Försvarsutskottets betänkande
2014/15:FöU10

Riksrevisionens rapport om informationssäkerhet i den civila statsförvaltningen

Sammanfattning

I betänkandet behandlar utskottet regeringens skrivelse 2014/15:84 Riksrevisionens rapport om informationssäkerhet i den civila statsförvaltningen. En följdmotion (SD) har väckts med anledning av skrivelsen.

Riksrevisionens samlade slutsats av sin granskning (RIR 2014:23) är att arbetet med informationssäkerhet inte är ändamålsenligt, sett till de hot och risker som finns, och lämnar ett antal rekommendationer till regeringen och dess stöd- och tillsynsmyndigheter.

Regeringen instämmer i huvudsak i Riksrevisionens slutsats men vill understryka att sedan Riksrevisionens granskning har de förutsättningar som gällde under den förra mandatperioden dock ändrats. Frågor om allmän ordning, säkerhet och krisberedskap, inklusive ansvaret för Regeringskansliets egen krisberedskap, är t.ex. nu samlat under inrikesministerns ansvar. Utvecklande av tillsyn, regelverk och incidentrapportering är exempel på andra åtgärder som regeringen överväger på informationssäkerhetsområdet.

Utskottet ser allvarligt på Riksrevisionens samlade slutsats men kan samtidigt konstatera att regeringen i sin skrivelse instämmer i Riksrevisionens slutsats i huvudsak och har inlett ett förändringsarbete sedan granskningen gjordes. Pågående beredningar inom Regeringskansliet av genomförda utredningar, samt uppdrag ställda till myndigheter, kommer att bilda viktiga underlag för framtiden.

Utskottet vill vidare framhålla att samhällets krisberedskap vilar på ansvarsprincipen, även i frågor om informationssäkerhet. Utskottet vill även framhålla vikten av samverkan mellan offentliga, privata och internationella aktörer.

Utskottet föreslår att riksdagen lägger regeringens skrivelse Riksrevisionens rapport om informationssäkerhet i den civila statsförvaltningen (skr. 2014/15:84) till handlingarna och avslår samtliga motionsyrkanden.

I betänkandet finns en reservation (SD) och ett särskilt yttrande (V).

Innehållsförteckning

Utskottets förslag till riksdagsbeslut

1. Informationssäkerhet i den civila statsförvaltningen

Riksdagen avslår motion
2014/15:3068 av Mikael Jansson m.fl. (SD) yrkandena 1 och 2.

Reservation (SD)

2. Skrivelsen

Riksdagen lägger skrivelse 2014/15:84 till handlingarna.

Stockholm den 19 maj 2015

På försvarsutskottets vägnar

Allan Widman

Följande ledamöter har deltagit i beslutet: Allan Widman (FP), Åsa Lindestam (S), Hans Wallmark (M), Peter Jeppsson (S), Lena Asplund (M), Alexandra Völker (S), Mikael Jansson (SD), Jan R Andersson (M), Kent Härstedt (S), Daniel Bäckström (C), Jakop Dalunde (MP), Lotta Olsson (M), Paula Holmqvist (S), Roger Richtoff (SD), Stig Henriksson (V), Mikael Oscarsson (KD) och Mattias Ottosson (S).

Redogörelse för ärendet

Ärendet och dess beredning

I betänkandet behandlas regeringens skrivelse 2014/15:84 Riksrevisionens rapport om informationssäkerhet i den civila statsförvaltningen. Riksrevisionens granskningsrapport (RIR 2014:23) överlämnades av riksdagen till regeringen den 20 november 2014.

Syftet med den rapport som behandlas i skrivelsen har varit att granska om arbetet med informationssäkerhet i den civila statsförvaltningen är ändamålsenligt utifrån ökande hot och risker.

En följdmotion har väckts med anledning av skrivelsen (SD).

