REMISSYTTRANDE

2015-09-17

FRA beteckning
20 400:3449/15:2

Justitiedepartementet
Enheten för samordning av samhällets krisberedskap (SSK)
103 33 Stockholm

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

FRA handläggare	FRA föreg. datum	FRA föreg. beteckning
Alexandra Lindgren		

Remiss av betänkandet Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten (SOU 2015:23)

I Sammanfattning

FRA ställer sig positivt till de flesta förslag som presenteras i betänkandet och välkomnar särskilt förslaget om att regeringen antar en strategi som tar sikte på att stärka informations- och cybersäkerheten i staten.

Idag saknas det ett gemensamt nationellt grepp för kravställning av informationssäkerhet. FRA anser därför att en nationell styrmodell är den enskilt viktigaste åtgärden som föreslås i betänkandet. För att uppnå en gemensam helhetssyn på informationssäkerhet i staten bör styrmodellen utformas så att den kan användas för kravställning i all statlig verksamhet inklusive den som rör rikets säkerhet. På sådant sätt erhålls en enhetlig hantering av informationssäkerhet som kan anpassas till olika verksamheters behov av skyddsåtgärder. En sådan styrmodell är en förutsättning för att genomföra många av de övriga förslagen i utredningen.

Den nationella strategin bör inte fokusera enbart på it-incidentrapportering för att uppnå en nationell lägesbild. Det är ett av många verktyg för att skapa en sådan lägesbild. Vidare är den största utmaningen att omsätta befintlig kunskap till skyddsåtgärder för att kunna förebygga och hantera it-incidenter.

FRA
Box 301
161 26 BROMMA

Telefon
08 - 471 46 00

Telefax

Org.nr
20 21 00 - 0365

Kravet på it-incidentrapportering bör inte omfatta verksamhet som rör rikets säkerhet och bör i stället hanteras i annan ordning.

MSB:s föreskriftsrätt avseende sensorssystem bör inte omfatta FRA:s TDV som används för de mest skyddsvärda verksamheterna.

FRA ställer sig positivt till förslaget att samverkan mellan myndigheter på informationssäkerhetsområdet ska ske inom ramen för ett nytt myndighetsråd. Rådet bör dock inte regleras i förordningsform.

FRA instämmer i att det är viktigt att statliga myndigheter ska kunna kommunicera säkert med varandra via nätverk. FRA anser dock inte att SGSI på förhand ska pekas ut som grund för ett säkert statlig nätverk.

FRA tillstyrker förslaget att de myndigheter tagit fram rapporten om kryptografiska funktioner (bilaga 4 till betänkandet) får i uppdrag utveckla processerna som föreslås i den. FRA förordar att Försvarets materielverk (FMV) får i uppdrag att leda detta arbete.

FRA ser även positivt på utredningens förslag att stärka den sektorsvisa tillsynen inom informationssäkerhetsområdet. FRA kan i egenskap av expertmyndighet inom teknisk informationssäkerhet stödja myndigheter som utövar tillsyn.

II Synpunkter på betänkandet

FRA har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på betänkandet. FRA:s synpunkter följer betänkandets disposition.

1.1 Förslag till förordning för statliga myndigheters informationssäkerhet

4 och 7 §§
FRA anser att definitionen av informationssäkerhet samt utgångspunkterna för klassificering av information bör överensstämma med informationssäkerhetsaspekterna i förslaget till ny säkerhetsskyddslag som framförs i betänkandet En ny säkerhetsskyddslag (SOU 2015:25). Se vidare 9.2.3.

8 §
FRA är i grunden positivt till åtgärder som leder till att myndigheter använder säkra produkter. FRA, Myndigheten för samhällsskydd och beredskap (MSB), Försvarsmak-

ten (FM) och FMV har gemensamt tagit fram rapporten Förslag till nationell strategi och åtgärdsplan för säkra kryptologiska funktioner, se bilaga 4 till betänkandet. I rapporten har dessa myndigheter utvecklat sina idéer kring hur produktsäkerhet kan uppnås. Detta kan dels uppnås genom att använda certifierade produkter, dels genom att använda kompletterande åtgärder enligt principen om säkerhet i lager.

