2015-09-14

Justitiedepartementet
10333 Stockholm
justitiedepartementet.registrator
@regeringskansliet.se

LFV yttrande över SOU 2015:23 Information- och cybersäkerhet i Sverige

Dokumentnummer
D-2015-048396
Ärendenummer
Ä-2015-002479

Ert datum

Er beteckning

Handläggare
Jaanivald, Liine
011-192074T
011-19 25 75F
liine.jaanivald@lfv.se

Sekretess

Utredningens förslag innebär en höjd ambitionsnivå för samhällets informationssäkerhet och vissa av förslagen medför ökade kostnader. Som affärsverk finansierar LFV sin verksamhet i princip uteslutande med s.k. en routeavgifter reglerade på EU nivå eller intäkter på grund av avtal avseende tjänster och produkter som verket tillhandahåller. I huvudsak har LFV inte möjlighet att påverka de s.k. en route avgifternas nivåer eftersom dessa regleras genom EU regelverket. EU regelverket innebär krav på flygtrafiktjänsten att genomföra betydande kostnadssänkningar. Den kostnadsdrivande utvidgningen av informations- och cybersäkerheten, samt finansieringen därav, bör nogsamt övervägas, särskilt för icke-anslagsfinansierade myndigheter.

Styrning och tillsyn av informationssäkerheten i staten stärks
Utredningen föreslår att en nationell styrmodell för informationssäkerhet etableras för att skapa ett systematiskt informationssäkerhetsarbete i statlig verksamhet. LFV noterar att det är väsentligt att en sådan styrmodell omhändertar de olika särkrav som myndigheterna har.

Förslaget avser i första hand de statliga myndigheterna och ska vara normerande för dessa men utredaren nämner att styrmodellen på sikt kan utsträckas till att omfatta hela den offentliga sektorn. LFV noterar att en stor del av verksamheten som tidigare bedrivits inom den offentliga sektorn idag bedrivs i privat regi. Behovet av informationssäkerhet för denna verksamhet har dock inte förändras till följd av detta, skyddsvärdet är detsamma. Se SOU 2015:25.

Det föreslås att myndigheternas internrevision behöver utvecklas till att inkludera uppföljning och kontroll av myndigheternas informationssäkerhet. LFV menar att uppföljning inte är en uppgift för internrevisionen. Organisationen ansvarar själv för att följa upp sin verksamhet. Myndighetens uppföljning kan bestå av controllers, kvalitets- eller complianceavdelning el. dyl. Internrevisionens uppgift är att se till att en uppföljning finns på plats, är dokumenterad och implementerad och att den fungerar ändamålsenligt.

LFV
Koncernfunktioner
Hospitalsgatan 30 Norrköping
011-19 20 00 T, 011-19 25 75 F
lfv@lfv.se
www.lfv.se
Org nr. 202100-0795

Däremot torde det vara möjligt att reglera att informationssäkerhet ska vara ett område för internrevisionens riskbedömning samt att internrevisionen ska granska myndighetens egen uppföljning.

Staten ställer tydliga krav som upphandlare av tjänster som innehåller informationshantering eller av it-tjänster.
LFV förutsätter att resonemanget om en möjlighet att använda upphandlingsförfarandet enligt lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS) inte enbart omfattar upphandling som normalt görs enligt Lag (2007:1091) om offentlig upphandling utan även fall då upphandling görs enligt lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster. LFV ställer sig positivt till en möjlighet att använda upphandlingsförfarandet enligt LUFS om myndigheten gör bedömningen att upphandling annars inte kan ske med erforderliga garantier för säkerhet.

Förslag till förordning för statliga myndigheters informationssäkerhet
I MSBFS 2009:10 Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter om statliga myndigheters informationssäkerhet regleras att en myndighets arbete med informationssäkerhet ska bedrivas i former enligt Ledningssystem för informationssäkerhet (SS ISO/IEC 27001: 2006) och Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002:2005). Således finns det redan idag en tydlig styrning avseende myndigheters informationssäkerhet. LFV menar att det därmed inte föreligger ett behov av förordning för statliga myndigheters informationssäkerhet vid sidan av MSBs föreskrifter på området.

Definitioner 4 §
Definitionen av informationssäkerhet som förmågan att upprätthålla konfidentialitet, riktighet, tillgänglighet och spårbarhet i informationshanteringen synes innebära en utvidgning av begreppet, då spårbarhet normalt inte omfattas av begreppet.

LFV noterar att samma definition av samhällsviktig verksamhet finns i MSBFS 2015:3 föreskrifter och allmänna råd om statliga myndigheters risk- och sårbarhetsanalyser som trädde ikraft 2015-03-01. Det torde inte finnas behov av att reglera samma definition i två olika författningar. Det bör övervägas om regleringen istället bör ske i form av hänvisning.

Myndighetens informationssäkerhetsarbete
6§ LFV ifrågasätter kravet på att den som har ett utpekat ansvar för informationssäkerhetsfrågor inom myndigheten ska sitta i myndighetens

LFV
Koncernfunktioner
Hospitalsgatan 30 Norrköping
011-19 20 00 T, 011-19 25 75 F
lfv@lfv.se
www.lfv.se
Org nr. 202100-0795

ledning. LFV föreslår att regleringen ändras till ”Hos myndigheten skall det, om det inte är uppenbart obehövligt, finnas en anställd med utpekat ansvar för informationssäkerhetsfrågor. Denne skall vara direkt underställd myndighetens chef” jmf. Säkerhetsskyddsförordning (1996:633) 6 § Chef för säkerhetsskyddet.

