RIKSREVISIONEN

RiR 2007:10

Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen

ISBN 978 91 7086 110 2
RiR 2007:10
Tryck: Riksdagstryckeriet, Stockholm 2007

Till regeringen
Arbetsmarknadsdepartementet
Finansdepartementet
Försvarsdepartementet
Justitiedepartementet
Näringsdepartementet

Datum 2007-06-01
Dnr 31-2007-0056

Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen

Riksrevisionen har granskat regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen. Resultatet av granskningen redovisas i denna rapport.

Företrädare för Regeringskansliet, Krisberedskapsmyndigheten, Säkerhetspolisen, Post- och telestyrelsen samt Verket för förvaltningsutveckling har beretts tillfälle att faktagranska och lämna synpunkter på utkast till rapporten.

I enlighet med 9 § lagen (2002:1022) om revision av statlig verksamhet överlämnas rapporten till regeringen. Rapporten överlämnas samtidigt till Riksrevisionens styrelse.

Revisionsrapporten innehåller även slutsatser som avser Krisberedskapsmyndigheten, Säkerhetspolisen, Post- och telestyrelsen samt Verket för förvaltningsutveckling i deras egenskap av myndigheter med särskilda uppgifter inom informationssäkerhetsområdet och överlämnas därför även till dessa. Dessa myndigheter har dock inte granskats.

Riksrevisor Karin Lindell har beslutat i detta ärende. Granskningen har genomförts av revisionsdirektör Björn Undall (föredragande), revisionsdirektör Bengt E W Andersson och revisionsledare Margareta Bure. Biträdande granskningsenhetschef Rutger Banefelt har medverkat i den slutliga handläggningen.

Karin Lindell

Björn Undall

Innehåll

Sammanfattning

Ansvaret för styrning och ledning av statsförvaltningens informationssäkerhet är fördelat mellan riksdagen, regeringen, de av regeringen utsedda tillsyns- och stödmyndigheterna (expertmyndigheterna) samt de enskilda myndigheternas ledning. Riksrevisionen har i denna granskning valt att fokusera på regeringens ansvar för att ställa krav på och följa upp förvaltningens arbete med informationssäkerheten samt ta initiativ till åtgärder för att förbättra förutsättningarna för förvaltningens arbete inom detta område.

Granskningen har genomförts mot bakgrund av de problem som framkommit i Riksrevisionens granskningar av hur elva myndigheter tagit sitt ansvar för informationssäkerhetsarbetet. En analys av dessa problem presenteras också i granskningsrapporten.

Har myndigheterna gjort tillräckligt?

Myndigheterna har ansvar för att skydda sina informationstillgångar. Riksrevisionens slutsats utifrån de genomförda elva granskningarna är att myndigheterna inte utifrån gängse normer arbetar systematiskt med sin interna styrning och kontroll av informationssäkerheten. Riksrevisionens granskningar visar på följande allvarliga incidenter i myndigheternas verksamheter:

- Det finns exempel på myndigheter som inte har lyckats avvärja virusattacker, vilket fått till följd att verksamheten inte fungerat. Handläggarna hade exempelvis inte tillgång till nödvändig information.
- Allvarliga incidenter har inträffat när myndigheter bytt IT-system eller infört nya IT-system. Viktiga samhällstjänster för medborgare och företag på Internet fick stängas ned upp till två veckor. Handläggare fick svårt att genomföra sina uppgifter i ett nytt system.
- Brister i skyddet av myndigheternas hemsidor har lett till att obehöriga fått tillgång till integritetskänsliga uppgifter och även kunnat ändra i dessa.

Dessa incidenter har bland annat sin grund i brister i myndighetsledningarnas arbete med informationssäkerheten. De viktigaste ledningsproblemen är:

- Ledningen är osäker på vilka uppgifter den har i informationssäkerhetsarbetet och hur dessa uppgifter ska utföras.
- Ledningen begär inte något tydligt underlag om vilka risker och hot som finns för verksamheten. Ledningen får därmed inte tillräcklig insikt i vilka åtgärder som ska prioriteras för att skydda verksamheten.
- Ledningens beslut om säkerhetsåtgärder fullföljs inte. Ledningen följer inte heller upp om säkerheten uppfyller ledningens krav. Ledningen underrättar sig inte heller om att viktiga åtgärder som kontinuitetsplaner, rapportering och hantering av incidenter är utförda och fungerar som avsett.
- Ledningen underskattar betydelsen av utbildning och information till personalen inklusive sin ledningspersonal och styrelsen.

Tar regeringen sitt ansvar?

Riksrevisionen bedömer att de ovan beskrivna problemen är allvarliga och att de innebär risk för betydande negativa konsekvenser för statliga åtaganden som elektronisk förvaltning och nationell krishantering. Regeringens satsning på elektronisk förvaltning innebär att alltfler myndighetstjänster blir tillgängliga på Internet, att flera myndigheter tillsammans skapar samverkande e-tjänster samt en ökning av det IT-baserade utvecklingsarbetet i övrigt. För att denna reform av förvaltningen ska lyckas måste medborgare och företag ha förtroende för de e-tjänster som finns på Internet. Förtroendet för myndigheternas e-tjänster riskerar att minska om informationen inte kan skyddas. Det kan hända om obehöriga får åtkomst till känslig information eller om de kan förändra data eller på annat sätt kan agera så att tjänsterna inte kan användas. Då finns en betydande risk för att hela satsningen på e-förvaltning äventyras.

Brister i informationssäkerheten kan även påverka den nationella krishanteringen. Statliga myndigheter har som regel viktiga roller i samhällets förmåga att förebygga, förhindra och hantera kriser. Myndigheterna förutsätts därför ha en viss så kallad basförmåga för att kunna uppfylla sin roll och bidra till samhällets förmåga att klara kriser. Basförmågan är beroende av hur väl utformad myndighetens informationssäkerhet är.
Mot bakgrund av detta anser Riksrevisionen att regeringens styrning av informationssäkerheten är av stor vikt. Riksrevisionens samlade bedömning är att regeringen inte följt upp om den interna styrningen och kontrollen av informationssäkerheten i statsförvaltningen varit tillfredsställande. Regeringen har inte heller tagit tillräckliga initiativ för att förbättra förutsättningarna för förvaltningens arbete med informationssäkerheten. Sådana förutsättningar behandlas i det följande.

Otydliga krav och mandat

Riksrevisionen konstaterar att regeringen har vidtagit åtgärder som rör tekniska förutsättningar för myndigheternas informationssäkerhetsarbete, till exempel e-signaturer, e-legitimationer, säkert Internet etc. Däremot har ännu inga åtgärder vidtagits för att stödja myndigheternas interna styrning och kontroll av informationssäkerheten.

Granskade myndighetsledningar uppfattar inte tydligt vilka krav och regler som gäller för deras informationssäkerhetsarbete, exempelvis avseende ledningens ansvar och myndigheternas riskanalyser. Detta kan enligt Riksrevisionens bedömning orsakas bland annat av att författningarna på området inte ger någon tydlig och samlad vägledning[1]. Regeringen utlovade år 2001 en översyn av regleringen inom informationssäkerhetsområdet. Översynen har ännu inte genomförts. Riksrevisionen bedömer att översynen av regleringen är angelägen särskilt mot bakgrund av satsningen på e-förvaltning.

Regeringens strategi för informationssäkerhet ger inte heller någon tydlig vägledning. Den är inriktad på samhället som helhet och preciserar inte krav på myndigheterna.

Regeringen har som stöd till förvaltningen och som stöd för sitt arbete med styrningen av myndigheterna inrättat expertmyndigheter[2] med ansvar för olika frågor inom informationssäkerhetsområdet. Regeringen har dock inte givit expertmyndigheterna tillräckligt tydliga mandat vilket inneburit svårigheter för expertmyndigheterna att ge regeringen en samlad bild av informationssäkerhetsproblemen på myndigheterna. Tydliga mandat krävs också för att expertmyndigheterna ska kunna ge lämpliga föreskrifter som preciserar regeringens krav på myndigheternas arbete med informationssäkerheten.

Regeringen har inte följt upp myndigheternas arbete med informationssäkerhet

Granskningen visar att regeringen under de senaste tio åren i stora drag har varit medveten om vissa ledningsproblem på informationssäkerhetsområdet, men bilden har varit otydlig avseende statliga myndigheter och någon samlad problembild avseende statsförvaltningen har regeringen inte kunnat presentera.

Regeringen har inte ställt krav på de statliga myndigheterna att rapportera om de huvudsakliga problemen när det gäller informationssäkerheten. KBM:s lägesbedömningar om informationssäkerhet är en viktig källa för regeringens bedömning av informationssäkerhetsarbetet i samhället. Riksrevisionen konstaterar att regeringen inte har ställt krav på KBM att lämna informationen i sådan form att förhållanden som avser statliga myndigheter tydligt kan urskiljas från exempelvis kommuner och landsting. Samtidigt

1 Se särskild analys i bilaga 2.
2 Krisberedskapsmyndigheten (KBM), Säkerhetspolisen (SÄPO), Post- & telestyrelsen (PTS), Försvarets Radioanstalt (FRA), Verket för förvaltningsutveckling (Verva), Försvarsmakten (FM), Försvarets materielverk (FMV)

anser sig inte KBM ha ett sådant mandat att utöva tillsyn över myndigheternas informationssäkerhetsarbete som myndigheten anser behövs för att kunna ge regeringen ett bra underlag för sin styrning av den statliga förvaltningen.

Ledningsfrågorna i statliga myndigheter har inte berörts i direktiven till de statliga utredningar som avsett informationssäkerhetsfrågor.

Brister i regeringens beredning av informationssäkerhetsfrågorna

Enligt Riksrevisionen är regeringens organisering av Regeringskansliets arbete med informationssäkerhetsfrågorna och styrningen av expertmyndigheterna sammantaget otillräcklig för att hantera myndigheternas problem med sin informationssäkerhet. Inget departement har ett uttalat ansvar för att göra en samlad bedömning av myndigheternas interna styrning och kontroll av informationssäkerheten.

Granskningen visar att principerna för att fördela ansvar och bereda frågor inom Regeringskansliet medför att det krävs starka signaler (exempelvis allvarliga säkerhetsincidenter) för att Regeringskansliet ska uppmärksamma brister i enskilda myndigheter. Starka signaler krävs också för att identifiera generella problem i den statliga förvaltningen. Regeringen har dock inte nåtts av någon sådan signal, till exempel via KBM:s årliga lägesbedömning, och har alltså inte uppfattat att det föreligger ett behov av att åtgärda problem i myndigheternas informationssäkerhetsarbete. Riksrevisionen konstaterar vidare att inte heller de elva myndighetsgranskningar som gjorts under en period av två år har utgjort en tillräckligt stark signal för att regeringen skulle dra slutsatsen att det finns ett generellt problem i statsförvaltningen.

Riksrevisionens rekommendationer

Under senare tid har regeringen vidtagit flera åtgärder för att ge förvaltningen och samhället i övrigt bättre förutsättningar att upprätthålla en god informationssäkerhet. Dessa åtgärder är dock enligt Riksrevisionens bedömning inte tillräckliga för att lösa de problem som myndighetsledningarna har med informationssäkerhetsarbetet. Riksrevisionen rekommenderar därför regeringen att vidta följande åtgärder för att förbättra den interna styrningen och kontrollen av informationssäkerheten i statsförvaltningen.

Regeringen bör tydligare fokusera informationssäkerhetsfrågorna

Riksrevisionens elva granskningar av myndigheternas informationssäkerhetsarbete har inte uppfattats av regeringen som en signal på ett mer

generellt problem. I och med regeringens satsning på e-förvaltning krävs att regeringen också vidtar åtgärder för att fokusera informationssäkerhetsfrågorna. Särskilt Försvarsdepartementet och Finansdepartementet bör närmare samordna sitt arbete i frågor som rör myndigheternas informationssäkerhet.

Ge expertmyndigheterna tydligt mandat att följa upp och rapportera om myndigheternas arbete med informationssäkerheten

Expertmyndigheterna har hittills inte kunnat förse regeringen med sådan information att regeringen fått en tillräcklig inblick i de väsentliga problem som finns i myndigheternas arbete med sin informationssäkerhet. Regeringen bör därför tydliggöra expertmyndigheternas uppdrag så att någon av dessa får ett tydligt mandat att följa upp och rapportera om myndigheternas styrning och kontroll av informationssäkerhetsarbetet. Regeringen bör i samband med detta precisera syftet med de årliga lägesbedömningarna.

Ge myndigheterna bättre förutsättningar - ställ tydligare krav på arbetet med informationssäkerheten

Myndigheterna har själva ansvaret för sin informationssäkerhet. Riksrevisionens granskningar har dock visat att myndighetsledningarna är osäkra på hur de ska hantera informationssäkerhetsfrågor. Detta kan enligt Riksrevisionens bedömning bland annat bero på att tillräckligt tydliga krav från regeringen saknas. Regeringen utlovade år 2001 en översyn av regleringen inom informationssäkerhetsområde. Informationssäkerhetsutredningen förde år 2005 fram förslag på en förordning inom informationssäkerhetsområdet. Regeringen har ännu inte genomfört översynen av regleringen och inte heller tagit ställning till utredningens förslag. Riksrevisionen bedömer att översynen av regleringen är angelägen särskilt mot bakgrund av satsningen på e-förvaltning.

Regeringens strategi inom informationssäkerhetsområdet bör tydliggöras så att regeringen får en bättre grund för sin styrning inom statsförvaltningen och så att myndigheterna får bättre information om politikens innehåll.

Eftersom regeringen har givit KBM i uppdrag att ta fram en handlingsplan för genomförandet av regeringens strategi bör regeringens uppdrag enligt Riksrevisionens mening även omfatta att beakta myndigheternas interna styrning och kontroll av informationssäkerhetsarbetet.

I mål- och resultatstyrningen av de enskilda myndigheterna bör regeringen ta upp myndigheternas informationssäkerhetsarbete. Kraven på de enskilda myndigheterna bör anpassas efter deras skilda förutsättningar.

1 Riksrevisionens granskning

1.1 Motiv för granskningen

Inslaget av IT-stöd i den statliga förvaltningen är betydande, och IT-beroendet har blivit allt större. Merparten av förvaltningens verksamheter skulle sannolikt inte fungera i dag utan IT-stöd för att hantera information och utföra tjänster för enskilda, företag och andra myndigheter. Regeringen har i olika sammanhang, inte minst i samband med utvecklingen av elektroniska tjänster hos myndigheterna, påtalat vikten av att IT-stödet är säkert och att informationen skyddas.

Om informationssäkerheten brister är risken stor att myndigheterna inte kan fullfölja sina skyldigheter. Som exempel kan nämnas fallet att uppgifter i elektroniska handlingar eller register ändras eller raderas obehörigt. Följderna kan till exempel bli att medborgarnas möjlighet till insyn i myndigheternas förvaltning genom att begära ut allmänna handlingar kan äventyras (den grundlagsfästa offentlighetsprincipen, 2 kap. 1 § tryckfrihetsförordningen [1949:105]). Myndighetens beslut kan bli felaktiga om de grundar sig på felaktiga eller ofullständiga uppgifter. Hemliga uppgifter, som är känsliga till exempel för enskilda personer, kan felaktigt röjas för en obehörig. Utan spårbarhet kan det hända att felkällor inte hittas och därför inte kan åtgärdas. Även flera mindre angrepp eller olyckor skulle äventyra allmänhetens och företagens förtroende för de statliga informationssystemen och därmed förtroendet för själva verksamheterna.

Staten måste kunna garantera allmänheten och företagen att de statliga myndigheternas IT-användning uppfyller kraven på säkerhet. Granskningen utgår från att regeringen är ansvarig för sina myndigheters verksamhet och därmed också för deras sätt att säkerställa sin informationshantering[3]. Att regeringen valt att delegera det mesta av detta ansvar till myndigheterna själva och till sina expertmyndigheter inom området förändrar inte regeringens ansvar.

3 Se bland annat. 1, 44 och 45 §§ lagen (1996:1059) om statsbudgeten. Riksdag och regeringen ställer vidare krav på myndigheternas interna styrning och kontroll i bland annat. verksförordningen (1995:1322) och i förordningen (2006:1228) om intern revision.

1.2 Syfte och revisionsfrågor

Ansvaret för styrning och ledning av statsförvaltningens informationssäkerhet är fördelat mellan riksdagen, regeringen, de av regeringen utsedda tillsyns- och stödmyndigheterna samt de enskilda myndigheternas ledning. Riksrevisionen har i denna granskning valt att fokusera på regeringens ansvar för att följa upp förvaltningens arbete och ta initiativ till åtgärder för att förbättra förutsättningarna för förvaltningens arbete med informationssäkerheten.

Granskningen har genomförts mot bakgrund av de problem som framkommit i Riksrevisionens granskningar av elva myndigheters informationssäkerhetsarbete. En analys av dessa problem presenteras i granskningsrapporten.

Riksrevisionen har i denna granskning inte granskat expertmyndigheterna (Krisberedskapsmyndigheten med flera). Expertmyndigheterna har dock varit viktiga informationskällor i granskningen. Fakta om informationsutbytet och dialogen mellan regeringen och expertmyndigheterna är en del av den information som Riksrevisionen samlat in i granskningen.

1.3 Krav i regleringar

Flera författningar behandlar frågor om informationssäkerhet. De viktigaste är: verksförordningen (1995:1322), sekretesslagen (1980:100), förvaltningslagen (1986:223), säkerhetsskyddslagen (1996:627), personuppgiftslagen (1998:204), arkivlagen (1990:782), förordningen om myndigheternas riskhantering (1995:1300), förordningen (2006:942) om krisberedskap och förhöjd beredskap, säkerhetsskyddsförordningen (1996:633) och internrevisionsförordningen (2006:1228).[4] Dessa författningar tar bland annat upp ledningens ansvar, hantering av handlingar samt krav på risk- och säkerhetsanalyser. Ingen av dessa författningar innehåller emellertid krav på ett systematiskt arbetssätt med informationssäkerheten, exempelvis i form av krav på viss standard.

I dessa författningar finns istället andra krav som har bäring på myndigheters hantering av information. Vissa av dessa krav riktar sig direkt mot en viss typ av information medan andra rör vissa säkerhetsrelaterade åtgärder.

Skyddet för personuppgifter är av centralt intresse när det gäller myndigheternas informationshantering. Enligt 31 § personuppgiftslagen (1998:204), PUL, ska den som är personuppgiftsansvarig[5] vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Vilka åtgärder som bör väljas är enligt lagrummet beroende av de tekniska möjligheter som finns, kostnaden för åtgärderna, vilka risker som finns och hur pass känsliga de behandlade personuppgifterna är.

4 För närmare beskrivning av regleringen se bilaga 2.
5 Enligt 3 § PUL den som bestämmer ändamålen med och medlen för behandling av personuppgifterna. När det gäller personuppgifter som hanteras inom ramen för en myndighets verksamhet så är myndigheten personuppgiftsansvarig.

Datainspektionen ger den personuppgiftsansvarige råd att beakta[6]. När det gäller integritetsskydd bör även registerlagstiftningen nämnas. Dessa regelverk rör specifika verksamheter och kan innehålla förhållandevis detaljerade krav på informationshanteringen. Som exempel kan nämnas lagen (2003:763) om behandling av personuppgifter inom socialförsäkringens administration vilken bland annat uttryckligen reglerar vilka som har behörighet att få tillgång till socialförsäkringsdatabasen.[7]

Bland de *allmänna handlingar* som myndigheterna hanterar finns inte sällan sekretessbelagda uppgifter. Enligt 1 kap. 2 § sekretesslagen (1980:100) får inte uppgifter för vilka sekretess gäller röjas för enskild i andra fall än vad som närmare anges i lagen.[8]

När det gäller myndigheter som behandlar uppgifter som är sekretessbelagda med hänvisning till rikets säkerhet, 2 kap. sekretesslagen, ställer säkerhetsskyddslagen (1996:627) krav på att det finns ett säkerhetsskydd. Säkerhetsskyddet ska ge skydd mot spionerі, sabotage och terroristbrott, och enligt lagens 9 § ska utformningen av säkerheten vid behandling i IT-system särskilt beaktas.

Dessa exempel visar på situationer då regleringen ställer särskilda krav på hantering av en viss typ av information. Regleringen kan även uttrycka krav på att vissa säkerhetsåtgärder vidtas.

Även andra regelverk ställer krav på åtgärder av betydelse för informationssäkerhetsarbetet. Förordningen (2006:942) om krisberedskap och förhöjd beredskap kräver att samtliga myndigheter genomför en *riskanalys* en gång per år. Ur ett informationssäkerhetsperspektiv är en väl genomförd riskanalys ett viktigt säkerhetsverktyg och i princip en förutsättning för att andra säkerhetsverktyg ska kunna utnyttjas optimalt. Enligt förordningen ska myndigheten i riskanalysen *identifiera sårbarheter eller hot som kan allvarligt försämra myndighetens verksamhet inom sitt område.* Syftet är enligt 9 § i förordningen att stärka sin egen och samhällets krisberedskap. En redovisning baserad på riskanalysen ska skickas in till regeringen med en kopia till Krisberedskapsmyndigheten.

Även förordningen (1995:1300) om myndigheternas riskhantering ställer krav på att myndigheterna genomför en riskanalys. Förordningen riktas endast till myndigheter under regeringen och har till syfte att *identifiera sådana risker som kan innebära skador eller förluster för staten*.[9] Efter att ha värderat riskerna och uppskattat vilka kostnader riskerna medför ska myndigheten vidta lämpliga åtgärder för att begränsa riskerna och förebygga skador eller förluster.

I säkerhetsskyddsförordningen (1996:633) ges bestämmelser till säkerhetsskyddslagen utom när det gäller riksdagen och dess myndigheter. Förordningen innehåller även mer detaljerade instruktioner om vilka säker-

6 Datainspektionen, *Säkerhet för personuppgifter*, 1999 (Datainspektionens allmänna råd) s. 26.
7 Se lag (2003:763) om behandling av personuppgifter inom socialförsäkringens administration 16 20 §§.
8 Se 1 kap. 1 § sekretesslagen (1980:100).
9 1 och 3 §§ förordningen (1995:1300) om statliga myndigheters riskhantering.

hetsåtgärder som ska vidtas när det gäller IT-system i vilka hemliga uppgifter med hänsyn till rikets säkerhet finns. Av särskilt intresse är kravet på att de som berörs av regleringen, bland annat statliga myndigheter, ska upprätta en *säkerhetsanalys*. Analysen ska behandla uppgifter om vilka uppgifter som ska hållas hemliga med hänsyn till rikets säkerhet och skyddet mot terrorism.[10] Vidare ska en *säkerhetsskyddschef* utses. Säkerhetsskyddschefen ska utöva kontroll över säkerhetsskyddet och vara direkt underställd myndighetens chef.[11] Säkerhetsskyddsförordningen innehåller regler för hur vissa uppgifter som behandlas med hjälp av IT ska skyddas. Bland annat måste samråd med Försvarsmakten alternativt Säkerhetspolisen (SÄPO) ske innan ett register som innehåller uppgifter som i vissa fall kan skada totalförsvaret upprättas. Om flera personer ska använda systemet ska detta enligt 12 § säkerhetsskyddsförordningen vara försett med funktioner för behörighetskontroll och loggning. Förordningen innehåller även regler för kryptering och kommunikation av hemliga uppgifter.[12]

I detta sammanhang bör även verksförordningen nämnas. Kraven på effektiv verksamhet som ställs i förordningen skulle även kunna implicera krav på effektivt säkerhetsarbete. I en översyn av regleringen konstaterade utredaren att kravet på effektivitet innebär att ”förvaltningen skall åstadkomma avsedda resultat och uppnå de mål som fastställts av statsmakterna på ett så kostnadseffektivt sätt som möjligt utan att för den skull göra avkall på en hög kvalitet i arbetet”.[13]

I januari 2007 trädde även internrevisionsförordningen (2006:1228) i kraft. Förordningen innehåller i 4 § krav på att internrevisionen hos en myndighet ska granska om myndighetens interna styrning och kontroll är utformad så att myndigheten med en rimlig säkerhet uppnår en effektiv verksamhet. Reglerna förtydligas i Ekonomistyrningsverkets föreskrifter. I föreskrifterna ställs även krav på att en riskanalys genomförs årligen.

