10

DOMSTOLSVERKET
SVERIGES DOMSTOLAR

Avdelningen för domstolsutveckling, Rättsenheten

YTTRANDE

DATUM
2015-09-15

DIARIENR
1008-2015

Justitiedepartementet
103 33 Stockholm

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

Ert diarienummer Ju2015/2650/SSK

Domstolsverket ser positivt på att åtgärder vidtas i syfte att uppnå ett gemensamt förhållningssätt till informationssäkerhetsfrågor inom statsförvaltningen. Domstolsverket ser också positivt på det ökade ansvar och den tillsynsfunktion som föreslås tillkomma Myndigheten för samhällsskydd och beredskap.

Domstolsverket uppmärksammar, liksom också framhållits i betänkandet, att det avseende flera av förslagen finns behov av att närmare utreda förutsättningarna för och den närmare utformningen av dessa. Inför den fortsatta beredningen vill Domstolsverket framföra synpunkterna nedan. Domstolsverket vill även framföra följande synpunkter på förslag till ny förordning.

7 § Förordning för statliga myndigheters informationssäkerhet

Informationsklassificering ska i dag ske med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10). I förordningsförslaget föreslås att informationsklassificering även ska ske med utgångspunkt i krav på spårbarhet. Enligt Domstolsverket riskerar detta att bli så komplicerat och tidsödande att det inte fullt ut kommer att kunna genomföras. Verket bedömer därför att det finns skäl att i den fortsatta beredningen på nytt överväga hur klassificeringen bör ske.

8 § Förordning för statliga myndigheters informationssäkerhet

Enligt förslaget införs ett krav på myndigheter att använda *säkra* it-produkter. Genom skrivningens sista mening följer att, i de fall säkra it-produkter finns utpekade i verkställighetsföreskrifter som meddelats med stöd av förordningen, dessa ska användas. Domstolsverket ställer sig frågande till hur en myndighet, i de fall utpekade produkter saknas, ska kunna försäkra sig om att den produkt myndigheten avser att använda är en *säker* it-produkt. Det är otydligt vad som avses med en säker it-produkt.

Avsnitt 9.2.5 Informationssäkerhet som en del av myndighetens revision

Utredningen hänvisar i avsnitt 9.2.5 till Riksrevisionens årsrapport från 2007 där Riksrevisionen konstaterar att den interna kontrollen behöver stärkas eftersom granskning visat på flera olika typer av svagheter i myndigheternas interna styrning och kontroll. Det framgår dock inte att regeringen därefter vidtog åtgärder för att stärka den interna kontrollen genom förordning om intern styrning och kontroll (2007:603), som trädde ikraft den 1 januari 2008. Förordningen gäller för de myndigheter under regeringen som ska ha en internrevision inrättad i enlighet med internrevisionsförordningen.

Utredningens bedömning är att revision av informationssäkerhet bör utvecklas. Enligt Domstolsverket finns det dock oklarheter kring hur begreppet revision används i betänkandet, dvs. vilken revision det är som avses. Exempelvis förekommer sammansättningar av begreppet som framstår som otydliga, såsom *säkerhetsrevision* (betänkandet, s. 53), *intern revision* (betänkandet, s 235) och *internrevision* (betänkandet, s 235). Till det kommer att begreppen *uppföljning* respektive *revision* i hög utsträckning används synonymt även om det kan ifrågasättas om detta är avsiktligt. Det finns olika betydelser i begreppet revision beroende på dess syfte eller uppdrag, exempelvis internrevision, miljörevision, externrevision och interna revisioner enligt ISO-27000-familjen. Det är också skillnad mellan internrevision enligt internrevisionsförordningen (2006:1228) och interna revisioner enligt den ISO-standard som ligger till grund för MSB:s föreskrifter. Enligt Domstolsverket är det en brist i utredningen att det inte klargjorts vilken revision som avses när begreppet revision används.

Slutligen är Domstolsverket tveksam till förslaget att införa ett särskilt rapporteringskrav i förordning (2000:605) om årsredovisning och budgetunderlag för att tydliggöra myndighetsledningens ansvar för att upprätthålla säkerhet i myndighetens informationshantering (betänkandet, s. 230). Intern styrning och kontroll inom såväl informationssäkerhetsområdet som inom övriga områden ska redan i dag beaktas i samband med att myndighetsledningen intygar att myndighetens interna styrning och kontroll är betryggande. Det vore därför olyckligt att i förordning om årsredovisning och budgetunderlag peka ut informationssäkerhet som en enskild viktig parameter bland flera inom intern styrning och kontroll. Beträffande myndighetsförordningen (2007:515) anser verket att ansvaret för informationssäkerhetsområdet redan är inkluderat då myndighetsledningens ansvar avser all verksamhet.

Detta yttrande har beslutats av tf. biträdande chefsjuristen Amanda Rörby. Föredragande har varit hovrättsassessorn Lina Sandin. I handläggningen har också deltagit säkerhetschefen Håkan Sonesson och internrevisorn Mikael Boo.

Amanda Rörby