Myndigheten för civilt försvar

NATIONELLT CYBERSÄKERHETSCENTER
En del av FRA

Vägledning

Incidentrapportering och informationsskyldighet

Denna vägledning ger stöd vid tillämpningen av föreskrifter om incident-rapportering och informationsskyldighet enligt cybersäkerhetslagen.

Incidentrapportering och informationsskyldighet

Myndigheten för civilt försvar
651 81 Karlstad

Foto omslag: Myndigheten för civilt försvar, Plattform
Produktion: Advant

Publikationsnummer: MCF0175 – juni 2026
ISBN-nummer: 978-91-7927-773-4

Innehåll

Kapitel 1

Introduktion

1. Introduktion

Den 15 januari 2026 trädde cybersäkerhetslagen (2025:1506) i kraft. Cybersäkerhetslagen (CSL) genomför NIS2-direktivet[1] i svensk rätt och ersätter därmed den tidigare NIS-lagen, lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174). Cybersäkerhetslagen syftar till att höja den generella cybersäkerhetsnivån i Sverige och säkra kontinuiteten inom 18 utpekade sektorer som bedöms vara viktiga för samhällets funktion och ekonomi. För att nå dit ställer lagen skärpta säkerhetskrav på de organisationer som omfattas. I lagen benämns dessa organisationer som **verksamhetsutövare**.

CSL innehåller bland annat krav på att verksamhetsutövare ska rapportera betydande incidenter. Enligt lagen ska verksamhetsutövare rapportera incidenter som anses betydande om de har, eller riskerar att få, allvarliga konsekvenser för verksamhetsutövaren eller för andra juridiska eller fysiska personer. Betydande incidenter ska rapporteras i flera skeden enligt specificerade tidsgränser.

CSL innehåller även bestämmelser om att verksamhetsutövare ska informera mottagare av tjänster om betydande incidenter som sannolikt inverkar negativt på tillhandahållandet av tjänster. Verksamhetsutövare förväntas även informera mottagare om betydande cyberhot, inklusive vilka motåtgärder som mottagare kan vidta i syfte att minimera risken för att cyberhotet realiseras.

Myndigheten för civilt försvar har mot bakgrund av dessa krav i CSL tagit fram föreskrifter om incidentrapportering och informationsskyldighet. Myndigheten för civilt försvars föreskrifter om incidentrapportering och informationsskyldighet för väsentliga och viktiga verksamhetsutövare (MCFFS 2026:8), hädanefter CSL-föreskrifterna, träder i kraft den 1 juli 2026.

Från och med den 1 juli 2026 går Myndigheten för civilt försvars centrala cyberverksamhet över till Nationellt cybersäkerhetscenter (NCSC) vid Försvarets radioanstalt (FRA). NCSC tar i samband med det över den sammanhållande rollen för CSL-regleringen. Med anledning av detta övergår även mandatet att meddela föreskrifter om incidentrapportering och informationsskyldighet enligt cybersäkerhetsförordningen till FRA. Detta innebär också att verksamhetsutövare ska rapportera in betydande incidenter till NCSC från och med 1 juli 2026.

Not 1. Europaparlamentets och rådets direktiv 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148.

1.1 Syfte och målgrupp

Den här vägledningen riktar sig till verksamhetsutövare som omfattas av skyldigheterna om rapportering av betydande incidenter samt informationsskyldighet enligt CSL. Den syftar till att stödja verksamhetsutövare med tillämpningen av CSL-föreskrifterna. Vägledningen innehåller för detta syfte beskrivningar och exempel som avser att illustrera vilka typer av incidenter som ska rapporteras, samt hur krav på informationsskyldighet kan uppfyllas. Vägledningen utgör också ett stöd för verksamhetsutövare vid användningen av Myndigheten för civilt försvars rapporteringsverktyg, (för mer information, se bilaga 1). Den inkluderar en närmare beskrivning av rapporteringsprocessen samt redogör för hur verksamhetsutövare ska gå till väga när de rapporterar betydande incidenter.

Vissa statliga myndigheter omfattas av incidentrapporteringsplikt både enligt CSL och förordningen (2022:524) om statliga myndigheters beredskap (BF). I syfte att harmonisera och förenkla rapporteringsplikten för de som omfattas av båda regelverken har Myndigheten för civilt försvars föreskrifter om rapportering av it-incidenter för statliga myndigheter (MCFFS 2026:7) uppdaterats (hädanefter BF-föreskrifterna). Vägledningen riktar sig även till de utövare som omfattas av både CSL och BF. Hur dessa verksamhetsutövare ska förhålla sig till rapporteringsplikten redogörs också närmare för i denna vägledning.

Beskrivningarna ska inte betraktas som förhandsbesked om vad tillsynsmyndigheterna kan komma att bedöma i ett enskilt ärende. Medan krav i föreskrifter är bindande utgör vägledningen stöd vid tillämpning av reglerna och är inte bindande.

Vägledningen är ett levande dokument som kommer att uppdateras över tid.

1.2 Föreskriftsmandat

Myndigheten för civilt försvar har tagit fram CSL-föreskrifterna med stöd av 38 § p. 6 och 39 § p. 2–3 cybersäkerhetsförordningen (2025:1507). CSL-föreskrifterna syftar till att förtydliga kraven om incidentrapporteringsplikt och informationsskyldighet enligt CSL. Föreskrifterna innehåller bestämmelser om:

- rapportering av betydande incidenter, inkluderande (2 kap. CSL-föreskrifterna)
  - hur rapporteringen av betydande incidenter utförs, och
  - vilka uppgifter som ska rapporteras
- vad som utgör en betydande incident (3 kap. och 4 kap. CSL-föreskrifterna), samt
- informationsskyldighet vid betydande incidenter och betydande cyberhot (5 kap. i CSL-föreskrifterna).

