KAMMARKOLLEGIET
IS/IT-funktionen

Pendar Solimani
pendar.solimani@kammarkollegiet.se
08-700 06 78

2015-09-15
Dnr 3.1-2438-15
Ert dnr Ju2015/2650/SSK

Justitiedepartementet
103 33 Stockholm

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

Kammarkollegiet har anmodats att yttra sig över rubricerat betänkande. Utifrån de aspekter som Kammarkollegiet har att beakta vill kollegiet framföra följande.

Allmänna synpunkter

Kammarkollegiet anser att utredningen i allmänhet innehåller generella oklarheter och att det saknas en tydlig koppling mellan utredningens beskrivande delar och de förslag som lämnas.

Exempelvis framgår det av utredarens direktiv att denne ska ”klargöra begrepp som används inom informationssäkerhetsområdet och vid behov föreslå förtydligande eller alternativa benämningar och definitioner, särskilt av sådana som används i förslaget till nationell strategi”.

Den definition som anges i den föreslagna 4 § förordningen för statliga myndigheters informationssäkerhet är otydlig. Utredningen ger i olika avsnitt överlappande beskrivningar. Avseende definitionen ”informationssäkerhet” bör begreppet även innefatta att det är möjligt att säkerställa vem som är avsändare av information samt att det är rätt avsändare.

Utredningen anser att informationssäkerhet är känt och etablerat i statsförvaltningen och att begreppet därmed inte behöver en förtydligad definition. Samtidigt är det uppenbart att området fortfarande innebär väsentliga utmaningar för myndigheterna vad gäller både styrning och genomförande, vilket också utredningar från både Riksrevisionen och Myndigheten för samhällsskydd och beredskap (MSB) vittnar om. Kammarkollegiet anser utifrån rollen som en förvaltningsmyndighet,

utan särskilda krav på informationssäkerhetsarbete, att denna passiva hållning till begreppet är olycklig.

Kammarkollegiet vill framhålla risken för att just avsaknaden av precision i vad som avses, och vad som därmed förväntas av myndigheterna, bidrar till en del av de brister som utredningarna också pekar på.

Mot bakgrund av att utredningen lägger förslag om förstärkt styrning är det en påtaglig brist att utredningen varken har analyserat rådande definition av informationssäkerhet eller den befintliga styrningen och dess betydelse för de iakttagelser som Riksrevisionen och MSB gjort. Det innebär att det är svårt att ta ställning till bland annat förslagen om skärpta krav på ledningssystem och förstärkt tillsyn. Kammarkollegiet menar att det inte kan uteslutas att nuvarande styrning och organisering är tillräcklig och att området i första hand behöver fokusering och avgränsning snarare än förstärkt reglering och mer tillsyn.

Revision

Utredningens bedömning är att revision av informationssäkerhet bör utvecklas och att myndighetsledningens ansvar för att upprätthålla säkerhet i myndighetens informationshantering ska förtydligas genom rapporteringskrav i förordningen (2000:605) om årsredovisning och budgetunderlag. Utredningen använder flera ord inom häraden uppföljning/revision. Exempelvis används säkerhetsrevision (s. 53), intern revision (s. 235), internrevision (s. 235) och dessutom används uppföljning och revision i hög utsträckning som ett samlat begrepp utan att det framgår om de ska ses som synonymer eller stå för två olika saker. Kammarkollegiet menar att det i utredningen borde varit relevant att tydliggöra vad som menas med revision, eftersom respektive läsare utgår från den referensram som vederbörande har.

Det är i sammanhanget viktigt att skilja på internrevision enligt internrevisionsförordningen (2006:1228) och begreppet intern revision enligt ISO-27000 (LIS). Intern revision (löpande kontroller) enligt ISO ingår som en del i ledningssystemet. Internrevision i enlighet med internrevisionsförordningen och internationella standards för området bör inte, med hänsyn till syfte och uppdrag, vara en del av ledningssystemet.

Bestämmelserna i internrevisionsförordningen är kopplade till internationella standarder för internrevision som ges ut av The Institute of Internal Auditing (IIA). Utgångspunkten för om en revision ska ske är en bedömning av verksamhetens risker. Riskanalysen ska omfatta all verksamhet som myndigheten bedriver och ansvarar för och ska utmynna i en prioritering av granskningsområden utifrån risk och väsentlighet. Eftersom informationssäkerhet är ett bland många andra områden som ingår i myndighetens ansvarsområde kommer internrevisionens insatser i detta specifika område att ske i relation till riskerna i alla övriga områden.

