FÖRSVARSMAKTEN

Datum	Beteckning	
2015-09-15	FM2015-14342:2	Sida 1 (7)

Sändlista

Ert tjänsteställe, handläggare	Ert datum	Er beteckning
Linda Ericson, SSK	2015-05-06	Ju2015/2650/SSK

Vårt tjänsteställe, handläggare	Vårt föregående datum	Vår föregående beteckning
Magnus Sandbu, +46 (0)8 788 8225, magnus.sandbu@mil.se		

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

1. Sammanfattning

Försvarsmakten anser i enlighet med utredningen att det finns ett behov av att stärka samhällets informationssäkerhet, och att det är viktigt att praktiska förbättringsåtgärder snarast kan påbörjas.

Försvarsmakten bedömer att utredningens förslag sammantaget kan utgöra tillräcklig grund för att förbättra samhällets informationssäkerhet – även om förslaget innehåller kvarstående osäkerheter och oklarheter. Försvarsmakten tillstyrker därför att huvuddelen av utredningens förslag genomförs, se vidare nedan.

Försvarsmakten anser dock att vissa delar i förslaget bör utvecklas innan de realiseras – främst vad avser samordningen med ny säkerhetsskyddslag, myndigheters föreskrifts- och tillsynsrätt samt definitioner av begrepp.

Försvarsmaktens anser vidare att utredningens författningsförslag bör ses över i sin helhet.

Försvarsmakten anser också att myndighetsrådets reella befogenheter och styrmöjligheter måste klarläggas samt att det därefter görs en fördjupad resursbedömning vad avser förslaget om att inrätta ett myndighetsråd.

Postadress	Besöksadress	Telefon	Telefax	E-post, Internet
Försvarsmakten	Lidingövägen 24	08-788 75 00	08-788 77 78	exp-hkv@mil.se
107 85 Stockholm				www.forsvarsmakten.se

Synpunkter som lämnas i första stycket om säkra kryptografiska funktioner är utarbetade i samråd med Myndigheten för samhällskydd och beredskap, Försvarets materielverk och Försvarets radioanstalt.

2. Samordning med ny säkerhetsskyddslag

Utredningens förslag bör i större utsträckning samordnas med förslagen om en ny säkerhetsskyddslag (SOU 2015:25). En sådan förbättrad samordning bedöms vara nödvändig för effektivt införande av såväl ny säkerhetsskyddslag som NISU – med hänsyn till att båda bestämmelserna reglerar delar inom informationssäkerhetsområdet.

Behov av förbättrad samordning föreligger i bl a följande avseenden:
- Författningsförslaget bör tillföras en definition för it-system som är liktydig med den nya säkerhetsskyddslagens förordningsförslag (7 §)
- Myndigheters rätt till att utfärda föreskrifter respektive utöva tillsyn.

Utredningen föreslår att förordningen träder i kraft 1 januari 2016. Ikraftträdandet för ny säkerhetsskyddslag föreslås däremot ske ett år senare. Kvarstående arbete med NISU innan ikraftträdandet måste tillgodose samordning med ny säkerhetsskyddslag.

3. Strategier

Försvarsmakten anser att strategiens andra mål ska ändras till den formulering som anges i avsnitt 9.1.3 och bilaga 5, d v s ”att staten blir en tydlig kravställare”. Det är inte upphandling inom enbart it-området som påverkar möjligheterna att upprätthålla erforderlig informationssäkerhet. Infrastruktur, t ex elförsörjning, är exempel på annat sådant område.

Arbete med att utveckla en kommande strategi för försvaret av riket och dess oberoende mot antagonistiska hot med såväl defensiva som offensiva förmågor, som betänkandet anger i avsnitt 9.1.4, bör inledas snarast möjligt.

Utredningen anger att man kan gå vidare med en sådan senare strategi först efter det att utredningens föreslagna strategi för statens informations- och cybersäkerhet är realiserad.

Med hänsyn till den snabba utvecklingen inom området informations- och cybersäkerhet, samt andra direkt och indirekt påverkande områden, bör utveckling av flera strategier och andra övergripande åtgärder ske parallellt.