På grund av att teknikutvecklingen går allt snabbare och att produkter revideras mer frekvent finns risk att certifieringsprocesser släpar efter. Om verkställighetsföreskrifterna inte utformas på lämpligt sätt kan detta leda till att myndigheter måste välja ”gamla” produkter. Dessa kan också vara förknippade med sårbarheter som endast åtgärdats i ny ännu icke-certifierad version. Det kan också vara så att en myndighet har funktionella krav som inte tillgodoses av utpekade certifierade produkter. Verkställighetsföreskrifterna måste således kunna medge undantag.

11 §
FRA har efter, två regeringsuppdrag, utvecklat sensorsystemet tekniskt varnings- och detekteringssystem (TDV) för de mest skyddsvärda verksamheterna i Sverige. Eftersom förslagen i betänkandet, enligt vad som sägs i avsnitt 2.3, inte tar sikte på de mest skyddsvärda verksamheterna, bör MSB:s förskrivningsrätt utformas så att den inte omfattar FRA:s TDV.

15 §
FRA anser att det är otydligt vad som avses med anslutning till ”myndighetsgemensamma tjänster för e-förvaltning eller liknande syfte”.

16 §
I bestämmelsen används begreppen ”säkra och certifierade it-produkter”. I 8 § nämns endast ”säkra it-produkter”. Samma terminologi bör användas i 8 och 16 §§.

Se även 8 § avseende FRA:s synpunkter om risker med certifieringsprocesser.

17 §
I avsnitt 2.3 i betänkandet framgår att utredningen inte sökt föreslå lösningar på de utmaningar inom informationssäkerhetsområdet som rör rikets säkerhet. Vidare uttalas att åtgärdsförslagen inte avser att träffa säkerhetsskyddslagens tillämpningsområde. Enligt FRA:s mening träffar denna bestämmelse dock verksamhet som regleras av säkerhetsskyddslagen. Förslaget innebär att all verksamhet att kommer att omfattas av rapporteringsskyldigheten, även den som rör rikets säkerhet och omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400). I FRA:s försvarsunderrättelseverksamhet

förekommer exempelvis uppgifter som kan vara av synnerlig betydelse för rikets säkerhet. En sådan ordning som föreslås är inte lämplig för de allra mest skyddsvärda verksamheterna. Rapportering om it-incidenter i sådan verksamhet bör hanteras i annan ordning.

FRA anser även att man bör avvakta med förslaget i denna del tills EU:s direktiv (NIS-direktivet) om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen är beslutat.

FRA anser vidare att den föreslagna strategin inte bör fokusera it-incidentrapportering, utan framtagande av en nationell lägesbild och implementering av relevanta säkerhetsåtgärder på informationssäkerhetsområdet, se vidare 9.1.4 och 9.5.

18 §
FRA ställer sig positivt till att samverkan på informationssäkerhetsområdet utvecklas inom ramen för det föreslagna Myndighetsrådet för informationssäkerhet (myndighetsrådet). FRA anser dock inte att samverkan inom myndighetsrådet bör regleras i förordningsform. Övriga samverkan mellan myndigheter regleras inte på ett sådant sätt.

FRA anser att samtliga myndigheter som deltar i Samverkansgruppen för informationssäkerhet (SAMFI) också bör delta i samverkan inom ramen för myndighetsrådet. Samverkan inom informationssäkerhetsområdet sker också i andra fora t.ex. i SAMFI, Informationssäkerhetsrådet och Samverkansområdet för teknisk infrastruktur (SOTI). Enligt FRA behövs en genomlysning av befintlig samverkan. Informationssäkerhetsarbetet blir troligen effektivare om det sker inom ramen för myndighetsrådet i stället för att vara utspritt inom en mängd olika statliga samverkansgrupper.

20 §
Som framgår ovan har FRA efter två regeringsuppdrag utvecklat sensorsystemet TDV för de mest skyddsvärda verksamheterna i Sverige. MSB:s föreskrivningsrätt bör inte omfatta FRA:s sensorsystem. En sådan avgränsning av MSB:s föreskriftsrätt bör framgå tydligt av förordningen.