Rätten att utfärda föreskrifter om vad som utgör en betydande incident samt informationsskyldigheten delas med Post- och telestyrelsen (PTS). PTS ansvarar för sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster (mellan företag), rymden och post- och budtjänster. När det gäller verksamhetsutövare inom sektorerna digitala leverantörer, förvaltning av IKT-tjänster och digital infrastruktur[2] omfattas dessa av bestämmelser om vad som utgör en betydande incident enligt EU-kommissionens genomförandeförordning.[3] För mer information om rapporteringsplikten och informationsskyldigheten för dessa sektorer, besök PTS webbplats.[4]

Från och med 1 juli 2026 har FRA vidare rätt att utfärda föreskrifter om rapportering av it-incidenter för statliga myndigheter med stöd av 27 § p. 2 förordningen (2022:524) om statliga myndigheters beredskap. I syfte att harmonisera kraven med de föreskrifter som meddelas enligt CSL har myndigheten för civilt försvar reviderat tidigare föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8). Dessa upphör att gälla när de nya föreskrifterna om rapportering av it-incidenter för statliga myndigheter (MCFFS 2026:7) träder i kraft den 1 juli 2026. De upphävda föreskrifterna gäller dock fortfarande för it-incident som har identifierats och bedömts som rapporteringspliktig före ikraftträdandet.

Från och med den 1 juli 2026 tar FRA över föreskriftsrätten för bland annat incidentrapportering och informationsskyldighet enligt CSL samt incidentrapportering enligt BF från Myndigheten för civilt försvar. De föreskrifter som Myndigheten för civilt försvar har utfärdat gäller tillsvidare.

Not 2. Med undantag för tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster.

Not 3. EU-kommissionens genomförandeförordning 2024/2690 av den 17 oktober 2024 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster.

Not 4. Se Cybersäkerhetslagen och PTS ansvar (hämtad: 2026-06-03).

1.3 Incidentrapportering syftar till att stärka samhällets cybersäkerhet

Skyldigheten att rapportera betydande incidenter syftar till att öka förmågan att förebygga och hantera incidenter och minska deras konsekvenser för att kunna förbättra cybersäkerhetsarbetet i samhället – såväl nationellt som inom EU vid behov. Incidentrapporteringsskyldigheten bidrar till att stärka samhällets cybersäkerhet utifrån flera perspektiv.

Operativt stöd samt informationsgivning (i form av varningar) till samhället

Genom incidentrapporteringen kan den nationella CSIRT-enheten[5] bistå operativt och ge stöd till den drabbade aktören. Dessutom kan operativt stöd ges till sådana som drabbas av incidenten i förlängningen, såväl som sådana som skulle kunna drabbas av liknande incidenter. Vid behov kan informationsgivning, till exempel genom varningar, ske till allmänheten och till andra aktörer, både nationellt och inom EU. Exempelvis delas information med andra EU-medlemsstater genom CSIRT-nätverket.[6]

Regelbundna nationella lägesbilder till myndigheter, allmänheten och verksamhetsutövare

Genom incidentrapporteringsplikten får myndigheter med ansvar för cybersäkerhet och Sveriges säkerhet en bild över vad som händer i Sveriges cybermiljö och kan bedöma behov av åtgärder. Den sammantagna bilden möjliggör identifiering av avvikelser samt en samlad bild över till synes orelaterade händelser. Lägesbilden ligger till grund för beslutsfattande både inom myndigheterna och ytterst hos regeringen.

Stöd och rekommendationer

Genom incidentrapporteringsplikten kan ansvariga myndigheter ta fram och publicera stöd och rekommendationer till verksamhetsutövare i syfte att undvika liknande incidenter i framtiden, sprida erfarenheter och lärdomar men också identifiera förebyggande åtgärder mot vanligt förekommande incidenter.

Bidragande till forskning, utveckling och kompetensförsörjning

Genom incidentrapporteringsplikten identifierar ansvariga myndigheter typer av incidenter som verksamhetsutövare har särskilt svårt att hantera med de kunskaper, verktyg och den personal de har idag. Detta använder myndigheterna för att utforma och genomföra utlysningar om ny forskning eller utveckling, samt kompetensförsörjningsinsatser.

Not 5. CSIRT är en förkortning för ”Computer Security Incident Response Team”. Myndigheten för civilt försvar är Sveriges nationella CSIRT fram till den 30 juni 2026, därefter går det över till FRA.

Not 6. CSIRT-nätverket, som etablerades genom NIS-direktivet (EU) 2016/1148, är ett nätverk av nationellt utpekade CERT-funktioner för hantering av cyberincidenter.

Granskning av verksamhetsutövares efterlevnad av gällande krav på säkerhetsåtgärder samt incidentrapportering enligt CSL för ett säkrare cybersamhälle

Rapporteringsplikten enligt CSL utgör även ett viktigt underlag för tillsynsmyndigheterna som med hjälp av uppgifterna kan bedöma behov av tillsyn. Incidentrapporteringen bidrar till att tillsynsmyndigheterna kan säkerställa att verksamhetsutövare lever upp till gällande krav på säkerhetsåtgärder och ytterst att nätverks- och informationssystem är tillförlitliga och säkra. Tillsynsmyndigheterna kan även nyttja uppgifterna för att ta fram exempelvis sektorsspecifika analyser samt stöd riktade till verksamhetsutövare inom ramen för sin sektor eller för att planera tillsynsåtgärder framgent.

