



TREDJE SKEDETS RAPPORTERING:

Utvärdering och förebyggande åtgärder

Skedet ska rapporteras inom 4 veckor fr.o.m. det att rapporteringsplikt har konstaterats.

Uppgifter som omfattas av sekretess för skydd av rikets säkerhet ska rapporteras enligt särskild ordning.

I Skede 3 ska enbart sådana personuppgifter anges som är nödvändiga för att uppnå syftet med skedet. Syftet med insamlingen av uppgifter i Skede 3 är att MSB och den ansvariga tillsynsmyndigheten ska få en bild av:

1. hur incidenten respektive störningen upptäcktes,
2. vilka ekonomiska konsekvenser incidenten respektive störningen har medfört för leverantören,
3. hur förberedd leverantören var på att incidenten respektive störningen skulle kunna inträffa,
4. vilka hot och sårbarheter som dels bidrog till att incidenten kunde inträffa, och dels bidrog till att incidenten kunde orsaka störningen, samt *hur* incidenten kunde orsaka störningen,
5. särskilda förebyggande åtgärder som genomför med anledning av incidenten respektive störningen.



Allmänt

Ange vilken digital tjänst som har drabbats av en störning:

(Vid inrapportering av Skede 1 och Skede 2 brevledes återkommer MSB via mejl med ärendets tilldelade nummer. Ange det numret här. Listan på typer av digitala tjänster finns i vägledningen till incidentrapporteringsformuläret på www.msb.se.)

Typ av tjänst	Namnet på den störda tjänsten
Namnet på leverantören av tjänsten	Organisationsnummer
Incidentnummer:	

Rapporterar ni som leverantör av en digital tjänst eller på uppdrag av leverantören?

Vi rapporterar som leverantör av den störda tjänsten

Vi rapporterar på uppdrag av den ovan nämnda leverantören

(För mer information om hur frågorna ska förstås och kan besvaras, se vägledningen till incidentrapporteringsformuläret på www.msb.se.)

[FRIVILLIG FRÅGA – SE NEDERSTA SVARSALTERNATIVET]

46. Har, eller kommer, information om det inträffade rapporteras till någon annan myndighet än MSB?

Status	Rapporteringen sker till	Regelverk	Diarienummer

Ja, det är:

Nej

Okänt

Frågan är frivillig och vi väljer att inte svara

Upptäckten av incidenten respektive störningen

(För mer information om hur frågorna ska förstås och kan besvaras, se vägledningen till incidentrapporteringsformuläret på www.msb.se.)

47. Vem eller vad var först med att uppmärksamma er organisation om incidenten?

Er organisation	Extern, av er kontrakterad, organisation	Myndighet	Annan organisation	Andra	
<input type="checkbox"/> Personal	<input type="checkbox"/> Personal	<input type="checkbox"/> Personal	<input type="checkbox"/> Personal	<input type="checkbox"/> Media	<input type="checkbox"/> Okänt
<input type="checkbox"/> Tekniskt detekteringssystem	<input type="checkbox"/> Tekniskt detekteringssystem	<input type="checkbox"/> Tekniskt detekteringssystem	<input type="checkbox"/> Tekniskt detekteringssystem	<input type="checkbox"/> Privatpersoner	
<input type="checkbox"/> Annat	<input type="checkbox"/> Annat	<input type="checkbox"/> Annat	<input type="checkbox"/> Annat	<input type="checkbox"/> Annat	

48. Hur upptäcktes incidenten?

Uppgifter som omfattas av sekretess för skydd av rikets säkerhet ska rapporteras enligt särskild ordning.

Ange endast sådana personuppgifter som är nödvändiga utifrån rapporteringsskedets syftesbeskrivning.

För mer information om sekretess och personuppgiftsbehandling, se vägledningen till incidentrapporteringsformuläret på www.msb.se.