9.1.4 Strategins innehåll

FRA ställer sig positiv till utredningens förslag att regeringen ska anta en strategi för informations- och cybersäkerheten i staten. FRA anser dock att obligatorisk it-incidentrapportering (mål 4 i strategin) inte bör utgöra ett centralt *mål* i strategin. Målet bör vara att skapa en nationell lägesbild och förmåga att genomföra skyddsåtgärder. Se

även nedan 9.5. Obligatorisk it-incidentrapprotering kan dock utgöra ett viktigt medel för att skapa en nationell lägesbild.

9.2.1 En nationell styrmodell

I och med att det saknas ett enhetligt regelverk för statens informationssäkerhet, exempelvis finns inte några gemensamma grundläggande krav på informationssäkerhet, är det nationella informationssäkerhetsarbetet idag splittrat och statens resurser på området används inte effektivt. FRA anser därför att en nationell styrmodell är den enskilt viktigaste åtgärden som föreslås i betänkandet. Den föreslagna styrmodellen bör utgöra grunden för ett samlat nationellt informationssäkerhetsarbete. Förslaget är också en förutsättning för många av de övriga förslagen i betänkandet.

För att tillförsäkra att informationssäkerhetsarbetet blir så enhetligt som möjligt bör inte styrmodellen göra skillnad på civil och militär verksamhet och den bör utformas så att den kan omfatta all statlig verksamhet, även den mest skyddsvärda. På sådant sätt erhålls en enhetlig hantering av informationssäkerhet som kan anpassas till olika verksamheters behov av skyddsåtgärder. Styrmodellen bör inte heller göra skillnad på offentlig eller privat verksamhet, även om den initialt endast gäller för statliga myndigheter.

I betänkandet förordas att MSB får i uppdrag att ta fram styrmodellen i samverkan med övriga myndigheter i myndighetsrådet. FRA har ingen erinran mot att MSB får detta uppdrag men FRA vill understryka vikten av att styrmodellen tas fram genom myndighetsgemensam samverkan.

Styrmodellen bör innefatta

- inventering av informationstillgångar,
- klassificering av informationstillgångar efter menbedömning,
- tilldelning av skyddsnivåer utifrån klassificering och hotnivå, och
- normerande skyddsåtgärder kopplade till skyddsnivåer.

Fördelarna med en sådan gemensam styrmodell är följande.

- Styrmodellen utgör en nationell mekanism där aggregerad kunskap om hot och sårbarheter kan omsättas till skyddsåtgärder. En sådan nationell koppling saknas idag.
- Styrmodellen samlar de nationella resurserna på informationssäkerhetsområdet.
- Den enhetliga kravställning på informationssäkerhet hos myndigheter som följer av styrmodellen kommer att ge högre kvalitet och mer tydlighet i myndigeters informationssäkerhetsarbete. Detta kommer också att göra att efterlevnaden och

tillsynen av kraven i styrmodellen blir mer enhetlig. Det kan därför förväntas att styrmodellen leder till att under- respektive överinvesteringar i säkerhet på informationssäkerhetsområdet minskar.
- Styrmodellen är en förutsättning för att vidareutveckla och implementera den kryptostrateg som föreslås i bilaga 4 till betänkandet.
- Styrmodellen ger ett regelverk som kommuner och landsting samt privata aktörer kan välja att använda för sin egen informationssäkerhet.
- Den ökade tydligheten om vad staten kräver och efterfrågar hjälper även leverantörerna att ta fram rätt produkter med rätt säkerhetsegenskaper. Idag upplever många en otydlig och splittrad kravbild från myndigheter.
- En tydlig kravställning underlättar även för tillsyns- och revisionsinstanser samt utbildningsinstanser inom informationssäkerhetsområdet.

9.2.3 En ny förordning för statliga myndigheters informationssäkerhet

Av samma skäl som framförs i 9.2.1 bör informationssäkerhetsarbetet enligt förslaget till ny säkerhetsskyddslag[1] och förordning för statliga myndigheters informationssäkerhet utgå från samma terminologi och metodik (t.ex. informationsklassning). På så sätt säkerställs att informationssäkerhetsarbetet för det mest skyddsvärda verksamheterna och övriga verksamheter bedrivs på ett enhetligt sätt men med hänsyn till de säkerhetskrav som behövs för respektive verksamhet.

