PENSIONS MYNDIGHETEN

Remissyttrande

2015-09-09

Dnr/Ref. VER 2015-160

Justitiedepartementet
103 33 Stockholm

SOU 2015:23 Informations- och cybersäkerhet i Sverige

Inledning och sammanfattning

Informations- och cybersäkerheten i Sverige behöver stärkas och Pensionsmyndigheten ställer sig bakom flera av förslagen, trots att några dem är så övergripande beskrivna att de är svåra att bedöma. Detta gäller bland annat myndighetsrådet, den nationella styrmodellen och kravet på incidentrapportering.

Digitaliseringen i samhället och det offentligas utveckling och tillhandahållande av nya e-tjänster ställer höga krav på informationssäkerhet vilket är både resurs- och kompetenskrävande. Enligt vår uppfattning är det angeläget att samordning och samverkan mellan myndigheterna stärks, för att arbetet ska kunna bedrivas så effektivt som möjligt och med hög kvalitet. Vi ser att MSB har en nyckelroll i detta arbete.

En övergripande synpunkt är att det i det fortsatta beredningsarbetet är av största vikt att förslagen i det nu aktuella betänkandet bedöms och anpassas till redan gällande författningskrav och förslag i pågående utredningar inom angrändande områden. Vi vill i sammahanget särskilt peka på SOU 2015:25 En ny säkerhetsskyddslag, och MSB:s föreskrifter för statliga myndigheters informationssäkerhet (MSBFS 2009:10 och dess tänkta ersättare). Enligt vår uppfattning finns det exempel på att detta ännu inte fullt är uppnått, alternativt inte är formulerat på ett sådant sätt att det är fullt ut begripligt, kommunicerbart och praktiskt hanterbart.

Vi är kritiska till några av förslagen, bland annat kravet på kartläggning av informationsprocesser. Vi anser att varje myndighet ska få avgöra själva om just kartläggning av processer är den metod som passar dem bäst.

Vi är kritiska till MSB:s på vissa område väl otydliga och långtgående befogenheter att styra andra aktörers agerande. Detta gäller inte minst förslaget i 11 § i den föreslagna förordningen.

Vi vill också framhålla det utökade behovet av praktiskt stöd som de olika förslagen medför, vilket inte får underskattas och därför bör analyserades ytterligare.

När det gäller konsekvensanalysen delar vi uppfattningen att vissa av förslagen kan rymmas inom myndigheternas befintliga budget. Vi bedömer dock att den samlade ambitionshöjningen ofrånkomligen kommer att medföra ett ökat resursbehov för de enskilda myndigheterna och är kritiska till att detta inte framgår tillräckligt och anser därför det måste tas i beaktande om förslagen ska genomföras.

När det gäller den föreslagna strategin med tillhörande åtgärder är vi i stort positiva. Det har dock stor betydelse hur strategierna i praktiken kommer att genomföras. För att få avsedd effekt är det naturligvis också ytterst viktigt att det sätts mätbara konkreta mål, nerbrutet i en tidplan med tydligt ansvariga och uppföljning, rapportering och eskaleringsordning vid avvikelser.

Pensionsmyndigheten	Telefon	Fax	E-post	Org.nr
Box 38190 100 64 Stockholm	0771-771 771	08-658 13 00	registrator@pensionsmyndigheten.se	202100-6255

Synpunkter på förslaget till förordning (kap 1, sid 27-33)

3 § – Vi instämmer inte i bedömningen att Regeringskansliet ska undantas. Ordningen skulle rimma illa med behovet av en generell höjning av informationssäkerheten och bättre samordning inom staten där Regeringskansliet har en nyckelroll.

4 § – Definitionen av begreppet informationssäkerhet (”förmågan att upprätthålla”) anser vi inte vara korrekt i en jämförelse med praxis och svensk standard.

5 § – Vi anser att ett ledningssystem för informationssäkerhet enligt vedertagen standard bör föreskrivas och vänder oss mot att ett processinriktat arbetssätt föreskrivs.

7 § – Enligt vår uppfattning räcker det att föreskriva att ”myndigheter ska klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet”. De enskilda myndigheterna kan sedan avgöra om just kartläggning av informationsprocesser är den metod som passar bäst för den egna organisationen eller om någon annan metod ska användas.

