RIKSREVISIONEN

DNR: 5.1.1-2015-0781
DATUM: 2015-09-11

Justitiedepartementet
103 33 Stockholm

Yttrande över Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten (SOU 2015:23)

Riksrevisionen har beretts möjlighet att yttra sig över betänkanden från NISU 2014-utredningen, med uppdrag att föreslå strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system.

Riksrevisionen bejakar i stort utredningens förslag

Riksrevisionen anser att betänkandet på ett utmärkt sätt behandlar de problem som i dag finns när det gäller att införa och upprätthålla en god informationssäkerhet i statsförvaltningen. Riksrevisionen ställer sig positiv till flera av de förslag som lämnas i betänkandet.

Riksrevisionens granskning har visat på allvarliga brister gällande informationssäkerheten i statsförvaltningen. Det är ofta alltför lätt att bryta sig in i samhällsviktiga system och skyddet motsvarar sällan nivån på information som hanteras i systemen eller de hot som systemen bör skyddas mot. I dag kopplas IT-system samman mellan myndigheter och företag i en allt större utsträckning och myndigheterna hanterar ofta samma information men med olika nivå på skydd och klassning av informationen. En angripare behöver därmed troligtvis inte 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.

Försvarets radioanstalt pekar i underlagen till granskningen på att bristande säkerhet ofta kan kopplas till en önskan att pressa IT-kostnaderna. IT-budgeten är ofta 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. 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.

Mot bakgrund av det ovan angivna instämmer Riksrevisionen i utredningens slutsatser om att statlig upphandling ska innehålla en hänvisning till för staten gällande standarder och krav på certifiering i de situationer där säkerhetsnivåer har fastställts för respektive verksamhet. Vidare bejakar Riksrevisionen förslaget att Myndigheten för samhällsskydd och beredskap (MSB) ges i uppdrag att ta fram skyddsprofiler som anger minimikrav på säkerhet i vanligt förekommande it-produkter som används av statliga myndigheter.

I betänkanden föreslås vidare att det bör införas ett krav på att rapportera vilken leverantör som en statlig myndighet valt då ramavtal rörande it-lösningar används. Riksrevisionen bedömer att det finns ett betydande underskott av kunskap om förhållanden kopplade till myndigheternas informationssäkerhet. Varje myndighet bedömer sin egen risk kopplad till en eventuell outsourcing var för sig ovetandes om hur övriga myndigheter agerar. Ingen har därför kunskap om vilken riskkoncentration som sker hos ramavtalsleverantörerna och det går därför inte heller att bedöma om staten som helhet har en acceptabel risknivå med anledning av outsourcing. Riksrevisionen instämmer därför även i utredningens slutsats avseende ett sådant rapporteringskrav.

Incidentrapportering

Riksrevisionen är positiv till att inrätta ett system för obligatorisk IT-incidentrapportering för samtliga statliga myndigheter. Det ligger helt i linje med vad Riksrevisionen har rekommenderat i granskningen av informationssäkerheten i den civila statsförvaltningen (RiR 2014:23). MSB är enligt Riksrevisionens bedömning en myndighet som har goda förutsättningar att införa ett sådant system och utfärda verkställighetsföreskrifter. Detsamma gäller även beträffande förslaget att MSB bör få i uppdrag att förse statliga myndigheter med information om trender och utveckling när det gäller IT-incidenter. Det är naturligt att den myndighet som får i uppdrag att ansvara för incidentrapporteringssystemet också får i uppdrag sprida den kunskap som systemet genererar till övriga förvaltningen.

Etablera en nationell styrmodell för informationssäkerhet

Riksrevisionens granskning 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. 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 det följer att det saknas beslutsunderlag för att vidta nödvändiga åtgärder.

Granskningen visade också att det inte fanns någon samlad central funktion i Regeringskansliet med ansvar för att bereda frågor om informationssäkerhet i statsförvaltningen. Ärenden rörande informationssäkerhet hanterades 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 och att det därmed krävs kraft i styrningen för att skyddet ska kunna höjas till en ändamålsenlig nivå.

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 och en tydlig styrning 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.

Riksrevisionen delar därför utredningens slutsats att en nationell styrmodell för informationssäkerhet bör etableras.

