EN GRANSKNINGSRAPPORT FRÅN RIKSREVISIONEN

Informationssäkerheten i den civila statsförvaltningen

RIR 2014:23

RIKSREVISIONEN

Riksrevisionen är en myndighet under riksdagen med uppgift att granska den verksamhet som bedrivs av staten. Vårt uppdrag är att genom oberoende revision skapa demokratisk insyn, medverka till god resursanvändning och effektiv förvaltning i staten.

Riksrevisionen bedriver både årlig revision och effektivitetsrevision. Denna rapport har tagits fram inom effektivitetsrevisionen, vars uppgift är att granska hur effektiv den statliga verksamheten är. Effektivitetsgranskningar rapporteras sedan 1 januari 2011 direkt till riksdagen.

RIKSREVISIONEN

ISBN 978 91 7086 361 5
RIR 2014:23
FOTO: JOHNER
FORM: ÅKESSON & CURRY
TRYCK: RIKSDAGENS INTERNTRYCKERI, STOCKHOLM 2014

EN GRANSKNINGSRAPPORT FRÅN RIKSREVISIONEN

RiR 2014:23

Informationssäkerheten i den civila statsförvaltningen

RIKSREVISIONEN

TILL RIKSDAGEN

DATUM: 2014-11-10
DNR: 31-2013-1288
RIR 2014:23

Härmed överlämnas enligt 9 § lagen (2002:1022) om revision av statlig verksamhet m.m. följande granskningsrapport över effektivitetsrevision:

Informationssäkerheten i den civila statsförvaltningen

Riksrevisionen har granskat om arbetet med informationssäkerhet i den civila statsförvaltningen är ändamålsenligt utifrån ökande hot och risker. Granskningen avser regeringen och dess stöd- och tillsynsmyndigheter för informationssäkerhet. Resultatet av granskningen redovisas i denna granskningsrapport.

Företrädare för Säkerhetspolisen, Datainspektionen, Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Post- och telestyrelsen samt Regeringskansliet har fått tillfälle att faktagranska och i övrigt lämna synpunkter på utkast till slutrapport.

Rapporten innehåller slutsatser och rekommendationer som avser Regeringskansliet, Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt samt Säkerhetspolisen.

Riksrevisor *Claes Norgren* har beslutat i detta ärende. Revisionsdirektör *Per Dackenberg* har varit föredragande. Revisionsdirektörerna *Marcus Pettersson* och *Thomas Dawidowski* har medverkat vid den slutliga handläggningen

Claes Norgren Per Dackenberg

För kännedom:

Regeringen, Försvarsdepartementet

Justitiedepartementet, Näringsdepartementet, Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Post- och telestyrelsen samt Datainspektionen

Innehåll

forts.

Övrigt material

Till rapporten finns även två elektroniska underlag som kan laddas ner från Riksrevisionens webbplats www.riksrevisionen.se.

Underlag 1 Några myndigheters rapportering om informationssäkerhet
Underlag 2 Direktiv till två pågående utredningar

Sammanfattning

Vi lever i dag i ett samhälle där större mängder information än någonsin tidigare bearbetas, lagras, kommuniceras och mångfaldigas. Det finns stora möjligheter och fördelar med en ökad informationsanvändning. Samtidigt innebär den ökande utvecklingen av IT att samhället öppnas upp för stora risker som vi sannolikt inte är medvetna om i dag. Brister i hanteringen och säkerheten för informationen riskerar att få omfattande konsekvenser, såväl för samhället i stort som för enskilda. Brister kan också leda till ett försämrat förtroende för offentliga och privata aktörer som tillhandahåller viktiga tjänster. Informationssäkerhet omfattar därigenom hela samhället och är en angelägenhet för alla.

Granskningens bakgrund

Denna granskning tar sin utgångspunkt i den allt mer ökande användningen av information i samhället och i statsförvaltningen samt utifrån de brister som konstaterades genom Riksrevisionens tidigare granskningar av informationssäkerhet.

Riksrevisionen granskade under 2005–2007 elva myndigheter och deras arbete med informationssäkerhet. För sex av dessa myndigheter gjordes en djupare granskning. Denna serie av granskningar avslutades med en granskning som avsåg regeringens styrning av myndigheternas informationssäkerhetsarbete. Riksrevisionens samlade bedömning var att det fanns brister i myndigheternas arbete med informationssäkerhet och att regeringen inte hade följt upp om den interna styrningen och kontrollen av informationssäkerheten varit tillfredsställande. Regeringen hade inte heller tagit tillräckliga initiativ för att förbättra förutsättningarna för statsförvaltningens arbete med informationssäkerhet.

Granskningens syfte

Denna granskning har syftat till att utreda om arbetet med informationssäkerhet i den civila statsförvaltningen är ändamålsenligt utifrån ökande hot. Granskningen omfattar således varken styrningen av eller nivån på informationssäkerhet i samhället i stort. I granskningen har vi inriktat oss på den kunskap och information som samlats in om vilka hot som realiseras samt om hot och risker på en systematisk och övergripande nivå för den civila statsförvaltningen. Granskningen syftar också till att bedöma om

regeringen och ansvariga myndigheter för stöd och tillsyn har tillräcklig kunskap om de skyddsåtgärder som har vidtagits av myndigheter inom den civila statsförvaltningen.

Granskningen svarar på två frågor:

- Är regeringens styrning av informationssäkerhet i den civila statsförvaltningen effektiv?
- Har regeringens stöd- och tillsynsmyndigheter vidtagit tillräckliga åtgärder för att informera sig och regeringen om vilka hot som finns mot den civila statsförvaltningen, i vilken omfattning de realiseras och vilka skyddsåtgärder som vidtas?

Hur enskilda myndigheter arbetar med informationssäkerhet ingår inte i granskningen. Inte heller har granskningen sökt bevisa omfattningen av specifika brister i informationssäkerheten.

Granskningen avser regeringen (via Försvarsdepartementet, Justitiedepartementet, och Näringsdepartementet) samt stöd- och tillsynsmyndigheterna Myndigheten för samhällsskydd och beredskap (MSB), Försvarets radioanstalt (FRA), Säkerhetspolisen och Post- och telestyrelsen (PTS). Granskningen avser den civila delen av statsförvaltningen och omfattar därför inte hur Försvarsmakten bedriver arbetet med informationssäkerhet inom sitt verksamhetsområde.

Granskningens resultat

Riksrevisionens samlade slutsats av denna granskning är att arbetet med informationssäkerheten inte är ändamålsenligt, sett till de hot och risker som finns. Den tekniska utvecklingen har accelererat och de risker en organisation utsätts för ökar och kan förväntas fortsätta öka framöver. Som framgår av underlag i granskningen har vissa av riskerna förverkligats, och konsekvenserna har varit allvarliga. Detta understryker vikten av en god kännedom om beredskapen för att förebygga och hantera liknande och andra händelser. Ett riskbaserat tillvägagångssätt i arbetet med informationssäkerheten är en förutsättning för att på ett samlat sätt kunna värdera sannolikheten för att olika händelser ska inträffa och vilka konsekvenser som kan bli följden. Det finns flera riskområden inom statsförvaltningen när det gäller informationssäkerheten, såsom exempelvis kompetensbrist, upphandling, tillsyn/uppföljning/återrapportering samt styrning/omreglering/samordning.

En stor del av den information som skapas och lagras i samhället är viktig och samtidigt känslig. Är informationen förlorad, stulen, manipulerad eller spridd till obehöriga kan det få allvarliga följder. Konsekvenserna spänner från att det kan drabba hela samhällsfunktioner till att drabba enskilda. Granskningen har visat på omfattande brister i statsförvaltningen. Av underlaget till granskningen framgår att 84 procent av myndigheterna som själva administrerar sina IT-system uppger

att de har en informationssäkerhetspolicy. Samtidigt framgår att 38 procent av myndigheterna bedömer att kompetens, mandat eller resurser är otillräckliga för att utföra informationssäkerhetsarbetet på ett tillfredsställande sätt. Vidare uppger 42 procent av myndigheterna att det saknas regler för vad en riskanalys, som ska göras i ett systematiskt informationssäkerhetsarbete, ska omfatta eller när den ska ske. Slutligen uppger 65 procent av myndigheterna att de saknar en kontinuitetsplan. Riksrevisionens bedömning är därför att en stor andel myndigheter inte har centrala delar av ett systematiskt informationssäkerhetsarbete på plats.

Regeringen har inte någon samlad lägesbild som inkluderar hot, i vilken omfattning och mot vilka hoten realiseras samt vilka skyddsåtgärder myndigheterna vidtar. En sådan lägesbild har inte heller någon av regeringens stöd- och tillsynsmyndigheter. Det innebär att den samlade förmågan att kunna hantera de konsekvenser som kan bli följden av en allvarlig incident till stora delar är okänd. Av det skälet är det nödvändigt att regeringen och dessa myndigheter vidtar åtgärder, så att det går att få en samlad bild av läget och utifrån detta anpassar kraven på säkerheten till de behov som finns.

Riksrevisionens granskning har visat att

- regeringen inte utövat en effektiv styrning av informationssäkerheten i den civila statsförvaltningen och
- regeringens stöd- och tillsynsmyndigheter endast delvis har vidtagit nödvändiga åtgärder för att informera sig och regeringen om vilka hot som finns mot den civila statsförvaltningen, i vilken omfattning de realiseras och vilka skyddsåtgärder som vidtas.

Riksrevisionen drar denna slutsats mot följande bakgrund. Riksrevisionen har som ett led i granskningen uppdragit åt MSB, FRA och Säkerhetspolisen att analysera uppgifter om läget för informationssäkerheten i statsförvaltningen. Redovisningen av dessa uppdrag innebär väsentlig, ny information om läget. Vart och ett av myndigheternas yttranden pekar dessutom entydigt i samma riktning.

Regelsystemet för informationssäkerhet ser i huvudsak likadant ut i dag som det gjorde 2007 när Riksrevisionen senast granskade området. De brister som påpekades då kvarstår i stora drag även i dag, vilket innebär brister i regeringens styrning. Ett tydligt och väl anpassat regelverk är en förutsättning för att uppnå effektivitet i arbetet med informationssäkerhet. Riksrevisionen drar därför slutsatsen att det regelverk som styr myndigheternas arbete med informationssäkerhet bättre kan behöva anpassas till olika typer av statlig verksamhet för att kunna nå önskvärda mål.

Det saknas en samlad avvägning för staten hur mycket resurser som behöver satsas på skyddsåtgärder sett till de risker som finns. Som det nu är finns inte en samlad riskvärdering; i stället råder osäkerhet om hur starkt skyddet är, vilka händelser som ägt rum och hur hoten utvecklas. Om det hade funnits en samlad lägesbild hade det gett förutsättningar för en samlad värdering av riskerna och sannolikheten att hot realiseras.

Detta hade i sin tur kunnat vägas mot hur omfattande stödet behöver vara. Inträffade händelser (se kapitel 2) har visat att kostnaderna kan bli betydande, dels för att hantera händelsen, dels för att ställa till rätta efteråt. Risker för informationssäkerheten kan således potentiellt leda till omfattande skada, inte minst i form av extra kostnader och minskat förtroende för statsförvaltningen. Därför är det angeläget att åtgärder vidtas och prioriteras för att kontrollera dessa risker.

I dag har varje myndighet ett eget ansvar för hela sin verksamhet i såväl normalläge som i krisläge, vilket självfallet är helt nödvändigt för att verksamheten ska kunna bedrivas effektivt. Det är dock sannolikt inte tillräckligt; de flesta myndigheter har svårt att rekrytera och upprätthålla den kompetens som behövs för att möta behoven av säker informationshantering. De av regeringen utpekade stödmyndigheterna har begränsade resurser och saknar möjlighet att lämna operativt stöd till enskilda myndigheter i någon större utsträckning. Det finns alltså behov av ett bättre utbyggt stöd som riktar sig till hela statsförvaltningen, och som kompletterar de enskilda myndigheternas egen kompetens. Om så vore fallet skulle det kunna leda till en bättre säkerhet totalt i statsförvaltningen, samtidigt som den totala kostnaden för informationssäkerhet borde bli väsentligt lägre än om varje myndighet håller sig med specialistkompetens.

Riksrevisionens rekommendationer

Till regeringen

Granskningen har visat ett betydande kunskapsunderskott när det gäller läget för informationssäkerheten i statsförvaltningen. Den tillsyn som sker täcker i stort sett endast den mest skyddsvärda verksamheten – merparten av den civila statsförvaltningen lämnas utan tillsyn. Åtgärder vidtas inte alltid efter genomförda inspektioner. Det saknas också en systematisk och obligatorisk rapportering av incidenter. Allt detta leder till att det blir omöjligt att fånga den verkliga bilden av tillståndet för informationssäkerheten. Därav följer att det inte finns tillräckligt beslutsunderlag för att vidta nödvändiga åtgärder för att möta hoten och riskerna.

För att förbättra statens informationssäkerhet rekommenderar Riksrevisionen därför regeringen följande:

- Utöka tillsynen av informationssäkerheten i den civila statsförvaltningen, så att den omfattar väsentligt mer än endast de allra mest skyddsvärda delarna.
- Låt utreda om regelverket som styr arbetet med informationssäkerheten är ändamålsenligt i sin nuvarande utformning och om ansvar för att utöva tillsyn över informationssäkerheten i den civila statsförvaltningen kan samlas och koordineras på ett bättre sätt än i dag. Dessa brister konstaterade Riksrevisionen redan 2007, och då bristerna fortfarande inte är åtgärdade är det angeläget med en skyndsam hantering.

- Överväg att låta tillsynsmyndigheten få mandat att utfärda sanktioner mot myndigheter som inte vidtar nödvändiga åtgärder efter en tillsyn som visat på brister.
- Inför snarast en obligatorisk incidentrapportering för samtliga myndigheter. Ge en myndighet i uppdrag att hantera denna rapportering.

Det finns ingen samlad central funktion i Regeringskansliet med ansvar för att bereda frågor om informationssäkerhet i statsförvaltningen. I dag hanteras ärenden rörande informationssäkerhet på flera departement beroende på ärendets karaktär (intern styrning och kontroll, förvaltningspolitik, krishantering, infrastruktur, etc.). Riksrevisionen anser att informationssäkerhet är en viktig strategisk fråga för hela statsförvaltningen, att det krävs kraft i styrningen för att skyddet ska kunna höjas till en ändamålsenlig nivå. För att skapa bättre förutsättningar för en effektiv styrning i informationssäkerhet rekommenderar därför Riksrevisionen följande:

- Se till att det finns en funktion och en process i Regeringskansliet med syfte att samlat hantera informationssäkerheten. Denna funktion och process ska kunna bereda alla de ärenden regeringen måste besluta om för att öka informationssäkerheten i statsförvaltningen. Funktionen ska också vara mottagare av MSB:s information om en samlad lägesbild och annan nödvändig information om läget för informationssäkerheten i statsförvaltningen.

Till regeringens stöd- och tillsynsmyndigheter

Riksrevisionen har i denna granskning kunnat visa att de av regeringen utsedda stöd- och tillsynsmyndigheterna inom nuvarande mandat skulle kunna göra mera, både genom att öka kunskapen om säkerhetsläget och att lämna stöd till den övriga statsförvaltningen för att öka skyddet. Detta är naturligtvis en fråga om vad som ska prioriteras såväl inom dessa myndigheter som inom statsförvaltningen som helhet. För att förbättra statens informationssäkerhet rekommenderar Riksrevisionen därför följande:

- MSB bör fortsätta och även intensifiera sitt arbete med att söka skapa en gemensam lägesbild för informationssäkerhet i statsförvaltningen.
- MSB har enligt 9 § andra stycket förordningen (2006:942) om krisberedskap och höjd beredskap möjlighet att begära att flera myndigheter än i dag lämnar en redovisning av sin risk- och sårbarhetsanalys till Regeringskansliet och MSB. MSB bör utnyttja denna möjlighet för att därigenom öka den samlade kunskapen om informationssäkerhetsläget och därigenom kunna bidra till en förbättring.
- MSB bör lämna de myndigheter som inte uppfyller kraven i föreskrifterna om statliga myndigheters informationssäkerhet (MSBFS 2009:10) det stöd som är nödvändigt, så att de uppnår efterlevnad inom rimlig tid.
- Såväl Säkerhetspolisen som FRA genererar viktig kunskap om säkerhetsläget inom den mest skyddsvärda delen av statsförvaltningen. Säkerhetspolisen och FRA bör därför var för sig systematiskt avge aggregerade rapporter om säkerhetsläget till Regeringskansliet och MSB.

1 Inledning

Vi lever i dag i ett samhälle där större mängder information än någonsin tidigare bearbetas, lagras, kommuniceras och mångfaldigas. Det finns stora möjligheter och fördelar med en ökad informationsanvändning. Brister i hanteringen och i säkerheten för informationen riskerar dock att få omfattande konsekvenser, såväl för samhället i stort som för enskilda. Brister kan också leda till ett försämrat förtroende för offentliga och privata aktörer som tillhandahåller viktiga tjänster. Informationssäkerhet omfattar därigenom hela samhället och är en angelägenhet för alla.

1.1 Motiv

Dagens informationshantering präglas i ännu högre grad än tidigare av hög förändringstakt. År 1999 uttryckte regeringen att inriktningen för statsförvaltningen bör vara att all den information individer och företag behöver få från, och lämna till, myndigheter bör finnas tillgänglig elektroniskt.[1] År 2004 stegrades målsättningen genom att målet för varje myndighet ska vara att all information och service som med bibehållen eller ökad effektivitet, såväl ekonomisk som organisatorisk, kan tillhandahållas elektroniskt också ska tillhandahållas så.[2] I propositionen om behandling av personuppgifter inom studiestödsområdet år 2008 uttalar regeringen att den tekniska infrastrukturen för den offentliga förvaltningens kommunikation med medborgarna bör bygga på internet.[3] I den förvaltningspolitiska propositionen 2010 konstaterades slutligen att det finns en stor effektiviseringspotential att ta till vara med hjälp av tekniken och den ska också bidra till att förstärka förvaltningens öppenhet.[4]

Inslaget av IT-stöd i den statliga förvaltningen är utifrån regeringens ovan beskrivna ambition betydande och IT-beroendet har blivit allt större.[5] Merparten av statsförvaltningens verksamheter skulle sannolikt inte fungera tillfredsställande i dag utan IT-stöd.

---

1 Prop. 1999/2000:86, *Ett informationssamhälle för alla*, s 30.

2 Prop. 2004/05:175, *Från IT-politik för samhället till politik för IT-samhället*, s 93.

3 Prop. 2008/09:96, *Behandling av personuppgifter inom studiestödsområdet*, s. 64.

4 Prop. 2009/10:175, *Offentlig förvaltning för demokrati, delaktighet och tillväxt*, s 2.

5 Prop 2013/14:1, UO 6, s. 96.

Om informationssäkerheten brister är risken stor att myndigheterna inte kan fullfölja sina skyldigheter, vilket kan leda till ett minskat förtroende hos allmänheten. Trots den ökade betydelsen av ett fungerande informationssäkerhetsarbete anser såväl nationella som internationella bedömare att utvecklingen av antagonistiska IT-relaterade hot (attacker, IT-brott, spionage, kränkningar, etc.) numera går fortare än samhällets utveckling av skyddsåtgärder. Detta gäller kanske i ännu högre grad icke-antagonistiska hot såsom utvecklingsfel, mjuk- och hårdvarufel, handhavandefel och liknande.[6] Till detta kan läggas att i dagens samhälle har vi mer och mer rationaliserat bort möjligheterna att kunna använda manuella alternativ i händelse av störningar i IT-systemen. Dessutom har vi skapat så komplexa beroenden mellan olika IT-system att det blir svårt att få en korrekt bild av vilka konsekvenser en störning kan leda till.

Riksrevisionen granskade under 2005–2007 elva myndigheter och deras arbete med informationssäkerhet. För sex av dessa myndigheter gjordes en djupare granskning. Denna serie av granskningar avslutades med en granskning som avsåg regeringens styrning av myndigheternas informationssäkerhetsarbete.[7] Riksrevisionens samlade bedömning var att det fanns brister i myndigheternas arbete med informationssäkerhet och att regeringen inte hade följt upp om den interna styrningen och kontrollen av informationssäkerheten varit tillfredsställande. Regeringen hade inte heller tagit tillräckliga initiativ för att förbättra förutsättningarna för statsförvaltningens arbete med informationssäkerhet.

Denna granskning tar sin utgångspunkt i den allt mer ökande användningen av information i samhället och i statsförvaltningen samt utifrån de brister som konstaterades genom Riksrevisionens tidigare granskningar av informationssäkerhet. I Riksrevisionens riskanalys för staten identifieras informationssäkerhet som ett särskilt riskområde.

Regeringen har tillsatt två utredningar som har stor betydelse för informationssäkerheten i samhället. Dessa är översynen av säkerhetsskyddslagen[8] och utredningen som ska ta fram en nationell

---

6 MSB:s trendrapport, FRA:s trendrapport, Säkerhetspolisens och FRA:s yttranden till Riksrevisionen samt Swedish National Audit Office; Auditor General Mr. Claes Norgren, Country Papers on Topic 2 *Cyber Security*.

7 *Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten* (RiR 2005:26), *Granskning av Sjöfartsverkets interna styrning och kontroll av informationssäkerheten* (RiR 2005:27), *Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten* (RiR 2006:24), *Granskning av Migrationsverkets interna styrning och kontroll av informationssäkerheten* (RiR 2006: 25), *Granskning av Lantmäteriverkets interna styrning och kontroll av informationssäkerheten* (RiR 2006:26), *Granskning av Försäkringskassans interna styrning och kontroll av informationssäkerheten 2006* samt *Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen* (RiR 2007:10).

8 En modern säkerhetsskyddslag (dir. 2011:94).

strategi för informationssäkerhet.[9] Översynen av säkerhetsskyddslagen syftar till att bättre anpassa lagstiftningen till vad som krävs för att skydda verksamhet med betydelse för rikets säkerhet och till de krav som ställs på internationellt samarbete. Utredningen om strategi och mål för samhällets informationssäkerhet fokuserar på roller och ansvar på myndighetsnivå, men omfattar inte regeringens styrning av informationssäkerhetsarbetet i statsförvaltningen. Den inriktning och de avgränsningar som görs i Riksrevisionens granskning innebär därmed att den behandlar områden som inte omfattas av de två utredningar som regeringen har tillsatt.

1.2 Syfte och avgränsningar

Denna granskning syftar till att utreda om arbetet med informationssäkerhet i den civila statsförvaltningen är ändamålsenligt utifrån ökande hot och risker. Granskningen omfattar således varken styrningen av eller nivån på informationssäkerhet i samhället i stort. I granskningen har vi inriktat oss på den kunskap och information som samlats in om vilka hot som realiseras samt om hot och risker på en systematisk och övergripande nivå för den civila statsförvaltningen. Granskningen syftar också till att bedöma om regeringen och ansvariga myndigheter för stöd och tillsyn har tillräcklig kunskap om de skyddsåtgärder som har vidtagits av myndigheter inom den civila statsförvaltningen.

Granskningen svarar på två frågor:

- Är regeringens styrning av informationssäkerhet i den civila statsförvaltningen effektiv?
- Har regeringens stöd- och tillsynsmyndigheter vidtagit tillräckliga åtgärder för att informera sig och regeringen om vilka hot som finns mot den civila statsförvaltningen, i vilken omfattning de realiseras och vilka skyddsåtgärder som vidtas?

Granskningen inriktas på den styrning som regeringen och dess stöd- och tillsynsmyndigheter har gett övriga myndigheter i den civila statsförvaltningen genom sitt arbete med informationssäkerhet. Med styrning avses i denna granskning mål och krav, stöd, samordning, tillsyn och kontroll. Av särskilt intresse är den kunskap och information som samlats in som ligger till grund för systematiska och övergripande hotbildsanalyser för den civila statsförvaltningen. Enligt Riksrevisionen är sådana analyser en viktig

[9] Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system (dir. 2013:110).

förutsättning för att informationssäkerhetsarbetet ska kunna anses vara effektivt, eftersom de ger underlag för handlingsplaner och åtgärder.

Hur enskilda myndigheter arbetar med informationssäkerhet ingår inte i granskningen. Inte heller har granskningen sökt bevisa omfattningen av specifika brister i informationssäkerheten. Skälet till denna avgränsning är att problembilden i form av brister i myndigheternas informationssäkerhet var relativt tydlig redan när granskningen inleddes. Dessutom hade en granskning av enskilda myndigheters arbete med informationssäkerhet tagit mycket längre tid att genomföra.

Granskningen avser regeringen (via Försvarsdepartementet, Justitiedepartementet, och Näringsdepartementet) samt stöd- och tillsynsmyndigheterna Myndigheten för samhällsskydd och beredskap (MSB), Försvarets radioanstalt (FRA), Säkerhetspolisen samt Post- och telestyrelsen (PTS). Granskningen avser den civila delen av statsförvaltningen och omfattar därför inte hur Försvarsmakten bedriver arbetet med informationssäkerhet inom sitt verksamhetsområde.

1.3 Utgångspunkter

Den grundläggande utgångspunkten för granskningen är regeringsformen, budgetlagen och myndighetsförordningen samt kravet på att eftersträva hög effektivitet och god hushållning i statlig verksamhet.

När det gäller regeringens styrning utgår granskningen från beprövad erfarenhet för vad som betraktas som effektiv styrning. Det innebär framför allt att det bör ställas krav på en verksamhet, och att dessa krav sedan följs upp för att säkerställa att de fått genomslag. En effektiv styrning kan också innebära att det sätts upp olika mål. Effektiv styrning präglas också av transparens och att ansvar och befogenheter går att urskilja och är symmetriska. En viktig förutsättning för detta är enligt Riksrevisionen att besluten fattas på den nivå där rätt kompetens finns.

Riksrevisionen utgår från att den civila statsförvaltningen bör ha ett ändamålsenligt skydd för sin information. Riksrevisionen anser vidare att ett effektivt informationssäkerhetsarbete i statsförvaltningen kräver

1. grundläggande förutsättningar i form av ett ändamålsenligt regelverk, tydliga roller och ansvar samt krav på och organisering av ett systematiskt och processinriktat arbetssätt
2. systematiska analyser av hot och risker, såväl på organisationsnivå som på ett övergripande plan
3. att ansvariga aktörer vid behov beslutar om nya eller förändrade säkerhetsåtgärder, ser till att åtgärderna införs och slutligen kontrollerar säkerhetsåtgärdernas funktion

4. systematisk och regelbunden uppföljning som ger underlag för förbättringar.

