Myndigheten för samhällsskydd och beredskap

Datum	Diarienr	Utgåva
2018-12-20	MSB 2018-13470	1.0

Vägledning om rapportering av incidenter för leverantörer av samhällsviktiga tjänster enligt NIS-regleringen

MSB:s kontaktperson:
Carina Wetzel, 010-240 42 62
Publikationsnummer MSB 1327- december 2018
ISBN 978-91-7383-901-3

Innehållsförteckning

1. Inledning 4

2. Syftet med incidentrapportering 5

3. Begreppsförklaringar 6

4. Rapportering 7

4.1 Vem ska rapportera 7

4.2 Hur ska rapportering ske 7

4.3 När ska rapportering ske 8

4.4 Vad ska rapporteras 9

4.5 Rapporteringspliktiga incidenter 14

4.5.1 Energi 14

4.5.2 Transport 17

4.5.3 Bankverksamhet 18

4.5.4 Finansmarknadsinfrastruktur 18

4.5.5 Hälso- och sjukvård 19

4.5.6 Dricksvatten 21

4.5.7 Digital infrastruktur 22

1. Inledning

I juli 2016 antogs Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverk och informationssystem i hela unionen, (NIS-direktivet). NIS-direktivet har införts i Sverige genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) samt förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen). Dessutom har MSB tagit fram följande föreskrifter för leverantörer av samhällsviktiga tjänster:

- föreskrifter om anmälan och identifiering (MSBFS 2018:7)
- föreskrifter om informationssäkerhet (MSBFS 2018:8)
- föreskrifter om rapportering av incidenter (MSBFS 2018:9)

Leverantörer av samhällsviktiga tjänster ska utan onödigt dröjsmål rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller. Syftet med denna vägledning är att ge stöd åt leverantörer att rapportera incidenter enligt Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:9) om rapportering av incidenter för leverantörer av samhällsviktiga tjänster.

Om incidenten kan antas ha en brottslig grund är det viktigt att leverantören inte bara rapporterar incidenten till MSB utan även polisanmäler det inträffade.

I texten finns utdrag från Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:9) om rapportering av incidenter för leverantörer av samhällsviktiga tjänster. Dessa utdrag är inramade. Övriga texter är vägledande.

2. Syftet med incidentrapportering

Nätverks- och informationssystem spelar en viktig roll i samhället och deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet. Säkerhet i nätverk och informationssystem är idag avgörande för att samhället ska fungera. Ökad nätverk- och informationssäkerhet hos leverantörer av samhällsviktiga tjänster skyddar såväl individer som organisationer och samhället i stort.

Incidentrapportering syftar till att öka förmågan att förebygga och hantera incidenter och minska deras konsekvenser för att kunna förbättra informationssäkerheten för leverantören och i samhället. Vid en incident sker rapporteringen i ett tidigt skede vilket ger MSB möjlighet att medverka operativt i hanteringen genom att ge stöd till drabbad leverantör och genom samverkan med berörda aktörer. Vid behov kan MSB informera allmänheten och varna andra aktörer både nationellt och inom EU. Inrapporterade incidenter bidrar även till MSB:s lägesuppfattning över incidenter och deras konsekvenser och möjliggör effektiva förebyggande åtgärder och förståelse av resursbehov på kort och lång sikt. Det skapar möjlighet till gemensamma lösningar på gemensamma problem.

För att effektivt uppfylla syftet med rapporteringen är det viktigt att rapporten innehåller tillräckligt med information om den inträffade incidenten och hur den påverkat den samhällsviktiga tjänsten. MSB gör bedömningen att rapporterna kan ha ett högt skyddsvärde. Innehållet i inlämnade rapporter skyddas av sekretessbestämmelser samt tekniska och organisatoriska säkerhetsåtgärder motsvarande skyddsvärdet.

Incidentrapporterna kommer att användas för strategisk analys, risk- och sårbarhetsbedömningar samt erfarenhetsutbyten. Slutsatser från inkomna incidentrapporter sammanställs och görs tillgängliga i olika typer av analyser som stöd i förebyggande arbete på både leverantörs- och samhällsnivå. Hanteringen av incidentrapporterna sker på ett sådant sätt att skyddet av informationen upprätthålls.

Inkomna incidentrapporter delas utan dröjsmål med tillsynsmyndigheterna som bl.a. kan använda dem i sitt tillsynsarbete. Tillsynsmyndigheternas tillsyn när det gäller incidentrapporteringen omfattar många olika delar, t.ex. vilka incidenter som rapporteras, vilka som inte rapporteras, hur arbetet med rapportering har organiserats, vad som rapporteras och när rapportering sker.

