REMISSYTTRANDE

2018-04-19

FRA beteckning
20 400:3090/18:2

Finansdepartementet
Avdelningen för offentlig förvaltning,
Enheten för digital förvaltning
103 33 Stockholm

Er handläggare	Ert datum	Er beteckning
Anneli Hagdahl	2018-01-23	Fi2018/00106/DF

FRA handläggare	FRA föreg. datum	FRA föreg. beteckning
Kári Ólafsson		

Remiss av slutbetänkandet reboot – omstart för den digitala förvaltningen (SOU 2017:114)

FRA har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på betänkandet.

Sammanfattning

FRA har ingen erinran mot de mål som sätts upp för de statliga myndigheternas digitalisering, men det kan ifrågasättas om digitaliseringen av verksamheter som till stora delar omgärdas av sekretess som rör rikets säkerhet bör vara lika långtgående som för staten i övrigt.

FRA avstyrker förslaget att i förordning peka ut att FRA ska utföra säkerhetsgranskning av den svenska noden. Förslaget innebär att FRA på grund av resursbrist kan tvingas avstå från andra nödvändiga säkerhetsgranskningar.

Incidenter som påverkar funktionalitet och säkerhet i noden bör inte rapporteras till Digitaliseringsmyndigheten om rapporteringsskyldighet följer av 10 a § säkerhetsskyddsförordningen (1996:633).

FRA
Box 301
161 26 BROMMA

Telefon
08 - 471 46 00

Telefax

Org.nr
20 21 00 - 0365

FRA har inte några e-tjänster som kräver anslutning till valfrihetssystemet och noden. Det finns inte heller planer på att ta fram e-tjänster.

FRA bör undantas från kravet att skicka digital post.

FRA instämmer att den nationella informationssäkerheten idag kännetecknas av fragmentering. Samtidigt saknas en tydlig diskussion kring informationssäkerhetsfrågor i anslutning till flera av förslagen som framförs. Förslaget om incidentrapportering riskerar därtill att bidra till ökad fragmentering på informationssäkerhetsområdet. Det saknas även en diskussion huruvida förslagen kan träffas av säkerhetssyddslagstiftningen.

Förslagen om digitalisering innebär en ökad utmaning för statsförvaltningen att hantera informationssäkerhet på ett adekvat sätt. FRA:s erfarenheter från att utföra säkerhetsgranskningar är att brister i informationssäkerhetsarbetet inte sällan är av grundläggande karaktär hos organisationer, samt att organisationer som utkontrakterar i många fall saknar förutsättningar att ställa relevanta krav på den informationssäkerhet som ska tillhandahållas.

FRA:s synpunkter följer betänkandets disposition.

1.7 Förslag till förordning med mål för de statliga myndigheternas digitaliseringsarbete (s. 52)

FRA har ingen erinran mot förslaget i sig. FRA vill dock framhålla att det är viktigt i det övergripande digitaliseringsarbetet, såsom vid utformning av nya författningsförslag på området, att hänsyn tas till verksamheter som till stora delar omgärdas av sekretess som rör rikets säkerhet, exempelvis sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400) (OSL). Det kan ifrågasättas om digitalisering av dessa delar av statsförvaltningen bör vara lika långtgående som för staten i övrigt.

1.10 Förslag till förordning om ändring i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering (s. 55)

FRA avstyrker förslaget i 9 §, se mer nedan under avsnitt 17.6.6 och 22.8.

9 Informationssäkerhet – en naturlig del i digitaliseringen (s. 161)

FRA instämmer i bilden av att den nationella informationssäkerheten i dag kännetecknas av fragmentering. Såsom påpekas i betänkandet finns det flera aktörer som utan

större samordning agerar på informationssäkerhetsområdet. Det tillkommer också nya aktörer med kravställande roller inom området.[1] Det är därför angeläget att arbetet med att etablera en nationell modell enligt regeringens cybersäkerhetsstrategi[2] ges prioritet och får genomslag för att öka förutsättningarna för ett sammanhållet nationellt informationssäkerhetsarbete.

FRA vill betona att de standarder om ledningssystem som MSB föreskrivit att svenska myndigheter ska följa (ISO/IEC 27001:2014 och ISO/IEC 27002:2014) inte behandlar vilka säkerhetskrav som ska ställas utan *hur* arbetet med informationssäkerhet ska gå till, såsom metoder för kravställning. Standarderna belyser vikten av att informationssäkerhet utgör en integrerad del av arbetet med att digitalisera statsförvaltningen och beaktas genom hela processen, d.v.s. såväl vid utveckling, införande och förvaltning av it-system.

Förslagen om digitalisering innebär en ökad utmaning för statsförvaltningen att hantera informationssäkerhet på ett adekvat sätt. I detta sammanhang vill FRA betona att arbetet med grundläggande informationssäkerhet är viktigt. FRA har i över tio år genomfört it-säkerhetsgranskningar. Den samlade bild som framträder är att grundläggande brister är vanligt förekommande och att informationssäkerheten ofta inte motsvarar önskad nivå med avseende på existerande hotbild. Det kan röra sig om brister i lösenordshantering eller uppdateringsrutiner för mjukvara. Det kan även röra sig om att it-arkitekturen inte är byggd med hänsyn till informationssäkerhet samt okunskap om hur ett it-system ska konfigureras på ett säkert sätt.

