. Det är enligt utredningen viktigt att höja kunskapsnivån inom informationssäkerheten hos allmänheten, både för att på så sätt öka den totala säkerhetsnivån i landet, men även för att allmänheten då blir en mer kvalificerad kravställare gentemot tillverkarna.

3.1.5 Standarder och revision

En omfattande utveckling av standarder pågår inom informationssäkerhetsområdet. Utredningen redogjorde i sitt tredje betänkande, Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42) för de standarder som finns och vilka som är under utveckling. Det är enligt utredningen angeläget att informationssäkerhet blir föremål för revision. För att en lägsta nivå för informationssäkerhet skall kunna införas för samhällsviktiga verksamheter måste säkerheten kunna kontrolleras.

Det är inte minst viktigt att den som ansvarar för sådan verksamhet själv kan testa säkerheten i systemen. Ett sätt att underlätta för revision är att införa krav på eller uppmuntra till användandet av standarder. Standardiseringsarbete bör bedrivas så att revision, som kan visa på eventuella säkerhetsbrister, är möjlig.

Inom näringslivet är många positiva till en ökad användning av standarder. Användandet av standarder ger en ökad möjlighet att redovisa vad som säljs och att den kvalitet som utlovas uppfylls, men påverkar inte hur en tillverkare eller leverantör uppnår denna.

3.1.6 Föreskrifter och tillsyn

Några myndigheter har idag föreskriftsrätt som rör informationssäkerhet. Detta sker med stöd av lag och förordning. Några av dessa har dessutom tillsynsansvar inom sitt respektive föreskriftsområde. Enligt utredningens mening är det i princip en bättre ordning att föreskriftsrätt och tillsyn hålls åtskilda, även om nuvarande ordning för till exempel Säkerhetspolisen är väl motiverad.

Utredningen har i det tredje delbetänkandet lämnat förslag till en förordning om vissa åtgärder för informationssäkerhet hos staten. Under denna förordning föreslås att en myndighet skall ges föreskriftsrätt inom området och att tillsyn skall utövas. Enligt utredningens mening bör denna tillsyn utövas av annan myndighet än den som ges föreskriftsrätten, se vidare kapitel 4.

En ytterligare fråga som utredningen har pekat på är det särskilda ansvar staten har i fråga om informationssäkerheten i all samhällsviktig verksamhet, oavsett om den bedrivs i privat eller offentlig regi. För de myndigheter som idag bedriver verksamhet med stöd av sin föreskriftsrätt är det därför, enligt utredningens mening, önskvärt att denna inriktning tydliggörs. Detta förtydligande skulle även kunna utgöra ett stöd i myndigheternas egen verksamhetsplanering.

Utredningen har inte djupare analyserat sektorsmyndigheternas ansvar inom informationssäkerhetsområdet. En sådan analys är ett nödvändigt underlag för regeringens löpande översyn av myndigheternas verksamhet.

3.1.7 Förebyggande arbete och rådgivning

Med föreskriftsrätt följer normalt också uppgiften att ge mer praktiskt inriktade råd och anvisningar. Enligt utredningens mening är det viktigt att berörda myndigheter har tydliga mandat och resurser att bedriva uppsökande och rådgivande verksamhet inom informationssäkerhetsområdet, särskilt mot bakgrund av att medvetenheten överlag är låg.

Utredningen har i delbetänkande tre, Informationssäkerhet i Sverige och internationellt – en översyn (SOU 2004:32) föreslagit att den nationella strategin utvecklas till att omfatta förebyggande och förberedande insatser, liksom åtgärder som förstärker förmågan att upptäcka störningar och ingripa vid misstanke om brott. För några av de myndigheter som idag har föreskriftsrätt i frågor som berör informationssäkerhet kan det således finnas anledning att ytterligare förtydliga detta uppdrag och att tilldela resurser för uppgiften. Utredningen återkommer därför till dessa frågor i kapitel 4.

3.1.8 Utredningens kommentarer till administrativa funktioner

Utredningen har tidigare pekat på ett stort behov av samordning inom staten i frågor som rör gemensamma behov. Många av de informationssäkerhetsproblem som samhällets aktörer ställs inför förutsätter dessutom att det finns kompetens och förmåga att hantera tvärsektoriella frågeställningar. Vidare finns behov av att samordna och ta tillvara erfarenheter av internationella kontakter som olika myndigheter gör inom sina respektive sektorer.

Utredningen är medveten om de svårigheter som kan uppstå när en myndighet skall försöka uppnå samordnade resultat med hjälp av andra sektorsmyndigheter. En sådan samverkan ställer alltid stora krav på inblandade aktörer. Alternativet, om problem uppstår, är då att regeringen själv tvingas ta den samordnande uppgiften, något som ställer stora krav på resurser till Regeringskansliet. Som en förebild vill utredningen därför peka på den samverkan som under tiotals år har genomförts inom ramen för skydd och beredskap mot svåra påfrestningar (utgiftsområde 7:5).

Det faktum att varje myndighet har ett ansvar inom sin sektor motsäger således inte behovet av att någon eller några myndigheter

dessutom tar ansvar för de gemensamma frågorna eller de tvärsektoriella frågeställningarna. Utredningen ser att en kraftsamling och en bättre samordning och överblick skulle kunna uppnås genom att sammanföra de nu nämnda administrativa funktionerna till en myndighet. Detta skulle sannolikt också öka regeringens möjligheter att bedriva en sammanhållen informationssäkerhetspolitik. De organisatoriska konsekvenserna redovisas i kapitel 4.

3.2 Tekniska funktioner

En utgångspunkt för utredningen har varit att staten måste kunna säkerställa kompetens och förmåga att hantera såväl den egna kärnverksamheten som tvärsektoriella frågor i hela samhället. Staten bör därför ha en egen, kvalificerad teknisk kompetens inom informationssäkerhetsområdet utöver den grundnivå som normalt krävs inom sektorsmyndigheter. Den tekniska kompetensen kan bland annat användas till att testa och utveckla säkerheten i system som är viktiga för samhällets funktionalitet. Denna kompetens bör innehas och hållas uppdaterad av *en* statlig aktör för att staten till fullo skall kunna inrikta och utveckla den. IT-säkerhetsanalys kräver teknisk kompetens i sådan utsträckning att det förefaller irrationellt att flera aktörer skall ha denna funktion som deluppgift. En aktör bör ha ansvar för denna kompetens samt ha som specificerad uppgift att stödja andra som har behov.

Den tekniska kompetensen bör stödja brottsbeivrande myndigheter för att till exempel göra kriminalteknisk analys i samband med brottsutredningar.

Den tekniska kompetensen är inte minst viktig för att Sverige skall kunna hävda sig i internationella sammanhang där dessa frågor behandlas. Det kan till exempel vara i standardorganisationer, tekniska lösningar och regler för internationellt samarbete (till exempel inom EU:s institutioner och mellan myndigheter i medlemsstaterna) eller som underlag i politiska förhandlingar där tekniska frågor spelar en viktig roll (till exempel tekniska krav som förs in i EG-direktiv).

3.2.1 Certifiering och evaluering av IT-säkerhet i produkter och system

Samhället har ett ökat behov av certifierade produkter. Inom EU pågår en utveckling mot öppna system. Denna utveckling motiverar att det i Sverige finns möjligheter att få produkter certifierade och evaluerade, för att svensk industri inte skall vara beroende av utländska certifierings- och evalueringsorgan. Denna funktion bör fyllas av en statlig aktör såsom den gör i många andra länder. Det utesluter inte att det samtidigt finns privata aktörer som kan utföra liknande uppgifter efter marknadens behov. Försvarsmakten har särskilda behov som bör beaktas, inte minst mot bakgrund av de krav som redan existerar och som utnyttjas i försvarssamarbete mellan vissa länder. För att produkter som certifieras i Sverige skall vara gångbara internationellt, vilket är en viktig del i utvecklingen, måste de certifieras av ett erkänt certifieringsorgan (CB, Certification Body).

3.2.2 Signalskydd för hela samhället

Det är viktigt att den organisatoriska placeringen av signalskydd inte exkluderar någon av de verksamheter som har behov av signalskydd utan att hela samhällets behov av stöd inom området tillgodoses med beaktande av olika verksamheters varierade behov av skyddsnivåer.

Det är enligt utredningens mening viktigt att inom informationssäkerhetsområdet säkerställa kunskap och förmåga att kunna utföra dylika uppgifter. Sverige ansökte i juni 2004 på EU-nivå om att Totalförsvarets signalskyddsavdelning (TSA) skall bli vad som på engelska kallas Appropriately Qualified Authority (AQUA, en instans som godkänner lösningar för nationellt bruk). För att kunna leva upp till de krav som ställs är det viktigt att Sverige har tillräcklig kompetens för uppgiften.

Genom det ökade internationella samarbetet inom försvarssektorn ställs ökade krav från samarbetsparter på olika nationella funktioner, så som en National Communications Security Agency (NCSA), det vill säga en organisation i landet som ansvarar för signalskyddsfrågor och en National Distribution Agency (NDA), den organisation som är behörig att distribuera kryptonycklar.

Försvarsmakten har idag ansvaret för signalskyddet och resurstilldelningen inom totalförsvarsområdet. Det har därför varit svårt för aktörer utanför totalförsvarsområdet att få gehör för sina krav. Ingen enskild aktör har idag det övergripande ansvaret för samhällets signalskydd. De medel som skall finansiera verksamheten är i dagsläget en del av utgiftsområde 6:2, materielplanen, vilken styr all materielanskaffning, drift och underhåll av all materiel inom Försvarsmakten. Det är med nuvarande ordning således fråga om en prioritering mellan olika materielprojekt inom totalförsvaret och inte en fråga om samhällets samlade behov av signalskydd.

Detta förhållande bör enligt utredningens mening omprövas. Det är därvid viktigt att ha en helhetssyn på hur samhällets signalskyddstjänst regleras och organiseras. Frågor om föreskriftsrätt, kunskapsöverföring, kryptologisk kompetens, hantering av signalskyddsnycklar, utbildning med mera bör belysas mot bakgrund av hela samhällets behov av signalskyddstjänster, se vidare kapitel 4.

3.2.3 Aktiv IT-kontroll

Säkerheten i kritisk infrastruktur måste kunna kontrolleras utifrån de hot som framkommer i omvärldsanalyser och risk- och sårbarhetsanalyser. Detta motiverar att staten har kompetens för att kunna genomföra aktiv IT-kontroll. Kontrollen kan även omfatta administrativa aspekter då det visar sig att de tekniska bristerna är orsakade av bristande rutiner.

Avgörande för om aktiv IT-kontroll skall kunna få genomföras av ett statligt organ när det gäller samhällsviktig verksamhet bör inte vara ägarförhållanden. Både statligt och privat ägda företag bör kunna kontrolleras när det handlar om samhällsviktig verksamhet.

Myndigheten med ansvar för aktiv IT-kontroll skall inte bygga upp egna resurser för att åtgärda de brister eller fel som upptäcks. Den myndighet eller organisation som är systemägare, för de system som kontrolleras, skall ansvara för att detta upphandlas på marknaden.

Det bör finnas en process för att godkänna företag för uppgiften att genomföra aktiv IT-kontroll. Detta godkännande skall innebära att samma metoder och kvalitet på kontrollen kan erhållas oberoende av vem som genomför den. Kriterierna för detta godkännande bör utarbetas av den myndighet som har ansvaret för

att genomföra aktiv IT-kontroll. Detta gäller primärt kontroll av IT-säkerhet i samhällsviktiga system.

3.2.4 Utredningens kommentarer till tekniska funktioner

Utredningen förespråkar att de tekniska funktionerna aktiv IT-kontroll, teknisk analys[38] och signalskydd sammanförs under en myndighet. Funktionerna är viktiga var för sig men bildar gemensamt dessutom en helhet med stora möjligheter till korsbefruktning. Genom att placera funktionerna på en och samma myndighet blir beslutsvägarna korta och kompetensen ökar genom samverkan mellan funktionerna. Funktionerna är dessutom i vissa fall beroende av varandra för optimal prestanda. Hög, specialiserad teknikkompetens motiverar samlokalisering. Om funktionerna placeras på olika myndigheter riskeras kraftsplittring och svårigheter med överföring av information mellan aktörer. Om dessa funktioner byggs upp på flera ställen riskerar kompetensen att bli urvattnad. Många kommer då att genomföra uppgifter som inte faller inom aktörens kompetensområde.

Den myndighet som skall ha ansvar för de tekniska funktionerna bör enligt utredningen kunna hantera såväl gemensamma behov inom staten som tvärsektoriella frågeställningar i hela samhället och således inte enbart spegla totalförsvarets behov. Detta motiveras bland annat av den förskjutning som skett och pågår, från militära hot till frågor som rör den nationella säkerheten i vid mening, där brister i informationssäkerhet kan leda till omedelbara och omfattande konsekvenser för samhället. Det finns således anledning att öka insatserna och ändra prioriteringarna när det gäller informationssäkerhetsfrågor. Myndigheten bör tilldelas anslagsmedel för samtliga sina uppgifter.

Tekniska frågor är en delmängd av informationssäkerhet och för att hantera helheten måste dessa kompletteras med en omfattande omvärldsanalys. Den myndighet som får ansvar för de tekniska funktionerna bör nära samverka med den myndighet som har ansvar för omvärldsbevakning inom informationssäkerhetsområdet.

[38] Teknisk analys omfattar, utöver aktiv IT-kontroll, även bland annat tekniskt stöd vid kriminalteknisk analys, kodgranskning, teknisk rådgivning, evalueringsarbete, tekniskt arbete med standarder, internationellt tekniksamarbete med mera, samt den administrativa analys som krävs för fullgörandet av andra delar av teknisk analys.

3.3 Samverkan mellan privat och offentlig sektor

Utredningen har i tidigare betänkande redovisat de önskemål och möjligheter som finns till en fördjupad samverkan mellan privata och offentliga aktörer. Detta bygger på den gemensamma bild som vuxit fram under arbetets gång och som kan härledas till identifierade problem respektive behov inom informationssäkerhetsområdet, såväl nationellt som internationellt. Det finns således anledning att samverka kring gemensamma problem och att lära av varandras erfarenheter, som jämbördiga parter till ömsesidig nytta. Det kan handla om administrativa och tekniska lösningar eller att samverka för att öka medvetenheten i säkerhetsarbetet. I flera avseenden är också behoven och lösningarna sammanfallande för flertalet aktörer. Utredningen har mot denna bakgrund, i det tredje delbetänkandet, Säker Information – förslag till informationssäkerhetspolitik (SOU 2005:42), redovisat flera förslag till åtgärder som bland annat rör samverkan och kompetensförsörjning.

Den tekniska utvecklingen har skapat nya möjligheter och därmed nya säkerhetsproblem. En rimlig slutsats är därför att de aktörer som skapar de nya möjligheterna också borde vara bäst på att lösa de säkerhetsproblem som uppstår. Eftersom utvecklingen huvudsakligen sker på marknaden är det också där som säkerhetslösningarna måste utvecklas. Staten bör i första hand utnyttja sina olika roller som kravställare på säkerhet i olika verksamheter, i stället för att genom olika regulatoriska åtgärder försöka precisera tekniska krav på informationssystem. Dessutom har såväl privata som statliga aktörer likartade problem och behov i den dagliga verksamheten, vilket också kan ligga till grund för utbyte av praktiska erfarenheter. Utredningen konstaterar dock att intresset för informationssäkerhet inte är jämnt spritt inom näringslivet eller inom den offentliga sektorn.

Vidare framhölls i delbetänkandet att det borde vara möjligt att inom ytterligare sektorer eller områden utveckla samverkan i syfte att öka informationssäkerheten, särskilt om uppgiften att förebygga och förbereda inför tydliggörs för ytterligare myndigheter med sektorsansvar som involverar näringslivet som aktör.

Utredningen har vid flera tillfällen kunnat konstatera att olika representanter för näringslivet välkomnar en bredare samverkan kring informationssäkerhet till ömsesidig nytta men att denna samverkan måste vila på frivillighet. Staten måste hitta former för

en dialog med näringslivet som får anpassas till varierande förutsättningar. Utredningen föreslog att staten bör tydliggöra sin egen uppgift och utpeka en myndighet med sammanhållande ansvar. Denna myndighet skulle då kunna tjäna som ingång för samverkan med privata aktörer, liksom med kommuner och landsting.

3.3.1 Utredningens kommentarer och förslag till fortsatt samverkan

Genom tidigare betänkanden har utredningen visat att det finns sammanfallande problem och behov inom privat och offentlig sektor. Några av dessa områden kan vara utbildning, FoU och kompetensförsörjning. Detta är områden inom vilka både privat och offentlig sektor är beroende av funktionaliteten. Den privata sektorn kan dessutom bidra med olika tekniska lösningar. Utredningen anser att det finns anledning att samverka kring dessa, inte minst av praktiska skäl.

Utredningen har vidare i sitt senaste delbetänkande konstaterat att det inte finns någon definitiv lösning på problemet med informationssäkerhet. En väl förankrad samverkansprocess skulle dock kunna lära oss leva med problemen.

Den nu genomförda dialogen visar enligt utredningen att det dessutom finns problemställningar, som är av sådan art, att ingen av aktörerna ensam kan leverera lösningar. Följaktligen finns ett behov av att samverka för att identifiera och komma närmare lösningar på dessa. Det finns dessutom skäl att söka samverkan kring de prioriteringar som måste göras mellan olika problem och sektorer, i syfte att utnyttja tillgänglig kompetens och resurser på ett optimalt sätt.

Utredningens slutsats är att det i dagsläget finns en vilja till samverkan mellan aktörer i privat och offentlig sektor. Det är också utredningens uppfattning att näringslivet har ett intresse av att det finns adekvat utbildning, forskning och regelverk på informationssäkerhetsområdet. Den privata sidan kan bidra med tekniska lösningar, och samhällets behov utgör en marknad för näringslivets aktörer. Det finns således en ömsesidig nytta i detta gemensamma intresse. Initiativet att bilda ett självständigt samverkansorgan bör därför tas tillvara av stat, kommuner och landsting.

Ett sådant organ bör enligt utredningens mening ha till uppgift dels att medverka till att öka medvetenheten i informationssäkerhetsfrågor, dels att ge underlag för en optimal riskhantering hos alla aktörer.

De juridiska formerna för detta samverkansorgan bör diskuteras vidare. Enligt utredningens mening är det viktigt att verksamheten bedrivs som ett öppet forum, där delägarskap kan breddas till alla relevanta aktörer.

En första uppgift för samverkansorganet bör vara att identifiera de frågor som intressenterna anser är av gemensamt intresse och som inte kan lösas av en enskild aktör på egen hand. Andra frågor som kan behandlas är möjligheter till förbättringar av incidentrapportering med mera, samt implementering av standarder på informationssäkerhetsområdet.