3. Begreppsförklaringar

De uttryck som förklaras i NIS-lagen har samma innebörd i föreskrifterna. Ett uttryck som är centralt för hela incidentrapporteringen och som förklaras i lagen är incident, som innebär en händelse med en *faktisk negativ inverkan på säkerheten i nätverk och informationssystem*.

extern aktör	Underleverantör, inhyrda konsulter eller motsvarande.

Underleverantör inom den egna koncernen inbegrips inte i begreppet. Begreppet koncern har samma innebörd som i 12 § aktiebolagslagen (2005:551), dvs. att moderbolag och dotterbolag tillsammans utgör en koncern.

störning i den samhällsviktiga tjänsten	En konsekvens av incidenten som innebär att den samhällsviktiga tjänsten inte levereras i förhållande till normalt tillhandahållande.

Begreppet störning används på flera ställen i lagstiftningen, både för att identifiera om en tjänst är samhällsviktig och vid bedömningen av om en incident är rapporteringspliktig. Som exempel kan nämnas att antalet användare som påverkas av störningen är ett av de ingångsvärden som MSB har använt vid utformningen av vad som är rapporteringspliktigt enligt myndighetens föreskrifter om incidentrapportering.

Som ovan nämndes är en incident en händelse med en *faktisk negativ inverkan på säkerheten i nätverk och informationssystem*. Incidenten i sig är därmed endast kopplad till vad som hänt i de tekniska systemen. En incident kan dock få konsekvenser utanför den tekniska miljön. Om en samhällsviktig tjänst är beroende av nätverk och informationssystem är det mycket sannolikt att en incident i dessa nätverk och informationssystem får konsekvenser för tillhandahållandet av den samhällsviktiga tjänsten, det vill säga orsakar störningar i den samhällsviktiga tjänsten. Störningen – *konsekvensen* – kan se olika ut inom olika verksamheter. Om en incident orsakar en störning som är så stor att den innebär en *betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten* är incidenten rapporteringspliktig. För att kunna avgöra om störningen är så pass stor att incidenten är rapporteringspliktig finns kriterier framtagna inom respektive sektor (se kriterier och exempel i avsnitt 4.5). Leverantören behöver ha interna regler och arbetssätt på plats utan dröjsmål för att kunna identifiera en rapporteringspliktig incident.

I 12 § MSBFS 2018:8 om informationssäkerhet för leverantörer av samhällsviktiga tjänster ställs krav på leverantören för att kontinuitet ska kunna upprätthållas vid incidenter.

4. Rapportering

4.1 Vem ska rapportera

Den som är identifierad som en leverantör av en samhällsviktig tjänst[1] är ansvarig för att rapportera incidenter. Skyldigheten att rapportera incidenter gäller oavsett var incidenten har skett. Om en leverantör t.ex. har utkontrakterat driften av nätverk och informationssystem och en incident i dessa har en betydande inverkan på kontinuiteten i tillhandahållandet av den samhällsviktiga tjänsten ska leverantören rapportera den inträffade incidenten.

Leverantören bör se över sina avtal med externa aktörer[2] för att säkerställa att leverantören snarast får information om sådana incidenter så att rapporteringsplikten kan uppfyllas.

Leverantören kan välja att också låta den externa aktören rapportera incidenter till MSB på leverantörens uppdrag om det passar befintlig struktur för intern incidenthantering och -rapportering. Ansvaret för rapporteringen ligger dock alltid på leverantören av den samhällsviktiga tjänsten. Hur rapportering utförs omfattas av tillsyn.

4.2 Hur ska rapportering ske

2 kap. 2 §
Leverantörer av samhällsviktiga tjänster ska rapportera incidenter via anvisade kontaktvägar.

Rapportering sker i första hand genom att använda MSB:s incidentrapporteringsverktyg. För att få tillgång till verktyget krävs att varje person som är utsedd av leverantören att rapportera incidenter har ett aktivt incidentrapporteringskonto. Mer information om hur incidentrapporteringskonto aktiveras och hur rapportering sker finns på msb.se. Incidentverktyget innehåller ett formulär med frågor som utgår från kraven i föreskrifterna och som leverantören ska besvara. Formuläret finns att

[1] MSBFS 2018:7 med tillhörande vägledning ger stöd att identifiera om organisation är leverantör av samhällsviktig tjänst.
[2] Se avsnitt 3 för om begreppet extern aktör.

ladda ned på msb.se för att leverantören ska kunna läsa frågorna och förbereda incidentrapportering.

Om det bedöms finnas uppgifter i rapporteringen till MSB som omfattas av sekretess på grund av skydd av Sveriges säkerhet ska dessa inte rapporteras i incidentrapporteringsverktyget, utan överlämnas enligt särskild ordning.

