Ingela Darhammar Hellström

Avdelningen för risk- och sårbarhetsreducerande arbete
Verksamheten för samhällets informations- och cybersäkerhet
072-233 62 81

Konsekvensutredning rörande föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter

A. Allmänt

Beskrivning av problemet och vad man vill uppnå

Under det senaste årtiondet har inte bara användningen av informationsteknik i samhället ökat, utan även sårbarheten med avseende på detta. I dag har samhället inte förmåga att vare sig identifiera eller hantera allvarliga it-incidenter på ett systematiskt sätt och vi vet inte heller vad de grundar sig i eller vilken påverkan de har på enskilda användare, samhällsviktiga verksamheter eller samhällets säkerhet i stort. Många incidenter upptäcks aldrig. När en organisation har drabbats kan det ta flera dagar innan andra aktörer får kunskap om incidenten och kan agera, om de alls får veta att den inträffat. Bristen på information och en rättvisande lägesbild kan få långtgående konsekvenser för både statliga myndigheter och andra aktörer och försvårar det systematiska arbetet med samhällets informationssäkerhet. Det gör det svårt för beslutsfattare att förstå den totala effekten och eventuella beroendeförhållanden.

I betänkandet SOU 2015:23 Informations- och cybersäkerhet i Sverige föreslås att krav på it-incidentrapportering införs rörande it-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten levererar till en annan organisation. It-incidenterna föreslås rapporteras till MSB med undantag för it-incidenter med koppling till informationssystem där hemliga uppgifter behandlas. Dessa ska enligt utredarens förslag istället rapporteras till den myndighet som har tillsyn över säkerhetsskyddet enligt 39 § säkerhetsskydds-förordningen (1996:633), det vill säga Försvarsmakten eller Säkerhetspolisen.

Regeringen har genom förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (2015:xxx) infört regler om obligatorisk it-incidentrapportering för statliga myndigheter. Kravet börjar gälla den 1 april 2016. Det kommer att innebära att statens övergripande ansvar för informationssäkerhet i samhället görs tydligare, bland annat genom att det bidrar till att upprätthålla en korrekt omvärldsbevakning och lägesbild över området.

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

I takt med att beroendet av fungerande it-system och it-infrastruktur för både individ och samhälle har ökat har flera åtgärder vidtagits för att förbättra lägesbilden över inträffade it-incidenter i samhället främst genom att ge aktörer både inom den offentliga och privata sektorn en möjlighet att frivilligt rapportera it-incidenter till en nationell funktion.

Trots dessa insatser bedöms mörkertalet fortfarande vara stort vad gäller inträffade it-incidenter.[1] En kvarvarande utmaning är låg rapporterings-benägenhet när denna sker på frivillig basis. Problematiken finns inte bara nationellt utan även på EU-nivå där arbete pågår med att införa krav på obligatorisk it-incidentrapportering för aktörer inom en rad olika sektorer.

Ju fler som rapporterar in desto effektivare kan stödet för samhällets informationssäkerhet bli. Rapporteringen ger nämligen möjlighet att snabbt varna andra som kan vidta förebyggande åtgärder och på det sättet kan både konsekvenser och antalet drabbade aktörer begränsas. Genom rapporteringen kan dessutom ett empiriskt och statistiskt fastställt underlag skapas och som därigenom ger en samlad lägesbild över it-incidenterna i samhället. Detta ger ökad möjlighet att återkoppla med relevant information och stöd till berörda aktörer, inrikta förebyggande insatser, dra lärdom av it-incidenterna samt minska mörkertalet.

När det finns en skyldighet på förordningsnivå att rapportera men det inte i verkställighetsföreskrifter närmare har specificerats exakt hur rapporten ska utformas kan jämförbarheten påverkas negativt. Genom att enhetlig inrapportering saknas finns stora risker för att jämförbarheten mellan it-incidentrapporter förloras och att eventuella kopplingar mellan it-incidenter förbises på grund av brist på information.

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. Föreskrifterna bör kompletteras med allmänna råd.

Uppgifter om vilka som berörs av regleringen

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

---

[1] Efter jämförelser med norska mörkertalsundersökningar. Se 2014 Mørketallsundersøkelsen Informasjonssikkerhet, personvern og datakriminalitet (http://www.nsr-org.no/moerketall/).

Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Regeringen har genom förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (2015:xxx) gett MSB mandat att utfärda verkställighetsföreskrifter rörande obligatorisk it-incidentrapportering för statliga myndigheter.

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

Intern incidentrapportering är redan idag ett krav som följer av MSB:s föreskrifter MSBFS 2009:10 med tillhörande allmänna råd.

Nu gäller därför som första steg att hitta former för att anpassa befintliga arbetsprocesser och rutiner för att även uppfylla kraven på it-incidentrapportering till MSB. Vissa kostnader kan därmed uppstå, liksom kostnader vid eventuell anpassning av processer och rutiner för att underlätta användning av MSB:s tekniska gränssnitt för it-incidentrapportering. Dessa merkostnader bedöms bli förhållandevis låga. Särskilt då det inte är alla incidenter som ska rapporteras utan endast de som allvarligt kan påverka säkerheten hos myndigheten. Antalet it-incidenter som ska rapporteras till MSB jämfört med antalet internt rapporterade incidenter torde också bli förhållandevis lågt. MSB bedömer därför att myndigheternas merkostnader för att anpassa sina praktiska arbetsprocesser är begränsade.