Slutligen bör samverkan kunna utvecklas kring frågeställningar som rör rådgivning, FoU samt kompetensförsörjning och erfarenhetsutbyte.

Utredningen föreslår att det redovisade samverkansinitiativet tas tillvara och att staten omgående utser en utredare eller förhandlare som, i avvaktan på regeringens ställningstagande till utredningens övriga förslag, kan medverka till att skapa ett bättre underlag för ställningstagande till statens samverkan med andra aktörer inom informationssäkerhetsområdet samt klarlägga intresse och möjligheter för samverkan med Sveriges kommuner och landsting i dessa frågor.

3.4 Målstruktur för informationssäkerhet

Utredningen har tidigare pekat på att flera olika aktörer i den sektorsuppdelade statliga verksamheten behöver vidta åtgärder för att samhällets informationssäkerhet kontinuerligt skall förbättras. Därtill kommer ansvarsprincipen, likhetsprincipen och närhetsprincipen som ger varje myndighet ansvar för sin egen informationssäkerhet under normala omständigheter likväl som under påfrestningar och kris. På grund av informationssäkerhetens tvärsektoriella karaktär kan det vara svårt för den enskilda myndigheten att se sin respektive deluppgift i förhållande till samhällets övergripande informationssäkerhetsarbete.

Utredningen resonerade i sitt tredje delbetänkande, Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42) kring möjligheterna att formulera en målstruktur för

informationssäkerhet för att målsättningarna för olika verksamheters informationssäkerhetsarbete på ett effektivt sätt skall kunna samordnas. Utredningen förordade att informationssäkerhet, på grund av att det är en fråga som berör flera verksamheter, bör ses som ett verksamhetsområde, ingående i flera politikområden.

Mål för informationssäkerhet bör även formuleras för samhällsviktig verksamhet, oberoende av om verksamheten drivs i statlig, kommunal eller privat regi.

En målstruktur för informationssäkerhet ökar myndigheternas möjligheter att se sina respektive uppgifter i ett större sammanhang genom att de myndighetsspecifika prestationsmålen är logiskt spårbara till överordnade mål och operativa prestationsmål.

På verksamhetsområdesnivå bör finnas mål för samhällsviktiga verksamheter. Operativa mål, eller prestationsmål, med ett genomförande på ett till tre års sikt bör formuleras för nivån verksamhetsgren.

En tydlig målstruktur för informationssäkerhet skulle på ett klarare sätt peka ut ansvarig inom Regeringskansliet. Att lägga det övergripande ansvaret för den nationella informationssäkerheten under ett statsråd skulle av samtliga aktörer uppfattas som en politisk markering av att frågan har hög prioritet.

3.5 Utredningens slutsatser om utgångspunkter för organisation av informationssäkerhetsarbetet

Flera av de utgångspunkter som utredningen lyfter fram kan var och en ensam läggas till grund för val av organisation, med olika resultat beroende på vilka prioriteringar eller särintressen som styr valet. Den helhetssyn som enligt utredningen bör styra även valet av organisationslösning (och fördelningen av ansvar och befogenheter inom staten) måste med nödvändighet bygga på en sammanjämkning av flera av de grundläggande frågeställningar som utredningen lyfter fram.

Tre principer för organisation av informationssäkerhetsarbetet föreslås. Den första följer ansvarsprincipen. Den andra syftar till att tillgodose gemensamma behov inom staten. Den tredje organisationsprincipen syftar till att säkerställa kompetens och förmåga att hantera tvärsektoriella frågeställningar i hela samhället.

Mot denna bakgrund är utredningens första slutsats att det måste ligga inom varje myndighets ansvar att inom sitt område

svara för informationssäkerheten i den egna verksamheten och i kontakt med de aktörer som berörs av myndighetens verksamhet, vilket följer av ansvarsprincipen. Ansvar, befogenheter och skyldigheter bör förtydligas i berörda myndigheters instruktioner och i regleringsbrev. Föreskrifter bör utarbetas till den av utredningen föreslagna förordningen om vissa åtgärder för informationssäkerhet hos staten.

Utredningen föreslår att informationssäkerhetsarbetet bör organiseras så att kraftsamling kan ske på administrativa respektive tekniska frågeställningar. Utredningens andra slutsats är därför att gemensamma behov inom staten och tvärsektoriella frågeställningar i hela samhället bör samlas under en myndighet för administrativa funktioner respektive en myndighet för tekniska funktioner.

Utredningens tredje slutsats är att några myndigheter bör, inom ramen för sina nuvarande ansvarsområden, ges utökade uppgifter och resurser för att öka möjligheterna till förebyggande arbete, rådgivning med mera.

Utredningen har visat att det finns problemställningar, som är av sådan art, att ingen av samhällets aktörer ensamt kan lösa dem. En fjärde slutsats är därför att en samverkan mellan det privata och det offentliga bör utvecklas på informationssäkerhetsområdet.

Slutligen framhåller utredningen regeringens ledande och samordnande roll. Utredningens femte slutsats är att denna roll i informationssäkerhetsarbetet förutsätter en tydlig arbetsfördelning och organisation inom Regeringskansliet. En sammanhållande målstruktur bör tas fram, som även fångar in frågeställningarna om gemensamma och tvärsektoriella problem.

4 Organisatoriska konsekvenser av utredningens förslag

4.1 Utgångspunkter

I kapitlet beskrivs de organisatoriska konsekvenserna av den strategi och de förslag som utredningen redovisat i tidigare betänkande Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42), och i tidigare kapitel i detta betänkande. Med organisatoriska konsekvenser avses en förändrad myndighetsstruktur eller ansvars- och uppgiftsfördelning mellan olika organ.

I tidigare betänkanden har utredningen pekat på ett antal förhållanden och synsätt som kan vara vägledande för informationssäkerhetsarbetet. Några av dessa är särskilt viktiga för val av organisation inom staten:

1. Informationssäkerhet omfattar hela samhället och frågeställningen är därför vidare än totalförsvarets behov.
2. Det finns ett behov att kraftsamla och att tydligare fokusera den statliga verksamheten nationellt, inom EU och internationellt.
3. Alla statliga aktörer måste, inom ramen för sitt respektive sektorsansvar, medverka till förmågan att förebygga, förbereda inför, förhindra, upptäcka, hantera och ingripa vid störningar.
4. Ansvaret för förmågan i den statliga kärnverksamheten, liksom för säkerheten i samhällsviktiga verksamheter, måste tydliggöras. Vissa gemensamma behov förutsätter bättre samordning inom staten och i samverkan med andra, icke-statliga aktörer.
5. Kompetensen och förmågan att hantera tvärsektoriella frågor måste säkerställas inom informationssäkerhetsområdet.

Utredningen har identifierat tre organisationsprinciper som grund för sina slutsatser. Den första organisationsprincipen följer av ansvarsprincipen. Detta innebär att varje sektorsmyndighet har ansvaret för utvecklingen av informationssäkerheten inom sitt ansvarsområde och de aktörer som berörs av myndighetens verksamhet. I syfte att tydliggöra omfattningen delbetänkandet Säker information – förslag till informationssäkerhetspolitik av detta ökade ansvar har utredningen i det tredje (2005:42), lämnat ett förslag till förordning om vissa åtgärder för informationssäkerhet i den statliga verksamheten. Inom några områden finns det enligt utredningens mening anledning att ytterligare tydliggöra och förstärka detta ansvar och uppdrag. Post- och telestyrelsens (PTS) utökade ansvar och befogenheter inom området elektronisk kommunikation är ett sådant exempel. Finansinspektionens samverkan med aktörer inom finansmarknaden är ett annat. I andra fall kan det handla om att ge ökad prioritet och lyfta upp säkerhetsfrågorna i berörda myndigheters verksamhet och förstärka insatserna, till exempel inom energi- och transportsektorerna.

Den andra organisationsprincipen avser att tillgodose sådana behov som är gemensamma i den statliga verksamheten. Detta handlar framför allt om att uppnå en bättre samordning inom staten i administrativa och tekniska sammanhang.

Den tredje organisationsprincipen syftar till att säkerställa kompetens och förmåga att hantera tvärsektoriella frågeställningar i hela samhället, vare sig det handlar om att kunna hantera och ingripa vid störningar eller att ge underlag för förebyggande arbete hos alla aktörer.

Grundläggande för utredningsförslagen är också avsikten att skapa ett tydligare helhetsansvar för de frågor som rör informationssäkerhet och som kan ge underlag för en mer sammanhållen informationssäkerhetspolitik. Även om informationssäkerhet bör vara en naturligt integrerad del i alla informationssystem, offentliga såväl som enskilda, bör det på grund av informationsteknikens övergripande natur finnas en aktör på policynivå som inriktar, leder och samordnar det nationella informationssäkerhetsarbetet. Eftersom kravet på teknisk kompetens måste ställas mycket högt såväl i det förebyggande och operativa arbetet som i tillsynen av informationssäkerhet, bör det också finnas en aktör på teknisk nivå som leder och samordnar den tekniska delen av informationssäkerhetsarbetet.

Ansvaret för policyfrågor och den administrativa funktionen, liksom ansvaret för den tekniska funktionen skulle kunna samlas i en central myndighet för informationssäkerhet. Utredningen har dock stannat för att föreslå att Krisberedskapsmyndigheten (KBM) förstärks och ges samordningsansvaret för policy och administrativ informationssäkerhet. Samordningsansvaret för den tekniska informationssäkerheten föreslås läggas på en nybildad myndighet med ansvar för signalunderrättelser, signalskydd och hög teknikkompetens. Denna nya myndighet föreslås i huvudsak bygga på den kompetens som i dag finns inom Försvarets radioanstalt (FRA) men med utökat ansvarsområde och förstärkta resurser. och Den föreslagna förändringen motiverar också ett nytt namn som bättre återspeglar dess uppgifter än vad namnet Försvarets radioanstalt gör. Utredningen föreslår namnet Institutet för signalunderrättelsetjänst och teknisk informationssäkerhet (IST).

Motivet för uppdelning på två myndigheter med samordningsansvar för olika delar av informationssäkerheten är framför allt att det är rationellt och ger utrymme för synergieffekter med dessa myndigheters övriga ansvarsområden. Det bör också ge underlag för en bättre sammanhållen informationssäkerhetspolitik. Detta förutsätter dock ett välutvecklat löpande samarbete mellan de båda samordningsansvariga myndigheterna, liksom mellan dessa och andra myndigheter, näringslivet, och andra aktörer som har uppgifter och behov på informationssäkerhetens område.

Utredningens förslag kommer att få vissa konsekvenser för berörda myndigheters personal. I flera fall föreslår utredningen en förstärkning av kompetens och bemanning. De medel som hittills anslagits som projektmedel för informationssäkerhet via den så kallade civila ramen föreslås omvandlas till ordinarie anslagsmedel. Det innebär samtidigt en markering av att myndighetsorganisationen för informationssäkerhet får en permanent karaktär, efter de inledande årens mera projektinriktade uppbyggnadsperiod.

Det utökade ansvaret för informationssäkerhet som utredningen föreslår bör också återspeglas i organisation och bemanning på ledningsnivå i de båda myndigheter som föreslås få samordningsansvar.

Utredningen har tagit del av FOI:s rapport Underlag för utvärdering av uppgiftsfördelning inom informationssäkerhetsområdet,[39] som utarbetats för utredningens räkning Därutöver har

[39] Totalförsvarets forskningsinstitut, 2004, Underlag för utvärdering av uppgiftsfördelning inom informationssäkerhetsområdet, FOI-R-1369-SE.

utredningen haft en rad kontakter med berörda myndigheter och representanter för näringslivet. Det är bland annat mot bakgrund härav som utredningen har formulerat de organisatoriska förslag som redovisas i föreliggande kapitel.

Utredningstiden för det organisatoriska betänkandet har varit kort. Även om de organisatoriska slutsatserna utgår ifrån den strategi, de principer och de uppgifter som följer av tidigare betänkanden finns det anledning att påpeka detta. Det innebär att förslaget, vad gäller bemanning och resursinsatser, kan behöva värderas i detalj efter remissbehandlingen av betänkandet.

4.2 Tidigare reformer

Regering och riksdag har tidigare med anledning av propositionen Fortsatt förnyelse av totalförsvaret (prop. 2001/02:10) och propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158, bet 2001/02:FöU10, rskr 2001/02:261), fattat beslut om en rad åtgärder inom IT-säkerhetsområdet. Syftet med dessa åtgärder var att öka samhällets förmåga att förebygga, upptäcka och motverka dataintrång, datavirusspridning, manipulering av information eller programvaror samt andra händelser som hotade informationssäkerheten. Som en särskilt allvarlig form bedömdes samordnade åtgärder för att nå ekonomiska, politiska eller militära mål genom att påverka eller utnyttja en motståndares IT-system och informationen som lagras i dessa.

Informationssäkerhet betraktades som en väsentlig del i arbetet med att minska sårbarheten i samhället. Hoten mot IT-systemen bedömdes som ett globalt problem. Riksdagsbesluten innebar att nya IT-säkerhetsfunktioner inrättades inom vissa områden. En omvärldsanalysfunktion inrättades vid KBM med inriktning på kvalificerade IT-hot, en teknikkompetensfunktion inrättades vid FRA och en IT-incidentrapporteringsfunktion vid PTS. Dessutom beslöts att ett system för säkerhetsinriktad evaluering och certifiering av IT-produkter skulle inrättas vid Försvarets materielverk (FMV).

Propositionerna innebar en väsentlig ambitionshöjning inom IT-säkerhetsområdet. Ökade resurser för verksamheten har tillförts i första hand genom årliga projektmedel ur KBM:s så kallade civila ram.

4.3 Utredningens förslag till administrativa funktioner

4.3.1 Policy och samordningsansvar

Informationstekniken är tvärsektoriell och berör i princip alla aktörer i samhället. Samtidigt utgör den ett eget område eller en dimension i vilken det är möjligt att agera – till exempel att informera, bedriva handel, kommunicera, roa sig, begå brott eller skada samhällsviktig verksamhet. Ett förutseende, tydligt och kommunicerat nationellt informationssäkerhetsarbete skapar förtroende för IT, vilket främjar en ökad användning av IT och bidrar till att behålla och utveckla Sveriges roll som en ledande IT-nation. Av hänsyn till informationsteknikens övergripande natur behövs en utpekad aktör på policynivå som inriktar, leder och samordnar det nationella informationssäkerhetsarbetet. Utredningen föreslår att KBM ges denna roll.

I policyansvaret ligger att förvalta och utveckla den nationella informationssäkerhetsstrategin, att samordna informationssäkerhetsarbetet mellan samhällets aktörer, att under regeringen inrikta samhällets informationssäkerhetsarbete, att utgöra samhällets kontaktpunkt för informationssäkerhet och att under regeringen utgöra internationell kontaktpunkt genom att samordna och företräda Sverige i internationell samverkan där det bedöms lämpligt och där inte andra myndigheter är utpekade.

En dialog med liknande utländska myndigheter eller organisationer bidrar till helhetsbilden och ett kritiskt förhållningssätt till det sätt som informationssäkerhetsarbetet och skyddet av samhällsviktig infrastruktur i Sverige bedrivs. Att en statlig aktör på policyområdet utgör kontaktpunkt, när det inte finns etablerade samarbeten, underlättar och förbättrar internationell samverkan kring dessa frågor. En utpekad kontaktpunkt underlättar för utländska aktörer och ökar möjligheten att relevanta frågeställningar eller information fångas upp, respektive slussas vidare till rätt aktör i samhället. En uppgift bör också vara att säkerställa att alla myndigheters internationella erfarenheter inom området informationssäkerhet tas till vara.

Också nationellt har utpekandet av en samordnande myndighet betydelse för allmänhet, näringsliv, kommuner etc. Det underlättar för samtliga aktörer i samhället om de i policyfrågor kan vända sig till en myndighet med frågor som rör informationssäkerhet eller

skyddet av samhällsviktig infrastruktur. Syftet med en utpekad myndighet är att underlätta för utomstående och att uppmärksamma och samordna nya frågeställningar. Detta innebär i sig inget avsteg från ansvarsprincipen eftersom genomförandet av specifika uppgifter även fortsättningsvis ligger hos direkt ansvariga sektorsmyndigheter.

KBM:s nuvarande mandat att ha ett sammanhållande myndighetsansvar har inom området informationssäkerhet visat sig vara otillräckligt. Erfarenheterna har visat att övriga myndigheter i flera fall endast försett KBM med den information de själva ansett lämplig och endast i begränsad utsträckning medverkat i en samordning mellan myndigheterna. Mandatet bör därför stärkas till att bli samordnande och att ansvaret för förebyggande åtgärder på bredden i samhället förtydligas. KBM kan utgöra en neutral part genom att myndigheten inte har direkt kontroll- och tillsynsansvar och inte är en del av underrättelse-, säkerhets- eller polisorganisationerna. Detta är enligt internationella erfarenheter en fördel, inte minst i dialogen med näringslivet och andra icke-statliga aktörer.

Informationssäkerhet måste på grund av sin komplexa natur hanteras som ett eget kompetensområde samtidigt som det måste integreras med andra säkerhetsaspekter.

4.3.2 Föreskriftsrätt och tillsyn

Det finns, inte minst på grund av införandet av allt fler myndighetsövergripande IT-system, behov av att etablera en gemensam grundläggande säkerhetsnivå för system som stöder samhällsviktig verksamhet, kopplat till den förordning utredningen föreslagit.[40] KBM bör i sin roll som policymyndighet ges möjlighet att ge ut föreskrifter om en grundläggande säkerhetsnivå med stöd av en sådan förordning. Nära samverkan måste härvidlag etableras med sektorsansvariga myndigheter med egen föreskriftsrätt, exempelvis PTS, Finansinspektionen samt Säkerhetspolisen.

Den av utredningen föreslagna förordningen är avfattad så att den är subsidiär, det vill säga andra förordningar har företräde när konflikt uppstår.[41]

Även revision och tillsyn av föreskrifterna måste utvecklas. Detta bör dock genomföras av andra aktörer än KBM, exempelvis av

[40] Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42), s. 31 ff.
[41] Förslag till förordning om vissa åtgärder för informationssäkerheten hos staten, 1 § 2st.

Statskontoret i en ny roll. Statskontorets verksamhet är för närvarande föremål för omorganisation och det råder osäkerhet om myndighetens framtida konstitution. Utredningen avstår därför från att lägga förslag som berör myndigheten.

Det är också viktigt att tillsyn och kontroll utformas så att den sker utifrån ett helhetsperspektiv och inte begränsas till att endast avse hanteringen av information av betydelse för rikets säkerhet, vilket är Säkerhetspolisens ansvar. Det är dock angeläget att ansvarsfördelningen mellan KBM och den myndighet som efterträder Statskontoret tydliggörs, vad avser övriga uppgifter inom informationssäkerhetsområdet.