LFV noterar att kravet på att myndigheten aktivt, genom utbildning och övning, ska verka för att en god säkerhetskultur etableras i organisationen omfattar väsentligt mer än informationssäkerhet och lämpligen torde regleras i annan författning alternativt begränsas till att endast omfatta informationssäkerhet.

7§ LFV noterar att kravet på att myndigheten ska klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet behöver tydliggöras. LFV noterar även att denna klassificering av information utgör ett parallellt system till den klassificering av information som föreslås i SOU 2015:25. LFV vill även påpeka att det i vissa fall föreligger särkrav på informationshantering beroende på myndighetens verksamhetsområde, t.ex. ska LFV följa EU förordning73/2010 om kvalitetskraven på flygdata och flyginformation för ett gemensamt europeiskt luftrum.

8§ LFV noterar att kravet på att använda utpekade it-produkter är formulerat som ett absolut krav. LFV föreslår att regleringen ändras till ”I de fall säkra it-produkter finns utpekade i verkställighetsföreskrifter som meddelats med stöd av denna förordning ska dessa användas om det inte är uppenbart obehövligt.

Säkra kryptografiska funktioner
LFV noterar att de tre paragraferna avseende säkra kryptografiska funktioner är identiska med regleringen som finns i förordning (2006:942) om krisberedskap och höjd beredskap. LFV förutsätter att regleringarna inte kommer att finnas i båda förordningarna då dessa i väsentlig del tillämpas av samma myndigheter. Det bör övervägas om regleringen istället bör ske i form av hänvisning.

Upphandling och utveckling av it-system och it-produkter
15§ LFV förutsätter att informationsklassning som åsyftas är densamma som i 7§ och att ramarna för denna klassificering bör tydliggöras.

16§ LFV noterar att kravet på att endast använda säkra och certifierade it-produkter kopplas till den samhällsviktiga verksamheten som myndigheten bedriver. LFV förutsätter att det som åsyftas är samhällsviktig verksamhet så

LFV
Koncernfunktioner
Hospitalsgatan 30 Norrköping
011-19 20 00 T, 011-19 25 75 F
lfv@lfv.se
www.lfv.se
Org nr. 202100-0795

som den definieras i MSBFS 2015:3 Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser. MSB har tidigare uppmärksammat att det funnits olika tolkningar bland myndigheterna gällande vilka verksamheter som ska/bör anses vara samhällsviktiga och på vilken detaljnivå dessa ska identifieras.

Trots att MSB i MSBFS 2015:3 syftat till att förtydliga vilken detaljeringsgrad som myndigheternas redovisning av samhällviktig verksamhet ska innehålla och vilken samhällsviktig verksamhet som avses torde det alltjämt föreligga stora skillnader i myndigheternas arbete med att identifiera samhällsviktig verksamhet. Det bör därför övervägas om syftet med regleringen kan uppnås utan referens till begreppet samhällsviktig verksamhet.

LFV noterar att kravet på att använda utpekade it-produkter är formulerat som ett absolut krav. LFV föreslår att regleringen ändras till ”I de fall säkra itprodukter finns utpekade i verkställighetsföreskrifter som meddelats med stöd av denna förordning ska dessa användas om det inte är uppenbart obehövligt.”

It-incidentrapportering
LFV noterar att det finns förslag på ny säkerhetsskyddsförordning med nya informationssäkerhetsklasser som planeras träda ikraft 1 januari 2017. Vidare noteras att den hantering som föreslås i andra stycket inte torde vara ändamålsenlig och kostnadseffektiv. LFV föreslår att den rapporteringspliktiga myndigheten endast rapporterar it-incidenten vid ett tillfälle till en myndighet.

Tillsyn, föreskrifter och myndighetsrådets uppgifter
LFV noterar att informationssäkerhet inom ramen för säkerhetsskydd samt tillsyn och rätt att meddela föreskrifter för denna regleras enligt författningarna avseende säkerhetsskydd. Den tillsyn som den föreslagna informationssäkerhetsförordningen kommer att reglera överlappar delvis tillsynen enligt SOU 2015:25. Detta torde försvåra förutsättningarna för överblickbarhet för de aktörer som har att följa föreskrifterna.

Övrigt
De presenterade författningsförslagen innebär betydande krav avseende myndigheters informationssäkerhetsarbete. Mot bakgrund av detta anser LFV att det planerade ikraftträdandet 1 januari 2016 inte är rimligt, utan bör senareläggas. Lämpligen bör ikraftträdandet ske koordinerat med ev. ny säkerhetsskyddslag och säkerhetsskyddsförordning.

LFV
Koncernfunktioner
Hospitalsgatan 30 Norrköping
011-19 20 00 T, 011-19 25 75 F
lfv@lfv.se
www.lfv.se
Org nr. 202100-0795

Beslut i detta ärende har fattats av generaldirektören. Föredragande har juristen Liine Jaanivald varit. Medverkat i beslutet har även chefsjurist Petra Sernulf.

Norrköping 2015-09-14

…….
Olle Sundin
Generaldirektör LFV

LFV
Koncernfunktioner
Hospitalsgatan 30 Norrköping
011-19 20 00 T, 011-19 25 75 F
lfv@lfv.se
www.lfv.se
Org nr. 202100-0795