1.4 Styrning av informationssäkerhet

Regeringen kan ta initiativ till olika åtgärder för att förbättra förutsättningarna för förvaltningens arbete med informationssäkerhet:

- *Förslag till förändrad reglering.*
- *Instruktioner* för myndigheterna: I vissa myndigheters instruktioner anges krav på informationssäkerhet kopplad till särskilda verksamheter.
- *Regeringens strategi* för informationssäkerheten: Mål och strategi för informationssäkerheten anges i propositionerna *Samhällets säkerhet och beredskap* (prop. 2001/02:158) och *Samverkan vid kris – för ett säkrare samhälle* (prop. 2005/06:133).

10 5 § säkerhetsskyddsförordningen (1996:633).
11 6 § säkerhetsskyddsförordningen (1996:633).
12 13 § säkerhetsskyddsförordningen (1996:633).
13 SOU 2004:23. *Från verksförordning till myndighetsförordning*, s. 267.

- *Organisering av stöd*[14]: Det finns ett flertal myndigheter som har särskilda uppgifter relaterade till informationssäkerhet: Krisberedskapsmyndigheten (KBM), Säkerhetspolisen (SÄPO), Post- och telestyrelsen (PTS), Försvarets radioanstalt (FRA), Försvaretsmaterielverk (FMV), Datainspektionen (DI) samt Verket för förvaltningsutveckling (Verva). Riksrevisionen har valt att kalla dessa myndigheter för expertmyndigheter. Expertmyndigheterna kan få regeringsuppdrag inom informationssäkerhetsområdet.
- *Regleringsbrev:* Regeringen kan ställa kortsiktiga krav på enskilda myndigheters verksamheter och informationssäkerheten. Sådana krav formuleras i regleringsbrev och avser som regel insatser som myndigheten ska genomföra under aktuellt budgetår. Ett exempel är när Domstolsverket i regleringsbrev 2004 fick i uppdrag att återrapportera en utredning om informationssäkerheten inom domstolsväsendet.
- *Uppföljning/tillsyn:* SÄPO och DI har mandat att utöva tillsyn när det gäller vissa aspekter på myndigheternas informationssäkerhet.
- *Kunskapsutveckling:* Under 2000-talet har regeringen tillsatt två särskilda informationssäkerhetsutredningar. Regeringen har också beslutat om en satsning på forskning inom säkerhetsområdet.

1.5 Bedömningsgrunder

1.5.1 Definition av informationssäkerhet

Olika åtgärder för att skydda information i IT-system eller skydda IT-system (programvara och dokumentation), det vill säga olika typer av informationstillgångar, benämns sammantaget för informationssäkerhet. Särskilda aspekter på informationssäkerheten enligt den internationellt accepterade standarden SS-ISO/IEC27001/17799, även kallad LIS-standarden[15] är:

- Skydd av konfidentialitet/sekretess, det vill säga att endast behöriga användare kommer åt informationen i verksamhetens informationssystem.
- Skydd av tillgänglighet, det vill säga att behöriga användare har tillgång till den information och funktioner de är behöriga till i rätt tid och omfattning för att kunna ge en god service.
- Skydd av riktighet (informations- och datakvalitet), det vill säga så att obehöriga inte ändrar eller modifierar informationen samt att den uppfyller verksamhetens krav på kvalitet.
- Skydd av spårbarhet, det vill säga att man kan se vem som gjort vad med informationen och i informationssystemen och vid vilken tidpunkt, till exempel om informationen påverkats i strid med myndighetens regler.

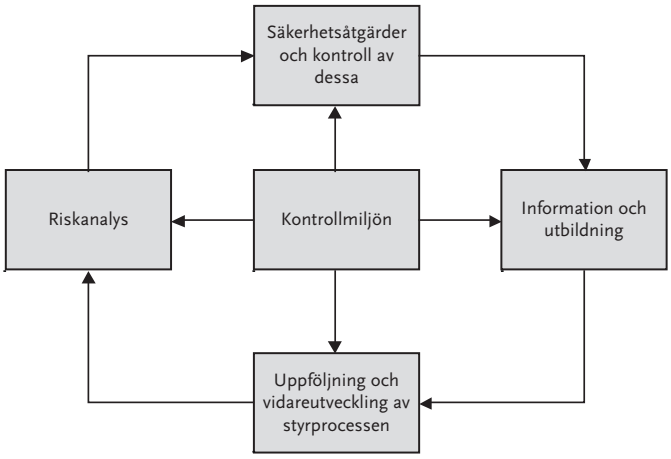
14 Expertmyndigheternas uppdrag beskrivs i bilaga 1.
15 SS-ISO/IEC 27001/17799, Information Security Management – Specification with Guidance for Use.

1.5.2 *Bedömningsgrund för granskning av myndighetsledningarna*

Som framgår av Riksrevisionens granskning saknas tydliga krav i regleringen[16] på myndigheternas informationssäkerhetsarbete avseende systematiskt arbetssätt. Mot den bakgrunden utvecklade Riksrevisionen för myndighetsgranskningarna en revisionsnorm för systematiskt arbetssätt som i huvudsak[17] bygger på LIS-standarden och på ett etablerat synsätt på hur intern styrning och kontroll bör organiseras (COSO[18]). Normen har utformats i enlighet med strukturen i COSO: ledningens kontrollmiljö, riskanalyser, kontrollfunktioner, information och utbildning samt uppföljning, utvärdering och vidareutveckling. Normen har visat sig fungera väl i granskningsarbetet och har accepterats av revisionsobjekten[19].

För att kunna hantera informationssäkerheten i enlighet med *best practice*[20] behöver myndigheternas ledningar internt styra och kontrollera arbetet med informationssäkerheten på ett bra sätt. Grunden för vad som kan betraktas som god styrning och kontroll av arbetet med informationssäkerheten utgörs dels av de författningar som berör informationssäkerhetsfrågorna, dels av standarder som uttrycker best practice beträffande ledningssystem för informationssäkerhet, särskilt den internationellt accepterade LIS-standarden.

De viktigaste delprocesserna som LIS-standarden innehåller har fördelats på styrnings- och kontrollområdena i COSO-modellen (se figur 1).



Figur 1. COSO-modellen.

16 Se avsnitt 1.3 Krav i regleringar.
17 Även vissa erfarenheter från andra nationella revisionsorgan, bland annatbland annat GAO i USA, OAG i Kanada, har utnyttjats i arbetet med bedömningsgrunden.
18 Committee of Sponsoring Organizations of the Treadway Commission (COSO) har beskrivit den interna styrningens och kontrollens olika beståndsdelar och deras samband i den s.k. COSO-modellen.
19 Normen har behandlats i seminarier med Swedish Standard Institute (SiS), Krisberedskapsmyndigheten, Statskontoret samt en säkerhetschef inom bank- och försäkringssektorn. Enligt Riksrevisionen är LIS-standarden i linje med regleringen. Skillnaderna är att regleringen täcker en mindre del av myndigheternas säkerhetsarbete och en mindre del av de statliga informationstillgångarna samt att regelverket är mindre preciserat med undantag för säkerhetsarbetet som gäller den hemliga informationen. LIS-standarden kan på så sätt sägas presicera kraven på myndigheternas arbete inom informationssäkerhetsområdet, men täcker även områden som inte direkt reglerats i lagar och förordningar.
20 Avser det enligt forskning och erfarenhet bästa sättet att utföra något.

COSO-modellen i kombination med LIS-standarden ger följande krav på god ledning, styrning och kontroll av informationssäkerhetsarbetet i myndigheten, nämligen att:

- myndighetsledningen skapar en god säkerhetskultur och andra grundläggande förutsättningar såsom krav på säkerhetsnivåer och organisering av säkerhetsarbetet – *kontrollmiljö*.
- ledningen ser till att det genomförs systematiska analyser av hot mot informationstillgångarna och risker för att befintliga skyddsåtgärder inte räcker till – *riskanalys*.
- ledningen ser till att beslut fattas på föreskrivet sätt om nya eller förändrade säkerhetsåtgärder, detta för att tillgodose ledningens krav på säkerhetsnivå i verksamheten och att beslutade åtgärder införs samt att deras funktion kontrolleras – *säkerhetsåtgärder och ledningens kontroll av dessa*.
- ledningen ser till att alla IT-användare, chefer, styrelsemedlemmar och säkerhetspersonal systematiskt får information och utbildning som avser deras skyldigheter och uppgifter i informationssäkerhetsarbetet – *information och utbildning om informationssäkerhet*.
- ledningen systematiskt och regelbundet *följer upp, förvaltar och vidareutvecklar* den interna styrning och kontroll som ledningen utformat.

Tillsammans bildar dessa styrnings- och kontrollområden myndighetens ledningssystem för informationssäkerhet. Denna norm används som bedömningsgrund för den samlade problembilden som presenteras i kapitel 2.

I den fortsatta texten används begreppen myndighetsledning och ledning synonymt.

1.5.3 Bedömningsgrund för regeringens styrning

Förutom ansvarsprincipen (som redovisas i kapitel 3) finns ingen av riksdagen eller av regeringen beslutad norm för regeringens styrning av myndigheternas interna styrning och kontroll av informationssäkerheten. Därför har Riksrevisionen utgått från huvuddragen i de bedömningsgrunder som tillämpats i myndighetsgranskningarna (LIS-standarden och COSO). Regeringen bör välja åtgärder som innebär att detaljstyrning av myndigheternas interna kontroll av informationssäkerheten undviks.

Enligt Riksrevisionen bör regeringens styrning av myndigheternas interna kontroll av sin informationssäkerhet innebära att:

- regeringen tillser att *kraven* på myndigheternas styrning och interna kontroll av sin informationssäkerhet är tydliga,
- regeringen *följer upp* förvaltningens arbete genom att ställa krav på myndigheterna att lämna en för regeringen användbar rapportering av de huvudsakliga bristerna i sin informationssäkerhet.[21]

21 För expertmyndigheternas del ska rapporteringen även avse förändringar i förvaltningsövergripande risker.

- regeringen *samordnar* frågor om informationssäkerhet inom Regeringskansliet för att undvika bristande konsekvens i beslutsfattandet och ojämn fördelning av information och kunskaper (uppfattning om hot, risker, sårbarhet, behov av åtgärder) inom området,
- regeringen också tillser att regeringens utlovade[22] åtgärder eller av riksdagen eller regeringen beslutade *åtgärder genomförs* samt att effekterna av dessa åtgärder följs upp.

1.6 Genomförande

1.6.1 Sammanfattande problembild från granskade myndigheter

Riksrevisionen har sammanställt iakttagelserna från elva granskningar[23] av myndigheter (varav sex myndigheter har granskats mer ingående) och analyserat dem för att kunna beskriva mer generella eller väsentliga typer av problem. Problemen redovisas efter samma COSO-struktur som i myndighetsgranskningarna, det vill säga under rubrikerna ledningens kontrollmiljö, riskanalyser, säkerhetsåtgärder och ledningens kontroll av dessa, information och utbildning samt ledningens uppföljning och vidareutveckling av sin styrning och kontroll av informationssäkerheten.

1.6.2 Informationsinsamling från expertmyndigheter

Riksrevisionen har intervjuat fyra expertmyndigheter – KBM, SÄPO, PTS och Verva – för att få information om expertmyndigheternas arbete med informationssäkerhetsfrågor. Dessa myndigheter har väsentliga funktioner i statsförvaltningens arbete med informationssäkerhet. Sammantaget gjorde Riksrevisionen sex myndighetsintervjuer med chefer och experter vid myndigheterna med ingående kännedom om respektive myndighets arbete med förvaltningens informationssäkerhet. Riksrevisionens frågor[24] handlade om huruvida Riksrevisionens problembild var känd, tänkbara problemorsaker, rapporteringen till regeringen, regeringens styrning av informationssäkerhetsområdet i allmänhet och specifikt av expertmyndigheterna. I anslutning till intervjuerna ombads myndigheterna att lämna dokument som belyste deras arbete med informationssäkerhet.

22 Till exempel utlovades åtgärder i regeringens propositioner.
23 Grunden för urvalet av de elva myndigheterna är att de har samhällsviktiga verksamheter, är starkt IT-beroende och att informationssäkerheten är en viktig förutsättning för myndigheternas verksamheter. Urvalet täcker in flera samhällsområden: försvar, sjöfart, arbetsmarknad, socialförsäkring, pensioner, invandring, lantmäteri, bolagsfrågor, energiförsörjning och telekommunikationer.
24 Problembild och frågor översändes till samtliga intervjupersoner i förväg.

1.6.3 *Informationsinsamling från Regeringskansliet*

Sammanlagt genomförde Riksrevisionen 20 intervjuer med ett urval av myndighetshandläggare, kanslirå̊d, ämnessakkunniga, departementsråd, enhetschefer och statssekreterare inom Näringsdepartementet[25], Justitiedepartementet, Finansdepartementet, Försvarsdepartementet och Arbetsmarknadsdepartementet. Vid intervjuerna ställdes frågor[26] om de problem som Riksrevisionen funnit på myndigheterna och Regeringskansliets uppfattning om problembilden, hur Regeringskansliet fördelar och organiserar ärenden om informationssäkerhet, vilken insamling av underlag om informationssäkerhet som sker, vilken analys som görs av insamlat material samt vilka åtgärder regeringen vidtagit för att förbättra förvaltningens arbete med informationssäkerhet. I samband med intervjuerna fick Riksrevisionen tillgång till dokument som ytterligare belyste Regeringskansliets arbete med informationssäkerhet.

1.6.4 *Särskilt konsultuppdrag om regleringen av informationssäkerheten*

En konsult har på uppdrag av Riksrevisionen gjort en genomgång av väsentlig författningsreglering av informationssäkerhet för att få fram eventuella brister som kan vara bidragande orsaker till de problem som Riksrevisionen identifierat (se bilaga 2).

1.6.5 *Genomgång av offentligt material*

I granskningen har Riksrevisionen gjort en genomgång av offentligt material såsom utredningar, propositioner, utskottsbetänkanden m.m. som rör informationssäkerhet.

25 Departementen valdes därför att de antingen är ansvariga för granskade myndigheter eller därför att de har särskilda roller i informationssäkerhetsfrågor.
26 Problembild och frågor översändes till samtliga intervjupersoner i förväg.

1.7 Rapportens disposition

I kapitel 2 redovisar Riksrevisionen den samlade problembilden från elva granskade myndigheter. Iakttagelserna är strukturerade i enlighet med COSO-modellen: kontrollmiljö, riskanalys, säkerhetsfunktioner och ledningens kontroller av dessa, information och utbildning samt uppföljning och utvärdering av ledningens styrning och kontroll av informationssäkerheten. Vidare beskrivs expertmyndigheternas syn på problembilden.

Av kapitel 3 framgår riksdagens och regeringens ställningstaganden. I kapitel 4 redovisas rapporteringen till regeringen om myndigheternas informationssäkerhetsarbete. Kapitel 5 belyser hur regeringen i Regeringskansliet organiserat arbetet med förvaltningens informationssäkerhet. I kapitel 6 redovisas regeringens initiativ för att förbättra förvaltningens arbete med informationssäkerhet. I kapitel 7 redovisar Riksrevisionen sina slutsatser, bedömningar och rekommendationer.

I bilaga 1 finns en beskrivning av expertmyndigheternas uppdrag. I bilaga 2 sammanfattas en analys av regleringen av informationssäkerheten. Bilaga 3 innehåller en förteckning över intervjuer vid Regeringskansliet.

2 Granskade myndigheter – den samlade problembilden

Under åren 2005 och 2006 har Riksrevisionen granskat och avrapporterat hur myndighetsledningarna[27] vid elva myndigheter styr och kontrollerar informationssäkerhetsarbetet. Samtliga granskade myndigheter är starkt beroende av sina IT-system för sina verksamheter. Vidare är informationssäkerheten en viktig förutsättning för verksamheterna. Sex myndigheter var föremål för en mera ingående granskning, vilket framgår av listan nedan.

Sammantaget uppvisar de elva myndigheterna ett vitt spektrum av problem. I denna sammanfattning tar vi upp de mest väsentliga problemen. Vi avser därmed problem som är vanligt förekommande eller som är särskilt allvarliga. För närmare detaljer se respektive granskningsrapport (se källförteckning).

De myndigheter som Riksrevisionen granskat mer ingående är följande:

- Arbetsmarknadsverket (AMV). AMV:s cirka 10 000 medarbetare svarar för den offentliga arbetsförmedlingen med 320 lokala arbetsförmedlingar samt webbtjänster.
- Försäkringskassan (FK). FK:s 16 000 medarbetare på 330 försäkringskontor administrerar de försäkringar och bidrag som ingår i socialförsäkringen. FK gör utbetalningar av cirka 1,5 miljarder kronor varje dygn, året om.
- Lantmäteriverket (LMV). LMV:s 2 000 medarbetare på 100 orter arbetar med fastighetsindelning och ger landskaps- och fastighetsinformation.
- Migrationsverket (MV). MV:s 3 000 medarbetare ansvarar bland annat för behandling av tillstånd för besök och bosättning i Sverige samt medborgarskapsfrågor.
- Statens pensionsverk (SPV). De 350 medarbetarna beräknar och utbetalar pensioner till 260 000 mottagare – till ett värde av 10 miljarder kronor per år för främst statsanställda.
- Sjöfartsverket (SjöV). SjöV är ett affärsverk. De 1 300 medarbetarna svarar för bland annat lotsning, isbrytning, sjöräddning och sjökartering.

27 Fokus har legat på myndighetschefen och ledningsgruppen (motsv.).

De myndigheter som Riksrevisionen granskat mer översiktligt är:

- Bolagsverket (BV). BV:s 530 medarbetare registrerar nya företag och gör registerändringar för befintliga företag, tar emot årsredovisningar och registrerar företagsinteckningar.
- Försvarsmakten (FM). FM:s 17 000 medarbetare utvecklar och använder operativa insatsförband, nationella skyddsstyrkor och utlandsstyrkan.
- Post- och telestyrelsen (PTS). Styrelsens 250 medarbetare arbetar med tillsyn och föreskrifter inom områdena elektronisk kommunikation (tele, IT och radio) och post.
- Räddningsverket (SRV). Verkets 800 medarbetare arbetar med räddningsinsatser samt råd och stöd för att minska antalet olyckor i samhället och deras effekter.
- Svenska kraftnät (SK). De cirka 260 medarbetarna vid affärsverket sköter stamnätet för elkraft och har systemansvaret för den svenska elförsörjningen.

De myndigheter som Riksrevisionen har granskat tillhör statsförvaltningens största myndigheter och har omfattande skyddsvärda informationstillgångar. Riksrevisionen har alltså valt myndigheter för vilka informationssäkerhet borde vara en väsentlig fråga för myndighetsledningen. Den problembild Riksrevisionen visar i detta kapitel bedömer Riksrevisionen därför i väsentliga drag kan vara generell för myndigheter som har omfattande och viktiga informationstillgångar. Riksrevisionen har vid urvalstidpunkten med något undantag inte haft information om förekomst av väsentliga brister i informationssäkerhetsarbetet vid respektive myndighet. Urvalet är alltså inte negativt.

2.1 Myndigheternas bedömning av sin informationssäkerhet

De sex myndigheter som Riksrevisionen har granskat mer ingående besvarade inledningsvis en enkät med frågor om bland annat deras egen bedömning av systematiken i sitt informationssäkerhetsarbete och sin informationssäkerhet. Myndigheterna gav en positiv bild av sitt eget informationssäkerhetsarbete. De ansåg att deras informationssäkerhetsarbete omfattade de moment som Riksrevisionen efterfrågade utifrån sin bedömningsnorm och att deras säkerhetsarbete därmed bedrevs systematiskt. De ansåg också att deras informationssäkerhet var tillräcklig eller i något fall behäftad med mindre brister. Som kommer att framgå av resten av detta kapitel visade sig deras bedömningar inte överensstämma med Riksrevisionens iakttagelser och bedömningar.

2.2 Vanliga problem i myndigheternas informationssäkerhetsarbete

I det följande ges en samlad beskrivning av Riksrevisionens viktigaste iakttagelser. Varje avsnitt inleds med en beskrivning av Riksrevisionens bedömningsgrund som fokuserar ledningens styrning och kontroll av myndighetens informationssäkerhetsarbete.

2.2.1 Ledningens kontrollmiljö

Bedömningsgrund

Kontrollmiljön omfattar de viktigaste förutsättningarna som myndighetsledningen kan skapa för ett effektivt informationssäkerhetsarbete, nämligen

- att visa ett tydligt engagemang
- att målmedvetet arbeta med myndighetens säkerhetskultur
- att besluta om mål för och krav på säkerheten
- att ändamålsenligt organisera och följa upp säkerhetsarbetet.

De granskade myndigheternas verksamheter är starkt beroende av en säker hantering av omfattande databaser som avser enskilda eller företag och som innehåller information som är sekretessbelagd och är svår eller dyr att återskapa. Sådana informationstillgångar är skyddsvärda. Det krävs att myndighetsledningen då har ett betydande engagemang samt en väl utvecklad förståelse för de ledningsuppgifter som måste utföras.

Ledningen bör beskriva sina krav och övergripande beslut i en sammanhållen policy, en informationssäkerhetspolicy. I denna bör ledningen precisera mål för myndighetens informationssäkerhetsarbete, hur verksamhetens mål är beroende av att kraven på säkerheten uppfylls och hur myndighetsledningen kommer att följa och styra säkerhetsarbetet. Vilka konsekvenser som bristande säkerhetsbeteende innebär för den enskilde medarbetaren bör också beskrivas. På så sätt blir all personal medveten om att informationssäkerheten är viktig för att uppnå rätt kvalitet i verksamheten.

Vidare är det viktigt att ledningen skapar lämpliga organisatoriska förutsättningar för arbetet med informationssäkerhet. Detta innebär bland annat att organisera sitt eget säkerhetsarbete, att ge ett uttalat stöd till dem som arbetar med informationssäkerhet samt att avsätta tillräckliga resurser för att kunna uppnå det skydd som ledningen ställt krav på.

Iakttagelser

I granskningarna framkom brister i ledningens förtrogenhet med vad informationssäkerhetsarbetet omfattar, hur olika delar i detta arbete hänger samman och, kanske framför allt, vilket ansvar ledningen har för myndighetens säkerhetsarbete och säkerhetskultur.

Myndigheterna hade tagit fram informationssäkerhetspolicyer, men i dessa angav inte ledningen hur säkerhetskrav och säkerhetsåtgärder bidrar till att målen för verksamheten[28] uppfylls. Värdet och nyttan av informationssäkerheten uttrycks med andra ord inte tillräckligt tydligt.

Riksrevisionen fann problem när det gäller ledningarnas sätt att organisera arbetet med informationssäkerhet. Eftersom arbetet inte organiserades på ett tydligt sätt, försvårade detta ledningens möjlighet att följa upp informationssäkerheten. Exempel på sådana problem är följande:

- Besluten om hur säkerhetsarbetet skulle bedrivas skilde sig markant från hur säkerhetsarbetet utfördes i praktiken.
- Ledningen uppmärksammade inte att informationssäkerhetspolicyn var inaktuell.
- Ledningen utsåg inte ansvariga för viktiga uppgifter i säkerhetsarbetet såsom att samordna, sammanställa och följa upp övergripande riskanalyser och åtgärdsplaner. Ingen fick till exempel i uppgift att vara samordnare av informationssäkerheten, och även andra roller som beskrevs i arbetsordningen bemannades inte eller var otydligt preciserade vad avser uppgifter och mandat.

