SPV

Datum
2015-09-14

Vår beteckning
MD 2015/217

Ert datum
2015-05-06

Er beteckning
Ju2015/2650/SSK

Vår referens
Hans Brännlund, 060-18 76 86

Justitiedepartementet
Enheten för samordning av samhällets krisberedskap (SSK)
103 33 Stockholm

Yttrande över betänkande SOU 2015:23 Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten

Statens tjänstepensionsverk (SPV) har tagit del av betänkandet och stödjer utredningens förslag, men lämnar några synpunkter och kommentarer.

Som beskrivits om utredningens inriktning ska förslagen begränsas till det statliga området, men kan bli tydligare i vissa delar genom att täcka in myndigheters utkontraktering, köp av tjänster från privata aktörer och kontakter med andra än enbart andra myndigheter.

Bilaga 1, utdrag ur betänkandet med markeringar för givna kommentarer.

Författningsförslaget

Nedan redovisas ett antal synpunkter på författningsförslaget (markerat i bilaga 1):

- 5 §, kommentar som rör leverans till *annan organisation*, det bör även gälla för vad som levereras till allmänheten och enskilda.
- 8 §, kommentar som rör val av säkra *it-produkter*, det bör även gälla tjänster (beroende på hur it-produkt valts att definieras).
- 10 §, kommentar som rör *annan myndighet, en så kallad värdmyndighet,* att myndigheten har ansvar för rapportering av incidenter oavsett om informationssäkerhetsarbetet administreras av en värdmyndighet direkt eller via en privat underleverantör.
- 15 §, kommentar som rör ansvar och roller i samband med upphandling och utveckling av *it-system eller it-produkter,* det bör även gälla tjänster (processer).
- 16 §, kommentar som rör *upphandling av it-produkter* respektive *säkra och certifierade it-produkter,* Det bör även gälla tjänster respektive säkra tjänster. Dessutom är det kanske inte alltid möjligt att ställa krav på *certifierade* it-produkter, andelen certifierade it-produkter kanske inte är tillräckligt omfattande. Det är också viktigt att ramavtalen fungerar även när omsättningen på certifierade it-produkter är snabbare än förnyelsen av ramavtalen.
- 17 §, kommentar som rör *leverans till annan organisation*, det bör även gälla vad som levereras till enskild.

SPV lämnar också några kommentarer och reflektioner på betänkandet, se nedanstående texter.

Myndighetsrådets uppgifter
Det bör klargöras på vilken nivå som stöd ska ges, det skiljer en del mellan vad som nämns nedan (från sidan 220 respektive 225-226). Det vore önskvärt med bistånd av expertkompetens mer allmänt än enbart om gällande it-standarder och certifikat.

Förvaltningsmyndigheter under regeringen
Då det gäller revision och återrapporteringskrav är frågan om man över huvud taget ska peka ut särskilda åtaganden specifikt, som ansvaret för att upprätthålla säker informationshantering. Myndighetens ledning har redan ett utpekat ansvar för verksamheten som helhet, av vilken informationssäkerheten är en del. Istället för att årligen lämna tilläggsupplysning i årsredovisningen förespråkar SPV en skrivelse i myndighetsförordningen.

Möjligheten att tillämpa lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS)
I lagen beskrivs användningsområdet för LUFS vara inköp av försvarsmateriel, varför SPV inte kan se hur denna lag skulle kunna användas bredare.

Konsekvenser av förslagen
Hela utredningen med en höjd ambitionsnivå lyfter fram behovet av insatser för att öka informationssäkerheten inom myndigheterna, behov av kompetenser, mer arbetet med informationsklassning och uppföljningar, ökade resurser för upphandling. SPV bedömer att en ökad ambitionsnivå kräver resurstillskott av ny och eventuellt dyrare kompetens för att kunna uppfylla intentionerna i denna utredning.

Statens intäkter
På lång sikt kan genomförande av utredningens förslag leda till kostnadsminskning, men inledningsvis kommer det nog att kräva ökade resurser. Istället för att prata om en kostnadsminskning kanske det snarare kan röra sig om att undvika kostnadsökningar genom att undvika oönskade händelser som orsakas av brister inom informations-säkerhetens område, i takt med ökad mängd informationssystem och integrationer.

Finansiering
Behoven inom många organisationer att hantera dessa frågor fullt ut riskeras att underskattas. Det blir ökade krav, exempelvis på internt arbete med informationsarbetet, kompetensutveckling, processförbättringar, krav på leverantörer, vid upphandling av produkter och tjänster. Kompetens och resursfrågan måste stärkas, särskilt vid mindre myndigheter.