7 § – Ett annat begrepp än ”IT-incidenter” bör användas i förordningen och strategin. I utkastet till reviderad MSBFS om statliga myndigheters informationssäkerhet används ”informationssäkerhetsincident” och rimligen måste samma begrepp användas. Dessutom behöver begreppet definieras, oavsett vilket som används. Begreppet IT-incidenter leder tanken till ITIL vilket troligen inte är avsikten eller ändamålsenligt.

8 §– Dels bör begreppet ”säkra it-produkter” definieras, dels bör det även utökas till att även gälla tjänster. Se även kommentar nedan under strategi 2.

9 §– Vi föreslår strykning av ”…under fredstida krissituationer och höjd beredskap”, alternativt formuleras ”…även under fredstida krissituationer och höjd beredskap”.

11 §– Vi föreslår rubriken ”Särskilda krav på vissa myndigheter” eller liknande.

11 § – Skrivningarna i denna bestämmelse ger MSB alltför långtgående befogenheter att ställa krav inom de angivna områdena och mot vilka myndigheter som helst. Vi avstyrker bestämmelsen i sin nuvarande utformning och.

18 § – Det föreslagna myndighetsrådets roll och ansvar, inklusive legala status, behöver förtydligas. Baserat på nuvarande beskrivning är vi tveksamma till inrättandet av detta råd. Exempelvis är vi tveksamma till rådets tänkta uppgift att utveckla och förvalta krav och skyddsnivåer. Antingen bör rådet ”bara” vara rådgivande till MSB eller så bör rådet knytas närmare till ett ansvar som Regeringskansliet har.

19 och 20 §§ – Utöver MSB:s föreskrivande och tillsynsroll, bör det även föreskrivas att MSB ska lämna stöd.

Avslutningsvis bör förordningen enligt vår uppfattning även förskriva vad andra särskilda myndigheter såsom t ex FRA, FOI, Polismyndigheten och Säkerhetspolisen ska göra för att bidra till att stärka övriga statliga myndigheters informationssäkerhet.

Synpunkter på den föreslagna strategin och åtgärder (bilaga 5, sid 329-336):

Initialt föreslår vi att en ensning sker av strategiförslagens övergripande formuleringar. I vissa fall uttrycker de en målbild av ett uppnått tillstånd (exempelvis ”kommunicerar säkert”) och i vissa fall uttrycker det något som kommer att hända (”blir en tydlig kravställare”) och i vissa fall uttycker de något som ska hända (”Sverige ska vara”). Vi föreslår att strategierna uttrycks som uppnådda tillstånd.

Nr 1 - Styrning och tillsyn av informationssäkerhet i staten stärks

Strategin – Förslag till ny formulering ”Styrning, stöd och tillsyn av informationssäkerhet i staten stärks”.

Åtgärderna – Angående att en nationell styrmodell för informationssäkerhet föreslås etableras är vi tveksamma. Det skulle kunna vara positivt, men förutsatter att det sker fullt ut baserat på och helt i linje med svensk och internationell standard och styrmodell för informationssäkerhet (SS-ISO/IEC-27000-serien), kompletterat med tydliga roller och ansvar mellan involverade aktörer och som även i övrigt hänger ihop inte minst med en ny lag och förordning för Rikets/Sveriges säkerhet. Om avsikten inte är att fullt ut basera den nationella styrmodellen på vedertagen standard är vi avvisande till förslaget. Bland annat på sidorna 241, 244 och 283 framställs internationella standarder som ett sätt att skapa förtroende såväl inom organisation som mellan olika parter. Det kan inte heller vara ekonomiskt försvarbart att Sverige ska ta fram en helt egen nationell modell. Underlättandet av internationell samverkan och med kommersiella aktörera är ytterligare ett starkt argument.

Det som försvårar både införandet och efterlevandet av svensk och internationell standard såväl som en nationell styrmodell är bl.a. avsaknaden av praktiska exempel baserade på erfarenhet av införande. Myndigheter har sedan 2010 haft krav på sig att införa och bedriva ett ledningssystem för informationssäkerhet enligt SS-ISO/IEC 27001 och 27002. Här anser vi att MSB kan ta en större stödjande roll.

