Myndigheten för samhällsskydd och beredskaps författningssamling

Utgivare: Key Hedström, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

MSBFS 2016:2
Utkom från trycket den 11 mars 2016

Myndigheten för samhällsskydd och beredskaps föreskrifter[1] om statliga myndigheters rapportering av it-incidenter;

beslutade den 1 mars 2016.

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 21 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Inledande bestämmelse

1 § Denna författning innehåller föreskrifter om hur statliga myndigheter till Myndigheten för samhällsskydd och beredskap ska rapportera it-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten levererar till en annan organisation, enligt 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Kontaktuppgifter

2 § Varje myndighet ska meddela aktuella kontaktuppgifter för den funktion vid myndigheten som ska ta emot information om it-incidenter från Myndigheten för samhällsskydd och beredskap.

Rapporteringspliktiga it-incidenter

3 § I 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap finns grundläggande bestämmelser om vilka it-incidenter som ska rapporteras till Myndigheten för samhällsskydd och beredskap.

[1] Allmänna råd som ansluter till föreskrifterna finns på sid 5.

De rapporteringspliktiga it-incidenterna kan utgöras av kategorierna

1. störning i mjuk- eller hårdvara,
2. störning i driftmiljö,
3. informationsförlust eller informationsläckage,
4. informationsförvanskning,
5. hindrad tillgång till information,
6. säkerhetsbrist i en produkt,
7. angrepp,
8. handhavandefel,
9. oönskad eller oplanerad störning i kritisk infrastruktur, eller
10. annan plötslig oförutsedd händelse som lett till skada.

När rapportering ska ske

4 § Varje myndighet ska rapportera en it-incident senast 24 timmar efter det att myndigheten upptäckt den rapporteringspliktiga incidenten.

Hur rapportering ska ske

5 § Rapporterna ska lämnas till Myndigheten för samhällsskydd och beredskap via anvisade kontaktvägar.

6 § En rapport ska innehålla

1. myndighetens namn,
2. en beskrivning av it-incidenten som även inkluderar en övergripande redovisning av händelseförlopp och vidtagna åtgärder,
3. den exakta eller uppskattade tidpunkten för när it-incidenten inträffade,
4. när myndigheten upptäckte it-incidenten och om den alltjämt pågår eller är avslutad,
5. till vilken eller vilka kategorier enligt 3 § som it-incidenten hör, samt
6. myndighetens initiala bedömning av it-incidentens omfattning och konsekvenser, både faktiska och potentiella.

I rapporten ska om möjligt även anges bedömd sekretess för den information som rapporteras in.

Om den rapporterande myndigheten vid sin interna incidentutredning konstaterar att inrapporterade uppgifter om kategorier, omfattning och konsekvenser varit missvisande eller felaktiga ska myndigheten komplettera eller korrigera sin rapport så snart som möjligt.

7 § På begäran av Myndigheten för samhällsskydd och beredskap ska en rapporterande myndighet lämna uppgifter som kompletterar rapporteringen enligt 6 §.

Sådana uppgifter ska lämnas snarast, om inget annat överenskommits med Myndigheten för samhällsskydd och beredskap.

8 § En myndighet som inte kan lämna en rapport enligt 6 § får i samråd med Myndigheten för samhällsskydd och beredskap lämna en preliminär rapport. Samråd ska ske innan tidsfristen för rapportering enligt 4 § går ut. Rapporten ska innehålla den information som finns att tillgå vid inrapporteringstillfället samt när myndigheten upptäckte it-incidenten, om den fortfarande pågår eller är avslutad, samt vilken eller vilka kategorier i 3 § som orsakat incidenten.

Den fullständiga rapporten enligt 6 § ska i ett sådant fall lämnas senast två veckor från det att it-incidenten upptäcktes.

Utkontraktering

9 § Om en myndighet överlåter en del av sin informationshantering till en icke statlig aktör ska myndigheten i överlåtelseavtalet se till att motparten åtar sig att rapportera it-incidenter i berörda system till myndigheten på ett sätt som motsvarar kraven enligt denna författning. Myndigheten ska utan dröjsmål vidarebefordra en sådan rapport till Myndigheten för samhällsskydd och beredskap.

Skyldigheten enligt första stycket gäller med avseende på avtal som träffas efter denna författnings ikraftträdande.

Polisanmälda it-incidenter

10 § I det fall en myndighet har polisanmält en it-incident behöver myndigheten inte lämna en rapport enligt 6 § utan endast en kopia på polisanmälan.

Denna författning träder i kraft den 4 april 2016.

Myndigheten för samhällsskydd och beredskap

HELENA LINDBERG

Ingela Darhammar Hellström
(Avdelningen för utveckling av samhällsskydd)

Myndigheten för samhällsskydd och beredskaps allmänna råd om statliga myndigheters rapportering av it-incidenter

Dessa allmänna råd ansluter till Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters rapportering av it-incidenter. Termer och uttryck som används i föreskrifterna används med samma betydelse i dessa allmänna råd.

Allmänna råd har en annan juridisk status än föreskrifter. Allmänna råd är inte tvingande. Deras funktion är att förtydliga innebörden i lag, förordning eller myndighetsföreskrifter och att ge generella rekommendationer om deras tillämpning.