1.4 Hur vägledningen ska läsas

Kapitel	Innehåll	Målgrupp
1	Redogör för vägledningens och incidentrapporteringens syfte och föreskriftsmandat.	Samtliga verksamhetsutövare som omfattas av CSL och rapporterar betydande incidenter till FRA.
2	Redogör för centrala begrepp vid tillämpning av föreskrifterna.	Samtliga verksamhetsutövare som omfattas av CSL och rapporterar betydande incidenter till FRA.
3	Redogör för vad som utgör betydande incidenter (3–4 kap. CSL-föreskrifterna).	Verksamhetsutövare inom sektorerna energi, transporter, hälso- och sjukvård, dricksvatten, avloppsvatten, offentlig förvaltning, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion bearbetning och distribution av livsmedel, tillverkning samt forskning.
4	Redogör för hur rapporteringen av betydande incidenter ska gå till (2 kap. CSL-föreskrifterna).	Samtliga verksamhetsutövare som omfattas av CSL och rapporterar betydande incidenter till FRA.
5	Redogör för informationsskyldigheten vid betydande incidenter och cyberhot till mottagare av tjänsterna (5 kap. CSL-föreskrifterna).	Verksamhetsutövare inom sektorerna energi, transporter, hälso- och sjukvård, dricksvatten, avloppsvatten, offentlig förvaltning, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion bearbetning och distribution av livsmedel, tillverkning samt forskning.
Bilaga 1	Stöd vid ifyllande av rapporteringsformulär.	Samtliga verksamhetsutövare som omfattas av CSL och rapporterar betydande incidenter till FRA.
Bilaga 2	Checklista.	Samtliga verksamhetsutövare som omfattas av CSL och rapporterar betydande incidenter till FRA.
Bilaga 3	Lista över ansvariga tillsynsmyndigheter.	Samtliga verksamhetsutövare som omfattas av CSL och rapporterar betydande incidenter till FRA.

Kapitel 2

Centrala begrepp

2. Centrala begrepp

I det här kapitlet framgår centrala begrepp och definitioner vid tillämpning av reglerna om incidentrapportering och informationsskyldighet. CSL inför ett antal centrala uttryck inklusive definitioner av dessa. CSL-föreskrifterna inför också ett antal ytterligare, kompletterande uttryck inklusive deras definitioner. I tabellerna nedan redogörs för de centrala begreppen och deras betydelse, i vilka bestämmelser som begreppen används samt en kort kommentar om hur begreppet används i CSL-föreskrifterna. Det är viktigt att notera att CSL ersätter flera centrala uttryck som fanns i NIS-lagen.

Tabell 1. Begrepp och definitioner av relevans för incidentrapportering samt informationsskyldighet som framgår av cybersäkerhetslagen

Begrepp	Definition	Hänvisning i CSL-föreskrifterna	Hur begreppet används
Betydande cyberhot	Ett cyberhot ska anses vara betydande om det, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en verksamhetsutövares nätverks- och informationssystem eller användarna av verksamhetsutövarens tjänster genom att vålla betydande skada.	3 kap. 2 § p. 1, 3 kap. 4 § p. 1 3 kap. 7 § p. 1 (Generella rapporteringskriterier) 5 kap. 2 § (Informationsskyldighet till mottagare)	Om ett cyberhot är betydande så kan det under vissa omständigheter omfattas av bestämmelser om rapporteringsplikt eller informationsskyldighet.
Cyberhot	En potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer.		Se betydande cyberhot.
Incident	En händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.		Begreppet är av central betydelse. En händelse omfattas endast av rapporteringsplikt om en incident, enligt definitionen, har inträffat.
Nätverks- och informationssystem	Ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen om elektronisk kommunikation, en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av a och b för att de ska kunna användas, skyddas och underhållas.	2 kap. 4 § 3 kap. 2 § 3 kap. 4 § 3 kap. 5 § 3 kap. 7 §	I CSL-föreskrifterna används begreppet synonymt med system.

Tabell 2. Begrepp och definitioner av relevans enligt CSL-föreskrifterna

Begrepp	Definition	Hänvisning föreskrifterna	Hur begreppet används
Angrepps-indikatorer	Teknisk information som utgör indikatorer på förberedelse till, pågående eller genomfört cyberangrepp.	2 kap. 4 § p. 5 (Incidentanmälan) 2 kap. 6 § p. 4 (Slutrapport, Lägesrapport)	Angreppsindikatorer är en av de uppgifter som verksamhetsutövare behöver lämna vid rapportering.
Betydande sårbarhet	En sårbarhet som har inneburit att en betydande cybersäkerhetsrisk i enlighet med artikel 3 p. 38 i Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828, i den ursprungliga lydelsen (cyberresiliensförordningen).	3 kap. 2 § p. 2 3 kap. 4 § p. 2 3 kap. 7 § p. 2	En betydande sårbarhet som har uppstått i verksamhetsutövarens system och möjliggör (exempelvis, kan utnyttjas för att orsaka) en allvarlig driftstörning eller ekonomisk skada för verksamhetsutövaren, eller betydande skada för andra fysiska eller juridiska personer, räknas i sig som en incident som omfattas av rapporteringsplikt.

Tabellen fortsätter!

Begrepp	Definition	Hänvisning föreskrifterna	Hur begreppet används
Information i behov av utökat skydd	Information där externa krav ställd på att skydda informationens konfidentialitet, riktighet eller tillgänglighet för att uppnå ett tillräckligt skydd eller att identifieringen av interna behov resulterat i ett motsvarade behov av skydd.	2 kap. 4 § p. 6 (Incidentanmälan) 3 kap. 1 § p. 3 (Generella rapporteringskriterier för betydande incidenter) 3 kap. 6 § p. 1 (Generella rapporteringskriterier för betydande incidenter)	Incidenter där information i behov av utökat skydd påverkats kan under vissa omständigheter omfattas av rapporteringspliktigt. Verksamhetsutövaren behöver beskriva påverkan på information i behov av utökat skydd vid rapportering av betydande incidenter.
Sektorkritiskt system	Ett system som är nödvändigt för att kunna bedriva intern verksamhet eller tillhandahålla externa tjänster inom sektorsverksamhet.	3 kap. 1 § p. 1 3 kap. 1 § p. 2 4 kap. 1 § p. 1 (Sektorsspecifika rapporteringskriterier, Offentlig förvaltning) 4 kap. 2 § p. 1 (Sektorsspecifika rapporteringskriterier, Energi) 4 kap. 3 § (Sektorsspecifika rapporteringskriterier, Energi) 4 kap. 4 § (Sektorsspecifika rapporteringskriterier, Energi) 4 kap. 5 § (Sektorsspecifika rapporteringskriterier, Transporter) 4 kap. 6 § (Sektorsspecifika rapporteringskriterier, Transporter) 4 kap. 7 § (Sektorsspecifika rapporteringskriterier, Hälso- och sjukvård) 4 kap. 8 § (Sektorsspecifika rapporteringskriterier, Dricksvatten) 4 kap. 8 § (Sektorsspecifika rapporteringskriterier, Avloppsvatten)	Att incidenten inneburit nedsatt funktionalitet eller otillgänglighet i sektorskritiska system är en av de premisser som gör allvarliga driftstörningar rapporteringspliktiga enligt 3–4 kap. i CSL-föreskrifterna.
Sektorsverksamhet	Sådan verksamhet som omfattas av cybersäkerhetslagen.	2 kap. 3 § p. 6 (Upplysning) 2 kap. 6 § p. 3 (Slutrapport/ Lägesrapport) 3 kap. 1 § (Generella rapporteringskriterier) p. 1–2 4 kap. 1 § p. 1 a-b) 4 kap. 2 § p. 1 a-b) 4 kap. 3 § p. 2 4 kap. 4 § p. 2 4 kap. 5–6 §§ 4 kap. 7 § p. 1 a–b) 4 kap. 8 § p. 2 4 kap. 9 § p. 2	Att incidenten inneburit påverkan på sektorsverksamhet är en av en av de premisser som gör allvarliga driftstörningar rapporteringspliktiga enligt 3–4 kap. CSL-föreskrifterna.