49. Vem eller vad var först med att uppmärksamma er organisation om störningen i den digitala tjänsten?

Er organisation	Extern, av er kontrakterad, organisation	Myndighet	Annan organisation	Andra	<input type="checkbox"/> Okänt
<input type="checkbox"/> Personal	<input type="checkbox"/> Personal	<input type="checkbox"/> Personal	<input type="checkbox"/> Personal	<input type="checkbox"/> Media	
<input type="checkbox"/> Tekniskt detekteringssystem	<input type="checkbox"/> Tekniskt detekteringssystem	<input type="checkbox"/> Tekniskt detekteringssystem	<input type="checkbox"/> Tekniskt detekteringssystem	<input type="checkbox"/> Privatpersoner	
<input type="checkbox"/> Annat	<input type="checkbox"/> Annat	<input type="checkbox"/> Annat	<input type="checkbox"/> Annat	<input type="checkbox"/> Annat	

50. Hur upptäcktes störningen i den digitala tjänsten?

Uppgifter som omfattas av sekretess för skydd av rikets säkerhet ska inte rapporteras i verktyget. Läs mer [här](#).

Ange endast sådana personuppgifter som är nödvändiga utifrån rapporteringsskedets syftesbeskrivning.

För mer information om sekretess och personuppgiftsbehandling, se vägledningen till incidentrapporteringsformuläret på www.msb.se.

Ekonomiska konsekvenser

(För mer information om hur frågorna ska förstås och kan besvaras, se vägledningen till incidentrapporteringsformuläret på www.msb.se.)

51. Hur mycket förväntas incidenten respektive störningen kosta för er organisation?

	Kostnad i SEK	Säker bedömning	Osäker bedömning	Kan ej bedöma
Incidenten bedöms som minst kosta		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Incidenten bedöms som mest kosta		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Incidenten bedöms mest sannolikt kosta		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Störningen bedöms som minst kosta		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Störningen bedöms som mest kosta		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Störningen bedöms mest sannolikt kosta		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

52. Har er organisation slutgiltigt fastställt...

Incidentens kostnader?	<input type="checkbox"/> Ja	<input checked="" type="checkbox"/> Nej	<input type="checkbox"/> Okänt
Störningens kostnader?	<input type="checkbox"/> Ja	<input checked="" type="checkbox"/> Nej	<input type="checkbox"/> Okänt

53. Hur täcker er organisation kostnaderna för incidenten?

Posten	Procentandel av totalkostnaden som hämtas från posten	Säker bedömning	Osäker bedömning	Kan ej bedöma
Fasta medel från budget för incidenthantering		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rörliga medel från budget för incidenthantering		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Åskade medel från annan budget		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lån		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Försäkring		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Annan källa		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

54. Hur täcker er organisation kostnaderna för störningen i den digitala tjänsten?

Posten	Procentandel av totalkostnaden som hämtas från posten	Säker bedömning	Osäker bedömning	Kan ej bedöma
Fasta medel från budget för incidenthantering		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rörliga medel från budget för incidenthantering		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Äskade medel från annan budget		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lån		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Försäkring		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Annan källa		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Tidigare vidtagna åtgärder för att hantera liknande incidenter

(För mer information om hur frågorna ska förstås och kan besvaras, se vägledningen till incidentrapporteringsformuläret på www.msb.se.)

55. Hade liknande incidenter i nätverk eller informationssystem inträffat före den aktuella incidenten? Ja Nej Okänt

[BESVARAS ENDAST OM "JA" VALDES I FRÅGA 55]

56. Hade en störning någon gång uppstått i den digitala tjänsten i samband med att den eller de incidenterna inträffade? Ja Nej Okänt**57. Hade liknande störningar i den digitala tjänsten inträffat före den aktuella störningen?** Ja Nej Okänt

58. Hade liknande incidenter i nätverk eller informationssystem identifierats och analyserats i en riskanalys hos organisationen vid tiden för den aktuella incidenten?

Ja

Nej

Okänt

[BESVARAS ENDAST OM "JA" VALDES I FRÅGA 58]

59. Hade den analysen inkluderat möjligheten att incidenten skulle kunna orsaka den aktuella störningen i den digitala tjänsten?

Ja

Nej

Okänt

60. Hade liknande störningar i den digitala tjänsten identifierats och analyserats i en riskanalys hos organisationen vid tiden för den aktuella störningen?