4.3 När ska rapportering ske

Den första rapporteringen ska ske sex timmar från det att leverantören har identifierat att en incident är rapporteringspliktig (i formuläret kallas den första rapporteringen *Skede 1*), med uppföljande rapportering inom 24 timmar (*Skede 2*) respektive fyra veckor (*Skede 3*).

Leverantören ska ha interna regler och arbetssätt på plats för att upptäcka incidenter.[3] Dessutom bör interna regler och arbetssätt tydliggöra hur arbete ska ske med att identifiera vilka incidenter som är rapporteringspliktiga enligt MSBFS 2018:8.

Föreskriftskravet ska inte tolkas som krav på ökad bemanning. NIS-lagen ställer krav på att leverantören ska rapportera incidenter utan onödigt dröjsmål. Tidsfristen för rapportering räknas från den tidpunkt då leverantören med stöd av sina interna regler och arbetssätt identifierat en incident som rapporteringspliktig. En verksamhet kan t.ex. vara obemannad och en incident som inträffar under helgen identifieras inte förrän på måndagen, rapporteringsplikten inträffar då sex timmar senare. Det bör dock betonas att arbetet med identifieringen, även om det inte behöver ske med hjälp av extrabemanning, ändå ska genomföras utan onödigt dröjsmål. Inkomna rapporter vidarebefordras utan dröjsmål av MSB till berörd tillsynsmyndighet samt avseende incidenter inom sektorn hälso- och sjukvård även till Socialstyrelsen.

Tidsfristen på sex timmar är framtagen med anledning av möjligheten för MSB/CERT-SE (Computer Emergency Response Team), som är Sveriges nationella CSIRT (Computer Security Incident Response Team), att vid behov och när så är möjligt hjälpa leverantören med incidenten och varna andra. Det är därför viktigt att få en övergripande bild av incidenten på ett tidigt stadium. MSB ska, för Sveriges räkning, vid behov, informera övriga medlemsstater om gränsöverskridande incidenter. I och med kravet på rapportering inom sex timmar och sedan uppföljande rapportering inom 24 timmar kan MSB/CERT-SE skapa en samlad lägesuppfattning. Vid inrapporterad incident bedömer MSB/CERT-SE om det finns behov av att agera på incidenten. Därefter inleds

[3] Enligt krav i 11 § MSBFS 2018:8 om informationssäkerhet för leverantörer av samhällsviktiga tjänster.

eventuellt incidenthantering som bland annat kan innebära kontakt med rapporterande leverantör och andra drabbade, sökning bland tillgänglig information hos till exempel MSB/CERT-SE:s kontaktnät, informera eller samordna åtgärder för att drabbade ska kunna återgå i normal drift, informera andra aktörer, såväl nationellt som internationellt samt vid behov allmänheten.

MSB och tillsynsmyndigheterna behöver även uppgifter om åtgärder för det förebyggande arbetet och för tillsynen. Med hänsyn till att det tar tid att slutligt hantera incidenter har bedömningen gjorts att leverantörer bör få fyra veckor på sig att lämna sådana uppgifter. Även om incidenten ännu inte är slutligt hanterad efter fyra veckor ska rapportering ändå ske. Leverantören får då lämna tillgänglig information. En inlämnad rapport kan korrigeras eller kompletteras inom ett år från första rapporteringstillfället, se avsnitt 4.4

4.4 Vad ska rapporteras

Nedan följer en genomgång av vad incidentrapporten ska innehålla. I incidentrapporteringsverktyget finns ett formulär som är utformat för att både underlätta rapporteringen för leverantörerna och för MSB:s analyser av inrapporterade incidenter på en aggregerad nivå. Det är därför centralt att rapportering sker genom incidentrapporteringsverktyget. Detta förutsätter, som nämns i avsnitt 4.2, att leverantören aktiverar sitt incidentrapporteringskonto i enlighet med instruktion från MSB. Är rapporteringsverktyget inte tillgängligt kan formuläret laddas ned i pdf-form.

I rapporteringen bör endast sådana personuppgifter som är nödvändiga för att ange kontaktpersoner respektive beskriva incidenten, exempelvis i form av ip-adresser, lämnas.

Enligt 2 kap. 10 § säkerhetsskyddsförordningen (2018:658)[4] ska säkerhetshotande händelser och verksamhet skyndsamt anmälas till Säkerhetspolisen respektive Försvarsmakten. Sådana incidenter ska inte rapporteras till MSB.

[4] Träder i kraft 2019-04-01, motsvarande krav finns i 10 a § säkerhetsskyddsförordningen (1996:633).

2 kap. 4 § 2 p.

Kontaktuppgifter till utsedd kontaktperson eller kontaktfunktion för incidenten och för störningen.