KBM bör också tillsammans med den föreslagna nya myndigheten, IST, inrikta och leda den verksamhet som skall stödja samhället när det gäller behovet av kryptografiska funktioner. En viktig del i detta är att möjliggöra för regeringen och myndigheter att samverka på ett säkert sätt med gemensamma metoder som säkerhetsgranskats och godkänts. KBM bör svara för policynivån och bemyndigas att ge ut erforderliga föreskrifter och rekommendationer för signalskyddsverksamheten. KBM bör även bemyndigas att ha ansvaret för administrativt godkännande av signalskyddssystem.

Uppgiften som signatär inom ramen för CCRA (Common Criteria Recognition Arrangement) föreslås överföras från Swedac till KBM (se avsnitt 4.5.2).

KBM:s föreslagna ansvar för föreskrifter inom området informationssäkerhet sammanfaller i vissa delar med föreskriftsrätten för Nämnden för elektronisk förvaltning. Nämnden upphör vid årsskiftet och dess föreskriftsrätt vad avser informationssäkerhet bör överföras till KBM.

4.3.3 Helhetsbild

Helhetsbilden utgör en gemensam kartbild av verkligheten. Utifrån denna bör de ingående delarna i ett nationellt informationssäkerhetssamarbete inriktas, ledas och samordnas. Samtidigt kan de ingående delarna löpande bidra till att utveckla helhetsbilden. Det är utifrån en samlad helhetsbild som det går att göra rätt prioritering av insatser och säkerhetskrav samt att rätt identifiera nya problemområden.

KBM sammanställer en helhetsbild genom sitt utpekade ansvar för omvärldsanalys från öppna källor och underlag från

sektorsansvariga myndigheter samt genom samverkan med olika samhällsaktörer, inklusive underrättelse- och säkerhetsmyndigheter samt näringsliv. Denna kan i en förändrad organisation utvecklas ytterligare, bland annat genom att KBM får en förbättrad tillgång till underrättelserapporter.

Idag avrapporteras helhetsbilden avseende samhällets informationssäkerhet bland annat genom den årliga lägesbedömningen samt utifrån perspektivet samhällsviktig infrastruktur genom den årliga hot- och riskrapporten.

KBM hanterar också de årliga risk- och sårbarhetsanalyser (RSA) som myndigheter är ålagda att leverera till regeringen. Informationssäkerhetsaspekterna i dessa är ett begränsat men potentiellt viktigt bidrag till helhetsbilden. Användningen av RSA som underlag till helhetsbilden bör utvecklas. Helhetsbilden på informationssäkerheten bör också kunna utgöra ett värdefullt underlag för inriktningen av samhällets hela arbete med säkerhet och krisberedskap och den medelsfördelning som är förknippad med detta.

4.3.4 Forskning och studier

Nära kopplat till helhetsbilden är möjligheten att i ett längre tidsperspektiv initiera och finansiera strategiska forskningsinsatser samt i ett kortare tidsperspektiv studier. Initiering av forskning och studier bör ha sin utgångspunkt i helhetsbilden, samtidigt som de bidrar till densamma. Möjligheter att bidra till finansieringen av denna typ av verksamhet är därför en viktig del i arbetet med samhällets informationssäkerhet. Motiven och förslagen liksom KBM:s roll har utvecklats i utredningens tidigare betänkande Säker information – förslag till informationssäkerhetspolitik (2005:42). Det bör finnas en särskild budget för detta ändamål.

4.3.5 Samverkan

Det finns behov av en formaliserad samverkan med KBM som samordnande myndighet mellan aktörer i samhället som äger, driver eller på annat sätt har ansvar för samhällsviktig verksamhet eller infrastruktur. I denna samverkan skall berörda sektorsmyndigheter medverka. Informationsutbytet kan avse incidenter, bästa metod, hot, risker och sårbarheter. Informationen

måste fungera både inom, respektive mellan, stat, kommuner, näringsliv och andra organisationer. Samverkan utgör ett viktigt underlag till helhetsbilden liksom den till ömsesidig nytta förmedlar känslig eller förtrolig information, frågeställningar och påverkan. Det kan innefatta:

- Att delta i och analysera utvecklingen inom EU och i övriga internationella sammanhang och att delta i relevanta arbetsgrupper eller fora för att strategiskt påverka de processer inom EU och internationellt som berör Sverige. Det bidrar också till att stärka Sveriges position i dessa aktiviteter.
- Att utveckla formerna för samverkan med näringsliv och andra icke-statliga organisationer.
- Att vidareutveckla relationerna och bygga förtroende gentemot underrättelse- och säkerhetstjänsterna, polisen och andra organisationer.
- Att etablera permanenta eller temporära råd i olika syften. Ett sådant kan vara att få en bättre balans mellan tekniska och juridiska aspekter på ett tidigt stadium i nya lagförslag.
- Att samordna statens medverkan i standardiseringsarbetet. Huvudansvaret bör dock åvila befintliga aktörer på området.

Formerna för samverkan och diskussion bör syfta till att förtrolig och känslig information kan delas. Samverkan bidrar också till helhetsbilden. KBM bör i extraordinära situationer ha ett delegerat ansvar att inom givna ramar samordna informationssäkerhetsarbetet.

4.3.6 Stöd och förebyggande arbete

Förebyggande arbete syftar till att höja medvetenheten om informationssäkerhet, risker och möjligheter till skydd på bredden i samhället. Det kan innefatta:

- Att utveckla metoder för säkerhetsanalyser i informationssystem.
- Att ge vägledning för en säkerhetsnivå med tillämpning av standarder för informationssäkerhet.
- Att initiera breda utbildningsinsatser och medvetandehöjande åtgärder gentemot samhället och IT-användarna.
- Att initiera eller genomföra riktade specialutbildningar i informationssäkerhet.
- Att rikta säkerhetsinformation till allmänheten.

- Att medverka till att informationssäkerhet integreras i utbildningen på grundskole-, gymnasie- och högskolenivå.
- Att initiera eller medverka till att fortbildning i informationssäkerhet genomförs på ledningsnivå.

Det är till stor del genom det förebyggande arbetet som samhällets robusthet för informationssäkerhet förbättras och operationaliseras. Ansvaret bör även fortsättningsvis vila på KBM, med förstärkta resurser för ändamålet. Det förebyggande arbetet handlar främst om utbildningsinsatser och medvetandehöjande åtgärder, produktion av vägledningar samt fördelning av medel från den så kallade civila ramen.

De behov som finns och som uppstår avseende stöd och förebyggande åtgärder bör hanteras löpande genom samordning mellan samhällets aktörer. En grundläggande princip bör vara att staten endast tar ansvar för skyddsåtgärder som marknadens aktörer inte förmår hantera, exempelvis kollektiva nyttigheter eller vid exceptionellt höga krav på sekretess.

Erfarenheter från bland annat Nederländerna och Tyskland visar att näringslivet kan och bör spela en aktiv roll. Den tyska informationssäkerhetsmyndigheten Bundesamt für Sicherheit in der Informationstechnik (BSI) identifierar samhällets behov av informationssäkerhet men anlitar till största delen näringslivets aktörer för att utveckla, producera och leverera efterfrågade produkter och tjänster.

4.3.7 Scenario- och övningsverksamhet

Scenario- och övningsverksamhet utgör ett viktigt verktyg för att kritiskt värdera modeller och lösningar. Det gäller också på informationssäkerhetsområdet. I dag bedrivs övningar på informationssäkerhetsområdet inom Försvarsmakten både nationellt och internationellt. Vidare förekommer numera omfattande övningsverksamhet inom den samhällsviktiga verksamheten, till exempel elförsörjning, telekommunikation och finanssektorn. Scenario- och övningsverksamhet med inslag av informationssäkerhet har förekommit, men måste utvecklas och ges större fokus.

Utifrån helhetsbilden och policyansvaret på informationssäkerhetsområdet samt utifrån KBM:s befintliga kompetens på övningsområdet är det naturligt att KBM har det samordnande myndighetsansvaret för övningar på

informationssäkerhetsområdet. Liksom i det förebyggande arbetet kan övningsverksamheten till stor del hanteras av näringslivet. KBM:s roll bör främst vara att identifiera, uppmärksamma och formulera behov och mål för insatserna.

4.3.8 Frivillig krisresurs

Vid allvarliga informationssäkerhetsrelaterade händelser kan befintlig personal och kompetens inom en eller flera organisationer som ansvarar för samhällsviktig verksamhet vara otillräcklig. Kunskapsbanken på området är naturligt begränsad, och kan svårligen hållas bredare inom den offentliga verksamheten än vad normalförhållandena kräver.

Ett sätt att bidra till att kunna hantera en allvarlig eller extraordinär situation vore att kunna mobilisera kompetens dit den behövs, för att begränsa en skada eller att arbeta förebyggande mot nya attacker eller angrepp. Ett sådant nationellt säkerhetsinitiativ skulle vara att upprätta en kompetensbank.

En jämförelse som kan göras är med hur deltidsbrandkårer byggs upp och fungerar. Enskilda individer står till förfogande för att kunna rycka ut med kort varsel och deras arbetsgivare har i förväg accepterat den påverkan detta kan innebära i företagets eller myndighetens verksamhet. Den tänkta modellen förutsätter att de personer med spetskompetens inom informationssäkerhet som ingår, regelbundet får öva scenarier under organiserade former.

Det samordnande ansvaret för att ta tillvara sådana frivilligresurser bör läggas på KBM som ges uppgiften att hantera kontakterna och upprätta erforderliga avtal med enskilda och berörda företag samt tillse att övningsverksamhet genomförs.

4.3.9 Signalskyddsutbildning

Användning av kryptografiska funktioner för att erhålla säkerhet vid kommunikation, lagring av information samt för att garantera autentisering och identifiering ökar i samhället. Svenska myndigheters internationella arbete medför att det ställs krav på säker hantering av information som behandlas elektroniskt vid respektive myndighet samt vid förmedling av informationen.

Utbildning är en viktig del i informationssäkerhetsarbetet. Den utbildning som krävs för att erhålla behörighet att hantera och

nyttja signalskydd bedrivs idag vid Totalförsvarets signalskyddsskola (TSS). För att skapa möjlighet till helhetssyn vad avser den utbildning som erfordras inom informationssäkerhetsområdet samt för att uppnå synergieffekter bör signalskyddsutbildningen utvecklas så att utbildning kan ges inom hela informationssäkerhetsområdet.

Utredningen föreslår därför att huvudmannaskapet för signalskyddsutbildning överförs från Försvarsmakten till KBM.

4.4 Utredningens förslag till tekniska funktioner

4.4.1 Totalförsvarets signalskyddstjänst

Totalförsvarets signalskyddstjänst ingår i Försvarsmakten och leds och samordnas av MUST Säkerhetskontor.[42] I ledningsfunktionen ingår framtagning av regelverk, handböcker och instruktionen samt genomförande av dialoger och informationsmöten på central respektive regional nivå. ”Kundkretsen” utgörs av ca 90 myndigheter och företag, de senare företrädesvis ur försvarsindustrin. För närvarande är ca 40 totalförsvarsgemensamma signalskyddssystem och ett antal försvarsmaktsspecifika system i drift. I ledningsfunktionen ingår även att inrikta Totalförsvarets signalskyddsskola (TSS).

Signalskyddsverksamheten kontrolleras administrativt, i samverkan med KBM vad avser civila myndigheter och FMV vad avser försvarsindustrin, varvid organisation, behörighet, nyckelhantering med mera är föremål för kontroll. Dessutom genomförs teknisk kontroll (signalkontroll) för att säkerställa att kryptosystemen utnyttjas riktigt och att den tekniska funktionen är korrekt. Godkännandet sker genom Försvarsmakten.

Vid utveckling av nya signalskyddssystem genomförs ett omfattande arbete att verifiera att systemen fungerar på avsett sätt, innan ett godkännande kan utfärdas. Detta gäller även vid modifiering av befintliga system. Vid utformningen av kryptografiska mekanismer samarbetar MUST Säkerhetskontor med FRA. I utvecklingsarbetet ingår även att ta fram system för generering av kryptonycklar, certifikat och system för

[42] Signalskyddstjänsten hanterades tidigare inom Försvarsmakten/TSA (Totalförsvarets signalskyddssamordning)

personalisering av totalförsvarets aktiva kort så att kryptografiskt riktiga kryptonycklar kan distribueras till användare. I utvecklings- och verifieringsrollen ingår även att stödja anskaffning.

En omfattande verksamhet inom signalskyddsområdet är att i samråd med nyckelansvariga myndigheter fastställa och tilldela kryptonyckelserier samt kontinuerligt producera och distribuera kryptonycklar till totalförsvaret. I arbetet ingår även att distribuera totalförsvarets aktiva kort och certifikat samt att utöva rollen som totalförsvarets CA (Certificate Authority). Dessutom utövas rollen som NDA (National Distribution Authority) vid samverkan med andra nationer.

MUST Säkerhetskontor stöder även Regeringskansliet i krypto- och signalskyddsfrågor. I detta arbete utövas expertrollen som NCSA (National Communications Security Authority) i olika internationella samarbeten där kryptoverksamhet berörs. Exempel är stöd till Europeiska Rådets sekretariat och vid vissa gemensamma EU-projekt som Galileo, TESTA etc. Även granskning och verifiering av andra nationers godkända kryptosystem avsedda att skydda EU-information genomförs. Något formellt beslut om denna roll har dock inte fattats.

4.4.2 Signalskyddsverksamhet vid KBM

Signalskyddsverksamheten vid KBM har som syfte att åstadkomma en bättre informationssäkerhet genom att hos krishanteringssystemets aktörer skapa förmåga att förhindra obehörig insyn i och påverkan av elektronisk kommunikation. Arbetet avser inriktning, utveckling och samordning av civila myndigheters samt vissa samhällsviktiga företags signalskydds-verksamhet genom samverkan med Försvarsmakten, FMV och företrädare för näringslivet.

Verksamheten består av utveckling, underhåll, redovisning och förrådshållning av signalskyddsmaterial och annan teknisk utrustning för det civila försvaret samt att bedriva signalskyddsövningar och ge användarstöd. Myndigheten sprider också signalskyddsinformation och kompetensutvecklar personal inom signalskyddsorganisationen på central och regional nivå. KBM hanterar också de fasta kostnader som uppkommer i samband med förvaltning av utrustning. Det gäller bland annat sekretessutrustning för telefoner och underhållsavtal. KBM distribuerar också kryptonycklar enligt gällande regler.

Budgetomslutningen är drygt 16 miljoner kronor. Antalet årsanställda är ca 10 personer.

4.4.3 Signalunderrättelsetjänst och teknikkompetens

FRA är central förvaltningsmyndighet med ansvar för signalunderrättelsetjänst (signalspaning) enligt den inriktning som regeringen anger och de uppdrag som lämnas av Försvarsmakten och andra uppdragsgivare. Signalspaning innebär att med mottagarsystem och andra elektroniska hjälpmedel registrera radiosignaler för att hämta in underrättelser. FRA:s signalspaning innefattar två delar: teknisk signalspaning (TES) och kommunikationsspaning (KOS).

Inriktningen har under senare år successivt förskjutits från de traditionella militära hoten mot nya säkerhetshot.

Utöver signalspaningsuppdraget har FRA uppgifter inom svensk informationssäkerhet. Det gäller kryptologisk expertis, där FRA sedan 1980-talet svarar för att bemanna de kryptologiska funktionerna vid MUST.

FRA har också sedan 2003 en särskild teknikkompetensfunktion (TKF) till stöd för statliga myndigheter och företag med samhällsviktig verksamhet, som bland annat medverkar i tester av säkerheten i myndigheters IT-system tillsammans med berörda myndigheter.

Miljön på FRA är teknikorienterad vilket främjar möjligheterna att attrahera teknisk personal med hög kompetens och att behålla en kritisk kunskapsmassa. FRA följer den nationella och internationella utvecklingen och deltar i olika samarbeten med andra aktörer inom informationssäkerhetsområdet.

Med ett eget forsknings- och utvecklingsprogram arbetar FRA för att ligga före i utvecklingen med att förutse och bedöma behov och säkerhetsnivåer. Det görs främst genom att utnyttja kompetens och metoder som härrör sig från FRA:s kärnverksamhet – signalunderrättelsetjänst. FRA kan också i virtuell laboratoriemiljö simulera de miljöer som finns hos uppdragsgivarna och på detta sätt fortare hitta brister som kan äventyra informationssäkerheten.

Med hjälp av FRA:s metoder och teknikstöd har till exempel tjänsten Aktiv IT-kontroll visat resultat hos uppdragsgivarna och pekat ut brister i system och nätverk. Ibland har bristerna varit så allvarliga att det har kunnat påverka tillgängligheten till nationens

tekniska infrastruktur. I vissa fall har den upptäckta bristen kunnat innebära skador för rikets säkerhet om en angripare hade kunnat utnyttja bristen innan den säkrades.

FRA har redan nu erfarenhet och färdiga krisberedskapsprocesser som har testats och används i verkliga fall för att stödja insatser vid myndighetskriser. Dessa kommer att vara värdefulla om det skulle uppstå en nationell kris med IT-inslag.

FRA:s erfarenhet av intrångsdetekteringssystem för att spåra onormal trafik i nätverk gör att man snabbt kan sjösätta ett nationellt system om en ny signalunderrättelsetjänstslag träder i kraft. Det gör att Sverige i framtiden inte blir lika beroende av omvärldens välvilja för att upptäcka attacker mot Sverige. Idag har FRA med hjälp av signalunderrättelsetjänstens internationella kontaktnät kunnat samverka och bland annat erhållit information om pågående angrepp mot nationella intressen och på detta sätt kunnat påbörja identifiering av inblandad aktör innan skada hunnit inträffa. Ett förslag till en tydligare rättslig reglering av FRA:s signalunderrättelsetjänst är för närvarande på remiss.[43] Förslaget innebär förändrade förutsättningar för signalunderrättelsetjänsten och ökade möjligheter för den nybildade myndigheten att skydda landet mot IT-attacker från utlandet.

En stor del av informationssäkerhetsarbetet handlar om den del av informationen som hanteras genom kommunikation mellan datorer. Samverkan mellan FRA:s kryptologer och TKF:s FoU-personal har här varit till fördel. Nyttan har varit dubbelriktad då man allt oftare har behov av både kryptologikompetens och erfarenheter av ”reverse engineering” (återskapande av källkod för analys och bearbetning, då man inte har tillgång till källkoden) för att kunna finna brister.