Ja

Nej

Okänt

61. Hade er organisation en kontinuitetsplan som kan användas för liknande incidenter vid tidpunkten för den aktuella incidenten?

Ja

Nej

Okänt

[BESVARAS ENDAST OM "JA" VALDES I FRÅGA 61]

62. Aktiverade er organisation kontinuitetsplanen för att hantera den här incidenten?

Ja

Nej

Okänt

63. Hade er organisation en kontinuitetsplan som kan användas för liknande störningar i den digitala tjänsten vid tidpunkten för den aktuella incidenten?

Ja

Nej

Okänt

[BESVARAS ENDAST OM "JA" VALDES I FRÅGA 63]

64. Aktiverade er organisation kontinuitetsplanen för att hantera den här störningen i den digitala tjänsten? Ja Nej Okänt**65. Har er organisation ett mål för genomsnittlig återställningstid vid incidenter i nätverk eller informationssystem?***(I fältet tidsenhet kan exempelvis minuter, timmar, dagar, etc. anges.)*

	Antal	Tidsenhet
<input type="checkbox"/> Ja, det finns ett mål för den typ av incident som rapporteras här:		
<input type="checkbox"/> Ja, det finns ett generellt mål för incidenter:		
<input type="checkbox"/> Nej		
<input type="checkbox"/> Okänt		

66. Har er organisation ett mål för genomsnittlig återställningstid vid störningar i den digitala tjänsten?*(I fältet tidsenhet kan exempelvis minuter, timmar, dagar, etc. anges.)*

	Antal	Tidsenhet
<input type="checkbox"/> Ja, det finns ett mål för den typ av störning som rapporteras här:		
<input type="checkbox"/> Ja, det finns ett generellt mål för störningar:		
<input type="checkbox"/> Nej		
<input type="checkbox"/> Okänt		

67. Har er organisation ett mål för maximal återställningstid vid incidenter i nätverk eller informationssystem?*(I fältet tidsenhet kan exempelvis minuter, timmar, dagar, etc. anges.)*

	Antal	Tidsenhet
<input type="checkbox"/> Ja, det finns ett mål för den typ av incident som rapporteras här:		
<input type="checkbox"/> Ja, det finns ett generellt mål för incidenter:		
<input type="checkbox"/> Nej		
<input type="checkbox"/> Okänt		

68. Har er organisation ett mål för maximal återställningstid vid störningar i den digitala tjänsten?

(I fältet tidsenhet kan exempelvis minuter, timmar, dagar, etc. anges.)

	Antal	Tidsenhet
<input type="checkbox"/> Ja, det finns ett mål för den typ av störning som rapporteras här:		
<input type="checkbox"/> Ja, det finns ett generellt mål för störningar:		
<input type="checkbox"/> Nej		
<input type="checkbox"/> Okänt		

69. Har er organisation ett mål för genomsnittlig tid mellan incidenter i nätverk eller informations-system?

(I fältet tidsenhet kan exempelvis minuter, timmar, dagar, etc. anges.)

	Antal	Tidsenhet
<input type="checkbox"/> Ja, det finns ett mål för den typ av störning som rapporteras här:		
<input type="checkbox"/> Ja, det finns ett generellt mål för störningar:		
<input type="checkbox"/> Nej		
<input type="checkbox"/> Okänt		

70. Har er organisation ett mål för genomsnittlig tid mellan störningar i den digitala tjänsten?

(I fältet tidsenhet kan exempelvis minuter, timmar, dagar, etc. anges.)

	Antal	Tidsenhet
<input type="checkbox"/> Ja, det finns ett mål för den typ av störning som rapporteras här:		
<input type="checkbox"/> Ja, det finns ett generellt mål för störningar:		
<input type="checkbox"/> Nej		
<input type="checkbox"/> Okänt		

Hot, sårbarheter och hur störningen orsakades

(För mer information om hur frågorna ska förstås och kan besvaras, se vägledningen till incidentrapporteringsformuläret på www.msb.se.)