Regeringen ansvarar framför allt för att de grundläggande förutsättningarna finns på plats (punkt 1). Av 1 kap. 6 § regeringsformen framgår att regeringen styr riket. Innebörden av grundlagens bestämmelse är att regeringen har ansvar både för att ta initiativ till förändringar och att verkställa dessa. Regeringen delegerar en del av sitt ansvar till myndigheterna, vilket innebär att regeringen inför riksdagen ytterst är ansvarig för allt som myndigheterna gör. Samtidigt har regeringen inte ett operativt ansvar för vilka åtgärder som vidtas eller inte vidtas.

För att resurserna inom den offentliga sektorn ska utnyttjas på bästa sätt och användas där de bäst behövs krävs dessutom att regeringen följer upp myndigheternas verksamhet och resultat (punkt 4). Detta krävs för att veta om verksamheten är organiserad på ett ändamålsenligt sätt och ger önskvärda effekter.

Informationssäkerhet är en tvärsektoriell fråga och det ställer ökade krav på samverkan mellan departementsområden och myndigheter. Kunskapsuppbyggnad, uppföljning och utvärdering är centrala inslag i styrningen av tvärsektoriella frågor vilket ställer ökade krav på regeringens förmåga att prioritera mellan och samordna olika perspektiv.

Det finns i dag ett omfattande regelverk som behandlar informationssäkerhetsområdet. Reglerna anger bland annat vilka krav som ställs på de statliga myndigheterna och återfinns i lagstiftning och inom ramen för regeringens styrning genom förordningar m.m. Vissa myndigheter har också utfärdat föreskrifter och allmänna råd. Regelverket beskrivs i kapitel 3.

Vad gäller att ta fram risk- och sårbarhetsanalyser, samt vidta åtgärder för att komma till rätta med brister (punkt 2 och 3) är arbetet baserat på *verksamhetsansvaret* och *ansvarsprincipen*. Verksamhetsansvaret innebär att varje enskild myndighet är ansvarig för att den egna informationssäkerheten är tillräcklig utifrån den verksamhet myndigheten bedriver. Ansvarsprincipen innebär att den myndighet som normalt ansvarar för en verksamhet har samma ansvar under en krissituation. Principen innebär också att myndigheten har en skyldighet att verksamheten även ska fungera vid en krissituation. Genom ansvarsprincipen har myndigheterna också en skyldighet att aktivt samverka med andra aktörer för att kunna lösa sina uppgifter vid en krissituation.

För att ytterligare stärka samhällets informationssäkerhet har regeringen gett ett antal myndigheter i uppdrag att utöva tillsyn och ge stöd. Dessa myndigheter kan i denna egenskap få en speciell kunskap och information om informationssäkerhetsarbetet på myndigheterna, samt om risker och sårbarheter i en vidare bemärkelse. De blir därmed viktiga för att kunna bedöma risker och sårbarheter på en systematisk och övergripande nivå.

1.4 Genomförande

I denna granskning har information inhämtats huvudsakligen på tre sätt: dels genom dokumentstudier, dels via intervjuer och skriftliga frågor till berörda myndigheter och Regeringskansliet, dels också genom att Riksrevisionen gett MSB, FRA och Säkerhetspolisen i uppdrag att sammanställa och analysera läget för informationssäkerheten i den civila statsförvaltningen. Den information som på dessa sätt har inhämtats har sedan bearbetats och analyserats och därigenom lett fram till de slutsatser och rekommendationer som redovisas i denna granskningsrapport.

Den första frågan, *om regeringens styrning,* har utretts genom att kartlägga och analysera de uppgifter och krav på åtgärder och redovisningar som ställts på myndigheterna. Styrningen utgår från myndigheternas instruktioner, särskilda förordningar, regleringsbrev och i förekommande fall särskilda regeringsbeslut. För att belysa regeringens styrning har vi också gått igenom samtliga kommittédirektiv, utredningsbetänkanden, departementspromemorior, propositioner (inklusive budgetpropositioner) som skulle kunna haft relevans för det granskade området.

Regeringskansliet har i faktagranskningen av rapporten framfört synpunkten att det är regeringens formella styrning av myndigheternas arbete med informationssäkerhet som har granskats, vilket endast utgör en del av den styrning som sker. Av ett flertal källor framgår att informella kontakter utgörs av kontakter mellan företrädare för myndigheter och Regeringskansliet eller regeringen. Kontakterna syftar oftast till att utbyta information och kunskap, men ibland även till att förtydliga regeringens styrning.[10] I 2010 års förvaltningspolitiska proposition uttalade regeringen även att kontakterna mellan Regeringskansliet och andra myndigheter är viktiga inslag i en effektiv förvaltning. De bör, menar regeringen, syfta till informations- och kunskapsutbyte samt förtydliganden av regeringens styrning.[11] Riksrevisionen ställde mot bakgrund av detta ett antal skriftliga frågor till Regeringskansliet om man har använt sig av informell styrdialog för att få information om myndigheternas informationssäkerhet och om det finns något underlag som visar det. Regeringskansliet ansåg att man inte kunde besvara dessa frågor. Regeringskansliet framhöll att ett relativt stort antal frågor inte kan besvaras av Regeringskansliet, då många av frågorna gäller beslut som har fattats av regeringen, inte Regeringskansliet.

---

[10] Se bland annat Regeringskansliet: Utvecklingsprogrammet för styrning, *Styrning av de statliga myndigheterna och informella kontakter*, PM 2013-09-16 eller SOU 2007:75 *Att styra staten – regeringens styrning av sin förvaltning*.

[11] Prop. 2009/10:175, bet. 2009/10:FiU38, rskr. 2009/10:315.

För regleringsbrev och årsredovisningar har vi gått fem år tillbaka i tiden. För utredningsdirektiv, utredningsbetänkanden, departementspromemorior och propositioner har vi dock ansett oss tvungna att gå tillbaka ända till 2007 för att kunna fånga upp signaler från tiden för krisberedskapsreformen[12] och bildandet av MSB.

Vi har besökt de granskade myndigheterna och intervjuat olika nyckelpersoner. Vi har även skickat myndigheterna skriftliga frågor. Detsamma har skett i fråga om Regeringskansliet.

För att svara på frågan om *stöd- och tillsynsmyndigheterna vidtagit tillräckliga åtgärder för att informera sig och regeringen,* har vi tagit del av de analyser som gjorts på myndigheterna och den rapportering som gjorts till regeringen.

Rapporteringen till regeringen görs på flera olika sätt: genom årsredovisningar, särskilda redovisningar utifrån regeringsuppdrag och i publika rapporter. För att åskådliggöra vad myndigheter i statsförvaltningen rapporterar till regeringen om informationssäkerhet har vi dessutom gått igenom årsredovisningar från ett urval myndigheter.

Vi har också gett stöd- och tillsynsmyndigheterna samt Datainspektionen olika redovisningsuppdrag:

- MSB har gått igenom 23 myndigheters risk- och sårbarhetsanalyser från 2013 för att undersöka hur dessa hanteras. Detta redovisas i avsnitt 4.1.1.
- FRA har redovisat hur dess IT-säkerhetsanalyser och penetrationstester går till, och vad de visar om läget på berörda myndigheter. Detta redovisas i avsnitt 4.2.
- Säkerhetspolisen har redovisat sin syn på läget för informationssäkerhet på de myndigheter och bolag som är mest skyddsvärda. Underlaget för denna redovisning är de 18 tillsyner Säkerhetspolisen gjort under de senaste nio åren. Detta redovisas i avsnitt 4.3.
- Datainspektionen har redovisat hur inspektionens verksamhet går till. Detta redovisas i avsnitt 4.4.

Vi bedömer att dessa redovisningar ger ett tillräckligt underlag för att kunna svara på de båda revisionsfrågorna utifrån de ovan beskrivna förutsättningarna för ett effektivt informationssäkerhetsarbete.

[12] Prop. 2007/08:92, *Stärkt krisberedskap – för säkerhets skull*.

1.5 Rapportens disposition

Granskningsrapporten är disponerad enligt följande.

- I kapitel två ges några exempel ur verkligheten som får belysa den operativa kontexten och vad som händer när informationssäkerheten brister.
- I kapitel tre belyser vi regelstrukturen och vilka krav som gäller för myndigheternas informationssäkerhet. Kapitlet behandlar också de olika stöd- och tillsynsmyndigheterna på området, vilket ansvar de har och hur verksamheten ser ut.
- Fjärde kapitlet handlar om vilken kunskap stöd- och tillsynsmyndigheterna har om informationssäkerheten i den civila statsförvaltningen och vad de har rapporterat till regeringen
- Femte kapitlet redogör för vilka åtgärder regeringen vidtagit i sin styrning av informationssäkerheten.
- I det slutliga sjätte kapitlet drar Riksrevisionen sina slutsatser utifrån de iakttagelser som gjorts och lämnar rekommendationer till regeringen och de granskade myndigheterna.

2 Vad händer egentligen när informationssäkerheten brister?

Att myndigheterna bör eftersträva god informationssäkerhet handlar inte bara om att följa de regler som finns för sakens skull. I dagens samhälle är tillgång till tillförlitlig information, ofta i realtid, en kritisk resurs.

En stor del av den information som skapas och lagras i samhället är viktig och samtidigt känslig. Personuppgifter kan innehålla integritetskänslig information, vilket därför omgärdas av särskild lagstiftning. Det handlar exempelvis om informationen i patientjournaler, brottsutredningar eller underrättelseverksamhet. Vissa system i samhället bygger på IT för att kunna fungera. Andra exempel på känslig information rör tekniska produkter, affärsförhållanden och förhållanden som rör andra stater. Är informationen förlorad, stulen, manipulerad eller spridd till obehöriga kan det få allvarliga följder.

Många system i samhället är som tidigare nämnts beroende av informationsteknologi för att kunna fungera. Dessutom tillkommer att beroenden och kopplingar mellan olika tekniska system är en sårbarhetsfaktor i sig genom att störningar kan få konsekvenser som både är svåra att förutse och hantera.

Vad som utgör ett hot eller en risk varierar från stater och statsunderstödda aktörer, terrorister, organiserad brottslighet till fel och störningar som inte orsakas av antagonister utan beror på mjuk- eller hårdvarufel, processbrister, bristande kvalitetskontroll, slarv, missbedömningar eller rena olycksfall. Vilka som drabbas och på vilket sätt har en stor spännvidd i form av globala effekter vid exempelvis attacker mot finansiella system, nationella effekter i form av störningar i el- eller vattenförsörjning eller på individnivå som i exemplet med Tieto nedan där en kommun inte hade möjlighet att utfärda parkeringstillstånd åt funktionshindrade.

Regeringen ser IT som ett centralt verktyg för att åstadkomma verksamhetsutveckling i statsförvaltningen. Eftersom mer och mer av myndigheternas verksamhet digitaliseras och kopplas samman ökar också risken för att verksamheten inte kan bedrivas på ett tillfredsställande sätt om inte IT-verksamheten fungerar.

Följande avsnitt avser att illustrera de omfattande konsekvenser som brister i informationssäkerhet kan leda till. Redovisningen beskriver såväl tekniska fel som organiserad brottslighets stöld av kontokortsinformation, antagonistiska attacker mot länder eller verksamheter, dataintrång mot myndigheter och industrispionage.

Riktade cyberattacker

Dagens IT-angrepp kommer från resursstarka och kunniga aktörer. Dessa har uttalade mål och syften med sina angrepp, till exempel underrättelseinhämtning, ekonomisk brottslighet, industrispionage och olika former av påverkan (sabotage och utslagning av hela samhällsfunktioner). Angreppen blir alltmer sofistikerade och riktade och samhällets sårbarheter utnyttjas på ett systematiskt sätt av antagonistiska aktörer.[13]

Under 2010 upptäcktes vad som kallats det värsta dataviruset någonsin och det fick namnet Stuxnet. Viruset var en mask, det vill säga att det sprider sig själv utan hjälp av oförsiktiga användare. Viruset utgjorde enligt bedömare en riktad attack mot styrsystemen i en iransk kärnkraftsanläggning.[14] Angreppet skedde mot så kallade SCADA-system[15] i kärnkraftverket som styrde generatorer i de centrifuger som används för att anrika uran. Liknande system används även för att styra kylningen av reaktorstavar. Viruset och de metoder som användes var enligt experter mycket avancerade och innehöll exempelvis funktioner som förfalskade indata för övervakningssystemet för att undgå upptäckt.[16]

Angrepp mot industriella informations- och styrsystem underlättas i dag väsentligt genom den ökande uppkopplingen av systemen mot internet. Sådana system används bland annat för att styra eldistribution, vattenförsörjning, trafikljus och sjukhusutrustning, och antagonistiska angrepp mot sådana system kan därför ställa till med mycket stor skada.[17]

Ett exempel på manipulation av industriella informations- och styrsystem i Sverige är attacken mot det kommunala bostadsbolaget Platens fastigheter i Motala. Någon hackade sig in den datacentral som reglerar fjärrvärmen till bolagets fastigheter och stängde av värmen för 700 lägenheter samt ett äldreboende.[18]

---

13 FRA: *Trender och utmaningar idag och imorgon*.

14 MSB: *Trendrapport – samhällets informationssäkerhet 2012*, s. 31.

15 Supervisory Control and Data Acquisition.

16 http://techworld.idg.se/2.2524/1.356435/sasaboterade-stuxnet-irans-karnkraftverk.

17 MSB: *Trendrapport – samhällets informationssäkerhet 2012*, s. 55.

18 http://sverigesradio.se/sida/artikel.aspx?programid=160&artikel=4239787.

Ett annat exempel är Finland som utsattes för dataspionage där ryska och kinesiska underrättelsetjänster misstänks för att under en period av fyra år ha utövat verksamhet mot utrikesministeriet.[19]

Ett tredje exempel är cyberattacken mot Estland. Från slutet av april till mitten av maj 2007 genomfördes omfattande angrepp mot den estniska delen av internet. Händelsen hade av allt att döma ett direkt samband med oroligheter i Estland i samband med förflyttningen av ett ryskt krigsminnesmärke. Angreppen följde ett mönster där enkla åtkomstattacker efterhand följdes av underrättelseinhämtning och fokuserade, välkoordinerade attacker som involverade mycket stora botnät[20]. Under denna tid fungerade inte nätet normalt. Det blev svårt att nå myndigheter och massmedia via internet, nätbankerna fick under en period avbryta sin verksamhet och under en period var det svårt för flera aktörer att kommunicera med omvärlden via internet.

Ekonomisk brottslighet, integritetsförluster och industrispionage

Ett exempel på ekonomisk brottslighet som nämns i tidningen Ny Teknik är en cyberattack där förövarna stal 300 miljoner kronor från privatpersoner. Tjuvarna stal kontouppgifter genom att hacka sig in i IT-systemet hos ett indiskt kreditkortsföretag. De höjde uttagsgränserna på krediter och skickade sedan kontoinformation till kriminella gäng som de samarbetade med. Gängmedlemmar tog sedan ut pengarna via automater.[21]

Ett annat exempel är attacken mot IT-företaget Logica. Förövaren lyckades bryta sig in i Logicas servrar där flera myndigheter förvarade mängder med känsliga uppgifter och kunde lägga beslag på känsliga personuppgifter från Kronofogden, Skatteverket och Polisen.[22]

Ett tredje exempel är uppgifter om kinesiska hackargrupper som slår mot teknikföretag. Tidningen Ny Teknik refererar i en artikel till en rapport av ett amerikanskt säkerhetsföretag som hävdar att en kinesisk grupp är ansvarig för en stor mängd attacker mot olika teknikföretag. Gruppen uppges bestå av hundratals, kanske till och med flera tusen personer. De kinesiska hackarnas främsta intresse är enligt tidningen tekniska verksamheter, exempelvis IT, rymd, satellit och telekom. Omfattningen av de attacker säkerhetsföretaget kartlagt sedan 2006 uppgår till 141 drabbade verksamheter, varav 20 större industriföretag. I artikeln uppger tidningen också att svenska forskare vid KTH följer de kinesiska angreppen: ”’Vi har ett projekt sedan 2005 som

---

[19] Svenska Dagbladet den 31 oktober 2013.

[20] Se bilaga 1 för förklaring av *botnät*.

[21] Ny teknik den 10 maj 2013.

[22] Dagens Nyheter den 5 december 2013.

följer deras organisation, utbildning, träning och de verktyg de använder. Det mest imponerade de gjort var när de hackade sig in på den franska militära underrättelsetjänstens huvuddator i Paris och speglade deras hårddiskar. Sedan ett flertal år hackar de bland annat amerikanska företags- och myndighetsservrar – varje vecka. Det är en del av deras träning', säger Lars-Olov Strömberg, lärare på KTH i Stockholm och föreståndare för universitetets IT-forensiska labb."[23]

Tekniska fel[24]

Fredagen den 25 november 2011 drabbades IT-driftleverantören Tieto av ett tekniskt fel, vilket kom att få direkta konsekvenser för cirka 50 av företagets kunder inom såväl privat som offentlig sektor. Konsekvenserna varierade kraftigt. Vissa kunder kom lindrigt undan, med enstaka funktioner utslagna under några dagar. De värst drabbade saknade i princip möjlighet att använda sina IT-lösningar under flera veckor.

Det tekniska felet hos Tieto tog två dygn att åtgärda. Kundernas data kunde emellertid inte återställas enbart genom att byta ut en komponent i den tekniska utrustningen. Maskinvarufelet utlöste nämligen en kedja av incidenter som resulterade i en komplex och tidsödande återställningsprocess. Därför dröjde det betydligt längre innan Tieto kunde återställa kundernas lagrade data till samma skick som innan maskinvarufelet inträffade.

Åtskilliga av Tietos kunder fick ganska omgående allvarliga problem, eftersom verksamheten hos dem pågår ständigt. Ett exempel var att 350 av Apoteket AB:s apotek över hela landet plötsligt inte fick kontakt med sina IT-system och därför inte kunde lämna ut receptbelagda mediciner enligt normala rutiner.

En närliggande verksamhet, Apotekens Service AB, drabbas också av driftstoppet hos Tieto. Företagets externa webbplats låg nere under cirka tio dagar. Webbplatsen är en viktig informationskälla för vård- och omsorgssektorn i Sverige. Den innehåller bland annat läkemedelsinformation, kontaktuppgifter och information om driftstörningar.

Även det statligt ägda bostadsfinansieringsföretaget SBAB drabbades av driftstoppet och händelsen var kritisk redan på fredagen, som råkade infalla den 25:e, det datum i månaden då många får ut sin lön. Inom bank- och finanssektorn betraktas detta kalenderdatum av tradition som en extra känslig tidpunkt, då störningar kan få stora konsekvenser. Företaget lyckades emellertid begränsa skadan och kundernas tillgång till likvida medel påverkades inte i

---

[23] Ny Teknik den 22 februari 2013.

[24] Hela detta avsnitt bygger på MSB:s rapport *Reflektioner kring samhällets skydd och beredskap vid allvarliga IT-incidenter. En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011.*

någon mer betydande omfattning. Däremot fick driftstörningen stor effekt på SBAB:s låneverksamhet, som inte var i normal drift förrän påföljande onsdag.

Hos den statliga myndigheten Vetenskapsrådet tvärstannade den normala verksamheten då myndigheten drabbades av ett nästan totalt driftstopp för IT-stödet. Ekonomisystemet fungerade inte, e-posten var borta, myndighetens webbtjänster gick inte att nå. Ansökningssystemet, det ärendehanteringssystem som hanterar forskningsansökningar och granskningar, var inte heller tillgängligt. För att överhuvudtaget kunna kommunicera med omvärlden fick Vetenskapsrådet inrätta en tillfällig blogg på internet.

Stora delar av den kommunala administrationen i Sollentuna berördes när handläggarna inte längre kunde arbeta med sina ärenden. Vid sidan av utbetalningsproblemen kunde socialkontoret inte nå sin journalföring, och alla ansökningar om ekonomiskt bistånd fick därför hanteras manuellt. Dokument och datafiler i administrationen gick inte att nå, vilket skapade förseningar i handläggning av bygglov, ärenden hos överförmyndaren, handläggning av livsmedelsärenden och miljö- och hälsoskyddsärenden. Protokoll från kommunfullmäktige och kommunstyrelse försenades, det gick inte att utfärda parkeringstillstånd till funktionshindrade, månadsbokslut försenades och idrottsföreningar kunde inte boka lokaler. Dessutom innebar driftstoppet att inpasseringen till lokaler som ägs av kommunen fick skötas manuellt.

Hos Svensk Bilprovning påverkade driftstoppet den rikstäckande verksamheten under hela den påföljande arbetsveckan. En konsekvens var att den automatiska vidarerapportering av godkända kontrollbesiktningar som normalt sker till Transportstyrelsen inte längre fungerade. Trivialt, kan tyckas, men detta fel fick snabbt till följd att många fordon automatiskt blev belagda med körförbud. Först efter tio dygn rapporterade Bilprovningen att bolagets kontrollstationer åter fått fungerande IT-stöd och att kontrollbesiktningar och bokning fungerade som vanligt igen.

För Nacka kommun dröjde det fem dagar innan webbplatsen åter var i drift. Under tiden kommunicerade kommunen med omvärlden på andra sätt. En vecka efter driftstoppet var flera centrala IT-system i Nacka fortfarande inte i drift. Handlingar och protokoll var inte tillgängliga, funktioner för kommunal felhantering fungerade inte och inloggning med e-legitimation var inte i drift. Först i mitten av december kunde Nacka kommun meddela att verksamheten till 95 procent kunnat återgå till det normala. Först den 4 januari fungerade alla datasystem igen. Tre månader efter händelsen pågick fortfarande arbete med att hinna ikapp. Kostnaden till följd av haveriet uppskattades till minst 7,5 miljoner kronor.

Sammanfattande iakttagelser

De här relaterade händelserna har ägt rum. Konsekvenserna har varit allvarliga. Liknande saker kommer att hända igen – var, när och i vilken omfattning vet ingen. Detta understryker vikten av en god kännedom om beredskapen för att förebygga och hantera liknande och andra händelser. Ett riskbaserat tillvägagångssätt i arbetet med informationssäkerheten är en förutsättning för att på ett samlat sätt kunna värdera sannolikheten för att olika händelser ska inträffa och vilka konsekvenser som kan bli följden. Det finns flera riskområden inom statsförvaltningen när det gäller informationssäkerheten, såsom exempelvis kompetensbrist, upphandling, tillsyn/uppföljning/återrapportering samt styrning/omreglering/samordning.

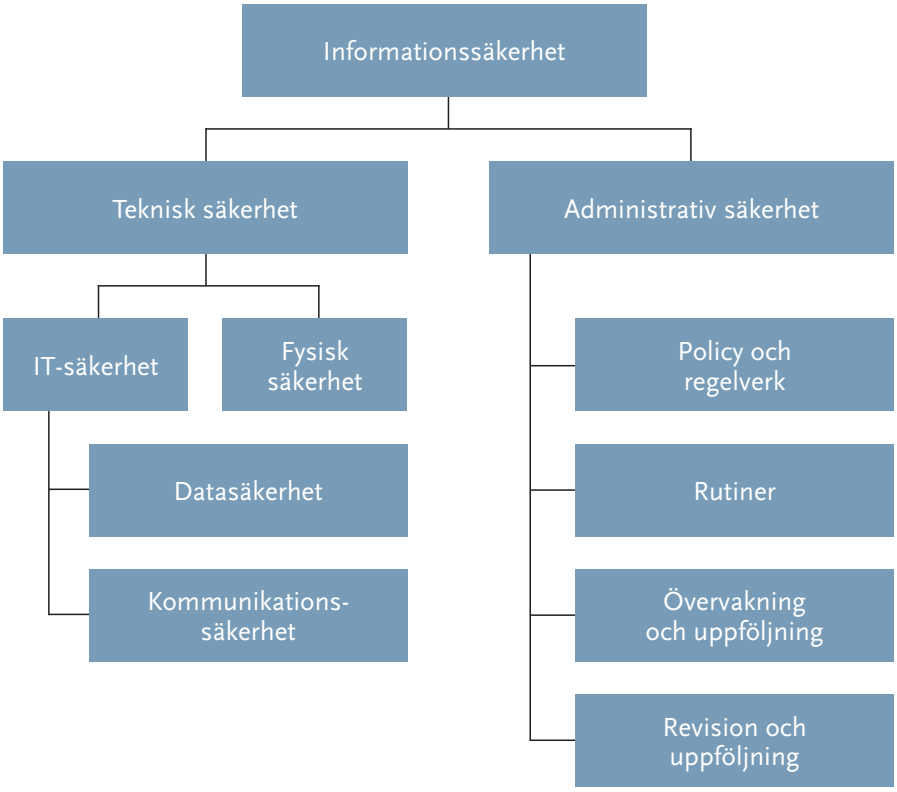
3 Reglering, stöd och tillsyn

I detta kapitel beskriver vi den huvudsakliga rättsliga regleringen som rör informationssäkerheten i statsförvaltningen och vad informationssäkerhet innebär.[25] Här behandlas regeringens styrning och utgångspunkten för grundläggande förutsättningar i form av kravställning gentemot myndigheterna genom lagar, förordningar och föreskrifter. Kapitlet behandlar också regeringens styrning och utgångspunkten för grundläggande förutsättningar i form av organisering genom en beskrivning av vilka stöd- och tillsynsmyndigheter som finns och vad dessa ska och kan göra. Dessa myndigheter är Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap (MSB) och Försvarets radioanstalt (FRA). Kapitlet omfattar även reglerna om personuppgiftsbehandling och arkivering samt myndigheterna Datainspektionen, Post- och telestyrelsen och Riksarkivet, eftersom dessa regler och myndigheters uppdrag delvis berör frågan om informationssäkerhet.

Med informationssäkerhet avser Riksrevisionen säkerhet för informationstillgångar. Säkerheten syftar till att upprätthålla förmågan till *konfidentialitet, riktighet* och *tillgänglighet*. Informationssäkerhet är ett begrepp som omfattar säkerhet för information oavsett dess form, alltså inte endast IT-säkerhet. Enligt Swedish Standards Institute (SIS) kan informationssäkerhet illustreras på följande sätt.

[25] Utöver de lagar, förordningar och föreskrifter som behandlas i kapitlet finns även regler som delvis har bäring på informationssäkerhet. Det rör sig om offentlighets- och sekretesslagen (2009:400), förordningen (2007:603) om intern styrning och kontroll samt ett antal olika registerförfattningar. Offentlighets- och sekretesslagen ställer krav på att vissa uppgifter inte får röjas eller lämnas ut, vilket också innebär att uppgifterna ska skyddas. Lagen ställer dock inte upp några krav för hur detta ska ske. Förordningen om intern styrning och kontroll avser den process som syftar till att myndigheten med rimlig säkerhet fullgör de krav som framgår av 3 § myndighetsförordningen (2007:515). Det är krav på att verksamheten bedrivs effektivt, enligt gällande rätt och de förpliktelser som följer av Sveriges medlemskap i Europeiska unionen samt att verksamheten redovisas på ett tillförlitligt och rättvisande sätt. Förordningen ställer därmed krav på att myndigheterna har en process för styrning och kontroll som säkerställer att kraven på ledningssystem för informationssäkerhet (LIS) uppfylls. Förordningen ställer dock inte i sig några krav på informationssäkerhet.