Ett annat problem var att myndighetsledningarna inte hade skapat tillräckliga rutiner för att ta fram underlag för beslut i viktiga ledningsfrågor på informationssäkerhetsområdet. En indikation på detta är att ledningsgrupper inte diskuterade hur säkerhetsläget förhåller sig till ledningens krav och till verksamhetsmålen samt vilka risker myndigheten inte är skyddad mot. Ett annat exempel är att ingen myndighetsledning hade ställt tydliga och ändamålsenliga krav på vilket beslutsunderlag som de ville ha för att avgöra hur pass stora resurser som myndigheten borde satsa på informationssäkerhetsarbetet. Vidare kunde ingen myndighet visa hur säkerhetskostnaderna och säkerhetsinvesteringarna utvecklats över tiden och vilka faktorer som främst påverkat denna kostnadsutveckling.

28 Det vill säga hur möjligheterna att uppnå målen påverkas av brister i skyddet av informationstillgångarnas tillgänglighet, riktighet och konfidentialitet.

2.2.2 *Arbetet med riskanalys*

Bedömningsgrund

I riskanalysen inventerar och analyserar myndigheten hot och sårbarhet. Möjliga säkerhetsåtgärder inventeras och beslutas. Hot riktade mot de sårbara punkter som finns i myndighetens IT-system skapar risker för att myndighetens verksamhetsmål, till exempel ”alla tjänster till våra brukare ska göras till säkra e-tjänster på Internet senast år X”, inte kan uppnås. Riskanalysen innebär att ledningen tar ställning till hur riskbenägen den vill vara, det vill säga vilka risker som ska mötas med säkerhetsskydd respektive vilka risker som får kvarstå (den så kallade utestående eller öppna risken). Riskanalysen förutsätter att ledning, verksamhetsansvariga och specialister samordnar sitt arbete. Specialister i samverkan med verksamhetsansvariga chefer bör identifiera såväl sårbara punkter, händelser och verksamhetsförändringar som kan hota de olika verksamhetsmålen, som kostnadseffektiva skyddsåtgärder mot en viss risk eller händelse. Analyserna samordnas och utgör sedan underlag för ledningens prioriteringar och beslut om informationssäkerhetsåtgärder.

Ledningen behöver ge arbetet med riskanalyser vissa förutsättningar. Ansvar för riskanalysens skilda delar ska tydliggöras. Som underlag för analysen bör de skyddsvärda informationstillgångarna identifieras[29] och dokumenteras i en överblickbar förteckning eller databas. De tillgångar som är strategiska för verksamheten bör informations- eller säkerhetsklassas och ledningen bör ange och fastställa en viss säkerhetsnivå för respektive tillgång. Riskanalysen bör utföras med beslutade och dokumenterade metoder[30]. I riskanalysarbetet ingår att analysera tänkbara eller inträffade incidenter för att på så sätt kunna skapa säkerhetsåtgärder eller sätt att undvika dem. Analysen bör omfatta alla typer av risker för bristande tillgänglighet, riktighet, sekretess och spårbarhet som är väsentliga för verksamheten. När analysen är klar bör det finnas en tydlig och uppföljningsbar åtgärdsplan där alla beslutade säkerhetsåtgärder förtecknas med ansvariga, färdigtidpunkter och kostnader.

Iakttagelser

Myndighetsledningarna hade påtagliga svårigheter med att ta fram en bra riskanalys för hela myndigheten. Viktiga brister i arbetet med riskanalyser fanns både i förhållande till myndigheternas egna beslutade riktlinjer för riskanalys och i förhållande till aktuell standard. Myndighetsledningarna hade

29 Identifieringen bör omfatta vilka de är, vem som är ägare eller har ansvar för dem, var de finns samt vilka beroenden som finns mellan olika informationstillgångar.
30 Exempel på riskanalysmetoder är SBA Scenario, RiscPac, CRAMM, RA, ISAP, ISF Sprint och Proteus.

inte begärt och inte heller fått underlag för att ta ställning till vilka risker myndighetsledningen är beredd att ta, vilka risker som ska minskas, vilka som kan undvikas och vilka som ska få kvarstå. Ledningarna hade därmed en otydlig och ofullständig uppfattning om de risker som myndigheten står inför. Tydliga ledningsbeslut om vilka risker myndigheten skulle skydda sig mot respektive vilka risker ledningen beslutat sig för att inte skydda myndigheten mot saknades också.

Myndighetsledningarna hade delegerat ansvaret för informationssäkerhetsarbetet till så kallade systemägare[31] utan att ha utsett någon ansvarig – eller själv tagit denna roll – för avvägningar mellan skilda systemägares behov av säkerhetsåtgärder. Någon samlad avvägning på myndighetsnivå av säkerhetsinvesteringarna inom informationssäkerhetsområdet kom därför aldrig till stånd. I flera fall förekom inte heller någon formaliserad samverkan mellan olika säkerhetsområden – IT-säkerhet, informationssäkerhet, personsäkerhet, fysiskt skydd – vilket medförde att ledningen inte fick en samlad bild av riskerna för verksamheten.

De flesta myndigheterna saknade en samlad åtgärdsplan som hade givit ledningen möjligheter till övergripande beslut om risker och säkerhetsåtgärder. Besluten om säkerhetsåtgärder fanns i stället i skilda systemsäkerhetsplaner, men även dessa saknades ofta eller var inaktuella i strid med ledningens policy. I åtgärdsplanerna saknades ibland även väsentliga säkerhetsåtgärder såsom distansarbets- och e-postpolicyer samt rutiner för rapportering och hantering av incidenter.

Granskningarna visar att ledningarna inte hade skapat tillräckliga förutsättningar för riskanalyserna. Vanliga problem var att myndighetsledningarna inte fattat beslut om metoder för riskanalysarbetet. Vidare saknades aktuella och heltäckande förteckningar över skyddsvärda informationstillgångar. En av de granskade myndigheterna kunde visa att ett metodiskt och dokumenterat arbete bedrevs för att säkerhetsklassificera informationstillgångarna (inkl. IT-systemen), det vill säga att fastställa säkerhetsnivåer. Några myndigheter hade tidigare börjat klassificera informationen men fullföljde inte arbetet. Det innebär att myndigheterna saknade aktuellt underlag[32] för att besluta om säkerhetsnivån. En myndighets IT-avdelning menade att oklarheter kring IT-systemens säkerhetsnivåer medförde att IT-avdelningen inte hade underlag för att prioritera säkerhetsinsatser ifall incidenter skulle inträffa.

En vanlig brist gällde den omvärldsbevakning som behövs som grund för riskanalysen, till exempel bevakning av hot och sårbarheter i samband med informationsutbytet med andra myndigheters och organisationers IT-system. Det förekom också problem för en myndighet att analysera konsekvenser av mer omfattande verksamhetsförändringar för informationssäkerheten. Ansvar och inriktning för omvärldsbevakningen, liksom ansvar för rapportering till myndighetsledningen fanns inte tydligt beslutat.

31 Person som ansvarar för systemet i dess helhet och har ansvar för systemets förvaltning.

32 Vi vill påpeka att inom myndigheterna fanns kunskap om vilka informationstillgångar som var mer verksamhetskritiska än andra, men kunskapen var inte dokumenterad eller spridd.

Vanliga uttalanden från myndigheterna var vidare att det inte gjordes en tillräcklig riskanalys i samband med att nya system utvecklades. Vissa säkerhetskrav som ställdes på nyutvecklade IT-system analyserades och infördes först när systemen var färdigställda. Även analysen av risker och behov av säkerhetsåtgärder i samband med systembyten eller byten av systemversioner hade brister, vilket bland annat flera allvarliga incidenter i samband med sådana händelser indikerar. Detta medförde betydligt högre kostnader för att skydda dessa system än som annars skulle ha varit fallet.

Hos flera myndigheter fanns brister i hanteringen av säkerhetsincidenter. Bristerna gällde hur incidenter skulle definieras, vilka typer av incidenter som skulle rapporteras till ledningen och vem som var ansvarig för incidenthanteringen. Det fanns även brister när det gäller hur incidenter skulle dokumenteras, sammanställas och analyseras samt hur bristerna skulle åtgärdas och erfarenheter av detta återföras till berörda verksamheter i form av informations- och utbildningsinsatser. Dock har de allvarliga incidenter som upptäckts rapporterats snabbt till ledningarna.

2.2.3 Säkerhetsåtgärder och ledningens kontroll av dessa

Bedömningsgrund

I ledningens ansvar ingår att försäkra sig om att alla säkerhetsåtgärder som man beslutat om faktiskt genomförs och ger det skydd som avsetts. Genom interna kontrollfunktioner kan ledningen kontrollera beslutade säkerhetsåtgärder, att säkerhetsnivåerna uppfylls samt skaffa sig en överblick över kostnaderna för säkerhetsarbetet. Exempel på säkerhetsåtgärder som ledningen behöver kontrollera är ansvarsfördelning, samordningsfunktioner, styrdokument, regler, rapporteringsvägar, behörighetskontroller, loggningsförfaranden, kontinuitetsplaner och användarutbildning.

Iakttagelser

Granskningarna visade att ledningarna hade svårigheter att organisera sin uppföljning av att beslutade säkerhetsåtgärder var införda och fungerade som tänkt. Arbetet med att genomföra beslutade säkerhetsåtgärder släpade i flera fall efter eller hade inte genomförts. Detta förhållande var ofta inte känt hos myndighetsledning och säkerhetschefer.

Riksrevisionen fann flera exempel på att beslutade säkerhetsåtgärder aldrig hade fullföljts. Hos en myndighet hade en konsult gjort en genomgång av informationssäkerheten och rapporterat väsentliga brister till ledningen. Bristerna åtgärdades inte. Hos ett par myndigheter hade ledningen beslutat om att ta fram systemsäkerhetsplaner, vilket linjechefer och systemägare

sedan inte genomförde. En säkerhetschef trodde att myndigheten hade systemsäkerhetsplaner för alla verksamhetskritiska system. Det visade sig att det fanns en systemsäkerhetsplan för endast ett system och att planen inte hade uppdaterats.

Uppgifter om kostnaderna fanns enbart i enskilda IT-systems förvaltningsplaner och redovisning. Därmed saknade samtliga myndigheter överblickbara sammanställningar av kostnaderna för beslutade säkerhetsåtgärder. Den information som Riksrevisionen avser är hur säkerhetskostnaderna och säkerhetsinvesteringarna utvecklats över tiden och vilka faktorer som främst har påverkat denna kostnadsutveckling. Exempel på sådana faktorer är inrättande av nya eller ytterligare IT-plattformar, utfasning av åldrade system, skärpta säkerhetskrav med mera. Hur säkerhetskostnaderna utvecklats kunde alltså inte följas och därmed kunde myndigheterna inte utöva en effektiv kostnadsstyrning.

Kontinuitetsplaner[33] fanns hos de flesta myndigheter men avsåg enskilda verksamheter eller processer. Samlade – myndighetsövergripande – kontinuitetsplaner saknades.[34] Ett vanligt problem var också att åtgärderna i kontinuitetsplanerna inte övades tillräckligt ofta eller ingående.

Vid en myndighet kontrollerades inte att säkerhetskopiorna av den verksamhetskritiska informationen var användbara[35].

Vår granskning visar att det fanns brister i arbetet med säkerhet och brister i ledningens kontroll av säkerhetsåtgärder. Att allvarliga incidenter såsom långvariga driftavbrott och att känsliga uppgifter röjs, har inträffat hos flera av myndigheterna har sin grund bland annat i brister i dessa åtgärder.

2.2.4 Information och utbildning om informationssäkerhet

Bedömningsgrund

Information och utbildning avser ledningens åtgärder för att ge all personal relevant information och kunskaper om krav och policyer, om den anställdes eget ansvar för säkerheten, om de väsentliga hot och risker som ska beaktas i deras arbete och hur personalen ska agera i skilda situationer. Utbildningen ska avvägas med hänsyn till arbetsuppgifter, behörighet, anställningstid med mera. Dessutom ska denna del av ledningssystemet säkerställa att ledningen får information från verksamhetschefer om personalens kunskaper om informationssäkerhet och om huruvida beslutade regler följs.

33 I en kontinuitetsplan beskrivs de åtgärder som krävs för att de viktigaste delarna av verksamheten ska påverkas så lite som möjligt vid en allvarlig incident.
34 I en sådan plan ges ledningen möjlighet att prioritera tillgängligheten till skilda verksamheter inom myndigheten.
35 Utan sådan kontroll är det inte säkert att det är möjligt att återläsa förstörd information från säkerhetskopiorna.

Iakttagelser

Den del av ledningssystemet för informationssäkerhet som avser information och utbildning om informationssäkerhet och uppföljning av personalens kunskap och följsamhet till beslutade regler var den mest eftersatta.

Myndighetsledningarna visade med något undantag litet intresse när det gäller både sin egen, styrelsens och övriga medarbetares kunskaper och information i säkerhetsfrågor. Någon gemensam utbildning inom ledningsgrupperna och styrelsen har inte genomförts inom någon av de granskade myndigheterna. Vid två myndigheter tog ledningen ett policybeslut om att all personal måste gå en utbildning i informationssäkerhet. Vid den ena myndigheten genomfördes denna satsning fullt ut. Vid den andra genomfördes inte satsningen. Det var inte heller lätt för personal att få tillgång till en aktuell, relevant och samlad information om informationssäkerhet på myndigheternas intranät. Vidare hade myndigheternas samordningsfunktioner inte tillgång till någon aktuell och samlad dokumentation av arbetet med informationssäkerhet i organisationen. Viktiga delar av dokumenten var spridda inom organisationen.

Ett vanligt problem var att chefer på olika nivåer inte ansåg att de behövde kontrollera att personalen har rätt kompetens och följer policyer och riktlinjer. Detta motiverade cheferna med att de litar på sin personal. Därmed får ledningen ingen bild av den faktiska säkerhetskulturen inom myndigheten.

2.2.5 *Uppföljning, förvaltning och vidareutveckling av ledningssystemet för informationssäkerhet*

Bedömningsgrund

Den snabba förändringstakten i omvärlden och i de egna verksamheterna kräver att ledningen systematiskt och regelbundet värderar förutsättningarna för den interna styrning och kontroll som ledningen utformat. Uppföljningen bör avse följande väsentliga delar i ledningssystemet: delegationer, val av standard för informationssäkerhetsarbetet, riskanalys, kontrollfunktioner och säkerhetsåtgärder samt information och utbildning. Resultaten från denna uppföljning och kontroll utgör underlag för förvaltning och utveckling av ledningssystemet.

Iakttagelser

Myndigheterna kunde inte påvisa en systematisk process för uppföljning och vidareutveckling av informationssäkerhetsarbetet och dess ledningssystem. Som skäl angavs ofta att ledningen utgår från att de som fått ansvar för informationssäkerheten utför sina uppgifter enligt beslutat regelverk.

Den uppföljning som myndigheterna ändå gör är händelsestyrd och föranleds ofta av säkerhetsincidenter. Den är sällan formaliserad och dokumenterad. Ansvaret för uppföljning är sällan tydligt.

I några fall hade myndigheterna inte följt med i utvecklingen av den standard som myndigheten följde, vilket lett till att ledningen inte uppmärksammat att tidigare förutsättningar och krav för ledningssystemet inte var tillräckligt aktuella och relevanta. Ledningen kan då inte ta ställning till om förändringarna i standarden bör föranleda anpassning av det egna ledningssystemet.

2.3 Samlad bedömning utifrån elva myndighetsgranskningar

Riksrevisionens granskningar visar att myndigheterna med ett par undantag hade allvarliga brister i sina ledningssystem för informationssäkerhet. Exempel på sådana brister är att myndighetsledningarna inte ägnade informationssäkerhetsfrågorna tillräcklig uppmärksamhet och att ledningarna inte utformat sina egna ledningsuppgifter på ett bra sätt. Frågor som tveklöst – också enligt intervjuade inom myndighetsledningarna – borde vara förbehållna ledningen visade sig inte behandlas av vare sig myndighetsledningarna eller någon annan. Som exempel på sådant som enligt Riksrevisionen borde vara väsentliga ledningsfrågor kan nämnas

- vilka risker myndigheten vid viss tidpunkt saknar skydd mot,
- om kostnaderna för säkerhet är rimliga i förhållande till det ökande IT-beroendet,
- om delegationerna inom säkerhetsområdet fungerar.

Granskningarna visade att det fanns en föreställning om att informationssäkerhetsfrågorna är av teknisk natur och att de därför inte hör hemma på ledningens agenda. Detta har medfört en mycket långtgående delegering, vilket med undantag av ovan nämnda ledningsuppgifter[36] inte i sig utgör något problem om ledningen följer upp delegerade uppgifter. Så har dock inte varit fallet. Att ledningen inte efterfrågat övergripande ledningsinformation ser Riksrevisionen som en indikation på brister i ledningens uppfattning av ledningsuppgifterna på informationssäkerhetsområdet.

Riksrevisionen fann också andra viktiga brister, till exempel att inte riskanalysarbetet styrdes och kontrollerades systematiskt av ledningen, vilket resulterade i att ledningen fick en ofullständig bild av de risker och hot som myndigheten stod inför. Även en samlad och uppföljningsbar plan över nya säkerhetsåtgärder (åtgärdsplan) saknades, vilket innebar att ledningen saknade information om vilka beslutade åtgärder som genomförts och kontrollerats. Sammantaget saknades tillräckligt underlag för att ledningarna skulle

36 Bedömningar på dessa punkter kan enligt Riksrevisionen knappast delegeras med undantag för framtagningen av bedömningsunderlaget.

kunna ha en tillräcklig överblick över vilka risker som beaktats och vilka risker som kvarstod.

Riksrevisionens granskningar visade också att myndighetsledningarna hade svårigheter att organisera uppföljning. Ledningarna följde inte upp om beslutade säkerhetsåtgärder var införda och fungerade som tänkt. Ansvaret för uppföljning och rapportering var också otydligt. Myndigheterna kunde inte påvisa en systematisk process för uppföljning och vidareutveckling av informationssäkerhetsarbetet och dess ledningssystem. Myndighetsledningarna kunde inte kunde få tillförlitlig och relevant information om hur informationssäkerheten utvecklats över tiden. Det visade sig exempelvis att säkerhetsåtgärder släpade efter eller att de inte hade genomförts och att detta förhållande var mindre känt hos myndighetsledning och säkerhetschefer.

Myndighetsledningarna visade vidare litet engagemang när det gällde egen och övriga chefers och medarbetares utbildning i och information om informationssäkerhet. Om chefer och övrig personal inte har tillräcklig och aktuell kunskap om de regler och krav som ledningen ställt ökar risken för brister i informationssäkerheten.

Riksrevisionen har genomfört en uppföljning av vad tio av de granskade myndigheterna gjort efter granskningen. Samtliga myndigheter har tagit till sig Riksrevisionens iakttagelser av problem samt rekommendationer. I flera fall har ledningen informerat såväl styrelsen som personalen om granskningen. Ledningarna har beslutat om handlingsplaner eller har aviserat att sådana ska tas fram. I några fall har myndigheterna genomfört flera konkreta insatser för att förbättra informationssäkerheten, till exempel översyn av styrdokument, infört KBM:s BITS samt utbildat all personal.

2.4 Expertmyndigheternas uppfattning om Riksrevisionens problembild

Riksrevisionen har genomfört intervjuer med expertmyndigheterna KBM, SÄPO, PTS och Verva om den bild av problemen i myndigheternas interna styrning och kontroll av informationssäkerheten som Riksrevisionens granskningar visat.

Problembilden är på en övergripande nivå känd för expertmyndigheterna. Underlaget för respektive myndighets bild av problemen i den statliga förvaltningen är dock olika. Av de intervjuade expertmyndigheterna kan enbart SÄPO[37] sägas ha kunskap som kommer från genomförda inspektioner av informationssäkerheten med utgångspunkt i säkerhetsskyddslagen[38].

37 Även DI genomför inspektioner utifrån personuppgiftslagen (1998:204).
38 SÄPO kontrollerar myndigheters verksamhet utifrån rikets säkerhet och skyddet mot terrorism. Tio av de kontrollerade myndigheterna är enligt SÄPO i detta sammanhang särskilt skyddsvärda. Av dessa tio har Riksrevisionen granskat tre. När det gäller en av de granskade myndigheterna fick SÄPO fram samma problembild.

Övriga expertmyndigheter har via externa källor fått vetskap om problemen. KBM menar att problembilden har varit densamma i tio års tid och att den är känd för regeringen[39].

Flera tänkbara orsaker till brister i ledningens styrning och kontroll av informationssäkerheten omnämns i intervjuerna:

- Det finns ingen förordning eller föreskrift som reglerar myndigheternas interna kontroll inom informationssäkerhetsområdet.
- Ledningens engagemang i informationssäkerhet är otillräckligt. Säkerhetsfrågorna uppmärksammas inte tillräckligt av ledningen. Informationssäkerheten hanteras skilt från andra säkerhetsområden och har hittills mest uppfattats som tekniska frågor som kan delegeras till IT--verksamheten. Det kan finnas ett motivationsproblem för ledningen när effekterna av säkerhetsinvesteringarna är oklara. Föreslagna säkerhetsåtgärder kan då uppfattas som för dyra.
- Informationsklassificeringen genomförs ofta inte på ett tillfredsställande sätt och risk finns att myndigheterna därför underskattar behovet av skydd för informationen. Myndigheterna har svårt att ange skilda typer av informations värde för verksamheten. Vidare har myndigheterna ofta svårt att inse sitt beroende av information och IT-stöd.
- Riskanalysen för informationssäkerhet är inte en naturlig del av myndighetens samlade riskanalys. Säkerhetsanalyser saknas ofta eller är bristfälliga.
- Snabba förändringar i praxis (standarder och best practice) för informationssäkerheten kan ha lett till osäkerhet om vad som gäller i arbete med informationssäkerhet.
- Övergången från slutna IT-miljöer i myndigheterna till öppna miljöer med e-tjänster på Internet är en ovan situation för myndigheterna: De har svårt att hinna med att se över säkerhetsåtgärderna. Komplexiteten i IT-systemen ökar, liksom integrationen mellan systemen. Kunskapen om detta och den sårbarhet som det innebär är otillräcklig. Dessutom finns en ovana bland organisationer att gå från skydd av viss sekretessbelagd information till att skydda informationstillgångar.
- Utbildning av personal på olika nivåer i myndigheterna är otillräcklig.

39 I Statskontorets rapport 1991-12-05 (dnr 617/91-5) Myndigheternas säkerhetsanalyser av sina ADB-system redovisas en liknande problembild, bland annat oklar ansvarsfördelning, avsaknad av policy för säkerhetsarbetet och brister i utbildning och information.

3 Riksdagens och regeringens ställningstaganden

Regeringen har lämnat flera propositioner som berör informationssäkerhet. År 1996 lämnade regeringen i proposition (1995/96:125) *Åtgärder för att bredda och utveckla användningen av informationsteknik* ett förslag till en nationell IT-strategi. Riksdagen ansåg att det fanns behov av ett mer samlat och samordnat ansvar för *IT-säkerhetsfrågorna* och att regeringen skulle återkomma till riksdagen med en mer utvecklad strategi på IT-säkerhetsområdet. I strategin skulle regeringen precisera statens ansvar och ange hur säkerhetsarbetet skulle inordnas i det nationella handlingsprogrammet för IT samt hur säkerhetsarbetet borde organiseras.[40] Kammaren biföll utskottets förslag. Statskontoret fick därefter regeringens uppdrag att ta fram en nationell strategi. (Se avsnitt 4.1).