4.4.4 Motiv för samordning av signalskyddet

Utredningen föreslår att ansvaret för signalskydd överförs från Försvarsmakten, MUST säkerhetskontor, till den nybildade myndigheten, ITS. Även KBM:s ansvar för signalskydd föreslås överföras. Det administrativa godkännandet av signalskyddssystem föreslås dock placeras vid KBM. Föreskriftsrätt för samhällsviktiga system, inklusive signalskyddstjänsten, föreslås ges till KBM. Den

[43] En anpassad försvarsunderrättelseverksamhet (Ds 2005:30).

nya myndigheten, IST, bör ges föreskriftsrätt för tekniskt godkännande av kryptoprodukter.

KBM:s signalskyddsverksamhet bedrivs i huvudsak i Sollefteå. Överföringen bör leda till en utökad bemanning av verksamheten i Sollefteå.

Signalskydd och signalunderrättelsetjänst kan ses som två sidor av samma mynt. Det finns fördelar med ett nära samarbete mellan dessa båda områden. Länder med brister i signalskyddet har ofta dålig kontakt mellan signalskydd och signalunderrättelsetjänst. Det behövs kompetens i att forcera bristfälligt signalskydd för att kunna skapa ett eget bra signalskydd. Kompetensen härför finns inom nuvarande FRA.

Samhället har ett växande behov av signalskydd. Eftersom staten har ett ansvar för samhällsviktig verksamhet, även icke-militär sådan, finns behov av en organisation med hög kompetens också utanför totalförsvaret.

Svensk kryptoindustri har idag svårt att konkurrera med utländsk, då det inte finns en inhemsk organisation som kan godkänna kryptosystem utanför totalförsvaret. Vid offertförfarande från EU:s institutioner och organ krävs allt oftare att systemen är godkända nationellt. Det visar på ytterligare ett behov av att bredda omfattningen av samhällets signalskydd, vilket kan ske genom en flyttning av signalskyddsfunktionen från Försvarsmakten till den nybildade myndigheten för teknisk informationssäkerhet. Verksamheterna för nyckelproduktion och signalkontroll finns dessutom redan placerade i FRA:s lokaler.

Det finns dessutom positiva synergieffekter av en förändrad placering av signalskyddsfunktionen. Ansvarsområdet för FRA:s Teknikkompetensfunktion, TKF, gäller idag IT-säkerhet med signalskyddet exkluderat. FRA har kompetenser som främjar signalskyddsverksamheten och ger synergivinster, viktiga kunskapsvinster och arbetsrotation. Det gäller kommunikationsspaning, trafikbearbetning, forceringsverksamhet, signalanalys, teknisk signalunderrättelsetjänst, signalhantering, hantering av stora dataflöden med mera.

Det växande behovet av kvalificerade resurser för informationssäkerhet utanför det militära området innefattar också ett ökande behov av signalskydd för myndigheter och samhällsviktig verksamhet.

Flera länder med hög nivå inom området, har signalskydd och signalunderrättelsetjänst kopplade till varandra. FRA har omfattande internationella partnerkontakter avseende

informationssäkerhet. Genom att det i tongivande länder är samma eller närstående organisationer som svarar för verksamheten kan dessa upparbetade kontakter utnyttjas även för signalskydd. Det blir också lättare i det internationella samarbetet för andra länder att kontakta Sverige, då det finns en naturlig samarbetspartner istället för flera med oklara gränsdragningar.

Förtroendet för en organisation inom informationssäkerhetsområdet är centralt. FRA:s signalunderrättelsetjänst (som utnyttjar brister i signalskydd och informationssäkerhet) påverkar förtroendet för arbetet med att förebygga informationssäkerhetsbrister. Detta måste beaktas i FRA:s organisation och arbete.

För att vara en tillgång vid nya behov och för nya samarbetspartners är det angeläget att den nybildade myndighetens civila karaktär tydliggörs. Samtidigt måste Försvarsmaktens behov av signalskydd alltid tillgodoses, även i en förändrad organisation.

Försvarsmakten är den organisation som kanske tidigast av alla konfronterats med informationssäkerhetsproblem och därför tvingats agera för att skydda vitala samhällsintressen. Dessutom hanteras stora mängder sekretessbelagt material på totalförsvarets område. Följaktligen har Försvarsmakten också tvingats säkerställa både administrativ och teknisk kompetens inom det egna ansvarsområdet i syfte att åstadkomma kvalificerade informationssäkerhetslösningar. Utvecklingen med att ta fram kvalificerade IT-säkerhets och kryptolösningar har bland annat skett med stöd av FRA och FMV. Försvarsmakten utvärderar också IT-säkerhets och kryptolösningar för att kunna använda resultatet såväl internt som hos tillsynsmyndigheterna.

Utredningen har också föreslagit att den nationella strategin för informationssäkerhet måste innefatta en förstärkt förmåga inom området nationell säkerhet. Detta har redovisats i det tredje delbetänkandet.

Utredningen har betraktat informationssäkerhet i ett bredare perspektiv än enbart ur totalförsvarets synvinkel. Informationssäkerheten berör alla samhällets aktörer och arbetet måste därför organiseras utifrån hela samhällets behov. Detta motsäger inte det faktum att Försvarsmakten även i framtiden kommer att ställas inför kvalificerade problemställningar som motiverar egen hög kompetens och resurser. Men dessa problemställningar är principiellt ett sektorsproblem enligt utredningens synsätt. I vissa avseenden skiljer sig dessa till inriktning och omfattning från andra myndigheters problem.

Utredningen har avfärdat tanken att organisera informationssäkerhetsarbetet genom att utvidga Försvarsmaktens ansvarsområde. Detta skulle kunna ställa Försvarsmakten inför den omöjliga uppgiften att prioritera mellan egna intressen och samhällets behov. Mot denna bakgrund har utredningens utgångspunkt utvecklats till att söka organisera informationssäkerhetsarbetet utifrån hela samhällets behov, vilka är större än totalförsvarets. Enligt utredningens mening bör utvecklingen av Försvarsmaktens egen förmåga på informationssäkerhetsområdet fortsättningsvis hanteras tillsammans med synen på den nationella säkerheten och Försvarsberedningens pågående arbete.

Staten måste av nationella säkerhetsskäl och för att kunna vara en pådrivande aktör i det europeiska och internationella samarbetet om teknisk informationssäkerhet ha en hög kompetens. Det är en krävande uppgift som är beroende av specialister med enstaka starkt begränsade kompetensprofiler. Om dessa är utspridda på flera olika aktörer innebär det överlappande arbetsuppgifter och en icke optimal användning av ekonomiska och andra resurser.

En effekt som uppstår vid samordning av alla tekniska delfunktioner hos en myndighet är snabbare beslutsvägar. Det är av stor vikt att snabbt kunna sätta ihop en insatsgrupp för att stödja insatser vid nationella kriser med IT-inslag och för att kunna medverka till identifiering av inblandade aktörer i IT-relaterade hot mot samhällsviktiga system. Med en delad organisationsbild är det svårare att upprätthålla en kritisk kompetensmassa.

Om uppgiften att leda och samordna signalskyddstjänsten inom totalförsvaret överförs från Försvarsmakten, erfordras att de medel som finns avsatta i materielplanen för utveckling också förs över. Försvarsmakten kommer oavsett vem som har det samordnande ansvaret för signalskyddstjänsten att vara en av de största avnämarna.

I 39 § förordningen (2000:555) med instruktion för Försvarsmakten föreskrivs att Försvarsmakten får meddela övriga statliga myndigheter föreskrifter i fråga om signalskyddstjänsten inom totalförsvaret. Försvarsmakten har därför tagit fram Försvarsmaktens föreskrifter (FFS 2005:2) om signalskyddstjänsten inom totalförsvaret. Skälet är att åstadkomma enhetlighet i verksamheten. De som har tillgång till signalskyddssystem men som inte omfattas av föreskrifterna, till exempel företag, förbinder sig genom avtal att följa dem.

Enligt utredningen finns det skäl att utvidga tillämpningsområdet för föreskrifterna i syfte att bättre täcka in de behov som

finns i hela samhället. Föreskriftsrätten bör då, i konsekvens med det vidare syftet, överföras till den myndighet som skall ha policyansvaret och det samordnande administrativa ansvaret för signalskyddet. Utredningen föreslår därför att Försvarsmaktens föreskriftsrätt övertas av KBM när en ny, utvidgad förordning om signalskyddet träder i kraft.

Sverige har på senare år deltagit alltmer aktivt i internationella signalskyddssammanhang. För att det internationella arbetet skall vara väl koordinerat behövs en utpekad National Communications Security Agency (NCSA), det vill säga en organisation i landet som ansvarar för signalskyddsfrågor, och en National Distribution Agency (NDA), en organisation som är behörig att distribuera kryptonycklar.

Försvarsmakten har ansökt om att få fylla dessa funktioner. Utredningen anser det nödvändigt för att det internationella arbetet på signalskyddsområdet skall fungera att detta förhållande avgörs. Det är inte minst viktigt för att Sverige, liksom andra medlemsländer, förväntas bidra till kvalificerad informationssäkerhet för EU. Det är också nödvändigt för att anpassa Sverige till de regler som används i internationella insatser. Ett avgörande kan innebära att Försvarsmaktens roll som NCSA och NDA formaliseras eller att annan myndighet utses. Utredningen föreslår att den nybildade myndigheten, IST, ges uppgifterna som NCSA och NDA.

4.5 Övriga organisatoriska förslag

4.5.1 Sitic – Sveriges IT-incidentcentrum

Sveriges IT-incidentcentrum, Sitic vid Post- och telestyrelsen (PTS) ansvarar för systemet för informationsutbyte om IT-incidenter mellan samhällets alla aktörer - myndigheter, kommuner, organisationer, näringsliv och enskilda. Uppgiften är bland annat att snabbt sprida information om IT-incidenter, att lämna information och råd om förebyggande åtgärder, att sammanställa och ge ut statistik som underlag för kontinuerliga förbättringar i det förebyggande arbetet.

Sitic samverkar med bland annat KBM, FRA, Statskontoret, RPS, Säkerhetspolisen och FMV i uppbyggnaden av centrumet.

Inrättandet av Sitic innebär inget avsteg från ansvarsprincipen. Varje myndighet eller annan organisation ansvarar själv för sin informationssäkerhet.

Sitic lämnar också förebyggande information, dels som publiceras som förebyggande råd, dels i seminarieform. Statistik förs över IT-incidenter och Sitic har bidragit till det testverktyg för IT-säkerhet som finns på PTS webbplats.

Internationella kontakter och samarbete är av avgörande betydelse för ett incidentcentrum för tillgång till omedelbar information och erfarenhetsutbyte. Inom EU deltar Sitic bland annat i EGC-gruppen, the European Government CERT Group, där liknande nationella centra ingår. Sitic är också en av 1990-talet ackrediterade medlemmar i den europeiska organisationen Task Force Collaboration of Security Incident Response Teams (TF-CSIRT). Ackrediteringen innebär att centrat uppfyller kriterierna för fullständig medverkan i organisationens hantering av incident- och sårbarhetsinformation.

Sitic är även fullvärdig medlem i Forum of Incident Response and Security Teams, FIRST. Det är en global organisation bestående av incidenthanteringsgrupper som tillsammans hanterar och förebygger incidenter inom området informationssäkerhet.

Rapporteringen av incidenter till Sitic har blivit mindre än förväntat från starten. Det beror på flera orsaker. Många känner fortfarande inte till Sitics arbete. Statliga myndigheter och kommuner är inte skyldiga att rapportera incidenter. Sekretessfrågan var initialt oklar, varför många företag tvekade att rapportera av sekretesskäl. Allt fler luckor i säkerhetssystemen rapporteras direkt från programleverantörerna. Marknaden erbjuder också program med allt snabbare uppdatering av bland annat virusskydd och brandväggar, vilket har en god förebyggande effekt. Samtidigt ökar mängden skadlig kod som sprids i näten från år till år.

Statistikföringen fyller ändå en funktion för att spegla frekvensen och förekomsten av IT-incidenter som kan jämföras med internationell statistik. Den är ett komplement till Sitics arbete med identifiering av risker och uppgifterna att lämna information och råd.

Om Sitic skall fungera som avsett krävs ett nära och förtroendefullt samarbete med andra aktörer inom informationssäkerhetsområdet, inte minst med KBM och den nya myndigheten, IST, som föreslås få särskilt samordnande uppgifter för den nationella informationssäkerheten. Det är angeläget att

sådana väl fungerande samarbetskanaler finns såväl på ledningsnivå i myndigheterna som på handläggarnivå. Utredningen anser att särskild vikt bör läggas vid att upprätthålla ett väl fungerande samarbete.

Sitic har en budgetomslutning på 15 miljoner kronor. Personalstyrkan är drygt 10 personer. En mera utåtriktad förebyggande information från Sitic kan kräva ytterligare resurser. Finansieringen sker för närvarande ur KBM:s så kallade civila ram. Utredningen föreslår att verksamheten, som numera kan ses som permanent, finansieras med ordinarie anslagsmedel, vilket kan ske genom att den civila ramen reduceras i motsvarande grad.

4.5.2 Certifieringsorganet för Common Criteria

Det nationella systemet för evaluering och certifiering av IT-säkerhet i produkter och system i enlighet med IS 15408 Evalueringskriterier för IT-säkerhet i produkter och system (Common Criteria) etablerades efter riksdagens beslut under 2002. FMV har fått regeringens uppdrag att bygga upp systemet. FMV har sedan många år kontakter och samarbeten med de underrättelse- och säkerhetsmyndigheter i andra länder som är aktiva inom området. För beskrivning av informations-säkerhetsstandarden (Common Criteria) hänvisas till utredningens betänkande Säker information – förslag till informations-säkerhetspolitik (2005:42).

Certifieringsorganet är nu etablerat som en oberoende funktion inom FMV med namnet Sveriges Certifieringsorgan för IT-säkerhet, CSEC. Arbetet med att etablera certifieringsordningen är genomfört. Detta arbete omfattar bland annat utarbetande av kvalitetsmanual, ansvarsbeskrivningar, beskrivningar av processer för licensiering av evalueringslaboratorier, regler för genomförande av certifieringar samt utbildning av certifierare och evalueringsföretag.

Grundutbildningen av certifierarna avslutas under hösten. Utbildningen är ettårig och omfattar bland annat övningar där autentiska IT-produkter granskas under handledning av internationella experter. Ett utbildningsmaterial för evalueringsföretagen har utarbetats och utbildning har genomförts för dessa. Examinerade deltagare kan nu börja verka inom certifieringsförordningen. Utbildningen är regelbundet återkommande.

CSEC deltar i den internationella samarbetsorganisationen CCRA, som utvecklar standarden för granskning av IT-säkerhet i produkter och system och har där deltagit i olika arbetsgrupper. Certifieringsorganet har i år deltagit i den slutliga tekniska beredningen av den nya versionen av Common Criteria, liksom i granskningen av Tysklands certifieringsorgan.

Ansökan för ackreditering av CSEC till Styrelsen för ackreditering och teknisk kontroll (Swedac) lämnas under hösten 2005. CSEC är därmed redo att genomföra de första certifieringsuppdragen. Uppbyggnaden av verksamheten har tagit tre år. Härnäst genomförs certifieringar, varefter CCRA granskar det svenska systemet. Det internationella erkännandet av certifieringsordningen kan förväntas före utgången av 2006.

Utredningen finner att de motiv som anfördes inför riksdagsbeslutet om etableringen av ett svenskt system för evaluering och certifiering alltjämt är giltiga. Utredningen har också i tidigare betänkanden betonat vikten av att tillämpa existerande internationella standarder inom IT-säkerhetsområdet. Common Criteria syftar till att sammankoppla ledningsfunktioner, inklusive riskhantering, och mer detaljerade tekniska specialstandarder med hur krav på säkerhets- och skyddsfunktioner ska kunna härledas, uttryckas och verifieras i de tekniska lösningarna i IT-produkter och program.

Utredningen har tagit del av rapporter och synpunkter från FMV och Swedac och funnit att det föreligger skilda uppfattningar om vem som har huvudansvaret för den nationella certifieringsordningen, certifieringsorganet eller signatären. Dessa skillnader har skapat oklarheter varför instruktion bör ges till berörda myndigheter som tydliggör deras roller.

Swedac har framfört att signatärskapet bör handhas av en myndighet som har ett övergripande föreskrivande ansvar för informationssäkerhet. Utredningen delar denna uppfattning och anser därför att signatärskapet bör föras över till KBM. Detta bör genomföras snarast. Samtidigt är det angeläget att såväl Swedacs som CSEC:s kompetens i tekniska frågor tas tillvara.

Swedacs uppgifter och roll för ackreditering och teknisk kontroll föreslås i övrigt oförändrad.

CSEC beräknas för 2006 ha en budgetomslutning på 12 miljoner kronor. Antalet sysselsatta motsvarar 8 heltidstjänster. Finansieringen har hittills skett genom projektmedel från KBM:s så kallade civila ram. När verksamheten med certifiering har kommit igång tillkommer vissa avgiftsintäkter.

För kostnader som kan hänföras till enskilda certifieringar, bör kostnadstäckande avgifter tas ut enligt sedvanliga principer för avgiftsfinansiering. Kostnaden för grundverksamheten beräknas dock ligga kvar i stort sett på nuvarande nivå.

Utredningen föreslår att CSEC:s grundverksamhet i framtiden finansieras genom ordinarie anslagsmedel då den fyller en viktig roll i arbetet för säkrare IT-produkter och program och då verksamheten nu kan betraktas som etablerad. Finansiering bör ske genom motsvarande reduktion av den så kallade civila ramen.

4.5.3 Rikspolisstyrelsen och Statens kriminaltekniska laboratorium

Utredningen har i tidigare betänkanden framhållit att det statliga åtagandet medför krav på att bygga upp förmåga inom flera viktiga områden och att lösa ett antal uppgifter i den statliga verksamheten. Långt ifrån alla krav eller uppgifter är beroende av hur staten organiserar sin verksamhet. Inom några områden kan det dock enligt utredningens mening finnas anledning att ytterligare tydliggöra vissa myndigheters ansvar och uppdrag. Utredningen har i sitt tredje delbetänkande Säker Information – förslag till informationssäkerhetspolitik (SOU 2005:42) föreslagit att den nationella strategin utvecklas till att omfatta förebyggande och förberedande insatser, liksom åtgärder som förstärker förmågan att upptäcka störningar och ingripa vid misstanke om brott. För några av de myndigheter som idag har föreskriftsrätt i frågor som berör informationssäkerhet kan det således finnas anledning att ytterligare förtydliga detta uppdrag och att tilldela resurser för uppgiften

Polisväsendet har ett brett mandat inom brottsbekämpning, med stöd av flera lagar och förordningar. Säkerhetspolisen har dessutom den föreskriftsrätt som följer av Säkerhetsskyddsförordningen (1996:627). Huvudsyftet enligt säkerhetsskyddslagen är att kunna upptäcka, ingripa och utreda misstankar om brott mot rikets säkerhet.[44] Med föreskriftsrätten följer också uppgiften att ge mer praktiskt inriktade råd och anvisningar för myndigheter, kommuner och vissa företag.

Allvarliga IT-incidenter utgör i grunden ofta brott. Inom informationssäkerhetsområdet har det visat sig att en rad myndigheter och andra organisationer har behov av polisens

[44] Brottsbalken (1962:700) kap. 19.

medverkan i olika arbets- och samverkansgrupper. Polisen och Säkerhetspolisen kan genom sina operativa uppdrag tillföra erfarenheter inom området.

Rikskriminalpolisen är Sveriges kontaktpunkt inom ramen för G8:s 24/7 High Tech Crime arrangemang och Interpols National Central Reference Point System, NCRP, vilket understryker att polisen är en viktig aktör i samhällets informationssäkerhetsarbete.

För att möta dessa omvärldskrav och ett önskemål om samordning internt inom polisen, har en för Rikskriminalpolisen och Säkerhetspolisen gemensam funktion S-BIT etablerats. Då verksamheten inte fått öronmärkta medel för området har funktionen endast ett begränsat antal tjänster, mot planerade 12. För att leva upp till de beskrivna målen och de krav och önskemål som ställs på polisen inom området informationssäkerhet är det önskvärt att särskilda medel kan avsättas för ändamålet. S-BIT:s verksamhet bör därför delvis finansieras med medel ur KBM:s så kallade civila ram eller genom anslagstilldelning.

Allt större del av den brottsutredande verksamheten kommer i kontakt med IT och kräver kunskaper om bevissäkring och undersökning i IT-miljö, så kallad IT-forensisk verksamhet. Inom det IT-forensiska området och vid vissa tekniska problem, lämnar FRA i vissa fall stöd till polisen. Det är dock viktigt att påpeka att kriminalteknisk verksamhet i huvudsak bedrivs inom polisen, Säkerhetspolisen och Statens Kriminaltekniska Laboratorium, SKL. Det är därför av vikt att metodutvecklingen vad gäller IT-forensisk verksamhet sker inom polisen, i första hand vid SKL. Den föreslagna myndigheten, IST, bör dock kunna vara en stödjande resurs, särskilt ifråga om kryptologisk kompetens.

Enligt utredningen är det nödvändigt att Säkerhetspolisen har tydliga mandat och resurser att bedriva uppsökande och rådgivande verksamhet inom området informationssäkerhet

Utredningen har pekat ut ett särskilt ansvar för staten ifråga om informationssäkerheten i all samhällsviktig verksamhet, oavsett om den är i privat eller offentlig ägo. För Säkerhetspolisen liksom för andra myndigheter som idag bedriver verksamhet med stöd av sin föreskriftsrätt är det därför enligt utredningen önskvärt att denna inriktning tydliggörs. Det kan utgöra ett stöd i Säkerhetspolisens prioriteringar och inriktning av den egna verksamheten.

5 Ekonomiska konsekvenser av utredningens förslag

Utredningens förslag innebär en höjd ambitionsnivå för samhällets informationssäkerhet. Vissa av förslagen medför ökade kostnader. Det gäller dels ökade resursbehov vid Krisberedskapsmyndigheten (KBM), dels vid den föreslagna myndigheten, IST, som föreslås få policyansvar och administrativt samordnande ansvar respektive tekniskt samordnande ansvar för samhällets informationssäkerhet.

Finansiering föreslås ske genom avräkning från KBM:s så kallade civila ram, 7:5 Krisberedskap. Efter avräkning av medel ur anslaget 7:5 Krisberedskap kvarstår ett ökat anslagsbehov med 43 miljoner kronor per år för att kunna genomföra utredningens förslag till förbättrad informationssäkerhet.

Utredningen föreslår en överflyttning av ansvar och verksamhet för signalskydd från Försvarsmakten, MUST Säkerhetskontor, till den nybildade myndigheten, IST. Även KBM:s ansvar och verksamhet för signalskydd föreslås överflyttat till IST. Det administrativa godkännandet av signalskyddssystem föreslås dock placeras vid KBM.

Utredningen föreslår också en överföring av huvudmannaskapet för signalskyddsutbildningen från Försvarsmakten till KBM. Förslagen avses ej få direkta kostnadseffekter för statsbudgeten.

Vidare föreslås att finansieringen av Sitic – Sveriges IT-incidentcentrum vid Post och telestyrelsen och CSEC – Sveriges Certifieringsorgan för IT-säkerhet skall finansieras via anslag. De har hittills finansierats via projektmedel ur KBM:s civila ram. Den civila ramen föreslås reducerad i motsvarande grad.

Utredningen har också i sitt tidigare betänkande Säker information – förslag till informationssäkerhetspolitik (2005:42) föreslagit att KBM genom sin roll i forskningshänseende bör utveckla ett tematiskt forskningsområde kring Informationssäkerhet. För att en satsning skall uppfattas som meningsfull inom forskarsamhället bör den årliga ramen vara 10-15

miljoner kronor, beroende på medfinansiering. Finansieringen av KBM:s insats i en sådan satsning föreslås ske via projektmedel ur den civila ramen.

Utredningen har i samma betänkande även understrukit den betydelse som beräkningskraft vid nuvarande FRA, i form av datorer med mycket hög kapacitet, har för signalskyddet och informationssäkerheten. Utredningen konstaterade att beräkningskraften kontinuerligt måste öka men att takten i dag är för låg. Detta leder till att den nationella informationssäkerheten inte kommer att möta framtidens krav. Frågan om en finansiering av en nödvändig uppgradering av beräkningskraften måste därför lösas i samband med att den nya myndigheten etableras.

5.1 Resursbehov vid Krisberedskapsmyndigheten

Huvudfinansiering av informationssäkerhetsarbetet bör ske genom myndigheternas sakanslag. Sådan verksamhet som har en direkt koppling till fredstida krishantering bör även fortsättningsvis finansieras ur civila ramen 7:5 Krisberedskap.

Utredningens förslag innebär att verksamheten för informationssäkerhet och analys utvecklas och breddas. Det gäller omvärldsbevakning och analys avseende hot, sårbarheter, risker och skydd inom området informationssäkerhet, resurser för samordning inom forskning, EU, internationella frågor och gentemot andra myndigheter och kommuner. Vidare gäller det samverkan med näringslivet samt det förebyggande arbetet, stödet till olika aktörer, utbildnings- och medvetandehöjande aktiviteter riktade till utbildningsväsendet och allmänheten samt scenario- och övningsverksamhet. Tillkommande anslagsbehov härför beräknas till 30 miljoner kronor.

Övningsverksamhet, uppbyggnad av förmåga att leda verksamhet vid inträffade händelser samt för att utveckla frivilligkompetens bör även fortsättningsvis finansieras ur civila ramen.

Överföringen av signalskyddsansvaret från KBM till den nya myndigheten reducerar KBM:s kostnader med 10 miljoner kronor. Dock tillkommer vissa tjänster som en följd av KBM:s föreslagna roll som ansvarig för administrativt godkännande av signalskyddssystem. Netto beräknas KBM:s kostnader för uppgifter inom signalskyddet reduceras med ca 7 miljoner kronor.

Överföringen av huvudmannaskapet för signalskyddsutbildningen har beräknats ske genom överföring av anslag utan kostnadseffekter.

Totalt beräknas tillkommande anslagsbehov, exklusive signalskyddsutbildning, därför netto för KBM till 23 miljoner kronor.

5.2 Resursbehov vid den nya myndigheten, ITS

Teknikkompetensfunktionen (TKF) vid Försvarets radioanstalt (FRA) har hittills finansierats genom projektanslag från KBM:s så kallade civila ram med 15 miljoner kronor per år. Härtill kommer intäkter av uppdrag åt statliga myndigheter och statligt ägda bolag för aktiv IT-kontroll och IT-säkerhetsanalyser med ca 6 miljoner kronor per år.

Utredningen beräknar det totala resursbehovet för TKF till 35 miljoner kronor för att möta behovet av en förbättrad informationssäkerhet med stöd till myndigheter och samhällsviktig verksamhet.

Finansieringen via den civila ramen, 15 miljoner kronor per år, förslås ersättas med ordinarie anslag. Den civila ramen reduceras i motsvarande omfattning. Härtill kommer tillkommande anslagsbehov med 20 miljoner kronor för TKF för att möta en ökad ambitionsnivå och efterfrågan vad gäller informationssäkerhet, om verksamheten bedrivs utan avgiftsfinansiering.

Utredningen föreslår att den nybildade myndigheten, ITS, övertar KBM:s ansvar för den signalskyddsverksamhet som främst bedrivs i Sollefteå. Anslag härför, 10 miljoner kronor, tillförs ITS. En reduktion genomförs av KBM:s anslag enligt 5.1. KBM:s övriga verksamhet i Sollefteå påverkas ej av förändringen.

Ansvaret för signalskydd överförs från Försvarsmakten, MUST Säkerhetskontor, till ITS. Motsvarande överföring sker av anslaget härför. Överföringen har beräknats kunna ske utan tillkommande nettokostnader.

5.3 Sitic – Sveriges IT-incidentcentrum

Sveriges IT-incidentcentrum vid Post- och Telestyrelsen har en budgetomslutning på 15 miljoner kronor som hittills finansierats med projektmedel ur KBM:s civila ram. Utredningen föreslår att

verksamheten fortsättningsvis finansieras via ordinarie anslag och att den civila ramen reduceras i motsvarande grad.

5.4 CSEC – Sveriges Certifieringsorgan för IT-säkerhet

Sveriges Certifieringsorgan för IT-säkerhet vid Försvarets materielverk beräknas i full funktion ha en budgetomslutning på 12 miljoner kronor. I framtiden tillkommer avgiftsintäkter. Utredningen föreslår att CSEC:s grundverksamhet i framtiden finansieras via ordinarie anslag och att den civila ramen reduceras i motsvarande grad.

5.5 Rikspolisstyrelsen

För Rikskriminalpolisens och Säkerhetspolisens gemensamma funktion S-BIT har ett resursbehov motsvarande tolv personer beräknats. Därav har resurser motsvarande tre personer tillförts genom omprioriteringar i verksamheten. Ett belopp om 10 miljoner kronor bör därför överföras från KBM:s civila ram, som föreslås reduceras i motsvarande grad. Därutöver förutsätter utredningen att den nya myndigheten, ITS, skall kunna lämna tekniskt stöd utan kostnad för Rikskriminalpolisen och Säkerhetspolisen.

6 Utredningens arbete

Föreliggande betänkande, Informationssäkerhetspolitik – organisatoriska konsekvenser, är InfoSäkutredningens slutbetänkande. Tidigare betänkanden är InfoSäkutredningen – delrapport 1 om signalskydd (SOU 2003:27), Informationssäkerhet i Sverige och internationellt – en översikt (SOU 2004:32) samt Säker information – förslag till informationssäkerhetspolitik (SOU 2005:42).

Utredningen har sedan starten 2002 fått tilläggsdirektiv vid flera tillfällen. Det ursprungliga direktivet omfattade organisering av signalskydd och tilläggsdirektiv gav utredningen uppdrag att utvärdera den organisatoriska fördelning av funktioner på informationssäkerhetsområdet som gjordes med anledning av Samhällets säkerhet och beredskap (prop. 2001/02:158). Totalförsvarets forskningsinstitut (FOI), skrev på utredningens uppdrag rapporten Underlag för utvärdering av uppgiftsfördelning inom informationssäkerhetsområdet (FOI-R—1369—SE). Detta material, i kombination med utredningens egna kontakter, har varit underlag för utredningens analys av rådande uppgiftsfördelning.

Ett av uppdragen inom ramen för direktivet var internationell jämförelse och med anledning av det företog utredningen ett antal studieresor (Australien, Frankrike, Norge, Storbritannien, USA och Tyskland). För att komplettera det internationella materialet uppdrog utredningen åt KBM att göra en länderanalys med betoning på organisering av informationssäkerhetsarbetet.

För att belysa de frågor som direktiv och tilläggsdirektiv stipulerade har utredningen haft en expertgrupp med representanter för de myndigheter som är närmast berörda av frågorna. Utredningen har också sammanträffat med representanter för näringslivet.

Flertalet sakkunniga och experter har medverkat med värdefullt underlag i utredningens arbete.

De ekonomiska konsekvenserna av utredningens förslag redovisas i detta slutbetänkande. Vad gäller andra viktiga områden, såsom kommunal självstyrelse, brottslighet, sysselsättning och offentlig service i olika delar av landet, småföretag, jämställdheten mellan kvinnor och män, integrationspolitiska mål samt personlig integritet, så har utredningen gjort bedömningen att dessa inte påverkas i nämnvärd utsträckning av utredningens förslag.

Särskilt yttrande av experterna Stefan Kristiansson och Håkan Gustafsson

Med anledning av den inriktning som utredningen har tagit under dess absoluta slutskede, har vi som Försvarsmaktens experter funnit oss föranledda att lämna ett särskilt yttrande dels över hur utredningen har genomförts, dels utredarens förslag.

Inledningsvis vill vi dock bejaka stora delar av utredningens innehåll bl.a. behovet av en övergripande nationell informationssäkerhetsstrategi. Vi kan däremot inte ställa oss bakom utredarens förslag i kapitel 4 Organisatoriska konsekvenser av utredningens förslag samt kapitel 5 Ekonomiska konsekvenser av utredningens förslag.

Fram till veckan före slutjustering av texten beskrevs inte Försvarsmaktens särskilda behov, kompetens och förmåga på ett korrekt sätt. Först efter det att förslaget till organisatorisk lösning presenterats för utredningens experter och i slutjusteringsskedet av texten, har utredaren valt att införa en mer rättvisande beskrivning. Vi menar därför att förslaget till organisatorisk lösning grundats på ett bristfälligt underlag.

Vi anser att det är förvånande att utredaren i kretsen av utredningens experter inte har diskuterat den föreslagna organisationslösningen eller alternativ till densamma. Därmed torde inte heller utredarens förslag vara tillräckligt belyst.

Vi kan inte ställa oss bakom utredarens förslag till organisatorisk lösning eftersom detta inte ger Försvarsmakten nödvändiga förutsättningar att utvecklas till ett modernt insatsförsvar med snabbinsatskapacitet, vilket beslutats av statsmakterna. Det är inte rimligt att resurser, som är vitala för Försvarsmaktens utveckling inom informationssäkerhetsområdet, överförs till andra myndigheter.

Förkortningar

AQUA	Appropriately Qualified Authority
BITS	basnivå för IT-säkerhet
BSI	Bundesamt für Sicherheit in der Informationsteknik
CA	Certificate Authority
CB	Certification Body
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CSEC	Sveriges certifieringsorgan för IT-säkerhet
DNV	Det Norske Veritas
Ds	Departementsskrivelse
EGC	European Government CERT Group
EU	Europeiska Unionen
FFS	Försvarsmaktens föreskrifter
FHS	Försvarshögskolan

FIRST	Forum of Incident Response and Security Teams
FMV	Försvarets materielverk
FOI	Totalförsvarets forskningsinstitut
FRA	Försvarets radioanstalt
IEC	International Electrotechnical Commission
IP	Internet Protocol
IS	Internationell standard
ISO	International Organisation for Standardisation
IST	Institutet för signalunderrättelsetjänst och teknisk informationssäkerhet
IT	Informationsteknik
JK	Justitiekanslern
KBM	Krisberedskapsmyndigheten
KBV	Kustbevakningen
Kom	Kommissionen i EU
KOS	kommunikationsspaning (i signalspaning)
LEK	Lag (2003:389) om elektronisk kommunikation
LIS	ledningssystem för informationssäkerhet
MUST	Militära underrättelse- och säkerhetstjänsten
NCSA	National Communication Security Agency
OECD	Organisation for Economic Co-operation and Development

PKI	Public Key Infrastructure
PTS	Post- och telestyrelsen
PUL	Personuppgiftslagen (1998:204)
RKP	Rikskriminalpolisen
RPS	Rikspolisstyrelsen
RSA	risk- och sårbarhetsanalyser
RÖS	röjande signaler
Samfi	KBM:s samverkansgrupp för informationssäkerhet
S-BIT	Samordningsfunktionen för brottsrelaterade IT-incidenter
SGSIS	Svenska statens säkra Intranät
SHS	spridnings- och hämtningssystem
SIS	Standardisering i Sverige
Sitic	Sveriges IT-incidentcentrum
SKL	Statens kriminaltekniska laboratorium
SOU	Statens offentliga utredningar
SRV	Statens räddningsverk
SPF	Styrelsen för psykologiskt försvar
Swedac	Styrelsen för ackreditering och teknisk kontroll
TES	teknisk signalspaning
TESTA	Trans-European Services for Telematics between Administrations (EU:s IP-baserade nätverk)

TF-CSIRT	Task Force Collaboration of Security Incident Response Team
TKF	teknikkompetensfunktion
TSA	Totalförsvarets signalskyddssamordning
TSS	Totalförsvarets signalskyddsskola
UE	Union Européenne (Europeiska Unionen)

Kommittédirektiv

Angående vissa frågor om informationssäkerheten i samhället

Dir. 2002:103

Beslut vid regeringssammanträde den 11 juli 2002

Sammanfattning av uppdraget

En utredare skall lämna förslag på hur signalskyddsverksamheten i samhället skall utformas. I uppdraget ingår att bedöma behovet av signalskydd i samhällsviktig verksamhet samt att lämna förslag till organisatorisk placering, lokalisering, uppgifter, ledning och samordning av signalskyddstjänsten.

Den särskilda utredaren kommer också att få i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas och till hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden. Utredaren planeras också få uppdraget att genomföra den utvärdering som regeringen aviserat i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158).

Regeringen avser att återkomma under hösten med tilläggsdirektiv när det gäller dessa uppdrag.

Inledning

I takt med att samhället har blivit allt mer beroende av olika informationssystem har vikten av att förbereda sig för hot av olika slag ökat. Regeringen har närmare beskrivit hotbilden för attacker via informationssystem i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 104 f). Där konstateras att en av svårigheterna med hanteringen av de IT-relaterade hoten är att urskilja vem aktören är, eftersom ingen absolut åtskillnad mellan olika typer av aktörer kan göras. Detta faktum gör att det är särskilt svårt att skydda sig eftersom säkerhetsåtgärderna måste anpassas till samtliga typer av aktörer. Ytterligare en försvårande faktor är att de IT-relaterade hoten är geografiskt gränslösa. Den som vill göra

intrång i eller på annat sätt manipulera ett informationssystem i Sverige kan befinna sig var som helst i världen.

