MSBFS
Remissutgåva

Förslag till Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 9, 13 och 14 §§ förordning (2018:1175) om informationssäkerhet för samhällsviktiga tjänster och digitala tjänster.

1 kap. Inledande bestämmelser

Tillämpningsområde

1 § Denna författning innehåller bestämmelser om hur leverantörer av samhällsviktiga tjänster enligt Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:xx) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster ska rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller, enligt förordning (2018:1175) om informationssäkerhet för samhällsviktiga tjänster och digitala tjänster.

2 § Skyldigheten att rapportera omfattar även incidenter som inträffar i informationshantering som har utkontrakterats till extern aktör.

Begreppsförklaringar

3 § De uttryck som förklaras i 2 § lag (2018:1174) om informationssäkerhet för samhällsviktiga tjänster och digitala tjänster har samma innebörd i denna författning.

4 § I denna författning avses med

kontinuitet i samhällsviktig tjänst	Förmåga hos leverantören att i samband med en störning i den samhällsviktiga tjänsten fortsätta tillhandahålla varor eller tjänster i en i förväg accepterad kvalitet och omfattning.
leverantör	En organisation som uppfyller kraven i Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:xxx) om kriterier för samhällsviktiga tjänster.

Systemviktiga finansiella infrastrukturföretag	- Värdepapperscentraler enligt lag (1998:1479) om värdepapperscentraler och kontoföringar av finansiella instrument - Centrala motparter enligt definitionen i artikel 2 punkt 1 i Europarparlamentets och rådets förordning 648/2012/EU om OTC-derivat, centrala motparter och transaktionsregister. - Clering organisationer för massbetalningar enligt lag (2007:528) om värdepappersmarknaden

2 kap. Rapportering

Hur rapportering ska ske

1 § Rapport ska lämnas till Myndigheten för samhällsskydd och beredskap via anvisade kontaktvägar.

Snarast efter anmälan till tillsynsmyndigheten enligt 23 § lag (2018:1174) om informationssäkerhet för samhällsviktiga tjänster och digitala tjänster ska leverantören på anvisat sätt upprätta ett incidentrapporteringskonto hos Myndigheten för samhällsskydd och beredskap i enlighet med 2 kap. 2 § Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS2018:xxx) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster.

När rapportering ska ske

2 § Leverantören ska utan onödigt dröjsmål, dock senast inom sex timmar från det att leverantören har identifierat en incident som rapporteringspliktig, notifiera Myndigheten för samhällsskydd och beredskap och redovisa 3 § punkt 1-8 utifrån en initial bedömning.

Leverantören ska utan onödigt dröjsmål, dock senast inom 24 timmar från det att leverantören har identifierat en incident som rapporteringspliktig, komplettera 3 § punkt 1-8 samt redovisa punkt 9.

Leverantören ska inom fyra veckor från det första rapporteringstillfället redovisa 3 § punkt 10 samt vid behov ändra eller komplettera punkt 1-9.

Innehåll i rapport

3 § En rapport ska innehålla följande information

1. Leverantörens namn samt organisationsnummer.
2. Kontaktuppgifter till utsedd kontaktperson för incidenten.
3. Berörd samhällsviktig tjänst.
4. 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 nätverks- och informationssystem återgick till normaldrift,
   c) händelseförlopp,
   d) hanteringen av incidenten, samt
   e) typ, orsak och konsekvenser.
5. Om incidenten bedöms ha fått konsekvenser inom andra medlemsstater inom EU.
6. Om incidenten har påverkat andra leverantörer och i så fall på vilket sätt.
7. Namn och organisationsnummer samt kontaktuppgifter till extern aktör dit informationshantering har utkontrakterats i det fall incidenten inträffat hos den externa aktören.
8. En beskrivning av incidentens inverkan på den samhällsviktiga tjänsten, utifrån
   a) tidpunkt för när störningen i tjänsten inträffade samt när och hur den upptäcktes,
   b) om störningen i tjänsten fortfarande pågår eller tidpunkt för när den upphörde alternativt förväntas upphöra,
   c) en beskrivning av hur tjänsten har störts och konsekvenser av störningen,
   d) användare som påverkas av störningen, samt
   e) vilket geografiskt område som påverkas.
9. Planerade åtgärder för att minimera följderna av incidenten.
10. Vidtagna och planerade åtgärder för att förhindra upprepning av liknande incidenter.

4 § Om den rapporterande leverantören inom ett år från det att incidenten har slutrapporterats konstaterar att tidigare lämnade uppgifter enligt 3 § är missvisande eller felaktiga ska leverantören så snart som möjligt meddela de nya uppgifterna till Myndigheten för samhällsskydd och beredskap.

3 kap. Rapporteringspliktiga incidenter inom energi

1 § Leverantörer inom el ska rapportera incidenter som har betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten. Med betydande inverkan avses i denna bestämmelse

1. leveransavbrott i minst två timmar, eller
2. att styrning och övervakning av stamnätstjänst, regionnätstjänst eller elproduktion inte har kunnat genomföras under två timmar.