I IT-propositionen (1999/00:86) *Ett informationssamhälle för alla* beskrevs Statskontorets förslag till nationell strategi. Enligt propositionen innefattades informationssäkerhetsfrågorna i det prioriterade området ”tilliten till IT”. Regler och system borde – för att användarna skulle ha förtroende för dem – vara säkra, förutsägbara och teknikneutrala. De skulle också vara internationellt erkända och skydda individens integritet. Trafikutskottet ansåg att riksdagen skulle godkänna regeringens förslag till ansvarsfördelning, men ställde samtidigt återigen krav på att regeringen skulle ge ett förslag till ett mer samlat ansvarstagande för Sveriges informationssäkerhet. ”Trafikutskottet utgår, i likhet med försvarsutskottet, från att regeringen snarast återkommer till riksdagen med förslag som redovisar de konkreta åtgärder – och eventuella författningsförslag – som behövs för ett mer samlat ansvarstagande för Sveriges informationssäkerhet än hittills. Riksdagen har tidigare i ett tillkännagivande till regeringen begärt en sådan redovisning.”[41] Kammaren biföll utskottets förslag.

I regeringens proposition (2001/02:10) *Fortsatt förnyelse av totalförsvaret* uttrycker regeringen att ”det är angeläget att ett nationellt harmoniserat regelverk upprättas för att säkerställa överblick och samordning av olika regler och för att skapa sammanhållna och entydiga regler avseende informationssäkerhet.”[42]

40 Trafikutskottets bet. 1995/96 TU:19, rskr. 1995/96:282.
41 Trafikutskottets bet. 1999/2000:TU9.
42 Prop. 2001/02:10 *Fortsatt förnyelse av totalförsvaret*.

Regeringen presenterade en strategi i proposition (2001/02:158) *Samhällets säkerhet och beredskap*. En viktig utgångspunkt i strategin är ansvarsprincipen som innebär att ansvaret för informationssäkerhet ska ligga hos de myndigheter, företag och organisationer som har det normala verksamhetsansvaret. Regeringen presenterade också förslag på hur samhällets hantering av informationssäkerhet därutöver skulle organiseras. Regeringen föreslog (utifrån Statskontorets och Sårbarhets- och säkerhetsutredningens förslag[43]) fyra verksamhetsområden inom fyra olika myndigheter. Regeringen menade att det behövdes en sammanhållande funktion som också hade ansvar för omvärldsanalys, vilket senare lades på KBM. Vidare föreslogs en IT-incidenthanteringsfunktion som PTS fick ansvar för. Teknikkompetens fick FRA ansvar för, och FMV fick ansvar för evaluering och certifiering av IT-säkerhetsprodukter.[44]

I sin behandling av båda propositionerna underströk Försvarsutskottet i sitt betänkande på nytt vikten av samordning och tvärsektoriella lösningar för hela samhällets skydd mot informationsoperationer. Utskottet menade att de åtgärder som regeringen redovisat fick ses som steg på vägen i en utvecklingsprocess. Enligt utskottet borde regeringen därför efter ett par år följa upp erfarenheterna av den nya strategin och ordningen och göra en övergripande översyn av verksamheten samt redovisa denna för riksdagen.[45] Kammaren biföll utskottets förslag.

I proposition (2004/05:175) Från *IT-politik för samhället till politik för IT-samhället* presenterade regeringen några preciseringar angående säkrare Internet. I övrigt hänvisade regeringen till InfoSäkutredningen som fått regeringens uppdrag att utvärdera tidigare initiativ inom informationssäkerhetsområdet.[46] Trafikutskottet gjorde ingen annan bedömning än regeringen.[47] Kammaren biföll utskottets förslag.

I proposition (2005/06:133) *Samverkan i kris – för ett säkrare samhälle* pekade regeringen på att den nationella strategin för informationssäkerhet behövde utvecklas. De förebyggande och de förberedande åtgärderna borde enligt regeringen bli en del av myndigheternas sektorsansvar och deras instruktionsmässiga uppgifter för att ge en ökad säkerhet. ”I detta kan det ingå att också förbättra integritetsskyddet samt att kunna upptäcka, ingripa mot och agera i samband med störningar. Regeringen anser att det bör finnas en förmåga att förhindra och hantera allvarliga störningar i samhällsviktig verksamhet. Det behövs också insatser från rättsvårdande myndigheter och att frågan om den personliga integriteten uppmärksammas.” Vidare angav regeringen att KBM skulle få i uppdrag att ta fram mål för informationssäkerhet och en handlingsplan för att genomföra strategin.

43 Statskontoret 1998:18 *Sammanhållen strategi för samhällets IT-säkerhet* och SOU 2001:41 *Säkerhet i en ny tid*.
44 Prop. 2001/02:158 *Samhällets säkerhet och beredskap*
45 Försvarsutskottets bet. 2001/02:FöU10. Betänkandet behandlar prop. 2001/02:10 och prop. 2001/02:158.
46 Prop. 2004/05:175 Från *IT-politik för IT-samhället till politik för IT-samhället*.
47 Trafikutskottets bet. 2005/06:TU4.

Regeringen ansåg att InfoSäkutredningens förslag till mål skulle kunna utgöra grund för fortsatt arbete. De mål som regeringen avsåg var

- krav på prestationsförmåga eller säkerhet för samhällsviktig verksamhet
- krav på tillämpning av standarder
- kompletterande åtgärder för informationssäkerhet.[48]

I försvarsutskottets betänkande behandlades propositionen tillsammans med tre motioner i vilka kritik riktades mot regeringens hantering av informationssäkerhetsfrågorna. Bland annat ställdes krav på tydligare säkerhetspolicy och utvärdering av incidenthanteringen. Regeringen kritiserades för att ha delegerat ansvaret inom IT-säkerhetsområdet till KBM. Enligt en motionär borde ”riksdag och regering ansvara för den övergripande strategin och erforderlig samordning”. Utskottet avstyrkte motionerna och menade att ”arbete som syftar till att öka informationssäkerheten i samhället pågår inom många områden”.[49] Kammaren biföll utskottets förslag.

Sammanfattningsvis konstaterar Riksrevisionen att regeringen inte har presenterat åtgärder som avser förtydliganden av myndigheternas ansvar för intern styrning och kontroll av informationssäkerhet. Riksdagen har inte heller ställt krav på en sådan rapportering. Inte heller har den harmonisering som utlovades i september 2001 genomförts.

48 Prop. 2005/06:133 *Samverkan i kris – för ett säkrare samhälle*.
49 Försvarsutskottets bet. 2005/06:FöU9.

4 Rapporteringen till regeringen om myndigheternas informationssäkerhetsarbete

Av Riksrevisionens intervjuer med företrädare för Regeringskansliet respektive för KBM, Verva, PTS och SÄPO framkom att följande källor inom statsförvaltningen är de som huvudsakligen under 2000-talet gett regeringen information om myndigheternas interna styrning och kontroll av informationssäkerheten:

- Statliga utredningar som berör informationssäkerhet.
- Expertmyndigheternas rapportering i vilken ÖCB:s och dess efterträdare KBM:s årliga lägesbedömningar är centrala.
- Myndigheternas risk- och sårbarhetsanalyser.

4.1 Statliga utredningar

De statliga utredningar som lämnat förslag på informationssäkerhetsområdet sedan slutet av 1990-talet har berört i huvudsak tekniska frågor: säkert Internet, e-signaturer, signalspaning, kryptering, ansvarsfrågor m m.

De statliga utredningarna har också givit underlag till regeringens strategi. Detta gäller framför allt Statskontorets rapport *Sammanhållen strategi för samhällets IT-säkerhet* (Statskontoret 1998:18), utredningen *Säkerhet i en ny tid* (SOU 2001:41) och den senaste informationssäkerhetsutredningens (InfoSäkutredningen) betänkanden: *Informationssäkerhet i Sverige och internationellt – en översikt* (SOU 2004:32), *Säker information. Förslag till informationssäkerhetspolitik* (SOU 2005:42) och *Informationssäkerhetspolitik. Organisatoriska konsekvenser* (SOU 2005:71).

I Statskontorets rapport lämnades förslag som berör myndigheternas informationssäkerhetsarbete på ett mer konkret sätt. Statskontoret menade att alla myndigheter med samhällsviktig information bör göra risk- och sårbarhetsanalyser. Vidare föreslogs en harmonisering av lagstiftningen och krav på myndighetsledningarna att ta ansvar för de anställdas utbildning i informationssäkerhet.[50] Arbetsgruppen för skydd mot informationskrigföring som samtidigt hade fått uppdrag av regeringen lämnade liknande förslag.[51]

50 Statskontoret 1998:18 *Sammanhållen strategi för samhällets IT-säkerhet.*
51 Rapport 2 som är hemligstämplad. Vissa utdrag är offentliga. Enligt SOU 2001:41 *Säkerhet i en ny tid* överensstämmer arbetsgruppens förslag med Statskontorets.

InfoSäkutredningen menade att ansvarsprincipen fortfarande bör gälla, men att ansvar, befogenheter och skyldigheter bör förtydligas i berörda myndigheters instruktioner och i regleringsbrev. Föreskrifter, råd och anvisningar om en grundläggande säkerhetsnivå bör utarbetas till den förordning om vissa åtgärder för informationssäkerheten i staten som utredningen föreslår. Förordningen ska enligt förslaget ställa krav på att myndigheterna ska ha informationssäkerhetspolicy och säkerhetssamordnare.[52]

Utredningen menade också att staten ska vara föregångare när det gäller användningen av standarder och att staten bör verka för en bred användning av standarder inom statlig verksamhet. Bland de standarder som presenterades fanns LIS-standarden.[53]

Sammanfattningsvis konstaterar Riksrevisionen att utredningarna inte tar upp problem i myndigheternas interna styrning och kontroll av informationssäkerhetsarbetet.

4.2 Expertmyndigheternas rapportering

Expertmyndigheterna rapporterar viss information om myndigheternas informationssäkerhet – skriftligt eller muntligt – till regeringen utifrån sina ansvarsområden.

SÄPO rapporterar till berört departement efter det att inspektion eller brottsutredning genomförts. Myndigheten lämnar också årligen i sin årsredovisning viss information till regeringen som grundas på myndighetens tillsyn av hanteringen av hemliga uppgifter. Rapporten har en öppen och en hemlig del. I SÄPO:s publikation *Säkerhetspolisen 2006* redovisas en kort lista över de brister som SÄPO funnit vid kontrollerade företag och myndigheter under 2006. Den problembild som SÄPO presenterar motsvarar i stort den problembild som Riksrevisionen fått fram i sina elva granskningar.

PTS rapporterar incidenter utifrån sitt IT-incidentscentrums – Sitic – insamling av incidenter från bland annat myndigheter. Eftersom det är frivilligt att rapportera till Sitic är det sannolikt inte en fullständig bild av incidenterna som Sitic kan ge.

Verva rapporterar inte till regeringen om frågor som rör informationssäkerheten hos myndigheterna.

I KBM:s sammanhållande myndighetsansvar för samhällets informationssäkerhet ingår att sammanställa en helhetsbild av informationssäkerheten. Detta ska bland annat ske genom att analysera omvärldsutvecklingen

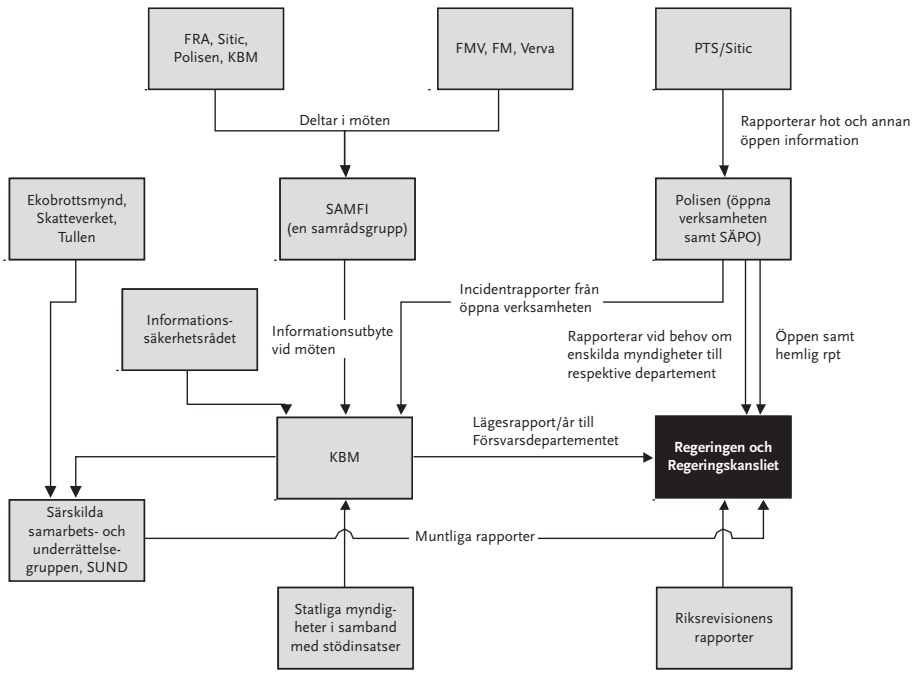
52 SOU 2005:71, *Informationssäkerhetspolitik. Organisatoriska konsekvenser.*
53 SOU 2005:42, *Säker information. Förslag till informationssäkerhetspolitik.*

inom området mot bakgrund av erhållet underrättelseunderlag, och KBM ska årligen lämna en samlad bedömning till regeringen. KBM har ingen formell grund för en myndighetsinriktad informationsinsamling och kan följaktligen inte lämna någon myndighetsinriktad rapportering till regeringen.

FRA kan enbart rapportera övergripande om de iakttagelser myndigheten gör utifrån sina konsultuppdrag.

Expertmyndigheterna rapporterar vidare om olika informationssäkerhetsfrågor i sin återrapportering av regeringsuppdrag, till exempel uppdragen om e-identitet, e-legitimation, säkrare Internet, säker elektronisk kommunikation och elektroniska dokument etc.

Figuren nedan visar väsentliga källor[54] i regeringens informationsförsörjning.



Figur 2. Regeringens informationsförsörjning inom statsförvaltningen beträffande informationssäkerhet

54 Även Riksrevisionens rapporter utgör underlag för regeringen.

4.2.1 *KBM:s lägesbedömningar*

Den enda rapportering som på en övergripande nivå behandlar informationssäkerheten i statsförvaltningen är KBM:s årliga lägesbedömning till regeringen. Underlaget till lägesbedömningen 2007 består av ett flertal källor:

- konsultrapport om Internet,
- en enkät till kommuner, landsting, länsstyrelser och statliga myndigheter med frågor om hot/incidenter, sårbarheter/risker, skyddsåtgärder, ledningens roll och ansvar samt Internetberoende och säkerhetsarbete,
- KBM:s egna ”djupintervjuer” med övriga expertmyndigheter,
- intervjuer med några av de särskilt utpekade samhällsviktiga myndigheterna,
- information från medverkande i KBM:s olika utbildningar eller från myndigheter i KBM:s stödverksamhet
- uppgifter tillgängliga på Internet.

Det bör observeras att KBM:s informationsinsamling bygger på frivillig medverkan från olika aktörer och inte på ett specifikt mandat. KBM har enligt intervjuer inte mandat att granska de statliga myndigheternas informationssäkerhet på samma sätt som Riksrevisionen. Enligt intervjuer inom Regeringskansliet har dock KBM möjlighet att följa upp enskilda myndigheter utifrån samma frågeställningar som Riksrevisionen har utgått från i sina myndighetsgranskningar.

Samtliga sju myndigheter i SAMFI[55] lämnar också uppgifter till lägesbedömningen. Lägesbedömningen stäms av inom SAMFI och Informationssäkerhetsrådet[56], men ansvaret för rapportens innehåll är fullt ut KBM:s. Informationsutbytet i SAMFI har dock inte varit problemfritt under de fyra år som SAMFI funnits. Det framgår såväl av intervjuerna som av lägesbedömningarna att KBM har haft problem med att få fram relevant information. Även om informationsutbytet nu är bättre kvarstår det faktum att SÄPO och FRA av sekretesskäl inte kan lämna information till KBM om problem i enskilda myndigheter. Sådan information lämnar SÄPO och FRA muntligt, och i vissa fall skriftligt, direkt till regeringen när behov bedöms föreligga.

Syftet med lägesbedömningarna har inte preciserats av regeringen. Av intervjuer med såväl KBM som Regeringskansliet framgår att lägesbedömningens innehåll, detaljeringsnivå och hur innehållet ska tolkas och användas av Regeringskansliet inte närmare har diskuterats. Det framgår vidare av intervjuer med KBM att myndigheten inte har närmare kunskap om hur lägesbedömningen kommer till användning inom Regeringskansliet.

Från början var syftet med lägesbedömningarna att rapportera till regeringen, och KBM angav att rapporteringen skulle vara övergripande. I senare lägesbedömning anger KBM att informationen även bör kunna vara till stöd för andra aktörer. Slutligen anger KBM åren 2006 och 2007 att lägesbedöm-

55 Samverkansgrupp för Informationssäkerhet, se bilaga 1.
56 Se bilaga 1.

ningen även ska vara ett inriktningsdokument för KBM:s arbete. Därmed har KBM gett lägesbedömningen tre olika syften.

Genom att KBM har kommit att fokusera sina insatser på kommuner och landsting bygger också en större del av lägesrapporterna på information från dessa. Ovannämnda enkät skickades till samtliga myndigheter men endast 14 länsstyrelser och 28 andra myndigheter svarade. Detta begränsar möjligheterna för KBM att rapportera en samlad bild för den statliga förvaltningen och indikerar också svagheter i KBM:s mandat.

I lägesbedömningarna anger KBM att myndigheten i bedömningarna för fram förslag till åtgärder. Riksrevisionen konstaterar dock att dessa förslag inte är så tydliga att det framgår vem som ska göra vad, om det inte är KBM självt som ska vidta åtgärder. Av intervjuer framgår att KBM inte i lägesbedömningen ger förslag som rör andra myndigheter. Sådana förslag ska tas upp i ett annat dokument. KBM har hittills dock inte överlämnat något sådant dokument med förslag till åtgärder till regeringen.

4.2.2 KBM:s lägesbedömningar i ett COSO-perspektiv

KBM:s budskap om ledningens interna styrning och kontroll av informationssäkerhetsarbetet är inte strukturerat efter COSO-indelningen (se kap. 1) och inte heller presenterat på så sätt att den fortsatta giltigheten för iakttagelser från tidigare år framgått. Genom att sammanställa uppgifter från de fyra lägesbedömningarna och tidigare ÖCB:s redovisning framträder dock en bild som kan kopplas till COSO-strukturen. Bilden avser problem bland skilda typer av organisationer utan att särredovisa de statliga myndigheterna.

När det gäller kontrollmiljön återkommer KBM i samtliga lägesbedömningar till att det finns problem i många organisationer med ledningarnas engagemang i informationssäkerhetsfrågor. Även i ÖCB:s analys från år 2001 anges att det är viktigt att verksamhetsansvariga är medvetna om sitt ansvar för risk- och sårbarhetsanalyser och för att vidta åtgärder för att skydda informationen. I de första tre lägesbedömningarna tar KBM upp svårigheter att förankra informationssäkerhetsfrågor på ledningsnivå och i organisationer. KBM menar bland annat att informationssäkerhetssamordnare har svårigheter att få gensvar hos ledningen. I lägesbedömningen år 2007 har KBM, enligt Riksrevisionen, i viss mån ändrat perspektiv på ledningsfrågorna och anger i stället att det är ledningens ansvar att informationssäkerhetsarbetet får bra förutsättningar.

KBM tar regelmässigt i sina lägesbedömningar upp problem med risk- och sårbarhetsanalyserna. Ett problem är att riskanalyserna sällan innehåller analyser av informationssäkerhetsrisker. Säkerhetsarbetet bygger inte på ett helhetstänkande utan bedrivs uppdelat på IT-säkerhet, fysisk säkerhet och informationssäkerhet.

ÖCB tog inte upp riskhanteringen som ett problem men angav redan år 2001 att det är viktigt att verksamhetsansvariga är medvetna om sitt ansvar för risk- och sårbarhetsanalyser och för att vidta åtgärder för att skydda informationen. Risker och sårbarhet ska hanteras av de verksamhetsansvariga och beslut om riskacceptans ska fattas på rätt nivå.

Ett problem som KBM återkommer till i flera lägesrapporter är brister i informationen om incidenter och deras konsekvenser. Det finns bland annat ett mörkertal i incidentrapporteringen.

När det gäller hoten understryker KBM att det största hotet mot enskilda organisationer utgörs av insider.

Upprepade gånger påpekar KBM att om inte Internet kan betraktas som säkert riskerar tilliten till informationssamhället att skadas eller gå förlorad.

När det gäller kontrollfunktioner och säkerhetsåtgärder återkommer KBM till att det främst är de administrativa säkerhetsåtgärderna som brister snarare än de tekniska. De största bristerna i informationssäkerheten inom svenska organisationer är kopplade till mjuka faktorer som kompetens, kunskap och medvetenhet.

Säkerheten kan ofta höjas med små medel, menar KBM. Att detta ändå inte sker beror i många organisationer på avsaknad av riskanalys och på bristfällig kompetens. Ett vanligt och allvarligt problem är bristen på kontinuitetsplanering. Vidare saknar många organisationer enligt lägesbedömningen år 2007 en utarbetad kris- och katastrofplan.

KBM bedömer i samtliga rapporter att det finns ett stort behov av information och utbildning för att höja kunskapen och medvetenheten om betydelsen av informationssäkerhet. Detta gäller på alla nivåer i en organisation, inklusive ledningen. Att personal bryter mot informationssäkerhetsregler beror på bristande kunskap snarare än på ont uppsåt.

KBM behandlar inte uppföljning och vidareutveckling av ledningens interna styrning och kontroll i sina lägesbedömningar. Det är inte förrän i lägesbedömningen år 2007 som KBM anger LIS-standarden som lämplig men KBM säger då inget om ledningens uppgift att följa upp och förbättra sitt ledningssystem.

De förslag eller råd som KBM lämnar i lägesbedömningarna är sammanfattningsvis:

- Informationssäkerheten måste förankras på ledningsnivå.
- Det är angeläget att åstadkomma en större integration mellan IT-säkerhet och fysisk säkerhet.
- Informationssäkerhetsfrågor ska ingå i risk- och sårbarhetsanalysen.
- Det bör övervägas om det finns behov av föreskrifter som ålägger organisationer som driver samhällsviktiga system att åtminstone leva upp till en grundläggande informationssäkerhetsnivå.
- Organisationer bör åläggas att redovisa vidtagna säkerhetsåtgärder, till exempel i samband med årsredovisningen.

- Utbudet av kvalificerade utbildningar till både medarbetare och chefer bör öka för att stärka säkerhetsmedvetandet och beställarkompetensen.

Utöver att redovisa iakttagelser som rör informationssäkerheten i samhället, anger KBM återkommande i lägesbedömningarna att det är en otydlig ansvarsfördelning mellan expertmyndigheterna och även gentemot andra myndigheter.[57] Motsvarande uttalande finns i ÖCB:s lägesbedömning från 2001. Uppgifts- och ansvarsfördelningen inom Regeringskansliet är enligt KBM:s lägesbedömning 2005 fortfarande otydlig. Det saknas en samordnande funktion och helhetsbild inom Regeringskansliet.

4.3 Myndigheternas risk- och sårbarhetsanalyser

Enligt intervjuer är myndigheternas risk- och sårbarhetsanalyser ett viktigt underlag för att bedöma myndigheternas informationssäkerhetsarbete. Det finns flera olika typer av riskanalyser som regleras i skilda förordningar:

- säkerhetsskyddsförordningen (1996:633)
- förordningen (1995:1300) om statliga myndigheters riskhantering
- förordningen (2006:942) om krisberedskap och höjd beredskap[58]
- internrevisionsförordningen (2006:1228).