Tabellen fortsätter!

Begrepp	Definition	Hänvisning föreskrifterna	Hur begreppet används
System	Nätverks- och informations-system enligt 1 kap. 2 § p. 16 cybersäkerhetslagen.	2 kap. 4 § p. 4 3 kap. 2 § 3 kap. 4 § 3 kap. 5 § 3 kap. 7 § 4 kap. 2 § p. 2 5 kap. 2 § (informationsskyldighet)	Begreppet är av central betydelse. Används som en förkortad version av nätverks- och informationssystem enligt 1 kap. 2 § p. 16 cybersäkerhetslagen.
Viktig samhälls-funktion	En samhällsfunktion som är nöd-vändig för samhällets grundläggande behov, värden eller säkerhet.	2 kap. 5 § p. 1 e 3 kap. 6 § p. 3	Verksamhetsutövare behöver uppge om incidenten inneburit påverkan på viktiga samhällsfunktioner vid rapportering. Om incidenten inne-burit påverkan på andra organisationer som tillhandahåller viktiga samhällsfunktioner kan den under vissa omständigheter omfattas av rapporteringsplikt.

Tabell 3. Ytterligare uttryck i CSL-föreskrifterna

Begrepp	Definition	Hänvisning föreskrifterna	Hur begreppet används
Autenticitet	Ett objekt (en bärare av information, en komponent i ett system, ett helt system eller något annat) har autenticitet (är ”äkta”) om det är vad det utges eller utger sig för att vara.		Om en händelse inneburit negativ påverkan på systems autenticitet så utgör det en incident enligt CSL.
Betydande cybersäkerhetsrisk	Cybersäkerhetsrisk som, baserat på dess tekniska egenskaper, kan antas innebära en hög sannolikhet för en incident som kan medföra allvarliga negativa konsekvenser, inbegripet genom att orsaka betydande materiell eller immateriell förlust eller störning.		Används för att beskriva betydande sårbarhet (se tabell 2).
Grundorsak	Det som initierar händelseförloppet som gav upphov till incidenten.	2 kap. 5 § 3 kap. 8 §	Återkommande incidenter som har samma grundorsak kan under vissa omständigheter omfattas av rapporteringsplikt.
Gränsöverskridande konsekvenser	Konsekvenser utanför Sveriges gränser.	2 kap. 3 § 2 kap. 5 §	Vid rapportering av betydande incidenter måste verksamhetsutövare uppge uppgifter om potentiella gränsöverskridande konsekvenser.
Konfidentialitet	Att information och system skyddas mot obehörig åtkomst och insyn.		Används för att beskriva information i behov av utökat skydd (se tabell 2). samt incident (se tabell 1).
Mottagare av tjänster	Fysiska samt juridiska personer som använder de tjänster som verksamhetsutövaren tillhandahåller och som omfattas av CSL.	2 kap. 5 § 5 kap. 1–2 §§	Centralt för informationsskyldigheten.
Riktighet	Att information och system skyddas mot oönskad förändring.		Används för att beskriva information i behov av utökat skydd (se tabell 2). samt incident (se tabell 1).
Tillgänglighet	Att information och system är åtkomliga för behöriga personer vid rätt tillfälle.		Används för att beskriva information i behov av utökat skydd (se tabell 2). samt incident (se tabell 1).

Kapitel 3

Betydande incidenter ska rapporteras

3. Betydande incidenter ska rapporteras

Verksamhetsutövare som omfattas av CSL ska rapportera betydande incidenter. Definitionen av vad som utgör en incident återfinns i CSL.

Definition av incident · 1 kap. 2 § p. 10 CSL

En händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos

- lagrade,
- överförda eller
- behandlade uppgifter eller
- hos de tjänster som erbjuds genom, eller är tillgängliga, via nätverks- och informationssystem.

En incident är alltså varje händelse som äventyrar uppgifternas, eller tjänsternas, skyddsvärda egenskaper avseende tillgänglighet, riktighet inklusive autenticitet, eller konfidentialitet. För att en incident ska vara rapporteringspliktig enligt CSL ska den vara betydande.

Definition av betydande incident · 2 kap. 5 § CSL

En incident ska anses vara betydande om den

- har orsakat, eller
- kan orsaka,
- allvarlig driftstörning för den erbjudna tjänsten eller
- ekonomisk skada för den berörda verksamhetsutövaren, eller
- om den har påverkat eller
- kan påverka
- andra fysiska eller juridiska personer genom att vålla betydande skada.

I 2 kap. 5 § andra stycket CSL fastställs att **allvarlig driftstörning, ekonomisk skada**, och **betydande skada för andra fysiska eller juridiska personer** utgör konsekvenser som gör en incident betydande och därmed rapporteringspliktig. Enligt definitionen är både incidenter som **kan** resultera i eller **har** resulterat i sådana konsekvenser betydande.