Angående det föreslagna myndighetsrådet, se kommentar ovan under 18 §.

Nr 2 - Staten blir en tydlig kravställare

Åtgärderna – Angående att MSB ska få i uppdrag att ta fram skyddsprofiler som anger miniminikrav på säkerhet för vanligt förekommande IT-produkter, anser vi att detta bör utökas även till att omfatta de generella tjänster som myndigheter ofta upphandlar, som i praktiken ofta är minst lika svårt och viktigt.

Nr 3 - Statliga myndigheter kommunicerar säkert

Åtgärderna – Det är önskvärt om det förtydligas i förslaget till strategi (såsom framgår i både sammanfattningen på sid 18 och på sid 246) att det är de myndigheterna som nämns i bilagan till krisberedskapsförordningen (2006:942) som avses.
Om vi uppfattar det rätt utifrån bilaga 4, är det tänkt att man för skyddsvärd information ska använda två separata krypteringsprodukter för att uppnå god säkerhet enligt kombinationsprincipen. Det är i så fall viktigt att detta görs så praktiskt enkelt som möjligt att tillämpa och att stöd för införande finns tillgängligt.

Nr 4 – Samtliga statliga myndigheter rapporterar it-incidenter för att skapa underlag för bättre kunskap och lägesbeskrivningar

Strategin - Se kommentar ovan under 7 §.

Åtgärderna – Vi är i grunden positiva till att införa obligatorisk incidentrapportering, men tidigare ambitioner om att införa detta har inte förverkligats och det beror helt på hur det införs vilket behöver beskrivas mycket mera tydligt. Det hade varit önskvärt om betänkandet gått djupare in på dessa frågeställningar då det finns flera svåra ”detaljfrågor”. Vi förutsätter att MSB kommande verkställighetsföreskrifter också kommer att tas fram i samråd med berörda aktörer och skickas ut på allmän remiss.

Nr 5 – Förebyggande och bekämpande av it-relaterad brottslighet stärks.

Strategin – Vi är positiva till strategin som sådan, men anser att detaljformuleringen om att Sverige ska skapa nödvändiga förutsättningar för de brottsbekämpande myndigheterna för att ”garantera samma skydd” mot cyberbrottslighet som mot brottslighet i allmänhet, kan misstolkas. Brottsbekämpande myndigheter garanterar inte skydd mot brottslighet inom något område.

Nr 6 – Sverige ska vara en stark internationell partner

Vi har inga synpunkter i denna del.

Synpunkter på Konsekvensanalysen (kap 10, sid 277-284)

Som anges på sid 277 medför utredningens förslag en höjd ambitionsnivå för statens informationssäkerhet, men att åtskilliga av åtgärdsförslagen ändå kan rymmas inom myndigheternas befintliga budget. Vi håller med om att MSB behöver en viss utökad budget och att vissa av förslagen kan rymmas inom myndigheters befintliga budgetar, men anser här att betänkandet trots allt underskattar behovet av ökad resursåtgång. Dessutom anser vi det inte vara relevant eller korrekt att (sid 282) att framhålla att kostnaderna kan antas vara marginella jämfört med de totala verksamhetskostnaderna. Så kan vara fallet men vid behov av omprioritering kan konsekvenserna ändå bli stora.

Nedan följer några exempel på arbetsuppgifter som åtminstone för flera myndigheter kommer att medföra ökade kostnader och ökad resursåtgång.

- Kravet i 7 § i förordningen om att kartlägga sina informationsprocesser.
- Den nya nationella styrmodellen.
- Ökad resursåtgång för att bli en kvalificerad kravställare (enligt sid 212 måste det offentliga lägga mycket mera tid på detta).
- Kravet på säkra och certifierade produkter.
- Anslutning, drift och förvaltning av ny obligatorisk SGSI-anslutning.
- Den nya obligatoriska incidentrapporteringen.

Detta yttrande har beslutats av generaldirektör Katrin Westling efter föredragning av avdelningschef, säkerhetschef och säkerhetsskyddschef Henrik Engström. I den slutliga handläggningen har även informationssäkerhetsansvarig Ingrid Holmström deltagit.

Katrin Westling Palm

Henrik Engström