Myndigheten för samhällsskydd och beredskap

Datum	Diarienr	Utgåva
2018-12-20	MSB 2018-13472	1.0

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

MSB:s kontaktperson:
Carina Wetzel, 010-240 42 62
Publikationsnummer MSB 1325- december 2018

Innehållsförteckning

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), förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen) samt myndighetsföreskrifter.

EU-kommissionen beslutade i januari 2018 om en genomförandeförordning som närmare specificerar krav på säkerhetsåtgärder och incidentrapportering för leverantörer av digitala tjänster. Kontroll av efterlevnad av reglerna sker genom tillsyn som utförs av den utpekade tillsynsmyndigheten Post- och Telestyrelsen (PTS).

Leverantörer av digitala tjänster ska utan onödigt dröjsmål rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av en digital tjänst som de erbjuder inom Europeiska unionen. Syftet med denna vägledning är att ge stöd åt leverantörer att rapportera incidenter enligt Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:10) om rapportering av incidenter för leverantörer av digitala tjänster.

Vägledningen ger inte stöd i hur Kommissionens genomförandeförordning (EU) 2018/151 av den 30 januari 2018 (genomförandeförordningen) ska tolkas.

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 2018:10) 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 digitala 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 tillsynsmyndigheten 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 här samma innebörd som i 12 § aktiebolagslagen (2005:551), dvs. att moderbolag och dotterbolag tillsammans utgör en koncern.

störning i den digitala tjänsten	En konsekvens av en incident som innebär att den digitala tjänsten inte levereras som normalt.

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.[1]

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 digital 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 digitala tjänsten, det vill säga orsakar störningar i den digitala tjänsten. Störningen – *konsekvensen* – kan se olika ut inom olika verksamheter. Om en incident orsakar en störning som är så stor att den innebär en *avsevärd inverkan på tillhandahållandet av den digitala tjänsten* är incidenten rapporteringspliktig. För att kunna avgöra om störningen är så pass stor att incidenten är rapporteringspliktig finns kriterier framtagna, vilka dessa är framgår av art. 4 i genomförandeförordningen. Kriterierna ska användas för att leverantören med hjälp av sina interna processer ska kunna identifiera om en incident är rapporteringspliktig. Det tydliggörs i genomförandeförordningen (skäl 10) att de fall som anges i

[1] I genomförandeförordningen nämns exempelvis incident som orsakar störningar i samband med hantering av driftskontinuitet. (art 2 punkt 3)

genomförandeförordningen inte bör ses som en uttömmande förteckning över rapporteringspliktiga incidenter.

I art 2 genomförandeförordningen ställs även krav på säkerhetsaspekter som leverantören ska beakta för att säkerställa en nivå av säkerhet för de nät- och informationssystem som de använder för att erbjuda sina digitala tjänster.

4. Rapportering

4.1 Incidentrapporteringskonto

För att en leverantör ska kunna rapportera incidenter krävs att leverantören har tillgång till minst ett incidentrapporteringskonto. För att MSB ska kunna upprätta konton vissa uppgifter från leverantören.

4 §

En leverantör ska utan dröjsmål och på anvisat sätt ansöka hos Myndigheten för samhällsskydd och beredskap om att få tilldelat ett incidentrapporteringskonto genom att anmäla en kontaktperson och ansvarig för incidentrapporteringskontot.

Uppgifterna nedan ska lämnas i ansökan.

1. För- och efternamn.
2. E-postadress.
3. Mobiltelefonnummer.
4. Organisation.
5. Organisationsnummer.

Uppgifterna ska hållas uppdaterade.

5 §

Leverantören ska på anvisat sätt aktivera ett incidentrapporterings-konto hos Myndigheten för samhällsskydd och beredskap.

Detta innebär att leverantören så snart möjligt efter att ha konstaterat att den omfattas av NIS-regleringen ska ansöka om ett konto hos MSB för att kunna rapportera en incident. För att använda det incidentrapporteringsverktyg som MSB tillhandahåller behöver leverantören ha aktiverat ett incidentrapporteringskonto innan rapportering sker.

MSB kommer att kontrollera identiteten och behörigheten hos den som är utpekad kontaktperson. Denna kontaktperson kommer att intyga att utpekade incidentrapportörer är behöriga att rapportera incidenter å leverantörens vägnar.

Incidentrapportören kan vara kontaktpersonen själv eller kan vara en eller flera personer hos leverantörens personal, hos konsult eller underleverantör beroende på hur man har organiserat sin incidentrapporteringsprocess.

MSB skapar incidentrapporteringskonton och utfärdar certifikat för varje person som ska ha ett sådant konto.

För mer information om ansökan, se msb.se.

4.2 Hur rapportering ska ske

6 §

Incidenter ska rapporteras till Myndigheten för samhällsskydd och beredskap via anvisade kontaktvägar.

Den som är leverantör av en digital tjänst är ansvarig för att rapportera incidenter. Hur rapportering utförs omfattas av tillsyn.

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 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 med hjälp av sina interna processer upptäcka incidenter[2]. Dessutom bör interna processerna tydliggöra hur arbete ska ske med att identifiera vilka incidenter som är rapporteringspliktiga enligt genomförandeförordningen.

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 processer 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 tillsynsmyndigheten.

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 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.

[2] Enligt krav i art. 2 p. 2 genomförandeförordningen.

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 4.1 och 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)3 ska säkerhetshotande händelser och verksamhet skyndsamt anmälas till Säkerhetspolisen respektive Försvarsmakten. Sådana incidenter ska inte rapporteras till MSB.

8 § p. 2

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.

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

8 § 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.

8 § p. 6

En beskrivning av inträffad incident, utifrån

a) hur störningen upptäcktes,

b) dess påverkan för den digitala tjänsten,

c) användare som påverkas av störningen, samt

d) geografiskt område som påverkas.

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.

8 § p. 7
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

8 § p. 8
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.

8 § p. 9
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.

8 § p. 10

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 säkerhetsaspekter bör en grundorsaksanalys alltid ingå i.

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.

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.

9 §

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.