2 § Leverantörer inom gas ska rapportera incidenter som har betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten. Med betydande inverkan avses i denna bestämmelse

1. leveransavbrott i minst två timmar, eller
2. genom att styrning och övervakning inom ramen för systemansvarstjänst inte har kunnat genomföras under två timmar.

3 § Leverantörer inom olja i form av flytande drivmedel och bränslen ska rapportera incidenter som har betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten. Med betydande inverkan avses i denna bestämmelse

1. leveransavbrott i minst två timmar, eller
2. att styrning och övervakning av ledningar, överföring och distributionsnätverk inte har kunnat genomföras under två timmar.

4 kap. Rapporteringspliktiga incidenter inom transport

1 § Leverantörer inom transport ska rapportera incidenter som har betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten. Med betydande inverkan avses i denna bestämmelse

1. att störningen i tjänsten varar i en timme eller mer och kan antas påverka
   a) 1000 användare eller fler, eller
   b) ett sammanhängande geografiskt område om 10 000 km^2 eller mer, eller
2. att störningen i tjänsten varar i minst två timmar.

5 kap. Rapporteringspliktiga incidenter inom bankverksamhet

1 § Leverantörer inom bankverksamhet ska rapportera incidenter som har betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten. Med betydande inverkan avses i denna bestämmelse

1. att transaktioner inte kan eller sannolikt inte kommer att kunna initieras eller behandlas för mer än 25 % av leverantörens normala antal transaktioner, eller
2. att transaktioner inte kan eller sannolikt inte kommer att kunna initieras eller behandlas för mer än 25 % av leverantörens användare, eller
3. oplanerade avbrott vars sammanlagda tid under en 24-timmars period överstiger 3 timmar.

6 kap. Rapporteringspliktiga incidenter inom finansmarknadsinfrastruktur

1 § Leverantörer inom finansmarknads-infrastruktur ska rapportera incidenter som har betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten. Med betydande inverkan avses i denna bestämmelse

1. avbrott som överstiger två timmar, eller
2. avvikelse från sådan konnektivitet som avses i art. 11 punkt 5 Kommissionens delegerade förordning 2017/584, eller
3. störning som påverkar systemviktiga finansiella infrastrukturföretag.

7 kap. Rapporteringspliktiga incidenter inom hälso- och sjukvård

1 § Leverantörer inom hälso- och sjukvård ska rapportera incidenter som har betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten. Med betydande inverkan avses i denna bestämmelse

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

8 kap. Rapporteringspliktiga incidenter inom leverans och distribution av dricksvatten

1 § Leverantörer inom leverans och distribution av dricksvatten ska rapportera incidenter som har betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten. Med betydande inverkan avses i denna bestämmelse

1. leveransavbrott i minst två timmar, eller
2. att styrning och övervakning av tjänsten inte har kunnat genomföras under en tidsperiod om minst två timmar.

9 kap. Rapporteringspliktiga incidenter inom digital infrastruktur

1 § Leverantörer inom digital infrastruktur ska rapportera incidenter som har betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten. Med betydande inverkan avses i denna bestämmelse

1. att en toppdomäns namnservertjänst har en tillgänglighet på mindre än 100 procent,
2. förlorad konfidentialitet eller riktighet i lagrade, överförda eller behandlade data för en toppdomäns namnservertjänst som 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 för en rekursiv namnservertjänst som 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 för en auktoritativ namnservertjänst som berört fler än 2 500 domännamn.

Allmänna råd

MSBFS
Remissutgåva

Förslag till Myndigheten för samhällsskydd och beredskaps allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster

Följande allmänna råd ansluter till Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster. Termer och uttryck som används i föreskrifterna har samma betydelse här.

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.

1 kap. Inledande bestämmelser

Tillämpningsområde

Har avtal ingåtts med extern aktör innan denna författning har trätt i kraft bör leverantören analysera de krav som ställts på informationssäkerhet och genomföra en riskbedömning. Riskbedömningen bör ligga till grund för framtida hantering av avtalen.

2 kap. Rapportering

Hur rapportering ska ske

En leverantör bör inför rapportering kontrollera vilka de anvisade kontaktvägarna är på www.msb.se.

När rapportering ska ske

Rutiner för incidentrapportering bör anslutas till de rutiner för intern incidenthantering som leverantören ska ha på plats enligt rutiner för intern incidenthantering i enlighet med 11 § Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:xxx) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.

Innehåll i rapport

Kontaktuppgifter bör inkludera roll, telefonnummer och e-postadresser samt uppgift om tillgänglighet. Om inte uppgifter till kontaktperson finns, kan uppgifter till kontaktfunktion ges. Vid byte av kontaktperson eller kontaktfunktion bör uppgifterna uppdateras snarast.

En beskrivning av konsekvenser bör göras utifrån tillgänglighet, riktighet och konfidentialitet.

Vid identifiering av vilka åtgärder som planeras bör samtliga förhållanden som har bidragit till incidenten beaktas, inklusive grundorsaken.