71. Har ni identifierat några hot med koppling till incidenten? Ja Nej Okänt



Hot

[UNDERAVSNITTET HOT FYLLS ENBART I OM "JA" VALDES I FRÅGA 71]

Flera hot kan anges genom att fylla i pdf-dokumentet Hot som finns tillsammans med det här formuläret på www.msb.se.

Ange endast faktiskt förekommande hot. Hot som skulle kunna förekomma, men som ni inte vet om de förekommer, ska inte anges.

72. Vilken typ av hot är det?

Något som orsakar eller bidrar till att orsaka att...

Sådana här incidenter inträffar

Konsekvenserna av sådana här incidenter förvärras

Sådana här störningar inträffar när sådana här incidenter inträffar

Konsekvenserna av sådana här störningar förvärras

73. Beskriv hotet:

Uppgifter som omfattas av sekretess för skydd av rikets säkerhet ska rapporteras enligt särskild ordning.

Ange endast sådana personuppgifter som är nödvändiga utifrån rapporteringskedets syftesbeskrivning.

För mer information om sekretess och personuppgiftsbehandling, se vägledningen till incidentrapporteringsformuläret på www.msb.se.

74. Har ni identifierat några sårbarheter med koppling till incidenten?

Ja

Nej

Okänt



Sårbarheter

[UNDERAVSNITTET SÅRBARHETER FYLLS ENBART I OM "JA" VALDES I FRÅGA 74]

Flera hot kan anges genom att fylla i pdf-dokumentet Sårbarheter som finns tillsammans med det här formuläret på www.msb.se.

Ange endast sådant som ni anser att er organisation saknar.

75. Vilken typ av sårbarhet är det?

Avsaknad av något som skulle kunna...

Förhindra eller bidra till att förhindra att sådana här incidenter inträffar

Förhindra eller mildra eller bidra till att förhindra eller mildra konsekvenserna av sådana här incidenter

Förhindra eller bidra till att förhindra att sådana här störningar inträffar när sådana här incidenter inträffar

Förhindra eller mildra eller bidra till att förhindra eller mildra konsekvenserna av sådana här störningar

76. Beskriv sårbarheten:

Uppgifter som omfattas av sekretess för skydd av rikets säkerhet ska rapporteras enligt särskild ordning.

Ange endast sådana personuppgifter som är nödvändiga utifrån rapporteringsskedets syftesbeskrivning.

För mer information om sekretess och personuppgiftsbehandling, se vägledningen till incidentrapporteringsformuläret på www.msb.se.



77. Beskriv varför och hur incidenten orsakade störningen:

Uppgifter som omfattas av sekretess för skydd av rikets säkerhet ska rapporteras enligt särskild ordning.

Ange endast sådana personuppgifter som är nödvändiga utifrån rapporteringskedets syftesbeskrivning.

För mer information om sekretess och personuppgiftsbehandling, se vägledningen till incidentrapporteringsformuläret på www.msb.se.

78. Genomför ni särskilda förebyggande åtgärder med anledning av incidenten eller störningen?

Flera åtgärder kan anges.

Ja

Nej

Okänt



Förebyggande åtgärder

[AVSNITTET FÖREBYGGANDE ÅTGÄRDER FYLLES ENBART I OM "JA" VALDES I FRÅGA 78 (D.V.S. OM NI GENOMFÖR SÄRSKILDA HANTERINGÅTGÄRDER)]

Flera åtgärder kan anges genom att fylla i pdf-dokumentet Förebyggande åtgärder som finns tillsammans med det här formuläret på www.msb.se.

79. Namnge åtgärden:

80. Vad förebyggs med åtgärden?

- Incidenten | Störningen | Störningens konsekvenser

81. Vilken status har åtgärden?

- Identifierad | Planerad | Pågående
 Genomförd | Okänt

82. Vilken är den avsedda effekten med åtgärden?

Att förebygga hot – Ta bort eller förändra något som...