Endast säkerhetsskyddsförordningen reglerar uttryckligt informationssäkerhetsfrågor. Enligt förordningen ska myndigheterna analysera om myndigheten har uppgifter som ska hållas hemliga med hänsyn till rikets säkerhet[59] och skyddet mot terrorism. I de fall myndigheterna har sådan information ställs vissa krav på skyddet.

Enligt förordningen (1995:1300) om statliga myndigheters riskhantering ska myndigheterna identifiera risker för ekonomiska skador eller förluster för staten. Detta ska sammanställas i en riskanalys.

Förordningen (2006:942) om krisberedskap och höjd beredskap är när det gäller riskanalysernas innehåll allmänt hållen. Det anges inte vilka specifika områden, till exempel informationssäkerhet, som bör vara med i analysen. Myndigheterna kan själva välja nivå på och omfattning av analysen. Förordningen ändrades år 2006 så att alla myndigheter från och med år 2007 ska skicka en kopia av risk- och sårbarhetsanalysen till KBM. Detta innebär att KBM:s tidigare analyser av myndigheternas risk- och sårbarhetsanalyser baserats på ett urval.

KBM har tagit fram vägledningar för arbetet med risk- och sårbarhetsanalyser. Dessa vägledningar är allmänt hållna och tar inte upp specifika riskområden, till exempel informationssäkerhet.

57 I regleringsbrevet 2004 för KBM fick myndigheten i uppdrag att i samverkan med Statskontoret, FRA och SÄPO kartlägga bland annat ansvarsfördelningen inom onformationssäkerhetsområdet. I KBM:s svar tas bland annat upp den oklara ansvarsfördelningen samt behov av föreskrifter som beskriver en basnivå för informationssäkerhet.

58 Ersatte förordningen (2002:472) om åtgärder för fredstida krishantering och höjd beredskap som upphävdes år 2006.

59 Enligt förordningen ska myndigheterna analysera om myndigheten har uppgifter i sin verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet av denna undersökning (säkerhetsanalys) ska dokumenteras.

Av internrevisionsförordningen framgår att internrevisionen utifrån en analys av verksamhetens risker självständigt ska granska om ledningens interna styrning och kontroll är utformad så att myndigheten med en rimlig säkerhet uppnår en effektiv verksamhet, följer lagar, förordningar och andra regler, samt lämnar en tillförlitlig redovisning och rättvisande rapportering av verksamheten.

Kravet på myndigheterna att redogöra för informationssäkerheten i risk- och sårbarhetsanalyserna är således inte tydligt. Detta innebär att analyserna inte kan ge en samlad bild av myndigheternas informationssäkerhet.

Riksrevisionens granskningar av myndigheternas informationssäkerhetsarbete visar att de riskanalyser som tas fram utifrån beredskapsförordningen eller förordningen om statliga myndigheters riskhantering inte utgör ett tillräckligt underlag för informationssäkerhetsarbetet.

5 Organisering av regeringens arbete med informationssäkerheten

Detta kapitel behandlar hur hanteringen av informationssäkerhetsfrågor i statsförvaltningen har organiserats i Regeringskansliet.

5.1 Ansvarsfördelning inom Regeringskansliet

Regeringskansliets hantering av informationssäkerhetsfrågor styrs av ansvarsprincipen. Med det avses att myndigheter, företag och organisationer som har det normala verksamhetsansvaret även har ansvar för informationssäkerheten.[60]

I samtliga intervjuer som Riksrevisionen gjorde i Regeringskansliet poängterades att det är den enskilda myndigheten som ansvarar för sin egen informationssäkerhet och för att ställda krav uppfylls. I Regeringskansliet innebär ansvarsprincipen att varje fackdepartement har ansvar för att följa upp sina respektive myndigheters informationssäkerhetsarbete och få fram eventuella ledningsproblem. I praktiken innebär det att varje myndighetshandläggare vid departementen hanterar frågor som handlar om den ”egna” myndighetens informationssäkerhet. Detta förutsätter dock att myndighetshandläggaren får signaler om att det finns behov av att uppmärksamma informationssäkerhetsarbetet. Sådana signaler kan vara IT-incidenter vid myndigheten, uppmärksamhet i massmedier eller att frågan om informationssäkerhet väcks inom Regeringskansliet. Uteblir denna signal berörs endast i undantagsfall informationssäkerhetsfrågorna.

De som intervjuats inom Regeringskansliet påpekar svårigheten att definiera informationssäkerhet och att hantera olika aspekter av informationssäkerhet som en generell fråga. Hur frågor som berör informationssäkerhet fördelas mellan departementen avgörs tydligast av den ansvarsfördelning som är fastställd i bilaga till instruktionen[61] för Regeringskansliet. Beroende på vad informationssäkerhetsfrågan handlar om (kris/krig, beredskap, säkerhet, nya begrepp, IT-användning i staten, e-förvaltning, intern styrning och kontroll, EU, utbildning/forskning etc.) styrs frågan till det departement som huvudsakligen berörs. Ett ärende som rör flera departements verksamhets-

60 Prop. 1999/2000:30, Det nya försvaret.
61 Förordning (1996:1515) med instruktion för Regeringskansliet

områden ska handläggas inom det departement till vilket det huvudsakligen tillhör och beredas i samråd med övriga berörda statsråd, så kallad gemensam beredning.[62] Detta kan exemplifieras med följande som framkommit i intervjuer i Regeringskansliet.

Enligt Försvarsdepartementet skulle de brister i myndigheternas styrning och kontroll av informationssäkerheten som Riksrevisionen konstaterat kunna betraktas som brister i den nationella krishanteringen och därmed är det Försvarsdepartementet som ansvarar för eventuell samordning, till exempel när det gäller att samordna åtgärder för att förebygga och förhindra kriser. Det finns emellertid inget formellt uttalat ansvar för Försvarsdepartementet att hantera frågan på detta sätt. Enligt intervjuer inom Försvarsdepartementet ansvarar departementet för de så kallade högre hotnivåerna (kris och krig) i samhället. De som har intervjuats anser att myndigheternas så kallade basförmåga[63], bland annat förmåga till bra intern styrning och kontroll av informationssäkerhetsarbetet, ska hanteras enligt ansvarsprincipen. Därmed har inget departement ansvar för att ta fram en samlad och aktuell bild av myndigheternas basförmåga. Försvarsdepartementet pekar på att departementet skulle kunna ha ansvar för en samlad bild, men det skulle enligt departementet bryta mot ansvarsprincipen. Detta trots att departementet ansvarar för KBM som har ett ansvar för att ta fram en samlad bild.

Om bristerna däremot betraktas som problem i myndighetsstyrningen ur ett förvaltningspolitiskt perspektiv eller om de anses generella är det Finansdepartementet som ska ansvara för samordningen. Det krävs enligt intervjuerna emellertid mycket kraftiga argument för att en fråga som informationssäkerhet ska betraktas som en generell fråga. Enligt intervjuade på Finansdepartementet har inte argumenten, i utredningar, från expertmyndigheter, från andra departement eller från politiskt håll, hittills varit så kraftfulla att det skulle ha motiverat att behandla informationssäkerhet som en generell fråga inom Regeringskansliet[64]. Det finns inte heller något departement som har ett uttalat samordningsansvar för frågor som omfattar myndigheternas interna styrning och kontroll av informationssäkerhet. Däremot finns det ett uttalat samordningsansvar för vissa specifika informationssäkerhetsfrågor. Exempelvis är Näringsdepartementet samordningsansvarigt för frågor som rör elektronisk kommunikation. Finansdepartementet å sin sidan är enligt uppgift ansvarigt för frågor som rör intern styrning och kontroll, men inte för intern styrning och kontroll inom specifika tillämpningsområden såsom informationssäkerhet.

62 Samrådsformer i Regeringskansliet, PM 1997:4.

63 Samhällets basförmåga utgörs av den normala robusthet och beredskap som finns inbyggd i samhället. Utifrån denna grund vidtas de åtgärder som krävs för att kunna möta de ökade krav och påfrestningar som kan uppstå vid ett väpnat angrepp. Detta utgör tillsammans samhällets grundförmåga.

64 Som framgår längre fram i rapporten i avsnitten om regeringens åtgärder har Informationssäkerhetsutredningen 2005 föreslagit en förordning om vissa åtgärder för informationssäkerhet hos staten . Frågan bereds för närvarande inom Försvarsdepartementet.

5.1.1 *Ansvarsprincipen i praktiken*

Brister i informationssäkerheten hos statliga myndigheter kan komma fram i exempelvis myndigheternas rapportering till ansvarigt departement, i expertmyndigheternas rapportering, i Riksrevisionens granskningsrapporter, i rapporter från massmedier eller genom att allmänheten hör av sig. I dessa fall ska ansvarigt departement i första hand uppmärksamma problemet, i enlighet med ansvarsprincipen.

Ansvarsprincipen innebär att departementets dialog med myndigheten, både den löpande dialogen och den årliga mål- och resultatdialogen, blir särskilt viktig för att fånga upp eventuella problem i myndighetens informationssäkerhetsarbete. Enligt Riksrevisionen är dialogen dock inte tillräcklig för att uppmärksamma allvarliga brister i myndighetsledningens styrning och kontroll av informationssäkerhetsarbetet, vilket granskningen visar. Det är vidare tveksamt om den enskilda myndighetshandläggaren kan göra en tillräckligt kvalificerad bedömning av myndighetens informationssäkerhet. Detta bekräftas i intervjuer med myndighetshandläggare.

Informationssäkerhetsproblem berörs som tidigare påpekats emellertid endast i undantagsfall i myndighetshandläggarens dialog med sin myndighet om det inte finns en särskild anledning att uppmärksamma frågan. I intervjuer med myndighetshandläggarna för tre granskade myndigheter framkommer att de, efter det att Riksrevisionen publicerat sina granskningar, i dialogen med myndigheten tagit upp dessa granskningar för diskussion om problemen och vad myndigheten gör åt situationen. Vissa exempel finns på att regleringsbreven också använts. Enligt uppdrag i regleringsbrevet till LMV för år 2007 ska LMV med utgångspunkt i Riksrevisionens granskning av verkets interna styrning och kontroll av informationssäkerheten (RiR 2006:26), redovisa vilka åtgärder som har vidtagits med anledning av Riksrevisionens rekommendationer.

5.1.2 *Gemensam beredning*

Utifrån sett kan ansvarsprincipen anses leda till splittring i hanteringen av informationssäkerhetsfrågor. Enligt intervjuade inom Regeringskansliet är uppdelningen på olika departement dock inget problem, utan samordning sker genom gemensam beredning. Genom denna process säkerställs enligt intervjuerna att alla berörda aktörer ges möjlighet att reagera och därmed säkerställs även kvaliteten.

Enligt intervjuer är det är framför allt i budgetprocessen som Regeringskansliet har möjlighet att identifiera generella frågor, till exempel brister i myndigheternas interna styrning och kontroll av informationssäkerheten. Om flera departement rapporterar liknande problem inom myndigheterna,

finns det möjlighet för Finansdepartementet att beteckna ett problem som generellt för flera myndigheter. I intervju med Finansdepartementet påpekas att departementet inte kan agera på förhand i generella informationssäkerhetsfrågor, till exempel när det gäller intern styrning och kontroll av informationssäkerheten. Det vore att agera mot ansvarsprincipen. Riksrevisionens elva myndighetsgranskningar har enligt intervjuerna inte varit aktuella att diskutera i budgetprocessen i syfte att bedöma om det föreligger ett generellt problem som behöver hanteras. Av intervjuer framkommer att departementen avvaktar Riksrevisionens sammanfattande rapport.

KBM:s lägesbedömningar som tas emot av Försvarsdepartementet är potentiellt ett viktigt underlag för regeringens bedömning av myndigheternas informationssäkerhet. Någon gemensam diskussion i Regeringskansliet – formell eller informell – om lägesbedömningarnas betydelse för arbetet inom andra departement än Försvarsdepartementet har inte ägt rum. Finansdepartementet hade inte vid intervjutillfället någon aktuell bild av vad som framkommit i den senaste lägesbedömningen 2007. Departementet ansåg att de tidigare lägesredovisningarna inte inneburit tillräckligt starka skäl för departementet att agera. KBM har enligt intervjuer i Regeringskansliet inte framfört något förslag om myndighetsledningarnas arbete med informationssäkerheten.

Försvarsdepartementet pekar vidare i en intervju på myndigheternas risk- och sårbarhetsanalyser som ett viktigt redskap för att se till att myndighetsledningen har kunskap om informationssäkerheten. På samma sätt kan även departementen genom analyserna få mer kunskap om myndigheternas informationssäkerhet.

I mars år 2007 bildades en statssekreterargrupp med uppgift att bevaka frågor som rör utvecklingen av e-förvaltningen. Tanken är att gruppen ska agera så att det blir en förenklad gemensam beredning. Intervjuade inom Regeringskansliet bedömer att gruppen kommer att behandla även informationssäkerhetsfrågor. En arbetsgrupp förbereder ärendena som ska tas upp i statssekreterargruppen.

5.2 Internt stöd inom Regeringskansliet

Det finns inom Regeringskansliet ingen funktion eller formellt nätverk som enbart ansvarar för informationssäkerhetsfrågor och stöd till andra enheter inom detta område. Departementen har inte heller några särskilt utsedda handläggare som analyserar behovet av styrning av informationssäkerhet. En handläggare på Försvarsdepartementet har informationssäkerhet som bevakningsområde, men i detta ingår inte frågor som rör myndigheternas basförmåga. Sammantaget innebär detta att det inte finns någon funktion

inom Regeringskansliet med uppgift att göra en samlad analys av den information om informationssäkerhet som rapporteras till regeringen.

Det finns dock ett informellt nätverk av personer från flera departement med intresse för informationssäkerhet. Nätverket var mest aktivt inför och under den senaste informationssäkerhetsutredningen (åren 2002–2005). Därefter har aktiviteten minskat. Inom Näringsdepartementet arbetar en handläggare med IT-säkerhetsfrågor utifrån ett IT-politiskt perspektiv (främst säker IT-infrastruktur och säker elektronisk kommunikation).

Riksrevisionen vill dock understryka att regeringen utnyttjar sina expertmyndigheter vid behov, till exempel för att utreda frågor om informationssäkerhet. Vid departementen finns också ämnessakkunniga med ansvar för särskilda frågor som rör informationssäkerhet.

5.3 Regeringskansliets uppfattning om Riksrevisionens problembild

Sammantaget är kunskapen inom Regeringskansliet om de problem som Riksrevisionen funnit[65] högst varierande. Statssekreterarna på de berörda departementen hade ännu inte hunnit bilda sig någon uppfattning om myndigheternas problem med informationssäkerhet. Enligt statssekreterarna borde den typ av problem som Riksrevisionens granskningar visar kunna fångas upp av den nyligen etablerade statssekreterargruppen för elektronisk förvaltning och dess interdepartementala beredningsgrupp.

Enligt de intervjuade inom Regeringskansliet har kunskapen om problemen blivit bättre tack vare informationssäkerhetsutredningen, KBM:s lägesbedömningar och Riksrevisionens myndighetsgranskningar. Försvarsdepartementet ansåg sig också ha ett väl fungerande informationsutbyte om informationssäkerhet med sina expertmyndigheter. Inom Finansdepartementet var man, som tidigare nämnts, insatt i KBM:s tidigare års lägesbedömningar men bedömde att varken KBM eller någon annan hade framfört något larm om att det förelåg ett generellt problem.

Intervjuer med myndighetshandläggare visade att de inte hade kännedom om problemen vid sina myndigheter förrän Riksrevisionens granskningar av myndigheterna presenterats.

De intervjuade ansåg att situationen är allvarlig om det är så att problemen är generella. I så fall kan detta få konsekvenser för regeringens bedömning inom flera områden, bland annat av myndigheternas grundläggande förmåga att hantera incidenter (basförmåga). Vidare framkom vikten av att myndigheter kan garantera säkra e-tjänster så att förtroendet för dessa tjänster inte äventyras och därmed övergången till elektronisk förvaltning.

65 Inför intervjuerna i Regeringskansliet presenterades en skriftlig sammanfattande problembild.

Tänkbara orsaker till problemen kan enligt de intervjuade vara myndigheternas brist på kunskap och information om hot och skyddsåtgärder. Myndigheternas risk- och sårbarhetsanalyser behöver utvecklas. Det saknas också tydliga formella krav att utgå från i informationssäkerhetsarbetet, menade de intervjuade.

6 Regeringens initiativ

Detta kapitel beskriver vilka åtgärder som regeringen vidtagit för att ge bättre förutsättningar för förvaltningens informationssäkerhetsarbete.

6.1 Regeringens initiativ för förändringar i regleringen

Riksrevisionen har analyserat regleringen av myndigheternas informationssäkerhet (se bilaga 2). Sammanfattningsvis kan Riksrevisionen konstatera att de mer uttryckliga kraven på myndigheternas informationssäkerhet dels är kopplade till hanteringen av en viss typ av information, exempelvis personuppgifter, dels rör vissa typer av åtgärder, främst riskanalyser. Det är vidare främst konfidentialitet och riktighet som regleringen avser att skydda. Kravet på effektivitet är emellertid så generellt hållet att det inte framgår vilken typ av säkerhet som ska uppnås. Regeringen har tagit vissa initiativ för att förändra regleringen. I regeringens proposition (2001/02:10) Fortsatt förnyelse av totalförsvaret uttrycker regeringen att ”det är angeläget att ett nationellt harmoniserat regelverk upprättas för att säkerställa överblick och samordning av olika regler och för att skapa sammanhållna och entydiga regler avseende informationssäkerhet.”[66] Riksrevisionen konstaterar, liksom Infosäkutredningen[67] att en samlad översyn inte har påbörjats ännu, även om vissa förändringar har gjorts inom vissa delområden.

Förändringar som genomförts sedan år 2002 och som berör informationssäkerhet är följande:

- I samband med att en ny organisation för informationssäkerhet med KBM, PTS, FRA och FMV infördes år 2002 upphörde den dåvarande beredskapsförordningen som inkluderade förordningens 22 a § om informationssäkerhet. Detta innebar att den nedlagda myndigheten ÖCB:s föreskrifter inom IT-säkerhetsområdet (FA 22) upphörde att gälla år 2003. Enligt den nya förordningen (2002:472) om fredstida krishantering och höjd beredskap och den senare förordningen (2006:942) om krisberedskap och höjd beredskap har KBM inte någon föreskriftsrätt inom informationssäkerhetsområdet.
- Verva har fått föreskriftsrätt inom området elektronisk kommunikation.

66 Prop. 2001/02:10, *Fortsatt förnyelse av totalförsvaret.*
67 SOU 2005:42, *Säker information. Förslag till informationssäkerhetspolitik.* Delbetänkande i InfoSäkutredningen

- Sekretesslagen medger numera PTS möjlighet att sekretesslägga inrapporterade incidenter till Sitic.
- I förordningen (2006:942) om krisberedskap och förhöjd beredskap ställs krav på att myndigheterna ska skicka en kopia av sin risk- och sårbarhetsanalys till KBM.

Därutöver bereds för närvarande två förordningar: en vid Finansdepartementet, biträtt av Ekonomistyrningsverket, avseende intern styrning och kontroll i myndigheterna och en vid Försvarsdepartementet avseende det förslag till förordning om vissa åtgärder för informationssäkerhet i statsförvaltningen som Informationssäkerhetsutredningen år 2005 lämnade. Förslaget till förordning om intern styrning och kontroll vid statliga myndigheter fokuserar behovet av att myndigheterna tar fram ändamålsenliga risk- och sårbarhetsanalyser. Om informationssäkerhet är en viktig fråga för verksamheten ska detta enligt Regeringskansliet framkomma i dessa analyser och i åtgärdsplaner. Ekonomistyrningsverket (ESV) får enligt 13 § internrevisionsförordningen (2006:1228) meddela tillämpliga föreskrifter. ESV kommer att ta fram vägledningar och utbildningar i intern styrning och kontroll. I förordningsarbetet har Finansdepartementet inte fokuserat på olika sakfrågor, till exempel informationssäkerhet.

Frågan om att föreskriva en viss standard, till exempel LIS-standarden, för myndigheternas informationssäkerhetsarbete, har diskuterats i regeringen. Enligt intervjuer inom regeringskansliet är det dock inte aktuellt att regeringen anger en standard. En sådan skulle strida mot ansvarsprincipen och innebära en långtgående detaljstyrning. Det finns exempel på länder som här har valt en annan väg.[68]

6.2 Regeringens strategi för informationssäkerhet

Enligt intervjuer inom Regeringskansliet beskriver propositionerna *Samhällets säkerhet och beredskap* (prop. 2001/02:158) och *Samverkan vid kris – för ett säkrare samhälle* (prop. 2005/06:133) sammantaget regeringens strategi för informationssäkerhet. Enligt intervjuer omfattar strategin inte myndighetsledningarnas interna styrning och kontroll av informationssäkerheten.

Av intervjuer inom Försvarsdepartementet framgår att InfoSäkutredningens förslag år 2005 till strategi även bör ses som en del av regeringens strategi, och att KBM bland annat ska utgå från den i sitt arbete med den nationella handlingsplanen för informationssäkerhet. Strategin i InfoSäkutredningen omfattar följande tio punkter, nämligen att[69]

68 I Danmark har regeringen beslutat att alla myndigheter ska ha infört LIS-standarden före utgången av år 2006. Om så skett ska granskas av den danska riksrevisionen.
69 SOU 2005:71, *Informationssäkerhetspolitik. Organisatoriska konsekvenser.*

- utveckla Sveriges position inom EU och i internationella sammanhang
- skapa förtroende, trygghet, säkerhet och öka integritetsskyddet
- främja ökad användning av IT
- förebygga och hantera störningar i informations- och kommunikationssystem
- förstärka underrättelse- och säkerhetstjänstens arbete samt utveckla delgivningen av underrättelseinformationen
- förstärka förmågan inom området nationell säkerhet
- utnyttja samhällets samlade kapacitet på informationssäkerhetsområdet
- fokusera på samhällsviktig verksamhet
- öka medvetenheten om säkerhetsrisker och möjligheter till skydd
- säkerställa kompetensförsörjningen.

Några av dessa tio punkter kan enligt Riksrevisionen kopplas till ledningens interna styrning och kontroll av informationssäkerheten, det vill säga det är frågor som ledningen bör uppmärksamma i sin styrning. Dessa är att

- skapa förtroende, trygghet, säkerhet och öka integritetsskyddet
- förebygga och hantera störningar i informations- och kommunikationssystem
- fokusera på samhällsviktig verksamhet
- öka medvetenheten om säkerhetsrisker och möjligheter till skydd
- säkerställa kompetensförsörjningen.

Av regeringens strategi för fortsatt utveckling av elektronisk förvaltning – *Bättre service för varje skattekrona*[70] - framgår också krav på integritet och säkerhet i förvaltningens hantering av information, till exempel vid informationsutbyte och elektronisk kommunikation. Syftet är att stärka tilliten till och effektiviteten i systemen. I strategin betonas bland annat krav på tydligt ledarskap och hög kompetens hos förvaltningsledningen när det gäller verksamhetsutveckling med hjälp av IT.

Regeringen har också i december 2006 tagit beslut om en strategi för ökad säkerhet i Internets infrastruktur[71]. Strategin omfattar även information, kunskapsutveckling och internationellt arbete. Med information avses att informera Internetanvändare, till exempel myndigheter, så att dessa inte utsätter sig för onödiga risker och att de skyddar sin IT-infrastruktur.

70 Bilaga till protokoll vid regeringssammanträde, 2006-06-21, nr 21.
71 Regeringen Näringsdepartementet. Strategi för ökad säkerhet i Internets infrastruktur (protokoll 116 vid regeringssammanträde 2006-12-07 N2006/5335/ITFoU)

6.3 Organisering av stöd till förvaltningen och Regeringskansliet

Organisering är en annan typ av åtgärd som regeringen lagt stor vikt vid. En ny struktur för organiseringen av informationssäkerhetsarbetet med uppdelning av ansvaret på fyra myndigheter (KBM, PTS, FRA och FMV) infördes 2002. KBM fick i uppgift att ha ett sammanhållande myndighetsansvar inom informationssäkerhetsområdet.

Regeringens styrning av sina expertmyndigheter sker genom instruktion, regleringsbrev och uppdrag. Följande åtgärder kan nämnas.

- PTS har fått flera regeringsuppdrag att utreda frågor om ökad säkerhet på Internet och har redovisat flera delrapporter. Den senaste uppdragsredovisningen[72] (år 2006) omfattade ett förslag till strategi för ett säkrare Internet.
- En ny myndighet, Verva, inrättades den 1 januari 2006. Myndigheten har enligt regeringens strategi för utveckling av elektronisk förvaltning en central roll när det gäller att främja utvecklingen i enlighet med strategin. Myndigheten fick i november 2006 regeringens uppdrag[73] att leda och samordna statsförvaltningens utvecklingsarbete avseende säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar. Vidare fick Verva ett uppdrag[74] i februari 2007 att följa upp övergången till e-förvaltningen. Myndigheten har också fått ansvar för att fullfölja tidigare insatser som avser e-legitimation, e-identitet och e-signaturer. Verva har vidare föreskrivningsrätt[75] inom området elektroniskt informationsutbyte. Den första föreskriften beslutades i januari 2007 och avsåg format för elektronisk hantering av fakturor i staten.
- KBM ska enligt sin instruktion årligen ge regeringen en lägesbedömning inom informationssäkerhetsområdet. I regleringsbrev för 2007 har KBM fått i uppdrag att redovisa konkreta åtgärder (en nationell handlingsplan) för att få en bättre informationssäkerhet i samhället.

Det bör i detta sammanhang nämnas att det pågår en offentlig utredning (SOU 2007:31) som berör flera av expertmyndigheterna och organiseringen av deras uppgifter nyligen avlämnat ett betänkande. Utredningen berör informationssäkerhetsfrågor och ger bland annat förslag om att KBM:s informationssäkerhetsarbete överförs till FRA.

72 Uppdraget gavs i Regleringsbrev 2006 för Post- och telestyrelsen
73 Regeringsbeslut 16, 2006-11-30, Fi2006/6773, Fi2006/967
74 Regeringsbeslut 3, 2007-02-22, Fi2007/1399, Fi2004/4657
75 Förordning (2005:860) med instruktion för Verket för förvaltningsutveckling

6.4 Regleringsbreven

Regleringsbreven har under 2000-talet inte innehållit några generella krav på den statliga förvaltningens informationssäkerhetsarbete. Regleringsbreven har heller inte använts för att samla in uppgifter i syfte att få en generell bild av myndigheternas informationssäkerhet. Några myndigheter har dock via regleringsbreven fått uppgifter på informationssäkerhetsområdet. Ett exempel är att Domstolsverket i regleringsbrev 2004 fick i uppdrag att bedöma vilka författningsändringar som behövdes för att skapa ett för domstolsväsendet gemensamt regelverk för informationssäkerhet.

6.5 Forskning och standardisering

Regeringen har beslutat om en satsning på forskning inom säkerhetsområdet. Tidigare forskning, initierad av KBM, har inte varit inriktad på frågor som rör ledningarnas interna styrning och kontroll av informationssäkerhet. KBM arbetar för närvarande (våren 2007) med att etablera tematisk forskning på informationssäkerhetsområdet.

Regeringen har vidare tillsatt en IT-standardiseringsutredning. Denna fick i november 2006 tilläggsdirektiv med frågor om informationssäkerhet. Av direktivet framgår att utredningen ytterligare ska analysera IT-standardiseringens betydelse som en viktig förutsättning för en sammanhållen e-förvaltning, omfattande såväl stat som kommuner och landsting. I utredarens arbete ska också informationssäkerhetsfrågorna ges en framträdande roll inom en sammanhållen e-förvaltning.[76]

76 Tilläggsdirektiv till IT-standardiseringsutredningen (N2006:05), dir. 2006:117. Beslutad vid regeringssammanträde 2006-11-30.

7 Slutsatser och rekommendationer

Ansvaret för styrning och ledning av statsförvaltningens informationssäkerhet är fördelat mellan riksdagen, regeringen, de av regeringen utsedda tillsyns- och stödmyndigheterna samt de enskilda myndigheternas ledningar. Riksrevisionen har i denna granskning valt att fokusera på regeringens ansvar för att följa upp statsförvaltningens arbete och ta initiativ till åtgärder för att förbättra förutsättningarna för förvaltningens arbete med informationssäkerheten.

Granskningen har genomförts mot bakgrund av de problem som framkommit i Riksrevisionens granskningar av elva myndigheters informationssäkerhetsarbete.

7.1 Slutsatser om myndigheternas ansvar

Myndigheterna har sitt ansvar för att skydda sina informationstillgångar. Riksrevisionens slutsats utifrån de genomförda elva granskningarna är att myndigheterna inte utifrån gängse normer arbetar systematiskt med sin interna styrning och kontroll av informationssäkerheten. I Riksrevisionens granskningar har följande allvarliga incidenter i myndigheternas verksamheter framkommit:

- Det finns exempel på myndigheter som inte har lyckats avvärja virusattacker, vilket fått till följd att verksamheten inte fungerat. Handläggarna hade exempelvis inte tillgång till nödvändig information.
- Allvarliga incidenter har inträffat när myndigheter bytt IT-system eller infört nya IT-system. Handläggare fick svårt att genomföra sina uppgifter. Viktiga samhällstjänster för medborgare och företag på Internet fick stängas ned upp till två veckor.
- Brister i skyddet av myndigheternas hemsidor har lett till att obehöriga fått tillgång till integritetskänsliga uppgifter och även kunnat ändra i dessa.

Dessa incidenter har bland annat sin grund i brister i myndighetsledningarnas arbete med informationssäkerheten. De viktigaste ledningsproblemen är:

- Ledningen är osäker på vilka uppgifter den har i informationssäkerhetsarbetet och hur dessa uppgifter ska utföras.

- Ledningen begär inte något tydligt underlag om vilka risker och hot som finns i verksamheten. Ledningen får därmed inte tillräcklig insikt i vilka åtgärder som ska prioriteras för att skydda verksamheten.
- Ledningens beslut om säkerhetsåtgärder fullföljs inte. Ledningen följer inte heller upp om säkerheten uppfyller ledningens krav. Ledningen är inte alltid medveten om att viktiga åtgärder som kontinuitetsplaner, rapportering och hantering av incidenter inte fungerar.
- Ledningen underskattar betydelsen av utbildning och information till personalen inklusive ledningspersonal och styrelsen.

7.2 Slutsatser om regeringens ansvar

Riksrevisionen bedömer att de ovan beskrivna problemen är allvarliga och att de innebär risk för betydande negativa konsekvenser för statliga åtaganden som elektronisk förvaltning och nationell krishantering.

Regeringens satsning på elektronisk förvaltning innebär att alltfler myndighetstjänster blir tillgängliga på Internet, att flera myndigheter tillsammans skapar samverkande e-tjänster samt en ökning av det IT-baserade utvecklingsarbetet i övrigt. För att denna reform av förvaltningen ska lyckas måste enskilda och företag ha förtroende för de e-tjänster som finns på Internet. Förtroendet för myndigheternas e-tjänster riskerar att minska om informationen inte kan skyddas. Det kan hända om obehöriga får åtkomst till känslig information eller om de kan förändra data, eller på annat sätt kan agera så att tjänsterna inte kan användas. Då finns en betydande risk för att hela satsningen på e-förvaltning äventyras. Detta har också påtalats i intervjuer med Regeringskansliet, expertmyndigheter och granskade myndigheter.

Brister i informationssäkerheten kan även påverka den nationella krishanteringen. Statliga myndigheter har som regel viktiga roller i samhällets förmåga att förebygga, förhindra och hantera kriser. Myndigheterna förutsätts därför ha en viss så kallad basförmåga för att kunna uppfylla sin roll och bidra till samhällets förmåga att klara kriser. Basförmågan är beroende av hur väl utformad myndighetens informationssäkerhet är.

I tidigare avsnitt har Riksrevisionen slagit fast att myndigheterna har ett eget ansvar för sin informationssäkerhet enligt ansvarsprincipen. Regeringen har ett ansvar för att ställa krav på och följa upp förvaltningens arbete med informationssäkerheten samt ta initiativ till åtgärder för att förbättra förutsättningarna för förvaltningens arbete inom detta område. *Riksrevisionens samlade bedömning är att regeringen inte följt upp om den interna styrningen och kontrollen av informationssäkerheten i statsförvaltningen varit tillfredsställande. Regeringen har inte heller tagit tillräckliga initiativ för att förbättra förutsättningarna för förvaltningens arbete med informationssäkerheten.*

7.2.1 Otydliga krav och mandat

Riksrevisionen konstaterar att regeringen har vidtagit åtgärder som rör tekniska förutsättningar för myndigheternas informationssäkerhetsarbete, till exempel e-signaturer, e-legitimationer, säkert Internet etc. Verva har fått i uppdrag att främja och följa utvecklingen av e-förvaltning och därmed även beakta vissa säkerhetsfrågor. Däremot har inga åtgärder vidtagits för att stödja myndigheternas interna styrning och kontroll av informationssäkerheten.

Granskade myndighetsledningar uppfattar inte tydligt vilka krav och regler som gäller för deras informationssäkerhetsarbete, exempelvis avseende ledningens ansvar och myndigheternas riskanalyser. Detta kan enligt Riksrevisionens bedömning orsakas av att författningarna på området inte ger någon tydlig och samlad vägledning[77]. Detta problem har också tidigare uppmärksammats av regeringen, men åtgärder är ännu inte vidtagna. Den av regeringen tidigare aviserade översynen och harmoniseringen av författningarna på informationssäkerhetsområdet har hittills inte genomförts.[78] Hösten 2005 lämnade InfoSäkutredningen ett förslag till förordning om informationssäkerhet. Detta förslag bereds fortfarande inom Försvarsdepartementet.

Regeringens strategi för informationssäkerhet ger inte heller någon tydlig vägledning, eftersom den är inriktad på samhället som helhet. Regeringen har gett KBM i uppdrag att utifrån strategin ta fram förslag på en nationell handlingsplan. Huruvida KBM:s uppdrag att ta fram en nationell handlingsplan utifrån strategin även kommer att omfatta frågor som särskilt berör de statliga myndighetsledningarnas arbete med informationssäkerheten är oklart.

Vid Finansdepartementet pågår ett arbete med en förordning om intern styrning och kontroll. Enligt uppgift planeras förordningen att träda i kraft i början av år 2008. Huruvida den aviserade förordningen kommer att minska problemen med styrning och kontroll av informationssäkerheten återstår att se.

Det finns ett antal expertmyndigheter (KBM, SÄPO, PTS, FRA, Verva, FM, FMV) med ansvar för olika frågor inom informationssäkerhetsområdet, och som ska ge stöd till regeringen och myndigheterna. Regeringen har dock inte givit expertmyndigheterna tillräckligt tydliga mandat, vilket inneburit svårigheter för dem att ge regeringen en samlad bild av informationssäkerhetsproblemen på myndigheterna. Tydliga mandat krävs också för att expertmyndigheterna ska kunna ge lämpliga föreskrifter som preciserar regeringens krav på informationssäkerheten. Den tidigare inrättade expertmyndigheten ÖCB (nedlagd 2002) hade föreskriftsrätt inom informationssäkerhetsområdet, vilket gav myndigheten mandat att utöva tillsyn över myndigheternas

77 Se särskild analys i bilaga 2.
78 Prop. 2001/02:10, Fortsatt förnyelse av totalförsvaret

informationssäkerhetsarbete. Efterträdaren KBM anser att myndigheten idag inte har ett lika omfattande mandat som ÖCB hade, och att KBM därmed inte kan granska myndigheterna. Istället är det för närvarande Verva som har föreskriftsrätt vad gäller standarder och liknande krav som ska vara gemensamma för elektroniskt informationsutbyte mellan myndigheterna under regeringen. Det framgår dock inte om Verva har rätt att föreskriva och ge allmänna råd om hur myndigheter ska utöva sin styrning och kontroll av informationssäkerheten, det vill säga utforma sina ledningssystem för informationssäkerhet.

7.2.2 Regeringen har inte följt upp myndigheternas arbete med informationssäkerhet

Genom att regeringen ställer krav på rapporteringen från enskilda myndigheter, från expertmyndigheterna och andra källor kan regeringen få en bild av eventuella generella problem som kräver åtgärder av regeringen. Granskningen visar att regeringen under de senaste tio åren i stora drag har varit medveten om vissa ledningsproblem på informationssäkerhetsområdet, men bilden har varit otydlig avseende statliga myndigheter och någon samlad problembild av den statliga förvaltningen har regeringen inte kunnat presentera.

Regeringen har inte ställt krav på de statliga myndigheterna att rapportera om de huvudsakliga ledningsproblemen när det gäller informationssäkerheten. Dessa aspekter har inte heller varit föremål för närmare diskussion inom ramen för regeringens mål- och resultatstyrning (regleringsbrev, myndighetsdialoger).

KBM:s lägesbedömningar av informationssäkerheten är en viktig källa för regeringens bedömning av informationssäkerhetsarbetet i samhället. Riksrevisionen konstaterar dock att regeringen inte har ställt krav på KBM att lämna specifik information om statliga myndigheter. Samtidigt anser KBM att myndigheten inte har ett sådant mandat att utöva tillsyn över myndigheternas informationssäkerhetsarbete som myndigheten behöver för att kunna ge regeringen ett bra underlag för sin styrning.

Ledningsfrågorna i statliga myndigheter har inte berörts i direktiven till de statliga utredningar som avsett informationssäkerhetsfrågor. Eftersom rapporteringen till regeringen varit översiktlig, och inte särskilt lyft fram problem i den statliga förvaltningen, har regeringen sannolikt inte uppfattat att det finns ett behov av mer information om och analys av statliga myndigheters informationssäkerhet. Regeringen har inte inom Regeringskansliet låtit genomföra någon sådan analys och inte heller uppdragit åt utredning, expertmyndighet eller annan att göra det. Dokumenterade analyser av myndigheternas ledningsproblem och vilka risker som det innebär för verksamheterna saknas. Likaså saknas analyser av vilka åtgärder som regeringen kan behöva vidta för att komma till rätta med problemen.

7.2.3 Brister i regeringens beredning av informationssäkerhetsfrågorna

Enligt Riksrevisionen är regeringens organisering av arbetet med informationssäkerhetsfrågorna och styrningen av expertmyndigheterna sammantaget otillräcklig för att hantera myndigheternas problem med sin informationssäkerhet.

Styrande för arbetet inom Regeringskansliet är ansvarsprincipen och principen om gemensam beredning. Ansvarsprincipen innebär i praktiken att varje myndighetshandläggare vid departementen hanterar frågor som rör den ”egna” myndighetens informationssäkerhet. Det är emellertid tveksamt om myndighetshandläggarna har fått tillräckliga förutsättningar (till exempel genom utbildning) att kunna bedöma den enskilda myndighetens informationssäkerhet. Vidare bygger myndighetshandläggarens dialog på ett förtroende för att myndigheten har tillräcklig kunskap för att hantera interna frågor om hur informationssäkerheten ska genomföras. Detta innebär att det krävs rapporter från myndigheter, medier eller någon annan aktör om att det inte fungerar för att departementet ska agera. Granskningen visar att denna dialog mellan departement och myndighet inte har varit tillräcklig för att uppmärksamma enskilda myndigheters problem med sitt informationssäkerhetsarbete.

Enligt Regeringskansliet ska myndighetsproblem som är av mer generellt slag kunna fångas upp i olika former av samråd inom Regeringskansliet och kanske främst i den så kallade gemensamma beredningen. Tydliga signaler krävs för att Regeringskansliet ska uppmärksamma enskilda myndigheters problem med informationssäkerhet. Det krävs också tydliga signaler för att Regeringskansliet ska uppmärksamma ett problem som ett generellt problem i förvaltningen och därmed ta initiativ till särskilda insatser från regeringens sida. Sådana signaler måste föras fram av någon aktör. När det gäller informationssäkerhet uppfattar Riksrevisionen Försvarsdepartementet som en central aktör tillsammans med sin myndighet KBM. Finansdepartementet kan också uppmärksamma generella problem i samband med budgetprocessen. Ingen av dessa potentiella aktörer har emellertid hittills uppfattat några tydliga indikationer – internt via myndighetshandläggare eller externt från expertmyndigheter - på behov av att särskilt uppmärksamma frågor om myndigheternas interna styrning och kontroll av informationssäkerheten. Regeringskansliet har inte heller uppfattat Riksrevisionens elva granskningar som indikation på generella problem inom statsförvaltningen. Riksrevisionen konstaterar att samrådet inom Regeringskansliet inte fångat upp de mer generella ledningsproblem som Riksrevisionen funnit.

Inget departement har ett uttalat ansvar för att göra en samlad bedömning av myndigheternas interna styrning och kontroll av informationssäkerheten. Intern styrning och kontroll av myndigheternas verksamhet är en generell fråga som Finansdepartementet ansvarar för. Departementet uttalar

sig emellertid inte i specifika frågor som är föremål för intern styrning och kontroll, till exempel informationssäkerhet. Däremot är informationssäkerhet en viktig aspekt i utvecklingen av e-förvaltning, som Finansdepartementet ansvarar för. Försvarsdepartementet hanterar huvudsakligen de högre hotnivåerna i samhället och hur samhällets grundsäkerhet klarar av kris och krig. Viktigt för samhällets grundsäkerhet är myndigheternas basförmåga, dvs. att de har en sådan robusthet och beredskap att de även kan möta krav och påfrestningar vid kriser. I basförmågan ingår myndigheternas informationssäkerhet. Trots detta starka samband ansvarar inte Försvarsdepartementet för frågor som rör myndigheternas basförmåga. Försvarsdepartementet har dock ansvar för informationssäkerhetsfrågor i och med ansvaret för KBM som har ett sammanhållande myndighetsansvar inom informationssäkerhetsområdet. Riksrevisionens granskning visar också på brister i dialogen mellan departementen beträffande informationssäkerhetsfrågor som avser basförmågan.

Inom Regeringskansliet finns det ämnessakkunniga som ansvarar för vissa sakfrågor med anknytning till informationssäkerhet, men ingen av dem har styrning och kontroll av informationssäkerhet som ansvar. Inom Regeringskansliet finns inte heller någon funktion eller något formellt nätverk[79] som ansvarar för sådant analysarbete som skulle kunna utgöra stöd för enskilda departement. Regeringen har dock nyligen inrättat en särskild statssekreterargrupp för att hantera frågor om bland annat utvecklingen av elektronisk förvaltning. Gruppen biträds av en särskild interdepartemental beredningsgrupp. Av intervjuer med statssekreterare framkommer att den typ av problem som Riksrevisionen funnit bör kunna fångas upp av dessa grupper.

Regeringen har valt att delegera flertalet informationssäkerhetsfrågor till expertmyndigheterna. Fördelningen av ansvar på expertmyndigheterna är emellertid otydlig när det gäller uppföljning och tillsyn av statliga myndigheters interna styrning och kontroll av informationssäkerhetsarbetet. KBM:s mandat att utöva tillsyn och utfärda föreskrifter riktade mot myndigheternas informationssäkerhetsarbete - såsom ÖCB gjorde - är inte tillräckligt preciserat och förväntningarna på KBM:s lägesrapporter inte klarlagda.

79 Under tidigare år träffades informationssäkerhetsintresserade handläggare från Näringsdepartementet, Försvarsdepartementet, Justitiedepartementet, Utrikesdepartementet och Finansdepartementet informellt.

7.3 Riksrevisionens rekommendationer

Under senare tid har regeringen vidtagit ett antal åtgärder för att ge förvaltningen och samhället i övrigt bättre förutsättningar att upprätthålla en god informationssäkerhet. Dessa åtgärder är dock enligt Riksrevisionens bedömning inte tillräckliga för att lösa de problem som myndighetsledningarna har med informationssäkerhetsarbetet. Riksrevisionen rekommenderar därför regeringen att vidta följande åtgärder för att förbättra den interna styrningen och kontrollen i statsförvaltningen.

7.3.1 Regeringen bör tydligare fokusera informationssäkerhetsfrågorna

Riksrevisionens elva granskningar av myndigheternas informationssäkerhetsarbete har inte uppfattats av regeringen som en signal på ett mer generellt problem. I och med regeringens satsning på e-förvaltning krävs att regeringen också vidtar åtgärder för att fokusera informationssäkerhetsfrågorna. Särskilt Försvarsdepartementet och Finansdepartementet bör närmare samordna sitt arbete i frågor som rör myndigheternas informationssäkerhet.

7.3.2 Ge expertmyndigheterna tydligt mandat att följa upp och rapportera om myndigheternas arbete med informationssäkerheten

Expertmyndigheterna har hittills inte kunnat förse regeringen med sådan information att regeringen fått en tillräcklig inblick i de väsentliga problem som finns i myndigheternas arbete med sin informationssäkerhet. Regeringen bör därför tydliggöra expertmyndigheternas uppdrag så att någon av dessa får ett tydligt mandat att följa upp och rapportera om myndigheternas styrning och kontroll av informationssäkerhetsarbetet. Regeringen bör i samband med detta precisera syftet med de årliga lägesbedömningarna.

7.3.3 Ge myndigheterna bättre förutsättningar - ställ tydligare krav på arbetet med informationssäkerheten

Myndigheterna har själva ansvaret för sin informationssäkerhet. Riksrevisionens granskningar har dock visat att myndighetsledningarna är osäkra på hur de ska hantera informationssäkerhetsfrågor. Detta kan enligt Riksrevisionens bedömning bland annat bero på att tillräckligt tydliga krav från regeringen saknas. Regeringen utlovade år 2001 en översyn av regleringen inom informationssäkerhetsområdet. Informationssäkerhetsutredningen kom 2005 med förslag på en förordning inom informationssäkerhetsområ-

det. Regeringen har ännu inte genomfört översynen av regleringen och inte heller tagit ställning till utredningens förslag. Riksrevisionen bedömer att översynen av regleringen är angelägen särskilt mot bakgrund av satsningen på e-förvaltning.

Regeringens strategi inom informationssäkerhetsområdet bör tydliggöras så att regeringen får en bättre grund för sin styrning inom statsförvaltningen och så att myndigheterna får bättre information om politikens innehåll.

Eftersom regeringen har givit KBM i uppdrag att ta fram en handlingsplan för genomförandet av regeringens strategi bör regeringens uppdrag enligt Riksrevisionens mening även omfatta att beakta myndigheternas interna styrning och kontroll av informationssäkerhetsarbetet.

I mål- och resultatstyrningen av de enskilda myndigheterna bör regeringen ta upp myndigheternas informationssäkerhetsarbete. Kraven på de enskilda myndigheterna bör anpassas efter deras skilda förutsättningar.