Allmänna råd

Kontaktuppgifter bör hållas uppdaterade och bör inkludera roll, telefonnummer och e-postadress samt uppgift om tillgänglighet.

Kontaktuppgifter efterfrågas för att MSB vid behov ska kunna ta kontakt för hantering av incidenten och/eller störningen. Personen/funktionen kan vara densamma som för leverantörens interna hantering av incidenter, men leverantören kan också välja att MSB ska kontakta någon annan i organisationen. En sådan kontakt kan exempelvis bli aktuell om flera leverantörer rapporterat liknande incidenter inom kort tid och det finns behov av att klarlägga eventuella samband eller om den inlämnade incidentrapporten behöver kompletteras. Om incidenten pågår en längre tid och kontaktuppgifterna ändras, bör detta meddelas MSB.

2 kap. 4 § p. 5

En beskrivning av inträffad incident, utifrån

a) tidpunkt för när incidenten inträffade och när den upptäcktes,

b) om den fortfarande pågår eller tidpunkt för när drabbade nätverk och informationssystem återgick till normaldrift,

c) händelseförlopp,

d) hanteringen av incidenten, samt

e) typ, orsak och konsekvenser.

Information om *incidentens* innehåll och förlopp rapporteras i incidentrapporteringsformuläret Skede 1 (inom 6 timmar) och Skede 2 (inom 24 timmar). Eftersom det kan vara svårt att ha en fullständig bild av incidenten redan när Skede 1 ska rapporteras ställs en begränsad uppsättning frågor om incidenten i det skedet. I Skede 2 ställs ytterligare frågor som utökar och fördjupar bilden av incidenten.

I Skede 1 ska leverantören ange om incidenten har inträffat i en tjänst som tillhandahålls av en extern aktör, när incidenten inträffade, när den upptäcktes av leverantören, när hanteringen av incidenten inleddes och (om incidenten inte har angetts vara pågående) när incidenten upphörde. Om incidenten har angetts vara pågående ställs också frågan om hur länge som leverantören bedömer att incidenten kommer att fortsätta att pågå. Det finns även fritextfält för beskrivning av incidenten och dess hantering.

2 kap. 4 § p. 6

En beskrivning av störningen, utifrån

a) tidpunkt för när störningen uppstod samt när och hur den upptäcktes,

b) om störningen fortfarande pågår eller tidpunkt för när den upphörde alternativt förväntas upphöra,

c) dess påverkan på den samhällsviktiga tjänsten,

d) användare som påverkas av störningen, samt

e) geografiskt område som påverkas av störningen.

Information om *störningens* innehåll och förlopp rapporteras i Skede 1. Eftersom det kan vara svårt att ha en fullständig bild av störningen redan när Skede 1 ska rapporteras ställs huvudsakligen övergripande frågor om störningen.

I Skede 1 ska leverantören ange när incidenten inträffade, när leverantören blev uppmärksammad på störningen, när hanteringen av störningen inleddes och (om störningen inte har angetts vara pågående) när störningen upphörde. Om störningen har angetts vara pågående ställs också frågan om hur länge som leverantören bedömer att störningen kommer att fortsätta att pågå. Leverantören ska också ange om tjänsten kan eller kunde tillhandahållas medan störningen pågår eller pågick, hur stor minskning av den samhällsviktiga tjänstens kapacitet som rapportören bedömer att störningen medför, vilka typer av aktörer, vilka sektorer och om leverantörer av samhällsviktiga tjänster påverkas negativt av störningen. Vidare ska anges var i Sverige användare påverkas negativt av störningen, hur många användare som påverkas negativt av störningen samt om människors hälsa, användarnas ekonomi eller användarnas förtroende för den samhällsviktiga tjänsten påverkas negativt av störningen i den samhällsviktiga tjänsten. Även störningen och dess hantering kan beskrivas i fritext.

2 kap. 4 § p. 7

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

De flesta leverantörer har en förhållandevis god bild av vilken konsekvens en störning i den samhällsviktiga tjänsten får för användarna. Ibland kan dock störningen i tjänsten påverka även andra än användarna av tjänsten. Även om det kan vara svårt att göra en bedömning av sådana konsekvenser kan det vara information som är mycket värdefull för hanteringen av både incidenten och störningen samt för det förebyggande arbetet. Det kan t.ex. handla om människors hälsa, ekonomi eller förtroende för den samhällsviktiga tjänsten.

Det går också att i fritext beskriva sådana konsekvenser i incidentrapporteringsformuläret.

2 kap. 4 § p. 8
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. Det går också att beskriva konsekvenserna i fritext i incidentrapporteringsformuläret

2 kap. 4 § p. 9
Uppgift om åtgärder för att minimera konsekvenserna av incidenten.