Vilka incidenter som ska anses betydande beskrivs vidare i 3–4 kap. CSL-föreskrifterna.[7] Föreskrifterna redogör närmare för när incidenter är att anses som betydande därför att de har inneburit eller kan innebära en allvarlig driftstörning, ekonomisk skada för verksamhetensutövaren samt betydande skada för andra fysiska eller juridiska personer. I 3 kap. CSL-föreskrifterna framgår det även att **återkommande incidenter**, under vissa omständigheter, kan anses vara betydande och därmed rapporteringspliktiga om de sammantaget inneburit ekonomisk skada.[8]

Ett antal sektorer behöver även beakta sektorsspecifika rapporteringskriterier i 4 kap. CSL-föreskrifterna vid bedömning av rapporteringsplikt. Sektorerna som omfattas av dessa kompletterande bestämmelser inkluderar offentlig förvaltning, energi, transport, hälso- och sjukvård, dricksvatten och avloppsvatten. Verksamhetsutövare som omfattas av dessa kriterier behöver tillämpa bestämmelser om allvarlig driftstörning i 3 kap. 1 § (de generella kriterierna) och kap. 4 (de sektorsspecifika kriterierna) parallellt.

Följande avsnitt går igenom de rapporteringskriterier som framgår i kap. 3–4 CSL-föreskrifterna och som ligger till grund för rapporteringsplikten för majoriteten av verksamhetsutövare som omfattas av CSL och tillhörande regleringar.

Not 7. Notera att sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster (mellan företag), post- och budtjänster samt rymden inte omfattas av kap. 3–4 i CSL-föreskrifterna. För mer information, se avsnitt 1.2 i vägledningen.

Not 8. Återkommande incidenter som resulterat i ekonomisk skada anses även vara betydande enligt EU-kommissionens genomförandeförordning (EU) 2024/2690.

3.1 Rapporteringskriterier för betydande incidenter

Vad som utgör en betydande incident framgår i 3–4 kap. CSL-föreskrifterna. Föreskrifterna följer en enhetlig struktur. Vad som utgör en betydande incident har tydliggjorts under särskilda avsnitt i föreskrifterna:

- allvarlig driftstörning för verksamhetsutövaren,
- ekonomisk skada för verksamhetsutövaren,
- betydande skada för andra fysiska eller juridiska personer, och
- återkommande incidenter.

I vägledningens avsnitt 3.1.1 beskrivs vad som anses utgöra en allvarlig driftstörning (3 kap. 1–2 §§ CSL-föreskrifterna), avsnitt 3.1.2 vad som anses utgöra ekonomisk skada för verksamhetsutövare (3 kap. 3–5 §§ CSL-föreskrifterna), avsnitt 3.1.3 vad som anses utgöra betydande skada för andra fysiska och juridiska personer i (3 kap. 6–7 §§ CSL-föreskrifterna) och vad som anses utgöra återkommande incidenter i avsnitt 3.1.5 (3 kap. 8 § CSL-föreskrifterna). I vägledningens avsnitt 3.1.4 redogörs för när en incident blir rapporteringspliktig för att den **kan** resultera i allvarlig driftstörning, ekonomisk skada eller betydande skada för andra fysiska eller juridiska personer (se 3 kap. 2, 4 och 7 §§ i CSL-föreskrifterna).

3.1.1 Allvarlig driftstörning för verksamhetsutövaren

3 kap. 1 § CSL-föreskrifterna

Med betydande incident som har orsakat allvarlig driftstörning för verksamhetsutövare avses en incident där

1. otillgänglighet eller nedsatt funktionalitet i ett eller flera sektorskritiska system har inneburit att
   a. sektorsverksamhet endast har kunnat bedrivas i begränsad utsträckning i mer än 12 timmar
   b. personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än 48 timmar
2. information i behov av utökat skydd tillhörande verksamhetsutövaren som behandlas i ett eller flera sektorskritiska system har blivit tillgänglig för obehöriga, förvanskats eller förstörts, eller
3. ett eller flera sektorsspecifika kriterier om allvarlig driftstörning för verksamhetsutövare i kap. 4 uppfylls.

DEFINITION · CSL-föreskrifterna

Sektorskritiskt system

Ett sektorskritiskt system definieras i CSL-föreskrifterna (1 kap. 3 §) som ett system som är nödvändigt för att kunna bedriva intern verksamhet eller tillhandahålla externa tjänster inom sektorsverksamhet.

Begreppet sektorskritiskt system är ett centralt begrepp då det nyttjas för att definiera allvarlig driftstörning enligt 3–4 kap. CSL-föreskrifterna. Detta då nedsatt funktionalitet eller otillgänglighet i sektorskritiska system är en av de förutsättningar som avgör om en driftstörning är rapporteringspliktig.

Verksamhetsutövaren behöver själv bedöma vilka system som är sektorskritiska inom dennes sektorsverksamhet (för information om i vilka bestämmelser i CSL-föreskrifterna som definitionen tillämpas se tabell 2 i kapitel 2 i vägledningen). Sektorskritiska system inkluderar sådana system som är nödvändiga för att verksamhetsutövaren ska kunna bedriva den sektorsverksamhet som specificeras i CSL (för mer information om sektorsverksamhet, se tabell 2). Det inkluderar både system som används i tjänster som tillhandahålls externt och system som används internt om de behövs för att kunna tillhandahålla externa tjänster inom sektorsverksamheten. Interna system bör räknas som sektorskritiska om deras funktionalitet är central för att sektorsverksamheten ska kunna bedrivas enligt normalläge. Även utkontrakterade system kan räknas som sektorskritiska om de behövs för att bedriva sektorsverksamheten.