Källförteckning

Lagar

Arkivlagen (1990:782)
Förvaltningslagen (1986:223)
Lagen (2003:763) om behandling av personuppgifter inom socialförsäkringens administration
Lagen (2003:389) om elektronisk kommunikation
Lagen (2000:832) om kvalificerade elektroniska signaturer
Lagen (1996:1059) om statsbudgeten
Sekretesslagen (1980:100)
Personuppgiftslagen (1998:204)
Säkerhetsskyddslagen (1996:627)

Förordningar

Arkivförordningen (1991:446)
Förordningen (SFS 2003:396) om elektronisk kommunikation
Förordningen (1995:686) om intern revision
Förordningen (2006:942) om krisberedskap och förhöjd beredskap
Förordningen (2002:472) om åtgärder för fredstida krishantering och höjd beredskap
Förordningen (1995:1300) om myndigheternas riskhantering
Internrevisionsförordningen (2006:1228)
Säkerhetsskyddsförordningen (1996:633)
Verksförordningen (1995:1322)
Förordningen (1988:1122) med instruktion för Överstyrelsen för civil beredskap
Förordningen (1994:714) med instruktion för Försvarets radioanstalt
Förordningen (1995:679) med instruktion för Riksarkivet och landsarkiven
Förordningen (1996:103) med instruktion för Försvarets materielverk
Förordningen (1997:401) med instruktion för Post- och telestyrelsen
Förordningen (1998:1192) med instruktion för Datainspektionen
Förordningen (2000:555) med instruktion för Försvarsmakten
Förordningen (2002:518) med instruktion för Krisberedskapsmyndigheten
Förordningen (2002:1050) med instruktion för Säkerhetspolisen

Förordningen (2005:860) med instruktion för Verket för förvaltningsutveckling
Förordningen (1996:1515) med instruktion för Regeringskansliet. Bilaga med *fördelning av förvaltningsärenden och lagstiftningsärenden* till Instruktion för Regeringskansliet

Föreskrifter och allmänna råd till föreskrifter

E-nämnden 2004: *Vägledning för myndigheternas användning av e-legitimationer och elektroniska underskrifter* (2004:2, beslutad 9 juni 2004)
Datainspektionen: *Allmänna råd – Säkerhet för personuppgifter*, 1999
Ekonomistyrningsverket: *Föreskrifter till internrevisionsförordningen* (ESV cirkulär 2007:1)
Försvarsmakten Högkvarteret. *Försvarsmaktens föreskrifter om säkerhetsskydd* (FFS 2003:7, beslutade 20 oktober 2003)
Rikspolisstyrelsens *föreskrifter om säkerhetsskydd* (RPSFS 2004:11, FAP 244-1).
Verket för förvaltningsutveckling: *Föreskrift (VERVAFS 2007:1) om statliga myndigheters elektroniska fakturor; Allmänt råd (VERVAFS 2007:1AR)* om *statliga myndigheters elektroniska fakturor*
Överstyrelsen för civil beredskap: *Föreskrifter om grundsäkerhet för samhällsviktiga datasystem hos beredskapsmyndigheter* (ÖCB FS 1998:1).[80]

Betänkanden från utskott i riksdagen

Försvarsutskottets betänkande 2001/02:FöU10
Försvarsutskottets betänkande 2005/06:FöU9
Trafikutskottets betänkande 1995/96 TU:19, rskr. 1995/96:282
Trafikutskottens betänkande 1999/2000:TU9
Trafikutskottets betänkande 2005/06:TU4

Interna handledningar (motsv.) inom Regeringskansliet

Finansdepartementet Budgetavdelningen 2001: *Ekonomisk styrning – en handledning för Regeringskanslets verksamhets- och budgetberedning* (2001-05-18)
Regeringskansliet Statsrådsberedningen 2002: *Samrådsformer i Regeringskansliet*, PM 1997:4 (version reviderad 2002-02-06)

80 I syfte att förtydliga föreskrifterna meddelade ÖCB allmänna råd till dessa. Föreskrifterna och de allmänna råden kallas FA22 (Föreskrifter och Allmänna råd till då gällande beredskapsförordning (1993:242) 22 a § och 52 §)

Propositioner, skrivelser, regeringens strategier

Proposition 1995/96:125 *Åtgärder för att bredda och utveckla användningen av informationsteknik*
Proposition 1999/00:30 *Det nya försvaret*
Proposition 1999/00:86 *Ett informationssamhälle för alla*
Proposition 2001/02:10 *Fortsatt förnyelse av totalförsvaret*
Proposition 2001/02:158 Sam*hällets säkerhet och beredskap*
Proposition 2004/05:175 *Från IT-politik för IT-samhället till politik för IT-samhället*
Proposition2004/05:80 *Forskning för ett bättre liv*
Proposition 2005/06:133 *Samverkan vid kris – för ett säkrare samhälle*
Proposition 2006/07:1 *Utgiftsområde 2*, bilaga 1, avsnitt 2
Regeringskansliet: Näringsdepartementet 2006: Faktapromemoria *En strategi för ett säkert informationssamhälle* (2005/06:FPM116, 2006-09-06)
Regeringskansliet Finansdepartementet: *Bättre service för varje skattekrona – Strategi för fortsatt utveckling av elektronisk förvaltning*.
(Bilaga till protokoll vid regeringsammanträde 2006-06-21, nr 21)
Regeringen Näringsdepartementet: *Strategi för ökad säkerhet i Internets infrastruktur* (protokoll II 6, vid regeringssammanträde 2006-12-07 N2006/5335/ITFoU)

Offentliga utredningar, departementspromemorior

Arbetsgruppen för skydd mot informationsoperationer 1998: Rapport 2 med en strategi och ansvarsfördelning för skydd mot informationsoperationer (19 augusti 1998 , FO98 1297/MIL)
Försvarsdepartementet, Försvarsberedningen 2001: *Ny struktur för ökad säkerhet – nätverksförsvar och krishantering* (Ds 2001:44)
Finansdepartementet 2006: *Intern styrning och kontroll i staten – Förslag till ett gemensamt ramverk* (Ds 2006:15)
Regeringens direktiv till Informationssäkerhetsutredningen (dir. 2002:103, beslut den 11 juni 2002)
Regeringens direktiv till IT-standardiseringsutredningen (dir. 2006:36; N 2006:05)
Regeringens tilläggsdirektiv till IT-standardiseringsutredningen (dir. 2006:117, Näringsdepartementet)
Regeringens direktiv Utformningen av ett system med en krisledande myndighet (dir. 2006:81, regeringens beslut 29 juni 2006)
Regeringens direktiv Översyn av Statens räddningsverk, Krisberedskapsmyndigheten och Styrelsen för psykologiskt försvar för att skapa en myndighet för frågor om samhällets beredskap och säkerhet (dir. 2006:80, regeringens beslut 29 juni 2006)

SOU 2001:41 *Säkerhet i en ny tid* (Sårbarhets- och säkerhetsutredningen)
SOU 2003:27 *Signalskydd* (delbetänkande av Informationssäkerhetsutredningen)
SOU 2004:23 *Från verksförordning till myndighetsförordning*
SOU 2004:32 *Informationssäkerhet i Sverige och internationellt – en översikt*
SOU 2005:42 *Säker information.* Förslag till informationssäkerhetspolitik
SOU 2005:71 *Informationssäkerhetspolitik*. Organisatoriska konsekvenser
SOU 2007:31 *Alltid redo! En ny myndighet mot olyckor och kriser*

Regleringsbrev, uppdrag och andra regeringsbeslut

Regleringsbrev 2004 för Domstolsverket med krav på att återrapportera om informationssäkerheten i domstolsväsendet
Regleringsbrev 2006 till PTS med uppdrag att ta fram ett förslag till strategi för ett säkrare Internet i Sverige
Regleringsbrev 2004 för Krisberedskapsmyndigheten med uppdrag att i samverkan med FRA och Statskontoret kartlägga ansvaret för vidareutveckling av tekniskt stöd och den ansvarsfördelning som gäller för de frågor inom informationssäkerhetsområdet som rör BITS.
Regleringsbrev 2007 för Krisberedskapsmyndigheten med uppdrag att ta fram en nationell handlingsplan för informationssäkerhet
Regleringsbrev 2007 för Lantmäteriverket med återrapporteringskrav om åtgärder med anledning av Riksrevisionens granskning av informationssäkerheten
Regeringens uppdrag till Ekonomistyrningsverket att leda och samordna införandet av elektronisk fakturahantering i staten (Finansdepartementet 14 december 2006)
Regeringens uppdrag till Verket för förvaltningsutveckling att leda och samordna statsförvaltningens utvecklingsarbete med säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar (regeringsbeslut 16, 2006-11-30, Fi2006/6773 (delvis), Fi2006/967)
Regeringens uppdrag till Verket för förvaltningsutveckling att samordna automatisering av viss ärendehantering på myndigheter under regeringen och förenkling av tillgången till viss information ur statliga register och databaser. Regeringen uppdrar också åt Verva att följa upp arbetet med att utveckla e-förvaltningen (regeringsbeslut 3, 2007-02-22, Fi2007/1399 (delvis) Fi2004/4657
Tillsättande av statssekreterargrupp och interdepartementat arbetsgrupp för samordning av arbetet med elektronisk förvaltning (regeringssammanträde 2007-03-15)

Regeringens uppdrag till Vinnova att utarbeta en nationell strategi för säkerhetsforskning (2004).
Regeringens uppdrag till KBM att, i samverkan med VINNOVA, ansvara för att genomföra ett nationellt program för säkerhetsforskning (7 september 2006, Fö2006/2104/CIV)

Dokument från expertmyndigheter och andra myndigheter

Domstolsverket 2004: *Informationssäkerhet i domstolsväsendet,* DV-rapport 2004:8.
Krisberedskapsmyndigheten 2005: *Föreskrifter och tekniskt stöd inom området informationssäkerhet* – Ansvarsfördelning och ambitionsnivå med utgångspunkt från BITS, 2005-02-25, dnr 1279/2004)
Krisberedskapsmyndigheten 2007: *Budgetunderlag* för perioden 2008–2010 (2007-02-13, 0071/2007). I syfte att stärka den långsiktiga kunskapsuppbyggnaden inom informationssäkerhetsområdet planeras i början av denna period en riktad temautlysning för att främja svensk forskning på området.
Krisberedskapsmyndigheten 2006. *Hot- och riskrapport 2006*, KBM:s temaserie 2006:7
Krisberedskapsmyndigheten 2007. *IT-baserat informationspaket DISA* om informationssäkerhet (riktas till all personal)
Krisberedskapsmyndigheten. *Lägesbedömningar* 2004, 2005, 2006 och 2007
Krisberedskapsmyndigheten. *Minnesanteckningar* från möten i Informationssäkerhetsrådet
Krisberedskapsmyndigheten. *Minnesanteckningar* från möten i SAMFI Samverkansgruppen för Informationssäkerhet
Krisberedskapsmyndigheten. Rekommendation *Basnivå för informationssäkerhet (BITS)* (KBM 2006:1) + IT-stödet BITS PLUS
Krisberedskapsmyndigheten 2007. *Samhällsviktigt! Förslag till definition av samhällsviktig verksamhet ur ett krisberedskapsperspektiv*
Krisberedskapsmyndigheten. *Utbildning Esperanta* i informationssäkerhet som riktas till ledningspersonal
Krisberedskapsmyndigheten 2007. Utlysning om tematisk forskning på informationssäkerhetsområdet
Krisberedskapsmyndigheten 2007: *Årsredovisning* för budgetåret 2006.
Post- och telestyrelsen 2006. Rapport *Strategi för ett säkrare Internet i Sverige* (2006:12)
Post- och telestyrelsen 2005. *PTS i dag*
Post- och telestyrelsen 2003. *Surfa säkrare – Goda råd om säkerhet på Internet*
Post- och telestyrelsen 2006. *Årsredovisning 2005*, bland annat med rapportering om det interna arbetet med att utveckla PTS:s informationssäkerhet
Statskontoret 1991. Rapport *Myndigheternas säkerhetsanalyser av sina ADB-system* (1991-12-05, dnr 617/91-5)

Statskontoret 1998. Rapport *Sammanhållen strategi för samhällets IT-säkerhet*
Statskontoret 2003. *Vägledning i informationssäkerhet OffLIS* (2003:23)
SÄPO 2007. Publikationen *Säkerhetspolisen 2006*.
Vinnova, FMV och KBM 2006: Utlysning av initiering av säkerhetsforskning
Vinnova 2005: Slutrapport om ett nationellt forskningsprogram för säkerhetsforskning
ÖCB:s Årssammanställning av omvärldsanalys 2001

Standarder och internationella praxis

Standarden SS-ISO/IEC27001/17799, även kallad LIS-standarden[81]
Committee of Sponsoring Organizations of the Treadway Commission (COSO) har beskrivit den interna styrningens och kontrollens olika beståndsdelar och deras samband i den så kallade COSO-modellen
SIS, Bowin, Joachim (red), *Handbok 550 – Terminologi för informationssäkerhet,* SIS Förlag AB, Stockholm, 2003

EU, OECD och andra internationella organ

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, 2002
Europaparlamentets och rådets direktiv (2003/98/EG) om vidareutnyttjande av information från den offentliga sektorn, det så kallade PSI-direktivet.

Andra nationers regeringar, revisionsorgan och myndigheter

Danmark Ministeriet vor Videnskab Teknologi og Udvikling 2003: Rapport om standard för it-sikkerhedsprocesser i staten
Danmark regeringens ekonomiudvalg 2004: Beslut om att indföre en faelles standard for it-sikkerhedsprocesser i staten over en treårig periode. Standarden är baerad på Dansk Standards DS 484.
Norge Riksrevisjonen 2005: Riksrevisjonens undersökelse av myndighetenas arbeid med å sikre IT-infrastruktur.

81 SS-ISO/IEC 27001/17799, *Information Security Management – Specification With Guidance for Use.*

Riksrevisionen

Riksrevisionen 2005: *Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten*, 2005 (Rapport RiR 2005:26)
Riksrevisionen 2005: *Granskning av Sjöfartsverkets interna styrning och kontroll av informationssäkerheten*, 2005 (Rapport RiR 2005:27)
Riksrevisionen 2005: *Bolagsverkets informationssäkerhet* (2005-08-19, dnr 32.2005-0717)
Riksrevisionen 2006: *Granskning av Försäkringskassans interna styrning och kontroll av informationssäkerheten*, 2006
Riksrevisionen 2006: *Post- och telestyrelsens informationssäkerhet*, (2006-02-09, 32-2005-0738)
Riksrevisionen 2006: *Löpande granskning av Affärsverket Svenska Kraftnät 2005*, (2006-02-13, dnr 32-2005-0714)
Riksrevisionen 2006: *Försvarsmaktens styrning av informationssäkerhetsarbetet* (2006-06-21, 32-2005-0551)
Riksrevisionen 2006: *Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten*, 2006 (Rapport RiR 2006:24)
Riksrevisionen 2006: *Granskning av Migrationsverkets interna styrning och kontroll av informationssäkerheten*, 2006 (Rapport RiR 2006:25)
Riksrevisionen 2006: *Granskning av Lantmäteriverkets interna styrning och kontroll av informationssäkerheten*, 2006 (Rapport RiR 2006:26)
Riksrevisionen 2007: *Löpande granskning av Affärsverket Svenska Kraftnät 2006* (2007-02-12, 32-2006-0700)
Riksrevisionen 2007: *Uppföljning av Post- och telestyrelsens ledning av informationssäkerhetsarbetet* (2007-03-12, 32-2006-0726)

Konsultrapporter

Andersson, Helena 2007. *Rättsliga aspekter på myndigheternas informationssäkerhet* (2007-04-16). Utredning beställd av Riksrevisionen.

Bilaga 1 Expertmyndigheternas uppgifter

Det finns ingen myndighet som har en generell uppgift att följa upp (utvärdera och granska) enskilda myndigheters styrning och kontroll av informationssäkerhetsarbetet. I stället finns flera så kallade expertmyndigheter med särskilda uppgifter inom området informationssäkerhet. Expertmyndigheterna samverkar med varandra i flera fora.

Uppgifter enligt myndigheternas instruktioner

Datainspektionen (DI) är en central förvaltningsmyndighet med uppgift att verka för att människor skyddas mot kränkning av personlig integritet på grund av behandling av personuppgifter[82]. DI:s uppgift är också att se till att god sed iakttas i kreditupplysnings- och inkassoverksamhet. DI ska särskilt inrikta sin verksamhet på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud enligt personuppgiftslagen (1998:204). DI ska följa och beskriva utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik.

Försvarets radioanstalt (FRA) skall ha hög teknisk kompetens inom informationssäkerhetsområdet[83]. Försvarets radioanstalt får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig ur sårbarhetssynpunkt eller ur ett säkerhets- eller försvarspolitiskt avseende. Försvarets radioanstalt skall därvid särskilt kunna stödja insatser vid nationella kriser med IT-inslag, medverka till identifieringen av inblandade aktörer vid IT- relaterade hot mot samhällsviktiga system,genomföra IT-säkerhetsanalyser, och ge annat tekniskt stöd. Försvarets radioanstalt skall samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet.

Försvarets materielverk (FMV) är en central förvaltningsmyndighet med uppgift att anskaffa, vidmakthålla och avveckla materiel och förnödenheter på uppdrag av Försvarsmakten samt att inom detta område stödja Försvarsmaktens verksamhet[84]. FMV utvärderar och certifierar IT-säkerhetsprodukter.

82 Förordning (1998:1192) med instruktion för Datainspektionen.
83 Förordning (1994:714) med förordning för Försvarets Radioanstalt
84 Förordning (1996:103) med instruktion för Försvarets materielverk.

Av säkerhetsskyddsförordningen åläggs även Försvarsmakten vissa uppgifter. Av § 13 säkerhetsskyddsförordningen framgår att kryptering av hemliga uppgifter endast får ske med system som godkänts av Försvarsmakten. Vidare framgår av §39 säkerhetsskyddsförordningen att Försvarsmakten har tillsynsansvar över säkerhetsskyddet vid ett antal myndigheter.

Krisberedskapsmyndigheten (KBM) är en central förvaltningsmyndighet för frågor om samhällets säkerhet när det gäller krishantering och civilt försvar[85]. KBM bedriver bland annat omvärldsbevakning, omvärldsanalyser, sammanställer risk- och sårbarhetsanalyser och genomför övergripande analyser av dessa, utvecklar metoder för risk- och sårbarhetsanalyser. KBM ska ha ett sammanhållande myndighetsansvar för samhällets informationssäkerhet genom att sammanställa en helhetsbild av informationssäkerheten, bland annat genom att årligen lämna en lägesbedömning till regeringen.

KBM har enligt uppgift inriktat sina insatser inom informationssäkerhetsområdet främst mot kommuner och landsting, vilka KBM bedömer behöver mest stöd, och i mindre omfattning mot statliga myndigheter.

Post- och telestyrelsen (PTS) är en central förvaltningsmyndighet med ett samlat ansvar, sektorsansvar, inom postområdet och området för elektronisk kommunikation[86]. PTS ska bland annat främja tillgången till säkra och effektiva elektroniska kommunikationer enligt de mål som anges i lagen (2003:389) om elektronisk kommunikation. PTS kan meddela föreskrifter enligt förordningen (2003:396) om elektronisk kommunikation. PTS kan utöva tillsyn enligt lagen (2000:832) om kvalificerade elektroniska signaturer samt meddela föreskrifter inom detta område.

Vid PTS finns rikscentralen för IT-incidentrapportering (Sitic) som tar emot incidentrapporter från företag och myndigheter, larmar om IT-säkerhetshot med mera. PTS har enligt uppgift regelbundna avstämningsmöten med DI, KB, FRA, FMV, FM, Verva, Polisen. PTS har även regelbundna möten med operatörer och andra organisationer.

Riksarkivet och landsarkiven är statliga arkivmyndigheter med det särskilda ansvaret för den statliga arkivverksamheten och för arkivvården i landet, vilket framgår av arkivlagen (1990:782), arkivförordningen (1991:446)[87]. Riksarkivet ska särskilt verka för att myndigheterna och sådana enskilda organ som förvarar statliga arkiv på ett ändamålsenligt sätt fullgör sina skyldigheter enligt arkivlagen att bevara, vårda och hålla sina arkiv ordnade så att arkiven tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättskipning och förvaltning samt forskningens behov.

Säkerhetspolisen (SÄPO) har till uppgift att inom Rikspolisstyrelsen leda och bedriva polisverksamhet för att förebygga och avslöja terrorism och brott mot rikets säkerhet. SÄPO ska bland annat utföra uppgifter

85 Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten
86 Förordning (1997:401) med instruktion för Post- och telestyrelsen
87 Förordning (1995:679) med instruktion för riksarkivet och landsarkiven

enligt säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633)[88]. Bland uppgifterna ingår rådgivning, kontroll och information till myndigheter och företag som omfattas av säkerhetsskyddslagstiftningen. Beträffande informationssäkerhet ska SÄPO kontrollera att hemliga uppgifter skyddas.

Verket för förvaltningsutveckling (Verva) är en central förvaltningsmyndighet för utveckling av en sammanhållen statlig förvaltning[89]. I detta ingår bland annat att främja utvecklingsarbetet i statsförvaltningen och användningen av informationsteknik i offentlig förvaltning, till exempel genom att främja användningen av enhetliga kvalitetskrav och riktlinjer för användningen av informationsteknik och utveckla användbarheten av och tillgängligheten till elektronisk information och elektroniska tjänster. Av 3 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte framgår att Verva får meddela föreskrifter i fråga om standarder eller liknande krav som skall vara gemensamma för elektroniskt informationsutbyte för myndigheter under regeringen. Denna uppgift övertog myndigheten från den tidigare e-nämnden.

Verva har regeringens uppdrag (november 2006) att leda och samordna statsförvaltningens utvecklingsarbete med säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar.
Verva har också sedan februari 2007 regeringens uppdrag att samordna automatisering av viss ärendehantering på myndigheter under regeringen dels förenkling av tillgången till viss information ur statliga register och databaser. I uppdraget ingår också att Verva följer upp arbetet med att utveckla e-förvaltningen.

Fram till och med 2006 hade även Statskontoret vissa uppgifter om informationssäkerhet, men dessa är sedan den 1 januari 2007 överförda till Verva. Statskontoret utvecklade under 2000-talet en vägledning i informationssäkerhet – OffLIS – som var en anpassning av LIS-standarden till offentlig förvaltning (Statskontoret 2003:23). I vägledningen ingick också ett IT-stöd. Denna vägledning har senare integrerats i KBM:s rekommendation Basnivå för informationssäkerhet (BITS) (KBM 2006:1). Statskontoret har också medverkat i upphandling av tjänster som knyter an till informationssäkerhet, till exempel e-legitimation och elektroniska underskrifter.

Den tidigare så kallade e-nämnden tog 2005 fram förslag till föreskrifter om informationssäkerhet för 24-timmarsmyndigheter. Vidare publicerade e-nämnden en grundläggande vägledning för myndigheternas användning av e-legitimationer och elektroniska underskrifter. E-nämnden lades ned samtidigt som Verva inrättades den 1 januari 2006 och e-nämndens uppgifter överfördes till Verva.

88 Förordning (2002:1050) med instruktion för Säkerhetspolisen
89 Förordning (2005:860) med instruktion för Verket för förvaltningsutveckling

Samverkan

När regeringen preciserade ansvaret för de fyra expertmyndigheterna uttalade regeringen även att dessa myndigheter tillsammans ska samverka för att inte riskera att ansvarsområdena överlappar. Sådan samverkan sker i flera fora, bland annat i Informationssäkerhetsrådet, Samverkansgruppen för Informationssäkerhet (SAMFI) och Arbetsgruppen för Näringslivssamverkan. Syftet med Informationssäkerhetsrådet och SAMFI har diskuterats av de medverkande under senare tid, och i slutet av 2006 fastställdes syfte och arbetsformer.

Informationssäkerhetsrådet omfattar statliga myndigheter och företag. Rådet är ett verktyg för KBM:s verksamhet och rådet ger råd och stöd, men kan inte fatta beslut. Syftet är att gemensamt uppmärksamma behov av olika åtgärder. Syftet är också att skapa ett kvalificerat nätverk där deltagarna kan byta erfarenheter och ta del av varandras kompetens. Rådet har bland annat behandlat InfoSäkutredningen (2005), KBM:s lägesbedömningar, förslag till forskning om informationssäkerhet, BITS samt KBM:s uppdrag att ta fram en handlingsplan.