Detta yttrande har beslutats av undertecknad generaldirektör i närvaro av säkerhetsskyddschef Hans Brännlund, föredragande och biträdande säkerhetsskyddschef Jan-Olof Flink.

Med vänlig hälsning
Statens tjänstepensionsverk

Joakim Stymne

Hans Brännlund

Bilaga 1

Förtydligande markeringar för kommentarer ovan, SOU 2015:23.

Författningsförslag
Utdrag
5 §
Varje myndighet ansvarar för att, genom ett risk- och sårbarhetsbaserat, systematiskt och processinriktat arbetssätt, upprätthålla en tillräcklig nivå av informationssäkerhet för den information de ansvarar för eller hanterar i tjänster som myndigheten levererar till en *annan organisation*. Myndigheten ska i sitt informationssäkerhetsarbete särskilt beakta behovet av ledningssystem och etablerade standarder för informationssäkerhet.
8 §
Myndigheten ska, med stöd av risk- och sårbarhetsanalyser, välja och använda säkra *it-produkter* vid hantering av information där bristande informationssäkerhet kan medföra en betydande försämring av myndighetens förmåga att bedriva sin verksamhet. I de fall säkra itprodukter finns utpekade i verkställighetsföreskrifter som meddelats med stöd av denna förordning ska dessa användas.
10 §
Kraven i 5–9 §§ gäller endast i tillämpliga delar sådana myndigheter vars informationshantering eller vars informationssäkerhetsarbete administreras av en *annan myndighet*, en så kallad *värdmyndighet*. En sådan värdmyndighet som avses i första stycket ska informera den anlitande myndigheten om inträffade it-incidenter som har eller kan ha påverkat säkerheten hos den anlitande myndighetens information.
15 §
I samband med upphandling och utveckling av *it-system eller it-produkter* ska myndigheten i förhållande till leverantören klarlägga ansvar och roller för informationssäkerhetsarbetet. Myndigheten ska även fastställa processer för hur säkerhetskrav ska hanteras och hur uppföljning ska ske. Upphandlingen eller utvecklingen ska föregås av informationsklassning och riskanalys av berörd information. Resultatet av klassningen och riskanalysen ska vara styrande för utformningen av säkerhetskrav som ställs vid upphandling eller utveckling. Kraven i första och andra stycket gäller även vid anslutning till myndighetsgemensamma tjänster för e-förvaltning eller liknande syfte. En myndighet ska endast uppdra åt någon annan att hantera myndighetens information om hanteringen kan ske med tillräcklig säkerhet och enligt denna författning. I detta ingår att försäkra sig om att it-incidenter som har eller kan ha påverkat säkerheten rapporteras till myndigheten.
16 §
I samband med upphandling av *it-produkter* som är avsedda att användas i samhällsviktig verksamhet som myndigheten bedriver eller ansvarar för ska, då sådana finns tillgängliga, endast *säkra och certifierade it-produkter* användas. I de fall säkra it-produkter finns utpekade i verkställighetsföreskrifter ska dessa användas.

17 §
En myndighet ska till Myndigheten för samhällsskydd och beredskap skyndsamt rapportera it-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten levererar till en annan *organisation*. För incidenter som ska anmälas till en tillsynsmyndighet enligt bestämmelserna i 10 a § säkerhetsskyddsförordningen (1996:633) gäller rapporteringsplikten enligt första stycket inte förrän tillsynsmyndigheten har meddelat den rapporteringspliktiga myndigheten att incidenten inte längre är föremål för behandling hos tillsynsmyndigheten.

Myndighetsrådets uppgifter
Från sidan 220, utdrag

> Myndighetsrådet bör med bland annat stöd av den nationella styrmodellen och tillsammans med den nya upphandlingsmyndigheten ge stöd till myndigheter som har behov av expertkompetens vad gäller it- och informationssäkerhet. Stödet bör ges till myndigheter som står inför upphandling av informations- och it-lösningar och *bör bestå av allmänna rekommendationer om bl.a. it-standarder och krav på certifiering.*