För de myndigheter som utkontrakterar sin informationsbehandling kan det uppstå vissa initiala kostnader i samband med att rutiner och processer behöver modifieras. Enligt de föreslagna föreskriftkraven ska myndigheten då säkerställa att it-incidenter kan rapporteras och att kompletterande uppgifter kan lämnas som om myndigheten utfört behandlingarna själv. Något krav på omförhandling av redan ingångna utkontrakteringsavtal ställs dock inte. Vid nya avtal behöver dock kravet på it-incidentrapportering beaktas.

Föreskriftskravet att en rapport ska skickas inom 24 timmar efter att myndigheten upptäckt it-incidenten behöver också belysas vid ett resonemang om kostnader och konsekvenser. Regleringen ska inte tolkas som krav på ökad bemanning utan tidsfristen på 24 timmar räknas från den tidpunkt då myndigheten med stöd av sina egna interna processer och rutiner upptäcker incidenten. Vidare är den mängd information som ska lämnas inom 24 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 obligatorisk it-incidentrapportering är nationella. Inom EU pågår ett arbete med det så kallade NIS-direktivet. Direktivet innehåller bland annat krav på it-incidentrapportering. Ett införande av obligatorisk it-incidentrapportering för statliga myndigheter bedöms enligt MSB vara en viktig förberedelse för att kunna hantera de krav som föreslås i NIS-direktivet.

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

MSB gör bedömningen att det är av vikt att föreskrifterna som närmare reglerar vad, när och hur it-incidenter ska rapporteras träder i kraft i anslutning till den tidpunkt som obligatoriet införs på förordningsnivå. Detta för att det redan från början ska vara tydligt för de statliga myndigheterna vad som ska rapporteras och hur. MSB kommer dock att säkerställa att inrapporteringsförfarandet görs så enkelt som möjligt för berörda myndigheter vilket innebär att några anpassningar av arbetssätt och tekniska gränssnitt hos myndigheterna inte ska vara en förutsättning för att rapporter ska kunna lämnas in. Detta innebär i förlängningen att det inte torde finnas något behov av övergångsbestämmelser. Föreskrifterna kan därför börja gälla i sin helhet när de träder ikraft.

Ikraftträdandet av denna reglering förutsätter en särskild informationsinsats av MSB. Samtliga frågor, om exempelvis vad som ska rapporteras, kommer inte att kunna besvaras genom reglering. Därutöver gör MSB bedömningen att 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 utbildnings-insatser och ytterligare informationsspridning kommer att bedömas löpande. En lämpligt utformad informationsinsats kan på ett effektivt sätt bidra till att beskriva syftet med rapporteringen och vikten av att både kunna begränsa konsekvenser och spridning av allvarliga it-incidenter samt bygga upp en samlad lägesbild när det gäller samhällets informationssäkerhet.

B. Kommuner och landsting

Markera med x

(x) Regleringen bedöms inte få effekter för kommuner eller landsting.

( ) Regleringen bedöms få effekter för kommuner eller landsting.

Beskrivning av effekter för kommuner eller landsting

Föreskrifterna gäller endast statliga myndigheter. Kommuner och landsting har möjlighet att rapportera på samma sätt även om det inte finns sådan skyldighet idag.

C. Företag

Markera med x

(x) Regleringen bedöms inte få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Konsekvensutredningen innehåller därför inte någon beskrivning av punkterna i avsnitt C.

( ) Regleringen bedöms få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Konsekvensutredningen innehåller därför en beskrivning av punkterna i avsnitt C.

Föreskrifterna gäller endast statliga myndigheter. MSB ser det som positivt att företag rapporterar på samma sätt även om det inte finns någon sådan skyldighet idag.

D. Samråd

Beskrivning av ett eventuellt tidigt samråd

MSB fick av regeringen i uppdrag, Fö2012/717/SSK, att 2012 presentera ett förslag på ett system för it-incidentrapportering för statliga myndigheter, Nationellt system för it-incidentrapportering dnr 2012-2637. Vid utformningen av denna uppdragsredovisning (vilken även inkluderade föreskriftsförslag) inrättade MSB två olika externa grupper som stöd för arbetet; en arbetsgrupp bestående av representanter för MSB, Säkerhetspolisen och dåvarande Rikskriminalpolisen, samt en bredare referensgrupp till vilken samtliga av regeringen för uppdragsarbetet utpekade aktörer bjöds in. Uppdragsredovisningens föreskriftsförslag ligger till grund för det nu framtagna förslaget till föreskrifter.

E. 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 Ingela Darhammar Hellström som lämpligast nås på ingela.d.hellstrom@msb.se, 010-240 42 68 alternativt 072-233 62 81 eller Helena Andersson som nås på helena.andersson@msb.se, 010-240 41 33 eller 073-025 11 33.