- | | |
|---|---|
| <input type="checkbox"/> Kan orsaka att incidenten inträffar | <input type="checkbox"/> Kan förvärra incidentens konsekvenser |
| <input type="checkbox"/> Orsakar eller bidrar till att orsaka att sådana här störningar inträffar när en sådan här incident inträffar | <input type="checkbox"/> Orsakar eller bidrar till att orsaka att konsekvenserna av sådana här störningar förvärras |

Att förebygga sårbarheter – Införskaffa eller införa något som...

- | | |
|---|--|
| <input type="checkbox"/> Kan förhindra att incidenten inträffar | <input type="checkbox"/> Kan förhindra eller mildra incidentens konsekvenser |
| <input type="checkbox"/> Skulle kunna förhindra att sådana här störningar inträffar när en sådan här incident inträffar | <input type="checkbox"/> Skulle kunna förhindra eller mildra konsekvenserna av sådana här störningar |
| <input type="checkbox"/> Annan avsedd effekt | <input type="checkbox"/> Okänd avsedd effekt |

83. Hur mycket bedöms åtgärden kosta?

	Kostnad i SEK	Säker bedömning	Osäker bedömning	Kan ej bedöma
Åtgärden bedöms som minst kosta		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Åtgärden bedöms som mest kosta		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Åtgärden bedöms mest sannolikt kosta		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



84. Beskriv vad åtgärden är och går ut på:

Uppgifter som omfattas av sekretess för skydd av rikets säkerhet ska rapporteras enligt särskild ordning.

Ange endast sådana personuppgifter som är nödvändiga utifrån rapporteringsskedets syftesbeskrivning.

För mer information om sekretess och personuppgiftsbehandling, se vägledningen till incidentrapporteringsformuläret på www.msb.se.



FÖRHANDSGRANSKNING

Skede 3

MSB uppmanar er att se över (och vid behov gå tillbaka och justera) uppgifterna en sista gång för att säkerställa att:

- Information som omfattas av sekretess för skydd av rikets säkerhet inte inkluderats. Om sådan information har inkluderats så ska rapporteringen antingen ske enligt särskild ordning eller så ska informationen som angetts i fritextfälten justeras.
- Personuppgifter som inte är nödvändiga att förmedla till MSB och den ansvariga tillsynsmyndigheten inte har inkluderats.

Syftesbeskrivning för Skede 3

I Skede 3 ska enbart sådana personuppgifter anges som är nödvändiga för att:

1. hur incidenten respektive störningen upptäcktes,
2. vilka ekonomiska konsekvenser incidenten respektive störningen har medfört för leverantören,
3. hur förberedd leverantören var på att incidenten respektive störningen skulle kunna inträffa,
4. vilka hot och sårbarheter som dels bidrog till att incidenten kunde inträffa, och dels bidrog till att incidenten kunde orsaka störningen, samt *hur* incidenten kunde orsaka störningen,
5. särskilda förebyggande åtgärder som genomför med anledning av incidenten respektive störningen

Sekretessbedömning för Skede 3

Bedömer ni att den information som ni har lämnat i det här skedets rapportering omfattas av sekretess?

(Det är viktigt att notera att MSB och den ansvariga tillsynsmyndigheten vid ett utlämningsärende kommer att göra en egen bedömning av eventuella sekretessgrunder. I det kommer er bedömning beaktas, men inga garantier kan lämnas om att respektive myndighets bedömning överensstämmer med er.)

<input type="checkbox"/> Ja, OSL 18 kap. 8 § (Säkerhets- eller bevakningsåtgärd)	<input type="checkbox"/> Ja, OSL 18 kap. 13 § (Risk- och sårbarhetsanalyser m.m.)	<input type="checkbox"/> Ja, OSL 19 kap. 1 § (Affärs- och driftförhållanden)
<input type="checkbox"/> Ja, OSL 21 kap. 7 § (Behandling i strid med dataskyddsregleringen)	<input type="checkbox"/> Ja, annan sekretess	<input type="checkbox"/> Nej
		<input type="checkbox"/> Kan ej bedöma



[BESVARAS ENDAST OM DEN FÖREGÅENDE FRÅGAN HAR BESVARATS JAKANDE]

Vänligen ange vilken information ni avser omfattas av vilken sekretess, och motivera er bedömning: