Statens servicecenter

YTTRANDE 1(4)

Datum
2015-10-05

Dnr
10668-2015/1131

Myndigheten för samhällsskydd och beredskap
Remissvar, dnr 2014-6391
651 81 KARLSTAD

Statens servicecenters remissyttrande avseende Förslag till Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet

Allmänna synpunkter

Det sätt på vilket statsförvaltningen arbetar med information och informationstillgångar har över tid utvecklats och förändrats. Som exempel kan nämnas utkontraktering av tjänsteutförande och eller it-drift, i såväl privat som statlig regi. Bland annat mot bakgrund av detta ställer sig Statens servicecenter därför positiv till att Myndigheten för samhällsskydd och beredskap (MSB) reviderar tidigare föreskrifter (MSBFS 2009:10) om statliga myndigheters informationssäkerhet.

Inom angränsande områden har det genomförts större utredningar som var och en för sig och tillsammans kan antas påverka statliga myndigheters informationssäkerhetsarbete. Här kan nämnas betänkandet En ny säkerhetsskyddslag (SOU 2015:25) och betänkandet Informations- och cybersäkerhet i Sverige (SOU2015:23), vilka bägge är under remissbehandling. I de bägge betänkandena har det förts fram författningsförslag vars konsekvenser för de enskilda myndigheterna ännu inte går att bedöma.
Statens servicecenter anser att MSB:s föreskrifter och allmänna råd för statliga myndigheters informationssäkerhet bör utformas och fastställas först när det står klart vilka författningskrav som i övrigt kan komma att ställas på myndigheternas informationssäkerhetsarbete.
Statens servicecenter anser därför att tidpunkten för uppdateringen av MSB:s föreskrift är olämplig och avstyrker förslaget att den nya föreskriften ska träda i kraft redan den 1 januari 2016.

Statens servicecenter väljer även att kritisera det faktum att MSB i det nya förslaget till föreskrift tar bort hänvisningen till de svenska och tillika internationella informationssäkerhetsstandarderna SS-ISO/IEC 27001 och 27002.
Statens servicecenter anser att standardisering och tillämpning av standarder har stor betydelse för statliga myndigheters förmåga till, och intresse av, etablering, uppbyggnad och förvaltning av ett systematiskt informationssäkerhetsarbete. Bland annat avseende organisation, verksamhet och innehåll. Att aktivt bidra till en bred användning av nationella tillika internationella fastställda och allmänt accepterade informationssäkerhetsstandarder, anser Statens servicecenter vara särskilt betydelsefullt när det gäller statliga myndigheters relationer med andra

Postadress
Statens servicecenter
FE-15
801 71 Gävle

Besöksadress
Ruddammsgatan 30
Gävle

Telefon
0771-456 000

E-post
registrator@statenssc.se

myndigheter men även i förhållande till andra aktörer. Användningen av standarder bedöms påtagligt bidra till ökade förutsättningar för att lyckas formulera och överenskomma om gemensamma krav- och målbilder för informationssäkerheten mellan beställare och leverantörer, till exempel vid utkontraktering av tjänster.

I konsekvensutredningen saknar Statens servicecenter en redogörelse som motiverar ett förslag till förändring av den nu gällande modellen för informationsklassificering (MSB publikationsnummer MSB 0040-09) och som MSB publicerar på www.msb.se.
Denna modell omfattar informationssäkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet till skillnad mot den nu föreslagna klassificeringsmodellen som även innefattar spårbarhet.

Enligt Statens servicecenters syn kan spårbarhet bådes ses som en särskild aspekt i samband med informationsklassificering (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. Mot denna bakgrund vore det därför önskvärt att MSB mer tydligt redogör för sina argument för och skäl till att nu revidera och utöka klassificeringsmodellen till att även innefatta spårbarhet. Därtill vilka brister man identifierat att dagens modell leder till och vilka nyttor man bedömer att den nya modellen kommer att bidra till.

Förslag till ny föreskrift om statliga myndigheters informationssäkerhet
Statens servicecenter anser att 5 § ska förtydligas med en hänvisning till att statliga myndigheter i sitt informationssäkerhetsarbete ska utgå ifrån de svenska (tillika internationella) informationssäkerhetsstandarderna SS-ISO/IEC 27001 respektive SS-ISO/IEC 27002.

