Strålsäkerhetsmyndigheten
Swedish Radiation Safety Authority

Försvarsdepartementet
fo.remissvar@regeringskansliet.se

Remissvar
Datum: 2021-12-21
Er referens: Fö2021/00796
Diarienr: SSM2021-6173
Dokumentnr: SSM2021-6173-2
Handläggare: Anders Verneholt
Telefon: 08-799 43 99

Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

Sammanfattning

- Strålsäkerhetsmyndigheten (SSM) anser att det i det fortsatta lagstiftningsarbetet ytterligare bör belysas i vilken utsträckning de tekniska säkerhetsgranskningar som nämns i utredningen är nödvändiga vid tillsyn av informationssystem, om tillsynsmyndigheter kan ta hjälp av expertkompetens utanför den egna myndigheten vid sådan granskning samt hur förslaget förhåller sig till rättighetsskyddet.

- SSM föreslår att en uppgiftsskyldighet införs för samrådsmyndigheten. Uppgifts-skyldigheten bör bl.a. avse uppgifter eller upplysningar om omfattningen av samrådsmyndighetens granskning och vilka omständigheter samrådsmyndigheten har beaktat och på vilket sätt dessa bedömts.

- SSM delar inte utredningens bedömning att eventuella kostnader för tillsynsmyndigheterna inte påverkas i någon större utsträckning för det fall SSM som tillsynsmyndighet förväntas genomföra de föreslagna tekniska säkerhetsgranskningarna. För att kunna utföra sådana kontroller skulle SSM behöva rekrytera ett antal personer med särskild kompetens som det idag råder brist på. SSM uppskattar att anslaget skulle behöva förstärkas med mellan 5-10 miljoner kronor.

- SSM delar utredningens bedömning att det i dagsläget inte föreligger förutsättningar att införa en certifieringsordning för IKT-produkter, -tjänster och -processer.

- SSM välkomnar utredningens förslag att regeringen ska ge ett uppdrag åt Försvarets materielverk (FMV) att utreda frågan om att införa en certifieringsordning för IKT-produkter, -tjänster och -processer vidare i samråd med de övriga myndigheterna som ingår i det nationella cybersäkerhetscentret.

- SSM stödjer också utredningens förslag om att eventuellt kompletterande krav på ett så kallat myndighetsgodkännande inte bör vara aktuellt förrän en utvärdering av befintliga och kompletterande bestämmelser har genomförts.

Strålsäkerhetsmyndigheten
Swedish Radiation Safety Authority

SE-171 16 Stockholm
Solna strandväg 96
Tel:+46 8 799 40 00
Fax:+46 8 799 40 10
E-post: registrator@ssm.se
Webb: stralsakerhetsmyndigheten.se

- SSM välkomnar förslaget att säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem ska överföras till säkerhetsskyddslagen samt att befintligt krav på verksamhetsutövare att göra en särskild säkerhetsskyddsbedömning utvidgas till att även omfatta planerade väsentliga förändringar av informationssystem som kan ha betydelse för säkerhetskänslig verksamhet.

- Vidare tillstyrker SSM förslaget om införandet av en lämplighetsprövning vid driftsättning eller en väsentlig förändring av ett informationssystem och kravet på att lämplighetsprövningen ska dokumenteras.

- SSM ser positivt på de förslag utredningen presenterar avseende ett utvidgat samrådsförfarande och en stärkt samrådsroll för Säkerhetspolisen och Försvarsmakten.

Synpunkter

Avsnitt 12.5.6 Det föreligger f.n. inte behov av en nationell särskild ordning för certifiering i säkerhetskänslig verksamhet
SSM delar utredningens bedömning att det i dagsläget inte föreligger förutsättningar att införa en certifieringsordning för IKT-produkter, -tjänster och -processer. SSM välkomnar utredningens förslag att regeringen ska ge ett uppdrag åt FMV att utreda frågan vidare i samråd med de övriga myndigheterna som ingår i det nationella cybersäkerhetscentret.

Kapitel 13 Krav på godkännande och utvidgat samrådsförfarande för informationssystem
SSM välkomnar förslaget att säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem ska överföras till säkerhetsskyddslagen samt att befintligt krav på verksamhetsutövare att göra en särskild säkerhetsskyddsbedömning utvidgas till att även omfatta planerade väsentliga förändringar av informationssystem som kan ha betydelse för säkerhetskänslig verksamhet.

