



Vägledning om rapportering av incidenter

Bedömningsverktyg

Innehållsförteckning



<i>Syfte.....</i>	<i>1</i>
<i>Vem ska rapportera?.....</i>	<i>2</i>
<i>Hur ska rapportering ske?.....</i>	<i>3</i>
<i>När ska rapportering ske?.....</i>	<i>4</i>
<i>Vad ska rapporteras?.....</i>	<i>5</i>
<i>Rapporteringspliktiga incidenter.....</i>	<i>7</i>



Nätverks- och informationssystem är av högsta betydelse för samhället, och dess säkerhet är därför en central del för ekonomisk och samhällelig stabilitet.

Incidentrapportering stärker förmågan att förebygga och hantera incidenter, för att kunna skydda både leverantörer av samhällsviktiga tjänster och samhället i helhet. När en incident inträffar, sker rapporteringen redan i ett tidigt skede och MSB kan därför medverka operativt i hanteringen och ge stöd till de som drabbats tillsammans med berörda aktörer. Incidentrapporterna delas sedan snabbt med tillsynsmyndigheter, som använder dem i sitt tillsynsarbete. Deras granskning omfattar bland annat vilka incidenter som rapporteras, hur rapporteringen organiseras och när den sker.

Det är viktigt att förstå syftet med incidentrapportering, och huruvida de fungerar i praktiken för att få en djupare förståelse för hur man som organisation kan applicera dem till verksamheten.

1. Vem ska rapportera?



Den som identifierar sig som en leverantör av en samhällsviktig tjänst måste rapportera incidenter, oavsett var de inträffar. Det vill säga, även om driften av nätverk och informationssystem är utlagd på en extern aktör och en incident påverkar tjänsten, är det fortfarande leverantörens ansvar att rapportera den.

För att säkerställa snabb information om incidenter bör leverantören ha tydliga avtal med sina externa samarbetspartners. Det är möjligt att låta den externa aktören rapportera direkt till MSB, men det övergripande ansvaret för rapporteringen *ligger alltid hos leverantören*. Den givna tillsynsmyndigheten granskar senare hur rapporteringen sker.

2. Hur ska rapportering ske?



Leverantörer av samhällsviktiga tjänster ska rapportera incidenter via anvisade kontaktvägar - det vill säga till MSB. Incidenter rapporteras främst via MSB:s incidentrapporteringsverktyg, vilket ni finner via länken;

Incidentrapporteringsverktyg

För att använda verktyget måste de personer som rapporterar ha ett aktivt incidentrapporteringskonto, vilket skapas genom formuläret i länken;

Skapa konto för incidentrapportering

Information om hur kontot aktiveras och hur rapporteringen går till finns att se på msb.se. Verktöget innehåller ett formulär med frågor som följer föreskrifterna och ska besvaras av leverantören.

Formuläret kan laddas ner från msb.se (se länk ovan för incidentrapporteringsverktyg) för att underlätta förberedelser. Om rapporten innehåller uppgifter som rör Sveriges säkerhet och omfattas av sekretess ska dessa inte rapporteras i verktyget, utan dessa hanteras enligt särskilda riktlinjer. Ni hittar mer information om hur dessa rapporteras via länken ovan.

3. När ska rapportering ske?



Den första incidentrapporten (Skede 1) ska skickas inom **sex timmar** efter att leverantören identifierat att incidenten är rapporteringspliktigad. Därefter ska uppföljande rapporter lämnas in inom **24 timmar** (Skede 2) och senare ska en slutlig rapport lämnas in inom **fyra veckor** (Skede 3). För att genomföra dessa rapporter följer ni hänvisningarna i punkt 1 och 2 ovan.

Leverantören ska ha interna rutiner för att upptäcka och bedöma rapporteringspliktiga incidenter enligt MSBFS 2018:8. Kravet innebär *inte* att extra personal behöver anställas, men identifieringen ska ske utan onödigt dröjsmål. Om en incident upptäcks på exempelvis en måndag efter en helg, startar rapporteringstiden från den tidpunkten.

MSB vidarebefordrar inkomna rapporter direkt till tillsynsmyndigheter och vid behov till Socialstyrelsen för incidenter inom hälso- och sjukvård. Rapporteringsfristen på *sex timmar* gör det möjligt för MSB/CERT-SE att ge stöd och varna andra vid behov. MSB kan också informera andra EU-länder vid gränsöverskridande incidenter.

Den slutliga rapporten (Skede 3) ska lämnas inom fyra veckor och innehålla information om åtgärder och förebyggande arbete. Om incidenten ännu inte är helt utredd ska tillgänglig information rapporteras, och uppgifterna kan kompletteras eller korrigeras inom ett år.