Figur 2.1 Beskrivning av begreppet informationssäkerhet

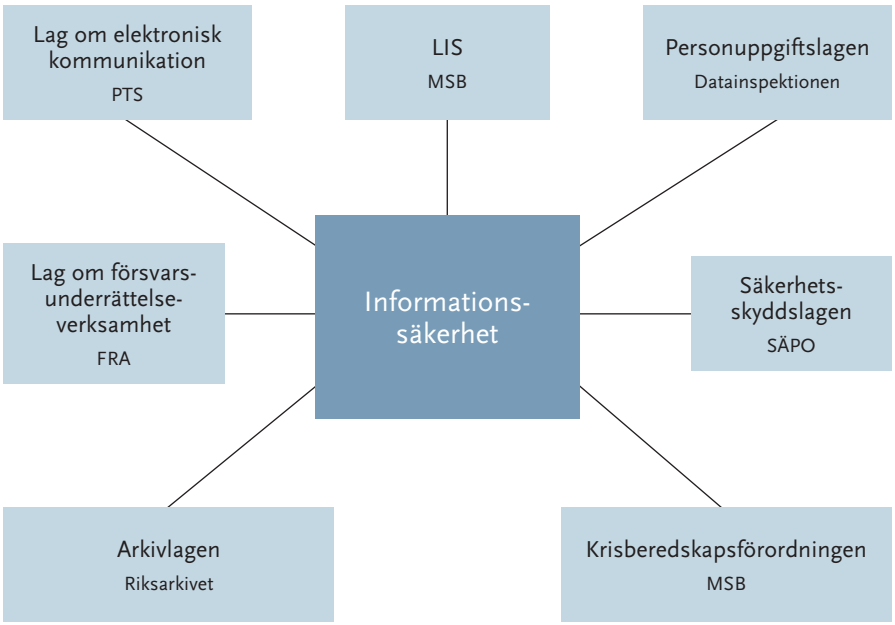


Källa: SIS HB 550 – Terminologi för informationssäkerhet, utgåva 3.

Riksrevisionens granskning omfattar utifrån definitionen ovan såväl teknisk säkerhet som administrativ säkerhet. Området informationssäkerhet är ett komplext och omfattande område och rapporten innehåller därmed en del begrepp som kanske inte är helt självklara för alla. I bilaga 1 finns därför en lista med förklaringar till vissa centrala begrepp.

Figuren nedan visar de regelverk och aktörer som är relevanta för informationssäkerheten i den civila delen av statsförvaltningen.

Figur 2.2 Ett urval av centrala regelverk och aktörer som styr informationssäkerhet i den civila statsförvaltningen



3.1 Säkerhetsskydd

3.1.1 Vilka krav ställs på säkerhetsskydd

Säkerhetsskyddslagen (1996:627), säkerhetsskyddsförordningen (1996:633) samt Rikspolisstyrelsens föreskrifter (RPSFS 2010:3) är de regelverk som ställer krav på att vissa verksamheter ska ha ett tillfredsställande säkerhetsskydd. Såväl offentliga som privata verksamheter som är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism omfattas av lagen. Med säkerhetsskydd avses skydd mot brott som kan hota rikets säkerhet, skydd av hemliga uppgifter som rör rikets säkerhet och skydd mot terrorism. Säkerhetsskyddet ska förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Det ska också förhindra att obehöriga får tillträde till platser där de kan få tillgång till uppgifter som omfattas av sekretess som rör rikets säkerhet eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning). Slutligen ska säkerhetsskyddet även förhindra att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning).

Säkerhetsskydd innebär således att myndigheter och andra som säkerhetsskyddslagstiftningen omfattar ska vidta förebyggande åtgärder för att skydda mot brott som kan hota rikets säkerhet, såsom spionerі och sabotage. Hemliga uppgifter som rör rikets säkerhet ska även de skyddas. Säkerhetsskyddet omfattar också skydd mot terrorism.

Verksamhet som omfattas av säkerhetsskyddslagstiftningen ska ha det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. En säkerhetsanalys utgör grunden för ett väl anpassat säkerhetsskydd och är dels en undersökning som syftar till att kartlägga vad som är skyddsvärt i en verksamhet, dels en handling som dokumenterar de resonemang som leder fram till vad som är skyddsvärt. Undersökningen ska också relatera det skyddsvärda till de hot som verksamheten kan utsättas för och de säkerhetssårbarheter som verksamheten kan vara behäftad med. I förlängningen syftar säkerhetsanalysen till att ta fram ett beslutsunderlag för säkerhetsskyddsåtgärder samt att skapa spårbarhet för detta underlag.[26]

3.1.2 Säkerhetspolisens tillsyn

Av säkerhetsskyddslagen (1996:627) följer att verksamheter som har betydelse för rikets säkerhet eller behöver skyddas mot terrorism ska utforma ett skydd för verksamheten i enlighet med kraven i lagen, det så kallade säkerhetsskyddet. Säkerhetspolisen är enligt 39 § säkerhetsskyddsförordningen (1996:633) den myndighet som har ansvar för att utöva tillsyn av säkerhetsskyddet i de civila delarna av statsförvaltningen. Säkerhetspolisen samverkar också sedan 2012 med den militära underrättelse- och säkerhetstjänsten i Försvarsmakten (MUST) och FRA när det gäller att skydda samhället mot allvarliga IT-hot.

Säkerhetspolisen har av regeringen fått ansvaret att prioritera sina insatser utifrån en helhetsbedömning av skyddsbehovet, framför allt när det gäller IT-säkerhet och skydd mot elektroniska angrepp. Säkerhetspolisen har därför inriktat sin tillsyn mot den mest skyddsvärda verksamheten i statsförvaltningen. Denna prioritering medför att tillsynen främst inriktas på myndigheter med sådan verksamhet där konsekvenserna av ett angrepp skulle bli så allvarliga att rikets säkerhet hotas. Säkerhetspolisens tillsyn kompletteras med rådgivning till de granskade myndigheterna.

Vid en tillsyn kontrollerar Säkerhetspolisen att den granskade myndigheten följer säkerhetsskyddslagstiftningen och vilka säkerhetsskyddsåtgärder som den granskade myndigheten har vidtagit. Säkerhetspolisen granskar alltid den säkerhetsanalys och de styrande dokument som ska finnas. Bedömningarna i säkerhetsanalysen ska motivera vidtagna skyddsåtgärder och säkerställa en samverkande helhet. Därefter granskas informationssäkerhet, IT-säkerhet (penetrationstester) och fysiskt skydd kopplat till de skyddsvärden som säkerhetsanalysen pekat ut. Säkerhetspolisen besöker myndigheten och intervjuar verksamhetskunniga och säkerhetsansvariga. Efter avslutad tillsyn lämnar Säkerhetspolisen en tillsynsrapport till den granskade myndigheten med förslag på åtgärder för att förbättra säkerhetsskyddet samt erbjuder stöd

[26] Säkerhetspolisen: *Säkerhetsskydd – en vägledning*, s. 12.

i form av rådgivning efter tillsynen. Tillsynsrapporten överlämnas även för kännedom till den granskade myndighetens huvudman i Regeringskansliet. En tillsyn tar relativt mycket resurser i anspråk och brukar ta mellan sex och åtta månader att genomföra. Säkerhetspolisen genomför en eller två tillsyner per år.

3.2 Systematiskt informationssäkerhetsarbete och stödfunktioner för samhällets informationssäkerhet

3.2.1 Vilka krav ställs på systematiskt informationssäkerhetsarbete?

Ledningssystem för informationssäkerhet (LIS) är ett sätt att styra en verksamhets informationssäkerhet på ett systematiskt sätt. Dagens LIS har sin bakgrund i en brittisk standard som utkom 1995 och som sedermera blev svensk och internationell standard i form av SS-ISO/IEC 17799 *Ledningssystem för informationssäkerhet* från 1999.[27] Verket för förvaltningsutveckling (Verva) utfärdade föreskrifter som trädde i kraft 2008 med krav på att myndigheter under regeringen skulle tillämpa ett ledningssystem för informationssäkerhet.[28]

Av 30 a § krisberedskapsförordningen framgår att varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Därvid ska behovet av säkra ledningssystem särskilt beaktas. Även om kravet finns i krisberedskapsförordningen avser det inte endast krisberedskapsarbete, utan gäller generellt för informationssäkerhetsarbete i statsförvaltningen. MSB har även enligt 34 § krisberedskapsförordningen rätt att utfärda verkställighetsföreskrifter för det som föreskrivs i 30 a §.

MSB:S verkställighetsföreskrifter om ledningssystem för informationssäkerhet (MSBFS 2009:10) trädde i kraft den 1 februari 2010, och utformades i stor utsträckning med Vervas föreskrifter som förlaga.

MSB:s föreskrifter ska tillämpas av i stort sett alla myndigheter under regeringen. Föreskrifterna är kortfattade och omfattar endast sex paragrafer, men kompletteras med allmänna råd. Av föreskrifterna följer att myndigheternas arbete ska bedrivas enligt svensk standard i form av ISO 27001 och 27002, vilket innebär mer detaljerade krav att förhålla sig till. Av 4 § framgår att myndigheterna ska

---

[27] Statskontoret 2003:23: *Ledningssystem för informationssäkerhet vid 24-timmarsmyndigheter, Vägledning och mallregelverk*, s. 11 f.

[28] Vervas föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte (VERVAFS 2007:2).

- upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet
- utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet
- klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet
- utifrån risk- och sårbarhetsanalyser och inträffade incidenter avgöra hur risker ska hanteras, samt besluta om åtgärder för myndighetens informationssäkerhet
- dokumentera granskningar och säkerhetsåtgärder av större betydelse som vidtagits.

Av 5 § följer att myndighetens ledning löpande ska informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet på myndigheten.[29]

3.2.2 MSB:s stödjande arbete

Utöver ansvaret inom området samhällets krisberedskap har MSB även ett särskilt uppdrag inom området samhällets informationssäkerhet. Uppdraget innebär att MSB ska göra följande:

- Stödja och samordna arbetet med samhällets informationssäkerhet.
- Analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer.
- Rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder inom olika nivåer och områden i samhället.[30]

Utöver ovan nämnda ska MSB även svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera IT-incidenter. MSB ska i detta arbete sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade. Funktionen ska även vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa. Den funktion inom MSB som i huvudsak hanterar frågan har namnet CERT-SE (Computer Emergency Response Team). Det finns i dag ingen skyldighet för myndigheter

[29] Som stöd för myndigheternas arbete med informationssäkerhet i enlighet med föreskrifterna har MSB distribuerat standarder för informationssäkerhet till berörda myndigheter. MSB har även upprättat en särskild webbplats – informationssäkerhet.se – med råd och stöd för att införa LIS.

[30] 11 a § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

att rapportera IT-incidenter, och MSB är därför beroende av att myndigheter, privata aktörer, med flera lämnar uppgifterna frivilligt.

MSB bedriver sitt stödjande arbete med samhällets informationssäkerhet inom en rad områden. En del utgörs av strategi- och utredningsarbete som innefattar regeringsuppdrag, nationell strategi och handlingsplan, nationell plan för hantering av allvarliga IT-relaterade kriser, m.m. MSB:s roll kopplad till det systematiska informationssäkerhetsarbetet innefattar bland annat utfärdandet av föreskrifter och metodutveckling (risk- och sårbarhetsanalyser, kontinuitetshantering, informationsklassning, m.m.). MSB arbetar också mycket med forskning, utveckling och informations- och cybersäkerhetsövningar.

MSB har fått i uppdrag av regeringenatt kontinuerligt redovisa en lägesbedömning på informationssäkerhetsområdet avseende hot, sårbarheter och risker på samhällsnivå.[31] Detta görs på flera sätt, till exempel genom den rapportering om samhällets informationssäkerhet som sker i MSB:s risk- och sårbarhetsanalys, MSB:s årsredovisning samt den nationella risk- och förmågebedömningen (NRFB). MSB tar också fram händelserelaterade rapporter, till exempel om Tietoincidenten.

Eftersom MSB inte har något mandat att bedriva tillsyn[32] över myndigheternas informationssäkerhet bygger informationsinsamling på deltagandet i ett antal olika nätverk och samverkansgrupper.[33] Den samverkan som sker i olika fora, internationell samverkan och frivillig incidentrapportering ger MSB möjlighet att inhämta kunskap om vad som sker ute i samhället, och informationen ger en grund för den avrapportering som MSB gör på olika sätt.[34] Deltagandet i nationella samverkansfora präglas av att diskussionerna, inom ramen för offentlighets- och sekretesslagstiftningen, förs i förtroende med utgångspunkt i *The Chatham House Rules*. Det innebär att deltagarna kan använda sig av den information som framkommer i diskussioner, men inte får avslöja från vem informationen härrör.[35] Deltagandet i internationella fora kan ske på olika sätt, både enligt *Chatham House Rules* och genom formella avtal mellan länder.

---

31 Regeringens skrivelse (2009/10:124) *Samhällets krisberedskap – stärkt samverkan för ökad säkerhet*, s.71.

32 Skriftligt yttrande från Försvarsdepartementet, dnr Fö2014/172/SSK.

33 MSB deltar i följande grupper: Samverkansgruppen för informationssäkerhet (SAMFI), Informationssäkerhetsrådet, Grupp för informationsdelning med inriktning på vårdsektorn, Grupp för informationsdelning med inriktning på industriella informations- och styrsystem (SCADA), Grupp för informationsdelning med inriktning på finanssektorn, Nationella telesamverkansgruppen, Grupp för informationsdelning inom underrättelse- och säkerhetstjänsterna, Nationellt CERT-forum, Forskningsnätverket (SWITS), Kommunnätverket (KIS), Landstingsnätverket (NIS) samt Myndighetsnätverket (SNITS).

34 Intervju på MSB 2014-01-15.

35 http://www.chathamhouse.org/about/chatham-house-rule.

3.2.3 FRA:s stödjande arbete

Av FRA:s instruktion[36] framgår att FRA ska ha hög teknisk kompetens inom informationssäkerhetsområdet och att FRA ska stödja statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig ur sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.

FRA ska 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 eller ge annat tekniskt stöd. FRA ansvarar även för att tilldela civila myndigheter och samhällsviktiga företag av Försvarsmakten godkänd signalskyddsutrustning som gör det möjligt för dem att elektroniskt utbyta sekretessbelagd information med varandra.[37] Den tekniska rådgivning som FRA utför utgörs exempelvis av rådgivning om säkerhetsåtgärder, stöd i kravställning vid upphandling av IT-drift eller hjälp med utformning av tekniska och administrativa rutiner för säkerhetsarbete. FRA:s primära roll är dock att vara oberoende granskare och tekniskt sakkunnig expert, inte att leverera färdiga lösningar. FRA kan också bistå med rådgivning när en statlig myndighet eller statligt ägt bolag inte klarar av att hantera en IT-incident, till exempel ett dataintrång i särskilt känsliga system med allvarliga konsekvenser. Det rör sig både om åtgärdsförslag och praktisk hjälp med att hantera och utreda incidenten.

3.3 Krisberedskap

3.3.1 Vilka krav ställs på krisberedskap

Förordningen (2006:942) om krisberedskap och höjd beredskap (krisberedskapsförordningen) syftar till att statliga myndigheter genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och höjd beredskap. Förordningen innehåller flera bestämmelser med bäring på informationssäkerhetsarbetet hos myndigheter.

Enligt 9 § krisberedskapsförordningen ska varje myndighet årligen analysera om det finns sådana sårbarheter eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. MSB har enligt 34 § rätt att utfärda verkställighetsföreskrifter om hur dessa analyser ska redovisas. MSB har

[36] Förordning (2007:937) med instruktion för Försvarets radioanstalt.

[37] Enligt 31 § krisberedskapsförordningen ska Regeringskansliet, Kustbevakningen, MSB och FRA ha säkra kryptografiska funktioner, som tilldelas av FRA. MSB beslutar om vilka övriga myndigheter, kommuner, landsting, företag och organisationer som ska ha sådana funktioner som tilldelas av FRA.

dessutom enligt 31 och 33 §§ ett ansvar för civila myndigheters signalskydd. MSB beslutar vilka civila myndigheter som ska ha säkra kryptografiska funktioner.

Av MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2009:10) följer att de myndigheter som har ett särskilt ansvar för krisberedskap ska redovisa sin förmåga kopplat till informationssäkerhetsfrågor med hjälp av ett antal indikatorer. Redovisningen ska ske i form av en bedömning av om det finns tillräcklig förmåga hos myndigheten att upprätthålla informationstillgångarnas konfidentialitet, riktighet och tillgänglighet. De myndigheter som bedriver samhällsviktig verksamhet ska dessutom bedöma förmågan till redundans och robusthet inom myndigheten och dess ansvarsområdes kommunikationssystem (IT, tele och radio).[38]

3.3.2 MSB ansvarar på ett övergripande plan

Av MSB:s instruktion framgår att myndigheten ansvarar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret.[39] MSB:s arbete är inte begränsat till en viss grupp av aktörer eller organisationer utan uppdraget sträcker sig över såväl statlig och kommunal som privat verksamhet. Den del av myndighetens ansvar inom krisberedskapsområdet som har betydelse för de frågor som behandlas i granskningen är MSB:s föreskriftsrätt för kommuners, landstings och statliga myndigheters risk- och sårbarhetsanalyser. Utöver att utfärda föreskrifter har MSB även tagit fram en vägledning för hur myndigheter, kommuner och landsting bör arbeta med sina analyser.[40] Risk- och sårbarhetsanalyserna utgör ett viktigt underlag som MSB använder sig av för att göra sina nationella risk- och förmågebedömningar.

3.4 Försvarsunderrättelseverksamhet

FRA har ett flertal uppgifter utifrån svensk utrikes-, säkerhets- och försvarspolitik. Utifrån granskningens inriktning har Riksrevisionen undersökt vilka möjliga informationskällor regeringen har för att tillägna sig den kunskap om hot och skyddsåtgärder som krävs för att utvärdera och styra informationssäkerhetsarbetet i statsförvaltningen. Utifrån den aspekten har FRA:s försvarsunderrättelseverksamhet undersökts.

Enligt lagen (2000:130) om försvarsunderrättelseverksamhet ska försvarsunderrättelseverksamhet bedrivas till stöd för svensk utrikes-,

---

[38] MSB har vid faktagranskning av utkast till denna granskningsrapport uppgett att man nu ser över dessa föreskrifter, och avser att utfärda nya vid årsskiftet 2014/2015.

[39] Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

[40] MSB: *Vägledning för Risk- och sårbarhetsanalyser*, 2011.

säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Det är regeringen som bestämmer inriktningen, och inom ramen för denna inriktning får de myndigheter som regeringen bestämmer ange en närmare inriktning av verksamheten.[41] Det är följaktligen inte FRA själv som inriktar sin verksamhet, utan det gör de myndigheter som får ge FRA underrättelseuppdrag. Försvarsunderrättelseverksamheten vid FRA bedrivs bland annat genom signalspaning. Av 1 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen) följer att den myndighet som regeringen bestämmer (FRA) får inhämta signaler i elektronisk form vid signalspaning.

Av 2 a § signalspaningslagen följer att inhämtning inte får avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats.

Av de lagar och förordningar som reglerar FRA:s verksamhet framgår således att försvarsunderrättelseverksamhet ska bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet, exempelvis med avseende på dataintrång i statsförvaltningen. Verksamheten får endast avse utländska förhållanden. Signalspaningsverksamheten vid FRA är alltså omgärdad av ytterst stränga regler.

3.5 Övriga regler och aktörer

3.5.1 Personuppgiftslagen och Datainspektionen

Syftet med personuppgiftslagen (1998:204) är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. De bestämmelser som är inriktade på informationssäkerhet finns i 31 och 32 §§. Av 31 § framgår att lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

- de tekniska möjligheter som finns
- vad det skulle kosta att genomföra åtgärderna
- de särskilda risker som finns med behandlingen av personuppgifterna
- hur pass känsliga de behandlade personuppgifterna är.

Enligt 32 § har Datainspektionen möjlighet att fatta beslut om vilka säkerhetsåtgärder den personuppgiftsansvarige ska vidta enligt 31 § i enskilda fall. De uttryckliga lagkraven är textmässigt kortfattade men Datainspektionen

[41] 1 § lagen (2000:130) om försvarsunderrättelseverksamhet.

har gett ut allmänna råd för att ge exempel på hur man uppfyller lagkraven. Dessa allmänna råd är omfattande och påminner i flera delar om säkerhetsskyddslagen. Ett exempel på råd är det som handlar om säkerhet för personuppgifter där det pekas på ISO-standarderna 27001 och ISO/IEC 27002.

Datainspektionens uppdrag

Datainspektionens uppgift är att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter. Inom ramen för uppdraget ingår tillsyn av informationssäkerhet.

Tillsynen bedrivs ofta sektorsvis och på förekommen anledning. Datainspektionen granskar bland annat nya tekniska företeelsers påverkan på den personliga integriteten. Som exempel kan nämnas molntjänster eller sociala nätverkstjänster. I dessa fall är det ofta fråga om granskning av specifika behandlingar av personuppgifter, funktioner eller system utifrån ett visst perspektiv, till exempel elektroniskt utlämnande. Det är sällan fråga om en fullständig genomlysning av den totala personuppgiftsbehandlingen hos ett tillsynsobjekt eftersom det enligt Datainspektionens bedömning, ur ett integritetsskyddsperspektiv, är mer effektivt med begränsade granskningar.[42]

Tillsynen sker genom skriftväxling eller genom inspektioner på plats hos tillsynsobjektet. Vid en inspektion på plats får tillsynsobjektet besvara frågor och förevisa de system eller funktioner som har betydelse för den personuppgiftsbehandling som granskas. En sådan inspektion tar vanligtvis en eller en halv dag att genomföra.

För att få en uppfattning om verksamhetens inriktning och omfattning mot statliga myndigheter och statliga bolag har Datainspektionen på Riksrevisionens begäran tagit fram statistik över inspektionsverksamheten.

Av de uppgifter Datainspektionen har lämnat framgår att under 2013 har drygt två årsarbetskrafter (3 498 timmar) genomfört 61 aktiviteter riktade mot statliga myndigheter och statliga bolag. Av dessa aktiviteter har sju varit inspektioner på plats hos tillsynsobjektet. Detta kan jämföras med Säkerhetspolisens verksamhet med två tillsyner i genomsnitt årligen och som vardera tar cirka 4 000 timmar i anspråk.

Datainspektionen uppger med anledning av statistiken att det till synes låga totala antalet nedlagda inspektionstimmar bör ses utifrån myndighetens breda uppdrag och de begränsade resurserna myndigheten har tilldelats i förhållande till det breda uppdraget.[43]

---

[42] Datainspektionens yttrande till Riksrevisionen 2014-09-19.

[43] Datainspektionens yttrande till Riksrevisionen 2014-09-24.

3.5.2 Arkivlagstiftningen och Riksarkivet

Av arkivlagen (1990:782) följer att vissa handlingar hos en myndighet ska tas om hand för arkivering och att myndighetens arkiv ska bevaras, hållas ordnade och vårdas. I detta ingår enligt 6 § att skydda arkivet mot förstörelse, skada, tillgrepp och obehörig åtkomst. För att utveckla på vilket sätt myndigheter ska vårda sina arkiv har Riksarkivet gett ut omfattande krav och vägledning i form av föreskrifter och allmänna råd.[44] Av föreskrifterna och råden framgår exempelvis krav på säkerhet, autenticitet, åtkomst och gallring.[45] Det finns även krav på dokumentation och register för arkivet och handlingar, krav på vilken form av papper som ska användas, krav på att skadliga föremål (exempelvis häftklamrar) ska avlägsnas, hur transport av handlingar ska ske, m.m.[46] I Riksarkivets föreskrifter om elektroniska handlingar finns ett kapitel som uttryckligen behandlar informationssäkerhet.[47] Av 6 kap. 1 § följer att en myndighet ska skapa och upprätthålla rutiner för samt vidta åtgärder för att skydda handlingarna från skada, manipulation, obehörig åtkomst och stöld. Det ska ske med utgångspunkt i standarden för LIS.[48] I kapitlet ställs också krav på att myndigheten har en plan för informationssäkerhet, att riskanalyser genomförs innan driftsättning, att elektroniska handlingar ska förses med behörighetssystem, loggsystem och skydd mot skadlig kod om det inte är uppenbart obehövligt, att säkerhetskopior regelbundet framställs och att hantering och förvaring görs i enlighet med Riksarkivets övriga föreskrifter.[49]

Riksarkivets uppdrag

Riksarkivet är statlig arkivmyndighet och har det särskilda ansvar för den statliga arkivverksamheten och för arkivvården i landet som framgår av arkivlagen och arkivförordningen (1991:446).[50]

Riksarkivet utformar föreskrifter och allmänna råd för arkivhantering och följer upp hur dessa följs. Riksarkivet genomför inspektioner vid statliga myndigheter för att kontrollera att myndigheterna fullgör sina skyldigheter enligt arkivlagen.

Enligt arkivförordningen (1991:446) ska arkiven regelbundet inspekteras, och Riksarkivets målsättning är att myndigheterna ska inspekteras minst var femte

---

44 Av 2 § arkivförordningen (1991:446) följer att Riksarkivet har rätt att ge ut föreskrifter.

45 Se exempelvis Riksarkivets föreskrifter och allmänna råd om handlingar på mikrofilm (RA-FS 2006:2).

46 Riksarkivets föreskrifter och allmänna råd om handlingar på papper (RA-FS 2006:1).

47 Riksarkivets föreskrifter om elektroniska handlingar (RA-FS 2009:1).

48 SS-ISO/IEC 27001:2006 och SS-ISO/IEC 27002:2005.

49 Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling) RA-FS 2009:1.

50 1 § förordningen (2009:1593) med instruktion för Riksarkivet.