Signalskyddsverksamheten

Att skydda information som utväxlas i form av meddelanden och trafik eller information som lagras elektroniskt får allt större betydelse i dagens samhälle. Det gäller inte bara för sådan information som omfattas av bestämmelserna om sekretess i sekretesslagen (1980:100), utan också för andra uppgifter som hanteras i informationssystem av olika slag i samhället. Exempel på sådan skyddsvärd information kan vara uppgifter som gäller känslig infrastruktur, ekonomi och personlig integritet.

Utvecklingen av dagens signalskyddssystem sker till största delen inom Försvarsmakten utifrån de krav som behovet av att kunna hantera information som omfattas av sekretess till skydd för rikets säkerhet ställer. Utvecklingen av IT-säkerhetslösningar i samhället i övrigt styrs allt mer av behovet av att skydda information som inte omfattas av sekretess till skydd för rikets säkerhet. En utveckling av signalskyddstjänsten till att även kunna hantera andra kryptografiska skyddsbehov än de som utvecklas för totalförsvarsändamål och en bedömning av hela samhällets skyddsförmåga är därför påkallad.

Signalskyddstjänsten leds idag av en funktion inom Försvarsmakten (MUST/TSA). Att signalskyddstjänstens ledning organisatoriskt har denna placering kan innebära en risk för att de civila behoven inte prioriteras tillräckligt. Frågan om var signalskyddstjänsten på nationell nivå skall organiseras och lokaliseras bör därför övervägas.

I propositionen Ett informationssamhälle för alla (prop. 1999/2000:86) angav regeringen att den välkomnar en bred användning av kryptografi. Mot denna bakgrund bör det eventuellt finnas en rådgivande funktion i kryptografifrågor i Sverige. Därför finns behov av att undersöka i vad mån signalskyddstjänsten kan utgöra ett sådant rådgivande organ i samhället.

Det ökade samarbetet med andra stater och internationella organisationer medför vidare ett ökat statligt behov av att kunna hantera signalskyddsutrustning och kryptonycklar även i internationella sammanhang. Det bör övervägas om signalskyddstjänsten kan bistå i den utvecklingen.

Arbetet med informationssäkerhet inom offentlig sektor

Regeringen har i propositionerna Fortsatt förnyelse av totalförsvaret (prop. 2001/02:10, bet. 2001/02:FöU02, rskr. 2001/02:91) och Samhällets säkerhet och beredskap (prop. 2001/02:158, bet. 2001/02:FöU10, rskr 2001/02:261) redovisat sin strategi och förslag till åtgärder för att stärka informationssäkerheten i samhället och skyddet av de samhällsviktiga systemen. I propositionen Samhällets säkerhet och beredskap vidgades åtgärderna från att endast omfatta IT-säkerhet till att täcka hela informationssäkerhetsområdet. Det tidigare använda mer oprecisa begreppet ”informationsoperationer” utmönstrades därmed ur terminologin.

Regeringen har angett att målet bör vara att man skall upprätthålla en så hög informationssäkerhet i hela samhället att störningar i samhällsviktig verksamhet kan förhindras eller hanteras. Strategin för att uppnå detta mål liksom för övrig krishantering i samhället utgår från ansvarsprincipen, likhetsprincipen och närhetsprincipen.

Som ett första steg i en samlad strategi i informationssäkerhetsarbetet har fyra myndigheter fr.o.m. andra halvåret 2002 fått nya uppgifter. Dessa myndigheter är Krisberedskapsmyndigheten, Post- och telestyrelsen, Försvarets radioanstalt och Försvarets materielverk.

Detta första steg skall utvärderas efter två år som regeringen förutskickat i propositionen Samhällets säkerhet och beredskap.

Med anledning av att det finns många företag som är verksamma inom informationssäkerhetsområdet finns det dock skäl att ytterligare överväga vilken verksamhet staten skall bedriva inom detta område. Härvid skall beaktas att konkurrensen på den öppna marknaden inte får påverkas negativt.

Regeringen finner att de bästa förutsättningarna för ett gott beslutsunderlag kan skapas genom att utvecklingen inom informationssäkerhetsområdet följs.

Internationell verksamhet

Genom att hoten mot informationssystemen inte bara är en svensk angelägenhet, utan är av global natur, krävs internationell samverkan. Sådan samverkan bedrivs på flera olika områden, bl.a. inom EU. Olika myndigheter medverkar vidare i internationell samverkan som i regel har informationsutbyte som syfte. För att Sverige skall

få genomslag i sitt agerande på den internationella arenan bör det finnas en övergripande inriktning. Inriktningen bör också knyta an till och vara anpassad till respektive myndighets ansvarsområde.

Uppdraget

Den särskilda utredaren skall bedöma behovet av signalskydd i samhällsviktig verksamhet och lämna förslag på hur signalskyddsverksamheten i samhället skall utformas. Utredaren skall mot bakgrund av utvecklingen inom informationssäkerhetsområdet föreslå hur signalskyddstjänsten i Sverige skall vara organiserad. Utredaren skall också belysa hur signalskyddsutbildningen skall organiseras och var den skall lokaliseras.

Följande frågor bör besvaras.

- Hur bör signalskyddsverksamheten utvecklas så att den kan komma till nytta inom fler samhällssektorer?
- Vilka samhällssektorer har störst behov av signalskydd och vilka krav ställer de?
- Vem skall vara ansvarig för signalskyddet och hur skall detta vara organiserat?
- Vilka uppgifter skall signalskyddstjänsten ha och hur skall ledning och samordning ske?
- Hur säkerställs att det framtida behovet av kompetens inom det kryptografiska området kan tillgodoses?
- Hur säkerställs samordning med andra länders signalskyddsorganisationer på ett förtroendefullt och säkerhetsmässigt trovärdigt sätt?
- Hur åstadkoms en nationell distributionsfunktion för signalskyddsmateriel och signalskyddsnycklar för det internationella samarbetet?

Utredaren kommer att få i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas och hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet skall utformas i framtiden. I detta arbete skall gränsdragningsfrågor särskilt beaktas gentemot den översyn av de rättsliga aspekterna, inklusive de internationella, på området för informationssäkerhet som Justitiedepartementet avser att genomföra (jfr. prop. 2001/2002:158).

Utredaren planeras också få uppdraget att genomföra den ovan nämnda utvärderingen.

Direktiv angående dessa två senare uppdrag avser regeringen att återkomma med under hösten 2002 som tilläggsdirektiv.

Samråd och avrapportering

Utredaren skall bedriva arbetet i nära samarbete med Försvarsmakten, Försvarets radioanstalt, Rikspolisstyrelsen och Krisberedskapsmyndigheten.

Inom Regeringskansliet finns en informell grupp bestående av representanter från Justitiedepartementet, Utrikesdepartementet, Försvarsdepartementet och Näringsdepartementet som utbyter information i dessa frågor. Denna grupp bör utredaren använda som referensgrupp i arbetet. Även andra kontakter bör tas.

Utredaren skall lämna delrapport om signalskyddstjänsten senast den 28 februari 2003.

Utredaren skall lämna slutrapport senast den 6 maj 2005.

(Försvarsdepartementet)

Kommittédirektiv

Tilläggsdirektiv till utredningen angående vissa frågor om informationssäkerheten i samhället (Fö 2002:06)

Dir. 2003:29

Beslut vid regeringssammanträde den 20 februari 2003

Sammanfattning av uppdraget

Utredningen angående vissa frågor om informationssäkerheten i samhället skall lämna förslag till hur den nationella strategin för informationssäkerhetsarbetetbör utvecklas samt hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet skall utformas. I propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) anmälde regeringen sin avsikt att göra en utvärdering av de bedömningar som regeringen gjorde inom informationssäkerhetsområdet. Utredaren skall följa myndigheternas uppbyggnad av den informationssäkerhetsverksamhet som regeringen har givit myndigheterna i uppgift enligt propositionen. Utredaren skall vidare lämna förslag till hur OECD:s riktlinjer om nät- och informationssäkerhet kan genomföras.

Bakgrund

Med stöd av regeringens bemyndigande den 11 juli 2002 (dir. 2002:103) tillkallade chefen för Försvarsdepartementet en särskild utredare med uppdrag att föreslå hur signalskyddsverksamheten i samhället skall utformas. Utredaren skall enligt direktiven lämna en delrapport avseende detta uppdrag den 28 februari 2003. Regeringen angav i direktiven att den avsåg att återkomma med tilläggsdirektiv angående uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas och till hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden.

OECD (Organisation for Economic Co-operation and Development) antog den 25 juli 2002 en rekommendation om nya riktlinjer

för nät- och informationssäkerhet (OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security). Riktlinjerna syftar till att stödja utvecklingen av en säkerhetskultur i samhället genom att främja säkerhetstänkande vid utveckling och användning av nät och informationssystem. Riktlinjerna innehåller mål och principer för utvecklingen av nya nät och informationssystem.

Uppdraget

En utvecklad svensk informationssäkerhetsstrategi

Utredaren skall i det fortsatta arbetet, utöver det tidigare lämnade uppdraget, även lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas. Den i prop. 2001/02:158 s. 103 redovisade strategin för informationssäkerhetsarbetet skall utgöra grunden.

Utredaren skall göra jämförelser med hur andra länder har hanterat informationssäkerhetsfrågan när det gäller strategi, organisation och andra förhållanden som kan vara relevanta.

I sitt arbete skall utredaren beakta OECD:s riktlinjer för nät- och informationssäkerhet och lämna förslag till hur riktlinjerna kan genomföras i utredarens förslag.

Följande frågor skall besvaras.

- Hur bör den nationella strategin för informationssäkerhet vidareutvecklas?
- Hur säkerställs att den nationella strategin för informationssäkerhet möter de krav som ställs via det multinationella samarbete Sverige deltar i, främst EU?
- Utifrån en nationell strategi behöver den nuvarande samordningen av Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet förändras?
- Inom vilka delar av informationssäkerhetsområdet bör staten ha ett särskilt ansvar?
- Hur skall informationssäkerhetsarbetet finansieras?

Utvärdering förutskickad i prop. 2001/02:158

I propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) redovisade regeringen att de nya uppgifterna på informationssäkerhetsområdet skulle fördelas på de myndigheter som redan hade närliggande verksamhet. Regeringen anmälde också att man hade för avsikt att göra en utvärdering av denna fördelning av uppgifterna inom informationssäkerhetsområdet. Regeringen uteslöt inte att det skulle kunna finnas andra organisatoriska lösningar eller andra verksamheter inom informationssäkerhetsområdet som skulle kunna behövas ses över.

Som en förberedelse inför denna utvärdering skall utredaren skapa sig en god uppfattning av det ändamålsenliga i propositionens bedömningar att dela upp de nya uppgifterna genom att följa uppbyggnaden av verksamheten inom informationssäkerhetsområdet vid Krisberedskapsmyndigheten, Försvarets radioanstalt, Förvarets materielverk och Post- och telestyrelsen, inklusive den sistnämnda myndighetens uppdrag att inrätta en rikscentral för IT-incidentrapportering. Regeringen avser att återkomma till frågan om utvärderingen.

Författningsfrågor

Om utredaren finner att det finns ett behov av att föreslå författningsändringar skall utredaren lämna lagtekniskt genomarbetade förslag vid varje rapporteringstillfälle.

I detta arbete skall gränsdragningsfrågor särskilt beaktas gentemot den översyn av de rättsliga aspekterna, inklusive de internationella, på området för informationssäkerhet som Justitiedepartementet avser att låta genomföra (jfr. prop. 2001/02:158 s. 106).

I den mån det uppkommer frågor som rör behandling av personuppgifter skall de bestämmelser om skydd för den personliga integriteten vid behandling av sådana uppgifter som bl.a. finns i personuppgiftslagen (1998:204) och EG-direktivet om personuppgifter (95/46/EG) beaktas.

Utredningsarbetet

I sitt arbete skall utredningen ta hänsyn till OECD:s riktlinjer för nät- och informationssäkerhet.

Utredningen skall bedriva arbetet i nära samarbete med Rikspolisstyrelsen, Säkerhetspolisen, Datainspektionen, Statskontoret, Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk, Krisberedskapsmyndigheten, Totalförsvarets forskningsinstitut och Post- och telestyrelsen. Utredningen skall också ta de kontakter som behövs med viktiga IT-användare och andra intressenter, både inom den offentliga sektorn och i näringslivet, för att få en bild av vilka roller de spelar i informationssäkerhetsarbetet, deras behov och önskemål.

Utredningen skall utöver det som angavs i direktiven (2002:103) om att slutrapport skall lämnas senast 6 maj 2005 också lämna en delrapport angående uppdragen i detta tilläggsdirektiv senast den 1 mars 2004.

(Försvarsdepartementet)

Kommittédirektiv

Tilläggsdirektiv till utredningen angående vissa frågor om informationssäkerheten i samhället (Fö 2002:06)

Dir. 2004:46

Beslut vid regeringssammanträde den 7 april 2004.

Sammanfattning av uppdraget

Utredningen angående vissa frågor om informationssäkerheten i samhället skall genomföra den utvärdering som regeringen anmälde till riksdagen i proposition Samhällets säkerhet och beredskap (prop. 2001/02:158) vad avser de bedömningar som regeringen gjorde inom informationssäkerhetsområdet.

Bakgrund

Med stöd av regeringens bemyndigande den 11 juli 2002 (dir. 2002:103) tillkallade chefen för Försvarsdepartementet den 11 juli 2002 en särskild utredare med uppdrag att föreslå hur signalskyddsverksamheten i samhället skall utformas. Utredaren lämnade en delrapport avseende detta uppdrag den 28 februari 2003. Regeringen beslutade om tilläggsdirektiv för utredningen den 20 februari 2003 (dir. 2003:29) angående uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet för utvecklas och hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden. Utredaren fick också i uppdrag att följa myndigheternas uppbyggnad av den informationssäkerhetsverksamhet som regeringen har givit myndigheterna i uppgift enligt propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158). En delrapport skulle lämnas senast den 1 mars 2004.

I propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) redovisade regeringen att de nya uppgifterna på informationssäkerhetsområdet skulle fördelas på de myndigheter som redan hade närliggande verksamhet. Regeringen anmälde också

att man hade för avsikt att efter två år göra en utvärdering av denna fördelning av uppgifterna inom informationssäkerhetsområdet. Regeringen uteslöt inte att det skulle kunna finnas andra organisatoriska lösningar eller andra verksamheter inom informationssäkerhetsområdet som skulle kunna behövas ses över.

Uppdraget

Utredningen skall genomföra den utvärdering som regeringen anmälde till riksdagen i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) vad avser de bedömningar när det gäller uppgiftsfördelningen som regeringen gjorde inom informationssäkerhetsområdet. Utvärderingen skall redovisas i utredningens slutrapport senast den 6 maj 2005.

(Försvarsdepartementet)

Kommittédirektiv

Tilläggsdirektiv till utredningen angående vissa frågor om informationssäkerheten i samhället (Fö 2002:06)

Dir. 2005:53

Beslut vid regeringssammanträde den 28 april 2005.

Förlängd tid för uppdraget

Med stöd av regeringens bemyndigande den 11 juli 2002 tillkallade chefen för Försvarsdepartementet den 11 juli 2002 en särskild utredare med uppdrag att föreslå hur signalskyddsverksamheten i samhället skall utformas (dir. 2002:103). Utredaren lämnade en delrapport avseende detta uppdrag den 28 februari 2003. Regeringen beslutade om tilläggsdirektiv för utredningen den 20 februari 2003 (dir. 2003:29) med vilken utredningen gavs i uppdrag att lämna förslag till hur den nationella strategin för informationssäkerhetsarbetet bör utvecklas och hur Sveriges engagemang i det internationella arbetet inom informationssäkerhetsområdet bör utformas i framtiden. Utredaren lämnade en delrapport den 1 mars 2004.

Regeringen beslutade den 7 april 2004 om ytterligare tilläggsdirektiv till utredningen (dir. 2004:46) med uppdrag att genomföra den utvärdering som regeringen anmälde till riksdagen i propositionen Samhällets säkerhet och beredskap (prop. 2001/02:158 s. 105) om den i propositionen redovisade uppgiftsfördelningen mellan myndigheterna inom informationssäkerhetsområdet. Utredningen skulle enligt direktiven redovisa sitt slutbetänkande senast den 6 maj 2005.

Utredningstiden förlängs, vilket innebär att utredaren skall redovisa sitt uppdrag senast den 9 september 2005. En delrapport skall lämnas den 6 maj 2005.

(Försvarsdepartementet)

Dialoger med några privata aktörer

Utredningen har under arbetet med slutbetänkandet tagit initiativ till fortsatt dialog med ett urval aktörer från näringslivet, med erfarenheter från informationssäkerhetsarbete. Dessa har utgjort en informell referensgrupp till stöd för utredningens arbete. Dialogen har syftat till att finna förslag till avgränsning och konkretisering av såväl inriktning som former för en fördjupad samverkan mellan det privata och det offentliga. Under arbetets gång har incidenthantering, säkrare Internet, kompetensförsörjning och -utbyte samt beredning av vissa gemensamma frågor diskuterats. Vissa underhandskontakter har även tagits med Sveriges kommuner och landsting.

Flera av referensgruppens deltagare har under dialogerna betonat att de ser bristande säkerhet och tilltro till densamma som ett potentiellt hinder för framtida tillväxt., Därför arbetar flera i många sammanhang med kunder och partners i uppdrag och initiativ som syftar till att stärka säkerheten.

När det gäller informationssäkerhet framför referensgruppen ett starkt behov av att se helheten. Som en särskild utmaning ses statens arbete med informationssäkerhetsfrågor, där en stor del av både den samhällsviktiga infrastrukturen och kompetensen på IT-säkerhetsområdet finns hos näringslivet. Vetskapen om att privata och offentliga system strålar samman och påverkar varandra gör helhetssynen mer nödvändig än på många andra områden. Som utredningen framhöll i sitt delbetänkande är dessutom många privata system, som exempelvis bankernas betalningssystem, minst lika kritiska för samhällelig verksamhet som många offentliga system. Det finns således ett behov av samlad kunskap och rådgivning, även om den formella ansvarsfördelningen måste vara tydlig. Enligt referensgruppen är det därför nödvändigt att de strukturer som etableras för samverkan bidrar till att skapa

engagemang och ett förtroendefullt samarbete mellan offentliga och privata intressen.