4. Vad ska rapporteras?



I rapporteringen ska endast sådana personuppgifter som är nödvändiga för att ange kontaktpersoner respektive beskriva incidenten, exempelvis i form av ip-adresser, lämnas. Som tidigare nämnt ska säkerhetshotande händelser direkt anmälas till Säkerhetspolisen och Försvarmakten. Sådana incidenter ska alltså inte rapporteras till MSB.

Rapportens innehåll

- **Kontaktuppgifter**

- Kontaktuppgifter till utsedd kontaktperson eller kontaktfunktion för incidenten och för störningen. Kontaktuppgifter bör hållas uppdaterade och bör inkludera roll, telefonnummer och e-postadress samt uppgift om tillgänglighet.

- **Incidentens förlopp (rapporteras i skede 1 och 2)**

- *Grundläggande information*

- När incidenten inträffade, när leverantören blev medveten om störningen samt när hanteringen inleddes, alt. när störningen upphörde.

- *Påverkan på tjänsten*

- Om tjänsten kunde tillhandahållas under störningen, bedömd minskning av tjänstens kapacitet samt vilka aktörer, sektorer och leverantörer av samhällsviktiga tjänster som påverkats.

- *Påverkan på användare*

- Vilka geografiska områden i Sverige som drabbats, hur många användare som påverkats, eventuell påverkan på människors hälsa, ekonomi eller förtroende för tjänsten.

- **Bedömning av konsekvenser för andra än användare av den samhällsviktiga tjänsten.**

- Det kan t.ex. handla om människors hälsa, ekonomi eller förtroende för den samhällsviktiga tjänsten.

Forts. nästa sida.

4. Vad ska rapporteras?

Fortsättning



- **Bedömning av konsekvenser i andra medlemsstater inom EU.**

- Vissa incidenter respektive störningar får gränsöverskridande konsekvenser. I formuläret kan leverantören ange utpekade länder där gränsöverskridande konsekvenser av incidenten, respektive störningen, uppstått.

- **Uppgift om åtgärder för att minimera konsekvenserna av incidenten.**

- I formuläret efterfrågas *hanteringsåtgärder*. För varje åtgärd anges namnet på åtgärden eller hur den ska benämnas, vad som hanteras med åtgärden, vilken status åtgärden har, vad åtgärdens avsedda effekt är och en fritextbeskrivning av vad åtgärden är och går ut på.

- **Uppgift om tidigare vidtagna åtgärder för att förebygga och hantera liknande incidenter.**

- Den här punkten har fokus på förebyggande arbete. Mot bakgrund av tidigare inträffade incidenter kan leverantören ha infört flera olika åtgärder för att hantera att liknande incidenter inte ska uppstå igen. För att kunna bedöma om åtgärderna har önskad effekt och för att MSB och tillsynsmyndigheterna ska kunna bistå andra leverantörer i deras förebyggande arbete är sådan information värdefull.

- **Uppgift om nya åtgärder för att förhindra att liknande incidenter inträffar på nytt.**

- Vid rapportering av vilka åtgärder som planeras bör sådana åtgärder som vidtas för att hantera incidentens grundorsak redovisas. I incidentrapporteringsformuläret efterfrågas förebyggande åtgärder. För varje åtgärd anges namnet på åtgärden eller hur den ska benämnas, vad som förebyggs med åtgärden, vilken status åtgärden har, hur mycket åtgärden bedöms kosta, vad åtgärdens avsedda effekt är och en fritextbeskrivning av vad åtgärden är och går ut på.

Om den rapporterande leverantören inom ett år från det att rapportering har skett konstaterar att lämnade uppgifter är felaktiga ska uppgifterna korrigeras utan onödigt dröjsmål. Även uppgifter som vid rapportering är korrekta bör korrigeras om de senare visar sig vara felaktiga.

6. Rapporteringspliktiga incidenter



Nedan följer en genomgång av vilka incidenter som anses orsaka en så pass allvarlig störning på den samhällsviktiga tjänsten att de måste rapporteras. Det innebär att störningen har haft en betydande påverkan på tjänstens funktion.

Incidenter som **inte** uppfyller dessa kriterier behöver inte rapporteras. Kriterierna har fastställts av MSB i nära samarbete med respektive sektors tillsynsmyndighet. För vägledning kring tolkningen av kraven, kontakta berörd tillsynsmyndighet

- **Energisektorn:** Energimyndigheten
- **Transportsektorn:** Transportstyrelsen
- **Bankverksamhetsektorn:** Finansinspektionen
- **Sektorn för finansmarknadsinfrastruktur:** Finansinspektionen
- **Hälso- och sjukvårdssektorn:** Inspektionen för vård och omsorg
- **Dricksvattensektorn:** Livsmedelsverket
- **Sektorn för digital infrastruktur:** Post- och telestyrelsen.



Vill ni ha rådgivning gällande NIS2?

Hör av er till oss på sales@gridheart.com