år. En inspektion kan beröra hela arkivverksamheten inom en myndighet eller delar av den, såsom exempelvis arkivredovisning, gallring eller arkivlokaler. Inspektionen aviseras oftast i förväg, men oanmälda inspektioner förekommer också. De flesta inspektioner sker på plats i den inspekterade myndighetens lokaler, men inspektioner kan även utföras genom att myndigheten får besvara frågor per brev. Resultatet av inspektionerna kommuniceras i en inspektionsrapport. Rapporten beskriver hur väl myndigheten sköter sin arkivhantering. Om brister i arkivhanteringen konstateras kan Riksarkivet besluta om rättelse i form av ett föreläggande. Om en myndighet inte åtgärdar sina brister kan Riksarkivet besluta om en ny inspektion av myndigheten.[51]

3.5.3 Post- och telestyrelsen

Lagen (2003:389) om elektronisk kommunikation reglerar villkoren för att tillhandahålla elektroniska kommunikationstjänster. Syftet med lagen är att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer och största möjliga utbyte vad gäller urvalet av elektroniska kommunikationstjänster samt deras pris och kvalitet. Lagen ställer olika krav på de som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster, bland annat vad gäller teknisk och organisatorisk säkerhet. Lagen (2000:832) om elektroniska signaturer reglerar framställandet och utfärdandet av elektroniska signaturer, och syftet med lagen är att underlätta användningen av elektroniska signaturer. Lagen (2006:24) om nationella toppdomäner för Sverige på Internet reglerar den tekniska driften av nationella toppdomäner för Sverige på internet samt tilldelning och registrering av domännamn under dessa toppdomäner.

Post- och telestyrelsens uppdrag

Post- och telestyrelsen (PTS) är en av regeringens stöd- och tillsynsmyndigheter när det gäller informationssäkerhet i samhället. PTS har bland annat till uppgift att verka för robusta elektroniska kommunikationer (telekommunikationer, IT och radio) och ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation. PTS ska också lämna råd och stöd till myndigheter, kommuner och landsting samt företag, organisationer och andra enskilda i frågor om nätsäkerhet.[52] PTS utövar också tillsyn enligt lagen (2003:389) om elektronisk kommunikation, vilket innebär tillsyn av privata operatörer inom elektronisk kommunikation. PTS ansvarade tidigare för Sveriges IT-incidentcentrum (SITIC). Sedan 2011 har MSB övertagit denna funktion, som numera benämns CERT-SE. I samband med detta tydliggjordes de båda myndigheternas uppdrag inom informationssäkerhetsområdet.

---

[51] http://riksarkivet.se/tillsyn-och-radgivning.

[52] 4 § 15–17 förordningen (2007:951) med instruktion för Post- och telestyrelsen.

Till skillnad från regeringens andra stöd- och tillsynsmyndigheter, Säkerhetspolisen, FRA och MSB, har PTS inte något ansvar för att inhämta, analysera eller vidareförmedla information om informationssäkerheten på myndigheterna i statsförvaltningen. PTS har i stället ett sektorsansvar som innefattar bland annat tillsyn över de som tillhandahåller elektroniska kommunikationer (tjänster och nät) oavsett associationsrättslig form. PTS kan sägas ha tre roller som tillsynsmyndighet när det gäller informationssäkerhet. Förutom lagen om elektronisk kommunikation utövar myndigheten även tillsyn enligt lagen (2000:832) om elektroniska signaturer och lagen (2006:24) om nationella toppdomäner för Sverige på Internet.

I övrigt har PTS som sektorsmyndighet i uppdrag att tillse att samhällets behov av elektronisk kommunikation tillgodoses, och har därför ett särskilt uppdrag för att planera och vidta förberedelser för att skapa förmåga att hantera en kris och för att förebygga sårbarheter och motstå hot och risker.[53] I den rollen ligger att PTS har ett samlat ansvar för informationssäkerhet inom sektorn. En stor del av det uppdraget hänger samman med att elektroniska kommunikationer är driftsäkra och tillgängliga vid normalläge och vid extraordinära händelser. Vidare innebär det ett uppdrag att skydda abonnenters uppgifter vid användning av elektroniska kommunikationstjänster.[54]

3.6 Riksrevisionens tidigare iakttagelser av brister i regelverket

I Riksrevisionens tidigare granskning av regeringens styrning av informationssäkerhetsarbetet konstaterades att informationssäkerhetsrelevant reglering fanns spridd över hela rättsordningen. De säkerhetsverktyg som fanns i form av tekniska åtgärder, organisatoriska lösningar, rättsligt stöd, m.m. hade olika begränsningar och möjligheter. För att säkerställa ändamålsenlig användning behövde de olika säkerhetsverktygen samordnas. Ur ett informationssäkerhetsperspektiv ansåg Riksrevisionen att det krävdes att man anlade en helhetssyn på informationssäkerhetsarbetet och på dess reglering. Det fanns en rad krav i olika regleringar som hade bäring på myndigheters hantering av information.[55]

Regleringen av informationssäkerhet är i stora drag utformad på samma sätt i dag som den var 2007. Skillnaden är att MSB nu har rätt att utfärda föreskrifter om ledningssystem för informationssäkerhet (LIS). Några bindande regler för

---

53 11 § förordningen (2006:942) om krisberedskap och höjd beredskap.

54 5 kap. 6 b § samt 6 kap. 3 § lagen (2003:389) om elektronisk kommunikation.

55 Riksrevisionen: *Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen*, (RiR 2007:10), s. 81.

systematiskt informationssäkerhetsarbete fanns inte vid tidpunkten för den tidigare granskningen.

3.7 Sammanfattande iakttagelser

Av detta kapitel framgår att de fem regelverken delvis riktar sig mot samma objekt och i huvudsak reglerar samma fråga. Säkerhetsskyddslagstiftningen är ett omfattande och detaljerat regelverk, men avgränsat till verksamhet med betydelse för rikets säkerhet eller verksamhet som behöver skyddas mot terrorism. Personuppgiftslagen ställer genom Datainspektionens allmänna råd detaljerade och omfattande krav. De gäller dock endast hantering av personuppgifter, inte informationssäkerhet för verksamheten i stort även om säker hantering av personuppgifter i princip förutsätter ett systematiskt informationssäkerhetsarbete. MSB:s föreskrifter om ledningssystem för informationssäkerhet (LIS) omfattar till skillnad från personuppgiftslagen och säkerhetsskyddslagstiftningen inte krav på faktisk säkerhetsnivå, utan i stället krav på ett systematiskt arbetssätt.

Vad gäller de olika aktörerna på området framgår av kapitlet att Säkerhetspolisen är den enda myndigheten som har mandat att granska informationssäkerhet brett.[56] De verksamheter som granskas av Säkerhetspolisen utgör dock i praktiken en ytterst liten del av den totala statsförvaltningen.

FRA har i uppdrag att bedriva underrättelseverksamhet genom signalspaning, och den är riktad mot utländska aktörer. FRA har även i uppdrag att stödja statliga myndigheter och bolag i deras arbete med informationssäkerhet. Det gäller dock endast de mest samhällskritiska verksamheterna och endast på deras begäran.

MSB har ett omfattande uppdrag att stödja samhällets informationssäkerhet, men har inget uppdrag att utöva tillsyn. MSB är därför till stor del beroende av att aktörer lämnar uppgifter frivilligt. Den nätverksstruktur som MSB delvis grundar sin informationsinhämtning på ger enligt Riksrevisionen en insyn i vilka problem och hot som finns mot samhället i stort. Sättet att inhämta informationen kan dock innebära svårigheter för MSB att agera mot myndigheter och företag som deltar i informationsutbytet, eftersom agerandet kan riskera förtroendet och därmed grunden för informationsinsamlingen.

PTS har till skillnad från de andra stöd- och tillsynsmyndigheterna inte något ansvar för att inhämta, analysera eller vidareförmedla information om andra myndigheters informationssäkerhet. Genom sin tillsynsroll över elektroniska kommunikationer har PTS dock indirekt en viktig roll för statsförvaltningens

[56] Säkerhetspolisens granskning utgår från säkerhetsskyddsregleringen med bedömningsgrunden rikets säkerhet och den definition av informationssäkerhet som gäller där. Detta kan begränsa vad som kan göras i en granskning.

informationssäkerhet vad gäller att upprätthålla säkra elektroniska kommunikationer. Detta faller dock utanför syftet med granskningen och behandlas därför inte mer ingående.

Datainspektionen, som inte är utpekad stöd- eller tillsynsmyndighet, genomför tillsyn som omfattar informationssäkerhet, men dess tillsyn berör en delmängd av informationssäkerheten (integritetsskyddsaspekterna). Den tillsyn som utövas sker ur ett avgränsat perspektiv och i begränsad omfattning.

Riksarkivet har mandat att granska informationssäkerheten hos statliga myndigheter och bolag. Tillsynen är dock begränsad till att omfatta det som finns i myndigheternas arkiv, det vill säga i huvudsak allmänna handlingar. Mandatet omfattar därmed inte verksamhetens information och säkerheten för den i ett vidare perspektiv.

4 Vilken information har kommit regeringen till känna?

Utifrån granskningens inriktning har Riksrevisionen undersökt vilka möjliga informationskällor regeringen har för att tillägna sig den kunskap om hot, risker och skyddsåtgärder som krävs för att utvärdera och styra informationssäkerhetsarbetet i statsförvaltningen. Detta kapitel handlar om vad stöd- och tillsynsmyndigheterna vet om informationssäkerheten i statsförvaltningen och hur berörda myndigheter, olika slags utredningar, m.m. har rapporterat till regeringen om informationssäkerheten i statsförvaltningen. På så sätts belyses frågan om vilken information som regeringen fått. Kapitlet omfattar också sådan information som inte regeringen har blivit underrättad om, till exempel resultat av de undersökningar som Riksrevisionen låtit vissa av de granskade myndigheterna utföra. De utgångspunkter som kan kopplas till kapitlet är den om grundläggande förutsättningar i form av krav och organisering, regeringens såväl som stöd- och tillsynsmyndigheternas ansvar att se till att det genomförs systematiska analyser av hot och risker för att befintliga skyddsåtgärder inte är tillräckliga samt beslut om nya eller förändrade åtgärder och införande och kontroll av åtgärdernas funktion.

4.1 Vilken bild har MSB och vad har myndigheten rapporterat till regeringen?

4.1.1 MSB:s arbete med risk- och sårbarhetsanalyser

MSB identifierade under 2009 att det fanns ett behov av att utfärda föreskrifter och förenkla arbetet med risk- och sårbarhetsanalyser. Hela systemet med risk- och sårbarhetsanalyser borde hänga samman, från den lokala nivån upp till den centrala nivån, samt att de krav som ställs i de olika lagarna borde fungera tillsammans.[57]

Som stöd för redovisningen av krisberedskapsförmåga i risk- och sårbarhetsanalyserna används i dag ett antal indikatorer. Någon redovisning av indikatorerna för informationssäkerhet har dock inte alltid skett i de årliga sammanställningar av resultatet som MSB tar fram, då myndigheternas redovisning inte görs på ett sätt som medger en fullständig aggregering och

[57] Översyn av processen för fördelning av anslag 2:4 Krisberedskap – Uppdrag 15 i MSB:s regleringsbrev för 2009, s. 15.

övergripande analys.[58] För dessa indikatorer bedömer dessutom en stor del av myndigheterna att man endast till viss del eller inte alls uppfyller kriterierna. Ett skäl till detta kan enligt MSB vara att indikatorerna för informationssäkerhet är nytillkomna i förmågebedömningen 2012.[59] Det är enligt MSB möjligt att svaren reflekterar en viss osäkerhet bland respondenterna om hur faktorerna redundans och robusthet respektive konfidentialitet, riktighet och tillgänglighet ska tolkas och bedömas. De tre senare begreppen utgör grundkomponenter i ledningssystem för informationssäkerhet, vilket enligt MSB:s föreskrifter är ett krav för alla myndigheter. MSB konstaterar 2013 med anledning av detta att kommande enkäter för särskild förmågebedömning kanske tydligare bör efterfråga hur den berörda myndigheten tillämpar föreskrifterna.[60]

Ett av de moment som enligt MSB hittills visat sig vara svårt att omsätta är riskvärdering. Riskvärdering handlar enligt MSB ytterst om att värdera om den analyserade risken kan anses vara acceptabel.[61]

Det analys- och utvecklingsarbete som MSB genomför kommer även att beröra vilka analyser olika krisberedskapsaktörer behöver göra (innehåll, syfte och användning), tidsintervallet för sådana analyser, hur analyserna relaterar till varandra samt analysarbetets förväntade sammantagna effekter.[62]

Av de analyser som MSB använder som underlag framgår att behovet för myndigheter att samverka med andra aktörer när det gäller informationssäkerhet enligt MSB enbart delvis är identifierat och tillgodosett. Ett skäl är att det är svårt att identifiera dels vilken informationshantering som är samhällsviktig i Sverige, dels vilka verksamheter som har direkt samverkansbehov vid en störning (till exempel vilka verksamheter som har IT-drift i samma anläggningar och drabbas samtidigt vid driftbortfall).[63]

---

58 Se exempelvis MSB: *Risker och förmågor 2012 – Redovisning av regeringsuppdrag om nationell riskbedömning respektive bedömning av krisberedskapsförmåga*, s. 66.

59 MSB: *Risker och förmågor 2012 – Redovisning av regeringsuppdrag om nationell riskbedömning respektive bedömning av krisberedskapsförmåga*, s. 70.

60 MSB: *Risker och förmågor 2012 – Redovisning av regeringsuppdrag om nationell riskbedömning respektive bedömning av krisberedskapsförmåga*, s. 66.

61 MSB: *Risker och förmågor 2013 – Redovisning av regeringsuppdrag om nationell risk- och förmågebedömning*, s. 79. För närvarande pågår en översyn av MSB:s föreskrifter (MSBFS 2010:6) respektive (MSBFS 2010:7) om redovisning av risk- och sårbarhetsanalyser, och MSB har vid faktagranskningen av utkast till denna granskningsrapport uppgett att nya föreskrifter skulle kunna träda i kraft vid årsskiftet 2014/2015.

62 MSB: *Risker och förmågor 2013 – Redovisning av regeringsuppdrag om nationell risk- och förmågebedömning*, s. 79 f.

63 MSB: PM 2014-04-24 *Samlad bedömning av samhällets krisberedskapsförmåga 2013 – Komplettering av regeringsuppdrag nummer 26*, dnr 2013-5294, s. 16.

MSB har på begäran av Riksrevisionen gått igenom 23 myndigheters hantering av informationssäkerhet i sina risk- och sårbarhetsanalyserna för 2013.[64]. Genomgången visar att informationssäkerheten inte behandlas i samtliga av de undersökta risk- och sårbarhetsanalyser, trots att det finns uttryckliga krav på detta i föreskrifterna. Generellt för myndigheternas risk- och sårbarhetsanalyser är också att det inte alltid finns en röd tråd mellan beskrivna risker respektive beskrivna åtgärder, vilket även är fallet för informationssäkerhetsområdet.[65] I de fall som en myndighet tar upp informationssäkerhet i sin risk- och sårbarhetsanalys, bedömer MSB att detta ofta sker om myndigheten bedömt att det finns ett (prioriterat) hot. Det finns dessutom mycket sällan någon generell bedömning av informationssäkerheten i underlagen. Ingen myndighet har valt att beskriva sin informationssäkerhet utifrån en systematisk genomgång gentemot tillämpliga standarder eller genom en strukturerad genomgång av parametrarna konfidentialitet, riktighet och tillgänglighet. Allt detta gör det mycket svårt att aggregera informationen. Ingen myndighet nämner heller något i sin risk- och sårbarhetsanalys om säkerhet i samband med e-förvaltning, vilket enligt MSB är anmärkningsvärt då utvecklingen på området gått mycket snabbt de senaste åren.

MSB bedömer att det, enbart utifrån myndigheternas risk- och sårbarhetsanalyser inte går att få en kvalitetsmässigt godtagbar bild av myndigheternas förmåga på informationssäkerhetsområdet. MSB har framfört ett antal skäl till att så är fallet. Myndigheterna använder olika metoder för att identifiera risk, vilket omöjliggör jämförelser mellan myndigheter. Det är också så att enbart ett fåtal av samtliga myndigheter beskriver risker, sårbarheter och vidtagna åtgärder på informationssäkerhetsområdet, vilket gör att helhetsbilden brister. Ett annat skäl är att det ofta saknas kopplingar mellan redovisade risker och (planerade och vidtagna) åtgärder.[66] Det går därmed inte med stöd av risk- och sårbarhetsanalyserna i sin nuvarande utformning att ge en nationell, sammantagen bild av myndigheternas förmåga att hantera och motstå kriser på informationssäkerhetsområdet.

4.1.2 MSB:s trendrapport och annan rapportering om informationssäkerhet

MSB ger regelbundet ut trendrapporter och andra rapporter om informationssäkerheten i samhället. Den senaste trendrapporten ger enligt MSB en övergripande bild av situationen på informations- och cybersäkerhetsområdet,

---

64 Genomgången omfattar samtliga myndigheter som uppräknas i krisberedskapsförordningen undantaget länsstyrelserna. Genomgången har skett mot 5 § MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2010:7) punkterna 4 och 8. Enbart information med bäring på informationssäkerhet har inkluderats.

65 MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2010:7).

66 MSB har även fört fram att a) informationssäkerheten inte redovisas enskilt i underlagen utan ofta ligger med som bisatser till annat, vilket bidrar till otydlighet samt att b) det saknas en systematisk beskrivning av informationssäkerhetsarbetet vid myndigheterna, vilket försvårar aggregering och jämförelser.

samt en bedömning av vilka förhållanden som är särskilt angelägna att uppmärksamma.[67] Rapporten fokuserar på att beskriva vad som kan hända och till viss del vad som har hänt knutet till informationssäkerhet. Rapporten behandlar därmed risker, men säger ingenting om förmåga. Den ger heller ingen kunskap om vilka skyddsåtgärder som vidtas ute i förvaltningen. Utöver trendrapporter återrapporterar MSB löpande om samhällets informationssäkerhet inom ramen för den nationella risk- och förmågebedömningen (NRFB) samt i årsredovisningen och särskilda händelserapporter.

4.1.3 Ledningssystem för informationssäkerhet (LIS)

Efterlevnaden av LIS-föreskrifterna har följts upp två gånger sedan de trädde i kraft 2008. Den första uppföljningen gjordes av Stockholms Handelskammare på eget initiativ under 2008. Med anledning av enkätundersökningen konstaterade handelskammaren att 22 av 39 tillfrågade myndigheter inte följde föreskriften. Med hänvisning till undersökningen ställdes i riksdagen en fråga om myndigheternas IT-säkerhet som besvarades av dåvarande statsrådet Åsa Torstensson.[68] Statsrådet svarade att

> ”...med anledning av frågan har departementet underhand erfarit att flertalet av de statliga myndigheter som enligt utredningen inte arbetade enligt LIS-standarden numera gör det, eller har genomfört förstudier och driver projekt med tidplaner i denna riktning. Arbetet med att införa ledningssystem är en process som kräver tid och förberedelser. I de fall som det inte skett beror det på att myndigheten är mycket liten och anger begränsade informationssäkerhetsbehov”.

Statsrådet framförde att det i första hand ankommer på myndigheternas ledning och styrelse att införa LIS. Regeringen följer dock utvecklingen, både via den tillsyn som sker, Riksrevisionens rapporter, genom uppföljning av handlingsplanerna och i myndighetsdialogen.[69]

Under 2014 har MSB kartlagt hur statliga myndigheter tillämpar MSB:s föreskrifter om LIS. Det övergripande syftet med arbetet har varit att säkerställa att föreskrifternas utformning ger ett ändamålsenligt stöd för statliga myndigheters systematiska arbete med informationssäkerhet. Ett sekundärt syfte har varit att få en bild av hur informationssäkerhetsarbetet bedrivs vid svenska myndigheter.[70] Kartläggningen omfattade samtliga 351 myndigheter

---

67 MSB: *Trendrapport – samhällets informationssäkerhet 2012*, s. 6.

68 Svar på skriftlig fråga 2008/09:871 IT-säkerhet inom myndigheter och kommuner.

69 Svar på skriftlig fråga 2008/09:871 IT-säkerhet inom myndigheter och kommuner.

70 MSB: *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*, s. 11.

som har att följa föreskrifterna, varav 334 myndigheter (drygt 95 procent) har svarat på MSB:s frågor.[71]

Kartläggningen visar följande resultat för de myndigheter som har besvarat alla frågor som MSB har ställt.[72]

Policy och styrande dokument[73]

- 84 procent av myndigheterna har en informationssäkerhetspolicy.
- 26 procent av myndigheterna kontrollerar inte efterlevnaden, det vill säga ifall policyer och riktlinjer följs av medarbetarna.

Leda och samordna informationssäkerhetsarbetet[74]

- 74 procent av myndigheterna har utsett en informationssäkerhetschef eller motsvarande roll för att leda och samordna informationssäkerhetsarbetet.
- 81 procent av de som leder och samordnar informationssäkerhetsarbetet hos myndigheterna rapporterar direkt till myndighetens ledning.
- 38 procent av de som leder och samordnar informationssäkerhetsarbetet hos myndigheterna uppges sakna tillräcklig kompetens, resurser eller mandat för att utgöra uppdraget på ett tillfredsställande sätt.

Informationsklassning[75]

- 67 procent av myndigheterna har en informationsklassningsmodell för att identifiera informationstillgångarna och kunna ställa rätt krav på informationssäkerheten.
- 41 procent av myndigheterna uppger att det inte är tydligt uttalat vem som ansvarar för att informationsklassning genomförs.
- 59 procent av myndigheterna uppger att det inte är fastslaget när informationsklassning ska ske.

---

71 MSB: *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*, s. 7.

72 Myndigheter, som till exempel på grund av ringa storlek, har överlåtit sitt informationssäkerhetsarbete till en annan myndighet har endast besvarat frågor om hur detta reglerats med värdmyndigheten.

73 MSB: *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*, s. 7.

74 MSB: *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*, s. 7.

75 MSB: *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*, s. 8.

Riskanalys och dokumentation[76]

- 78 procent av myndigheterna har en metod för riskanalys.
- 42 procent av myndigheterna saknar regler för vad riskanalyser ska omfatta eller när det ska ske.
- 35 procent av myndigheterna saknar uttalat ansvar för vem som ska initiera riskanalyserna.

Kontinuitetsplanering[77]

- 65 procent av myndigheterna saknar en kontinuitetsplan.
- 59 procent av myndigheterna använder inte riskanalyserna som stöd vid kontinuitetsplanering.

Ledningens engagemang[78]

- 45 procent av myndigheter uppger att myndighetens ledning åtminstone i stor utsträckning löpande håller sig informerade om arbetet med informationssäkerhet.
- 37 procent av myndigheterna har ingen eller en mycket begränsad utvärdering av informationssäkerhetsarbetet på myndigheten.

Flera myndigheter har i kartläggningen också uttryckt önskemål om att få mer stöd för bland annat kravställning, uppföljning, informationsklassning och kontinuitetsplanering.

Enskilda svar i uppföljningen kan uppfattas som positiva. En samlad läsning av svaren visar dock att även om 84 procent av myndigheterna uppger att de har en informationssäkerhetspolicy så svarar 38 procent att kompetens, mandat eller resurser är otillräckliga för att utföra arbetet på ett tillfredsställande sätt, 42 procent att det saknas regler för vad riskanalysen ska omfatta eller när den ska ske och 65 procent att de saknar kontinuitetsplan. Riksrevisionens bedömning är därför att en stor andel myndigheter inte har centrala delar av ett systematiskt informationssäkerhetsarbete på plats. Riksrevisionen konstaterar också att MSB i rapporten inte lämnar någon sammanfattande bedömning av tillståndet och inte heller föreslår vilka eventuella åtgärder som behöver vidtas.[79]

---

[76] MSB: En *bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*, s. 8.

[77] MSB: *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*, s. 8.

[78] MSB: *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*, s. 8.

[79] MSB har vid faktagranskningen av utkast till denna granskningsrapport uppgett att ett analysarbete pågår för att klargöra vilka åtgärder som behöver vidtas.

4.1.4 Vad har MSB rapporterat till regeringen?

MSB har lämnat information till regeringen om hot, risker och förmåga gällande krisberedskap på flera sätt. När det gäller krisberedskap i stort har detta främst skett genom rapporter om samhällets krisberedskap och nationell risk- och förmågebedömning. Därutöver tillkommer den redovisning av samhällets informationssäkerhet som MSB själv gör i sin egen risk- och sårbarhetsanalys i egenskap av ansvarig för området. Rapporteringen är framför allt inriktad på risker och förmåga baserat på risk- och sårbarhetsanalyser och scenarioanalyser. MSB informerar regeringen löpande om hot och risker mot Sverige och svenska intressen, vilket även kan innefatta informationssäkerhetsrelaterad information när detta bedöms ha hög dignitet.

MSB:s trendrapport handlar om informationssäkerhet och dess hot och risker. MSB:s uppföljning av tillämpningen av föreskriften om LIS har avrapporterats i en publik rapport. Den genomgång av informationssäkerhetaspekterna i risk- och sårbarhetsanalyserna som berörs ovan är utförd på Riksrevisionens uppdrag. Denna information kan möjligen ha lämnats till regeringen efter det att den kommit Riksrevisionen till handa.

MSB:s rapportering till regeringen sker också i form av remissyttranden över utredningar som rör informationssäkerhet. MSB har på detta sätt pekat på att informationssäkerhetsarbetet behöver förbättras inom e-förvaltning och vård och omsorg. Dessutom har MSB enligt egen utsago de senaste fyra åren redovisat åtta regeringsuppdrag på informationssäkerhetsområdet.[80]

4.2 Vilken bild har FRA och vad har myndigheten rapporterat till regeringen?

4.2.1 Försvarsunderrättelseverksamhet

De kvalificerade aktörer som FRA följer inom sin försvarsunderrättelseverksamhet anges i regeringens årliga inriktning. Dessa aktörer är i huvudsak statsunderstödda och de utgör ett hot mot de mest skyddsvärda verksamheterna i Sverige. Vad gäller signalunderrättelseverksamhet ska FRA därmed leverera direkt och indirekt skydd mot kvalificerade IT-angrepp till de mest skyddsvärda svenska samhällsfunktionerna. FRA levererar utifrån sin försvarsunderrättelseverksamhet rapporter till regeringen om de aktörer och hot som följer av regeringens inriktning. Rapporteringen innehåller dock inte uppgifter om status på myndigheternas informationssäkerhet.

[80] Uppgift vid faktagranskning av utkast till denna granskningsrapport.