Riksrevisionen föredrog sin rapport i försvarsutskottet den 26 mars. Vid detta sammanträde redogjorde också statssekreterare Ann Linde (Justitiedepartementet) för regeringens skrivelse med anledning av Riksrevisionens granskning. Utredare Erik Wennerström föredrog vid samma tillfälle sin i sammanhanget relevanta utredning Informations- och cybersäkerhet i Sverige – strategi och åtgärder för säker information i staten (SOU 2015:23).

Bakgrund

Riksrevisionens granskning tar sin utgångspunkt i den alltmer ökande användningen av information i samhället och i statsförvaltningen samt de brister som Riksrevisionen har konstaterat i sina tidigare granskningar av informationssäkerheten.

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 av 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.

Den aktuella granskningen har syftat till att utreda om arbetet med informationssäkerhet i den civila statsförvaltningen är ändamålsenligt utifrån de ökande hoten. Granskningen omfattar således varken styrningen av eller nivån på informationssäkerhet i samhället i stort. I granskningen har Riksrevisionen inriktat sig 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 de ansvariga myndigheterna för stöd och tillsyn har tillräcklig

kunskap om de skyddsåtgärder som har vidtagits av myndigheterna 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) och 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.

Utskottets överväganden

Informationssäkerhet i den civila statsförvaltningen

Utskottets förslag i korthet

Riksdagen lägger regeringens skrivelse Riksrevisionens rapport om informationssäkerhet i den civila statsförvaltningen (skr. 2014/15:84) till handlingarna och avslår motionsyrkanden om en myndighetsövergripande strategi för it-säkerhet samt om att anställda vid myndigheter ska placeras med civilplikt för att vid en kris kunna handha it-säkerheten.

Jämför reservation (SD) och särskilt yttrande (V).

Riksrevisionens iakttagelser

Riksrevisionens samlade slutsats av sin granskning är att arbetet med informationssäkerhet 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 informationssäkerhet är en förutsättning för att på ett samlat sätt kunna värdera sannolikheten för att olika händelser ska inträffa och vilka konsekvenser det kan få. Det finns flera riskområden inom statsförvaltningen när det gäller informationssäkerhet, såsom kompetensbrist, upphandling, tillsyn, uppföljning, återrapportering samt styrning, omreglering och samordning. Riksrevisionens bedömning är att en stor andel myndigheter inte har centrala delar av ett systematiskt informationssäkerhetsarbete på plats.

Riksrevisionens granskning har visat att regeringen inte har utövat en effektiv styrning av informationssäkerheten i den civila statsförvaltningen. Regeringen har inte någon samlad lägesbild som inkluderar hot, i vilken omfattning och mot vilka hoten realiseras eller vilka skyddsåtgärder myndigheterna vidtar. En sådan lägesbild har inte heller någon av regeringens stöd- och tillsynsmyndigheter. Det innebär att den samlade förmågan att hantera konsekvenserna av en allvarlig incident till stora delar är okänd.

Riksrevisionen bedömer att regelsystemet för informationssäkerhet i huvudsak ser likadant ut i dag som det gjorde 2007 när området senast granskades. 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 kan behöva anpassas bättre till olika typer av statlig verksamhet för att de önskvärda målen ska kunna nås.

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 det inte någon samlad riskvärdering. I stället råder osäkerhet om hur starkt skyddet är, vilka händelser som inträffat 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.

I dag har varje myndighet ett eget ansvar för hela sin verksamhet i såväl normalläge som 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 detta fanns skulle det kunna leda till en bättre säkerhet totalt i statsförvaltningen, samtidigt som den totala kostnaden för informationssäkerhet skulle kunna 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 utövas 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. Av detta 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 om 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 av informationssäkerheten 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 sin granskning kunnat visa att de av regeringen utsedda stöd- och tillsynsmyndigheterna inom sina nuvarande mandat skulle kunna göra mer, både genom att öka kunskapen om säkerhetsläget och genom att lämna stöd till den övriga statsförvaltningen för att öka skyddet. För att förbättra statens informationssäkerhet rekommenderar Riksrevisionen därför följande:

- MSB bör fortsätta och även intensifiera sitt arbete med att försöka 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 fler myndigheter än i dag redovisar sin risk- och sårbarhetsanalys till Regeringskansliet och MSB. MSB bör utnyttja denna möjlighet för att 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 lämna aggregerade rapporter om säkerhetsläget till Regeringskansliet och MSB.

