Strålsäkerhetsmyndigheten
Swedish Radiation Safety Authority

Justitiedepartementet
103 33 Stockholm

Yttrande

Vårt datum: 2015-09-15
Diarienr: SSM2015-2603

Yttrande över betänkandet SOU 2015:23 – Informations- och cybersäkerhet i Sverige

Övergripande synpunkter

Allmänt

Strålsäkerhetsmyndigheten (SSM) är positiv till att styrningen av de statliga myndigheternas informationssäkerhet förbättras genom att det tas fram en strategi för informations- och cybersäkerhet i staten. Dock är några av förslagen så övergripande beskrivna att de är svåra att bedöma, bland annat vad gäller den nationella styrmodellen och kravet på incidentrapportering. Perspektivet behöver också lyftas för att se till att de föreslagna regelverken harmonierar med bland annat den föreslagna regleringen på säkerhetsskyddsområdet och MSB:s förslag på föreskrifter för statliga myndigheters informationssäkerhet. Detta är särskilt viktigt eftersom förordningsförslaget i NISU 2014 inte avser att träffa säkerhetsskyddslagens tillämpningsområde samtidigt som detta tillämpningsområde föreslås utvidgas.

SSM kan konstatera att myndighetens ansvar inom informationssäkerhet saknas i uppräkningen på myndigheter med särskilt ansvar inom informationssäkerhetsområdet (kapitel 7) och endast nämns översiktligt i kapitel 9. I myndighetens svar på remissen avseende SOU 2015:25 En ny säkerhetsskyddslag föreslår SSM att myndigheten ska vara säkerhetsstödjande myndighet och att avgränsning/samverkan mellan SSM och Affärsverket svenska kraftnät respektive MSB bör regleras. Detta bör beaktas i den av utredningen föreslagna översynen av den sektorsvisa tillsynen av informationssäkerheten.

SSM delar utredningens uppfattning att vissa av förslagen kan rymmas inom myndigheternas befintliga budget, men samtidigt anser SSM att den samlade ambitionshöjningen ofrånkomligen kommer att medföra ett ökat resursbehov för de enskilda myndigheterna.

Kap. 9 Överväganden och förslag

9.2.1 En nationell styrmodell

SSM är positiv till en gemensam modell för att styra och kontrollera informationssäkerheten i svensk statsförvaltning. Myndigheten anser att denna styrmodell måste baseras på etablerade standarder inom området för att man ska få en enhetlighet i hela samhället och inte bara inom statsförvaltningen.

Myndigheten vill även betona vikten av samråd med övriga myndigheter i utvecklandet av styrmodellen; särskilt med myndigheter som liksom SSM har ett ansvar för tillsyn av informationssäkerhet inom den kärntekniska sektorn (se avsnitt 9.2.4 i utredningen).

9.2.3 En ny förordning om statliga myndigheters informationssäkerhet

Utredningen föreslår att en ny förordning om statliga myndigheters informationssäkerhet införs. Förslaget innebär specifikt att vissa begreppsdefinitioner införs i en inledande bestämmelse. Myndigheten anser att man i det fortsatta arbetet genomgående bör använda de begrepp och definitioner av dessa som SIS TR 50 anger. Förslaget i 5 § att myndigheten endast ska *beakta* behovet av ett ledningssystem för informationssäkerhet riskerar att göra styrningen otydlig. Det är därför bättre att hänvisa till standarden SS ISO/IEC 27001:2014 med förslagsvis följande text: ”Myndigheten ska upprätta, införa, underhålla och ständigt förbättra ett ledningssystem för informationssäkerhet, inklusive nödvändiga processer enligt kraven i den svenska standarden för ledningssystem för informationssäkerhet.” Genom att på detta sätt hänvisa till vedertagna standarder inom området ökar förutsättningarna för att arbetet bedrivs systematiskt och enhetligt inom den offentliga förvaltningen och att det även blir en likartad hantering och begreppsapparat som i det privata näringslivet.