4.2.2 *IT-säkerhetsanalyser och penetrationstester*

På Riksrevisionens begäran har FRA lämnat ett yttrande om sin verksamhet som rör IT-säkerhetsanalyser och penetrationstester.[81] Följande avsnitt bygger på detta yttrande.[82]

FRA har inte något tillsynsansvar, utan kan enbart göra IT-säkerhetsanalyser på begäran av kund (statlig myndighet eller statligt bolag) eller som stöd till exempelvis Säkerhetspolisen eller den militära underrättelse- och säkerhetstjänsten (MUST) vid en tillsyn. FRA tar ut avgifter för att utföra IT-säkerhetsanalyserna.[83] Detta leder dock till att FRA endast kan hjälpa de som har budgeterat för IT-säkerhetsarbete, vilket inte alltid behöver sammanfalla med de som har den mest skyddsvärda informationen eller behöver mest hjälp.[84]

Vid IT-säkerhetsanalyser agerar FRA angripare i en IT-miljö i samråd med den beställande kunden. FRA får tillgång till systemdokumentation och information om systemen innan testet. Beställaren och FRA tar också tillsammans fram en lista på det inom beställarens IT-miljö som anses vara det mest skyddsvärda för verksamheten. Målet för IT-säkerhetsanalysen är vanligtvis att hitta så många brister som möjligt för att de ska kunna rättas till.

Efter genomförd analys avrapporterar FRA resultatet till beställaren i en skriftlig rapport, och ibland även med en presentation för ledningen. Rapporten innehåller alltid tillvägagångssätt, funna brister samt prioriterade åtgärdsförslag, men ibland även resultat från sårbarhetsskanning, statistik på lösenordskvalitet och förslag på vidare arbete. Rapporteringen från penetrationstesterna delges endast den myndighet som testet avser. FRA har inte gjort någon aggregerad avrapportering till regeringen eller Regeringskansliet av genomförda tester.

4.2.3 *Hur ser FRA på informationssäkerheten i de verksamheter man kommer i kontakt med?*

FRA:s övergripande bedömning är att det ofta är alltför lätt att bryta sig in i samhällsviktiga system. Skyddet motsvarar sällan nivån på informationen som hanteras i systemen eller de hot som systemen bör skyddas mot. De brister som FRA upptäcker leder i stort sett alltid till att en angripare kan ta över hela IT-miljön med möjlighet att läsa, manipulera eller förstöra all information som hanteras på IT-systemen.

---

81 Under 2013 genomförde FRA IT-säkerhetsanalyser vid elva olika statliga myndigheter och statligt ägda bolag. FRA har under de senaste 10 åren genomfört uppskattningsvis 120 IT-säkerhetsanalyser och 100 övriga granskningar/rådgivningar. FRA har även hanterat ett antal IT-incidenter per år.

82 FRA:s yttrande till Riksrevisionen informationssäkerhetsarbete och övergripande bedömning av myndigheters IT- och informationssäkerhet, september 2014.

83 I 11 § förordningen (2007:937) med instruktion för Försvarets radioanstalt föreskrivs att myndigheten får ta ut avgifter för genomförande av IT-säkerhetsanalyser.

84 Intervjuer med företrädare för FRA.

Problem kopplade till en önskan att pressa IT-kostnaderna är något som FRA har sett hos flera statliga myndigheter och statligt ägda bolag. IT-budgeten är hårt styrd, och externa krav på lönsamhet eller sparsamhet medför lösningar som till exempel outsourcing. Outsourcing i kombination med otillräcklig beställarkompetensen gör att outsourcing ofta blir en kortsiktig besparing, men i det långa loppet uppstår flera brister som är svåra att värdera i kronor. Den som outsourcar blir av med sin egen kompetens inom IT-området, vilket i sin tur gör att beställarkompetensen blir än mer lidande. Många beställare gör dessutom misstaget att förutsätta att säkerhet ingår i avtalet även om detta inte uttryckligen är specificerat. Så är inte fallet enligt FRA:s erfarenhet. Kommersiella driftleverantörers huvudsyfte är att generera vinst, och de kommer enligt FRA:s bedömning inte att göra kostnadsdrivande investeringar i säkerhet om det inte finns konkurrensskäl som talar för det. FRA har inte rätt att granska någon driftleverantörs nätverk eller sätt att administrera IT-driften vid statliga myndigheter eller statligt ägda bolag. FRA har, trots att driftleverantörerna inte har granskats, sett tydliga exempel där externa driftleverantörer och konsulter utsätter myndigheter för stora risker utan myndigheternas vetskap. FRA förespråkar inte att man helt bör sluta med outsourcing, men man bör tydligt se över kravställning mot externa driftleverantörer, samt vilka verksamheter som kan outsourcas.

Enligt FRA sammankopplas IT-system mellan olika myndigheter och företag i en allt större utsträckning. Till detta kommer en stadigt ökande användning av mobila enheter och olika tjänster på internet både i tjänsten och privat. FRA förutspår att de risker en organisation utsätts för kommer att öka i framtiden. Många myndigheter är anslutna till varandra och hanterar samma information, men med olika nivå på skydd och klassning av informationen. En angripare kanske inte behöver ge sig på de mest skyddsvärda verksamheterna för att få den information man är ute efter, utan den kan troligen fås via en mindre skyddsvärd verksamhet eller en driftsleverantör som har tillgång till att hämta informationen från ursprungsstället. Ingen kedja är starkare än den svagaste länken, och i statsförvaltningen hänger allt samman.

4.2.4 Vad har FRA rapporterat till regeringen?

FRA rapporterar löpande information av betydelse till regeringen utifrån vad myndigheten fångar upp genom sin försvarsunderrättelseverksamhet. Därav får regeringen information om hot och hotaktörer av en viss dignitet med intresse för samhällsviktig verksamhet även vad gäller informationssäkerhet. Den information som FRA får del av genom IT-säkerhetsanalyser och penetrationstester har förutom i enstaka fall inte rapporterats till regeringen, vare sig i aggregerad form eller specifikt för enskilda verksamheter. FRA har

vad gäller övergripande hot och risker dock använt sig av informationen i en trendrapport som har publicerats.[85]

4.3 Vilken bild har Säkerhetspolisen och vad har myndigheten rapporterat till regeringen?

4.3.1 Säkerhetspolisens tillsyn visar på omfattande brister i säkerheten

Som en del av Säkerhetspolisens tillsyn ingår att bedöma myndigheternas säkerhetsanalyser ur ett informationssäkerhetsperspektiv. Säkerhetspolisen har på begäran av Riksrevisionen gjort en övergripande expertbedömning av de 18 säkerhetsanalyser som blivit granskade sedan 2006, och särskilt i fråga om informationssäkerhet.[86]

Säkerhetspolisens övergripande bedömning är att analyserna generellt lider av allvarliga brister, även om undantag finns. Det saknas ofta en användbar systembeskrivning av det som ska skyddas. Det saknas också genomarbetade, välargumenterade och dokumenterade skadekonsekvensbeskrivningar för de IT-system som myndigheten eventuellt anser behöver skyddas. Om dessa beskrivningar ändå förekommer beskriver de ofta andra typer av konsekvenser än de som är knutna till rikets säkerhet och terrorism, till exempel ekonomiska konsekvenser eller konsekvenser för myndighetens anseende. Den förmåga en angripare kan tänkas ha tas sällan upp, vilket försvårar vad en myndighet ska behöva dimensionera sitt skydd mot. Det finns heller inte några beskrivningar av vilka specifika sårbarheter hos identifierade skyddsvärda system som får mycket allvarliga konsekvenser om de utnyttjas av en antagonist, och på vilket sätt detta kan ske.

4.3.2 Konsekvenserna kan bli allvarliga

Säkerhetspolisen bedömer att konsekvenserna av bristerna i säkerhetsskyddet kan bli allvarliga. Detta hänger samman med att de granskade myndigheterna är bland de mest skyddsvärda och att deras information rör rikets säkerhet.

Bristerna i att identifiera skyddsvärden under säkerhetsanalysen leder enligt Säkerhetspolisen till att de granskade myndigheterna inte kan ta fram välmotiverade kravspecifikationer på informationssäkerhetsområdet för den mest skyddsvärda informationen. Bristfälliga kravspecifikationer leder i sin tur till att de säkerhetsskyddsåtgärder som myndigheterna vidtagit eller planerar att vidta inte bidrar på ett spårbart sätt till att skydda de mest skyddsvärda

---

[85] FRA: *Trender och utmaningar i dag och i morgon – informationssäkerhet*.

[86] Säkerhetspolisen: *Underlag rörande Säkerhetspolisens bedömning av myndigheters säkerhetsanalyser ur ett informationssäkerhetsperspektiv*, 2014-07-11, dnr 2014-11898-4.

informationstillgångarna. Detta blir särskilt påtagligt då man engagerar externa leverantörer i sin IT-verksamhet eller lägger ut IT-verksamhet på privata och i vissa fall även utländska leverantörer. I dessa fall är en noggrann kravställning grundläggande för att kunna bedöma om en utläggning över huvud taget är lämplig, och om informationstillgångar i så fall ska få ett lämpligt skydd.

En annan allvarlig konsekvens av bristerna i säkerhetsanalyserna är att informationstillgångar med samma skyddsvärde riskerar få varierande nivåer på olika myndigheter. Detta är enligt Säkerhetspolisen särskilt allvarligt när det gäller att identifiera de mest skyddsvärda informationstillgångarna. Säkerhetspolisen har dessutom uppgett för Riksrevisionen att det vid uppföljningar ibland framkommer att redan påpekade brister inte åtgärdas.[87] Den åtgärd som Säkerhetspolisen kan vidta i ett sådant fall är att underrätta regeringen om detta förhållande. Avsaknaden av sanktionsmöjlighet och eventuella problem med anledning av detta är en av de frågor som ska behandlas i utredningen om en ny säkerhetsskyddslag.[88]

4.3.3 Vad har Säkerhetspolisen rapporterat till regeringen?

Säkerhetspolisen skickar varje tillsynsrapport till det departement som är ansvarig för den myndighet tillsynen avser. Regeringen har därmed fått en detaljerad redovisning av informationssäkerhetsläget hos de verksamheter som de 18 tillsynsrapporterna avser. Den aggregerade bild som Riksrevisionen hänvisar till ovan är framtagen på Riksrevisionens begäran, och Riksrevisionen saknar kunskap om huruvida informationen även har vidarebefordrats till regeringen. Utöver tillsynsrapporterna lämnar Säkerhetspolisen även annan information om hot och sårbarheter till regeringen.

4.4 Vilken bild har Datainspektionen och vad har myndigheten rapporterat till regeringen?

4.4.1 Vilken kunskap ger tillsynen?

Som tillsynsmyndighet enligt personuppgiftslagen (1998:204) granskar Datainspektionen skyddet för personuppgifter. Inspektionen ska verka för att personuppgiftsansvarigas informationssäkerhet uppfyller de krav som personuppgiftslagen ställer för att skydda de personuppgifter som behandlas. Informationssäkerhetsarbetet hos organisationer har ofta som övergripande syfte att skydda organisationens verksamhet medan personuppgiftslagen syftar till att skydda de registrerades personliga integritet. Det föreligger således skillnader mellan informationssäkerhet i ett generellt perspektiv och

[87] Intervju på Säkerhetspolisen 2014-06-19.

[88] En modern säkerhetsskyddslag (dir. 2011:94).

säkerhetskrav enligt personuppgiftslagen i såväl skyddsobjekt som syftet med informationssäkerhetsåtgärderna. Det innebär att det inte går att dra några slutsatser om en organisations informationssäkerhetsarbete i stort utifrån brister i skyddet för personuppgifter. Som exempel kan nämnas Datainspektionens granskning av så kallade bank-appar där bankerna utifrån ett verksamhetsperspektiv kunde sägas ha ett väl strukturerat informationssäkerhetsarbete, att skydda sina och kundernas pengar, men där det ändå fanns brister när det gäller informationssäkerheten för de personuppgifter som behandlades.

4.4.2 Vad har Datainspektionen rapporterat till regeringen?

Datainspektionen avrapporterar iakttagelser av informationssäkerhet vid behandling av personuppgifter till regeringen genom publika rapporter, eventuella regeringsuppdrag och årsredovisningen. Inspektionen rapporterar även till Regeringskansliet genom att vid behov översända tillsynsbeslut för kännedom. Datainspektionen har inte fått några särskilda regeringsuppdrag för att undersöka informationssäkerheten på en viss specifik myndighet eller mer generellt i statsförvaltningen. Datainspektionen har i sin årsredovisning återkommande framfört att ”Vid utveckling av e-förvaltning där fler än en myndighet är inblandad ser inspektionen ofta att ett allt större ansvar läggs på den enskilde… Inspektionen finner också ofta brister i IT-säkerheten … Tjänster för elektronisk förvaltning förefaller fortfarande många gånger utvecklas och tas i bruk utan att kraven på säkerhetsåtgärder beaktas tillräckligt.”[89]

4.5 Övriga myndigheternas rapportering i årsredovisningen

Riksrevisionen har även gått igenom årsredovisningarna för samma urval av myndigheter, vid sidan av stöd- och tillsynsmyndigheterna, som för genomgången av regleringsbreven för att få en uppfattning om myndigheterna självmant redovisar uppgifter om sin informationssäkerhet. Genomgången avser perioden 2009–2013.[90]

Genomgången visar att mindre än hälften av myndigheterna rapporterar något om informationssäkerhet eller datasäkerhet. För det stora flertalet myndigheter – cirka 70 procent – går det inte att få en uppfattning om hur läget är för informationssäkerhet genom att ta del av årsredovisningen.

För en mer detaljerad beskrivning av resultat och tillvägagångssätt hänvisar vi till bilaga 3.

---

[89] Datainspektionens årsredovisningar för 2009–2013.

[90] Se bilaga 2.

4.6 Rapportering från utredningar m.m.

Vi har gått igenom 63 utredningsbetänkanden som lämnats av parlamentariska kommittéer och särskilda utredare från och med 2007 och till dags dato och som kan vara av relevans för styrning av informationssäkerheten i statsförvaltningen.[91] Två av dessa har behandlat informationssäkerhet ur ett mer myndighetsövergripande perspektiv.

I E-delegationens betänkande *Så enkelt som möjligt för så många som möjligt – vägen till effektivare e-förvaltning* behandlas ett förslag till samverkanslösning för att stärka informationssäkerheten. Förslaget går ut på att fyra myndigheter bli utvecklingsmyndigheter för e-förvaltning inom var sitt utvecklingsområde. Myndigheterna i fråga är Skatteverket, Lantmäteriet, Transportstyrelsen och Bolagsverket.[92] Delegationen konstaterade att informationssäkerhet varit svårt att omsätta i de samarbetsprojekt som bedrivs inom e-förvaltningsområdet, och önskat ett ökat stöd för detta. Delegationen uttalade att det krävs en gemensam grund i form av säkerhetskultur, metoder och regler. MSB tog därför initiativ till att det borde inrättas ett nytt arbetsutskott inom delegationen för att förverkliga den strategi för informationssäkerhet som E-delegationen beslutat. Arbetsutskottet ska dels ta fram en handlingsplan för att förverkliga målen i strategin, dels lämna metodstöd till de projekt som genomförs i delegationen.[93] Enligt MSB är dock informationssäkerhetsfrågan fortfarande inte helt etablerad i alla delar av delegationens arbete.[94]

I ett betänkande från Informationssäkerhetsutredningen som handlar om vem som ska ansvara för Sveriges IT-incidentcentrum (Sitic) och Sveriges certifieringsorgan för IT-säkerhet (CSEC) behandlas informationssäkerheten i ett strategiskt perspektiv.[95]

Vi har även gått igenom 41 departementspromemorior som tagits fram av olika arbetsgrupper inom Regeringskansliet från och med 2007 som kan vara relevanta från informationssäkerhetssynpunkt. I en av promemoriorna som handlar om elektronisk kommunikation talas om att det ska säkerställas att

---

91 Av E-delegationen avlämnade betänkanden: SOU 2009:86, 2010:62, 2011:67, 2012:68 samt 2013:22. Övriga betänkanden är från Utredningen om stärkt krisberedskap i det centrala betalningssystemet (SOU 2011:78), Servicecenterutredningen (SOU 2011:38) samt Informationssäkerhetsutredningen (SOU 2010:25).

92 E-delegationens betänkande *Så enkelt som möjligt för så många som möjligt – vägen till effektivare e-förvaltning* (SOU 2011:67).

93 E-delegationens betänkande *Så enkelt som möjligt för så många som möjligt – förstärkt samordning av förvaltningsgemensamma tjänster* (SOU 2012:68) samt *Så enkelt som möjligt för så många som möjligt – samordning och digital samverkan* (SOU 2013:22).

94 Uppgift vid faktagranskning av utkast till denna granskningsrapport.

95 Informationssäkerhetsutredningen betänkande *Viss översyn av verksamhet och organisation på informationssäkerhetsområdet* (SOU 2010:25).

elektronisk kommunikation uppfyller rimliga krav på driftsäkerhet, och om att införa en skyldighet att rapportera integritetsincidenter.[96]

Den promemoria som mest ingående tar upp informationssäkerhet härrör från den senaste försvarsberedningen. I ett säkerhetspolitiskt sammanhang utvecklar beredningen de hot och risker som finns i Sverige och omvärlden och vilka krav det ställer. Bland annat föreslog man att hoten och riskerna inom informationssäkerhetsområdet borde utredas, vilket nu också sker i utredningen om att föreslå en strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och IT-system (NISU 2014, dir. 2013:110). I ett försvarspolitiskt sammanhang går beredningen vidare och konstaterar att Sveriges samlade förmåga att förebygga, motverka och aktivt hantera konsekvenserna av cyberhoten måste öka. Man anser bland annat att det internationella samarbetet ska utvecklas för att säkerställa en robustare cybersäkerhet.[97]

4.7 E-delegationens uppföljning av myndigheternas samlade arbete med e-förvaltning

E-delegationen har regeringens uppdrag att följa e-förvaltningsarbetet i statsförvaltningen. Vid två tillfällen har delegationen skickat ut en webbenkät för att följa upp utvecklingen.[98] Den första undersökningen gjordes 2011 och besvarades av 201 myndigheter. Den andra gjordes 2013 och besvarades av 137 myndigheter. Som en del av undersökningen ställdes ett antal frågor om informationssäkerhet. Frågorna, som var åtta till antalet, fokuserade på om och i så fall hur myndigheterna bedriver ett systematiskt informationssäkerhetsarbete. Frågorna var liknande de som MSB har ställt i sin uppföljning av LIS-föreskriften, men färre till antalet. Bilden som framkom tyder på en förbättring av det systematiska informationssäkerhetsarbetet från 2011 till 2013. Den samlade bilden av läget 2013 var dock lika problematisk som den som framträder i MSB:s uppföljning av LIS-föreskrifterna, det vill säga en stor andel myndigheter har inte ett systematiskt informationssäkerhetsarbete på plats.[99]

---

96 Departementspromemorian *Bättre regler för elektroniska kommunikationer* (Ds 2010:19).

97 Försvarsberedningen: *Vägval i en globaliserad värld* (Ds 2013:33) och *Försvaret av Sverige – Starkare försvar för en osäker tid* (2014: 20).

98 E-delegationen: *Uppföljning av myndigheternas arbete med e-förvaltning och e-tjänster 2011 respektive 2013*.

99 Uppgifterna från undersökningen är publicerade i rapporterna *E-delegationen, Uppföljning av myndigheternas arbete med e-förvaltning och e-tjänster 2011*, samt *Uppföljning av myndigheternas arbete med e-förvaltning och e-tjänster 2013*.

4.8 Sammanfattande iakttagelser

Iakttagelserna i detta kapitel visar att läget för informationssäkerheten är allvarligt i de delar av statsförvaltningen som det finns kännedom om, och att det varit så under lång tid. Därtill är kännedomen om läget lågt för större delen av statsförvaltningen. Detta bygger på det samlade underlag som Riksrevisionen gett i uppdrag till MSB, FRA och Säkerhetspolisen att ta fram. Underlaget är ny, unik information där var och en av delarna entydigt pekar i samma riktning, vilket ger bevisningen styrka.

Myndigheternas risk- och sårbarhetsanalyser lever inte upp till de krav som ställs när det gäller att redovisa informationssäkerhet. Bristerna är så omfattande att det inte går att ställa samman en gemensam bild av samlad förmåga att kunna motstå och hantera kriser inom informationssäkerhetsområdet. Det är även svårt att bilda sig en uppfattning om den enskilda myndighetens informationssäkerhet i ett flertal fall. Den trendrapport som MSB producerar behandlar risker och hot, men inte realiserade hot eller skyddsåtgärder.[100]

Många myndigheter brister i efterlevnad av LIS-föreskrifterna. E-delegationens uppföljning indikerade problem med informationssäkerhetsarbetet hos myndigheterna redan 2011. Verva följde aldrig upp efterlevnaden av föreskrifterna. MSB har inte hellerföljt upp myndigheternas tillämpning av LIS-föreskrifterna förrän 2014.

FRA:s underrättelseverksamhet är inriktad mot utländska hotaktörer av en viss dignitet som riktar sina operationer mot samhällsviktig verksamhet. Underrättelseverksamheten genererar en god kunskap om vilka hot som finns och indikerar vilka myndigheter som kan vara utsatta för angrepp. Underrättelseverksamheten genererar dock ingen kunskap om hur myndigheternas informationssäkerhet är beskaffad. FRA har tack vare sina IT-säkerhetsanalyser en god kunskap om hur läget är i en liten del av statsförvaltningen – i stort sett bland de myndigheter och bolag som har den mest skyddsvärda verksamheten. FRA underrättar dock inte regeringen om resultatet av respektive analys. FRA rapporterar heller inte bristerna på en aggregerad nivå.

Säkerhetspolisen har i sin tillsyn funnit systematiska brister i säkerhetsskyddsarbetet, framför allt i fråga om IT- och informationssäkerhet hos de mest skyddsvärda myndigheterna. Få myndigheter har varit föremål för Säkerhetspolisens tillsyn av informationssäkerhet. Säkerhetspolisen saknar därmed kännedom om statusen på merparten av myndigheterna i statsförvaltningen.

[100] Realiserade hot redovisas dock i viss utsträckning i särskilda händelserapporter.

Datainspektionens tillsyn avser visserligen informationssäkerhet, men har en annan utgångspunkt. Denna är att värna den personliga integriteten för dem som på något sätt är registrerade hos en myndighet eller ett företag.

Övriga myndigheter redovisar i liten utsträckning på eget initiativ om sin informationssäkerhet i årsredovisningen. Det förklaras naturligen av att det nästan aldrig finns som krav i regleringsbreven.

Endast i några få utredningar behandlas informationssäkerhet mer ingående. De två pågående utredningarna, om översyn av säkerhetsskyddslagen respektive en strategi för hantering och överföring av information i elektroniska kommunikationsnät och IT-system, har dock stor betydelse för informationssäkerheten i samhället.[101]

[101] Dir. 2011:94 respektive 2013:110.

5 Vilka åtgärder har regeringen vidtagit för att styra informationssäkerhetsarbetet?

För att undersöka vad regeringen vidtagit för åtgärder när det gäller informationssäkerhet har vi gått igenom olika typer av dokument som härrör från regeringen.[102] Riksrevisionen har sökt efter dokument innehållande såväl myndighetsövergripande styrning som mer specifik styrning av enskilda myndigheters informationssäkerhetsarbete. Det rör sig dels om rena styrdokument som särskilda regeringsuppdrag och regleringsbrev, dels om dokument som är bärare av styrsignaler som utredningsdirektiv, budgetpropositioner och vissa andra i sammanhanget relevanta propositioner. Dessutom tar vi upp hur Regeringskansliet har organiserat sin styrning av informationssäkerhet. Kapitlet svarar mot revisionsfrågan om regeringens styrning och kopplar till utgångspunkterna om grundläggande förutsättningar i form av krav och organisering samt beslut om nya eller förändrade åtgärder och införande och kontroll av åtgärdernas funktion.

5.1 Utredningsdirektiv

Riksrevisionen har gått igenom samtliga utredningsdirektiv för perioden 2007–2014. Sammanlagt identifierades 35 direktiv som vid en första anblick kunde ha bäring på styrningen av informationssäkerhet i statsförvaltningen. Av dessa 35 direktiv har Riksrevisionen identifierat tre stycken som har betydelse för styrningen av informationssäkerhetsarbetet i den civila statsförvaltningen på ett myndighetsövergripande sätt.[103] I ett av utredningsdirektiven finns informationssäkerhetsaspekter då uppdraget var att föreslå var vissa funktioner inom informationssäkerhetsområdet[104] skulle ha sin hemvist.[105]

---

[102] I kapitel 3 redogörs för regeringens styrning genom förordning.

[103] I 16 av 35 fall berör direktiven olika varianter av integritetsaspekter och behandling av personuppgifter på något sätt. Utredningsdirektiven avser därmed inte frågor om övergripande styrning av informationssäkerheten. I övriga 16 fall fanns ingen koppling till informationssäkerhet.

[104] CSEC som är Sveriges certifieringsorgan för IT-säkerhet, signatärskapet för de internationella organen CCRA och SOGIS-MRA samt Sitic som är Sveriges IT-incidentcentrum.

[105] Viss översyn av ansvarsfördelning och organisation när det gäller samhällets informationssäkerhet (dir. 2009:110).

Under denna gransknings gång har två pågående utredningar haft i uppdrag att hantera mer övergripande frågor som rör styrning och kravställning av informationssäkerhet.[106]

5.2 Regeringsuppdrag

Riksrevisionen har undersökt vilka eventuella regeringsuppdrag med anknytning till informationssäkerhet som har lämnats. Under perioden 2009 till 2014 har Riksrevisionen identifierat sex uppdrag som har lämnats till MSB och FRA och som har bäring på informationssäkerhet.

Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter

2009 fick MSB i uppdrag lämna förslag på åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter. MSB redovisade uppdraget 2010 och förslaget gick i huvudsak ut på att skapa ett nationellt operativt samverkanscenter lokaliserat på MSB. Ytterligare förslag var exempelvis att utreda obligatorisk IT-incidenthantering och tekniskt intrångsdetekterings- och varningssystem, att informationssäkerhet beaktas i risk- och sårbarhetsanalyser samt att ta fram en nationell plan för att hantera allvarliga IT-incidenter.

Nationell hanterandeplan för allvarliga IT-incidenter

2010 fick MSB i uppdrag att ta fram en nationell plan som klargör hur allvarliga IT-incidenter ska hanteras.[107] MSB redovisade uppdraget 2011 och har tagit fram en nationell plan för att hantera allvarliga IT-relaterade kriser.[108] Planen syftar till att underlätta för varje aktör genom att tillsammans med andra aktörer ta fram en gemensam lägesbild.[109]

System för obligatorisk IT-incidentrapportering för statliga myndigheter

2010 fick MSB i uppdrag av regeringen att utreda hur ett system för obligatorisk IT-incidentrapportering för statliga myndigheter kan utformas.[110] MSB redovisade 2011 ett förslag där systemet för incidentrapportering föreslogs införas stegvis och föregås av en pilotversion i mindre skala. MSB ansåg dock att ytterligare aspekter behövde utredas vidare varför MSB 2012 fick ett tillkommande uppdrag,

---

[106] En modern säkerhetsskyddslag (dir. 2011:94) samt Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system (dir. 2013:110).