I formuläret efterfrågas s.k. *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.

2 kap. 4 § p. 10
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.

Även leverantörens förmåga att kunna bedöma risken för att olika typer av incidenter inträffar är viktigt för att utveckla det förebyggande arbetet.

I incidentrapporteringsformuläret ställs särskilda frågor om liknande incidenter och störningar har inträffat tidigare, om sådana incidenter och störningar har analyserats i riskanalys, om det finns kontinuitetsplaner för sådana incidenter och störningar och om det finns mål för genomsnittlig respektive maximal återställningstid vid incidenter och störningar, samt om det finns mål för genomsnittlig tid mellan incidenter respektive mellan störningar.

2 kap. 4 § p. 11

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

Allmänna råd

Vid rapportering av vilka åtgärder som planeras bör sådana åtgärder som vidtas för att hantera incidentens grundorsak redovisas.

I de fall det förebyggande arbetet inte har varit tillräckligt effektivt kan nya åtgärder för att förhindra liknande incidenter behöva vidtas. Dessa redovisas under den här punkten.

I riskbedömningar och resonemang kring val av införda säkerhetsåtgärder bör alltid en grundorsaksanalys ingå.

För att identifiera grundorsaken till en incident behöver ibland orsakssambanden analyseras i flera steg. Exempelvis kan en incident som orsakats av ett handhavandefel ha sin grundorsak i bristande utbildning. Incidentens grundorsak behöver då åtgärdas genom en översyn av behoven av utbildning/kompetens liksom hur kunskapsnivån hos medarbetarna följs upp. Detta inkluderar även etablering av regler och arbetssätt som på ett långsiktigt och systematiskt sätt säkerställer att alla har rätt kompetens för sin uppgift.

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.

2 kap. 5 §

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.

Allmänna råd

Även uppgifter som vid rapportering är korrekta bör korrigeras om de senare visar sig vara felaktiga.

Kravet innebär att leverantören kan återkomma till MSB för att i ett senare skede korrigera tidigare lämnade uppgifter. Som följer av det allmänna rådet bör uppgifter korrigeras om de vid senare tillfälle visar sig vara felaktiga. Det kan exempelvis handla om att incidenten inledningsvis bedömdes ha orsakats av ett mänskligt fel men efter en djupare utredning visar det sig att det var ett angrepp som var orsaken.

Eftersom incidentrapporterna används för olika typer av analyser som i sin tur ligger till grund för beslut om hur exempelvis förebyggande arbete utformas är det centralt att underlaget är så rättvisande som möjligt.

4.5 Rapporteringspliktiga incidenter

Nedan följer en genomgång av vilka incidenter som bedöms orsaka en sådan störning på den samhällsviktiga tjänsten att de är rapporteringspliktiga, d.v.s. störningen har fått en betydande inverkan på den samhällsviktiga tjänsten. Incidenter som inte uppfyller nedan kriterier är inte rapporteringspliktiga. Samtliga kriterier har MSB tagit fram och beslutat om i nära samverkan med tillsynsmyndigheten inom respektive sektor. För stöd i tolkning av kraven kontakta respektive tillsynsmyndighet:

Energi – Energimyndigheten

Transport – Transportstyrelsen

Bankverksamhet – Finansinspektionen

Finansmarknadsinfrastruktur – Finansinspektionen

Hälso- och sjukvård – Inspektionen för vård och omsorg

Dricksvatten – Livsmedelsverket

Digital infrastruktur – Post- och telestyrelsen

4.5.1 Energi

El

3 kap. 1 §

Leverantörer inom el ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som

1. har pågått i minst två timmar och som har påverkat
   a) minst 2 000 kunder, eller
   b) minst 50 % av kunderna, eller
2. har påverkat styrning och övervakning av transmissionsnät, regionnät eller elproduktion.

Nedan följer ett antal exempel på incidenter som ska rapporteras. Exemplen ska inte ses som uttömmande.

Aktör A är ett svenskt elnätsbolag som får ett avbrott i leveransen, i ledningar där spänningen understiger 220 kV vilka används för överföring av el mellan regioner (regionnät). Avbrottet orsakas av en it-incident där övervakningen av

nätet momentant fallerar. Efter 90 minuter får man igång systemet, men efter sex timmar upptäcks att spänningen är för hög i ett område.

- Avbrottet är rapporteringsskyldigt eftersom:
  - det rör sig om ett bolag som bedriver elöverföring i regionnätet, samt,
  - styrningen och övervakningen har påverkats.
- Avbrottet *kan* också vara rapporteringsskyldigt om den höga spänningen under de sex timmarna påverkat minst 2 000 kunder, eller minst 50 % av kunderna. Det behöver inte vara totalt elavbrott för att vara rapporteringsskyldigt, oförmåga att leverera den avtalade kvaliteten i tjänsten räcker för att störningen ska klassas som betydande inverkan vid tillhandahållandet av tjänsten.