I 7 § bör ordet informationsprocesser bytas ut mot verksamhetsprocesser. Enligt SIS TR 50 ingår inte spårbarhet som en av de grundläggande aspekterna. Spårbarhet är en säkerhetsåtgärd som är en funktion till de övriga och bör därför inte finnas med i denna uppräkning.

Det föreslås vidare att 31–33 §§ i den nuvarande förordningen (2006:942) om krisberedskap och höjd beredskap flyttas till den nya förordningen (12–14 §§ Säkra kryptografiska funktioner). SSM vill i sammanhanget erinra om det förslag till förändring av krisberedskapsförordningen som innefattas i den redovisning av det regeringsuppdrag till MSB avseende det civila försvaret som nyligen remissbehandlats (Ju2015/30/SSK respektive Ju2015/67/SSK). De definitioner som i denna redovisning föreslås införas i krisberedskapsförordningen avseende säkra kryptografiska funktioner bör, om regeringen beslutar enligt förslaget, överföras till den nya förordningen om informationssäkerhet som en följd av att 31–33 §§ överflyttas.

9.3 Staten som tydligare kravställare

SSM stöder bilden av att det finns ett behov av utvecklad beställarkompetens. För att öka kompetensen inom området behövs ett ökat stöd till myndigheterna men också att det tas fram utbildningar som är anpassade till den offentliga sektorn.

9.4.1 Statliga nätverk

Utredningen föreslår att de statliga myndigheter som anges i bilagan till krisberedskapsförordningen ansluts till SGSI, vilket myndigheten ser positivt på. SSM efterlyser i sammanhanget, inte minst mot bakgrund av de resonemang som förs avseende SGSI:s nuvarande begränsningar, en analys av, och i förlängningen en strategi för, civila totalförsvarsmyndigheters nyttjande av Försvarets Telenät (FTN) och därmed sammanhängande kommunikationsnät, såsom FM IP-nät (FMIP). SSM menar att frågan om säkrare kommunikation i staten måste ses i ett helhetsperspektiv, och då även beakta de krav, såväl avseende konfidentialitet som tillgänglighet, vilka ställs på verksamhet under höjd beredskap eller under störda förhållanden. SSM delar inte fullt ut utredningens slutsats att (Försvarsmakts-) externa aktörer vars verksamhet är av kritisk betydelse för samhället idag har tillgång till FTN och FMIP.

9.4.2 Säkra kryptografiska funktioner.

SSM bejakar utredningens förslag att den nationella strategin med åtgärdsplan för säkra kryptografiska funktioner som återges i Bilaga 4 till utredningen kan tjäna som bas för att utveckla processen för säkra kryptografiska funktioner. Strategin bör emellertid omarbetas för att omhänderta konsekvenserna av en förändrad säkerhetsskyddslagstiftning, då det kan antas att den informationsmängd som kommer att falla under lagstiftningens tillämpningsområde kan komma att utökas väsentligt.

9.5 Incidenthantering

SSM är positiv till krav på obligatorisk rapportering av incidenter och att detta kan skapa en överblick över riskerna på informationssäkerhetsområdet. Det kan ge möjligheter till ökad kunskap för de enskilda myndigheterna. Däremot är det mycket viktigt att frågan om vad som ska rapporteras till MSB respektive Säkerhetspolisen inom säkerhetsskyddsområdet utreds vidare. Otydlighet om detta riskerar att leda till både felrapportering och att åtgärder försenas.

I detta ärende har generaldirektören Mats Persson beslutat. Säkerhetschefen Elisabeth Öhlén har varit föredragande. I den slutliga handläggningen har också enhetschefen Christer Sandström, signalskyddschefen Jonas Lindgren och verksjuristen Martin Henrysson deltagit.

STRÅLSÄKERHETSMYNDIGHETEN

Mats Persson

Elisabeth Öhlén