Försäkringskassan

REMISSYTTRANDE

Datum
2015-09-11

Vår beteckning
Dnr 24912-2015

Justitiedepartementet
103 33 Stockholm

Informations- och cybersäkerhet i Sverige - Strategi och åtgärder för säker information i staten (SOU 2015:23)

Justitiedepartementets dnr 2015/2650/SSK

Försäkringskassan är positiv till utredningens förslag om strategi och åtgärder för säker information i staten. Det finns dock några delar av utredningens förslag som Försäkringskassan anser behöver förtydligas och utvecklas.

Försäkringskassan önskar lyfta fram som en övergripande synpunkt att det är viktigt att de begrepp och krav som används i den föreslagna nya förordningen harmonierar med begrepp och krav som används i andra författningar och aktuella förslag till nya författningar inom angränsande områden inte minst SOU 2015:25 En ny säkerhetsskyddslag.

Försäkringskassan föreslår att begreppet informationssäkerhetsincident används genomgående istället för it-incident i förordningen och att det begrepp som används definieras.

1. Författningsförslag

11 §

Enligt den föreslagna paragrafen kan vissa myndigheter bli skyldiga att uppfylla särskilda krav på informationssäkerhet rörande användning av kommunikationsnät, sensorsystem för it-incidentidentifiering och kompetens för informationssäkerhetschef eller motsvarande. Enligt 20 § får Myndigheten för samhällsskydd och beredskap meddela föreskrifter för de särskilda krav som anges i bl.a. 11 §. Försäkringskassan ställer sig frågande till hur sistnämnda föreskriftsrätt är tänkt att förhålla sig till det ansvar som åläggs varje myndighet enligt 30 a § förordningen (2006:942) om krisberedskap och höjd beredskap (KBF). Försäkringskassan anser dessutom att hänsyn måste tas till myndigheternas olika förutsättningar när det ställs krav på särskilda tekniska lösningar. Om det exempelvis ställs krav på särskilda tekniska

Postadress
103 51 Stockholm

Besöksadress
LM Ericssons väg 30, Hägersten

Telefon
08-786 90 00

E-post
huvudkontoret@forsakringskassan.se

Internetadress
www.forsakringskassan.se

Telefax
08-411 27 89

Org.nr
202100-5521

lösningar vid utformningen av kommunikationsnät och införandet av sensorutrustning är en förutsättning för att dessa ska kunna införas att de tekniska lösningarna är förenliga med den befintliga it-miljön.

16 §

I den föreslagna paragrafen föreslås att ett krav på användande av certifierade eller säkra it-produkter införs. Försäkringskassan vill framföra att det är viktigt att klargöra vad som avses med säkra respektive certifierade it-produkter. Försäkringskassan önskar framhålla att genom att specifikt ställa krav på "säkra it-produkter" kan en förordning skapa övertro på produkternas förmåga att hantera identifierade risker. Produkternas hantering är minst lika viktig som produkten i sig. Eventuella brister i en produkt kan eventuellt kompenseras genom väl genomtänkt hantering. Det är svårt att göra motsatsen.

Försäkringskassan önskar även framhålla att genom att ställa krav på certifiering av säkra it-produkter kan låsningseffekter skapas. Med tanke på att produkter utvecklas ständigt på en global marknad är det inte säkert att certifiering som en "säker it-produkt" på svensk marknad är leverantörens högsta prioritet. Det kan skapa ytterligare komplikationer när det gäller open source-produkter. Förordande av specifika produkter är inte heller önskvärt ur ett arkitekturperspektiv där man vill kunna välja den produkt som bäst löser problemet med hänsyn till samtliga krav.

9.2.5 Informationssäkerhet som en del av myndighetens revision

Utredningens bedömning i avsnitt 9.2.5 anger att *"Revision av informationssäkerhet bör utvecklas. Myndighetsledningens ansvar för att upprätthålla säkerhet i myndighetens informationshantering förtydligas genom rapporteringskrav i förordning (2000:606) om årsredovisning och budgetunderlag"*

Försäkringskassan bedömer att det finns ett behov av att förstärka den interna styrningen och kontrollen inom informationssäkerhetsområdet, vilket bland annat lyfts fram av Internrevisionens senaste granskning på området. Försäkringskassan anser emellertid inte att det är regelverket som brister utan att det snarare är tillämpningen av den styrning som redan finns.

De brister betänkandet lyfter fram tyder på svagheter i myndigheternas interna styrning och kontroll och inte på den styrning som finns i MSB:s föreskrifter om statliga myndigheters informationssäkerhet, anvisade standarder eller i gällande förordningar. Av standarden för ledningssystem för informationssäkerhet (LIS) framgår obligatoriska krav för såväl ledningens roll och ansvar för uppföljning som för intern revision av ledningssystemets funktionalitet.