4. Myndigheters ansvar – föreskrifter och tillsyn

Informationssäkerheten för lägre skyddsvärden, som förslaget avser att reglera, inverkar på förutsättningar för säkerhetsskydd av de högre skyddsvärden som regleras av säkerhetsskyddslagen respektive -förordningen – och vice versa.

Författningsförslagen avseende ansvarsfördelning mellan myndigheter – främst avseende föreskriftsrätt och tillsynsansvar – måste därför omarbetas. Grundläggande princip bör i stället vara att myndighet som har föreskriftsrätt och tillsynsansvar för säkerhetsskyddet jml säkerhetsskyddslagen och -förordningen också har det för informationssäkerheten för de lägre skyddsvärdena. I det fall avsteg måste göras från denna princip bör krav ställas på samråd med dessa myndigheter.

I övrigt måste ändringar göras vad avser myndigheters ansvar enligt nedan.

En myndighets val och användning av säkra it-produkter kan påverka även andra myndigheter, vilket indirekt berörs i 8 §. Texten i 8 § bör därför ändras till "... *berörda myndigheters* förmåga att bedriva sin verksamhet".

I de av betänkandets bestämmelser som utgår från Försvarsmaktens tillsynsansvar, jml 39 § säkerhetsskyddsförordningen, bör *Försvarsunderrättelsedomstolen* och *Statens inspektion för försvarsunderrättelseverksamheten* tillföras.

5. Definitioner av begrepp

Utöver tidigare nämnda synpunkter rörande definitioner, bör övervägas att närmare tydliggöra nedanstående begrepps innebörd.

- Säkra respektive certifierade it-produkter (16§)
- Säkra kommunikationsnät (11 §)
- Utvecklade krav- och skyddsnivåer (7 §)
- Särskilda uppgifter inom informationssäkerhetsområdet (18 §)
- Säkra kryptografiska funktioner (12-14 §§)

6. Upphandling och utveckling

I förslaget till 15 § måste förtydligas vilken myndighet som ska anses vara beställare i fall en myndighet genomför upphandlingar för en eller flera andra myndigheter.

Innebörden av begreppet leverantör (15 §) måste även förtydligas. Begreppet kan exempelvis avse en eller flera av nedanstående:

- Återförsäljare av it-produkter – troligtvis mest relevant vid upphandling av COTS-produkter).
- Företag som tillverkar it-produkter eller har produktansvar.
- En annan statlig myndighet.

Kravställningen i 16 § kan misstolkas till att enbart omfatta själva upphandlingsprocessen och måste omformuleras, exempelvis till:

"Endast säkra och certifierade it-produkter som är avsedda att användas i samhällsviktig verksamhet som myndigheten bedriver eller ansvarar för ska användas...".

7. Vissa ansvarsförhållanden

I förslaget om myndighetens informationssäkerhetsarbete (6 §) anser Försvarsmakten att myndighetschefens ansvar för informationssäkerheten ska förtydligas. Exempel på ett sådan kompletterande text kan vara: *"Myndighetens chef ansvarar för informationssäkerheten i myndighetens verksamhet. Under chefen ska det i myndighetens ledning finnas en person...".*

Försvarsmakten anser att ansvarsförhållandena när det gäller utveckling och reglering av SGSI (Swedish Government Secure Intranet), samt Myndigheten för samhällskydd och beredskaps ansvar med anledning härav, måste förtydligas.

8. Säkra kryptografiska funktioner

Avseende säkra kryptografiska funktioner (avsnitt 9.4.2) delar Försvarsmakten utredningens uppfattning att den av Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarets materielverk och Försvarsmakten föreslagna nationella strategin med åtgärdsplan (bilaga 4) bör ligga till grund för utvecklingen av processerna på området. Säker kommunikation är avgörande för informationssäkerheten och frågan är därför av stor vikt för många myndigheter och det är angeläget att processerna snabbt kan komma på plats. Försvarets materielverk har genom CSEC (Sveriges certifieringsorgan för it-säkerhet) en central roll i den föreslagna modellen och har också stor erfarenhet av utveckling av processer inom området. Mot bakgrund av det föreslår Försvarsmakten att Försvarets materielverk får i uppdrag att, i samråd med de övriga nämnda myndigheterna, precisera underlaget så att det kan ligga till grund för konkreta uppgifter till respektive myndighet.

