Statens servicecenter

YTTRANDE 1(4)

Datum
2015-11-11

Dnr
10742-2015/1131

Justitiedepartementet
103 33 STOCKHOLM

Betänkandet SOU 2015:23 Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten (Ju2015/2650/SSK)

Allmänna synpunkter

Statens servicecenter delar utredarens bedömning om att informations – och cybersäkerheten i Sverige behöver utvecklas och förstärkas samt instämmer i flera av utredningens strategi- och åtgärdsförslag sammantaget bör leda till en förstärkt informations- och cybersäkerhetsförmåga inom staten. Förslaget till förordning behöver dock omarbetas, om det ska genomföras.

Statens servicecenter anser att utredningen hade tjänat på att i högre grad koordinera sitt arbete med utredningen om säkerhetsskyddslagen som resulterade i betänkandet SOU 2015:25, En ny säkerhetsskyddslag. I stället för att utgå ifrån den omoderna säkerhetsskyddslagen från 1996 med dess brister, borde förslaget ha anpassats till den nya lag om säkerhetsskydd som har föreslagits bli den gällande redan från 2017.

Vidare invänder Statens servicecenter mot att de förslag som lämnas i betänkandet endast riktar sig mot statliga myndigheter. Näringslivet, som har en betydelsefull roll som den största ägaren och förvaltaren av samhällsviktig informationsinfrastruktur och därigenom hanterar stora delar av statens information, omfattas inte av några av utredningens förslag. För att möta det överordnade målet om Sveriges säkerhet krävs ett systematiskt informationssäkerhetsarbete som bedrivs på bred front i samhället och av alla relevanta aktörer. I detta arbete måste, förutom staten, även kommuner, landsting och enskilda verksamheter involveras.

När det gäller det föreslagna kravet på it-incidentrapportering som återfinns i förordningsförslaget, 10 respektive 17 §§, framstår det för Statens servicecenter i egenskap av ”värdmyndighet” som otydligt hur och till vem eller vilka en incident ska rapporteras.

Ett exempel kan vara att Statens servicecenter drabbas av en it-incident, som enligt förslaget till ändring i 10 a § säkerhetsskyddsförordningen (1996:633) ska rapporteras till Säkerhetspolisen. Enligt 17 § andra stycket i utredningens förslag ska Statens servicecenters inte rapportera en sådan incident till Myndigheten för samhällsskydd och beredskap (MSB) förrän Säkerhetspolisen gett klartecken till det. Om incidenten bedöms påverka säkerheten för information som Statens servicecenter hanterar i egenskap av ”värdmyndighet” ska den dock, enligt 10 §

Postadress
Statens servicecenter
FE-15
801 71 Gävle

Besöksadress
Ruddammsgatan 30
Gävle

Telefon
0771-456 000

E-post
registrator@statenssc.se

andra stycket i utredningens förslag, rapporteras även till den anlitande myndigheten. Den anlitande myndigheten kan därmed, beroende på incidentens innebörd för den myndigheten, bli skyldig att rapportera incidenten till MSB, enligt 17 § första stycket i förslaget, trots att Säkerhetspolisen inte lämnat "värdmyndigheten" sitt klartecken till att rapportera den dit.

Vidare anser Statens servicecenter att begreppet "värdmyndighet" inte bör användas då det i andra organisatoriska sammanhang har en annan innebörd än den som avses i förordningsförslaget.

Statens servicecenter noterar också att MSB föreslås få flera uppdrag och ansvarsområden samt ökade anslag för att täcka de merkostnader förslagen för med sig för MSB. Den ekonomiska konsekvensanalysen kan däremot inte anses tillräcklig vad gäller de ekonomiska effekter som utredningens förslag medför för övriga myndigheter som resultat av ökade krav även på dessa.

Kommentarer till författningsförslag

Förslag till förordning för statliga myndigheters informationssäkerhet

Definitioner
4 §
Statens servicecenter avråder bestämt från den förslagna definitionen av informationssäkerhet i förordningen d.v.s. *förmåga att upprätthålla konfidentialitet, riktighet, tillgänglighet och spårbarhet i sin informationshantering…..*

Förslaget är otydligt och dessutom ett helt annat än förslaget till definitionen av informationssäkerhet i betänkandet (SOU 2015:25) En ny säkerhetsskyddslag, där informationssäkerhet definieras som *en säkerhetsskyddsåtgärd som ska förebygga dels att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, dels skadlig inverkan på andra informationstillgångar som avser säkerhetskänslig verksamhet.*

Statens servicecenter menar att de olika definitionerna skapar en olycklig dubbelreglering med olika betydelser av begreppet informationssäkerhet.

