2015-09-14

Dnr 2015/633

Justitiedepartementet
Enheten för samordning av samhällets krisberedskap
103 33 Stockholm

Kopia: Fritzes kundservice
106 47 Stockholm

Remissvar till Ju2015/2650/SSK, betänkandet SOU 2015:23 Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten

Sammanfattning

Riksgäldskontoret (hädanefter Riksgälden) är i stort positivt till utredningens förslag om en ny förordning för statliga myndigheters informationssäkerhet. Vidare ställer sig Riksgälden bakom förslaget att lyfta ur informationssäkerhetsfrågor ur förordning (2006:942) om krisberedskap och höjd beredskap.

Riksgälden anser att det är viktigt att den nya förordningen tydligt kravställer att informationssäkerhetsarbetet ska utgå från och följa svensk standard för ledningssystem för informationssäkerhet, dvs. ISO 27000-serien, då det är en allmänt vedertagen standard både i Sverige och internationellt. För Riksgälden har ledningssystemet för säkerhet haft en mycket positiv effekt på informationssäkerhetsarbetet.

Riksgälden anser vidare att det krävs en bättre harmonisering mellan lagstiftning inom områdena informationssäkerhet, säkerhetsskydd, krisberedskap och hantering av operativa risker, områden som är tätt sammanlänkade En översyn på övergripande nivå behövs för att säkerställa att regelverken samspelar, både i teorin och i det praktiska arbetet. En bättre samordning och en vägledning i hur lagstiftningen inom områdena på bästa sätt kan sättas i relation till varandra skulle underlätta och effektivisera myndigheternas arbete.

Riksgäldskontoret
ORG.NR
202100-2635

POSTADRESS POSTAL ADDRESS
SE-103 74 Stockholm
Sweden

BESÖK VISITORS
Jakobsbergsgatan 13

TELEFON TELEPHONE
NAT. 08 613 45 00
INT. +46 8 613 45 00

TELEFAX
NAT. 08 21 21 63
INT. +46 8 21 21 63

INTERNET
riksgalden@riksgalden.se
www.riksgalden.se

Synpunkter på förslaget till förordning för statliga myndigheters informationssäkerhet

I detta avsnitt ges kommentarer på vissa av de paragrafer som ingår i förslaget.

Terminologi (4§)

Definitioner bör ses över, exempelvis begreppet ”informationssäkerhet”. Förslagsvis bör terminologi från ISO 27000-serien användas, vilken är gängse praxis i Sverige. Vidare bör fler i förordningen ingående begrepp definieras för att öka tydligheten.

5 §

Att arbeta med ett ledningssystem för informationssäkerhet ger struktur, effektivitet och tydlighet. Formuleringen ”…ska […] särskilt beakta behovet av ledningssystem och etablerade standarder…” skulle kunna innebära att kravet tolkas olika av olika myndigheter. Detta skulle kunna leda till motsatt effekt än utredningens intention, d.v.s. att stärka myndigheternas arbete inom området. Förordningen bör istället ange att myndigheterna ska arbeta utifrån ett ledningssystem baserat på svensk standard för ledningssystem för informationssäkerhet.

6 §

För informationssäkerhetsarbetet vid myndigheterna är ledningens tydliga engagemang och ansvarstagande av stor vikt. Riksgälden anser att detta bör betonas i såväl den förslagna förordning som i myndighetsförordningen (2007:515). Ett sätt att uppnå detta genom att ange att myndighetens ledning ansvarar för att upprätthålla säkerhet i informations-hanteringen (detta motsvarar även utredningens alternativa förslag avseende internrevision, se kommentarer avseende avsnitt 9.2.5 nedan, vilket i sin tur strömlinjeformar bestämmelserna).

Hur arbetet organiseras, vilka roller som finns och hur ansvar fördelas inom myndigheten anser dock Riksgälden att det bör finnas utrymme för varje myndighet att själva avgöra baserat på behov och förutsättningar.

Formuleringen i förordningen kan vidare riskera att leda till frågor kring vad som avses med högsta ledningen och hur detta är tänkt att fungera i praktiken i t.ex. styrelsestyrda myndigheter (som Riksgälden) eller enrådighetsmyndigheter samt vilka kompetenskrav som bör ställas på en sådan utpekad person (se 9 § i förordningsförslaget).

Begreppet säkerhetskultur bör definieras och stycket lyftas till en egen paragraf.