Flera myndigheter och företag utkontrakterar (outsourcing) väsentliga delar av sin it-verksamhet till externa tjänsteleverantörer. Det finns dock ingen motsättning mellan informationssäkerhet och utkontraktering, på samma sätt som att egen it-drift inte garanterar en god informationssäkerhet. En återkommande brist som FRA dock ser vid utkontraktering är förlust av personal med it-kompetens. Det är viktigt att komma ihåg att ansvaret att upprätthålla en fullgod informationssäkerhet kvarstår hos den utkontrakterande organisationen. En förutsättning för att kunna ta detta ansvar är att den utkontrakterande organisationen behåller kompetens som gör det möjligt att identifiera vilka it-system som lämpar sig att utkontraktera (riskanalys) och ställa rätt krav på den informationssäkerhet som ska tillhandahållas.

[1] Ett exempel är tillsynen enligt den föreslagna lagen om informationssäkerhet för samhällsviktiga och digitala tjänster som troligen kommer att utövas av flertalet nya tillsynsmyndigheter, se prop. 2017/18:205 s. 57.
[2] Nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213).

Frågor om informationssäkerhet behandlas till övervägande del i avsnitt 9 (s. 161-167). En tydlig diskussion kring informationssäkerhetsfrågor saknas dock i anslutning till flera av förslagen i betänkandet. Detta ger intryck av att förslagen saknar koppling till informationssäkerhet och de utmaningar som följer av digitalisering. I andra förslag där informationssäkerhet diskuteras, såsom förslaget om incidentrapportering av händelser som påverkar noden, saknas synlig koppling till avsnitt 9 i och med att förslaget riskerar att leda till ytterligare fragmentering av informationssäkerheten, se nedan 17.6.5.

Vidare saknas en diskussion om förslagen kan komma att omfattas av säkerhetsskydds-lagen. Denna fråga har bäring på bl.a. vilka krav som ställs på informationssäkerhet, samt den tillsyn som kan komma att gälla.

13.6.2 Statliga myndigheter, kommuner och landsting *ska* ansluta sig till valfrihets-system (s. 230)

Kravet att ansluta sig till valfrihetssystemet omfattar myndigheter som tillhandahåller e-tjänster som kräver elektronisk identifiering. FRA har inte några e-tjänster. Det finns inte heller några planer på att ta fram sådana tjänster. Behovet av sådana tjänster är dessutom begränsat eftersom FRA:s verksamhet inte riktar sig till allmänheten på samma sätt som de flesta andra myndigheters verksamhet, se nedan allmänt om FRA.

17.6.3 Alla offentliga myndigheter som omfattas av eIDAS-förordningens krav ska ansluta sig till noden (s. 345)

Kravet att ansluta sig till noden omfattar myndigheter som tillhandahåller e-tjänster som kräver elektronisk identifiering på tillitsnivå 3. De synpunkter som lämnats avseende 13.6.2 gäller även frågan om anslutning till noden.

17.6.5 Incidentrapportering (s. 347)

Det håller på att växa fram ett flertal parallella system för rapportering av incidenter i it-system.

- Myndigheter ska rapportera it-incidenter enligt 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd be-redskap.
- Enligt artikel 33 dataskyddsförordningen ska personuppgiftsincidenter rapporte-ras.

- Motsvarande bestämmelser om rapportering av personuppgiftsincidenter i dataskyddsförordningen finns i förslag till brottsdatalag avseende brottsbekämpande myndigheters verksamhet.[3]
- Vidare föreslås incidentrapporteringsplikt för leverantörer av samhällsviktiga och digitala tjänster i samband med införandet av EU:s NIS-direktiv.[4]
- Enligt 10 a § säkerhetsskyddsförordningen ska incidenter som rör rikets säkerhet rapporteras i särskild ordning.

De skyldigheter att rapportera incidenter som följer, eller kommer att följa, av de olika författningarna överlappar varandra. En och samma incident kan komma att rapporteras enligt flera olika lagar och till olika tillsynsmyndigheter. Denna ordning är inte lätt att överblicka. Utredningens förslag om skyldighet att rapportera incidenter till Digitaliseringsmyndigheten kommer att bidra ytterligare till fragmentering inom informationssäkerhetsområdet.

I samtliga gällande författningar och författningsförslag finns undantag för rapportering i de fall som incidentrapportering även ska ske enligt 10 a § säkerhetsskyddsförordningen. I dessa fall ska incidenter endast rapporteras enligt bestämmelsen i säkerhetsskyddsförordningen. Enligt FRA:s mening bör samma ordning gälla enligt lagen om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Av den föreslagna lagen bör det framgå att skyldigheten att rapportera incidenter inte gäller sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen.