Aktör B är en ekonomisk förening som äger en vindkraftspark. Ett normalt år producerar anläggningen ca 85 GWh. Inmatningen sker på regionnätet via en systemtransformator. Under en sommarnatt med liten produktion inträffar en it-incident som omöjliggör produktion under 6 timmar. Dessutom fallerar övervakningen helt under 30 min då personalen står helt utelåsta från systemet.

- Avbrottet är rapporteringsskyldigt eftersom:
  - Elproduktionen är ansluten till regionnät, samt,
  - styrningen och övervakningen har påverkats.

Gas

3 kap. 2 §

Leverantörer inom gasförsörjningen ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som

3. innebär risk för en händelse som resulterar i en avsevärd försämring av försörjningssituationen för gas,
4. kan leda till avbrott i gasförsörjningen, eller
5. har påverkat styrning och övervakning inom ramen för systemansvarstjänst.

Nedan följer ett antal exempel på incidenter som ska rapporteras. Exemplen ska inte ses som uttömmande.

Aktör C är ett kommunalt bolag som äger naturgasledningar som ingår i det västsvenska naturgasnätet. Under en sommarnatt med liten förbrukning inträffar en it-incident som omöjliggör övervakningen av nätet under 4 h då personalen står helt utelåsta från systemet. I efterhand kan man se att flödet i ledningarna inte har påverkats.

- Avbrottet är rapporteringsskyldigt eftersom styrningen och övervakningen har påverkats.

Aktör D är en större gasleverantör till det västsvenska naturgasnätet, ett svenskt dotterbolag till en internationell koncern. Under en väldigt kall februaridag, mitt i arbetsveckan, får handlarna ett kommunikationsavbrott som leder till att de tappar marknadsövervakningen för spotmarknaden och möjligheten att handla under 12 h. Incidenten leder till att nomineringen för kommande dygn hos balansansvariga blir kraftigt missvisande.

- Avbrottet är rapporteringsskyldigt eftersom det har påverkat:
  - handel och leverans av naturgas,
  - det innebär risk för en händelse som resulterar i en avsevärd försämring av försörjningssituationen för gas, samt
  - styrningen och övervakningen har påverkats.

Olja

3 kap. 3 §
Leverantörer inom olja i form av flytande drivmedel och bränslen ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som 1. har pågått i minst 12 timmar, eller 2. påverkar styrning och övervakning av ledning, överföring och distributionsnätverk under minst två timmar.

Nedan följer ett antal exempel på incidenter som ska rapporteras. Exemplen ska inte ses som uttömmande.

Aktör E är ett svenskt dotterbolag till en internationell koncern. Aktören raffinerar drivmedel och bränsle för den skandinaviska marknaden. Råvarorna är råolja och brännolja av nästan uteslutande fossilt ursprung. Varorna säljs oftast vidare till ett annat bolag i koncernen innan försäljning till slutkund. Aktören producerar ett normalår ca 760 000 ton, varav allt säljs till det svenska dotterbolaget eller till svenska stationer inom koncernen. Under en helg drabbas raffinaderiet av en it-incident som leder till att ingen produkt kan färdigställas, aktören tvingas mellanlagra ofärdiga produkter i två dygn, innan hela processen är igång igen. Volymerna för distribution är återtagna på veckobasis, efter fem dagar.

- Avbrottet är rapporteringsskyldigt eftersom tjänsten omfattar:
  - import, export, produktion, raffinering, bearbetning eller försäljning som hanterar minst,
    - 500 000 ton/år för petroleumbaserade drivmedel och bränslen, samt
  - pågått i minst 12 timmar

Aktör F är ett aktiebolag som erbjuder drivmedelslagring som tjänst eller för upplåtelse av hela cisterner. Sammanhållen kapacitet för hela depån är cirka 450 000 m3, varav aktör F äger och hyr ca 200 000 m3. Under en vardag drabbas brandsäkerhetssystemet för depån av en it-incident som omöjliggör lastning eller lossning i lastbilsdepån under ett dygn, lossning via järnväg och lossning av fartyg påverkas inte.

- Avbrottet är rapporteringsskyldigt eftersom tjänsten omfattar;
  - tillhandahållande av drivmedelslager och depåer,
  - med sammanlagd kapacitet på minst 100 000 m3, och möjligen
  - med sammanlagd kapacitet på minst 20 000 m3 och med avgörande betydelse för regional försörjning, eller
  - med sammanlagd kapacitet på minst 10 000 m3 för jetbränsle, och
  - har pågått i minst 12 timmar.