7 §

Paragrafens stycken rör olika aktiviteter. För att förenkla och förtydliga anser Riksgälden att exempelvis stycket om IT-incidenter bör utgöra en egen paragraf.

Vidare är det otydligt om förordningen avser it-incidenter, informationssäkerhetsincidenter eller it-säkerhetsincidenter. För att den rapportering som efterfrågas ska bli korrekt och konsistent är det viktigt att lämpligt begrepp används och är tydligt definierat.

Riksgälden föreslår att förordningen anger att krav- och skyddsnivåer ”bör följas i lämplig omfattning”, istället för ”ska” som det nu står. Detta för att myndigheterna ska ha utrymme för att skapa en balanserad och riskbaserad skyddsnivå där effekt och kostnad står i paritet.

8 §

Riksgälden anser att risk- och sårbarhetsanalys endast är ett av flera tänkbara underlag för den bedömning som avses i paragrafen. Exempelvis kan även resultat från informationsklassificering användas som underlag.

Paragrafen använder begreppet säkra it-produkter. Begreppet bör definieras i förordningen. Vidare anser Riksgälden att det bör finnas utrymme för varje myndighet att bedöma om utpekade säkra it-produkter ger erforderligt skydd och är rimliga att använda ur verksamhets- och kostnadsperspektiv för att få en balanserad och kostnadseffektiv skyddsnivå.

9 §

Avsikten med paragrafen och omfattningen av kontinuitetsplaneringen bör förtydligas.

Det andra stycket bör läggas i en egen paragraf, då det inte är kopplar till uppföljning.

11 §

Rubriken bör ange att de särskilda kraven enbart avser vissa myndigheter.

Det bör finnas anledning att överväga de tre särskilda krav som anges i paragrafen. Riksgälden anser att kraven dels inte är tillräckligt tydliga och specifika, dels att det är otydligt varför just dessa krav är särskilt utpekade och vad syftet bakom detta är.

Vidare är det önskvärt att kompetenskraven omfattar alla roller som arbetar med ledning och samordning av informationssäkerhetsarbetet på samtliga myndigheter.

Riksgälden anser att även regeringskansliet och departement bör vara anslutna till samma säkra kommunikationsnät som myndigheter för att möjliggöra säker kommunikation av rapporter, riskanalyser, etc. som innehåller känslig information. Vidare finns för Riksgäldens del behov av säker kommunikation även med internationella aktörer, såsom EU och IMF (The International Monetary Fund).

15 – 16 §

Riksgälden är positiv till att vikten av kravställning vid utveckling och upphandling tydliggörs i förordningen.

Riksgälden är även positiv till generiska skyddsprofiler, men vill samtidigt framhålla komplexiteten i att ta fram bra generiska krav. Det är även viktigt att ett stort antal myndigheter med skilda verksamheter, olika it-strategier och olika storlekar involveras i arbetet.

Avseende certifiering bör det förtydligas vilken eller vilka typer av certifiering som avses. Vidare behövs vägledning för myndigheterna hur de i praktiken ska bedöma certifierade produkter, exempelvis om förutsättningar i certifiering inte stämmer med den egna tekniska miljön. På motsvarande sätt som med säkra it-produkter (se kommentaren på § 8 ovan) bör det finnas möjlighet för myndigheter att vid upphandling bedöma vilka produkter och lösningar som ger en erforderlig och effektiv skyddsnivå.

17 §

Aggregerad information, och även enskilda uppgifter, kan komma att röra rikets säkerhet. Riksgälden anser därför att det är av yttersta vikt att det innan kravet träder ikraft finns en säker och pålitlig teknisk lösning för rapportering, hantering (analys), kommunikation och lagring av informationen.

Riksgälden anser även att det bör anges att myndigheter ska få en återkoppling. Detta kan förbättra kvalitén i myndigheternas arbete då det exempelvis kan ge underlag till hotbildsbedömningar.

Angående definition av begreppet ”it-incident”, se tidigare kommentar.

18 §

Riksgälden anser att myndighetsrådets status, mandat, roll, deltagare och uppdrag bör förtydligas. De uppgifter som nu nämns är spretiga och omfattar både strategiska, operativa och tekniska frågor. Riksgälden anser även att förslaget skulle vinna på mer analys av hur och på vilket sätt ett myndighetsråd kan göra störst nytta innan det inrättas.