Allmänna råd är markerade med grå bakgrund.

Myndigheten för samhällsskydd och beredskap

CECILIA NYSTRÖM

Ingela Darhammar Hellström
(Avdelningen för utveckling av samhällsskydd)

Författningens syfte och tillämpningsområde (1-2 §§)

Bakgrund

Föreskrifterna om it-incidentrapportering syftar till att skapa en systematisk, bred och samlad rapportering av allvarliga it-incidenter. Rapporteringen ökar möjligheten att hantera och begränsa konsekvenserna av sådana it-incidenter och på det sättet bidra till att öka samhällets informationssäkerhet.

It-incidenthantering

Varje myndighet ansvarar för att ta fram de processer och rutiner som myndigheten behöver för att kunna uppfylla kraven på it-incidentrapportering enligt denna författning.

Av Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) framgår vilka krav som ställs på en myndighet. Myndigheten ska ha interna rutiner för att identifiera, rapportera, bedöma, hantera och dokumentera incidenter som kan påverka säkerheten i den informationshantering som myndigheten svarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Myndigheten ska även ha processer för att lära av sådana inträffade incidenter och utförda åtgärder.

It-incident

Begreppet ”it” (informationsteknik) bör tolkas som teknik för insamling, lagring, bearbetning, produktion, återfinnande, utplåning samt kommunikation och presentation av information (data, text, ljud, bild).

Med ”it-incident” bör förstås en oönskad och oplanerad it-relaterad händelse som kan påverka säkerheten i organisationens eller samhällets informationshantering och som kan innebära en störning i organisationens förmåga att bedriva sin verksamhet.

Begreppet it-incident rymmer både tekniskt orienterade säkerhetsincidenter och informationssäkerhetsaspekter. Definitionen harmonierar med svenska och internationella standarder inom ISO/IEC 27000-serien och de begrepp som används internationellt.

En it-incident kan således vara en händelse som påverkar eller stör data, telekommunikation, hård- eller mjukvara. Orsaken kan vara bristande kompetens, mänskliga misstag, tekniska sammanbrott eller naturhändelser.

Kontaktuppgifter

Kontaktuppgifter för den funktion vid myndigheten som ska ta emot information med koppling till it-incidenter bör inkludera telefonnummer, e-postadresser och postadress samt uppgift om bemanning.

Eventuella sekretessbelagda uppgifter som lämnas till MSB hanteras enligt gällande bestämmelser.

Rapporteringspliktig it-incident (3 §)

Varje myndighet gör en självständig bedömning av vilka it-incidenter som omfattas av rapporteringsskyldigheten i 20 §. Det har blivit allt vanligare att myndigheter, parallellt med att kommersiella it-relaterade tjänster upphandlas, även samverkar sinsemellan och med kommuner kring olika typer av it-relaterade lösningar. Sådana samarbeten kan till exempel vara gemensamma system, gemensamma driftmiljöer, gemensamma kommunikationslösningar eller molntjänster. Störningar i denna typ av lösningar kan leda till att verksamhet hos ett flertal myndigheter och i förlängningen samhället påverkas negativt. Det är därför viktigt att it-incidenter som allvarligt påverkar säkerheten rapporteras.

För bedömning av allvarlighetsgraden hos en it-incident kan myndigheten ta del av information som tillhandahålls på Myndigheten för samhällsskydd och beredskaps webbplats www.cert.se.

Som ledning för den bedömning som en rapporterande myndighet ska göra avseende vilken eller vilka kategorier en it-incident hänför sig till kan följande exempel och beskrivningar användas.

Störning i mjuk- och hårdvara

Kan exempelvis innefatta fel i system, komponent eller programvara samt oväntad funktion i system eller komponent eller systemkrasch.

Störning i driftmiljö

Kan exempelvis bestå i haveri i tekniskt system eller komponent, eller förlust av tillgänglighet i system. Hit räknas även störningar i system med säkerhetsfunktioner, exempelvis säkerhetskopiering.

Informationsförlust eller informationsläckage

Tillgänglighetsförluster kan vara permanenta eller temporära. Exempelvis är en informationsförlust orsakad av brand i serverhall ofta permanent, medan systemfel eller en omfattande överbelastningsattack kan leda till temporär tillgänglighetsförlust. Kategorin förlust av tillgänglighet till, eller läckage av

information i myndighetens informationssystem, kan inkludera felaktig avyttring av teknisk utrustning som innehåller information som inte ska vara allmänt tillgänglig, eller otillåtet offentliggörande av sådan information. Informationsläckage innebär att myndighetens information inte gått förlorad men att någon på obehörigt sätt skaffat sig tillgång till den.

Vid informationsläckage kan det vara svårt att bedöma hur stor spridning informationen fått eller om läckaget inneburit att den aktör som skaffat sig tillgång till informationen behållit den för eget bruk.

Osäkerhet om hur stor spridning informationen fått bör beaktas vid bedömning av hur allvarlig incidenten är.