Inrätta ett statligt myndighetsråd för informationssäkerhet

Riksrevisionen kan konstatera att det fortsättningsvis kommer att finnas ett antal aktörer med kompletterande såväl som delvis överlappande ansvar på informationssäkerhetsområdet. Det kan av den anledningen finnas anledning att skapa

en mer formell struktur för samverkan på området. Riksrevisionen delar därför utredningens slutsats att ett statligt myndighetsråd för informationssäkerhet bör inrättas.

Inför en ny förordning för statliga myndigheters 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 instämmer därför i utredningens förslag.

Tillsynen över den statliga sektorns informationssäkerhet bör samordnas och förstärkas. MSB ska utöva tillsyn

Utredningens förslag är i huvudsak identiskt med de rekommendationer som Riksrevisionen lämnade till regeringen i rapporten RiR 2014:23. Riksrevisionen delar således utredningens förslag om att tillsynen över den statliga sektorns informationssäkerhet bör samordnas och förstärkas. Riksrevisionen avstod dock från att föreslå vilken eventuell myndighet som kunde vara bäst lämpad att få ett sådant uppdrag, då granskningen endast berörde avsaknaden av tillsyn.

Riksrevisionen delar utredningens uppfattning att MSB genom sitt nuvarande uppdrag på informationssäkerhetsområdet rent kunskapsmässigt har förutsättningar att hantera ett tillsynsuppdrag. Utredningen har dock inte berört frågan om de svårigheter som finns med att samla tillsyn, främjande och normerande i en och samma myndighet och de avvägningar som då måste göras. Detta gäller särskilt då MSB utöver sin allmänt främjande roll även fördelar anlaget 2:4 för krisberedskap. Riksrevisionen vill därför uppmärksamma att ett eventuellt beslut att ge MSB mandat att utöva tillsyn på området kräver att gränssnittet mellan övriga myndigheter med liknande uppgifter på området blir tydligt. Det kräver också en tydlighet i kravställning på hur MSB i så fall rent organisatoriskt ska hantera sina olika roller internt i myndigheten.

Myndigheternas internrevision behöver utvecklas

Förslaget i betänkandet skulle innebära att respektive myndighets ledning bör intyga i årsredovisningen att myndigheten har en betryggande intern styrning och kontroll vad

gäller informationssäkerhet. I dag ska ledningen för de myndigheter som omfattas av 2 kap. 8 § förordningen om årsredovisning och budgetunderlag bedöma huruvida den interna styrningen och kontrollen vid myndigheten är betryggande.

Riksrevisionens granskning av myndighetens interna styrning och kontroll gäller främst den styrning och kontroll som är relevant för den finansiella rapporteringen. Kraven på myndighetens bedömning går redan i dag i detta avseende längre och omfattar all verksamhet i myndigheten, oavsett relevans för den finansiella rapporteringen. Förekomsten av en sådan bedömning från myndighetsledningen innebär inte tillkommande krav på revisorn att granska intern styrning och kontroll utöver vad som krävs för granskningen av årsredovisningen sammantaget.

Om det skulle förekomma ett separat krav på ett uttalande avseende den interna styrningen och kontrollen beträffande informationssäkerhet skulle detta kräva ökade granskningsinsatser och ökat krav på resurser vilket skulle medföra ökade kostnader för Riksrevisionen och därmed ett behov av ökat anslag. Riksrevisionen ställer sig därutöver tveksam till om det är motiverat att införa ett krav på ett separat uttalande beträffande informationssäkerhet. Det väcker bland annat frågor om riskerna för att röster höjs för att införa liknande krav på andra områden och verksamheter hos de myndigheter som omfattas av 2 kap. 8 § förordningen om årsredovisning och budgetunderlag. Myndigheterna har redan ett ansvar för att informationssäkerheten hanteras väl utifrån deras specifika verksamhetsrisker.

Riksrevisor Ulf Bengtsson har beslutat i detta ärende. Revisionsdirektör Thomas Dawidowski har varit föredragande. Revisionsdirektörerna Marcus Petterson och Per Dackenberg, säkerhetsskyddschef Ragnar Mårdh samt it-revisor Louise Ros har medverkat i den slutliga handläggningen.

Stockholm 2015-09-11

Ulf Bengtsson

Stockholm 2015-09-11

Thomas Dawidowski