Avseende framtagande av rekommendationer, kravställningar etc. är det viktigt att involvera både små, medelstora och stora myndigheter med olika typer av verksamheter, t.ex. genom remissförfarande. Detta för att hitta balans och genomförbarhet i förslagen.

I förordningen bör myndighetsrådet hanteras under en egen rubrik.

19 §

Det kommer att ta lång tid att genomföra tillsyn på alla myndigheter och det är viktigt att tillsynen är lärande och stödjande. Riksgälden anser att alternativa sätt att ge stöd till myndigheter som inte kommit igång med ledningssystemarbetet bör övervägas parallellt. Möjligen kan en väg vara att införandet av ledningssystem för informationssäkerhet uppdras i regleringsbrev.

Synpunkter på förslag och bedömningar i utredningen som inte direkt hänför till enskild paragraf i förslaget till förordning

En nationell styrmodell (avsnitt 9.2.1)

Utredningen gör bedömningen att en nationell styrmodell bör etableras. En sådan styrmodell bedöms kunna medföra stor påverkan på hur myndigheterna genomför sitt arbete. Det framgår dock inte av utredningen på vilken detaljeringsnivå modeller och metoder kommer att beskrivas eller huruvida dessa kommer att regleras i föreskrifter eller utgöra allmänna råd eller vägledningar. På motsvarande sätt som för ”säkra it-produkter” bör det finnas möjlighet för en enskild myndighet att avgöra hur informationssäkerhets-arbetet bäst genomförs i organisationen och integreras i organisationens proceser.

Riksgälden anser att en nationell styrmodell bör utgå från standard för informations-säkerhet, d.v.s. ISO 27000-serien. Styrmodellen ger då en bra vägledning för hur svenska myndigheter ska arbeta med de aktiviteter som beskrivs i ISO 27000-serien och bygger dessutom på vedertagna metoder.

Informationssäkerhet som en del av myndighetens revision (9.2.5)

Riksgälden är positivt till ökat fokus på informationssäkerhet och instämmer i att detta kan betonas genom internrevisionens granskningar. Samtidigt bygger internrevisorernas arbete på att, baserat på riskanalyser, bedöma vilka områden som bör prioriteras för granskningar. Att peka ut enskilda områden som ska granskas riskerar att underminera arbetet att granska baserat på riskbedömningar. Konsekvensen kan bland annat bli att författningsstyrda granskningar görs på bekostnad av för den aktuella verksamheten mer angelägna granskningar.

Som ett alternativ till reglering genom internrevisionsförordningen (2006:1228), enligt ovan, föreslår utredningen att i myndighetsförordningen (2007:515) införa bestämmelse att myndighetens ledning ansvarar för att upprätthålla säkerhet i sin informationshantering. Riksgälden ställer sig bakom detta då det sänder en mycket tydlig signal om områdets tyngd inom statsförvaltningen. Därefter kan respektive myndighet besluta om delegering, organisation och uppföljning/granskning baserat på myndighetens behov.

Framtida övningsutveckling inom informations- och cybersäkerhetsområdet (avsnitt 9.8.1)

I flera remisser under året har behovet av ökat fokus på övningar inom krisberedskap, informationssäkerhet och civilt försvar lyfts fram. Förutom dessa övningar tillkommer de samverkansövningar och interna övningar som redan idag genomförs. Tillsammans kan detta bli mycket omfattande. Riksgälden anser därför att det måste finnas utrymme för varje enskild myndighet att bedöma behovet och hur resurser ska prioriteras för att övnings-verksamheten ska bli effektiv, balanserad och avpassad till organisationens förutsättningar och behov.

Fördjupad dialog om kompetensförsörjning (avsnitt 9.8.2)

Riksgälden tillstyrker vikten av att säkerställa att det finns tillräcklig kunskap inom de myndigheter och organisationer som bedriver samhällsviktig verksamhet. Här saknas dock idag möjligheter till utbildning som täcker alla dimensioner en beredskapsmyndighet behöver kompetens inom. Informationssäkerhet, kontinuitetshantering, krisberedskap och säkerhetsskydd är intimt förknippade med varandra och har inbördes beroenden som kräver en bredare kompetensprofil än vad som i regel finns att tillgå på arbetsmarknaden. Riksgälden föreslår därför att MSB utreder om nya utbildningsprogram kan tas fram och samordnas mellan MSB, Polisen, Säkerhetspolisen och Försvarsmakten.

Lindblad, Hans, beslutande

Björlin, Lena, föredragande