Regeringens bedömning och åtgärder

Allmänt

Regeringen instämmer i huvudsak i Riksrevisionens slutsats att delar av arbetet med informationssäkerhet i den civila statsförvaltningen inte är ändamålsenliga. Sedan Riksrevisionens granskning har de förutsättningar som gällde under den förra mandatperioden dock ändrats, anför regeringen. Under denna mandatperiod har bl.a. frågor om allmän ordning, säkerhet och krisberedskap, inklusive ansvaret för Regeringskansliets egen krisberedskap, samlats under inrikesministerns ansvar. Inrikesministern ansvarar också för styrningen av bl.a. MSB, Polismyndigheten och Säkerhetspolisen. Regeringen har genom förändringarna skapat bättre förutsättningar för en mer sammanhållen styrning av informationssäkerheten.

Utredningar

Två särskilda utredare har haft i uppdrag ett se över frågor som rör informationssäkerhet. Som Riksrevisionen lyfter fram har dessa utredningar direkt bäring på kravställning och styrning av informationssäkerheten i statsförvaltningen.

Regeringen beslutade den 28 november 2013 om kommittédirektiv (dir. 2013:110) gällande strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system. Utredningen, som tog namnet NISU 2014, hade i uppdrag att föreslå en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och it-system. Utredningen redovisade betänkandet Informations- och cybersäkerhet i Sverige – strategi och åtgärder för säker information i staten den 10 mars 2015 (SOU 2015:23). Utöver förslaget till en ny strategi för informationssäkerhet har utredningen bl.a. pekat på vikten av att inrätta ett statligt myndighetsråd för informations- och cybersäkerhet och att förstärka tillsynen över den statliga sektorns informations- och cybersäkerhet.

Den andra utredningen som regeringen tillsatt rör säkerhetsskyddslagen (dir. 2011:94). En del av utredningens uppdrag har varit att föreslå hur reglerna om informationssäkerhet, som en del av säkerhetsskyddet, bör vara utformade. Utredningen har också haft i uppdrag att se över hur tillsynen över säkerhetsskyddet bör vara utformat och att ta ställning till om ett system med sanktionsåtgärder bör införas. Utredningen överlämnade sitt betänkande den 17 mars 2015 (SOU 2015:25), dvs. efter det att regeringens skrivelse överlämnades till riksdagen (se vidare nedan).

Utökad tillsyn och mandat att utfärda sanktioner

Riksrevisionen rekommenderar att regeringen utökar tillsynen av informationssäkerheten i den civila statsförvaltningen så att den omfattar mer än de mest skyddsvärda delarna.

Som Riksrevisionen beskriver i sin rapport finns det ett antal myndigheter med tillsynsansvar på informationssäkerhetsområdet. PTS, Datainspektionen, Riksarkivet, MSB och Säkerhetspolisen har alla på olika sätt ansvar för arbetet med samhällets informationssäkerhet. PTS utövar tillsyn enligt lagen (2003:389) om elektronisk kommunikation. Datainspektionens uppgift är att verka för att människor skyddas mot att deras personliga integritet kränks vid behandling av personuppgifter. I uppgiften ingår tillsyn av informationssäkerhet. Riksarkivet utformar föreskrifter och allmänna råd för arkivhantering och följer upp hur dessa följs, bl.a. genom att utföra inspektioner vid statliga myndigheter. MSB stöder och samordnar arbetet med samhällets informationssäkerhet samt analyserar och bedömer omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. MSB har dock inget tillsynsansvar när det gäller informationssäkerhet.