[107] Regeringsbeslut Fö21010/701/SSK.

[108] MSB: *Nationell hanterandeplan för allvarliga IT-incidenter*, dnr 2010-4545, s. 26.

[109] MSB: *Nationell hanterandeplan för allvarliga IT-incidenter*, dnr 2010-4545, s. 28.

[110] Regeringsbeslut Fö2010/701/SSK.

vilket redovisades senare samma år.[111] MSB kunde konstatera att en viktig del i arbetet med samhällets informationssäkerhet är en systematisk, bred och samlad rapportering av IT-incidenter.[112] Frågan om ett eventuellt införande av obligatorisk IT-incidentrapportering är vilande i nuläget med hänvisning till ett eventuellt kommande krav från EU på att införa ett sådant system.[113]

Ett nationellt tekniskt IT-intrångsdetekterings- och varningssystem (TDV)[114]

I april 2010 gav regeringen MSB och FRA två uppdrag rörande ett tekniskt IT-intrångsdetekterings- och varningssystem. FRA fick i uppdrag att lämna förslag på hur ett sådant system kan utformas.[115] MSB fick i sin tur i uppdrag att lämna förslag på vilka aktörer som ska omfattas ett sådant system.[116] 2011 redovisade MSB sina förslag, och rekommenderade att alla statliga myndigheter som är särskilt utpekade i bilagan till krisberedskapsförordningen skulle erbjudas att delta i systemet. FRA föreslog i sin redovisning av uppdraget att det de mest känsliga verksamheterna som är utsatta för ett stadigvarande och högt underrättelsehot från kvalificerade aktörer borde prioriteras. FRA fick 2011 ett kompletterande uppdrag att inkomma med en mer detaljerad redovisning samt att utarbeta en pilotversion av systemet.[117] 2012 redovisade FRA sitt kompletterande uppdrag och pilotprojektet, vilket innebär att TDV i dagsläget finns i drift hos ett fåtal användare.[118] Ett införande i större skala är enligt FRA beroende av regeringens uppfattning om att gå vidare med att implementera systemet.[119]

Tillgänglig och skyddad kommunikationsinfrastruktur för offentlig sektor

2010 fick MSB i uppdrag av regeringen att lämna förslag på en säker digital informations- och kommunikationsinfrastruktur för myndigheter, kommuner och landsting.[120] 2011 lämnade MSB sitt förslag på hur en tillgänglig och skyddad kommunikationsinfrastruktur för offentlig sektor skulle kunna skapas. Förslaget går i huvudsak ut på att skapa en sammanhållande organisatorisk struktur med uppdrag att samordna, inrikta, ansvara för drift och förvalta. Vissa

---

[111] Regeringsbeslut Fö2012/717/SSK, Regeringsbeslut II:1.

[112] MSB: *Nationellt system för it-incidentrapportering*, dnr 2012-2637, s. 95.

[113] Prop. 2013/14:144, *Lag om sprängämnesprekursorer och redovisning av krisberedskapens utveckling, s. 53.*

[114] Ett TDV består mycket förenklat av sensorer, en kommunikationslösning och en central funktion för analys. Sensorerna analyserar trafik som passerar i nätverk för att identifiera IT-angrepp. Om ett angrepp upptäcks skickas ett larm som kan gå såväl till den verksamhet som är utsatt för IT-angreppet som till en analyscentral. (Källa: FRA 10 360:3409/12.)

[115] Regeringsbeslut Fö2010/703/SSK.

[116] Regeringsbeslut Fö2010/702/SSK.

[117] Regeringsbeslut Fö2011/1681/SSK.

[118] Rapport från FRA, dnr 10 360:3409/12.

[119] Intervjuer på FRA.

[120] Regeringsbeslut Fö2010/702/SSK.

delar av infrastrukturen ska enligt förslaget tillhandahållas genom staten och andra genom näringslivet.[121] Frågan bereds fortfarande inom Regeringskansliet.

Säkerhetsgranskning

2010 fick MSB i uppdrag att säkerställa att myndigheten ska ha möjlighet att utifrån analyser av förmågebedömningar, genomförda risk- och sårbarhetsanalyser samt bedömningar av beroendeförhållanden föreslå enskilda myndigheter att anlita FRA för IT-säkerhetsanalyser.[122] I sitt svar till Regeringskansliet pekar MSB på att man under 2010 har lyft upp och utvecklat sitt analysarbete när det gäller informationssäkerhetsaspekter i förmågebedömningarna och risk- och sårbarhetsanalyserna. MSB anger även att man kontinuerligt arbetar med att analysera och bedöma omvärldsutvecklingen inom informationssäkerhetsområdet och bygger genom detta upp ändamålsenligt underlag för beslut om att föreslå enskilda myndigheter att anlita FRA för IT-säkerhetsanalyser.[123]

Uppdrag i regleringsbrev till MSB

I regleringsbrevet för 2009 fick MSB i uppdrag att redovisa hur arbetet med risk- och sårbarhetsanalyser och förmågebedömningar har förenklats samt bedöma om ytterligare komponenter behövs för att skapa en sammantagen bedömning av samhällets krisberedskap.[124]

2011 fick MSB i uppdrag att sammanställa en övergripande samlad bedömning av förmågor respektive risker och sårbarheter på lokal, regional och nationell nivå samt inom samverkansområden.

2012 skulle MSB med utgångspunkt i föregående års uppdrag redovisa en vidareutveckling av den övergripande samlade bedömningen avseende förmågor, risker och sårbarheter. I bedömningen skulle även informationssäkerhet beaktas.[125]

2014 får MSB dessutom uppdraget att analysera rapporteringsfrekvensen av risk- och sårbarhetsanalysarbetet för att kunna effektivisera krisberedskapen.[126]

---

[121] MSB: *Tillgänglig och skyddad kommunikationsinfrastruktur för offentlig sektor*, dnr 2010-6304, s. 20 f.

[122] Regeringsbeslut Fö2010/701/SSK.

[123] MSB: *Säkerhetsgranskning*, dnr 2010-6308.

[124] Uppdrag 15 i regleringsbrev till MSB för 2009.

[125] Uppdrag 10 i regleringsbrev till MSB för 2012.

[126] Uppdrag 29 i regleringsbrev till MSB för 2014.

5.3 Regleringsbrev

Riksrevisionen har gått igenom regleringsbreven för 35 civila myndigheter i statsförvaltningen som inte är stöd- eller tillsynsmyndigheter på området. Myndigheterna har valts efter två kriterier: dels myndigheter som är särskilt viktiga ur skyddssynpunkt, dels myndigheter som har stora anslag (se bilaga 2). Genomgången omfattar regleringsbreven för 2010–2014. Syftet med genomgången har varit att undersöka i vilken mån regeringen har ställt krav på att myndigheterna ska rapportera status på sin informationssäkerhet. Riksrevisionen har valt att kategorisera regleringsbreven i kategorierna ja, nej och delvis och dessa redovisas nedan i tabell 5.1.

Tabell 5.1 Urval av myndigheter med informationssäkerhetsrelaterade krav i regleringsbrev (RB) 2010–2014

Kategorisering	RB 2010	RB 2011	RB 2012	RB 2013	RB 2014
Ja	0	0	0	0	0
Nej	21	21	20	25	21
Delvis	13	13	14	10	14
Totalt	**34**	**34**	**34**	**35**	**35**

För att regleringsbrevet ska kategoriseras som ja krävs att myndigheten uttryckligen uppmanas att rapportera om informationssäkerhet/IT-säkerhet/datasäkerhet. Riksrevisionen har inte funnit något sådant krav i regleringsbreven för någon myndighet under ovan nämnda period.

De regleringsbrev som kategoriseras som delvis är sådana där återrapporteringen exempelvis rör ett enskilt system eller en enskild fråga eller där återrapporteringen berör intern styrning och kontroll eller IT i stort. Antalet regleringsbrev som har kategoriserats som att de delvis berör återrapportering av informationssäkerhet i vid bemärkelse är 13–14 stycken per år med en lägsta notering på 9 under år 2013. Begreppen informationssäkerhet, IT-säkerhet eller datasäkerhet nämns dock inte i något av dessa regleringsbrev.

Andelen regleringsbrev som inte innehåller något krav alls att rapportera om myndighetens informationssäkerhet varierar mellan 60 och 70 procent för de åren som har undersökts.

Av genomgången framgår även att regeringen inte har ställt några krav på att myndigheterna ska uppnå en viss nivå av informationssäkerhet. Regeringen ställer dock i några fall krav på enskilda system eller viss specifik hantering. Undersökningen visar att det är Kriminalvården, Kronofogdemyndigheten, Länsstyrelserna och SCB som har den mest omfattande styrningen av IT genom regleringsbrev.

5.4 Budgetpropositioner

Riksrevisionen har gått igenom budgetpropositionerna för åren 2010 till 2014 i syfte att undersöka i vad mån dessa tar upp frågor om informationssäkerhet. Informationssäkerhet behandlas nästan uteslutande under utgiftsområde 6 Försvar och samhällets krisberedskap samt under utgiftsområde 22 Kommunikationer. Informationssäkerhet berörs även i begränsad omfattning under utgiftsområdena 4, 5, 9 och 14.

Regeringens skrivningar om inriktningen för samhällets informationssäkerhet följer i stora drag samma linje under 2010–2014. I budgetpropositionen för 2010 konstaterar regeringen att ett ändamålsenligt arbete med informationssäkerhet är av central betydelse för samhällsutvecklingen.[127] Regeringen betonar att det är väsentligt att integrera informationssäkerhetsfrågorna och se dem som en naturlig del i bedömningen av samhällets förmåga, i arbetet med risk- och sårbarhetsanalyser.[128] I jämförelse med ansvarsprincipen uttrycker regeringen att det finns ett behov att samla resurserna för att skapa goda förutsättningar för att förebygga IT-incidenter såväl som för att hantera dem när de inträffar. Regeringen anser även att rapporteringen av IT-incidenter behöver förbättras.[129] MSB pekas ut som den centrala aktören i det breda arbetet med informationssäkerheten i samhället, som kontinuerligt ska analysera och bedöma omvärldsutvecklingen avseende hot, sårbarheter och risker samt konsekvenser för viktiga funktioner i samhället.[130]

I budgetpropositionen för 2012 anges för första gången betydelsen av att anpassa skyddsåtgärder till hot och risker. Detta förutsätter dock enligt regeringen kännedom om hur många incidenter som inträffar och omfattningen av dessa. Sådan kunskap förstärker möjligheten till ett samlat agerande vid IT-incidenter där konsekvenserna bedöms bli omfattande. En obligatorisk IT-incidentrapportering kan enligt regeringen vara en del av det arbetet.[131] Betydelsen av informationssäkerhet, särskilt som en del i samhällets krisberedskap, betonas i samtliga budgetpropositioner. Detsamma gäller för stärkt samordning och samverkan för att driva informationssäkerhetsarbetet framåt.

I budgetpropositionen för 2013 återkommer regeringen till frågan om betydelsen av tillgång till kunskap om hur läget är. Regeringens bedömning är att information om det aktuella läget vid en allvarlig händelse är en förutsättning för att de inblandade aktörerna ska få en ömsesidig förståelse

[127] Prop. 2009/10:1, UO 6, s. 78.

[128] Prop. 2009/10:1, UO 6, s. 78.

[129] Prop. 2009/10:1, UO 6, s. 78.

[130] Prop. 2010/11:1, UO 6, s. 83.

[131] Prop. 2011/12:1, UO 6, s. 91.

för situationen och därmed kunna vidta samordnade åtgärder. Ett system för obligatorisk IT-incidentrapportering kan enligt regeringen bidra till detta. Regeringen ansåg också att ett tekniskt detekterings- och varningssystem (TDV) borde genomföras succesivt inom ramen för FRA:s verksamhet i syfte att stärka skyddet för samhällsviktig verksamhet.[132]

Regeringens syn på risk- och sårbarhetsanalyser

Risk- och sårbarhetsanalyser samt förmågebedömningar utgör enligt regeringen viktiga underlag för att möjliggöra en effektiv uppföljning, styrning och inriktning av den sammantagna krisberedskapen i samhället.[133]

Ett återkommande krav från regeringen i budgetpropositionerna är att kvaliteten på inlämnade analyser och bedömningar behöver höjas. Arbetet med risk- och sårbarhetsanalyser bör enligt regeringen bedrivas samordnat med riskanalyser som regleras i annan författning.[134] Regeringen efterlyser också metodstöd till aktörerna i hela den process som arbetet med risk- och sårbarhetsanalyser och förmågebedömningar innebär.[135] Kvalitetshöjningar av analyserna tillsammans med ett fullgott metodstöd bör enligt regeringen innebära ett mer enhetligt arbetssätt som i sin tur också möjliggör jämförbarhet mellan aktörer och en samlad bild av vilka sårbarheter och risker som finns.[136]

I budgetpropositionen för 2012 skriver regeringen att myndigheterna i större utsträckning bör tydliggöra prioriterade och planerade åtgärder utifrån identifierade risker.[137] Tanken återkommer i budgetpropositionen för 2014 där regeringen skriver att arbetet med risk- och sårbarhetsanalyser i högre grad bör fokusera på att följa upp om tidigare identifierade brister har åtgärdats.[138] Regeringen anser även att planering för att utveckla och upprätthålla en god krisberedskap bör utgöra en integrerad del av verksamhetsplaneringen hos myndigheter, kommuner och landsting.[139]

---

[132] Prop. 2012/13:1, UO 6, s. 99.

[133] Prop. 2010/11:1, UO 6, s. 16 f.

[134] Prop. 2010/11:1, UO 6, s. 73.

[135] Prop. 2010/11:1, UO 6, s. 74.

[136] Prop. 2010/11:1, UO 6, s. 73.

[137] Prop. 2011/12:1, UO 6, s. 79.

[138] Prop. 2013/14:1, UO 6, s. 93.

[139] Prop. 2013/14:1, UO 6, s. 93.

5.5 Övriga propositioner av relevans

Riksrevisionen har gått igenom 33 propositioner från och med 2007/2008 och framåt som vid en första anblick kan tänkas vara av relevans för styrning av informationssäkerheten i statsförvaltningen. I fyra av dessa 33 propositioner finns skrivningar som är intressanta ur ett övergripande informationssäkerhetsperspektiv.

I propositionen om behandling av personuppgifter inom studiestödsområdet uttalar regeringen att den tekniska infrastrukturen för den offentliga förvaltningens kommunikation med medborgarna bör bygga på internet.[140]

I ett remissvar på den utredning som legat till grund för propositionen om utökat elektroniskt informationsutbyte yttrade Riksrevisionen med hänvisning till sin tidigare granskning av informationssäkerhet[141] att formerna, metoderna och takten för ett utökat elektroniskt informationsutbyte borde övervägas noga. Skälet till det var de brister i informationssäkerhet som Riksrevisionen upptäckt i denna granskning. Regeringen uttalade dock att en god informationssäkerhet är ett ständigt pågående utvecklingsarbete, och att de problem Riksrevisionen påtalat i stället fortlöpande får tas om hand i annan ordning och att de inte utgör ett hinder för att genomföra ett utökat elektroniskt informationsutbyte. Regeringen framhöll också att det redan finns kontrollfunktioner för att råda bot på brister i informationssäkerheten, till exempel intern styrning och kontroll som granskas av såväl extern revision som i förekommande fall intern revision. Dessutom ska myndighetens ledning i anslutning till undertecknandet av årsredovisningen bedöma huruvida den interna styrningen och kontrollen är betryggande.[142]

I propositionen om stärkt krisberedskap, som utgör grund för regeringens inriktning av krisberedskapsarbetet från 2007/2008 och framåt, framgår målsättningar och inriktning för bland annat informationssäkerhet på en övergripande nivå. Regeringen slår fast att ansvarsprincipen även fortsättningsvis bör vara utgångspunkt för arbetet med krisberedskap, men att ett större fokus bör ligga på det tvärsektoriella perspektivet.[143] Regeringens uppgift är att ansvara för den övergripande samordningen, prioriteringen och inriktningen av samhällets krisberedskap medan ansvaret för operativa åtgärder av nationell karaktär ligger på central myndighetsnivå.[144] Att styra samhällets krisberedskap är en process som bygger på omvärldsanalys, forskning samt risk- och sårbarhetsanalyser. Utifrån dessa delar i processen

---

[140] Prop. 2008/09:96, *Behandling av personuppgifter inom studiestödsområdet*, s. 64.

[141] Riksrevisionen: *Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen* s(RiR 2007:10).

[142] Prop. 2007/08:160, *Utökat elektroniskt informationsutbyte*, s. 64 f.

[143] Prop. 2007/08:92, *Stärkt krisberedskap – för säkerhets skull*, s. 7 f.

[144] Prop. 2007/08:92, s. 14.

kan krisberedskapsarbetet inriktas och mål och förmågekrav anges, och med detta som utgångspunkt kan krisberedskapsarbetet följas upp och utvärderas. Denna process bör förstärkas och utvecklas så att regeringen får ett tydligt beslutsunderlag och en samlad bedömning av samhällets förmåga att motstå och hantera kriser.[145] Betydelsen av analyserna som underlag innebär enligt regeringen att det är viktigt att de håller en god kvalitet och är jämförbara och enhetliga.[146] Regeringen uttalade också att det vid tillfället utöver säkerhetsskyddslagstiftningen fanns få krav på hur myndigheterna ska hantera den tekniska säkerheten i sina IT-system, varför MSB bör få utfärda generella föreskrifter om ledningssystem för informationssäkerhet (LIS).[147]

I propositionen om lag om sprängämnesprekursorer och redovisning av krisberedskapens utveckling redovisar regeringen utvecklingen av krisberedskapsarbetet. Regeringen pekar på risk- och sårbarhetsanalysernas betydelse och efterlyser en högre grad av samordning av arbetet med risk- och sårbarhetsanalyser på lokal, regional och nationell nivå. Myndigheterna bör förtydliga och utveckla redovisningen av vidtagna åtgärder och uppnådd förmåga. Dessutom bör mer arbete läggas på att följa upp på vilket sätt tidigare brister har åtgärdats.[148] Vidare delar regeringen MSB:s uppfattning att det är nödvändigt att förbättra informationssäkerheten och robustheten i infrastruktur för att minska sårbarheten i samhällsviktig verksamhet.[149] Regeringen uttalar sig också om vikten av funktioner för samverkan och samordning inom och mellan samhällssektorer och ansvarsområden samt en tydlig nationell strategi med bred förankring i samhället.[150]

5.6 Strategier, agendor och handlingsplaner

Regeringen, och dess myndigheter på uppdrag av regeringen, har tagit fram ett antal strategier, agendor och handlingsplaner som berör informationssäkerhet.[151] Vi redogör här kortfattat för några av dessa som är mest relevanta för informationssäkerheten.

---

145 Prop. 2007/08:92, s. 39.

146 Prop. 2007/08:92, s. 40.

147 Prop. 2007/08:92, s. 36 f.

148 Prop. 2013/14:144, *Lag om sprängämnesprekursorer och redovisning av krisberedskapens utveckling*, s. 31.

149 Prop. 2013/14:144, s. 25.

150 Prop. 2013/14:144, s. 51.

151 MSB: *Strategi för samhällets informationssäkerhet 2010–2015, Samhällets informationssäkerhet – nationell handlingsplan 2012, Strategi för informationssäkerhet i e-förvaltning* (dnr 2012-3430), *Ett fungerande samhälle i en föränderlig värld – nationell strategi för skydd av samhällsviktig verksamhet* (2011) samt *Handlingsplan för skydd av samhällsviktig verksamhet* (2013).

Strategi och handlingsplan för samhällets informationssäkerhet

Syftet med strategin för samhällets informationssäkerhet är att ange långsiktiga målsättningar, färdriktningar och arbetssätt för informationssäkerhet i hela samhället. Strategin gäller för åren 2010–2015.

För att konkretisera strategin har MSB tillsammans med övriga SAMFI-myndigheter[152] tagit fram en handlingsplan. Planen är ett verktyg för myndigheterna i SAMFI att ta fram prioriterade åtgärder, och ska också ses som en efterföljare till den handlingsplan som publicerades 2008 av Krisberedskapsmyndigheten (KBM) på uppdrag av regeringen. De mål och åtgärder som anges i handlingsplanen är kopplade till fem strategiska områden som anges i strategin för samhällets informationssäkerhet.[153] Handlingsplanen omfattar totalt 27 stycken aktiviteter. Exempel på mål och åtgärder i handlingsplanen är:

Mål: Att samtliga myndigheter och andra som säkerhetsskyddsförordningen omfattar har fått information om skyldigheten att undersöka vilken verksamhet som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skydd mot terrorism. *Åtgärder:* Samtliga myndigheter ska ges särskild information om gällande skyldighet att genomföra säkerhetsanalyser enligt säkerhetsskyddsförordningen, samt om kopplingen till riskhantering med utgångspunkt i MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10).

Mål: Det ska finnas en generisk modell för kontinuitetsplanering med väldefinierade begrepp som går att anpassa till olika verksamheters behov. *Åtgärder:* En analys genomförs som beskriver dels behoven av kontinuitetsplanering ur informationssäkerhetssynpunkt, dels hur området relaterar till exempelvis krisberedskap och samordning vid allvarliga IT-incidenter. Därefter utarbetas förslag på generiska metoder för kontinuitetsplanering ur denna aspekt som också går att synkronisera med en organisations övergripande kontinuitetsplanering.

Mål: Tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor. *Åtgärder:* Fortsatt arbete med tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor.

---

[152] Samverkansgruppen för informationssäkerhet (SAMFI). I SAMFI samarbetar de flesta myndigheter som av regeringen fått ett särskilt utpekat ansvar för olika aspekter av informationssäkerhet i samhället. Följande myndigheter samverkar inom SAMFI: Myndigheten för samhällsskydd och beredskap (MSB), Post- och telestyrelsen (PTS), Försvarets radioanstalt (FRA), Säkerhetspolisen, Rikskriminalpolisen (RKP), Försvarets materielverk (FMV), Sveriges Certifieringsorgan för IT-säkerhet (CSEC) samt Försvarsmaktens militära underrättelse- och säkerhetstjänst (MUST).

[153] Informationssäkerhet i verksamheter, kompetensförsörjning, informationsdelning, samverkan och respons, kommunikationssäkerhet och säkerhet i produkter och system.

Enligt MSB kommer större delen av åtgärderna i handlingsplanen att vara genomförda vid periodens slut.[154]

Strategi för informationssäkerhet i e-förvaltning

E-delegationen har med anledning av sitt uppdrag från regeringen tagit fram en strategi för informationssäkerhet i e-förvaltning. I inledningen till strategin anges att trots informationssäkerhetens betydelse som framgångsfaktor för svensk e-förvaltning finns det ännu inte etablerade former för hur säkerhetsarbetet ska bedrivas i de e-förvaltningstjänster som alltmer tar form. Ett gemensamt säkerhetsarbete är därför nödvändigt och i detta arbete bör tyngdpunkten ligga på ledning, styrning och analys. En tydlig styrning ger också underlag för att välja rätt tekniska åtgärder. De strategiska mål som anges är följande.

- Den enskilde känner tillit till att informationshantering i myndigheters, landstings och kommuners e-tjänster sker på ett sådant sätt att personlig integritet förenas med hög tillgänglighet, spårbarhet och riktighet.
- All informationshantering i e-förvaltning sker med de säkerhetsåtgärder som definieras utifrån risk- och sårbarhetsanalys samt informationsklassning.
- En god säkerhetskultur och gemensamt regelverk finns så att information behandlas med samma krav på säkerhet oavsett vilken myndighet, vilket landsting eller vilken kommun som tillhandahåller eller använder en e-tjänst.
- Tydlig ansvarsmodell för styrning och uppföljning av informationssäkerhet inom e-förvaltning är etablerad på nationell nivå.
- Samhällsviktiga funktioner som stöds av e-tjänster upprätthålls även i krisläge. Detta förutsätter väl utvecklade metoder för kontinuitetsplanering.
- Processer finns inom e-förvaltningsarbetet för att skapa en nationell informationssäkerhetsrelaterad lägesbild.
- Informationssäkerhet i enlighet med informationens krav på skyddsnivå upprätthålls även då information kommuniceras till och från enskilda.

IT i människans tjänst – en digital agenda för Sverige

Med utgångspunkt från målet för IT-politiken har regeringen beslutat om en digital agenda. Agendan pekar ut behov av insatser inom fyra strategiska områden med utgångspunkt i användarens perspektiv. Dessa är att det ska vara lätt och säkert att använda IT-tjänster och att de skapar nytta, att det behövs infrastruktur samt IT:s roll för samhällsutvecklingen. För att nå det övergripande målet krävs enligt regeringen att utvecklingen inom alla områden kontinuerligt följs upp och

[154] Intervju på MSB 2014-01-15.

analyseras. Då det inte finns någon statlig myndighet som ensam ansvarar för de IT-politiska frågorna har därför regeringen tillsatt Digitaliseringskommissionen.[155] Kommissionen har hittills avlämnat två betänkanden.[156]

Strategi och handlingsplan för skydd av samhällsviktig verksamhet

Strategin för skydd av samhällsviktig verksamhet syftar till att skapa en förbättrad förmåga att motstå och återhämta sig från allvarliga störningar i samhällsviktig verksamhet. Syftet med strategin är också att skapa förutsättningar för att samhället ska fortsätta fungera på en acceptabel nivå vid allvarliga händelser och störningar.[157]

Målet med handlingsplanen är att konkretisera strategin genom att initiera åtgärder och aktiviteter för att skapa förutsättningar för att all samhällsviktig verksamhet har integrerat ett systematiskt säkerhetsarbete i sin verksamhet på lokal, regional och nationell nivå senast 2020. Handlingsplanen är uppdelad i två delar: åtgärder för kunskapsutveckling samt aktiviteter för implementering av ett systematiskt säkerhetsarbete.[158] Åtgärdsdelen för kunskapsutveckling får, genom grunder och regelverk, forskning, utbildning och övning, störst betydelse i början då det finns ett behov av att öka kunskapen om samhällsviktig verksamhet. Arbetet kommer att ske inom ramen för MSB:s ordinarie verksamhet och i samverkan med berörda aktörer. Aktivitetsdelen för implementering av ett systematiskt säkerhetsarbete bygger på att MSB tillsammans med berörda aktörer skapar de förutsättningar och det stöd som behövs för att ägare och verksamhetsutövare av samhällsviktig verksamhet ska kunna nå målet år 2020. I handlingsplanen nämns att ett systematiskt informationssäkerhetsarbete i hela samhället är viktigt för att skydda samhällsviktig verksamhet.