17.6.6 Försvarets radioanstalt ska utföra tekniska säkerhetsgranskningar (s. 347 f.)

Utredningen föreslår att FRA ska utföra säkerhetsgranskningar av noden för att skydda den mot angrepp. FRA har inte något att erinra mot att det i förordningen anges att noden ska säkerhetsgranskas innan den tas i drift samt vid större ändringar av noden. Det bör dock inte anges att FRA ska utföra denna granskning.

Förslaget saknar motivering till varför det i förordning ska anges vilken organisation som ska utföra säkerhetsgranskningen. Det bör åligga Digitaliseringsmyndigheten att avgöra om granskning lämpligast utförs av en expertmyndighet inom informationssäkerhetsområdet, såsom FRA, eller om det är tillfyllest med en granskning utförd av en

[3] Se betänkandet Brottsdatalag (SOU 2017:29).
[4] Se regeringens proposition 2017/18:205 Informationssäkerhet för samhällsviktiga och digitala tjänster.

privat aktör. Enligt FRA:s mening är det lämpligare att bestämmelsen får en utformning som inte utpekar vilken myndighet eller privat aktör som ska utföra granskningen.

Det är stor efterfrågan på FRA:s granskningar samtidigt som FRA:s resurser är begränsade. Det är viktigt att FRA vid varje givet tillfället har utrymme att prioritera granskning av de verksamheter som har störst behov. Förslaget gör att FRA kan komma att behöva avstå från andra nödvändiga säkerhetsgranskningar. FRA kan inte heller garantera att tre månader är tillräckligt för att genomföra en säkerhetsgranskning. Därför är det inte lämpligt att i författning peka ut att FRA ska säkerhetsgranska noden eller att ange inom vilken tidsram en granskning ska ske.

En säkerhetsgranskning utvisar vilken informationssäkerhet ett it-system har, det innebär inget skydd i sig. Det krävs ett konsekvent arbete för att säkerställa att it-system har erforderlig informationssäkerhet.

I avsnittet anges även att konsekvenserna av ett eventuellt angrepp mot noden kan bli allvarliga. FRA saknar en analys huruvida noden rör rikets säkerhet och därmed omfattas av de säkerhetskrav och den tillsyn som gäller enligt säkerhetsskyddslagstiftningen.

I förslaget saknas uttryckliga bestämmelser om vilka åtgärder som ska vidtas om en säkerhetsgranskning, av FRA eller annan, utvisar att det föreligger allvarliga brister i informationssäkerheten. Rimligen faller ansvaret på Digitaliseringsmyndigheten att avgöra om noden ska vara i drift till dess att brister har åtgärdats.

21 En lag om infrastruktur för digital post (s. 397)

Det kan ifrågasättas om en skyldighet att skicka myndighetspost digitalt är lämplig för myndigheter vars verksamhet i hög grad omfattas av t.ex. försvarssekretess enligt 15 kap. 2 § OSL. Uppgifter rörande FRA:s verksamhet omfattas till stora delar av sådan sekretess. FRA bör därför undantas från skyldigheten att skicka myndighetspost digitalt.[5]

Upplysningsvis kan nämnas att FRA är undantaget från kraven på elektronisk hantering av

- utgående beställningar av varor och tjänster enligt 3 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte, samt

[5] Se även FRA:s remissyttrande (FRA:s dnr 20 400:3587/17:2) avseende utredningens delbetänkande digitalforvaltning.nu (SOU 2015: 2017:23) i Finansdepartementets ärende Fi2017/01289/DF.

- inkommande och utgående fakturor enligt 21 f § förordningen (2000:606) om myndigheters bokföring.[6]

22.8 Närmare om konsekvenserna

Konsekvenser av förslaget om tekniska säkerhetsgranskningar av noden (s. 451)

Enligt FRA:s mening är konsekvensanalysen bristfällig i denna del. Det är riktigt att det ingår i FRA:s uppgifter att utföra säkerhetsgranskningar och att dessa hanteras inom ramen för myndighetens anslag. Däremot får förslaget, mot bakgrund av de begränsade personalresurser FRA har, konsekvenser för FRA:s förmåga att utföra säkerhetsgranskningar i övrigt. FRA kan inte heller garantera att tre månader är tillräckligt för att genomföra en säkerhetsgranskning.

Allmänt om FRA

FRA är en myndighet med ca 800 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 vidare – 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 bl.a. enligt 15 kap. 2 § och 18 kap. 8 § OSL.

---

[6] Se Regleringsbrev för budgetåret 2018 avseende Försvarets radioanstalt, dnr Fö2017/00284/SUND.

FRA

I detta ärende har generaldirektören Dag Hartelius beslutat. I den slutliga handläggningen har också deltagit överdirektören Charlotta Gustafsson samt stabshandläggaren Aschtar Yakob (Cyber) samt juristen Kári Ólafsson (avd V/Rätts), tillika föredragande.

Försvarets radioanstalt

Dag Hartelius

Kári Ólafsson

Sändlista
För kännedom
Försvarsdepartementet/Sund
Försvarsdepartementet/Rättssekretariatet

Internt FRA
GD
ÖD
Chefsjuristen
C Plan
Informationschefen
Säkerhetsskyddschefen
AC