Säkerhetspolisen har ansvar för att utöva tillsyn av säkerhetsskyddet, inklusive informationssäkerhet, i de civila delarna av statsförvaltningen. Säkerhetsskyddsregleringen, och därmed tillsynsansvaret, omfattar bara de mest skyddsvärda verksamheterna. Om brister som upptäcks vid tillsynen inte rättas till ska Säkerhetspolisen under vissa förutsättningar anmäla detta till regeringen. Några sanktionsmöjligheter finns emellertid inte. En säkerhetsincident ska skyndsamt anmälas till Säkerhetspolisen i fall där en hemlig uppgift kan ha röjts, om röjandet kan antas medföra men för rikets säkerhet som inte endast är ringa.

Regeringen delar Riksrevisionens bedömning att en effektiv tillsyn är en viktig del i informationssäkerhetsarbetet. Regeringen anser därför att det finns skäl att överväga tillsynsbehovet för andra delar i den centrala statsförvaltningen än de som är mest skyddsvärda. Regeringen har också nyligen tagit emot ett förslag från NISU 2014 som till viss del behandlar frågan om tillsyn. Regeringen kommer efter remissbehandling att ta ställning till vilka åtgärder som bör vidtas.

Det är givetvis även angeläget att den tillsyn som utövas med stöd av säkerhetsskyddslagstiftningen är effektiv och ändamålsenlig. Riksrevisionen konstaterar att Säkerhetspolisen genom sin tillsynsverksamhet funnit systematiska brister när det gäller informationssäkerhet hos de mest skyddsvärda verksamheterna. I bl.a. det perspektivet framhåller Riksrevisionen sanktioner som ett möjligt verktyg för att förmå olika verksamheter att trygga sin informationssäkerhet och trygga sina skyddsvärden. Utredningen om säkerhetsskyddslagen har som tidigare nämnts haft till uppgift att överväga frågor om tillsyn och sanktioner, bl.a. mot bakgrund av den ökade internationaliseringen, informationsteknikens utveckling och avregleringen av offentlig verksamhet.

Regeringen avser att efter remissbehandlingen ta ställning till hur förslagen bör tas om hand.

Ett annat viktigt arbete i detta sammanhang är det EU-direktiv om nät- och informationssäkerhet (NIS-direktivet) som är under förhandling. Direktivet, som bl.a. gäller struktur för incidentrapportering på informationssäkerhetsområdet, innehåller krav på tillsyn och sanktioner. Ambitionen är att direktivet ska antas under våren 2015. Regeringen avser att ge en utredning i uppdrag att överväga och föreslå hur direktivet ska genomföras i svensk rätt.

Regelverk

Riksrevisionen har också rekommenderat regeringen att skyndsamt utreda om det regelverk som styr arbetet med informationssäkerhet 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.

NISU 2014 har haft i uppdrag att tydliggöra statliga myndigheters ansvar och roller utifrån de uppgifter och uppdrag på informationssäkerhetsområdet som de har i dag. Utredningen om säkerhetsskyddslagen har i sin tur haft i uppdrag att se över säkerhetsskyddsregleringen i dess helhet. De frågor som Riksrevisionen anser bör utredas har alltså delvis varit föremål för utredning helt nyligen. Efter remissbehandling kommer regeringen att ta ställning till förslagen och vidta nödvändiga åtgärder. I sammanhanget är även det kommande arbetet med att genomföra NIS-direktivet relevant.

På myndighetsnivå utfärdar MSB verkställighetsföreskrifter om ledningssystem för informationssäkerhet (MSBFS 2009:10). Föreskrifterna trädde i kraft den 1 februari 2010. MSB:s föreskrifter gäller för myndigheter under regeringen med undantag för Regeringskansliet, kommittéväsendet och Försvarsmakten. Av föreskrifterna följer att myndigheternas arbete ska bedrivas enligt svensk standard i form av ISO 27001 och 27002. Myndigheten har påbörjat ett arbete med att se över föreskrifterna.

Obligatorisk it-incidentrapportering

Riksrevisionen har även rekommenderat att regeringen snarast inför en obligatorisk incidentrapportering för samtliga myndigheter. Syftet med en sådan ordning är att stärka samhällets informationssäkerhet, både dess förebyggande och dess hanterande delar.