För att en incident ska vara rapporteringspliktig enligt 3 kap. 1 § CSL-föreskrifterna gäller det att den ska ha orsakat en allvarlig driftstörning för verksamhetsutövaren. En allvarlig driftstörning har inträffat när ett eller flera av kriterierna i 3 kap. 1 § CSL-föreskrifterna har uppfyllts. Notera att 3 kap. 1 § p. 3 CSL-föreskrifterna specificerar att en allvarlig driftstörning ska ses som betydande om den uppnår sektorsspecifika kriterier enligt kap. 4. De sektorsspecifika kriterierna avseende allvarlig driftstörning redogörs för i avsnitt 3.1.1.3.

3.1.1.1 Allvarlig driftstörning som påverkar förmågan att bedriva sektorsverksamhet

§ **PÅVERKAN PÅ FÖRMÅGAN ATT BEDRIVA SEKTORSVERKSAMHET · 3 kap. 1 § p. 1 CSL-föreskrifterna**

Otillgänglighet eller nedsatt funktionalitet i ett eller flera sektorskritiska system har inneburit att

a. sektorsverksamhet endast har kunnat bedrivas i begränsad utsträckning i mer än 12 timmar
b. personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i mer än 48 timmar.

I 3 kap. 1 § p. 1 CSL-föreskrifterna beskrivs under vilka omständigheter en incident med påverkan på sektorskritiska system blir rapporteringspliktig då den har fått en negativ påverkan på verksamhetsutövarens förmåga att bedriva sektorsverksamhet. Det innebär att incidenten i ett eller flera sektorskritiska system ska ha resulterat i en negativ påverkan på verksamhetsutövarens förmåga att tillhandahålla de externa tjänster som ingår i sektorsverksamheten.

Vid bedömning om incidenten är rapporteringspliktig enligt dessa kriterier måste verksamhetsutövaren utreda:

- om ett eller flera sektorskritiska system har varit otillgängliga eller haft nedsatt funktionalitet,
- i vilken utsträckning incidenten påverkat verksamhetsutövarens förmåga att bedriva verksamhet enligt normalläget, och
- hur länge incidenten har resulterat i att sektorsverksamhet inte har kunnat bedrivas enligt normalläge.

FAKTARUTA · SEKTORERNA 4 kap. CSL-föreskrifterna.

Sektorsspecifika kriterier för allvarlig driftstörning

De verksamhetsutövare som omfattas av sektorsspecifika kriterier i CSL-föreskrifterna behöver generellt inte rapportera enligt bestämmelser enligt 3 kap. 1 § p. 1 CSL-föreskrifterna då de omfattas av sektorsspecifika bestämmelser enligt 3 kap. 1 § p. 3 CSL-föreskrifterna. De sektorsspecifika bestämmelserna, som återfinns i CSL-föreskrifternas 4 kap., inkluderar lägre tröskelvärden som innebär att driftstörningar som påverkar verksamhetsutövarens förmåga att bedriva sektorsverksamhet blir rapporteringspliktiga efter en kortare tidsperiod.

Se avsnitt 3.1.1.3 för mer information om dessa kriterier.

Incidenten behöver inte nödvändigtvis ha påverkat ett eller flera sektorskritiska system som aktivt används för att tillhandahålla externa tjänster. Om ett eller flera system som används internt inom organisationen, och som anses vara sektorskritiska, till den grad att tillhandahållandet av externa tjänster eller produkter direkt eller indirekt påverkas, kan incidenten bedömas vara rapporteringspliktig. Noterbart är att incidenter som inträffar i system som tillhandahålls av en leverantör också kan vara rapporteringspliktiga om sådana system anses vara nödvändiga för verksamhetsutövarens förmåga att bedriva sektorsverksamhet.

Enligt 3 kap. 1 § p. 1 a CSL-föreskrifterna ska verksamhetsutövare rapportera incidenter som lett till otillgänglighet eller nedsatt funktionalitet i ett eller flera sektorskritiska system om det resulterat i att sektorsverksamheten endast kunnat bedrivas i begränsad utsträckning under 12 timmar. Vad det innebär att bedriva sektorsverksamhet i begränsad utsträckning behöver avgöras i det enskilda fallet och varierar beroende på vilken verksamhet som verksamhetsutövaren bedriver. Några indikatorer på att verksamhetsutövaren endast bedriver sektorsverksamhet i begränsad utsträckning inkluderar att:

- en eller flera externa tjänster inom sektorsverksamhet endast kan levereras till mottagare av tjänsterna i begränsad utsträckning, eller inte alls, i mer än 12 timmar, eller
- produktions-, bearbetnings- och/eller distributionskapacitet inom sektorsverksamhet har minskat på ett påtagligt sätt i mer än 12 timmar.

EXEMPEL

En allvarlig driftstörning inom sektorn tillverkning

Verksamhetsutövare A är en tillverkare av bilar. Ett åsknedslag orsakar ett strömavbrott som föranleder att ett sektorskritiskt system som används inom biltillverkningen blir otillgängligt. Bortfallet av det sektorskritiska systemet innebär att ett delmoment inom produktionen inte kan genomföras, och därav att produktionskapaciteten minskar med cirka 20 procent i mer än 12 timmar. Produktionsbortfallet resulterar i att kriterierna i 3 kap. 1 § p. 1 a CSL-föreskrifterna uppfylls. Incidenten är därför att betrakta som en allvarlig driftstörning och därför rapporteringspliktig.

Vidare gäller det enligt 3 kap. 1 § p. 1 b CSL-föreskrifterna att en incident anses som rapporteringspliktig om personal har behövt använda alternativa arbetssätt för att bedriva sektorsverksamhet i minst 48 timmar. Denna bestämmelse tar inte fasta på hur tillhandahållandet av externa tjänster har påverkats. Istället läggs fokus på huruvida verksamhetsutövaren behöver utnyttja alternativa arbetssätt, såsom reservrutiner, för att upprätthålla förmågan att bedriva sektorsverksamhet under utsatt tidsperiod.