I det tredje delbetänkandet framhöll utredningen vidare att det kan vara svårt att dra gränsen mellan vad som faller under det privata, enskilda åtagandet och vad som kan betraktas som offentligt åtagande. På motsvarande sätt är det svårt att dra gränsen mellan frågor lämpade för samverkan respektive vad som faller inom varje aktörs ansvarsområde. Enligt referensgruppen bör ansvarsprincipen, likhetsprincipen och närhetsprincipen oförändrat ligga som utgångspunkt för planeringen av samverkan mellan privat och offentligt, och då på ett tydligt sätt involvera de människor, företag och offentliga institutioner som gemensamt ansvarar för respektive problemställning. Den gemensamma ansträngningen ses som nödvändig för att effektivt förebygga, förekomma och avvärja störningar i infrastrukturen och är således inte ett sätt att lasta över de egna problemen på någon annan aktör. Utredning framförde i sitt delbetänkande att det finns samhällsviktig verksamhet både i offentliga och privata aktiviteter. Även här måste ansvarprincipen gälla i grunden, men kommuner, landsting, riksdag och regering måste när det gäller den sortens verksamhet känna – och ta - ett ökat ansvar. Detta gäller framför allt avseende normer, regler, samordning och men även finansiering. Det är svårt att entydigt precisera var dessa gränser går. Gränser måste troligtvis ständigt prövas i samråd och diskussion mellan representanter för berörda parter. Det finns enligt referensgruppen inget ”fixt och färdigt” svar.

En metod att långsiktigt få till stånd ett sådant samarbete är att etablera något slag av formell organisation. Enligt referensgruppen kan detta möjligen ske i stiftelseform, som ägs, drivs och styrs gemensamt av offentliga och privata intressen. Med ett tydligt och långsiktigt engagemang från staten bör en sådan organisation kunna delfinansieras av näringslivet. Enligt referensgruppen bör organisationen inom ramen för sin verksamhet kunna hantera frågor som rör incidenter, kunskapsutbyte och kompetensutveckling samt att stötta och utveckla svensk forskning på området. Det viktiga, enligt referensgruppens mening, är att finna en form för samverkan mellan privat och offentligt utan att rucka på ansvarsprincipen i de enskilda verksamheterna och utan att den information som är nödvändig att ta in i systemet blir offentlig i den mening att den pekar ut enskilda personer eller verksamheter. Enligt gruppen kan ingen privat verksamhet eller enskild statlig eller kommunal verksamhet ensam ta på sig den roll

som beskrivs ovan. Genom denna organisation skulle också gemensam kunskap kunna växa som är till nytta för svenskt företagande. Organisationen skulle kunna lägga ut uppgifter – inte bara till universitet och institutioner – utan också till företag. Organisationen skall också bygga upp egen kunskap, men framför allt nyttja den kunskap som redan finns i företag och institutioner. Även detta skall enligt referensgruppen ses i ett tillväxtperspektiv. Flera företag borde vara intresserade av att hitta former för att ställa sin kompetens till förfogande för en utvecklad informationssäkerhet, under förutsättning av att man kan finna en fungerande konstruktion - möjligen i någon form av partnerskap.

Frågor om säker Internet togs upp av referensgruppen. Nyttan med Internet överväger flerfaldigt riskerna, men samtidigt måste risker hållas under kontroll. På nationell nivå diskuterades tre typer av åtgärder:

- olika typer av säkerhetsbarriärer skapas, såväl vad gäller utrustning, operativt nyttjande som människan i systemet
- särskilda team måste finnas i systemet för att upptäcka attacker, finna motmedel som begränsar skadorna samt avslöjar den som angriper
- dessutom måste riskhantering vara en metod som används för att välja säkerhetstillämpningar. Helt säkra system kan inte byggas. Därför behöver vi utvärdera vilka risker vi tar. Sådana värderingar kommer att kunna göras tillgängliga på nätet som tjänster. Nationellt behöver vi komma överens om gemensamma standarder och tillämpningar för hur riskhanteringen skall tillämpas.

Eftersom Internet påverkar såväl kollektiv som personlig säkerhet har staten, enligt referensgruppen, särskilt ansvar för att leda utvecklingen av säkerheten. Samtidigt kan åtgärderna inte stanna på nationell nivå, utan det måste växa fram ett internationellt – i första hand europeiskt - sätt att gemensamt tackla dessa problem Det är då viktigt att arbeta i standardiseringsorgan och andra fora. För svenskt vidkommande innebär detta att två slags samarbete bör beslutas – ett långsiktigt och ett mer kortsiktigt.

Erfarenheten visar att informationssystemen utsätts för attacker, men också att säkerhetsnivån understundom är låg beroende på okunskap och slarv. Under lång tid har det diskuterats hur dessa erfarenheter - från både privat och offentlig verksamhet - skulle kunna tas till vara genom någon form av incidentrapportering och återkoppling med råd och stöd för att förebygga incidenter. Detta

är generellt ett svårt arbete, bland annat då det inte är bra för den egna konkurrenskraften att avslöja svagheter som det går att härleda till det egna varumärket. Dessutom framfördes meningen att samverkan mellan privat och offentligt försvåras genom den offentlighetsprincip som råder i statlig och kommunal verksamhet.

Referensgruppen menar att ett sätt att klara en samlad incidentrapportering och rådgivning för både privat och offentlig verksamhet - med respekt för offentlighetsprincipen och företagens krav på sekretess för att inte äventyra varumärket – är att bilda en gemensam organisation med uppgift att exempelvis kunna hantera incidentrapporter, ge råd i förebyggande syfte och i metodfrågor, beställa forskning och att lägga förslag till exempel inom utbildningssystemet för att höja kunskapsnivån.

Några av gruppens deltagare framförde att det finns ett långsiktigt behov av ett beredningsorgan som kan behandla frågor av karaktären lagar och förordningar, certifiering, riskhantering, kontroll, utbildning och övning. Även andra frågor av komplicerad art skulle kunna beredas för politiska ställningstaganden. Ett exempel på frågeställning som lyfts fram är att gemensamma regler för säkerhetsklassning kan växa fram för såväl civil som militär tillämpning. Detta för att kunna nyttja fördelarna av den viktiga nätverksbasering som pågår i samhället. I en sådan organisation bör såväl myndigheter som organisationer och industrier ingå. Vidare bör en sådan organisation kunna medverka i lämpliga europeiska och internationella fora för att påverka den långsiktiga inriktningen.

Kortsiktigt behövs ett organ som kan stödja statsmakterna med att främja svensk industri inom området. I EU sjösätts nu ett omfattande program på informationssäkerhetsområdet, ESP 21 (European Security Projects). Denna organisation under bildande har som syfte att stödja europeisk industri och forskning att bli starka inom säkerhetsområdet. På motsvarande sätt bör en svensk organisation växa fram, SSP 21 (Swedish Security Projects). Här kan politisk nivå, myndigheter, organisationer och industrin verka gemensamt för att ge svenska företag och forskning bästa förutsättningar för internationellt samarbete.

Referensgruppen ser gärna att ett samarbete tar hänsyn till standards - och öppna sådana - ett synsätt och område som gruppens deltagare aktivt driver i många sammanhang.

Det är angeläget att så snart som möjligt söka skapa samsyn om och hur uppbyggnaden av ett samverkansforum kan ske. Viktiga frågor är med vilka organ bilaterala överenskommelser skall göras,

hur förtroendekapital skall etableras, hur sekretesshantering skall ske etcetera. Inom ramen för denna process kommer också tillfälle ges att gå på djupet i skilda frågeställningar där samverkan mellan det privata och det offentliga innehåller betydande potentialer för skapande av mervärde, men formerna för samverkan har förhindrat eller inte möjliggjort att komma fram till lösningar.

Utredningens förslag om att snarast tillsätta en utredare eller förhandlare från statens sida välkomnas av de privata initiativtagarna, då detta på ett smidigt sätt löser kontaktytan mellan det offentliga och uppbyggnaden av ett samverkansforum.

Den tydliga behovsbild av samverkan som vuxit fram hos enskilda privata aktörer, föreningar och nätverk möjliggör att arbetet med att bygga ett samverkansforum kan fortskrida utan ett definitivt ställningstagande från vare sig staten, kommuner eller landsting. Öppenhet och lyhördhet är det sätt som säkerställer att den framtida strukturen får en sådan karaktär att hinder för offentlig medverkan undanröjes innan de uppstår.

OECD:s riktlinjer för säkerheten i informationssystem och nät

PÅ VÄG MOT EN SÄKERHETSKULTUR

ORGANISATIONEN FÖR EKONOMISKT SAMARBETE OCH UTVECKLING

ORGANISATIONEN FÖR EKONOMISKT SAMARBETE OCH UTVECKLING

Enligt artikel 1 i den konvention som undertecknades i Paris den 14 december 1960 och trädde i kraft den 30 september 1961 skall Organisationen för ekonomiskt samarbete och utveckling (OECD) verka för en politik som går ut på att

- åstadkomma högsta hållbara ekonomiska tillväxt och sysselsättning och en ökad levnadsstandard i medlemsländerna med bibehållen finansiell stabilitet, och på så sätt bidra till världsekonomins utveckling,
- bidra till en god ekonomisk utveckling i medlemsländerna och i icke-medlemsländer inom ramen för den ekonomiska utvecklingsprocessen, och
- bidra till världshandelns utveckling på multilateral och icke-diskriminerande basis i enlighet med internationella åtaganden.

De ursprungliga medlemsländerna i OECD är Österrike, Belgien, Kanada, Danmark, Frankrike, Tyskland, Grekland, Island, Irland, Italien, Luxemburg, Nederländerna, Norge, Portugal, Spanien, Sverige, Schweiz, Turkiet, Förenade kungariket och Förenta staterna. Följande länder blev medlemmar den dag som anges inom parentes: Japan (28 april 1964), Finland (28 januari 1969), Australien (7 juni 1971), Nya Zeeland (29 maj 1973), Mexiko (18 maj 1994), Republiken Tjeckien (21 december 1995), Ungern (7 maj 1996), Polen (22 november 1996), Sydkorea (12 december 1996) och Republiken Slovakien (14 december 2000). Europeiska gemenskapernas kommission deltar i OECD:s arbete (artikel 13 i OECD-konventionen).

Originally published by the OECD in English and in French under the titles:
OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: Vers une culture de la sécurité

For this Swedish edition

Published by arrangement with the OECD, Paris.
The quality of the Swedish translation and its coherence with the original text is the responsibility of the Ministry of Industry, Employment and Communications.

Originalets titel: OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security/Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: Vers une culture de la sécurité

Översättning: ÖD-översättargruppen AB

Utgiven av Näringsdepartementet efter en överenskommelse med OECD.

Version 5, 26 augusti 2005.

FÖRORD

OECD:s riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur antogs som en rekommendation från OECD-rådet vid dess 1 037:e session den 25 juli 2002.

INNEHÅLL

RIKTLINJER FÖR SÄKERHETEN I INFORMATIONSSYSTEM OCH NÄT

PÅ VÄG MOT EN SÄKERHETSKULTUR

FÖRORD

Användningen av informationssystem och nät och hela IT-miljön har förändrats dramatiskt sedan 1992, när OECD först gav ut sina Riktlinjer för säkerheten i informationssystem. Dessa fortgående förändringar innebär betydande fördelar men kräver också ett mycket starkare säkerhetstänkande av alla de myndigheter, företag, organisationer och enskilda användare som utvecklar, äger, tillhandahåller, förvaltar, underhåller och använder informationssystem och nät (”deltagare”).

I stället för de tidigare begränsade, isolerade systemen i till största delen slutna nät har vi fått allt kraftfullare persondatorer, konvergerande teknik och en utbredd användning av Internet. I dag är deltagarna allt oftare uppkopplade mot varandra och uppkopplingarna går över nationsgränserna. Dessutom stöder Internet viktiga infrastrukturer, såsom inom energi-, transport- och finanssektorerna, och spelar en viktig roll för företagens affärstransaktioner, hur stater tillhandahåller tjänster till medborgarna och hur enskilda medborgare kommunicerar och utbyter information. Också tekniken inom kommunikations- och informationsinfrastrukturen har förändrats påtagligt. Antalet varianter av accessutrustningar har mångdubblats och omfattar såväl fasta, trådlösa som mobila utrustningar, och allt fler anslutningar sker genom ständig uppkoppling. Som en följd av detta har den utväxlade informationen förändrats påtagligt i fråga om egenskaper, volym och känslighet.

På grund av den ökade möjligheten att koppla samman informationssystem och nät blir dessa nu utsatta för ett ökande antal och en större mångfald av hot och sårbarheter. Detta medför nya säkerhetsproblem. Dessa riktlinjer vänder sig därför till alla deltagare i det nya informationssamhället och pekar på behovet av en större medvetenhet och insikt om säkerhetsfrågorna och nödvändigheten att utveckla en ”säkerhetskultur”.

I. PÅ VÄG MOT EN SÄKERHETSKULTUR

Dessa riktlinjer har föranletts av att säkerhetsmiljön är i ständig förändring och de syftar till att främja utvecklingen av en säkerhetskultur. Detta betyder att de särskilt fokuserar på säkerhet vid utvecklingen av informationssystem och nät samt införande av nya sätt att tänka och beteenden vid användning av och interagerande inom dessa. Riktlinjerna innebär en tydlig brytning med den tid då säkerheten vid utformning och användning av informationssystem och nät alltför ofta var ett resultat av efterklokhet. Deltagarna blir alltmer beroende av informationssystem, nät och tillhörande tjänster, som måste vara tillförlitliga och säkra. Det är bara genom att ta vederbörlig hänsyn till alla deltagares intresse och systemens, nätens och de berörda tjänsternas natur, som man kan skapa verklig säkerhet.

Varje deltagare spelar en viktig roll för säkerheten. Deltagarna måste, alltefter sin roll i sammanhanget, vara medvetna om säkerhetsriskerna och förebyggande åtgärder, ta sitt ansvar och agera för att öka säkerheten i informationssystem och nät.

Att bygga upp en säkerhetskultur kommer att kräva både ledarskap och ett brett deltagande och bör leda till att säkerhetsplanering och säkerhetshantering får högre prioritet. Likaså måste förståelse skapas hos alla deltagare för behovet av säkerhet. Säkerhetsfrågorna bör hanteras med omsorg och ansvar på alla nivåer i myndigheter och företag och av alla inblandade deltagare. Dessa riktlinjer lägger grunden för arbetet med att införa en säkerhetskultur i hela samhället. På så sätt kommer deltagarna att kunna verka för att säkerheten skall bli en integrerad del i utformningen och användningen av alla informationssystem och nät. Alla deltagare bör införa och främja en säkerhetskultur som ett sätt att tänka, analysera och agera på vid hantering av informationssystem och nät.

II. MÅL

Dessa riktlinjer har som mål att

- främja en säkerhetskultur bland alla deltagare som ett sätt att skydda informationssystem och nät,
- göra deltagarna medvetna om riskerna för informationssystem och nät, om de regler, förfaranden, åtgärder och rutiner som står till buds för att ta itu med dessa risker och om nödvändigheten att införa och tillämpa dessa,
- främja ett ökat förtroende hos alla deltagare för informationssystem och nät och för det sätt på vilket de tillhandahålls och används,
- skapa en allmän referensram som hjälper deltagarna att förstå säkerhetsfrågorna och ta hänsyn till etiska värderingar vid utformningen och användningen av regler, förfaranden, åtgärder och rutiner för säkerheten i informationssystem och nät,
- uppmuntra alla deltagare att samarbeta och utbyta relevant information vid utformningen och användningen av regler, förfaranden, åtgärder och rutiner som rör säkerheten,

– arbeta för att alla som deltar vid utveckling och införande av standarder skall uppfatta säkerhet som ett viktigt mål.

III. PRINCIPER

Följande nio principer kompletterar varandra och skall ses som en helhet. De rör deltagare på alla nivåer, bl.a. beslutsfattare och användare. Deltagarnas ansvar varierar beroende på deras roll. Alla deltagare har nytta av medvetenhet, utbildning, informationsutbyte och praktisk träning som kan leda till ökad förståelse för området och ett bättre säkerhetsarbete. Insatserna för att förbättra säkerheten i informationssystem och nät bör vara förenliga med ett demokratiskt samhälles värderingar, särskilt behovet av ett öppet och fritt informationsflöde och en grundläggande omsorg om personlig integritet[1].

1) Medvetenhet

Deltagarna bör göras medvetna om behovet av säkerhet i informationssystem och nät och om vad de kan göra för att förbättra säkerheten.

Medvetenhet om riskerna och tillgängliga skydd är det första steget för att öka säkerheten i informationssystem och nät. Informationssystem och nät kan hotas av både inre och yttre risker. Deltagarna bör förstå att säkerhetsbrister kan vålla allvarlig skada för system och nät som de kontrollerar. De bör också vara medvetna om att de riskerar att skada andra på grund av systemens sammankopplingar och inbördes beroenden. De bör känna till de egna systemens konfiguration och tillgängliga uppdateringar, systemets plats i nätet, vedertagna metoder för att förbättra säkerheten samt andra deltagares behov.

2) Ansvar

Alla deltagare är ansvariga för säkerheten i system och nät.

Deltagarna är beroende av sammankopplade lokala och globala informationssystem och nät och bör förstå sitt ansvar för säkerheten i dessa. Deras ansvar bör vara anpassat till deras respektive roller. Deltagarna bör regelbundet se över de regler, förfaranden, åtgärder och rutiner som de själva tillämpar och bedöma om dessa är lämpliga för deras miljö. De som utvecklar, utformar och tillhandahåller produkter och tjänster bör ta hänsyn till säkerheten i system och nät. De bör sprida lämplig information, om bl.a. uppdateringar, i rätt tid, så att användarna bättre kan förstå produkternas och tjänsternas säkerhetsegenskaper och vilket deras eget säkerhetsansvar är.

[1] Utöver dessa säkerhetsriktlinjer har OECD utformat kompletterande riktlinjer om andra frågor som är viktiga för det globala informationssamhället. De behandlar skydd för personlig integritet (1980 års *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data)* och kryptering (1997 *OECD Guidelines for Cryptography Policy*). Föreliggande säkerhetsriktlinjer bör läsas tillsammans med dessa dokument.

3) Reaktion

Deltagarna bör agera snabbt och samarbeta för att förhindra, upptäcka och reagera på säkerhetsincidenter.

På grund av informationssystemens och nätens sammankoppling och risken för snabb och omfattande spridning av skador bör deltagarna agera skyndsamt och i samverkan för att hantera säkerhetsincidenter. De bör på lämpligt sätt utbyta information om hot och sårbarheter och införa rutiner för snabbt och effektivt samarbete för att förhindra, upptäcka och reagera på säkerhetsincidenter. Om det är tillåtet kan detta innefatta informationsutbyte och samarbete över nationsgränserna.

4) Etiska aspekter

Deltagarna bör respektera andra deltagares rättmätiga intressen.