Vidare tillstyrker SSM förslaget om införandet av en lämplighetsprövning vid driftsättning eller en väsentlig förändring av ett informationssystem och kravet på att lämplighetsprövningen ska dokumenteras.

SSM ser positivt på de förslag utredningen presenterar avseende ett utvidgat samrådsförfarande och en stärkt samrådsroll för Säkerhetspolisen och Försvarsmakten.

SSM stödjer också utredningens förslag om att eventuellt kompletterande krav på ett så kallat myndighetsgodkännande inte bör vara aktuellt förrän en utvärdering av befintliga kompletterande bestämmelser har genomförts. SSM delar här Säkerhetspolisens och Försvarsmaktens bedömning att det inte finns skäl att flytta ansvaret för säkerhetsskyddet från verksamhetsutövaren till en annan myndighet och att Säkerhetspolisen och Försvarsmakten istället ges en förstärkt samrådsroll.

Avsnitt 13.8 Ytterligare stärkt samrådsroll
SSM föreslår att en uppgiftsskyldighet införs för samrådsmyndigheten. Uppgifts-skyldigheten bör bl.a. avse uppgifter eller upplysningar om omfattningen av samråds-myndighetens granskning och vilka omständigheter samrådsmyndigheten har beaktat och på vilket sätt dessa bedömts.

Innan ett informationssystem som kan förutses komma att behandla säkerhetsskydds-klassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller om obehörig åtkomst till informationssystemet kan medföra en skada för Sveriges säkerhet som inte är obetydlig ska verksamhetsutövaren samråda med samrådsmyndigheten.[1] Det är dock tillsynsmyndigheten som svarar för tillsyn av säkerhetsskyddslagen, inbegripet säkerhetsskyddet för informationssystem.[2] SSM anser att det bör eftersträvas likhet i dessa myndigheters bedömningar av säkerhetsskyddet. För de fall då samrådsmyndigheten och tillsynsmyndigheten inte är samma myndighet bör därför tillsynsmyndigheten kunna infordra uppgifter som är relevanta för tillsynen.

Kapitel 14 Tillgång till informationssystem vid tillsyn

SSM anser att det i det fortsatta lagstiftningsarbetet ytterligare bör belysas i vilken utsträckning de tekniska säkerhetsgranskningar som nämns i utredningen är nödvändiga vid tillsyn av informationssystem, om tillsynsmyndigheter kan ta hjälp av expert-kompetens utanför den egna myndigheten vid sådan granskning samt hur förslaget förhåller sig till rättighetsskyddet. Skälen för SSM:s inställning redovisas nedan.

Tillsynsmyndigheten ska i den omfattning som det behövs för tillsynen, ha rätt att få tillgång till informationssystem som används i verksamhet som omfattas av tillsyn. Utredningen konstaterar att tillsynsmyndigheten vid tillsyn som regel behöver kontrollera ”vilka säkerhetsskyddsåtgärder som vidtagits i informationssystem” (s. 472). SSM instämmer i den bedömningen. Författningsförslaget i denna del motiveras dock av att det ”i de flesta fall” inte är tillräckligt att genomföra kontroller genom designgranskning, granskning av underlag samt intervjuer. Istället måste utredningens förslag förstås så att tillsynsmyndigheten aktivt ska kontrollera och testa funktionaliteten och tillräckligheten hos sådana säkerhetsskyddsåtgärder. Här nämns t.ex. ”simulerade angreppsförsök”, och att testerna ska avse ”säkerhetsskyddsåtgärderna i systemet tillsammans med dess omkringliggande infrastruktur, s.k. teknisk säkerhetsgranskning”. SSM anser att sådana tester går längre än vad som motiveras av det nyss identifierade behovet att kontrollera *vilka* säkerhetskyddsåtgärder som har vidtagits. I förhållande till det syftet finns det skäl att ifrågasätta om utredningen gjort en korrekt bedömning av hur effektiv den allmänna tillsynsbefogenheten enligt säkerhetsskyddslagen är. SSM noterar att det saknas resonemang om andra utformningar för att uppnå syftet med de kontroller som diskuteras. Vidare fordrar tillsynsinsatser av den typ som utredningen talar om helt andra förmågor och tillgång till spetskompetens hos tillsynsmyndigheten. Denna förmåga kräver långsiktighet och resurser för att byggas upp, bl.a. då det råder konkurrens om arbetskraft med tillräckliga kunskaper på området. SSM har i dag en kompetens som i dessa avseenden är på en mer generell nivå. SSM har därmed inte kapacitet att utföra de tekniska kontroller, t.ex. simulerade angreppsförsök, som utredningen menar krävs för att bedöma om en verksamhetsutövare har vidtagit tillräckliga säkerhetsskyddsåtgärder eller för att påvisa att en verksamhetsutövares informationssystem inte är exponerat mot oskyddade nätverk. Mot den bakgrunden anser SSM att det bör klarläggas i vilken utsträckning den förmågan är nödvändig för tillsynsmyndigheterna att bygga upp. SSM anser också att, för det fall tillsynsmyndigheten förväntas genomföra de föreslagna tekniska säkerhetsgranskningarna, det bör finnas en möjlighet för tillsynsmyndigheten att vid genomförande av tillsyn begära stöd från myndigheter med särskild expertkompetens för uppgiften.