Försvarsmakten anser att även Försvarsunderrättelsedomstolen och Statens inspektion för försvarsunderrättelseverksamheten ska ha säkra kryptografiska funktioner, och att detta måste framgå av författningstexten.

Som tidigare angivits i yttrandets punkt 4 finns behov av att närmare tydliggöra innebörden av begreppet kryptografiska funktioner, vilket kan påverka därtill relaterade bestämmelser i förordningsförslagets 12-13 §§. Exempel på förändring som då bör övervägas är att i ökad grad tillgodose behovet av kryptografiska funktioner genom upphandling och godkännande av vissa produkter – inte genom att strikt reglera tilldelning för samtliga typer av kryptografiska funktioner och produkter.

Förändringsförslag för förordning (2006:942) om krisberedskap och höjd beredskap saknas i betänkandet vad avser säkra kryptografiska funktioner.

9. It-incidentrapportering

För det fall Myndigheten för samhällsskydd och beredskap bemyndigas att utfärda närmare föreskrifter om hur rapporteringen ska genomföras måste Försvarsmaktens samråd inhämtas eftersom de kommer att beröra, inte bara Försvarsmakten, utan även de myndigheter som står under Försvarsmaktens tillsyn enligt 39 § i säkerhetsskyddsförordningen.

Inom Försvarsmakten förekommer även it-system för behandling av ytterst säkerhetskänsliga uppgifter. Såväl dessa system som uppgifter i dem omfattas av sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400). Försvarsmakten anser att det med hänsyn till sekretessen endast är möjligt rapportera avidentifierade uppgifter i fråga om eventuella incidenter i sådana system.

Avidentifieringen ska säkerställa att det inte är möjligt att härleda en incident till en viss myndighet, vilken verksamhet som är drabbad eller var incidenten har inträffat. Försvarsmakten antar att motsvarande förhållande kan gälla i fråga även om vissa it-system vid andra myndigheter.

10. Nationell styrmodell och myndighetsråd – konsekvenser

Utredningen föreslår att en nationell styrmodell för informationssäkerhet (10.2.1) ska utvecklas och förvaltas över tid, samt bedömer därav tillkommande resursbehov till tre till fyra tjänster för Myndigheten för samhällsskydd och beredskap.

Konsekvenser, bl a resursmässiga, av en sådan styrmodells införande för övriga berörda myndigheter bör närmare klarläggas innan förslaget realiseras. Erfarenheter talar för att införande av nya metoder, modeller och processer innebär ett omfattande arbete.

Motsvarande behov av fördjupad resursbedömning för andra berörda myndigheter, än Myndigheten för samhällskydd och beredskap, bör göras beträffande förslaget om inrättandet av ett myndighetsråd (10.2.2). Vidare måste myndighetsrådets reella befogenheter och styrmöjligheter klarläggas med hänsyn till den svenska förvaltningsmodellen med självständiga myndigheter.

11. Sensorsystem

Försvarsmakten anser i likhet med utredningen att det finns behov att analysera rättsliga frågor om personuppgiftsbehandling och sekretessregler. Frågan om behandling av personuppgifter ska dock ses i ett större sammanhang än ett enskilt sensorsystem kopplat till utbyggnaden av SGSI (förslag 2 på sidan 246). Myndigheter kan generellt ha ett behov av sensorer i interna nätverk eller i anslutning till publika nätverk för att upptäcka intrång, skadlig kod och tillgänglighetsattacker mot myndighetens it-system. Även Försvarsmakten har

behov av sensorsystem. Författningsregleringen i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst är inte ändamålsenlig för sensorsystem. En särskild författningsreglering måste därför kunna användas av alla myndigheter.

Detta yttrande har beslutats av chefsjurist Carin Bratt. I den slutliga handläggningen har deltagit försvarsjurist Magnus Sandbu, och som föredragande överste Roger Nordh.

Carin Bratt
Chefsjurist

Roger Nordh

Sändlista

Justitiedepartementet / SSK

För kännedom

Myndigheten för samhällsskydd och beredskap
Försvarets materielverk
Försvarets radioanstalt

Inom Högkvarteret
LEDS
INSS
PROD
MUST
JURS

Klicka här för att ange befattning.