EXEMPEL

En allvarlig driftstörning inom sektorn produktion, bearbetning och distribution av livsmedel

Verksamhetsutövare B är en distributör av livsmedel. En elektronisk kommunikationskabel grävs av i samband med ett vägarbete, vilket påverkar internetåtkomsten till distributörens huvudkontor och som i nästa led resulterar i att ett centralt affärssystem innehållandes bland annat ordrar och som kräver internetanslutning blir otillgängligt. För att distributionen av livsmedel ska kunna utföras enligt normalläge behöver personalen utnyttja alternativa arbetssätt under perioden affärssystemet är otillgängligt. Eftersom alternativa arbetssätt behövde nyttjas under mer än 48 timmar för att upprätthålla sektorsverksamhet under tiden som incidenten pågick uppfylls kriterierna i 3 kap. 1 § p. 1 b CSL-föreskrifterna. Incidenten är därför att betrakta som en allvarlig driftstörning och därmed rapporteringspliktig.

Notera att planerade avbrott i sektorskritiska system, exempelvis till följd av underhållsarbeten, som föranleder att personal behöver utnyttja alternativa arbetssätt för att kunna tillhandahålla externa tjänster i mer än 48 timmar också är rapporteringspliktiga.

3.1.1.2 Allvarlig driftstörning som påverkar information i behov av utökat skydd

§ PÅVERKAN PÅ INFORMATION I BEHOV AV UTÖKAT SKYDD
· 3 kap. 1 § p. 2 CSL-föreskrifterna

Information i behov av utökat skydd tillhörande verksamhetsutövaren som behandlas i ett eller flera sektorskritiska system har blivit tillgänglig för obehöriga, förvanskats eller förstörts.

Enligt 3 kap. 1 § p. 2 CSL-föreskrifterna behöver verksamhetsutövare rapportera incidenter som påverkat känslig information som behandlas i sektorskritiska system.

Vid bedömning om incidenten är rapporteringspliktig enligt dessa kriterier måste verksamhetsutövaren utreda om:

- incidenten har påverkat information i behov av utökat skydd,
- informationen behandlas i ett system som anses vara sektorskritiskt, och
- informationen har blivit tillgänglig för obehöriga, förvanskats eller förstörts.

Information i behov av utökat skydd definieras i CSL-föreskrifterna som information som på grund av externa krav kräver en viss nivå av skydd avseende konfidentialitet, riktighet inklusive autenticitet, eller tillgänglighet alternativt information som verksamhetsutövaren vid värdering bedömer ha behov av motsvarande nivå av skydd. Med externa krav kan exempelvis avses författningar såsom dataskyddsförordningen[9], lag (2018:558) om företagshemligheter eller offentlighets- eller sekretesslagen (2009:400). Vidare kan verksamhetsutövaren själv, utifrån interna krav, i samband med en informationsklassning ha gjort en bedömning att informationen är i behov av utökat skydd och därför ska hanteras på ett särskilt sätt.

För att en incident ska bli rapporteringspliktig enligt detta kriterium krävs vidare att informationen antingen har blivit tillgänglig för obehöriga, blivit förvanskad eller förstörd. Informationen bör betraktas som förvanskad eller förstörd även i de fall den inte kan återställas inom en rimlig tid. Vad som är en rimlig tid ska verksamhetsutövaren bedöma då denne fastställer sina acceptabla tider för otillgänglighet och bristande funktionalitet i enlighet med 3 kap. 15 § Myndigheten för civilt försvars föreskrifter om säkerhetsåtgärder och ledningens utbildning för väsentliga och viktiga verksamhetsutövare (MCFFS 2026:11). Vilka de tiderna är för ett specifikt system bör enligt det allmänna rådet till 4 kap. 10 § samma författning framgå av systemets driftdokumentation.

Om obehöriga har haft åtkomst till information i behov av utökat skydd bör det betraktas som att den har blivit tillgänglig för obehöriga. Rapporteringsplikten gäller oavsett om den obehöriga parten utgör interna eller externa obehöriga användare av system.

EXEMPEL

En allvarlig driftstörning inom energisektorn

Verksamhetsutövare C är ett energibolag. En cyberkriminell aktör utför ett intrång via ett affärssystem och lyckas bland annat få åtkomst till känsliga dokument som av företaget betraktas som affärshemligheter. Då företaget betraktar dokumentens innehåll som information i behov av utökat skydd, och informationen behandlades i ett system som av företaget bedöms vara sektorskritiskt, uppnår incidenten kriterierna i 3 kap. 1 § p. 2 CSL-föreskrifterna. Incidenten är därför att betrakta som en allvarlig driftstörning och därför rapporteringspliktig.

Not 9. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävandet av direktiv 95/46/EG (allmän dataskyddsförordning).

3.1.1.3 Allvarlig driftstörning enligt sektorsspecifika kriterier

§ **SEKTORSSPECIFIKA KRITERIER**
· 3 kap. 1 § p. 3 CSL-föreskrifterna

Ett eller flera sektorsspecifika kriterier om allvarlig driftstörning för verksamhetsutövare i 4 kap. CSL-föreskrifterna uppfylls.

Enligt 3 kap. 1 § p. 3 CSL-föreskrifterna så utgör även incidenter som träffas av kriterier i 4 kap. allvarlig driftstörning. Verksamhetsutövare som behöver tillämpa dessa bestämmelser inkluderar verksamhetsutövare inom sektorerna offentlig förvaltning, energi, transport, hälso- och sjukvård, dricksvatten och avloppsvatten.

Bestämmelserna i 4 kap. kompletterar bestämmelserna om allvarlig driftstörning i CSL-föreskrifterna 3 kap. 1 § p. 1 a och b, då de tar sikte på att definiera när incidenten har blivit rapporteringspliktig då den påverkat tillgången till sektorskritiska system och förmågan att bedriva sektorsverksamhet. Det innebär att 4 kap. CSL-föreskrifterna, för ett antal sektorer, beskriver under vilka omständigheter otillgänglighet eller nedsatt funktionalitet i sektorskritiska system omfattas av rapporteringsplikt. Avgörande för rapporteringsplikten är i vilken utsträckning det påverkar verksamhetsutövarens förmåga att bedriva sektorsverksamhet, alltså leverera externa tjänster till mottagare, enligt normalläge. Liksom 3 kap. 1 § p. 1 a och b så är en utgångspunkt för rapporteringsplikt enligt de flesta kriterier i kap. 4 att sektorsverksamhet endast kunna bedrivas i begränsad utsträckning alternativt att personal behövt utnyttja alternativa arbetssätt för att bedriva verksamhet under en specificerad tidsperiod.