9.2.4 Tillsyn

FRA tillstyrker förslaget. Avseende förslaget om översyn av den sektorsvisa tillsynen vill FRA framföra följande synpunkter.

I avsnittet avseende sektorsvis tillsyn anges att det inte är rimligt att kräva eller förutsätta att den bredd och djup i kompetensen som krävs ska finnas inom varje tillsynsmyndighet. FRA instämmer i denna synpunkt. Enligt FRA bör den sektorsvisa tillsynen genomföras i samverkan med utpekade myndigheter som har den höga expertkompetens som krävs. En sådan ordning skulle avsevärt bidra till en mer enhetlig tillämpning av gällande informationssäkerhetskrav.

FRA har den kompetens som krävs för att stödja tillsynsmyndigheterna vid informationssäkerhetsrelaterad tillsyn av teknisk karaktär. FRA stödjer redan idag ett flertal tillsynsmyndigheter i deras tillsynsuppdrag. Detta sker inom ramen för FRA:s uppdrag

[1] Betänkandet En ny säkerhetsskyddslag (SOU 2015:25) har varit ute på remiss jämte betänkandet som behandlas i detta remissyttrande.

enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt. FRA:s stöd ges endast efter begäran från respektive myndighet och är idag avgiftsfinansierad. Om FRA:s stödjande roll ska utökas behövs en översyn av hur denna verksamhet ska finansieras.

9.3.1 Kravställning vid upphandling

FRA anser att MSB bör ta fram skyddsprofiler med minimikrav på säkerhet i samråd med de myndigheter som ska verka inom ramen för myndighetsrådet. Det är viktigt att expertmyndigheternas kunskap om hot och sårbarheter omsätts till adekvata krav på säkerhet.

Det finns en säkerhetsrisk med att införa ett rapporteringskrav avseende vilka leverantör en statlig myndighet har valt. En sådan komplett samanställning över leverantörer till statliga myndigheter skulle ge invisning till sårbarheter i samtliga myndigheters säkerhetsskydd. Om någon obehörig får åtkomst till sammanställningen kan uppgifterna i den användas för att skada eller slå ut statlig verksamhet.

9.4.1 Statliga nätverk

FRA instämmer i att det är viktigt att statliga myndigheter ska kunna kommunicera säkert med varandra via nätverk. Sådana nätverk kräver dock en på förhand ställd kravanalys och att krav och säkerhet hanteras redan i utvecklingsfasen. Det är därför inte ändamålsenligt att på förhand peka ut SGSI för detta syfte innan det gjorts en grundlig riskanslys. Kravställning av statliga nätverk bör ta hänsyn till vilka verksamheter som ska anslutas. Det är även viktigt att krav ställs på de myndigheter som ansluts till nätverket. Kravställning av statliga nätverk bör ske inom ramen för myndighetsgemensam samverkan.

9.4.2 Säkra kryptografika funktioner

FRA tillstyrker förslaget. 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. FMV 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 detta föreslår FRA att FMV får i uppdrag att, i samråd med de övriga myndigheterna, leda utvecklingen av processerna som föreslås i den myndighetsgemensamma rapporten om kryptografiska funktioner (bilaga 4 till betänkandet). Det bör dock poängteras att detta arbete inte kan genomföras som en isolerad företeelse utan förutsätter tydliga krav i övrigt på informa-

tionssäkerhet. En förutsättning för att arbetet med säkra kryptologiska funktioner ska ha önskad effekt är därmed att den styrmodell som förslås i avsnitt 9.2.1 får ett tillräckligt konkret innehåll med krav på informationssäkerheten i staten.

9.5 Incidentrapportering

FRA instämmer i att det finns behov att skapa en nationell lägesbild för att förebygga och hantera it-incidenter. Obligatorisk it-incidentrapportering är dock endast *ett* verktyg av många för att skapa en sådan nationell lägesbild. Andra verktyg utgörs exempelvis av uppgifter från underrättelseverksamhet, sensorsystem samt uppgifter ur öppna källor. Värdet av att enbart fokusera på obligatorisk it-incidentrapportering för att uppnå en nationell lägesbild kan därför ifrågasättas.

