



CS-ST
Andreas Häll
010-240 42 13
andreas.hall@msb.se

Konsekvensutredning rörande föreskrifter om statliga myndigheters rapportering av it-incidenter

Allmänt

Beskrivning av problemet och vad man vill uppnå

Regeringen har genom förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap infört regler om it-incidentrapportering för statliga myndigheter. Kravet började gälla den 1 april 2016. Den 4 april 2016 trädde MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2) i kraft.

MSB bedömer att det är för få myndigheter som rapporterar it-incidenter och att antalet rapporterade incidenter borde vara fler.

En möjlig orsak till detta är att myndigheterna gör olika bedömningar av vilka incidenter som är rapporteringspliktiga. Föreskrifterna uppdateras därför med en tydligare beskrivning av vad som utgör en rapporteringspliktig incident.

I de nya föreskrifterna används begreppen "utökad och hög skyddsnivå". Dessa begrepp är hämtade från den informationsklassningsmodell som finns på informationssäkerhet.se. Begreppen används för att illustrera vilka konsekvenser som en it-incident behöver få för att bli rapporteringspliktig. Användningen av begreppen ska inte förstås som att en myndighet behöver använda sig av just dessa begrepp i sin informationsklassningsmodell.

I de nya föreskrifterna delas incidentrapporteringen upp i två steg där den första rapporteringen ska ske inom sex timmar från det att myndigheten identifierat it-incidenten som rapporteringspliktig. Detta ger MSB en ökad möjlighet att ge stöd vid den operativa hanteringen av incidenten. Det ger också MSB ökad möjlighet att varna vid större händelser.

Beskrivning av alternativa lösningar för det man vill uppnå och vilka effekterna blir om någon reglering inte kommer till stånd

Ett system för it-incidentrapportering ska kunna användas för att varna andra och därigenom minska konsekvenser av inträffade incidenter, utgöra underlag för analyser och en samlad lägesbild över tid när det gäller samhällets

informationssäkerhet. För att systemet ska kunna användas på avsett sätt behövs därför en tydlig struktur som klargör vad som ska rapporteras, när och hur. Det är således centralt att detta tydliggörs på föreskriftsnivå.

Uppgifter om vilka som berörs av regleringen

Författningen berör endast de statliga myndigheter som omfattas av förordningskravet på it-incidentrapportering.

Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Regeringen har genom 21 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap gett MSB mandat att meddela de ytterligare föreskrifter som behövs för verkställigheten av 20 § första stycket om rapportering av it-incidenter.

Uppgifter om vilka kostnadmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen

Rapportering av it-incidenter är redan idag ett krav som följer av MSB:s föreskrifter MSBFS 2016:2 med tillhörande allmänna råd. MSB:s förtydligande av vilka it-incidenter som ska rapporteras kan leda till att fler incidenter kommer att rapporteras. Eventuella merkostnader bedöms dock bli förhållandevis låga eftersom rapportering av it-incidenter redan är ett krav idag och det får förutsättas att samtliga myndigheter redan har arbetsprocesser för rapportering av incidenter.

Föreskriftskravet att den första rapporteringen ska göras inom sex timmar behöver också belysas vid ett resonemang om kostnader och konsekvenser. Regleringen ska inte tolkas som krav på ökad bemanning utan tidsfristen på sex timmar räknas från den tidpunkt då myndigheten med stöd av sina egna rutiner identifierat incidenten som rapporteringspliktig. Vidare är den mängd information som ska lämnas inom sex timmar samt anvisade kontaktvägar anpassade efter skyndsamhetskravet. Enligt MSB:s bedömning kommer därför inte heller detta krav föranleda att myndigheterna drabbas av ökade kostnader i någon större utsträckning.

Bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen

Föreskrifterna om statliga myndigheters rapportering av it-incidentrapportering är nationella och bedöms inte påverka de skyldigheter som följer av Sveriges anslutning till Europeiska unionen.

Bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser

Det är redan ett krav idag att myndigheter ska rapportera it-incidenter. Detta innebär att det inte finns något behov av övergångsbestämmelser.

Ikraftträdandet av denna reglering förutsätter en särskild informationsinsats av MSB. Det är nödvändigt att presentera exempel på vad som ska rapporteras och hur det ska gå till, hur informationen hanteras hos MSB samt hur återkoppling av information ska ske och till vilka intressenter. Behovet av särskilda utbildningsinsatser och ytterligare informationsspridning kommer att bedömas löpande.

Företag

Föreskrifterna gäller endast statliga myndigheter.

Kommuner och landsting

Föreskrifterna gäller endast statliga myndigheter.

Kontaktpersoner

Ange vem som kan kontaktas vid eventuella frågor

Kontaktperson vid frågor om konsekvensutredningen och de nya föreskrifterna om krav på statliga myndigheters rapportering av it-incidenter är Andreas Häll som lämpligast nås på andreas.hall@msb.se eller 010- 240 42 13 eller Helena Andersson som nås på helena.andersson@msb.se eller 010-240 41 33.