Från sidan 225-226, utdrag

> I avsnitt 9.2.2 har utredningen föreslagit att ett statligt myndighetsråd för informationssäkerhet ska inrättas. En ny bestämmelse om rådets uppgifter ska införas i förordningen. Det ska anges att myndighetsrådet har till uppgift att stödja och utveckla informationssäkerhetsarbetet i samhället, varvid det som exempel bör räknas upp att det i detta ingår att utgöra en gemensam beredning- och remissinstans på informationssäkerhetsområdet, bidra med stöd rörande informationssäkerhetsfrågor vid utfärdandet av föreskrifter på informationssäkerhetsområdet, förvalta och utveckla tillämpliga krav i standarder samt certifiering och ackreditering (kontrollordningar) för produkter och tjänster med bäring på informationssäkerhet i samhällsviktig verksamhet, *bistå med expertkompetens i samband med upphandling av tjänster och produkter på informationssäkerhetsområdet, och utveckla krav- och skyddsnivåer.*

Förvaltningsmyndigheter under regeringen
Från sidan 235, utdrag

> Som framgått har behovet av att skydda information blivit en allt viktigare angelägenhet för myndigheterna. Att i en sådan situation säkerställa att internrevisionen beaktar även informationssäkerhetsfrågorna har potential att öka fokus på frågorna och skapa än förbättrade förutsättningar för att ett systematiskt informationssäkerhetsarbete som får faktisk effekt kan bedrivas. *Utredningen föreslår därför att det i förordningen (2000:605) om årsredovisning och budgetunderlag införs en bestämmelse om att till årsredovisningen en tilläggsupplysning ska lämnas om genomförd internrevision och status för informationssäkerhetsarbete på myndigheten. Ett alternativ vore att i myndighetsförordningen (2007:515) införa en bestämmelse om att myndighetens ledning ansvarar för att upprätthålla säkerhet i sin informationshantering.*

Möjligheten att tillämpa lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS)

Från sidan 242-243, utdrag

> Om upphandlande myndighet efter att ha uttömt de möjligheter till kravställande som LOU medger likafullt inte anser att upphandling kan ske med erforderliga garantier för säkerhet i staten kan myndigheten i stället överväga att använda upphandlingsförfarandet enligt lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS). *Lagen är avsedd för upphandlingar av materiel och tjänster* som är av så känslig natur att upphandling enligt LOU eller lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster inte lämpar sig. LUFS är i stort sett parallell till dessa två lagar men till skillnad från dem innehåller LUFS bestämmelser om informationssäkerhet, försörjningstrygghet och underentreprenad. Lagen genomför huvudsakligen Europaparlamentets och rådets direktiv2009/81/EG.

Konsekvenser av förslagen

Från sidan 277, utdrag

> Utredningens förslag innebär en höjd ambitionsnivå för statens informationssäkerhet. *Åtskilliga av åtgärdsförslagen kan rymmas inom myndigheters befintliga budget.* Nedanstående beräkningar avser främst de kostnader som uppstår hos Myndigheten för samhällsskydd och beredskap, som är den myndighet som enligt den föreslagna förordningen får ett utökat förvaltningsansvar. Kostnader av mindre omfattning kan också komma att uppstå i andra delar av statsförvaltningen. Dessa är dock svårare att överblicka. De förslag i föregående kapitel som varit möjliga att kostnadsberäkna anges nedan.

Statens intäkter

Från sidan 282, utdrag

> *Utredningen bedömer att det snarare blir minskade kostnader på sikt än ökade statliga intäkter som följd av utredningens förslag. På informationssäkerhetens område är det sannolikt så att en förbättrad organisation, i enlighet med våra förslag i normalfallet dels leder till lägre kostnader, dels förorsakar genomförandekostnad men på sikt en kostnadsminskning tack vare bättre säkerhet.* En samordning inom statsförvaltningen som bygger på en gemensam styrmodell kan leda till lägre kostnader för statliga myndigheter, om man i stället för att utveckla egna varianter följer gemensamma principer. Standardiseringsinsatser, liksom de flesta it-investeringar, innehåller i teorin en inledande investeringskostnad och därefter en period av ökande effektivitet, möjligen lägre kostnader förutsatt att organisation, resurser och kompetens anpassas till den nya tekniken. Det är dock svårt att kvantifiera dessa effekter.

Finansiering

Från sidan 282, utdrag

> Eftersom informationssäkerhet normalt anses ingå i kostnaderna för respektive verksamhet är utgångspunkten att *flera förslag bör bäras av re-*

spektive verksamheter; kostnaderna kan antas vara ganska marginella i förhållande till de totala verksamhetskostnaderna.