Enligt FRA:s mening är i stället den stora utmaningen i informationssäkerhetsarbetet att *omsätta befintlig kunskap* till *skyddsåtgärder* för att kunna förebygga och hantera it-incidenter. Genom att införa en nationell styrmodell kommer detta arbete att underlättas.

Om obligatorisk it-incidentrapportering ska införas finns behov att förtydliga innebörden av begreppet allvarlig it-incident. Se även FRA: synpunkter avseende 17 § i avsnitt 1.1.

9.7 Internationella och regionala relationer

FRA tillstyrker förslaget. Enligt 4 § förordning (2007:937) med instruktion för Försvarets radioanstalt ska FRA samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet. FRA har därmed ett mångårigt samarbete med internationella partners inom informationssäkerhets- och kryptoområdena och kan bidra till regeringens arbete på detta område.

10.2.2 Upprättande av ett kansli för myndighetsrådets arbete

Uppgiften att genom samverkan inom ramen för myndighetsrådet förvalta och utveckla tillämpliga krav på standarder och certifiering av produkter och tjänster med bäring på informationssäkerhet i samhällsviktig verksamhet kommer sannolikt att vara resurskrävande för FRA. FRA håller därför inte med om de slutsatser om resursåtgång som dras i betänkandet. Det är sannolikt att FRA behöver tillföras medel för att kunna finansisera heltidstjänster för deltagande i detta arbete.

10.2.5 Säkrare kommunikation i staten

Kostnaden för sensorsystem är inte enbart en engångskostnad för teknik. FRA:s erfarenhet av utveckling av TDV-system visar att det även krävs resurser för drift och uppdateringar.

10.4 Finansiering

Avseende åtgärdsförslagen har det i betänkandet endast tagits höjd för ökade resurser vid MSB. Om samtliga föreslagna åtgärder ska genomföras krävs utökade resurser även för andra expertmyndigheter inom informationssäkerhetsområdet. För FRA:s del kommer myndighetens roll inom ramen för samverkan i myndighetsrådet att kräva extra resurser. Detta gäller i synnerhet kravställningen inom ramen för styrmodellen.

III Allmänt om FRA

FRA är en myndighet med ca 700 anställda som bedriver informationssäkerhetsverksamhet och förvarsunderrättelseverksamhet.

FRA ska ha hög teknisk kompetens inom informationssäkerhetsområdet. FRA får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhet- eller försvarspolitiskt hänseende. FRA ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifiering av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser, och ge annat tekniskt stöd.

FRA bedriver – efter inriktning från regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen inom Polismyndigheten – försvarsunderrättelseverksamhet till stöd för svensk utrikes, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Verksamheten fullgörs genom inhämtning, bearbetning och analys av information samt delgivning av underrättelser till berörda myndigheter. För att kunna bedriva försvarsunderrättelseverksamhet krävs en omfattande utvecklingsverksamhet.

Uppgifter rörande FRA:s verksamhet omfattas till stora delar av sekretess enligt bl.a.15 kap. 2 § OSL. För uppgifter i allmän handling rörande underrättelseverksamhet gäller sekretess i 95 år.

FRA

I detta ärende har generaldirektör Dag Hartelius beslutat. I den slutliga handläggningen har också deltagit avdelningschef Charlotte Lindgren, stf avdelningschef Anders Blennholm, planeringschef Johan Dahlstedt, kontorschef Ola Sommelius, jurist Kári Ólafsson samt informationssäkerhetsexpert Arvid Kjell, tillika föredragande.

Försvarets radioanstalt

Dag Hartelius

Arvid Kjell

Sändlista
För kännedom:
Försvardepartementet
Försvarsmakten
Myndigheten för samhällsskydd och beredskap
Försvarets materielverk
Säkerhetspolisen
Nationella operativa avdelningen inom Polismyndigheten
Post- och telestyrelsen

Internt FRA
GD
Chefsjuristen
C Plan
AC
C SÄK