Datum 2017-06-20
Diarienr 2017-1897
Ert datum 2017-03-22
Er referens FI2017/01289/DF

Avdelningen för utveckling av samhällsskydd
Enheten för systematiskt informationssäkerhetsarbete
Tina Andersson
+46(0)10-240 43 19
tina.andersson@msb.se

Regeringskansliet
Finansdepartementet

103 33 Stockholm

Betänkandet SOU 2017:23 digitalförvaltning.nu

Sammanfattning

Myndigheten för Samhällsskydd och beredskap (MSB) bejakar utredningens förslag om att öka styrningen över digitaliseringen inom offentliga sektorn genom att samla ansvaret för detta hos en myndighet. MSB ser positivt på att informationssäkerhets- och integritetsaspekter lyfts upp i delbetänkandet.

Ett systematiskt informationssäkerhetsarbete är en grundläggande förutsättning för såväl funktionaliteten hos som förtroendet för digitala tjänster. Med hänsyn till påvisade brister på området och deras konsekvenser anser MSB att delbetänkandets förslag till reglering behöver kompletteras på ett sådant sätt att kravställning och uppföljning av informationssäkerhets-aspekterna omhändertas på ett sammanhållet sätt i digitaliseringsarbetet.

Behov av informationssäker digitalisering

Att arbetet med informationssäkerhet kommer att behöva prioriteras högt i digitaliseringsutvecklingen följer både av kraven i den nya dataskydds-förordningen och det så kallade NIS-direktivet (Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen). Båda regelverken ska tillämpas från och med maj 2018.

MSB instämmer i utredningens bedömning att de offentliga aktörernas nivå skiljer sig avsevärt åt med avseende på informationssäkerhet. En tydligt reglerad skyldighet för offentliga aktörer att arbeta systematiskt och riskbaserat med informationssäkerhet finns idag bara för statliga myndigheter (MSBFS 2016:1), motsvarande reglering finns inte för kommuner och landsting. MSB, liksom Riksrevisionen, har dock vid flera kartläggningar kunnat konstatera att det finns stora brister hos många aktörer när det gäller informationssäkerhets-arbetet. Sådana brister försvårar arbetet med gemensamma digitaliserings-projekt, utgör hinder för nödvändigt informationsutbyte och minskar förtroendet för hur information skyddas. Ett exempel är när samma typ av information ges olika skydd hos offentliga aktörer. Då det i samverkansprojekt

av denna typ räcker med att enbart *en* brist hos *en* deltagande aktör orsakar ett problem, riskeras tilliten och förtroendet hos allmänheten för offentliga e-tjänster men kanske också offentlig sektor i stort. Det är inte tillräckligt att den enstaka e-tjänsten uppvisar en tillräcklig nivå av säkerhet om den aktör som tillhandahåller e-tjänsten brister i sitt systematiska informationssäkerhets-arbete. MSB vill också påpeka att e-tjänster är beroende av en robust och tillgänglig infrastruktur som "bärarnät" för tjänsterna.

Samhällsviktiga leverantörer av e-förvaltningstjänster måste kunna genomföra sina uppdrag, både i normalläge och i krisläge. Detta förutsätter systematiskt informationssäkerhetsarbete inklusive väl utvecklade metoder för kontinuitetsplanering. Ett samordnat säkerhetsarbete mellan deltagande aktörer och myndigheten med det samlade ansvaret ses som centralt. I detta arbete bör tyngdpunkten ligga på ledning, styrning och analys. En tydlig styrning ger också underlag för att välja rätt tekniska åtgärder.