Det vore olyckligt att i förordningen om årsredovisning och budgetunderlag eller i myndighetsförordningen peka ut informationssäkerhet som en enskild viktig parameter bland flera inom intern styrning och kontroll. Av myndighetsförordningen framgår det redan att "myndighetens ledning ska

säkerställa att det vid myndigheten finns en intern styrning och kontroll som fungerar på ett betryggande sätt". Detta täcker även in informationssäkerheten.

Försäkringskassan önskar uppmärksamma att det finns otydligheter avseende användningen av begreppen "uppföljning", "revision", "intern revision" och "internrevision" i betänkandet. I betänkandet används ett flertal begrepp med likvärdig innebörd. Exempelvis används *säkerhetsrevision* (sid 53), *intern revision* (sid 235), *internrevision* (sid 235) och *extern revision (sid 235)*. Begreppen "revision" och "uppföljning" används i hög utsträckning som ett samlat begrepp, utan att det framgår om man menar två olika saker eller ska se det som en och samma. Betänkandet anser att det särskilt är reglerna för intern revision som upplevs uppvisa brister utan att redogöra för bristerna eller vilka regler som avses. Det innebär att det blir otydligt vad utredningen menar med att revisionen bör utvecklas. Försäkringskassan menar att det är viktigt att i kommande förordningstext vara tydlig med vad som avses.

Det är även viktigt att skilja på internrevision enligt internrevisions-förordningen och intern revision enligt kravstandarden för LIS eftersom det är olika regelverk som styr dessa områden. Intern revision enligt kravstandarden för LIS är en del av ledningens uppföljning och kontroll – en del av ledningssystemet. Internrevision i enlighet med internrevisionsförordningen och internationella standarder för internrevisionsprofessionen bör inte, med hänsyn till syfte och uppdrag, vara en del av ledningssystemet. Se tabellen nedan.

Internrevisionsförordningen	**LIS**
Revisionen ska omfatta all verksamhet som myndigheten bedriver eller ansvarar för	Revisionen omfattar ledningssystemet för informationssäkerhet
Granskningens inriktning utgår från en analys av verksamhetens risker	Granskning ska bedrivas löpande med planerade intervall
Syftet är att granska och utvärdera hela kedjan som ingår i intern styrning och kontroll	Syftet är att säkerställa att alla delar i standarden är uppfyllda
Här krävs en bred kunskap inom styrnings- och managementfrågor samt övergripande kunskap om myndighetens hela verksamhetsområde	Här krävs detaljerad sakkunskap inom informationssäkerhetsområdet hos den funktion som ska utföra granskningarna

Betänkandet slår fast att revision och uppföljning är av avgörande betydelse för att kunna bedriva ett systematiskt informationssäkerhetsarbete. Att uppföljning

är viktigt framgår även av LIS liksom av gällande föreskrifter.[1] Följs inte verksamheten upp kan inte myndigheten sägas ha en betryggande intern styrning och kontroll.[2]

Löpande kontrollaktiviteter ("intern revision" av LIS) är en del av ledningssystemet. Följande modell som beskriver olika ansvarsnivåer i en organisation kan användas för att beskriva roller och ansvar.[3].

1. Första ansvarslinjen är myndighetens dagliga verksamhet. I myndigheten ska det finnas en god intern styrning och kontroll för att förebygga fel. Denna ansvarslinje äger och hanterar sina risker och kontroller.

2. Andra ansvarslinjen utgörs av myndighetens egna regelbundet och återkommande uppföljningar och kontroller. Chefer, controllers och särskilda funktioner är en del av denna ansvarslinje. Som särskilda funktioner kan nämnas säkerhet, regelefterlevnad samt "interna revisioner" av miljö-, informations- och kvalitetsledningssystem.

3. Tredje ansvarslinjen utgörs av Internrevisionen. Internrevisionen har ingen del i myndighetens dagliga arbete, uppföljning eller kontroller. Internrevisionen ska fungera oberoende i förhållande till de två första ansvarslinjerna och ska bedöma om de två första ansvarslinjerna har fungerat som det var tänkt, att intern styrning och kontroll är betryggande.

Behov av ett tydligare regelverk

Förslaget är att det i förordningen (2000:605) om årsredovisning och budgetunderlag bör införas en bestämmelse om att en tilläggsupplysning ges i årsredovisningen om genomförd internrevision och status för informationssäkerhetsarbetet. Alternativt att det i myndighetsförordningen (2007:605) införs en bestämmelse om att myndighetens ledning ansvarar för att upprätthålla säkerhet i sin informationshantering.