4.5.2 Transport

4 kap. 1 §

Leverantörer inom transport ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som

1. har pågått i minst en timme och kan antas ha påverkat
   a) minst 1000 användare, eller
   b) ett sammanhängande geografiskt område om minst 10 000 km^2, eller
2. har pågått i minst två timmar.

Med ”användare” avses transportköpare, t.ex. resenär/passagerare eller den som köper en godstransport samt användare av infrastruktur exempelvis operatörer, resenär/passagerare eller den som köper en godstransport.

4.5.3 Bankverksamhet

5 kap. 1 §

Leverantörer inom bankverksamhet ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som

1. innebär att transaktioner inte kan eller sannolikt inte kommer att kunna initieras eller behandlas för
   a) minst 25 % av leverantörens normala antal transaktioner, eller
   b) minst 25 % av leverantörens användare, eller
2. pågår sammanlagt minst tre timmar under en 24-timmars period.

Inom bankverksamhet relaterar kriterierna till antal transaktioner, antal användare och störningens längd avseende betaltjänster enligt 1 kap. 2 § punkt 1-6 lag (2010:751) om betaltjänster. Kriterierna överensstämmer i stora drag med de incidentrapporteringskrav som ställs i Europaparlamentets och rådets direktiv (EU) 2015/2366 (PSD 2) om betaltjänster på den inre marknaden.

4.5.4 Finansmarknadsinfrastruktur

6 kap. 1 §

Leverantörer inom finansmarknadsinfrastruktur ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som

3. innebär avvikelse från sådan konnektivitet som avses i art. 11 punkt 5 Kommissionens delegerade förordning (EU) 2017/584 av den 14 juli 2016 om komplettering av Europaparlamentets och rådets direktiv 2014/65/EU avseende tekniska tillsynsstandarder som specificerar organisatoriska krav för handelsplatser,
4. påverkar väsentliga tjänster hos systemviktiga finansiella infrastrukturföretag och har pågått i minst en timme, eller
5. har pågått i minst två timmar.

Kriterierna är i linje med CPMI-IOSCO:s principer för finansmarknadsinfrastruktur samt de incidentrapporteringskrav som ställs i EU:s direktiv om värdepappersmarknaden (Mifid 2).

Konnektivitet definieras som förmåga att utbyta information mellan två separata it-system eller datacenter som är uppkopplade genom nätverk. Konnektivitet har stor betydelse för en väl fungerande marknad och finansiell stabilitet. En störning i konnektivitet hos handelsplatser innebär att en ordnad handel i finansiella instrument inte kan genomföras.

4.5.5 Hälso- och sjukvård

7 kap. 1 §

Leverantörer inom hälso- och sjukvård ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som

1. innebär att anmälningsskyldighet inträder enligt 3 kap. 5 § första stycket patientsäkerhetslagen (2010:659),

Vid en händelse som har medfört eller hade kunnat medföra allvarlig vårdskada enligt definitionen i 1 kap 5 § PSL och där vårdgivaren påvisat att en incident varit en bidragande orsak till händelsen, ska incidentrapportering utföras.

En incident i vårdgivarens nätverk och informationssystem kan leda till bristande, utebliven, förvanskad eller felaktig information i exempelvis

- patientjournalsystem
- laboratoriedatasystem
- it- system för visning, lagring och behandling av patientinformation, såsom övervakning, röntgen, EKG etc.
- bloddatasystem
- receptexpedieringssystem

Exempelvis kan ett driftavbrott eller annan incident i ett patientjournalsystem bidra till eller orsaka att en patient får felaktig, utebliven eller fördröjd behandling eller diagnos och patienten därigenom drabbas av eller riskerar att drabbas av en allvarlig vårdskada. Dessa exempel ska inte ses som uttömmande utan det kan förekomma ytterligare system som berörs.
Utöver incidentrapportering till MSB ska vårdgivaren göra en anmälan enligt lex Maria till IVO.

2. har påverkat tillhandahållandet av ambulans och ambulanssjukvård enligt 7 kap. 6 § hälso- och sjukvårdslagen (2017:30),

Om ambulanstransport eller ambulanssjukvård inte kan verkställas på avsett sätt och detta helt eller delvis beror på en incident ska detta rapporteras. Det kan till exempel handla om att en incident i nätverk och informationssystem leder till fördröjning av ambulansdirigering eller ambulanstransport, eller att ambulanssjukvård (d.v.s. vårdåtgärder som vidtas av ambulanspersonal) inte kan tillhandahållas på det sätt som normalt skulle ske om incidenten inte hade inträffat.