Regeringen anser i likhet med Riksrevisionen att det är angeläget att en ordning för obligatorisk incidentrapportering införs. MSB fick den 14 april 2010 regeringens uppdrag (Fö2010/701/SSK) att utreda hur ett system för obligatorisk it-incidentrapportering för statliga myndigheter skulle kunna utformas. Uppdraget redovisades den 1 mars 2011 genom rapporten System för obligatorisk it-incidentrapportering för statliga myndigheter. I ett följduppdrag fick MSB den 12 april 2012 i uppdrag av regeringen att utifrån en fördjupad

analys komplettera förslaget om ett system för obligatorisk it-incidentrapportering. I uppdraget ingick att föreslå bl.a. definitioner och kriterier för när en incident ska rapporteras, vilka myndigheter som ska undantas från rapporteringsskyldigheten, hur incidenter av misstänkt brottslig karaktär ska hanteras samt en författningsreglering. Uppdraget redovisades den 30 november 2012 genom rapporten Nationellt system för it-incidentrapportering. MSB:s förslag bereds för närvarande i Regeringskansliet. Frågan innehåller dock flera utmaningar, bl.a. när det gäller förhållandet mellan incidentrapportering och brottsanmälningar och förhållandet mellan incidenter som inträffar i de mest skyddsvärda verksamheterna och andra incidenter.

Som beskrivits tidigare förhandlas för närvarande ett direktiv i EU om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen, det s.k. NIS-direktivet. Förslaget till direktiv innehåller bl.a. skyldigheter för alla medlemsstater att vidta förebyggande åtgärder och åtgärder för att hantera och svara på allvarliga risker och incidenter som påverkar nätverk och informationssystem. Aktörer som omfattas av förslaget kan vara myndigheter, kommuner, landsting och enskilda.

Regeringen är angelägen om att arbetet med att införa ett nationellt system för incidentrapportering fortsätter och att ett sådant system kommer på plats så snart som möjligt. Vid utformningen av ett sådant system är det emellertid angeläget att hitta rätt avvägningar när det gäller de ovan nämnda utmaningarna.

Hantering i Regeringskansliet av informationssäkerhetsfrågor

Riksrevisionen har slutligen rekommenderat regeringen att se till att det finns en funktion och en process i Regeringskansliet med syfte att samlat hantera informationssäkerhetsfrågor. Ansvaret för informationssäkerhet i den mån sådana frågor inte hör till ett annat departement, liksom samordning av samhällets krisberedskap, har som tidigare beskrivits samlats under inrikesministern i Justitiedepartementet. Ansvarsprincipen gäller dock fortfarande.

Övriga åtgärder

När det gäller de myndigheter som har ett särskilt ansvar för informationssäkerhet är det viktigt att fördelningen av ansvar och roller så långt det är möjligt är tydlig. Samtidigt ligger det i sakens natur att de berörda myndigheternas ansvar i vissa fall överlappar varandra. Mot den bakgrunden är det av stor vikt att myndigheterna samverkar. Regeringen välkomnar därmed de samverkansforum som har inrättats på området, t.ex. Samverkansgruppen för informationssäkerhet (SAMFI) och Nationell samverkan till skydd mot allvarliga it-hot (NSIT).

En central faktor för all form av incidentrapportering och hantering av incidenter och attacker är förmågan att veta att man är utsatt för en incident eller attack. Arbetet kommer att intensifieras när det gäller att skapa förutsättningar

för att myndigheter och andra berörda aktörer som bedriver särskilt skyddsvärd verksamhet ska kunna erbjudas att delta i ett nationellt tekniskt detekterings- och varningssystem (TDV).