SSM anser också att det finns anledning att närmare klargöra innebörden i de begrepp som används, såsom simulerade angreppsförsök och teknisk säkerhetsgranskning, vilka anges i avsnitt 14.2 där skälen för förslaget redogörs för. Motsvaras dessa av moment eller

[1] Se den föreslagna bestämmelsen 3 a kap. 2 § säkerhetsskyddslagen (2018:585).
[2] Se 8 kap. 1 § säkerhetsskyddsförordningen (2021:955), jfr även den föreslagna bestämmelsen 6 kap. 3 § säkerhetsskyddslagen

begrepp som beskrivs på andra platser i betänkandet anser SSM att det bör tydliggöras. Exempelvis behandlas i avsnitten 7.7–7.9 olika aspekter av säkerhet vid utveckling och konfiguration samt testning. Här återfinns moment som penetrationstest och säkerhetsgranskning. I avsnitt 14.2 används inte samma termer vilket ger viss osäkerhet om förväntade åtgärder.

Bedömningen av förslagets förenlighet med 2 kap. 6 § regeringsformen och artikel 8 Europakonventionen är kortfattad och beaktar att tillgången till system avser en avgränsad krets, nämligen aktörer som använder informationssystem i säkerhetskänslig verksamhet (s. 473). SSM vill påpeka att utöver själva verksamhetsutövaren och användare hos verksamhetsutövaren kan informationssystemen i sig beröra andra fysiska personer vilket också bör beaktas. Det underlättar tillsynsmyndighetens proportionalitetsbedömning om det tydligt har belysts under lagstiftningsförfarandet hur tillsynsåtgärderna förhåller sig till integritetsrättsliga principer och de registrerades fri- och rättigheter.

Kapitel 17 Konsekvensbeskrivning
SSM delar inte utredningens bedömning att eventuella kostnader för tillsynsmyndigheterna inte påverkas i någon större utsträckning, för det fall SSM som tillsynsmyndighet förväntas genomföra de föreslagna tekniska säkerhetsgranskningarna. SSM bedömer att en utökad förmåga och fördjupad kompetens, vilket krävs för att myndigheten självständigt ska kunna utföra t.ex. aktiva tekniska kontroller av verksamhetsutövarnas informationssystem, kräver ytterligare anslag. För att kunna utföra sådana kontroller skulle SSM behöva rekrytera ett antal personer med särskild kompetens. Myndigheten uppskattar att anslaget skulle behöva förstärkas med mellan 5–10 mnkr.

I detta ärende har generaldirektören Nina Cromnier beslutat. Utredaren Anders Verneholt har varit föredragande. I den slutliga handläggningen har också säkerhetsskyddschefen Nina Persson, verksjuristen Kim Elofsson och inspektören Patrick Yliaho deltagit.

Detta beslut expedieras utan underskrift.

STRÅLSÄKERHETSMYNDIGHETEN

Nina Cromnier

Anders Verneholt