Offentlig upphandling

Utgångspunkten att "staten ska ställa tydliga krav vid upphandling på it-området" inom informationssäkerhet är i och för sig invändningsfritt. Kollegiet anser dock att utredningen inte tycks vara tillräckligt insatt i upphandlingslagstiftningen varför utredningen innehåller brister i dessa avseenden.

Kraven i 15 och 16 §§ i förslaget till förordningen för statliga myndigheters informationssäkerhet medför att upphandlande myndigheter, vid kravställning i upphandling, blir styrda av resultatet av informationsklassningen och riskanalysen. Konsekvensen blir att upphandlande myndigheter, per automatik, måste ställa ett visst krav oberoende av det enskilda upphandlingsföremålet. Enligt Kammarkollegiets mening kan detta strida mot upphandlingsrättslig lagstiftning eftersom varje enskilt krav vid en upphandling måste vara proportionerligt och vara kopplat till det aktuella upphandlingsföremålet. Vidare kan en sådan reglering strida mot 6 kap. 2 § lagen (2007:1091) om offentlig upphandling (LOU) och 7 kap. 2 § lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster (LUFS) under förutsättning att kraven är utformade som tekniska specifikationer. Kammarkollegiet vill påpeka att leverantörer även ska ha möjlighet att visa att kraven på tekniska specifikationer uppfylls på ett likvärdigt sätt i förhållande till hänvisade standarder. Dessutom medför förslaget att marknaden av potentiella leverantörer koncentreras till enbart de leverantörer som tillhandahåller säkra och certifierade IT-produkter. Detta kan medföra en begränsning av konkurrensen på den inre marknaden, vilket strider mot syftet med upphandlingslagstiftningen och således är kontraproduktivt.

Oaktat stycket ovan har Kammarkollegiet på föreliggande underlag svårt att ta ställning till huruvida de åtgärder som föreslås är genomförbara eller om förslagen har brister innebärande effektivitetsförluster eller betydande kostnader för statsförvaltningen som inte kan motiveras. Exempelvis är den IT-upphandling som genomförs av statliga myndigheter av betydande omfattning och omsätter betydande belopp. De centrala IT-ramavtalen omsätter ca 7,5 miljarder kr och är en mindre del av IT-upphandlingen i staten. Den samlade statliga upphandlingen av IT-produkter och tjänster i Sverige bör omfatta mer än ca 40 miljarder kr. Förslaget att MSB ska ta fram skyddsprofiler som anger minimikrav på säkerhet i vanligt förekommande IT-produkter som används av statliga myndigheter saknar, precis som övriga förslag i punkten 9.3.1, tydliga avgränsningar. Detta kan innebära att både kostnader och krav på resurser är underskattade.

Det hävdas felaktigt i betänkandet att Kammarkollegiets ramavtal i praktiken leder till att "det i huvudsak är tre stora leverantörer som levererar exempelvis drifttjänster" (s. 239). Vad gäller Kammarkollegiets statliga IT-ramavtal har samtliga dessa tilldelats till betydligt fler än tre leverantörer.

Utredningen anför även att "LOU-systemet tenderar att gynna det lägsta priset när andra faktorer är lika" (s. 242). Istället hänvisas därför till möjligheten att genomföra upphandlingar enligt LUFS. Dessutom hänvisas till "upphandlingsförfarandet" enligt LUFS utan att det anges vilket specifikt upphandlingsförfarande som avses. Kammarkollegiet kan, i dylika fall, inte urskilja någon skillnad som motiverar användandet av LUFS framför LOU. Båda lagarna bygger på samma grundläggande principer vilket innebär att oaktat vilken av lagarna som tillämpas vid en upphandling måste ställda krav vara proportionerliga och kopplade till upphandlingsföremålet.

Det bör även påpekas att upphandlingar som genomförs med lägsta pris som tilldelningsgrund inte, per automatik, medför att kvaliteten på upphandlingsföremålet blir låg. Tvärtom kan det vara väldigt högt ställda kvalificeringskrav som säkrar hög kvalitet.

Mot bakgrund av det ovan anförda avstyrker Kammarkollegiet därför utredningens förslag avseende förordningen för statliga myndigheters informationssäkerhet.

Detta remissvar har beslutats av chefen för IS/IT-funktionen Johan Magnusson. I den slutliga handläggningen har chefen för Ekonomi- och förvaltningsfunktionen, Martin Sundelius, enhetschefen för IT-upphandlingen vid avdelningen Statens inköpscentral, Hans Sundström, internrevisionschefen Lars Agerberg och förvaltningsledaren Anna Rönmark deltagit. Föredragande har varit verksjuristen Pendar Solimani.

Johan Magnusson

Pendar Solimani