5.7 Regeringskansliets organisation för att hantera informationssäkerhet

Regeringskansliet är den myndighet under regeringen som förbereder regeringens ärenden och i övrigt är regeringen behjälplig. I Regeringskansliet har varje fackdepartement på regeringens vägnar ansvar för att följa upp sina respektive myndigheters informationssäkerhetsarbete. I praktiken innebär det att varje myndighetshandläggare hanterar frågor som handlar om myndighetens informationssäkerhet. Detta förutsätter dock

---

[155] Regeringskansliet: *IT i människans tjänst – en digital agenda för Sverige*, s. 18.

[156] *En digital agenda i människans tjänst – en ljusnande framtid kan bli vår* (SOU 2014:13) samt *Sveriges digitala ekosystem, dess aktörer och drivkrafter* (SOU 2013:31).

[157] MSB: *Ett fungerande samhälle i en föränderlig värld – Nationell strategi för skydd av samhällsviktig verksamhet*, 2011.

[158] MSB: *Handlingsplan för skydd av samhällsviktig verksamhet*, december 2013.

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.

Hur frågor som berör informationssäkerhet fördelas mellan departementen avgörs tydligast av den ansvarsfördelning som är fastställd i en bilaga till Regeringskansliets instruktion.[159] Beroende på vad informationssäkerhetsfrågan handlar om styrs den till det departement som huvudsakligen berörs. Ett ärende som rör flera departements verksamhetsområden ska handläggas inom det departement till vilket det huvudsakligen tillhör och beredas i samråd med övriga berörda statsråd (gemensam beredning).[160]

Inget departement har egentligen ansvar för att ta fram en samlad och aktuell bild av läget för informationssäkerheten i statsförvaltningen. Däremot finns det ett uttalat samordningsansvar för vissa specifika informationssäkerhetsfrågor. Exempelvis är Näringsdepartementet samordningsansvarigt för frågor som rör elektronisk kommunikation. Finansdepartementet å sin sida är ansvarigt för frågor som rör intern styrning och kontroll, men inte för intern styrning och kontroll inom specifika tillämpningsområden såsom informationssäkerhet.

Det finns inom Regeringskansliet ingen funktion eller formellt nätverk som enbart ansvarar för informationssäkerhetsfrågor och stöd till andra enheter inom detta område när det gäller regeringens styrning av myndigheterna. Departementen har inte heller några särskilt utsedda handläggare som analyserar behovet av styrning av informationssäkerhet. Sammantaget innebär detta att det inte finns någon funktion inom Regeringskansliet med uppgift att göra en samlad analys av det som rapporteras till regeringen om informationssäkerhet.

5.8 Sammanfattande iakttagelser

Genomgången av *utredningsdirektiv* visar att flertalet av de som berör informationssäkerhet endast gör det i begränsad omfattning. Regeringen har dock tillsatt två nu pågående utredningar som har direkt bäring på kravställning och styrning av informationssäkerhet i statsförvaltningen.

Regeringen har gett FRA och MSB flera *uppdrag* med stor betydelse för informationssäkerheten i statsförvaltningen. En obligatorisk IT-incidentrapportering och införandet av teknisk detekterings- och varningssystem (TDV) skulle enligt Riksrevisionen förmodligen avsevärt stärka

[159] Bilaga till förordningen (1996:1515) med instruktion för Regeringskansliet.

[160] 15 § förordningen (1996:1515) med instruktion för Regeringskansliet.

informationssäkerhetsarbetet genom att ge en bild av vad som faktiskt händer ute på myndigheterna. Inget av dessa två förslag har ännu genomförts; de bereds fortfarande i Regeringskansliet. Även frågan om tillgänglig och skyddad kommunikationsinfrastruktur bereds ännu i Regeringskansliet.

Av genomgången framgår att regeringen i liten utsträckning har informerat sig om status på informationssäkerheten genom *regleringsbrev*. Regeringen har i regleringsbreven heller inte ställt krav på myndigheternas nivå för informationssäkerhet. I de fall regleringsbreven innehåller krav på IT handlar det mer om effektivisering av myndighetens IT eller krav på enskilda system. Riksrevisionen har också ställt frågan till Regeringskansliet om det finns *särskilda regeringsbeslut* som avser informationssäkerhet, och fått till svar att det inte finns.

Budgetpropositionerna tar upp informationssäkerhet på en övergripande nivå – regeringen betonar vikten av en god informationssäkerhet i statsförvaltningen.

Risk- och sårbarhetsanalyser samt förmågebedömningar utgör enligt regeringen viktiga underlag för att möjliggöra en effektiv uppföljning, styrning och inriktning av den sammantagna krisberedskapen i samhället. Påpekandena om brister i risk- och sårbarhetsanalyserna har gjorts under flera år.

Av genomgången framgår att regeringen inte i någon större utsträckning har använt sig av *andra propositioner* för att styra informationssäkerhetsarbetet. Propositionen om stärkt krisberedskap och bildandet av MSB är egentligen det enda exemplet på en mer direkt styrning. Propositionen om krisberedskapens utveckling utgör mer indirekt styrning i form av uttalanden om betydelsen av god informationssäkerhet.

Riksrevisionens bedömning av *handlingsplanen för informationssäkerhet* är att mål och åtgärder är av blandad karaktär. En hel del av åtgärderna är sådana som faller inom ramen för myndigheternas ordinarie verksamhet och ansvar. Vissa mål och åtgärder är väldigt blygsamma, exempel på det är skrivningarna om kommunikationsinfrastruktur. Andra mål och åtgärder är sådant som enligt Riksrevisionen redan borde ha varit genomfört. Ett sådant exempel är generisk modell för kontinuitetsplanering.

Strategin och handlingsplanen för skydd av samhällsviktig verksamhet kommer att innefatta informationssäkerhet, men frågan behandlas väldigt summariskt i handlingsplanen.

Det finns ingen central funktion i Regeringskansliet med ett utpekat ansvar för att dels vara mottagare av strategiskt viktig information som underlag för styrning från regeringens sida, dels bereda ärenden som rör informationssäkerheten i statsförvaltningen. Beredningen blir onödigt omständlig och mer tidskrävande. Det kan göra det svårare att kraftsamla och att reagera snabbt vid behov.

6 Slutsatser och rekommendationer

Riksrevisionen har granskat om informationssäkerheten i den civila delen av statsförvaltningen är ändamålsenlig utifrån ökande hot. För att informationssäkerhetsarbetet i statsförvaltningen ska vara effektivt krävs enligt Riksrevisionen

- grundläggande förutsättningar i form av ett ändamålsenligt regelverk, tydliga roller och ansvar, samt krav på och organisering av ett systematiskt och processinriktat arbetssätt
- systematiska analyser av hot och risker, såväl på organisationsnivå som på ett övergripande plan
- att ansvariga aktörer vid behov beslutar om nya eller förändrade säkerhetsåtgärder, ser till att åtgärderna införs och slutligen kontrollerar säkerhetsåtgärdernas funktion
- systematisk och regelbunden uppföljning som ger underlag för förbättringar.

Syftet med granskningen har inte varit att undersöka hur enskilda myndigheter arbetar med informationssäkerhet eller att bevisa omfattningen av brister i informationssäkerheten. I granskningen har regeringen och dess stöd- och tillsynsmyndigheter för informationssäkerhet ingått.

6.1 Slutsatser

Riksrevisionens samlade slutsats av denna granskning är att arbetet med informationssäkerheten inte är ändamålsenligt sett till de hot och risker som finns. En stor del av den information som skapas och lagras i samhället är viktig och samtidigt känslig. Är informationen förlorad, stulen, manipulerad eller spridd till obehöriga kan det få allvarliga följder. Konsekvenserna spänner från att det kan drabba hela samhällsfunktioner till att drabba enskilda. Granskningen har visat på omfattande brister i statsförvaltningen. Regeringen har inte heller någon samlad lägesbild som inkluderar hot, i vilken omfattning och mot vilka hoten realiseras samt vilka skyddsåtgärder myndigheterna vidtar. Det har inte heller någon av regeringens stöd- och tillsynsmyndigheter. Det innebär att den samlade förmågan att kunna hantera de konsekvenser som kan bli följden av en allvarlig incident till stora delar är okänd. Av det skälet är det nödvändigt att regeringen och dessa myndigheter vidtar åtgärder, så att det går

att få en samlad bild av läget och utifrån detta anpassa säkerheten till de behov som finns.

Riksrevisionens granskning har visat att

- regeringen inte utövat en effektiv styrning av informationssäkerheten i den civila statsförvaltningen och
- regeringens stöd- och tillsynsmyndigheter endast delvis har vidtagit nödvändiga åtgärder för att informera sig och regeringen om vilka hot som finns mot den civila statsförvaltningen, i vilken omfattning de realiseras och vilka skyddsåtgärder som vidtas.

Riksrevisionen drar denna slutsats mot följande bakgrund. Riksrevisionen har som ett led i granskningen uppdragit åt MSB, FRA och Säkerhetspolisen att hämta in och analysera uppgifter om läget för informationssäkerheten i statsförvaltningen. Redovisningen av dessa uppdrag innebär väsentlig, ny information om läget. Vart och ett av myndigheternas yttranden pekar dessutom entydigt i samma riktning.

I det följande redovisas de slutsatser som Riksrevisionen dragit till följd av denna granskning.

Lägets allvar

Riksrevisionen kan konstatera att läget är allvarligt för de myndigheter som fått sina skydd testade mot intrång av FRA, och även för flera av de myndigheter vars säkerhetsskydd kontrollerats av Säkerhetspolisen. Enbart det faktum att myndigheterna har ett ansvar för sin informationssäkerhet verkar inte vara tillräckligt för att uppnå en god informationssäkerhet i statsförvaltningen.

Säkerhetspolisen har i sin tillsyn funnit systematiska brister i säkerhetsskyddsarbetet, framför allt i fråga om IT- och informationssäkerhet hos de mest skyddsvärda myndigheterna. Det handlar till exempel om skadekonsekvensbeskrivningar som antingen saknas eller innehåller ekonomiska eller andra konsekvenser för den egna verksamheten i stället för de som rör rikets säkerhet eller terrorism. Det kan också handla om att det saknas förmågebedömningar av tänkta angripare, vilket medför att det blir oklart hur informationssäkerheten ska dimensioneras. Dessa brister leder sammantaget till att dessa myndigheter inte kan ta fram ändamålsenliga kravspecifikationer för att värna de mest skyddsvärda informationstillgångarna. Riksrevisionen kan konstatera att det är betydande brister i säkerhetsarbetet som har upptäckts.

FRA:s penetrationstester som sker på begäran av en myndighet visar på att säkerhetsnivån är otillräcklig på flertalet av de myndigheter som blivit testade. FRA testar dessutom på detta sätt informationssäkerheten på en avgränsad del av statsförvaltningen, vilket innebär att FRA saknar kännedom om statusen

på informationssäkerhet för merparten av myndigheterna i statsförvaltningen. Om inte ens de mest skyddsvärda verksamheterna har ägnat frågan tillräcklig uppmärksamhet är risken stor att motsvarande brister återfinns även i övriga förvaltningen.

Bristande kännedom

Riksrevisionen kan konstatera att statusen på kunskapsläget för informationssäkerheten i statsförvaltningen är oklart. Varken regeringen eller någon av stöd- och tillsynsmyndigheterna har en bra och systematiskt underbyggd lägesbild, vilket är en förutsättning för att kunna säkerställa att man vidtar rätt åtgärder.

För att arbetet med informationssäkerhet i förvaltningen ska vara effektivt krävs kunskap om såväl hot och risker som vilka hot som förverkligas och vilka skyddsåtgärder myndigheterna vidtar. Regeringen har organiserat arbetet på ett sätt som gör att man får kunskap om hot och risker på en övergripande nivå. Genom säkerhetspolisens tillsyn får man även kunskap om realiserade hot och vidtagna skyddsåtgärder för de mest samhällskritiska verksamheterna. Vilka hot eller risker som realiseras mot de myndigheter som inte omfattas av säkerhetsskyddslagstiftningen eller vilka skyddsåtgärder dessa myndigheter vidtar finns dock ingen myndighet som kontrollerar. Regeringen har inte heller genom regleringsbrev eller på annat sätt krävt att myndigheterna lämnar sådan information. MSB och FRA har i avrapporteringen av regeringsuppdragen om obligatorisk incidenthantering och ett tekniskt detektering- och varningssystem uttryckt att dessa åtgärder åtminstone delvis skulle kunna ge sådan information. Dessa frågor bereds fortfarande i Regeringskansliet, flera år efter att behovet uttryckts. Regeringen har alltså i visst avseende styrt mot en förbättrad säkerhet genom att ge dessa myndigheter uppdrag. När sedan uppdragen redovisats blir de liggande länge i Regeringskansliet utan åtgärd, vilket försvårar att få till stånd en gemensam lägesbild att utgå från när säkerheten ska förbättras. Eftersom varken regeringen eller stöd- och tillsynsmyndigheterna i dag har den fulla bilden av i vilken omfattning hot realiseras eller vilka skyddsåtgärder myndigheterna vidtar, kan Riksrevisionen konstatera att en nödvändig förutsättning för ett effektivt arbete med informationssäkerhet saknas.

Myndigheternas risk- och sårbarhetsanalyser har omfattande brister när det gäller informationssäkerhet. Trots att det ställs uttryckliga krav på att informationssäkerhet ska beaktas i analyserna, är det inte alla myndigheter som gör det. Det är stora variationer mellan myndigheter på hur analyserna struktureras. Av dessa skäl är det svårt att aggregera informationen från flera myndigheter, vilket gör det omöjligt att upprätta en gemensam lägesbild av informationssäkerheten på central nivå. Detta leder i sin tur till att det blir svårt att analysera vilka brister som finns och därmed kunna göra en grundlig

riskbedömning. Då blir det naturligtvis också svårt att vidta lämpliga åtgärder för att bygga upp nödvändig förmåga.

Regeringen har uttalat att kvaliteten på risk- och sårbarhetsanalyserna behöver höjas. Regeringen ställer dock inte några specifika krav på myndigheternas analyser, utöver det som följer av krisberedskapsförordningen. MSB har fått i uppdrag att analysera och vidareutveckla sitt arbete med risk- och sårbarhetsanalyser och förmågebedömningar. Regeringen har inte talat om när analyserna ska uppnå tillräcklig kvalitet. I stället upprepar regeringen årligen i budgetpropositionen att arbetet med analyserna måste förbättras.

Både Säkerhetspolisen, genom sin tillsyn, och FRA, genom sin stödjande och rådgivande verksamhet, får kunskap om brister i enskilda myndigheters informationssäkerhet. Ingen av myndigheterna har dock lämnat någon mer aggregerad redovisning av bristerna och vilken status det är på myndigheternas informationssäkerhet till Regeringskansliet. Ett skäl som anges till varför så inte har skett är att det saknas en naturlig mottagare i Regeringskansliet. Riksrevisionen anser dock att både Säkerhetspolisen och FRA borde ha lämnat en sådan aggregerad redovisning till sina respektive huvudmän i Regeringskansliet för att tydliggöra problembilden. Genom att myndigheten överlämnar problembilden får regeringen bättre möjligheter att agera.

MSB har i sin rapportering till regeringen uttryckt att en obligatorisk incidentrapportering är nödvändig för att bedriva ett effektivt arbete med informationssäkerhet i samhället. Någon sådan skyldighet har ännu så länge inte införts. MSB har heller inget mandat att utöva tillsyn över myndigheternas informationssäkerhet. Avsaknaden av dessa verktyg försvårar för MSB att arbeta effektivt.

Det finns sedan fem år föreskrifter för ledningssystem för informationssäkerheten (LIS) utfärdade av MSB. Dessförinnan fanns motsvarande föreskrifter i kraft sedan 2008 utfärdade av Verva. LIS-föreskrifterna ska stödja uppbyggnaden och vidmakthållandet av informationssäkerheten på myndigheterna. Efterlevnaden har visat sig dålig när MSB 2014 utvärderade föreskrifterna då inte ens hälften av myndigheterna, enligt Riksrevisionens bedömning, kan anses uppfylla kraven i föreskrifterna. Riksrevisionen anser att detta talar starkt för att många myndigheter inte prioriterar informationssäkerheten. Det tyder också på att utfärdande av föreskrifter behöver kompletteras med ett uppföljnings- eller tillsynsansvar. Riksrevisionen anser att utvärderingen borde ha skett tidigare, inte minst mot bakgrund av att ett fungerande ledningssystem är avgörande för att uppnå god informationssäkerhet.

Regelsystemet för informationssäkerhet ser i huvudsak likadant ut i dag som det gjorde 2007 när Riksrevisionen senast granskade området. De brister som påpekades då kvarstår i stora drag även i dag, vilket innebär brister i

regeringens styrning. Ett tydligt och väl anpassat regelverk är en förutsättning för att uppnå effektivitet i arbetet med informationssäkerhet. Riksrevisionen drar därför slutsatsen att det regelverk som styr myndigheternas arbete med informationssäkerhet bättre kan behöva anpassas till olika typer av statlig verksamhet för att kunna nå önskvärda mål.

Regeringens åtgärder otillräckliga

Regeringen har på flera fronter uppmärksammat och betonat hur angeläget det är att myndigheterna har en hög informationssäkerhet. Detta har uttalats såväl i propositioner till riksdagen, i styrdokument ställda till myndigheterna som genom uttalanden i media. Även utredningsbetänkanden och departementspromemorior tar upp frågan. Regeringen har också tillsatt utredningar som berör informationssäkerheten. Frågan om informationssäkerhet är alltså i hög grad aktualiserad av regeringen, men trots det finns det stora brister.

Ett skäl till problemen att få till stånd en bättre informationssäkerhet är sannolikt att det inte finns någon funktion som ansvarar för informationssäkerheten som helhet i statsförvaltningen, inklusive Regeringskansliet, och som är mottagare av viktig information om denna. Inte heller har något av statsråden ett uttalat ansvar för just informationssäkerheten i statsförvaltningen. I dag hanteras frågor om informationssäkerhet antingen på det departement som respektive myndighet lyder under eller bereds i samråd med andra departement. Till saken hör att informationssäkerhet är en dimension som spänner över hela statsförvaltningen och dessutom har bäring på flera funktioner såsom förvaltningspolitik, intern styrning och kontroll, krishantering samt brottsbekämpning. Beroende på vilken funktion som anses mest styrande kommer ansvaret för att samordna ärendet att variera mellan olika departement. Överväger det förvaltningspolitiska samordnar Socialdepartementet, är det intern styrning och kontroll är Finansdepartementet samordningsansvarig, är det fråga om krishantering ligger ansvaret på Försvarsdepartementet[161] och gäller det brottsbekämpning är Justitiedepartementet ansvarigt. Dessa förhållanden gör att i praktiken är det inget departement som har ett samlat ansvar för informationssäkerheten i statsförvaltningen. Det innebär att det inte finns en given funktion i Regeringskansliet som kan stå för styrning och samordning av informationssäkerheten, såsom fallet är med till exempel krisberedskap där ett visst departement har ett utpekat ansvar. Det betyder dessutom att det saknas en självklar mottagare av information i Regeringskansliet när det gäller informationssäkerhet. Riksrevisionen anser att detta är en brist som orsakar svårigheter att styra och följa upp statusen på myndigheternas informationssäkerhet.

[161] Sedan den nya regeringen tillträtt i oktober 2014 har ansvaret för krishantering flyttats till Justitiedepartementet (inrikesministern).

Stöd- och tillsyn inte tillräckligt

Regeringens tillsyns- och stödmyndigheter, framför allt MSB, Säkerhetspolisen och FRA, är på olika sätt aktiva när det gäller informationssäkerhet. MSB verkar brett över hela den offentliga sektorn med uppdrag att främja en god informationssäkerhet, men har inte till uppgift att utöva tillsyn över informationssäkerheten i enskilda myndigheter. Rikspolisstyrelsen genom Säkerhetspolisen utövar tillsyn, men har av resursskäl inte möjlighet att göra det i hela förvaltningen utan har inriktat sin tillsyn på de myndigheter som har den allra mest skyddsvärda verksamheten. FRA agerar endast på begäran av enskilda myndigheter, och har i praktiken inte möjlighet att testa säkerheten på alla myndigheter. Dessa myndigheter samverkar också tillsammans med PTS, Försvarsmakten och Försvarets materielverk när det gäller informationssäkerhet (SAMFI).

Trots dessa myndigheters verksamhet och samverkan visar granskningen att det skulle behöva göras mer, och att myndigheterna saknar mandat för det. Säkerhetspolisen bedriver viss tillsyn inriktad på särskilt skyddsvärd verksamhet, vilket utgör en mindre del av den samlade statsförvaltningen. MSB utfärdar föreskrifter om ledningssystem för informationssäkerhet (LIS), men har inte till uppgift att utöva tillsyn över myndigheters arbete med informationssäkerhet. Datainspektionen utövar tillsyn, men utifrån ett avgränsat perspektiv och i en begränsad omfattning. Riksrevisionen bedömer att resurser för tillsyn generellt inte har prioriterats i tillräcklig utsträckning.

Oklart resursläge

När det gäller stödet till myndigheterna finns ett par resursaspekter som Riksrevisionen anser värda särskild uppmärksamhet.

Den första aspekten är att det saknas en samlad avvägning för staten hur mycket resurser som behöver satsas på skyddsåtgärder sett till de risker som finns. Som det nu är finns inte en samlad riskvärdering; i stället råder osäkerhet om hur starkt skyddet är, vilka händelser som ägt rum och hur hoten utvecklas. Med en samlad lägesbild framtagen hade det gett förutsättningar för en samlad värdering av riskerna och sannolikheten att hot realiseras. Detta hade i sin tur kunnat vägas mot hur omfattande stödet behöver vara. Inträffade händelser (se kapitel 2) har visat att kostnaderna kan bli betydande dels för att hantera händelsen, dels för att ställa till rätta efteråt. Risker för informationssäkerheten kan således potentiellt leda till omfattande skada, inte minst i form av extra kostnader. Därför är det angeläget att åtgärder vidtas och prioriteras för att kontrollera dessa risker.

Den andra aspekten är att i dag har varje myndighet ett eget ansvar för hela sin verksamhet i såväl normalläge som i krisläge, vilket självfallet är

helt nödvändigt för att verksamheten ska kunna bedrivas effektivt. Det är dock sannolikt inte tillräckligt; de flesta myndigheter har svårt att rekrytera och upprätthålla den kompetens som behövs för att möta behoven. De av regeringen utpekade stödmyndigheterna har begränsade resurser och saknar möjlighet att lämna operativt stöd till enskilda myndigheter i någon större utsträckning. Det finns alltså behov av ett bättre utbyggt stöd som riktar sig till hela statsförvaltningen, och som kompletterar de enskilda myndigheternas egen kompetens. Om så vore fallet skulle det kunna leda till en bättre säkerhet totalt i statsförvaltningen, samtidigt som den totala kostnaden för informationssäkerhet borde bli väsentligt lägre än om varje myndighet håller sig med specialistkompetens.

6.2 Rekommendationer

Denna granskning har visat att det råder oklarhet om läget i informationssäkerheten i statsförvaltningen. Med anledning av detta lämnar Riksrevisionen följande rekommendationer till regeringen och regeringens stöd- och tillsynsmyndigheter.

6.2.1 Rekommendationer till regeringen

Granskningen har visat ett betydande kunskapsunderskott när det gäller läget för informationssäkerheten i statsförvaltningen. Den tillsyn som sker inriktas i stort sett endast mot den mest skyddsvärda verksamheten – merparten av den civila statsförvaltningen lämnas utan tillsyn. Åtgärder vidtas inte alltid efter genomförda inspektioner. Det saknas också en systematisk och obligatorisk rapportering av incidenter. Allt detta leder till att det blir omöjligt att fånga den verkliga bilden av tillståndet för informationssäkerheten. Därav följer att det inte finns tillräckligt beslutsunderlag för att vidta nödvändiga åtgärder för att möta hoten och riskerna.

För att förbättra statens informationssäkerhet rekommenderar Riksrevisionen därför regeringen följande:

- Utöka tillsynen av informationssäkerheten i den civila statsförvaltningen, så att den omfattar väsentligt mer än endast de allra mest skyddsvärda delarna.
- Låt utreda om regelverket som styr arbetet med informationssäkerheten är ändamålsenligt i sin nuvarande utformning och om ansvaret för att utöva tillsyn över informationssäkerheten i den civila statsförvaltningen kan samlas och koordineras på ett bättre sätt än i dag. Dessa brister konstaterade Riksrevisionen redan 2007, och då bristerna fortfarande inte är åtgärdade är det angeläget med en skyndsam hantering.

- Överväg att låta tillsynsmyndigheten få mandat att utfärda sanktioner mot myndigheter som inte vidtar nödvändiga åtgärder efter en tillsyn som visat på brister.
- Inför snarast en obligatorisk incidentrapportering för samtliga myndigheter. Ge en myndighet i uppdrag att hantera denna rapportering.

Det finns ingen samlad central funktion i Regeringskansliet med ansvar för att bereda frågor om informationssäkerhet i statsförvaltningen. I dag hanteras ärenden rörande informationssäkerhet på flera departement beroende på ärendets karaktär (intern styrning och kontroll, förvaltningspolitik, krishantering, infrastruktur, etc.). Riksrevisionen anser att informationssäkerhet är en viktig strategisk fråga för hela statsförvaltningen, att det krävs kraft i styrningen för att skyddet ska kunna höjas till en ändamålsenlig nivå. För att skapa bättre förutsättningar för en effektiv styrning i informationssäkerhet rekommenderar därför Riksrevisionen följande:

- Se till att det finns en funktion och en process i Regeringskansliet med syfte att samlat hantera informationssäkerheten. Denna funktion, och process, ska kunna bereda alla de ärenden regeringen måste besluta om för att öka informationssäkerheten i statsförvaltningen. Funktionen ska också vara mottagare av MSB:s information om en samlad lägesbild och annan nödvändig information om läget för informationssäkerheten i statsförvaltningen.