Informationsförvanskning eller hindrad tillgång till information

Förvanskning av information kan leda till att informationen helt eller delvis har blivit korrumperad eller att det inte går att säkerställa dess riktighet.

Hindrad tillgång till information kan exempelvis innebära att informationen eller ett system där informationen finns inte kan användas på avsett sätt.

Säkerhetsbrist i en produkt

Kategorin kan exempelvis innefatta it-incidenter orsakade av säkerhets-luckor eller annan sårbarhet i tekniskt hjälpmedel som används av myndigheten.

Angrepp

I ett initialt skede kan det vara svårt att avgöra varifrån ett angrepp kommer eller om det faktiskt rör sig om ett angrepp. Till kategorin räknas exempelvis överbelastningsattack, införande av skadlig kod, intrång i informationssystem (s.k. hackning), olovligt nyttjande eller annat missbruk av lösenord, olovlig åtkomst till information genom skadliga program och obehörig användning av informationssystem.

Som angrepp räknas även angrepp som möjliggjorts eller genomförts av egen personal eller personer som på motsvarande sätt har en anknytning till den drabbade myndigheten, exempelvis inhyrd personal.

Handhavandefel

Kategorin omfattar exempelvis it-incidenter som orsakas av internt felaktigt bruk eller felaktig implementering av tekniskt system eller komponent.

Oönskad eller oplanerad störning i kritisk infrastruktur

Funktionen hos myndighetens informationssystem är ofta starkt beroende av tillgång till extern försörjning av el och kommunikationstjänster, men även

interna system för att trygga funktionen i kritisk infrastruktur. Till kategorin bör därför räknas it-incidenter som orsakas av exempelvis elektriskt fel, vattenskada eller störning i funktioner för avbrottsfri kraftförsörjning, kylning eller ventilation.

Annan plötslig oförutsedd händelse som lett till skada

Till kategorin kan räknas it-incidenter som orsakats av annan händelse än de som omfattas av kategorierna som nämnts ovan men som av rapporterande myndighet inte bedöms kunna sorteras in i någon av dessa kategorier.

Rapportering av it-incidenter (4-10 §§)

Tidsram

I och med att myndigheterna ska rapportera it-incidenten senast 24 timmar från upptäckt får Myndigheten för samhällsskydd och beredskap på ett tidigt stadium indikationer på om till exempel flera myndigheter eller organisationer samtidigt drabbats. Sådana incidenter kan kräva omedelbara åtgärder av fler aktörer än den rapporterande myndigheten. Fler aktörer än de som direkt är berörda kan på så sätt få en tidig information och varning. Detta innebär en möjlighet att begränsa konsekvenserna och spridningen av en inträffad it-incident.

Myndigheten anses ha upptäckt it-incidenten när information om den hanteras i utpekad intern process för hantering av it-incidenter eller när säkerhetsansvarig eller motsvarande fått kännedom om incidenten.

Anvisade kontaktvägar

Myndigheten för samhällsskydd och beredskap anvisar ett tekniskt gränssnitt för inrapportering av it-incidenter, samt tillhandahåller den information som behövs för att använda gränssnittet.

Av olika skäl kan det finnas behov av att använda alternativa av MSB anvisade kontaktvägar såsom kommunikation för e-post eller telefon.

Information om anvisade kontaktvägar för obligatorisk it-incident-rapportering finns på Myndigheten för samhällsskydd och beredskaps webbplats www.cert.se där information av betydelse för it-incidenthantering publiceras.

Rapport om en it-incident

En rapport enligt 6 § bör inte innehålla personuppgifter.

Konsekvenser bör beskrivas med stöd av den kategorisering som Myndigheten för samhällsskydd och beredskap tillhandahåller.

Kompletterande uppgifter

Om det finns misstankar om att de it-incidenter som har rapporterats kan få snabb spridning eller omfattande konsekvenser för samhället kan en fördjupad analys behövas. På begäran av Myndigheten för samhällsskydd och beredskap ska den rapporterande myndigheten lämna kompletterande uppgifter till rapporteringen enligt 6 §. Kompletterande uppgifter kan också komma att begäras in för att avgöra om it-incidenter som olika myndigheter har rapporterat in har något samband med varandra eller om de exempelvis har orsakats av samma säkerhetsbrist i en produkt. Syftet med kompletteringen är att bidra i arbetet med att begränsa skadan och förebygga att liknande it-incidenter inträffar i samhället.

Vilken information som den rapporterande myndigheten bör komplettera med och hur den ska hanteras avgörs i samråd med Myndigheten för samhällsskydd och beredskap. Information om hur de kompletterande uppgifterna och övrig information hanteras hos Myndigheten för samhällsskydd och beredskap finns på www.cert.se.

Om personuppgifter lämnas till Myndigheten för samhällsskydd och beredskap vid en begäran enligt 7 § ska behandlingen vid behov regleras genom särskild överenskommelse.

Preliminär rapport

En preliminär rapport bör endast lämnas i undantagsfall.

Beställningsadress:
Wolters Kluwers kundservice, 106 47 Stockholm
Telefon: 08-598 191 90, www.wolterskluwer.se
E-post: kundservice@wolterskluwer.se