Med hänsyn till att brister i informationssäkerheten hos de deltagande aktörerna, brister i informationssäkerheten för e-tjänster, liksom bristande förståelse för vikten av systematiskt informationssäkerhetsarbete, kan få allvarliga konsekvenser ser MSB ett behov av

- en informationssäkerhetsgranskning av den föreslagna e-tjänsten Mina Meddelanden, vilken utförs av en oberoende tredje part,
- en sammanställning av vilka informationssäkerhetsrisker som behöver elimineras eller reduceras för att en e-tjänst ska kunna anses ha tillräcklig informationssäkerhet,
- en analys av förutsättningarna för certifiering av e-tjänster ur ett informationssäkerhetsperspektiv,
- en kartläggning av aktörernas mognadsnivå avseende informationssäkerhetsarbete, inklusive analys av möjligheten att införa krav på miniminivå för informationssäkerhetsmognad för att erbjuda e-tjänster, samt
- en analys av möjligheterna till en tydligare styrning av informationssäkerhetsarbetet, inklusive en gemensam och enhetlig informationsklassning av de informationstillgångar som hanteras i de gemensamma e-tjänsterna.

Vidare ser MSB ett behov av att det ytterligare tydliggörs hur samarbetet mellan myndigheten med det samlade ansvaret och Datainspektionen, Post- och telestyrelsen samt MSB rörande digitalisering av offentlig förvaltning, personlig integritet och informationssäkerhet ska utformas utifrån myndigheternas mandat.

Uppföljning och mätning

Delbetänkandet belyser vikten av att den myndighet som har det samlade ansvaret för digitaliseringen ska mäta och följa upp digitaliseringens framskridande hos de olika aktörerna. Att dessa aktörer ställs inför krav på att snabbt visa resultat i form av ökad digitalisering i den offentliga förvaltningen kan enligt MSB:s bedömning medföra risker. Det kan resultera i att informationssäkerhetskraven, som anses öka kostnaderna, komplexiteten och användarvänligheten, nedprioriteras, vilket i sin tur kan resultera i säkerhetsbrister.

MSB ser det som angeläget att den myndighet som tilldelas det samlade ansvaret även får ett tydligt uppdrag att granska och följa upp informationssäkerhetsrelaterade aspekter och att mäta nyckeltal för området. Detta skulle exempelvis kunna uppnås genom en tydlig koppling mellan processen för intern styrning och kontroll och det systematiska informationssäkerhetsarbetet. Myndigheten skulle också i sin instruktion kunna få i uppdrag att stödja andra myndigheter i frågor om kravställning på informationssäkerhet vid utveckling av nationella digitala tjänster.

MSB anser att de nyckeltal som myndigheten med det samlade ansvaret ska följa upp ska omfatta informationssäkerhetsaspekter.

Övriga synpunkter

Delbetänkandet berör frågor rörande e-legitimation översiktligt, bland annat vikten av att säkerställa enskildas tillgång till e-legitimation. Utredaren avser att återkomma till ämnet i slutbetänkandet. MSB vill redan nu poängtera vikten av detta samt att analysera huruvida ett behov finns av e-legitimation för statsanställda. Detta ligger längre fram i utvecklingen av digitaliseringen, exempelvis när ett beslutsfattande kan ske digitalt.

I vissa passager omnämns informationsutbyte mellan deltagande aktörer, dvs. att myndigheter ska kunna utbyta information med varandra. I det fall utredaren avser att utveckla detta i slutbetänkandet så vill MSB betona att ytterligare, och allvarligare, informationssäkerhetsaspekter i dessa fall tillkommer som ställer högre krav på såväl e-tjänster som deltagande aktörer. Detta då informationen som sänds från en myndighet till en annan behöver ha samma skydd hos både sändare och mottagare samt att det måste säkerställas att mottagaren har den mognadsnivå i sin informationssäkerhetshantering som krävs för att sändaren ska vara säker på att informationen hanteras på rätt sätt.

I detta ärende har chefsjuristen Key Hedström beslutat. Tina Andersson har varit föredragande. I den slutliga handläggningen har också biträdande avdelningschefen Camilla Asp och verksamhetschefen Richard Oehme deltagit.

Key Hedström

Tina Andersson

Kopia: Ju/SSK