6.2.2 Rekommendationer till regeringens stöd- och tillsynsmyndigheter

Riksrevisionen har i denna granskning kunnat visa att de av regeringen utsedda stöd- och tillsynsmyndigheterna inom nuvarande mandat skulle kunna göra mera, både genom att öka kunskapen om säkerhetsläget och att lämna stöd till den övriga statsförvaltningen för att öka skyddet. Detta är naturligtvis en fråga om vad som ska prioriteras såväl inom dessa myndigheter som inom statsförvaltningen som helhet. För att förbättra statens informationssäkerhet rekommenderar Riksrevisionen därför följande:

- MSB bör fortsätta och även intensifiera sitt arbete med att söka skapa en gemensam lägesbild för informationssäkerhet i statsförvaltningen.
- MSB har enligt 9 § andra stycket förordningen (2006:942) om krisberedskap och höjd beredskap möjlighet att begära att flera myndigheter än i dag lämnar en redovisning av sin risk- och sårbarhetsanalys till Regeringskansliet och MSB. MSB bör utnyttja denna möjlighet för att därigenom öka den samlade kunskapen om informationssäkerhetsläget och därigenom kunna bidra till en förbättring.

- MSB bör lämna de myndigheter som inte uppfyller kraven i föreskrifterna om statliga myndigheters informationssäkerhet (MSBFS 2009:10) det stöd som är nödvändigt, så att de uppnår efterlevnad inom rimlig tid.
- Såväl Säkerhetspolisen som FRA genererar viktig kunskap om säkerhetsläget inom den mest skyddsvärda delen av statsförvaltningen. Säkerhetspolisen och FRA bör därför var för sig systematiskt avge aggregerade rapporter om säkerhetsläget till Regeringskansliet och MSB.

Referenslista

Författningar

Säkerhetsskyddslagen (1996:627)

Lagen (2000:130) om försvarsunderrättelseverksamhet

Lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen)

Offentlighets- och sekretesslagen (2009:400)

Lagen (2003:389) om elektronisk kommunikation

Lagen (2000:832) om elektroniska signaturer

Lagen (2006:24) om nationella toppdomäner för Sverige på Internet

Personuppgiftslagen (1998:204)

Arkivlagen (1990:782)

Säkerhetsskyddsförordningen (1996:633)

Förordningen (2006:942) om krisberedskap och höjd beredskap (krisberedskapsförordningen)

Förordningen (2007:603) om intern styrning och kontroll

Arkivförordningen (1991:446)

Myndighetsförordningen (2007:515)

Förordningen (1996:1515) med instruktion för Regeringskansliet

Förordningen (2007:937) med instruktion för Försvarets radioanstalt

Förordningen (2007:951) med instruktion för Post- och telestyrelsen

Förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap

Förordningen (2009:1593) med instruktion för Riksarkivet

MSB:s föreskrifter om ledningssystem för informationssäkerhet (MSBFS 2009:10)

MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2010:7)

Rikspolisstyrelsens föreskrifter om säkerhetsskydd (RPSFS 2010:3)

Riksarkivets föreskrifter om handlingar på mikrofilm (RA-FS 2006:2)

Riksarkivets föreskrifter om handlingar på papper (RA-FS 2006:1)

Riksarkivets föreskrifter om elektroniska handlingar (RA-FS 2009:1)

Vervas föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte (VERVAFS 2007:2)

Regeringens propositioner till riksdagen

Budgetpropositionerna för 2010–2014, utgiftsområde 6

Prop. 1999/2000:86, Ett informationssamhälle för alla

Prop. 2004/05:175, Från IT-politik för samhället till politik för IT-samhället

Prop. 2007/08:92, Stärkt krisberedskap – för säkerhets skull

Prop. 2007/08:160, Utökat elektroniskt informationsutbyte

Prop. 2008/09:96, Behandling av personuppgifter inom studiestödsområdet

Prop. 2009/10:175, Offentlig förvaltning för demokrati, delaktighet och tillväxt

Prop. 2013/14:1, UO 6

Prop. 2013/14:144, Lag om sprängämnesprekursorer och redovisning av krisberedskapens utveckling

Statens offentliga utredningar

E-delegationens betänkanden SOU 2009:86, 2010:62, 2011:67, 2012:68 samt 2013:22

Utredningen om stärkt krisberedskap i det centrala betalningssystemets betänkande SOU 2011:78

Servicecenterutredningens betänkande SOU 2011:38

Informationssäkerhetsutredningens betänkande SOU 2010:25

Regeringshandlingar

Regeringens skrivelse (2009/10:124) Samhällets krisberedskap – stärkt samverkan för ökad säkerhet

Kommittédirektiv (2011:94) till en modern säkerhetsskyddslag

Kommittédirektiv (2013:110) till en strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och IT-system

Kommittédirektiv (2009:110) till viss översyn av ansvarsfördelning och organisation när det gäller samhällets informationssäkerhet

Departementspromemorian Bättre regler för elektroniska kommunikationer (Ds 2010:19)

Försvarsberedningens promemoria Vägval i en globaliserad värld (Ds 2013:33)

Försvarsberedningens promemoria Försvaret av Sverige – Starkare försvar för en osäker tid (Ds 2014: 20)

Regleringsbrev för budgetåret 2009 avseende Myndigheten för samhällsskydd och beredskap

Regleringsbrev för budgetåret 2012 avseende Myndigheten för samhällsskydd och beredskap

Regleringsbrev för budgetåret 2014 avseende Myndigheten för samhällsskydd och beredskap

Regeringsbeslut Fö2010/701/SSK

Regeringsbeslut Fö2010/702/SSK

Regeringsbeslut Fö2010/703/SSK

Regeringsbeslut Fö2011/1681/SSK

Regeringsbeslut Fö2012/717/SSK

Rapporter och andra handlingar från myndigheter m.m.

Datainspektionen: Årsredovisningar för 2009–2013.

Digitaliseringskommissionen: Handlingsplan för Digitaliseringskommissionen – inriktning och ambitioner

E-delegationen: Uppföljning av myndigheternas arbete med e-förvaltning och e-tjänster 2011 respektive 2013

Försvarets radioanstalt: Rapport, dnr 10 360:3409/12

Försvarets radioanstalt: Trender och utmaningar idag och imorgon – informationssäkerhet

MSB: Vägledning för risk- och sårbarhetsanalyser, 2011

MSB: Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter – En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011

MSB: Trendrapport – samhällets informationssäkerhet 2012

MSB: Risker och förmågor 2012 – redovisning av regeringsuppdrag om nationell riskbedömning respektive bedömning av krisberedskapsförmåga

MSB: Risker och förmågor 2013 – redovisning av regeringsuppdrag om nationell risk- och förmågebedömning

MSB: Samlad bedömning av samhällets krisberedskapsförmåga 2013 – komplettering av regeringsuppdrag nummer 26, dnr 2013-5294

MSB: En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter

MSB: Nationellt system för it-incidentrapportering, dnr 2012-2637

MSB: Tillgänglig och skyddad kommunikationsinfrastruktur för offentlig sektor, dnr 2010-6304

MSB: Säkerhetsgranskning, dnr 2010-6308

MSB: Strategi för samhällets informationssäkerhet 2010–2015

MSB: Samhällets informationssäkerhet – nationell handlingsplan 2012

MSB: Strategi för informationssäkerhet i e-förvaltning (dnr 2012-3430)

MSB: Ett fungerande samhälle i en föränderlig värld – nationell strategi för skydd av samhällsviktig verksamhet, 2011

MSB: handlingsplan för skydd av samhällsviktig verksamhet, 2013

MSB: Nationell hanterandeplan för allvarliga IT-incidenter, dnr 2010-4545

Regeringskansliet: It i människans tjänst – en digital agenda för Sverige, 2011

Riksrevisionen: Granskning av regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen (RiR 2007:10)

Statskontoret: Ledningssystem för informationssäkerhet vid 24-timmarsmyndigheter, vägledning och mallregelverk (2003:23)

Säkerhetspolisen: Säkerhetsskydd – en vägledning, 2008

Säkerhetspolisen: Underlag rörande Säkerhetspolisens bedömning av myndigheters säkerhetsanalyser ur ett informationssäkerhetsperspektiv 2014-07-11, dnr 2014-11898-4

Övriga tryckta källor

Ny teknik den 10 maj 2013

Svenska Dagbladet den 31 oktober 2013

Dagens Nyheter den 5 december 2013

Ny Teknik den 22 februari 2013

Otryckta källor

Datainspektionen: Yttrande till Riksrevisionen 2014-09-19 respektive 2014-09-24, Vissa frågor till datainspektionen med anledning av Riksrevisionens granskning av informationssäkerhet i statsförvaltningen, dnr 2011-2014

Försvarets radioanstalt: Yttrande till Riksrevisionen 2014-09-29 om FRA:s informationssäkerhetsarbete och övergripande bedömning av myndigheters IT- och informationssäkerhet

Myndigheten för samhällsskydd och beredskap: Yttrande till Riksrevisionen 2014-08-29, Redovisning av informationssäkerhet enligt MSB:s nu gällande föreskrifter om myndigheters risk- och sårbarhetsanalyser (MSBFS 2010:7), dnr 2014-3194

Post- och telestyrelsen: Yttrande till Riksrevisionen 2014-09-01, Svar på Riksrevisionens arbetsfrågor med anledning av granskning av informationssäkerhet

Regeringskansliet: Yttrande till Riksrevisionen 2014-09-23 med underlag till Riksrevisionen

Säkerhetspolisen: Yttrande till Riksrevisionen 2014-07-11, Underlag rörande Säkerhetspolisens bedömning av myndigheters säkerhetsanalyser ur ett informationssäkerhetsperspektiv, dnr 2014-11898-4

Intervjuer på Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Säkerhetspolisen, Försvarsmaktens militära underrättelse-och säkerhetstjänst samt Post- och telestyrelsen

Bilaga 1

Centrala begrepp

Ansvarsprincipen

Den som har ansvar för en verksamhet under normala förhållanden ska ha det också under en krissituation. Det betyder att en verksamhet ska kunna ha förmåga att fortsätta utföras även under en kris.[162]

Botnät

Ett botnät är ett nätverk av datorer som har infekterats av datavirus och annan skadlig kod. Dessa datorer ansluter till en central styrande nod där de får uppgifter att utföra, till exempel att söka igenom webbsidor efter e-postadresser, skicka ut oönskad skräppost eller i vissa fall utföra överbelastningsattacker mot datasystem, till exempel för en myndighet. Ett botnät kan bestå av tusentals datorer, ofta kallade zombier, spridda över hela världen och med ägare som inte vet om att datorerna är infekterade. Sedan några år tillbaka har botnät börjat tillhandahållas på kommersiella villkor. Den som vill skicka skräppost i stor skala eller angripa en nätresurs kan hyra ett redan existerande botnät på den svarta marknaden.[163]

CERT-SE

MSB/CERT-SE är Sveriges nationella IT-säkerhetsincidentsfunktion vars uppgift är att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Funktionen är placerad på MSB inom Verksamheten för samhällets informations- och cybersäkerhet och har till uppgift att agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade. MSB/CERT-SE är Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder. Fram till och med 2010 fanns denna funktion på Post- och telestyrelsen och benämndes då Sitic.[164]

---

[162] Källa: Krisinformation.se 2014.

[163] Källa: Svenska Wikipedia 2014.

[164] Källa: MSB.se/CERT-SE 2014.

E-delegationen

E-delegationen är en kommitté under Näringsdepartementet som har i uppdrag att driva på e-utvecklingen inom den offentliga sektorn. Delegationen arbetar med e-förvaltning, sociala medier och vidareutnyttjande av offentlig information. Till exempel initierar och koordinerar man förstudier och projekt som leder till förvaltningsgemensamma tjänster som utgår från privatpersoners och företags behov samt tar fram riktlinjer för och följer upp utvecklingen av myndigheternas arbete med e-förvaltning.[165]

LIS

LIS står för Ledningssystem för informationssäkerhet. Det är en standard framtagen av Internationella standardiseringsorganisationen (ISO), och betecknas enligt ISO 27000-serien. Standarden syftar till att förbättra den interna kontrollen av informationssäkerheten, och kan tillämpas på alla typer av organisationer.[166]

Molntjänster

Molntjänster är IT-tjänster som en kund överlåter till en annan aktör att tillhandahålla över internet. Det kan till exempel handla om att laga data, använda serverprogram och säkerhetskopiera data. Utlokaliseringen av IT-tjänsterna – ofta benämnt *outsourcing* – innebär att kunden delvis förlorar kontrollen över dem. Informationssäkerheten kommer då även att vara beroende av den som tillhandahåller molntjänsterna. Om företaget som tillhandahåller tjänsterna verkar utomlands riskerar dessutom lagstiftningen i Sverige och det andra landet att vara oförenliga.[167]

Risk- och sårbarhetsanalys

Alla myndigheter under regeringen är enligt 9 § krisberedskapsförordningen (2006:942) skyldiga att årligen analysera om det finns sådan sårbarhet eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet. Myndigheten ska värdera och sammanställa resultatet av arbetet i en risk- och sårbarhetsanalys. Ett antal myndigheter som har ett särskilt ansvar för krisberedskapen enligt förordningen ska redovisa sina respektive risk- och sårbarhetsanalyser till Regeringskansliet och MSB. Denna redovisning ska innehålla de åtgärder som planeras och en bedömning av behovet av ytterligare åtgärder.[168]

---

[165] Källa: E-delegationen.se 2014.

[166] Källa: Swedish Standards Institute (SIS) 2014.

[167] Källa: Svenska Wikipedia 2014.

[168] Källa: Förordningen (2006:942) om krisberedskap och höjd beredskap (krisberedskapsförordningen).

SAMFI

SAMFI står för Samverkansgruppen för informationssäkerhet, som består av sex myndigheter: Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Post- och telestyrelsen, Rikspolisstyrelsen (Rikskriminalpolisen respektive Säkerhetspolisen) samt Myndigheten för samhällsskydd och beredskap. SAMFI ska verka för säkra informationstillgångar i samhället avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet samt genom informationsutbyte och samverkan stödja de medverkande myndigheternas arbete när det gäller samhällets informationssäkerhet. SAMFI:s verksamhet inriktar sig på att genomföra de åtgärdsförslag som finns i den nationella handlingsplanen för samhällets informationssäkerhet. Myndigheten för samhällsskydd och beredskap ansvarar för arbetet i SAMFI.[169]

Sitic

Sveriges IT-incidentcentrum (Sitic) var mellan 2003 och 2010 en nationell funktion på Post- och telestyrelsen med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Sitic fungerade som en rikscentral för IT-incidentrapportering. Från och med 2011 hör funktionen till MSB, och kallas för CERT-SE.[170]

Säkerhetsanalys

Säkerhetsskyddsförordningen (1996:633) föreskriver att myndigheter och andra som förordningen gäller för ska utföra säkerhetsanalyser. En säkerhetsanalys innebär att man undersöker vilka uppgifter i verksamheten 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. Syftet med säkerhetsanalysen är att i en verksamhet identifiera det särskilt skyddsvärda, det vill säga där konsekvenserna av en antagonistisk handling kan få betydelse för rikets säkerhet. Utan någon form av säkerhetsanalys blir ett säkerhetsskydd nästan alltid ineffektivt. Unikt för säkerhetsanalysen är att den fokuserar på skydd mot antagonistiska hot.

TDV

TDV står för tekniskt detekterings- och varningssystem. FRA har fått i uppdrag av regeringen att stärka informationssäkerheten i samhället genom ta fram ett förslag på ett TDV-system och en pilotversion av detta. Ett sådant system kan liknas vid ett mer avancerat antivirussystem. Systemet larmar för sådan trafik som utgör en del av ett IT-angrepp. Den trafik som orsakar ett larm kan analyseras för att ta reda på mer om angreppet, vilket sker i enlighet med överenskommelse med den myndighet som drabbats av angreppet. TDV är avsett att utgöra ett förstärkt skydd för de mest

[169] Källa: MSB.

[170] Källa: Post- och telestyrelsen 2014.

skyddsvärda funktionerna i samhället, och ska vara ett komplement till grundläggande informationssäkerhetsåtgärder.[171]

[171] Källa: FRA 2014.

Bilaga 2

Förteckning över granskade regleringsbrev för 35 myndigheter under 2010–2014

Arbetsförmedlingen

Bolagsverket

Brottsförebyggande rådet

Centrala studiestödsnämnden

Diskrimineringsombudsmannen

Ekobrottsmyndigheten

Elsäkerhetsverket

Finansinspektionen

Försäkringskassan

Kemikalieinspektionen

Konjunkturinstitutet

Konkurrensverket

Kriminalvården

Kronofogdemyndigheten

Kustbevakningen

Livsmedelsverket

Luftfartsverket

Läkemedelsverket

Länsstyrelserna

Migrationsverket

Pensionsmyndigheten

Patent- och registreringsverket

Riksgälden

Rikspolisstyrelsen

Statistiska centralbyrån

Skatteverket

Socialstyrelsen

Statens energimyndighet

Statens jordbruksverk

Statens servicecenter

Strålsäkerhetsmyndigheten

Svenska kraftnät

Trafikverket

Tullverket

Åklagarmyndigheten

Bilaga 3

Metod för sammanställning av myndigheters rapportering om informationssäkerhet i årsredovisningen

Riksrevisionen har gått igenom årsredovisningarna för samma urval av myndigheter, vid sidan av stöd- och tillsynsmyndigheterna, som för genomgången av regleringsbreven för att få en uppfattning om myndigheterna självmant redovisar uppgifter om sin informationssäkerhet.[172] Genomgången omfattar årsredovisningar för åren 2009–2013 och utgår från två frågor.

- Omnämns informationssäkerhet, IT-säkerhet eller datasäkerhet på något sätt i årsredovisningen?
- Går det utifrån årsredovisningen att bilda sig en uppfattning om status på myndighetens informationssäkerhet?[173]

Bedömningen av om det går att bilda sig en uppfattning utgår från kravet på att myndigheten ska ha ett ledningssystem för informationssäkerhet. Om en myndighet exempelvis skriver att den har infört ett ledningssystem enligt gällande standard och att myndigheten har certifierat sig eller åtminstone utvärderat att systemet fungerar har vi bedömt att myndigheten har informerat om att den har en tillräcklig informationssäkerhet. Om myndigheten skriver att den inte har infört något ledningssystem eller att man håller på att införa det har vi bedömt att myndigheten har informerat om att informationssäkerheten är otillräcklig. Om myndigheten inte uttryckligen har nämnt ett eventuellt ledningssystem, men det ändå av skrivningarna går att sluta sig till att myndigheten har eller inte har ett system har vi bedömt det på motsvarande sätt. Om en myndighet rapporterat tillräcklig såväl som otillräcklig informationssäkerhet bedöms av Riksrevisionen ur styrningssynpunkt som likvärdiga. Båda sätten att återrapportera ger regeringen kunskap om läget och ger möjlighet att agera respektive vetskap om att man inte behöver agera. De fall som bedöms som att man inte alls eller endast delvis kan bilda sig en uppfattning är ur styrningssynpunkt mer problematiska. I de fallen bör regeringen efterfråga mer information.

[172] Se bilaga 2.

[173] Det finns inget uttryckligt krav för myndigheter eller statliga bolag att rapportera om informationssäkerhet i sin årsredovisning.

Förekommer skrivningar om informationssäkerhet, it-säkerhet eller data-säkerhet?	År 2009	År 2010	År 2011	År 2012	År 2013
Ja	12	15	13	18	16
Nej	23	21	23	19	21

Av tabellen ovan framgår att antalet årsredovisningar som på något sätt omnämner begreppen informationssäkerhet, IT-säkerhet eller datasäkerhet pendlar mellan 12 och 18 stycken under dessa år. Myndigheter som inte nämner något om informationssäkerhet är Centrala studiestödsnämnden, Elsäkerhetsverket, Konkurrensverket, Kustbevakningen, Livsmedelsverket, Länsstyrelsen i Västra Götaland, Migrationsverket, Statens energimyndighet, Statens servicecenter och Tullverket. Det motsvarar lite drygt en fjärdedel av det totala antalet undersökta myndigheter.

Går det utifrån årsredovisningen att få en uppfattning om myndighetens informationssäkerhet?	År 2009	År 2010	År 2011	År 2012	År 2013
Nej	28	27	25	25	26
Delvis	7	4	4	8	8
Ja ej tillräcklig	1	5	7	4	1
Ja tillräcklig	0	0	0	0	2

Av tabellen ovan framgår att för det stora flertalet myndigheter (ungefär 70 procent i genomsnitt över åren) går det inte att få en uppfattning om informationssäkerheten på myndigheten genom att läsa årsredovisningen.

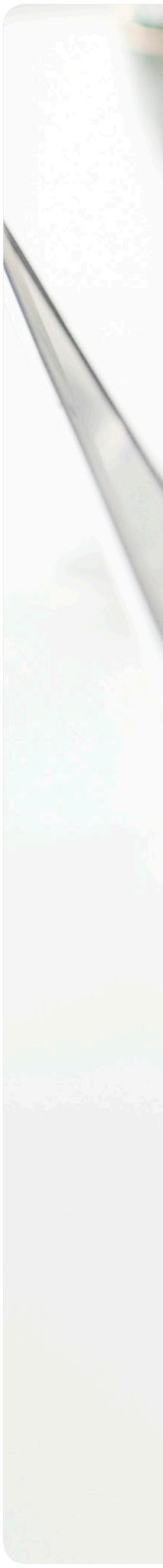
Tidigare utgivna rapporter från Riksrevisionen

Alla Riksrevisionens tidigare utgivna rapporter finns tillgängliga på www.riksrevisionen.se

2013	2013:1	Svensk rymdverksamhet – en strategisk tillgång?
	2013:2	Statliga myndigheters skydd mot korruption
	2013:3	Staten på elmarknaden – insatser för en fungerande elöverföring
	2013:4	Mer patientperspektiv i vården – är nationella riktlinjer en metod?
	2013:5	Staten på telekommarknaden
	2013:6	Ungdomars väg till arbete – individuellt stöd och matchning mot arbetsgivare
	2013:7	Bostadstillägget och äldreförsörjningsstödet till pensionärer – når förmånerna fram?
	2013:8	Energieffektivisering inom industrin – effekter av statens insatser
	2013:9	Sverige i Arktiska rådet – effektivt utbyte av medlemsskapet
	2013:10	På väg ut i världen – statens främjandeinsatser för export
	2013:11	Statens kunskapsspridning till skolan
	2013:12	Skattekontroll – en fråga om förtroendet för offentlig förvaltning
	2013:13	Landsbygdsprogrammet – från jordbruksstöd till landsbygdsstöd?
	2013:14	Sjunde AP-fonden – svarar förvaltningen av premiepensionen mot spararnas krav?
	2013:15	Kränkt eller diskriminerad i skolan – är det någon skillnad?
	2013:16	Statens tillsyn över skolan – bidrar den till förbättrade kunskapsresultat?
	2013:17	Ett steg in och en ny start – hur fungerar subventionerade anställningar för nyanlända?
	2013:18	Tågförseningar – orsaker, ansvar och åtgärder
	2013:19	Klimat för pengarna? Granskningar inom klimatområdet 2009–2013
	2013:20	Statens satsningar på nationella kvalitetsregister – leder de i rätt riktning?
	2013:21	Statens hantering av riksintressen – ett hinder för bostadsbyggande
	2013:22	Försvarsmaktens förmåga till uthålliga insatser
	2013:23	Transparensen i budgetpropositionen för 2014 – tillämpningen av det finanspolitiska ramverket

2014	2014:1	Statens insatser för riskkapitalförsörjning – i senaste laget
	2014:2	Bostäder för äldre i avfolkningsorter
	2014:3	Staten och det civila samhället i integrationsarbetet
	2014:4	Försvarets omställning
	2014:5	Effekter av förändrade regler för deltidsarbetslösa
	2014:6	Att överklaga till förvaltningsrätten – Handläggningstider och information till enskilda
	2014:7	Ekonomiska förutsättningar för en fortsatt omställning av försvaret
	2014:8	Försvaret – en utmaning för staten. Granskningar inom försvarsområdet 2010–2014
	2014:9	Stödet till anhöriga omsorgsgivare
	2014:10	Förvaltningen av regionala projektmedel – delat ansvar, minskad tydlighet?
	2014:11	Att tillvarata och utveckla nyanländas kompetens – rätt insats i rätt tid?
	2014:12	Livsmedelskontrollen – tar staten sitt ansvar?
	2014:13	Att gå i pension – varför så krångligt?
	2014:14	Etableringslotsar – fungerar länken mellan individen och arbetsmarknaden?
	2014:15	Nyanländ i Sverige – effektiva insatser för ett snabbt mottagande?
	2014:16	Swedfund International AB – Är finansieringen av bolaget effektiv för staten?
	2014:17	Det allmänna pensionssystemet – en granskning av granskningen
	2014:18	Statens dimensionering av lärarutbildningen – utbildas rätt antal lärare?
	2014:19	Valuta för biståndspengarna? – valutahantering i det internationella utvecklingssamarbetet
	2014:20	Överenskommelser mellan regeringen och SKL inom hälso- och sjukvården – frivilligt att delta men svårt att tacka nej
	2014:21	Exportkreditnämnden – effektivitet i exportgarantisystemet?
	2014:22	Primärvårdens styrning – efter behov eller efterfrågan?

Beställning: publikationsservice@riksrevisionen.se



Riksrevisionen har granskat om arbetet med informationssäkerhet i den civila statsförvaltningen är ändamålsenligt utifrån ökande hot och risker. Granskningen har inriktats mot den information som samlats in om vilka hot som realiseras samt de skyddsåtgärder som har vidtagits av övriga myndigheter.

Granskningen omfattar regeringen och dess stöd- och tillsynsmyndigheter: Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt samt i viss mån Post- och telestyrelsen.

Granskningen visar att arbetet med informationssäkerheten inte är ändamålsenligt sett till de hot och risker som finns. Regeringen har inte någon samlad lägesbild över hoten mot den civila statsförvaltningen, i vilken omfattning och mot vilka hoten realiseras samt vilka skyddsåtgärder myndigheterna vidtar. Detsamma gäller för regeringens stöd- och tillsynsmyndigheter.

Riksrevisionen lämnar vissa rekommendationer till regeringen och stöd- och tillsynsmyndigheterna, som bör kunna bidra till att stärka säkerheten. Bland annat att

- utöka tillsynen, så att den omfattar väsentligt mer än endast de allra mest skyddsvärda delarna av statsförvaltningen
- se till att det finns en funktion och en process i Regeringskansliet med syfte att samlat hantera informationssäkerheten
- snarast införa obligatorisk incidentrapportering för samtliga myndigheter.

ISSN 1652-6597
ISBN 978 91 7086 361 5
Beställning:
www.riksrevisionen.se
publikationsservice@riksrevisionen.se
Riksrevisionens publikationsservice
114 90 Stockholm

RIKSREVISIONEN

NYBROGATAN 55, 114 90 STOCKHOLM
08-5171 40 00
WWW.RIKSREVISIONEN.SE