I syfte att höja medvetenheten om vikten av informationssäkerhet och för att skapa en bild av läget hos berörda myndigheter har regeringen i respektive myndighets regleringsbrev för 2015 beslutat att myndigheter som har ett särskilt ansvar för krisberedskap och höjd beredskap särskilt ska redovisa sitt arbete med informationssäkerhet. I samma syfte har regeringen också beslutat att MSB ska genomföra en undersökning av hur Sveriges kommuner arbetar med informationssäkerhet. Dessa båda uppdrag kommer att bidra till att förbättra regeringens kunskap på området och därmed skapa förutsättningar för ett ändamålsenligt arbete med att stärka samhällets informationssäkerhet. Det har även inletts ett arbete som syftar till att öka regeringens kunskap om säkerhetsläget inom de mest skyddsvärda delarna av statsförvaltningen.

Sammanfattningsvis uttrycker regeringen i skrivelsen att man vidtagit flera åtgärder på informationssäkerhetsområdet i syfte att förbättra samhällets beredskap och robusthet mot allvarliga it-incidenter. Regeringen avser att även fortsättningsvis prioritera detta arbete.

Regeringen anser att Riksrevisionens rapport är slutbehandlad i och med skrivelsen.

En ny säkerhetsskyddslag

Utredningen om en översyn av säkerhetsskyddslagstiftningen överlämnade som tidigare nämnts sitt betänkande den 17 mars 2015 (SOU 2015:25), dvs. efter regeringens skrivelse hade överlämnats till riksdagen.

Utredningen föreslår att säkerhetsskyddslagen ersätts av en ny lag. Även den nya lagen bör benämnas säkerhetsskyddslag. En ny lag ska svara mot de förändrade kraven på säkerhetsskyddet, bl.a. när det gäller utvecklingen på informationsteknikområdet, en ökad internationell samverkan, en ökad sårbarhet i samhällsviktiga funktioner och att säkerhetskänslig verksamhet i allt större omfattning bedrivs i enskild regi. Utredningen gör bl.a. bedömningen att det för närvarande inte finns tillräckliga skäl för att ändra tillsynens inriktning och genomförande och föreslår därför inte att sanktioner ska införas. Det anses dock angeläget att noga följa utvecklingen och inom en inte alltför avlägsen framtid följa upp frågan.

Motionen

I motion 2014/15:3068 anför Mikael Jansson m.fl. (SD) att en handlingsplan ska tas fram över en myndighetsgemensam och övergripande strategi för it-säkerhet, där Riksrevisionens rekommendationer ska beaktas (yrkande 1), och att anställda vid myndigheterna ska placeras med civilplikt för att vid en kris kunna handha it-säkerheten (yrkande 2).

Motionärerna understryker att Riksrevisionen riktade svidande kritik på detta område redan 2007 och att den förra regeringen av allt att döma vidtog få åtgärder för att möta kritiken. Man konstaterar att den sittande regeringen pekar på skapandet av ett inrikesdepartement som en institutionellt viktig åtgärd för att samla it-säkerheten på färre händer. Vad som blir alltmer uppenbart, menar motionärerna, är att det kommer att krävas kraftfulla och genomtänkta åtgärder för att höja säkerheten i våra myndigheters it-system.

Det är till fördel för it-säkerheten att MSB tar fram handböcker och har ett kontinuerligt uppdrag att rapportera till regeringen i frågan och att FRA gör enstaka besök ute bland myndigheterna, men det räcker inte ända fram, enligt motionärerna. Det krävs ett övergripande it-säkerhetssystem och en gemensam strategi. Det är även för dyrt att varje myndighet ska ha egna it-säkerhetskonsulter. Sverige har i dag utrett frågan tillräckligt för att kunna iståndsätta ett gemensamt säkerhetssystem, anförs i motionen.

Utskottets ställningstagande

Utskottet ser allvarligt på Riksrevisionens slutsats att arbetet med informationssäkerheten i den civila statsförvaltningen inte är ändamålsenligt sett till de hot och risker som finns, men kan samtidigt konstatera att regeringen i sin skrivelse instämmer i Riksrevisionens slutsats i huvudsak och har inlett ett förändringsarbete sedan granskningen gjordes.