Myndighetens informationssäkerhetsarbete
7 §
Statens servicecenter avråder från den föreslagna regleringen i första meningen, att *Myndigheten ska kartlägga sina informationsprocesser och klassificera sin information...* Statens servicecenter uppfattar kravet på karläggning av informationsprocesser som omotiverat eftersom det finns andra metoder att identifiera informationstillgångar på. Respektive myndighet bör själv få välja det sätt som bäst passar den egna verksamheten. Statens servicecenter föreslår därför följande alternativa formulering: *Myndigheten ska klassificera sin information…*

Postadress
Statens servicecenter
FE-15
801 71 Gävle

Besöksadress
Ruddammsgatan 30
Gävle

Telefon
0771-456 000

E-post
registrator@statenssc.se

Statens servicecenter anser inte heller att förordningen ska innehålla en reglering om att information ska klassificeras baserat på spårbarhet. Enligt Statens servicecenters uppfattning kan spårbarhet både ses som en särskild aspekt i samband med informationsklassning (i likhet med andra och ibland förekommande egenskaper så som oavvislighet, tillförlitlighet och autenticitet) men också vara en säkerhetsåtgärd för att tillgodose krav på konfidentialitet och riktighet.

Statens servicecenter avråder även från användandet av begreppet *it-incidenter,* i såväl förslagen till förordning som till strategi eftersom begreppet även används i andra sammanhang där det har en helt annan betydelse. Statens servicecenter anser i stället att svensk och internationell standard ska beaktas och att begreppet *informationssäkerhetsincident* bör användas i såväl förordningen som strategin. Denna kommentar gäller för alla förekomster av begreppet i utredningens samtliga förslag.

Statens servicecenter avstyrker även den föreslagna bestämmelsen om att gemensamma krav- och skyddsnivåer ska användas. Då det ännu inte ens finns något förslag till gemensamma krav- och skyddsnivåer att förhålla sig till är det för tidigt att reglera detta i en förordning. Innan det sker bör förslag utarbetas och provas på frivillig väg.

8 §
Statens servicecenter anser att begreppet *säkra it-produkter* behöver definieras då det är otydligt vad som utgör en säker it-produkt. Vidare behöver begreppet, om det ska användas, utökas till att även omfatta tjänster.

Förutsatt att begreppet har definierats föreslår Statens servicecenter därför följande lydelse: *Myndigheten ska,…, välja säkra it-produkter och tjänster vid hantering av information där bristande informationssäkerhet kan medföra en betydande försämring av myndighetens förmåga att bedriva sin verksamhet.*

Upphandling och utveckling av it-system och it-produkter
16 §
Statens servicecenter avstyrker förslaget så som det är formulerat. Statens servicecenter är positiv till standardisering men menar att den föreslagna regleringen leder till en för myndigheterna oproportionerlig kostnadsökning eftersom samhällsviktig verksamhet utgör en omfattande del av de statliga myndigheternas verksamhet. Statens servicecenter menar även att formuleringen behöver ses över eftersom den föreslagna kan bli svår för myndigheter att tillämpa. Som exempel kan nämnas att det i stycket föreskrivs att *säkra och certifierade it-produkter* ska användas i det fall sådana finns tillgängliga samtidigt som det är oklart vad som avses med *säkra och certifierade it-produkter och även vad som ska gälla i fråga om it-tjänster.* Statens servicecenter vill i sammanhanget påpeka att statliga myndigheter (i likhet med

Postadress
Statens servicecenter
FE-15
801 71 Gävle

Besöksadress
Ruddammsgatan 30
Gävle

Telefon
0771-456 000

E-post
registrator@statenssc.se

kommuner, landsting och enskilda) i allt högre utsträckning upphandlar it i form av tjänster i stället för som tidigare i form av (hårdvaru-) produkter.

Slutligen ifrågasätter Statens servicecenter om det är förenligt med gällande upphandlingslagstiftning att i en författning peka ut exakt *vilka* it-produkter som ska användas.

Tillsyn, föreskrifter och myndighetsrådets uppgifter
18 §
Statens servicecenter anser det viktigt att informationssäkerhetsarbetet bedrivs sammanhållet och gemensamt inom statsförvaltningen. Förslaget om inrättande av ett myndighetsråd är ett viktigt steg för att åstadkomma detta.

19-20 §§
Givet att MSB ska ha en fortsatt stödjande och samordnande roll inom området informationssäkerhet, är Statens servicecenter tveksam till att MSB även ges den föreslagna tillsynsfunktionen. Vidare är den föreslagna avgränsningen mot den tillsyn som regleras i säkerhetsskyddsförordningen alltför otydlig, särskilt som definitionen av begreppet informationssäkerhet i den föreslagna förordningen skiljer sig från den som gäller enligt säkerhetsskyddslagen (1996:627).

Detta ärende har avgjorts av generaldirektör Thomas Pålsson efter föredragning av informationssäkerhets- och säkerhetschefen Lars Grundström. Vid den slutliga handläggningen av ärendet har även chefsjuristen Elisabet Ekman medverkat.

Thomas Pålsson
Generaldirektör

Lars Grundström
Informationssäkerhets- och säkerhetschef

Postadress
Statens servicecenter
FE-15
801 71 Gävle

Besöksadress
Ruddammsgatan 30
Gävle

Telefon
0771-456 000

E-post
registrator@statenssc.se