Som sagts ovan anser Försäkringskassan inte att det är regelverket som brister, det är snarare tillämpningen av den styrning som finns. Av myndighetsförordningen framgår det redan att "myndighetens ledning ska säkerställa att det vid myndigheten finns en intern styrning och kontroll som fungerar på ett betryggande sätt".[4] Detta täcker även in informationssäkerheten. Fungerar inte arbetet med informationssäkerhet enligt dagens regelverk med väsentliga avvikelser, kan den interna styrningen och kontrollen inte anses vara betryggande.

Ett sätt att följa upp tillämpningen är genom egna uppföljningsaktiviteter och internrevision. Dessa krav finns redan reglerade. Internrevisionen bör inte

---

[1] 3 § förordningen (2000:605) om årsredovisning och budgetunderlag

[2] 4 § 4 myndighetsförordningen (2007:515)

[3] Modellen som beskriver de tre ansvarslinjerna används både inom privat och statlig sektor. I IIA:s position paper "Three lines of defense" används ordet försvarslinje.

[4] 4 § 4 myndighetsförordningen (2007:515)

blandas ihop med intern revision enligt standarden för LIS eftersom det är två olika företeelser.

Att återredovisa informationssäkerhetsarbetet i årsredovisningen kan tillföra ett värde för regeringens uppföljning av informationssäkerhetsarbetet. Detta bör emellertid inte styras av en förordning, utan snarare utifrån regeringens behov av uppföljning via återrapporteringskrav i regleringsbreven.

7.7.3 Standardisering av informations- och it-säkerhet

Under rubriken nämns att "Inom offentlig upphandling möjliggör lagarna för den upphandlande myndigheten och enheten att hänvisa till standarder men hänvisningarna ska följas av ordet "likvärdiga" för att säkerställa konkurrens på lika villkor". Försäkringskassan önskar framföra att det i samband med varje upphandling ska göras en avvägning och bedömning av vilka säkerhetskrav som ska ställas, utifrån föremålet för upphandlingen. Att ett krav åtföljs av orden "eller likvärdigt" säkerställer i sig inte att kravet är förenligt med upphandlingslagstiftningen. Om hänvisning ska göras till en standard som är framtagen inom staten, måste kraven i standarden/kriterierna i denna vara relevanta för upphandlingsföremålet och i övrigt förenliga med gemenskapsrätten. Det är därför viktigt att upphandlande myndigheter och enheter får stöd i att ställa relevanta krav i samband med upphandling, vilket utredningen också föreslår att ett statligt myndighetsråd (se avsnitt 9.2.2, Inrättande av ett myndighetsråd) bland annat med stöd av den nationella styrmodellen och tillsammans med den nya upphandlingsmyndigheten ska göra.

9.3.1 Krav på upphandling

Koncentration av leverantörer (s. 239)

Utredningen anför under rubriken att hot- och riskbilden blir aggregerad på nationell nivå då allt större informationsmängder samlas hos ett fåtal leverantörer. Vidare att skälet till fåtalet leverantörer är att den svenska marknaden är begränsad och är en konsekvens av de krav som finns i lagen om offentlig upphandling, vilka leder till formell begränsning i mångfald leverantörer. Utredningen anför även att statliga myndigheter är hänvisade till att sköta sina upphandlingar via Kammarkollegiets ramavtal, som i praktiken leder till att det i huvudsak är tre stora leverantörer som levererar.

Försäkringskassan önskar framhålla att upphandlingar inom it-området m.m. inte får begränsas till den svenska marknaden. Någon formell begränsning av antalet leverantörer finns inte i lagen om offentlig upphandling. Gällande Kammarkollegiets ramavtal och statlig inköpssamordning, ska myndigheter enligt förordningen (1998:796) om statlig inköpssamordning avropa från de avtal som avses i förordningens 2 §, om myndigheten inte finner att en annan form av avtal sammantaget är bättre. En statlig upphandlande myndighet kan således välja att upphandla själv eller tillsammans med andra upphandlande myndigheter.

***Möjligheten att tillämpa lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS)* (s. 242)**

Utredningen tar under rubriken upp att om en upphandlande myndighet efter att ha uttömt de möjligheter till kravställande som LOU medger, likafullt inte anser att upphandling kan ske med nödvändiga garantier för säkerhet i staten, kan myndigheten i stället överväga att tillämpa LUFS. Försäkringskassan ser ett behov av närmare vägledning och stöd till upphandlande myndigheter gällande när LUFS kan bli tillämpligt.

Beslut i detta yttrande har fattats av t.f. säkerhetsdirektör Sture Hjalmarsson i närvaro av internrevisionschef Lina Gidlund, rättschef Eva Nordqvist, verksamhetsområdeschef Cecilia Mauritzon och säkerhetsstrateg Heini Möller, den senare som föredragande.

Sture Hjalmarsson

Heini Möller