Utskottet anser att de redan genomförda ändringarna inom Regeringskansliet har skapat förutsättningar för en mer sammanhållen styrning av informationssäkerhetsfrågorna men att arbetet inte får stanna vid detta, utan utvecklandet av informationssäkerheten i den civila statsförvaltningen måste fortgå på bred front för att bli ändamålsenligt mot bakgrund av ökande hot och risker. Det är exempelvis fortsatt viktigt att utveckla arbetet mot bakgrund av Riksrevisionens samlade synpunkter, t.ex. i fråga om risk- och sårbarhetsanalyser, lägesbilder, regelverk, incidentrapportering och tillsyn. Den pågående beredningen av betänkandena Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten och En ny säkerhetsskyddslag kommer att bilda viktiga underlag för framtiden.

I sammanhanget måste alla myndigheters roll och ansvar i arbetet framhållas, både ur ett ansvars- och ett samverkansperspektiv. Riksrevisionens rekommendationer till stöd- och tillsynsmyndigheterna bör tas i beaktande. Regeringens beslut om att myndigheter som har ett särskilt ansvar för krisberedskap och höjd beredskap ska redovisa sitt arbete med informationssäkerhet finner utskottet som särskilt viktigt, men också att MSB har fått i uppgift att genomföra en undersökning om hur kommunerna arbetar med informationssäkerhet. Att medvetandegöra offentliga och privata aktörer samt allmänheten om de hot som finns är överlag centralt i arbetet.

När det gäller en myndighetsgemensam och övergripande strategi för it-säkerhet finner utskottet sålunda att det pågår ett utvecklingsarbete som inte bör föregripas. Utskottet avstyrker därför det aktuella motionsyrkandet.

Utskottet vill vidare påminna om att samhällets krisberedskap vilar på ansvarsprincipen, även i frågor om informationssäkerhet. Detta innebär att anställda på myndigheter med ett särskilt ansvar för informationssäkerhetsfrågor också har detta ansvar vid en kris. Av dessa skäl behöver myndighetsanställda inte särskilt pekas ut som ansvariga vid en kris, vilket motionärerna anför. Utskottet vill dessutom påminna om att riksdagen våren 2010 beslutade om lagstiftning som bl.a. fastställde att totalförsvarsplikten endast ska tillämpas när försvarsberedskapen så kräver (prop. 2009/10:160, bet. 2009/10:FöU8, rskr. 2009/10:269).

Riksrevisionen konstaterar dock att det finns ett behov av ett bättre utbyggt stöd till statsförvaltningen när det gäller informationssäkerhet, då det är svårt att rekrytera och upprätthålla relevant kompetens på varje enskild myndighet och stödmyndigheterna har begränsade resurser. Utskottet vill av detta skäl även framhålla vikten av samverkan mellan offentliga, privata och internationella aktörer. Genom en utvecklad samverkan kan olika aktörers specialistkompetens komplettera varandra och bättre rationalitet uppnås. Denna aspekt tas också upp i betänkandet Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten, som för närvarande remissbehandlas. Utskottet finner sålunda inte skäl att heller bifalla motionsyrkandet om att anställda vid myndigheterna ska placeras med civilplikt att i kris handha it-säkerheten.

Avslutningsvis föreslår utskottet att riksdagen lägger regeringens skrivelse Riksrevisionens rapport om informationssäkerhet i den civila statsförvaltningen (skr. 2014/15:84) till handlingarna.

Reservation

Informationssäkerhet i den civila statsförvaltningen, punkt 1 (SD)

av Mikael Jansson (SD) och Roger Richtoff (SD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 1 borde ha följande lydelse:

Riksdagen tillkännager för regeringen som sin mening vad som anförs i reservationen.

Därmed bifaller riksdagen motion

2014/15:3068 av Mikael Jansson m.fl. (SD) yrkandena 1 och 2.

Ställningstagande

Riksrevisionen riktade en svidande kritik på informationssäkerhetsområdet redan år 2007. Förra regeringen vidtog av allt att döma få åtgärder för att möta kritiken. Den sittande regeringen pekar på skapandet av ett inrikesdepartement som en institutionellt viktig åtgärd för att samla it-säkerheten på färre händer. Vi anser att det blir alltmer uppenbart att det kommer att krävas kraftfulla och genomtänkta åtgärder för att höja säkerheten i våra myndigheters it-system.