Bestämmelsen anger ingen tidsgräns eller konsekvens avseende patienten utan fokus riktas på tillhandahållandet av tjänsten. Ambulanssjukvård är av den typen att även mindre störningar kan få allvarliga konsekvenser. Därför ska incidenter som har påverkat tillhandahållandet rapporteras även om en patient i det enskilda fallet inte har påverkats.

3. innebär att sådan hälso- och sjukvård som baseras på system som insamlar, bearbetar, lagrar eller distribuerar och presenterar information inte kan tillhandahållas i minst två timmar, eller

Om en incident i vårdgivarens nätverk och informationssystem leder till att avsedda hälso- och sjukvårdsåtgärder inte kan utföras under minst två timmar ska incidentrapportering ske. I detta fall finns ingen koppling till eventuella konsekvenser för patienten. En sådan incident behöver alltså inte påverka patienters hälsotillstånd för att ha en betydande inverkan på tillhandahållandet av tjänsten.

Uttrycket ”hälso- och sjukvård som baseras på system som insamlar, bearbetar, lagrar eller distribuerar och presenterar information” ska tolkas som sådana insatser i hälso- och sjukvården som genomförs med hjälp av informationssystem i enlighet med 2 kap 1 § Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården, alternativt mot bakgrund av eller med stöd av informationen i informationssystem. Incidentrapportering kan exempelvis orsakas av att information i journal-, övervaknings-, laboratoriedata-, bilddata- eller receptexpedieringssystem inte är tillgänglig eller tillförlitlig och att detta leder till att avsedda hälso- och sjukvårdsåtgärder fördröjs med minst två timmar. Den här typen av system exemplifieras även i punkt 1.

4. har pågått i minst sex timmar.

Bestämmelsen avser incidenter i alla nätverk och informationssystem som vårdgivaren använder. Det vill säga inte bara de system som används för hälso- och sjukvård enligt punkt 3, utan även t.ex. IP-telefoni eller administrativa system som t.ex. används för att användare ska kunna kontakta vårdenheten och få övriga upplysningar om hur dennes vård kommer bedrivas. Incidenter som inte fått några konsekvenser för patientsäkerheten, men som pågår en längre tid, kan indikera brister i det systematiska informationssäkerhetsarbetet och ska därför rapporteras.

4.5.6 Dricksvatten

8 kap. 1 §

Leverantörer inom leverans och distribution av dricksvatten ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som

1. har pågått i minst två timmar och som
   a) kan antas ha påverkat minst 2 000 personer,
   b) har påverkat akutsjukhus, eller

Om leverantören är osäker på om ett sjukhus är ett akutsjukhus eller inte bör det stämmas av det med vårdgivaren. Påverkan är kopplad till vård som bedrivs.

2. har påverkat styrning och övervakning av tjänsten.

Om övervakningen inte är kontinuerlig, ska påverkan bedömas i relation till när och hur övervakning sker i normalfallet.

Påverkan innebär inte enbart driftsavbrott. Beroende på systemets konstruktion finns en risk att felaktig funktion i styr- och reglersystemet skulle kunna både över- och underdosera kemikalier. Exempelvis kan underdosering vara problematiskt när det gäller klor eftersom en mikrobiologisk säkerhetsbarriär då slås ut. På motsvarande sätt kan felaktig funktion orsaka att pumpar antingen stannar eller kör så mycket att det skulle kunna orsaka tryckfall eller översvämningar i distributionen.

4.5.7 Digital infrastruktur

9 kap. 1 §

Leverantörer inom digital infrastruktur ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som innebär

1. att toppdomänens namnservertjänst har en tillgänglighet på mindre än 100 procent,
2. förlorad konfidentialitet eller riktighet i lagrade, överförda eller behandlade data i samband med tillhandahållande av en toppdomäns namnservertjänst som har berört fler än 2 500 domännamn,
3. att en rekursiv namnservertjänst har en tillgänglighet på mindre än 100 procent under en sammanhängande period som överstiger en timme,
4. förlorad konfidentialitet eller riktighet i lagrade, överförda eller behandlade data i samband med tillhandahållande av en rekursiv namnservertjänst som har berört fler än 10 000 användare,
5. att en auktoritativ namnservertjänst har en tillgänglighet på mindre än 100 procent under en sammanhängande period som överstiger två timmar, eller
6. förlorad konfidentialitet eller riktighet i lagrade, överförda eller behandlade data i samband med tillhandahållande av en auktoritativ namnservertjänst som har berört fler än 2 500 domännamn.

Även om informationen i en namnservertjänst är öppen, går det inte att utesluta att hanteringen av själva tjänsten förutsätter att vissa uppgifter är konfidentiella.