Eftersom informationssystemen och näten är så spridda i våra samhällen måste deltagarna vara medvetna om att deras agerande eller underlåtenhet att agera kan skada andra. Ett etiskt uppförande är därför absolut nödvändigt, och deltagarna bör försöka utforma och använda goda förfaranden och sträva efter ett uppförande som tar hänsyn till säkerhetsbehoven och respekterar andra deltagares rättmätiga intressen.

5) Demokrati

Säkerhet i informationssystem och nät bör vara förenlig med de grundläggande värderingarna i ett demokratiskt samhälle.

Säkerhetsarbetet bör genomföras på ett sätt som ligger i linje med de värden som erkänns av demokratiska samhällen, bl.a. friheten att utbyta tankar och idéer, det fria informationsflödet, konfidentialitet för information och kommunikation, skydd för personuppgifter samt öppenhet och insyn.

6) Riskbedömning

Deltagarna bör genomföra riskbedömningar.

Vid riskbedömning kartläggs hot och sårbarheter. Riskbedömningen bör vara tillräckligt omfattande så att den täcker alla viktiga inre och yttre faktorer, t.ex. teknik, fysiska och mänskliga faktorer, regelverk och tredjepartstjänster som kan påverka säkerheten. Riskbedömningar gör det möjligt att fastställa en godtagbar risknivå. Med utgångspunkt i hur den information som skall skyddas är beskaffad och utformad underlättar riskbedömningen också urvalet av lämpliga åtgärder för att hantera risken för möjliga skador på informationssystem och nät. På grund av den ökande sammankopplingen av informationssystem, bör riskbedömningen innefatta den möjliga skada som andra deltagare kan komma att vålla eller utsättas för.

7) Utformning och genomförande av säkerhetsåtgärder

Deltagarna bör införliva säkerheten som ett centralt inslag i informationssystem och nät.

System, nät och regler måste utformas, användas och samordnas på ett sätt som optimerar säkerheten. En viktig inriktning, men inte den enda, är utformningen och användningen av lämpliga skydd och lösningar för att undvika eller begränsa potentiella skador från identifierade hot och sårbarheter. Det krävs både tekniska och icke-tekniska skyddsåtgärder och lösningar och de bör stå i proportion till värdet av informationen i organisationens system och nät. Säkerheten bör vara ett grundläggande inslag i alla produkter, tjänster, system och nät och integreras vid utformningen och uppbyggnaden av system. För slutanvändarna består skyddsåtgärderna till stor del i att välja och konfigurera produkter och tjänster till sina system.

8) Säkerhetshantering

Deltagarna bör ha ett helhetsgrepp om säkerhetsarbetet.

Säkerhetsarbetet bör grundas på riskbedömning och bör vara dynamiskt, gälla alla nivåer av deltagarnas verksamhet och alla aspekter av deras användning. Säkerhetsarbetet bör ske med framförhållning när det gäller hur man skall reagera på nya hot och gå ut på att förebygga, upptäcka och agera vid incidenter, återställning av system, fortlöpande underhåll, översyn och revision. Regler, förfaranden, åtgärder och rutiner som rör säkerheten i informationssystem och nät bör samordnas och integreras för att skapa ett sammanhängande säkerhetssystem. Kraven på säkerhetshantering beror på graden av delaktighet, deltagarens roll, den aktuella risken och systemkrav.

9) Omprövning

Deltagarna bör se över och ompröva säkerheten i informationssystem och nät och vidta nödvändiga förändringar i fråga om regler, förfaranden, åtgärder och rutiner på säkerhetsområdet.

Nya och föränderliga hot och sårbarheter upptäcks fortlöpande. Deltagarna bör kontinuerligt se över, ompröva och anpassa alla aspekter av de egna säkerhetssystemen för att hantera denna riskutveckling.

REKOMMENDATION FRÅN RÅDET OM RIKTLINJER FÖR SÄKERHETEN I INFORMATIONSSYSTEM OCH NÄT

PÅ VÄG MOT EN SÄKERHETSKULTUR

RÅDET,

som beaktar konventionen om Organisationen för ekonomiskt samarbete och utveckling av den 14 december 1960, särskilt artiklarna 1 b, 1 c, 3 a och 5 b,

som beaktar rådets rekommendation om Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data av den 23 september 1980 [C(80)58(Final)],

som beaktar förklaringen om Transborder Data Flows vilken antogs av regeringarna i OECD:s medlemsländer den 11 april 1985 [Bilaga till C(85)139],

som beaktar rådets rekommendation om Guidelines for Cryptography Policy av den 27 mars 1997 [C(97)62/FINAL],

som beaktar ministerförklaringen om the Protection of Privacy on Global Networks av den 7–9 december 1998 [Bilaga till C(98)177/FINAL],

som beaktar ministerförklaringen om Authentication for Electronic Commerce av den 7–9 december 1998 [Bilaga till C(98)177/FINAL],

som erkänner att informationssystem och nät får allt större användning och är till allt större nytta för offentlig förvaltning, företag, organisationer och enskilda användare,

som erkänner att informationssystemens och nätens allt viktigare roll och det ökande beroendet av dem för stabila och effektiva nationella ekonomier och för den internationella handeln, liksom i det sociala, kulturella och politiska livet, gör att det behövs särskilda skyddsinsatser och förtroendeskapande åtgärder på området,

som erkänner att informationssystemen och näten och spridningen av dem över hela världen har gett upphov till nya och ökande risker,

som erkänner att data och information som lagras i och sprids via informationssystem och nät hotas av olika typer av obehörig åtkomst, användning, orättmätigt tillägnande, förändring, missbruk, överföring av sabotageprogram, tillgänglighetsattacker eller förstöring och kräver lämpliga skydd,

som erkänner att det är viktigt att höja medvetenheten om de risker som hotar informationssystem och nät, att sprida kunskap om de regler, förfaranden, åtgärder

och rutiner som står till buds för att hantera dessa risker och att uppmuntra till ett lämpligt uppförande som ett avgörande steg på väg mot en säkerhetskultur,

som erkänner att nuvarande regler, förfaranden, åtgärder och rutiner måste ses över så att de kan möta de ökande hoten mot informationssystem och nät,

som erkänner att det finns ett gemensamt intresse att främja säkerheten i informationssystem och nät genom en säkerhetskultur som bygger på internationell samordning och samarbete, för att möta de utmaningar som ligger i de potentiella skador som säkerhetsbrister kan vålla nationella ekonomier, internationell handel och deltagandet i det sociala, kulturella och politiska livet,

som vidare erkänner att de *Riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur* som återfinns i bilagan till denna rekommendation är frivilliga och inte inverkar på nationernas suveräna rättigheter, och

som erkänner att syftet med dessa riktlinjer inte är att hävda att det finns en enda lösning på säkerhetsfrågan eller att fastställa vilka regler, förfaranden, åtgärder och rutiner som är bäst i en given situation, utan att de bara syftar till att ge ett ramverk för att åstadkomma en bättre förståelse för hur deltagarna både kan dra nytta av och bidra till utvecklingen av en säkerhetskultur,

ÖVERLÄMNAR dessa *Riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur* till de myndigheter, företag, organisationer och enskilda användare som utvecklar, äger, tillhandahåller, förvaltar, underhåller och använder informationssystem och nät,

REKOMMENDERAR medlemsländerna att

införa och arbeta för en säkerhetskultur enligt beskrivningen i *OECD:s riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur* och se till att regler, förfaranden, åtgärder och rutiner på säkerhetsområdet utformas i enlighet med dessa riktlinjer,

samråda, samordna och samarbeta på nationell och internationell nivå för att främja användningen av riktlinjerna,

sprida riktlinjerna inom den offentliga och privata sektorn, bl.a. myndigheter, företag, organisationer och enskilda användare, för att främja en säkerhetskultur och uppmuntra alla berörda parter att ta sitt ansvar och vidta nödvändiga åtgärder för att använda riktlinjerna på ett sätt som är avpassat för deras individuella roll,

ställa riktlinjerna till förfogande för icke-medlemsländer utan dröjsmål och på lämpligt sätt,

se över riktlinjerna vart femte år för att främja internationellt samarbete om frågor kring säkerheten i informationssystem och nät,

ANMODAR the OECD Committee for Information, Computer and Communication Policy att arbeta för att riktlinjerna skall användas.

Denna rekommendation ersätter rådets rekommendation om Riktlinjer för säkerheten i informationssystem av den 26 november 1992 [C(92)188/FINAL].

BAKGRUND

Säkerhetsriktlinjerna sammanställdes första gången år 1992 och reviderades år 1997. Den aktuella översynen företogs under 2001 av the Working Party on Information Security and Privacy (WPISP), enligt ett uppdrag från the Committee for Information, Computer and Communications Policy (ICCP), och påskyndades efter händelserna den 11 september.

Den slutliga versionen sammanställdes av en expertgrupp från WPISP som sammanträdde i Washington, DC, den 10–11 december 2001, i Sydney den 12–13 februari 2002 och i Paris den 4 och 6 mars 2002. WPISP sammanträdde i Paris den 5–6 mars 2002, 22–23 april 2002 och 25–26 juni 2002.

OECD:s riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur antogs som en rekommendation från OECD-rådet vid dess 1037:e session den 25 juli 2002.

Originalets titel: **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**. ISBN 9264059172, © 2002, Organisation for Economic Co-operation and Development (OECD), Paris.

Översättningen utgiven efter en överenskommelse med OECD, det är inte en officiell OECD-översättning.

The original version of this book was published under the title **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**. ISBN 9264059172, © 2002, Organisation for Economic Co-operation and Development (OECD), Paris.

This translation is published by arrangement with the OECD. It is not an official OECD translation.

www.oecd.org/publishing/translations – Translated versions of OECD publications
www.oecdbookshop.org – OECD online bookshop
www.sourceoecd.org – OECD e-library
www.oecd.org/oecddirect – OECD title alerting service

Statens offentliga utredningar 2005

Kronologisk förteckning

1. Radio och TV i allmänhetens tjänst. Riktlinjer för en ny tillståndsperiod. Ku.
2. Radio och TV i allmänhetens tjänst. Finansiering och skatter. Ku.
3. Sveriges tillträde till 1995 års Unidroit-konvention om stulna eller olagligt utförda kulturföremål. Ku.
4. Liberalisering, regler och marknader. + Bilagor. N.
5. Postmarknad i förändring. N.
6. Säkert inlåst? En granskning av rymningarna från Kumla, Hall, Norrtälje och Mariefred 2004. Ju.
7. Försvarsfastigheter – information till riksdagen och effektiv lokalförsörjning. Fi.
8. Behov av rörlig ledningsstödsresurs. Fö.
9. KRUT Reformerat regelverk för handel med försvarsmateriel. UD.
10. Handla för bättre klimat. Från införande till utförande. M.
11. Välfärdsverksamhet för sjömän. N.
12. Bokpriskommissionens slutrapport. Det skall vara billigt att köpa böcker och tidskrifter. U.
13. Lördagsdistribution av dagstidningar. U.
14. Effektivare handläggning av anknytningsärenden. UD.
15. Familjeåterförening och fri rörlighet för tredjelandsmedborgare. UD.
16. Reformerat system för insättningsgarantin. Fi.
17. Vem får jaga och fiska? Rätt till jakt och fiske i lappmarkerna och på renbetesfjällen. Jo.
18. Prospektansvar. Fi.
19. Beskattningen vid omstruktureringar enligt fusionsdirektivet. Fi.
20. Konsumentskydd vid modemkapning. Ju.
21. Vinstandelar. Fi.
22. Nya upphandlingsregler. Fi.
23. en BRASkatt? – beskattning av avfall som förbränns. Fi.
24. Arbetslivsinriktad rehabilitering. Framtida organisation för Arbetslivstjänster och Samhall Resurs AB. N.
25. Gränslös utmaning – alkoholpolitik i ny tid. S.
26. Mobil med bil. Ett nytt synsätt på bilstöd och färdtjänst. + Bilaga, lättläst och Daisy. S.
27. Den svenska fiskerikontrollen – en utvärdering. Jo.
28. Dubbel bosättning för ökad rörlighet. Fi.
29. Storstad i rörelse. Kunskapsöversikt över utvärderingar av storstadspolitikens lokala utvecklingsavtal. Ju.
30. Lagen om byggfelsförsäkring. En utvärdering. M.
31. Stödet till utbildningsvetenskaplig forskning. U.
32. Regeringens stabsmyndigheter. Fi.
33. Fjärrvärme och kraftvärme i framtiden. M.
34. Socialtjänsten och den fria rörligheten. S.
35. Krav på kassaregister Effektivare utredning av ekobrott. Fi.
36. På väg mot ... En hållbar landsbygdsutveckling. Jo.

37. Tolkutbildning – nya former för nya krav. U.
38. Tillgång till elektronisk kommunikation i brottsutredningar m.m. Ju.
39. Skog till nytta för alla? N.
40. Rätten till mitt språk
Förstärkt minoritetsskydd. Ju.
41. Bortom Vi och Dom.
Teoretiska reflektioner om makt, integration och strukturell diskriminering. Ju.
42. Säker information. Förslag till informationssäkerhetspolitik. Fö.
43. Vårdnad – Boende – Umgänge
Barnets bästa, föräldrars ansvar.
Del A + B. Ju.
44. Smiley: Hygien och redlighet i livsmedelshanteringen. Jo.
45. Säkra förare på moped, snöskoter och terränghjuling. N.
46. Bättre arbetslivsinriktad rehabilitering. En fusion mellan Arbetslivstjänster och Samhall Resurs AB. N.
47. Kärnavfall – barriärerna, biosfären och samhället. M.
48. Ett utvecklat resurstilldelningssystem för högskolans grundutbildning. U.
49. Unionsmedborgares rörlighet inom EU. UD.
50. Arbetskraftsinvandring till Sverige – befolkningsutveckling, arbetsmarknad i förändring, internationell utblick. N.
51. Bilen, Biffen, Bostaden. Hållbara laster – smartare konsumtion. Jo.
52. Avgiftsfinansierad livsmedels-, djurskydds- och foderkontroll – för en högre och jämnare kvalitet. Jo.
53. Beskattning när tillgångar värderas till verkligt värde. Fi.
54. Framtidens kriminalvård. Del 1+2. Ju.
55. Bättre inomhusmiljö. M.
56. Det blågula glashuset.
– strukturell diskriminering i Sverige. Ju.
57. Enhetlig eller differentierad mervärdesskatt? + Bilagedel. Fi.
58. Ny reglering av offentliga uppköpserbjudanden. Ju.
59. Miljöbalken; miljökvalitetsnormer, miljöorganisationerna i miljöprocessen och avgifter. M.
60. Efter flodvågen – det första halvåret. Fö.
61. Personuppgifter för samhällets behov. Fi.
62. Anpassning av radio- och TV-lagen till den digitala tekniken. U.
63. Tryggare leveranser. Fjärrvärme efter konkurs. N.
64. en BRASkatt! – beskattning av avfall somdeponeras. Fi.
65. Registerkontroll av personal vid hem för vård eller boende som tar emot barn eller unga. S.
66. Makt att forma samhället och sitt eget liv – jämställdhetspolitiken mot nya mål. + Forskarrapporter.
+ Sammanfattning N.
67. Energideklarationer.
Metoder, utformning, register och expertkompetens. M.
68. Regionala stimulansåtgärder inom skatteområdet. Fi.
69. Sverige inifrån.
Röster om etnisk diskriminering. Ju.
70. Polisens behov av stöd i samband med terrorismbekämpning. Ju.
71. Informationssäkerhetspolitik.
Organisatoriska konsekvenser. Fö.

Statens offentliga utredningar 2005

Systematisk förteckning

Dubbel bosättning för ökad rörlighet. [28]
Regeringens stabsmyndigheter. [32]
Krav på kassaregister Effektivare utredning av ekobrott. [35]
Beskattning när tillgångar värderas till verkligt värde. [53]
Enhetlig eller differentierad mervärdesskatt? + Bilagedel. [57]
Personuppgifter för samhällets behov. [61]
en BRASkatt! – beskattning av avfall som deponeras. [64]
Regionala stimulansåtgärder inom skatteområdet. [68]

Utbildnings- och kulturdepartementet

Radio och TV i allmänhetens tjänst. Riktlinjer för en ny tillståndsperiod. [1]
Radio och TV i allmänhetens tjänst. Finansiering och skatter. [2]
Sveriges tillträde till 1995 års Unidroitkonvention om stulna eller olagligt utförda kulturföremål. [3]
Bokpriskommissionens slutrapport. Det skall vara billigt att köpa böcker och tidskrifter. [12]
Lördagsdistribution av dagstidningar. [13]
Stödet till utbildningsvetenskaplig forskning. [31]
Tolkutbildning – nya former för nya krav. [37]
Ett utvecklat resurstilldelningssystem för högskolans grundutbildning. [48]
Anpassning av radio- och TV-lagen till den digitala tekniken. [62]

Jordbruksdepartementet

Vem får jaga och fiska? Rätt till jakt och fiske i lappmarkerna och på renbetesfjällen. [17]
Den svenska fiskerikontrollen – en utvärdering. [27]
På väg mot ... En hållbar landsbygdsutveckling. [36]
Smiley: Hygien och redlighet i livsmedelshanteringen. [44]
Bilen, Biffen, Bostaden. Hållbara laster – smartare konsumtion. [51]
Avgiftsfinansierad livsmedels-, djurskydds- och foderkontroll – för en högre och jämnare kvalitet. [52]

Miljö- och samhällsbyggnadsdepartementet

Handla för bättre klimat. Från införande till utförande. [10]
Lagen om byggfelsförsäkring. En utvärdering. [30]
Fjärrvärme och kraftvärme i framtiden. [33]
Kärnavfall – barriärerna, biosfären och samhället. [47]
Bättre inomhusmiljö. [55]
Miljöbalken; miljökvalitetsnormer, miljöorganisationerna i miljöprocessen och avgifter. [59]
Tryggare leveranser. Fjärrvärme efter konkurs. [63]
Energideklarationer. Metoder, utformning, register och expertkompetens. [67]

Näringsdepartementet

Liberalisering, regler och marknader. [4]
Postmarknad i förändring. [5]
Välfärdsverksamhet för sjömän. [11]
Arbetslivsinriktad rehabilitering. Framtida organisation för Arbetslivstjänster och Samhall Resurs AB. [24]
Skog till nytta för alla? [39]
Säkra förare på moped, snöskoter och terränghjuling. [45]
Bättre arbetslivsinriktad rehabilitering. En fusion mellan Arbetslivstjänster och Samhall Resurs AB. [46]
Arbetskraftsinvandring till Sverige – befolkningsutveckling, arbetsmarknad i förändring, internationell utblick. [50]
Makt att forma samhället och sitt eget liv – jämställdhetspolitiken mot nya mål. + Forskarrapporter. + Sammanfattning. [66]