I SAMFI diskuterar expertmyndigheterna (KBM, PTS, FMV, FRA, Verva, Rikskriminalpolisen/SÄPO samt FM) de uppdrag och uppgifter som myndigheterna har fått av regeringen och hur dessa åtaganden ska genomföras av den enskilda myndigheten eller i samverkan mellan flera myndigheter. En viktig fråga för SAMFI har varit att stämma av myndigheternas råd och vägledningar om informationssäkerhet. Gruppen har bland annat diskuterat InfoSäkutredningen (2005), lämnat information om vad som är aktuella frågor för respektive myndighet samt diskuterat KBM:s lägesbedömningar, BITS, och andra insatser från KBM bland annat arbetet med den nationella handlingsplanen. Inom gruppen genomförs beslutade aktiviteter i projektform.

KBM har inom ramen för SAMFI initierat en arbetsgrupp för standardisering inom informationssäkerhetsområdet. Syftet med denna samverkan är att samordna aktiviteter, att följa och påverka den nationella och internationella utvecklingen, att motivera användandet av standarder samt att arbeta med utbildning och information inom området. För närvarande deltar cirka 15 myndigheter i detta samarbete.

Arbetsgruppen för Näringslivssamverkan inom informationssäkerhet syftar till att stärka samverkan mellan myndigheter och näringsliv inom området informationssäkerhet.

Expertmyndigheterna kan även ha egna referensgrupper (eller motsvarande) för sitt ansvar av informationssäkerheten. PTS har till exempel en referensgrupp för elektroniska signaturer.

Det bör också nämnas att regeringen även utnyttjar förvaltningsmyndigheter för att utföra vissa informationssäkerhetsuppgifter. Skatteverket (och tidigare Riksskatteverket) har haft regeringens uppdrag att utreda och föreslå lösningar för e-legitimationer och e-signaturer i förvaltningen. Detta arbete har gjorts i samverkan med flera myndigheter.

Stöd till förvaltningen

Expertmyndigheterna ger olika former av stöd till förvaltningen inom området informationssäkerhet. SÄPO kan ge stöd i anslutning till att SÄPO inspekterar en myndighet. Stödet kan även vara mer generellt i form av vägledningar, rådgivning och utbildningsinsatser. KBM, SÄPO, PTS och DI har tagit fram vägledningar eller råd för myndigheternas informationssäkerhetsarbete. Verva kommer att ta fram vägledningar (eller motsvarande) inom området säker elektronisk kommunikation och säkra elektroniska dokument. Verva har också föreskriftsrätt inom området elektronisk kommunikation. En föreskrift (VERVAFS 2007:1) och ett allmänt råd (VERVAFS 2007:1AR) har getts ut om statliga myndigheters elektroniska fakturor.

Expertmyndigheterna genomför ofta tillsammans seminarier om informationssäkerhet, ibland i samverkan med privata organisationer och föreningar som verkar inom området informationssäkerhet.

KBM har, i samråd med Statskontoret, tagit fram en särskild så kallad rekommendation – *Basnivå för informationssäkerhet* (BITS) – om hur informationssäkerhetsarbetet bör bedrivas. Denna rekommendation (KBM 2006:1) publicerades i januari 2006. BITS är anpassad till LIS-standarden. Till BITS finns också ett IT-stöd BITS PLUS. KBM har vidare under 2006 publicerat ett IT-baserat informationspaket – DISA – som riktas till all personal i förvaltningen.

Myndigheten har vidare under 2005 tagit fram en särskild utbildning i informationssäkerhet för ledningspersonal. Utbildningen bygger på scenarioövningar. Myndigheter har möjlighet att anlita KBM för att få råd om hur informationssäkerhetsarbete kan bedrivas.

Bilaga 2 Reglering av myndigheternas informationssäkerhet – utdrag ur konsultrapport[90]

Genomgång av reglering

Informationssäkerhetsrelevant reglering finns spridd över hela rättsordningen. De säkerhetsverktyg som finns i form av tekniska åtgärder, organisatoriska lösningar, legalt stöd med flera har olika begränsningar och möjligheter. För att säkerställa ändamålsenlig användning måste de olika säkerhetsverktygen samordnas. Ur ett informationssäkerhetsperspektiv måste därför en helhetssyn anläggas på informationssäkerhetsarbetet och på dess reglering.

Det finns en rad krav i olika regleringar som har bäring på myndigheters hantering av information. Vissa av dessa krav riktar sig direkt mot en viss typ av information medan andra rör vissa säkerhetsrelaterade åtgärder. Några exempel ges nedan.

Skyddet för *personuppgifter* är av centralt intresse när det gäller myndigheternas informationshantering. Enligt 31 § personuppgiftslagen (1998:204), PUL, ska den som är personuppgiftsansvarig[91] vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Vilka åtgärder som bör väljas är enligt lagrummet beroende av de tekniska möjligheter som finns, kostnaden för åtgärderna, vilka risker som finns och hur pass känsliga de behandlade personuppgifterna är.

Datainspektionen ger den personuppgiftsansvarige råd att beakta[92]. När det gäller integritetsskydd bör även registerlagstiftningen nämnas. Dessa regelverk rör specifika verksamheter och kan innehålla förhållandevis detaljerade krav på informationshanteringen. Som exempel kan nämnas lagen (2003:763) om behandling av personuppgifter inom socialförsäkringens administration vilken bland annat uttryckligen reglerar vilka som har behörighet att få tillgång till socialförsäkringsdatabasen.[93]

90 Grundas på rapport från konsulten, jur.kand. Helena Andersson, juridiska institutionen vid Stockholms universitet.
91 Enligt 3 § PUL den som bestämmer ändamålen med och medlen för behandling av personuppgifterna. När det gäller personuppgifter som hanteras inom ramen för en myndighets verksamhet så är myndigheten personuppgiftsansvarig.
92 Datainspektionen, Säkerhet för personuppgifter, 1999 (Datainspektionens allmänna råd) s. 26.
93 Se lag (2003:763) om behandling av personuppgifter inom socialförsäkringens administration 16 20 §§.

Bland de *allmänna handlingar* som myndigheterna hanterar finns inte sällan även sekretessbelagda uppgifter. Enligt 1 kap. 2 § sekretesslagen (1980:100) får inte uppgifter för vilka sekretess gäller röjas för enskild i andra fall än vad som närmare anges i lagen.[94]

När det gäller myndigheter som behandlar uppgifter som är sekretessbelagda med hänvisning till rikets säkerhet, 2 kap. sekretesslagen, ställer säkerhetsskyddslagen (1996:627) krav på att det finns ett säkerhetsskydd. Säkerhetsskyddet ska ge skydd mot spionerі, sabotage och terroristbrott och enligt lagens 9 § ska utformningen av säkerheten vid behandling i IT-system särskilt beaktas.

Dessa tre exempel visar på situationer då regleringen ställer särskilda krav på hantering av en viss typ av information. Regleringen kan även uttrycka krav på att vissa säkerhetsåtgärder vidtas.

Även andra regelverk ställer krav på åtgärder av betydelse för informationssäkerhetsarbetet. Förordningen om krisberedskap och förhöjd beredskap (2006:942) kräver att samtliga myndigheter genomför en *riskanalys* en gång per år. Ur ett informationssäkerhetsperspektiv är en väl genomförd riskanalys ett viktigt säkerhetsverktyg och i princip en förutsättning för att andra säkerhetsverktyg ska kunna utnyttjas optimalt. Enligt förordningen ska myndigheten i riskanalysen *identifiera sårbarheter eller hot som allvarligt kan försämra myndighetens verksamhet inom sitt område*. Syftet är enligt 9 § i förordningen att stärka sin egen och samhällets krisberedskap. En redovisning baserad på riskanalysen ska skickas in till regeringen med en kopia till Krisberedskapsmyndigheten.

Även förordningen om myndigheternas riskhantering (1995:1300) ställer krav på att myndigheterna genomför en riskanalys. Förordningen riktas dock endast till myndigheter under regeringen och har till syfte att *identifiera sådana risker som kan innebära skador eller förluster för staten*.[95] Efter att ha värderat riskerna och uppskattat vilka kostnader riskerna medför ska myndigheten vidta lämpliga åtgärder för att begränsa riskerna och förebygga skador eller förluster.

I säkerhetsskyddsförordningen (1996:633) ges bestämmelser till säkerhetsskyddslagen utom när det gäller riksdagen och dess myndigheter. Förordningen innehåller även mer detaljerade instruktioner om vilka säkerhetsåtgärder som ska vidtas när det gäller IT-system i vilka hemliga uppgifter med hänsyn till rikets säkerhet finns. Av särskilt intresse är kravet på att de som berörs av regleringen, bland annat statliga myndigheter, ska upprätta en *säkerhetsanalys*. Analysen ska innehålla uppgifter om vilka uppgifter som ska hållas hemliga med hänsyn till rikets säkerhet och skyddet mot terrorism.[96] Vidare ska en *säkerhetsskyddschef* utses. Säkerhetsskyddschefen ska utöva

94 Se 1 kap. 1 § sekretesslagen (1980:100).
95 1 och 3 §§ förordningen (1995:1300) om statliga myndigheters riskhantering.
96 5 § säkerhetsskyddsförordningen (1996:633).

kontroll över säkerhetsskyddet och vara direkt underställd myndighetens chef.[97] Säkerhetsskyddsförordningen innehåller regler för hur vissa uppgifter som behandlas med hjälp av IT ska skyddas. Bland annat måste samråd med Försvarsmakten alternativt SÄPO ske innan ett register som innehåller uppgifter som i vissa fall kan skada totalförsvaret upprättas. Om flera personer ska använda systemet ska detta enligt 12 § säkerhetsskyddsförordningen vara försett med funktioner för behörighetskontroll och loggning. Förordningen innehåller även regler för kryptering och kommunikation av hemliga uppgifter.[98]

I detta sammanhang bör även verksförordningen nämnas, kraven på effektiv verksamhet som ställs i förordningen skulle även kunna implicera krav på effektivt säkerhetsarbete. I en översyn av regleringen konstaterade utredaren att kravet på effektivitet innebär att ”förvaltningen skall åstadkomma avsedda resultat och uppnå de mål som fastställts av statsmakterna på ett så kostnadseffektivt sätt som möjligt utan att för den skull göra avkall på en hög kvalitet i arbetet”.[99] Otillräcklig säkerhet leder som Riksrevisionen visat till brister i verksamheten.

Den 1 januari 2007 trädde även internrevisionsförordningen (2006:1228) i kraft. Förordningen innehåller i 4 § krav på att internrevisionen hos en myndighet ska granska om myndighetens interna styrning och kontroll är utformad så att myndigheten med en rimlig säkerhet uppnår en effektiv verksamhet. Reglerna förtydligas i Ekonomistyrningsverkets föreskrifter. I föreskrifterna ställs även krav på att en riskanalys genomförs årligen.

Sammanfattningsvis kan vi konstatera att de mer uttryckliga kraven på att informationssäkerhet uppnås dels är kopplade till hanteringen av en viss typ av information, exempelvis personuppgifter, dels rör vissa typer av åtgärder, främst riskanalyser. Det är vidare främst konfidentialitet och riktighet som utgör målet för åtgärderna även om kraven på effektivitet är så generellt hållna att det inte framgår vilken typ av säkerhet som ska uppnås.

Definitioner

Eftersom flera av de krav som ställs på myndigheternas säkerhetsarbete är kopplade till en viss typ av information alternativt en viss situation har definitionerna stor betydelse för myndigheternas informationssäkerhetsarbete. Det är exempelvis stor skillnad mellan kraven som ställs på skyddet för sekretessbelagd information rörande rikets säkerhet jämfört med uppgifter som vare sig är sekretessbelagda eller innehåller personuppgifter. Det är även en betydande skillnad mellan reglerna för hur en krissituation ska

97 6 § säkerhetsskyddsförordningen (1996:633).
98 13 § säkerhetsskyddsförordningen (1996:633).
99 SOU 2004:23 Från verksförordning till myndighetsförordning s. 267.

hanteras respektive för hur den ordinarie verksamheten ska bedrivas. Ur ett informationssäkerhetsperspektiv är därför definitionerna av stor praktisk betydelse. Exempelvis skiljer sig de legala säkerhetskraven när det gäller uppgifter som rör rikets säkerhet mot hur andra uppgifter kan hanteras.

Analys

Ett ändamålsenligt regelverk skulle genom krav, utpekande av ansvar, tydliga definitioner och lämpliga sanktioner skapa förutsättningar för ett väl fungerande informationssäkerhetsarbete hos myndigheterna. Exempelvis skulle krav kunna ställas på att generella riskanalyser genomförs och följs upp, att myndighetens ledning ges ett uttryckligt ansvar för att en verksamhetsanpassad informationssäkerhetsnivå uppnås och att definitionen av informationssäkerhet ges en bred innebörd som motsvarar hur begreppet de facto används inom informationssäkerhetsområdet. En närmare analys visar dock på brister:

De legala krav som ställs på en säker informationshantering hos myndigheterna berör avgränsade områden och detaljeringsgraden skiljer sig åt.

- Skyddet för uppgifter som är sekretessbelagda med hänvisning till rikets säkerhet är jämförelsevis detaljreglerat.
- Hanteringen av övriga sekretessbelagda uppgifter är betydligt mer översiktligt reglerad med bestämmelserna i 15 kap. 9 § sekretesslagen som ett exempel.
- Skyddet för personuppgifter är även det reglerat men med skillnaden att de mer detaljerade beskrivningarna av åtgärder inte är bindande.

De krav som är av mer generell karaktär berör inte uttryckligen säkerhetsfrågor.

- De krav som ställs på myndigheters effektivitet i verksamheten är inte uttryckligen knutna till säkerhetsfrågor även om en sådan knytning kan impliceras. Internrevisionsreglerna nämner att verksamheten ska utföras på ett säkert sätt men ger ingen ytterligare ledning.

De krav som berör specifika säkerhetsåtgärder är avgränsade både när det gäller typen av åtgärd och syftet med den.

- Exempelvis är syftena med de regelverk som ställer krav på att myndigheterna genomför en riskanalys att stärka sin egen och samhällets krisberedskap, skydda information med hänsyn till rikets säkerhet respektive identifiera risker som kan innebära skador eller förluster för staten.
- Krav på någon heltäckande riskanalys som tar hänsyn till samtliga informationssäkerhetsaspekter görs inte.

Regleringen säkerställer endast delar av informationssäkerhetsbehovet. Reglering som uttryckligen och på ett tydligt sätt stöder riktighet, tillgänglighet och spårbarhet är begränsad. Utöver exemplen nedan ställer regleringen i huvudsak krav på konfidentialitet alternativt att vissa specifika åtgärder som riskanalyser vidtas.

- Det finns regler som säkerställer allmänna handlingars tillgänglighet men få krav ställs när det gäller övrig information.
- Datainspektionens allmänna råd om säkerhet kring personuppgifter innehåller rekommendationer rörande behörighetskontrollsystem, en åtgärd som i det närmaste är en förutsättning för att säkerställa spårbarhet och informationens riktighet. Utöver dessa icke bindande regler kan man möjligen tolka in krav på skydd för informationens riktighet och spårbarhet i allmänna regler om effektiv förvaltning. Effektivitetskravet blir i praktiken svårt att upprätthålla om obehöriga kan få tillgång till och ändra informationen.
- PUL innehåller vissa regler om rättning av felaktiga uppgifter vilket stöder informationens autenticitet.

Gränsdragningen mellan vad som faller inom respektive utanför myndighetens ansvarsområde när det gäller säkerhet är inte tydligt uttalad.

- Informationssäkerhet är ett komplicerat område. Vid sidan av de speciella krav som exempelvis ställs i PUL finns inte mycket ledning att hämta i regleringen. Detta kan resultera i att informationssäkerhetsfrågan ges inte mycket uppmärksamhet alternativt säkerhetsnivån hos myndigheterna kan komma att skilja sig åt mer än vad som är nödvändigt ur ett verksamhetsperspektiv eftersom ansvarsområdet tolkas på olika sätt.

Bilaga 3 Förteckning över genomförda intervjuer

Sammanlagt har 31 personer intervjuats vid totalt 20 intervjuer.

3 statssekreterare

Finansdepartementet
Försvarsdepartementet
Näringsdepartementet

17 departementstjänstemän

6 inom Finansdepartementet
3 inom Näringsdepartementet
2 inom Försvarsdepartementet
3 inom Arbetsmarknadsdepartementet
2 inom Justitiedepartementet

11 företrädare för expertmyndigheter

4 inom Krisberedskapsmyndigheten
2 inom Post- och Telestyrelsen
2 inom SÄPO
2 inom Verket för förvaltningsutveckling
1 inom Ekonomistyrningsverket

Tidigare utgivna rapporter från Riksrevisionen

2003 2003:1 Hur effektiv är djurskyddstillsynen?
2004 2004:1 Länsplanerna för regional infrastruktur – vad har styrt prioriteringarna?

2004:2 Förändringar inom kommittéväsendet
2004:3 Arbetslöshetsförsäkringens hantering på arbetsförmedlingen
2004:4 Den statliga garantimodellen
2004:5 Återfall i brott eller anpassning i samhället – uppföljning av kriminalvårdens klienter
2004:6 Materiel för miljarder – en granskning av försvarets materielförsörjning
2004:7 Personlig assistans till funktionshindrade
2004:8 Uppdrag statistik Insyn i SCB:s avgiftsbelagda verksamhet
2004:9 Riktlinjer för prioriteringar inom hälso- och sjukvård
2004:10 Bistånd via ambassader – en granskning av UD och Sida i utvecklingssamarbetet
2004:11 Betyg med lika värde? – en granskning av statens insatser
2004:12 Höga tjänstemäns representation och förmåner
2004:13 Riksrevisionens årliga rapport 2004
2004:14 Arbetsmiljöverkets tillsyn
2004:15 Offentlig förvaltning i privat regi – statsbidrag till idrottsrörelsen och folkbildningen
2004:16 Premiepensionens första år
2004:17 Rätt avgifter? – statens uttag av tvingande avgifter
2004:18 Vattenfall AB – Uppdrag och statens styrning
2004:19 Vem styr den elektroniska förvaltningen?
2004:20 The Swedish National Audit Office Report 2004
2004:21 Försäkringskassans köp av tjänster för rehabilitering
2004:22 Arlandabanan Insyn i ett samfinansierat järnvägsprojekt
2004:23 Regelförenklingar för företag
2004:24 Snabbare asylprövning
2004:25 Sjukpenninganslaget – utgiftsutveckling under kontroll?
2004:26 Utgift eller inkomstavdrag? – Regeringens hantering av det tillfälliga sysselsättningsstödet
2004: 27 Stödet till polisens brottsutredningar
2004:28 Regeringens förvaltning och styrning av sex statliga bolag
2004:29 Kontrollen av strukturfonderna
2004:30 Barnkonventionen i praktiken
2005 2005:1 Miljömålsrapporteringen – för mycket och för lite
2005:2 Tillväxt genom samverkan? Högskolan och det omgivande samhället
2005:3 Arbetslöshetsförsäkringen – kontroll och effektivitet

2005:4 Miljögifter från avfallsförbränningen – hur fungerar tillsynen
2005:5 Från invandrarpolitik till invandrarpolitik
2005:6 Regionala stöd – styrs de mot ökad tillväxt?
2005:7 Ökad tillgänglighet i sjukvården? – regeringens styrning och uppföljning
2005:8 Representation och förmåner i statliga bolag och stiftelser
2005:9 Statens bidrag för att anställa mer personal i skolor och fritidshem
2005:10 Samordnade inköp
2005:11 Bolagiseringen av Statens järnvägar
2005:12 Uppsikt och tillsyn i samhällsplaneringen – intention och praktik
2005:13 Riksrevisionens årliga rapport 2005
2005:14 Förtidspension utan återvändo
2005:15 Marklösen Finns förutsättningar för rätt ersättning?
2005:16 Statsbidrag till ungdomsorganisationer – hur kontrolleras de?
2005:17 Aktivitetsgarantin – Regeringen och AMS uppföljning och utvärdering
2005:18 Rikspolisstyrelsens styrning av polismyndigheterna
2005:19 Rätt utbildning för undervisningen Statens insatser för lärarkompetens
2005:20 Statliga myndigheters bemyndiganderedovisning
2005:21 Lärares arbetstider vid universitet och högskolor – planering och uppföljning
2005:22 Kontrollfunktioner – två fallstudier
2005:23 Skydd mot mutor Läkemedelsförmånsnämnden
2005:24 Skydd mot mutor Apoteket AB
2005: 25 Rekryteringsbidrag till vuxenstuderande – uppföljning och utbetalningskontroll
2005:26 Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten
2005:27 Granskning av Sjöfartsverkets interna styrning och kontroll av informationssäkerheten
2005:28 Fokus på hållbar tillväxt? Statens stöd till regional projektverksamhet
2005:29 Statliga bolags årsredovisningar
2005:30 Skydd mot mutor Banverket
2005:31 När oljan når land – har staten säkerställt en god kommunal beredskap för oljekatastrofer?

2006 2006:1 Arbetsmarknadsverkets insatser för att minska deltidsarbetslösheten
2006:2 Regeringens styrning av Naturvårdsverket
2006:3 Kvalitén i elöverföringen – finns förutsättningar för en effektiv tillsyn
2006:4 Mer kemikalier och bristande kontroll – tillsynen av tillverkare och importörer av kemiska produkter
2006:5 Länsstyrelsernas tillsyn av överförmyndare
2006:6 Redovisning av myndigheters betalningsflöden
2006:7 Begravningsverksamheten – förenlig med religionsfrihet och demokratisk styrning?

2006:8 Skydd mot korruption i statlig verksamhet
2006:9 Tandvårdsstöd för äldre
2006:10 Punktskattekontroll – mest reklam?
2006:11 Vad och vem styr de statliga bolagen?
2006:12 Konsumentskyddet inom det finansiella området – fungerar tillsynen?
2006:13 Kvalificerad yrkesutbildning – utbildning för marknadens behov?
2006:14 Arbetsförmedlingen och de kommunala ungdomsprogrammen
2006:15 Statliga bolag och offentlig upphandling
2006:16 Socialstyrelsen och de nationella kvalitetsregisten inom hälso- och sjukvården
2006:17 Förvaltningsutgifter på sakanslag
2006:18 Riksrevisionens Årliga rapport
2006:19 Statliga insatser för nyanlända invandrare
2006:20 Styrning och kontroll av regeltillämpningen inom socialförsäkringen
2006:21 Finansförvaltningen i statliga fastighetsbolag
2006:22 Den offentliga arbetsförmedlingen
2006:23 Det makroekonomiska underlaget i budgetpropositionerna
2006:24 Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten
2006: 25 Granskning av Migrationsverkets interna styrning och kontroll av informationssäkerheten
2006:26 Granskning av Lantmäteriverkets interna styrning och kontroll av informationssäkerheten
2006:27 Regeringens uppföljning av överskottsmålet
2006:28 Anställningsstöd
2006:29 Reformen av Försvarets logistik Blev det billigare och effektivare
2006:30 Socialförsäkringsförmåner till gravida Försäkringskassans agerande för en lagenlig och enhetlig tillämpning
2006:31 Genetiskt modifierade organismer – det möjliga och det rimliga
2006:32 Bidrag som regeringen och Regeringskansliet fördelar

2007 2007:1 Statlig tillsyn av bostad med särskild service enligt LSS
2007:2 The Swedish National Audit Office Annual report 2006
2007:3 Regeringens beredning och redovisning av skatteutgifter
2007:4 Beredskapen för kärnkraftsolyckor
2007:5 Regeringens skatteprognoser
2007:6 Vägverkets körprov – lika för alla?
2007:7 Den största affären i livet – tillsyn över fastighetsmäklare och konsumenternas möjlighet till tvistelösning
2007:8 Regeringens beredning av förslag om försäljning av sex bolag
2007:9 Säkerheten vid vattenkraftdammar

Beställning: publikationsservice@riksrevisionen.se