Statens servicecenter föreslår därför följande formulering:
”5 § Varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. Ledningssystemet ska ta sin utgångspunkt från, vid var tid gällande utgåva av standarderna, SS-ISO/IEC 27001 Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav, respektive SS-ISO/IEC 27002 Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder. Det ska säkerställas att det sker en adekvat resurstilldelning för informationssäkerhetsarbetet samt att löpande och regelbunden information lämnas till myndighetsledningen.”

I 8 § regleras hur myndigheter ska identifiera sina krav på informationssäkerhet. Statens servicecenter ifrågasätter värdet av en tvingande kartläggning av myndighetens verksamhetsprocesser och menar att det bör vara upp till myndigheten att själv välja det arbetssätt och den metod som passar myndigheten bäst i syfte att identifiera sina informationstillgångar och att därefter, vid behov, fördela roller och ansvar. Statens servicecenter föreslår därför

Postadress
Statens servicecenter
FE-15
801 71 Gävle

Besöksadress
Ruddammsgatan 30
Gävle

Telefon
0771-456 000

E-post
registrator@statenssc.se

följande formulering: "*8 § I syfte att underlätta identifiering av egna krav på informationssäkerhet ska myndigheten kartlägga sina informationstillgångar samt, vid behov, utse informationsägare till dessa.*"

I 9 § 3 föreskrivs att myndigheten regelbundet, och minst vartannat år, ska genomföra övningar med berörd del av organisationen för att pröva och utveckla myndighetens säkerhetsåtgärder för kontinuitetshantering avseende informationssäkerhet.
Statens servicecenter önskar här att MSB definierar och mer utförligt beskriver innebörden av begreppen "berörd del av organisationen" respektive "myndighetens säkerhetsåtgärder för kontinuitetshanteringen avseende informationssäkerhet". Detta för att förtydliga vilket resultat regleringen syftar till att åstadkomma.

I 10 § regleras att myndigheten med stöd av modeller som myndigheten beslutar ska vidta ett flertal åtgärder.
Statens servicecenter anser att det i detta avseende torde vara av mindre betydelse om den modell eller de modeller som används är beslutad av myndigheten eller inte så länge de ger verksamheten det stöd som behövs för genomförande av informationsklassning, riskanalys, fastställande av skyddsnivå etc.
Statens servicecenter föreslår därför följande lydelse:
"*10 § I syfte att hantera hot och risker som rör informationssäkerheten i verksamheten ska myndigheten:*

1. *klassa information med utgångspunkt i konfidentialitet, riktighet, tillgänglighet och spårbarhet i olika nivåer utifrån vilka konsekvenser som kan uppstå av ett bristande skydd,*
2. *identifiera, analysera och bedöma hot och risker för verksamhetens information, system och tjänster,*
3. *utifrån informationsklassningens resultat identifiera och införa åtgärder (skyddsnivå) som motsvarar informationens krav på skydd,*
4. *följa upp och utvärdera införda åtgärder och gjorda bedömningar av hot och risker,*
5. *kontinuerligt utveckla skyddet för att över tid upprätthålla informationens behov av säkerhet, samt*
6. *fortlöpande dokumentera genomförda åtgärder enligt denna paragraf.*"

Postadress
Statens servicecenter
FE-15
801 71 Gävle

Besöksadress
Ruddammsgatan 30
Gävle

Telefon
0771-456 000

E-post
registrator@statenssc.se

Förslag till Myndigheten för samhällsskydd och beredskaps allmänna råd om statliga myndigheters informationssäkerhet

I 8 § anges att myndigheten behöver kartlägga sina verksamhetsprocesser och det behov av informationshantering som behövs för att stödja dessa för att underlätta verksamhetens arbete med att ställa krav på informationens olika egenskaper.

Statens servicecenter menar dock att det kan finnas andra och för myndigheten bättre anpassade och mer effektiva sätt att identifiera sina informationstillgångar på för att därefter formulera de informationssäkerhetskrav som behövs för skydd av dessa. Detta kan åstadkommas utan att myndigheten genomför en verksamhetsanalys.

Mot bakgrund av ovanstående rekommenderar Statens servicecenter att kravet på genomförande av verksamhetsanalys tas bort.

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

Lars Grundström

Postadress
Statens servicecenter
FE-15
801 71 Gävle

Besöksadress
Ruddammsgatan 30
Gävle

Telefon
0771-456 000

E-post
registrator@statenssc.se