I dag tar MSB fram handböcker och FRA gör enstaka besök ute bland myndigheterna. Det är till fördel för it-säkerheten men räcker inte ända fram. Vi anser att det krävs ett övergripande it-säkerhetssystem och en gemensam strategi. Det är även för dyrt att varje myndighet ska ha egna it-säkerhetskonsulter. MSB har ett kontinuerligt uppdrag att rapportera till regeringen. Vi har i dag tillräckligt med utredningar för att iståndsätta ett gemensamt säkerhetssystem.

Vi anser sammanfattningsvis att en handlingsplan ska tas fram över en myndighetsgemensam och övergripande strategi för it-säkerhet där Riksrevisionens rekommendationer ska beaktas och att anställda vid myndigheterna ska placeras med civilplikt för att vid en kris kunna handha it-säkerheten. Detta bör ges regeringen till känna.

Särskilt yttrande

Skrivelsen, punkt 2 (V)

Stig Henriksson (V) anför:

Riksrevisionen har under perioden maj till november 2014 granskat om arbetet med informationssäkerhet i den civila statsförvaltningen är ändamålsenligt utifrån ökande hot och risker. Riksrevisionens samlade slutsats är att ”arbetet inte är ändamålsenligt, sett till de hot och risker som finns”.

Riksrevisionen noterar brister vad gäller kompetens, upphandling, tillsyn, uppföljning, återrapportering, styrning, reglering och samordning. Riksrevisionens bedömning är att ”en stor andel myndigheter inte har centrala delar av ett systematiskt informationssäkerhetsarbete på plats” och konstaterar att regeringen inte har någon samlad lägesbild som inkluderar hot. Det har inte regeringens tillsynsmyndigheter FRA, PTS eller MSB heller, enligt Riksrevisionen.

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 den samlade förmågan 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.

Riksrevisionen gjorde en liknande revision 2007 och dessvärre verkar påpekade brister inte ha åtgärdats i tillfredställande omfattning.

Riksrevisionen lämnar en rad rekommendationer för att regeringen och dess tillsynsmyndigheter ska komma till rätta med problemen och regeringen – i sin tur - anser att Riksrevisionens rapport är slutbehandlad i och med skrivelse 2014/15:84, där man redogör för vidtagna åtgärder med anledning av Riksrevisionens rapport.

Vid en genomläsning av skrivelse 2014/15:84 finner man emellertid en diskrepans mellan Riksrevisionens slutsatser och påpekade brister å ena sidan och regeringens redovisade åtgärder å den andra. Jag tycker att detta är allvarligt och att det fortfarande finns mycket att göra på området då 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.

Regeringen har dock verkat under en relativt kort tid och har framförallt behövt invänta det så kallade NIS-direktivet – ett förslag till direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen – som förväntas komma denna vår.

Jag kommer att följa frågan noggrant och förutsätter att regeringen efter slutbehandlingen av NIS-direktivet skyndsamt återkommer med konkreta och

snabbt verkande åtgärder inför detta allvarliga hot både mot samhället, men också mot enskilda personer.

BILAGA 1

Förteckning över behandlade förslag

Skrivelsen

Regeringens skrivelse 2014/15:84 Riksrevisionens rapport om informationssäkerhet i den civila statsförvaltningen.

Följdmotionen

2014/15:3068 av Mikael Jansson m.fl. (SD):

1. Riksdagen tillkännager för regeringen som sin mening vad som anförs i motionen om att en handlingsplan ska tas fram över en myndighetsgemensam övergripande strategi för it-säkerhet, där Riksrevisionens rekommendationer ska beaktas.
2. Riksdagen tillkännager för regeringen som sin mening vad som anförs i motionen om att anställda vid myndigheterna ska placeras med civilplikt att i kris handha it-säkerheten.

Tryck: Elanders, Vällingby 2015