Sektorsverksamhet inom sektorn offentlig förvaltning utgörs av den verksamhet som verksamhetsutövaren är skyldig att ha enligt författning. För kommuners del handlar det exempelvis om social omsorg, vatten och avlopp, och räddningstjänster, för regioner om hälso- och sjukvård, regional och lokal kollektivtrafik. Statliga myndigheters uppdrag framgår exempelvis av förordningen med myndighetens instruktion. Vid avgörandet av i vilken utsträckning en incident påverkar sektorsverksamhet i offentlig förvaltning bör dessa verksamhetsutövare därför göra en generell bedömning utifrån påverkan på den totala verksamheten de är skyldiga att ha enligt författning. Enligt 4 kap. 1 § p. 2 CSL-föreskrifterna blir incidenter som påverkar viss sektorsverksamhet inom andra sektorer även rapporteringspliktig för verksamhetsutövare inom offentlig förvaltning i den mån de själva bedriver sådan verksamhet, exempelvis verksamhet inom hälso- och sjukvård.

Tabellen nedan redogör vilka sektorer som omfattas av sektorsspecifika kriterier. Notera att det inom vissa sektorer även finns specifika kriterier på delsektorsnivå. Inom sektorn hälso- och sjukvård är det endast de som bedriver sektorsverksamhet som vårdgivare som omfattas av sektorsspecifika kriterier. Resterande verksamhetsutövare inom hälso- och sjukvård behöver endast tillämpa bestämmelserna i 3 kap. CSL-föreskrifterna.

Inom sektorn transporter förekommer även kriterier för kollektivtrafik. Kollektivtrafik omfattas av bestämmelser i CSL-föreskrifterna med anledning av att de omfattas av CER-direktivet[10] och därför även behöver tillämpa bestämmelser enligt CSL.

Tabell 4. Sektorsspecifika kriterier i CSL-föreskrifterna

Sektor	CSL-föreskrifterna
Offentlig förvaltning	4 kap. 1 §
Energi	4 kap. 2–4 §§
Elektricitet och fjärrvärme eller fjärrkyla	4 kap. 2 §
Gas och vätgas	4 kap. 3 §
Olja	4 kap. 4 §
Transporter	4 kap. 5–6 §§
Sjöfart, lufttransport, vägtransport	4 kap. 5 §
Järnvägstransport och kollektivtrafik[11]	4 kap. 6 §
Hälso- och sjukvård (vårdgivare)[12]	4 kap. 7 §
Dricksvatten	4 kap. 8 §
Avloppsvatten	4 kap. 9 §

Not 10. Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

Not 11. Notera att kollektivtrafik omfattas av dessa föreskrifter då de omfattas av Europaparlamentets och rådets direktiv 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet).

Not 12. Notera att det endast är vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU som omfattas av sektorsspecifika bestämmelser för hälso- och sjukvård. Entiteter eller verksamheter som inte utgör vårdgivare enligt denna definition ska endast följa de generella kriterierna.

3.1.2 Ekonomisk skada för verksamhetsutövaren

3 kap. 3 § CSL-föreskrifterna

Med betydande incident som har orsakat ekonomisk skada för verksamhetsutövaren avses en incident som sammantaget har inneburit en kostnad, enligt 5 §, som överstiger fem procent av den berörda verksamhetsutövarens totala årsomsättning under föregående räkenskapsår.

För verksamhetsutövare inom offentlig förvaltning gäller istället fem procent av verksamhetsutövarens anslag eller totala intäkter under föregående räkenskapsår.

För att en incident ska vara rapporteringspliktig enligt 3 kap. 3 § CSL-föreskrifterna gäller det att den ska ha orsakat ekonomisk skada i en viss omfattning för verksamhetsutövaren. En incident som resulterat i ekonomisk skada definieras i föreskrifterna som en incident som inneburit en kostnad som överstiger fem procent av verksamhetsutövarens totala årsomsättning under föregående räkenskapsår. Verksamhetsutövare inom sektorn offentlig förvaltning ska istället för den totala årsomsättningen beräkna kostnaden som andelen av verksamhetsutövarens anslag eller totala intäkter under föregående räkenskapsår.

Vid bedömning om incidenten är rapporteringspliktig enligt detta kriterium måste verksamhetsutövaren utreda:

- vilka kostnader incidenten har medfört enligt föreskrifternas 3 kap. 5 § (se stycket nedan),
- hur mycket incidenten sammantaget har kostat organisationen samt
- om den sammantagna kostnaden överstiger fem procent av verksamhetsutövarens årsomsättning, anslag eller totala intäkter enligt föregående räkenskapsår.

För att uppskatta storleken på den ekonomiska skadan ska både direkta och indirekta kostnader beaktas. Det bör både röra sig om de kostnader som verksamhetsutövaren behöver betala på grund av lag- eller avtalskrav, men också kostnader som verksamhetsutövaren väljer att ta för att exempelvis hantera incidenten. Beräkningen av kostnaden ska göras utifrån den information som finns att tillgå och baseras på en uppskattning. Vid beräkningen av kostnaden ska verksamhetsutövaren beakta följande direkta och indirekta kostnader (se 3 kap. 5 § i CSL-föreskrifterna):

1. kostnader för återställning av information som har förlorats eller förvanskats,
2. kostnader för utbyte eller återställning av system,
3. externa rådgivningskostnader för incidenthanteringstjänster, juridisk rådgivning, it-forensiska tjänster och saneringstjänster,

4. tillkommande personalkostnader,
5. kostnader på grund av att avtalsförpliktelser[13] inte har fullgjorts, och
6. uteblivna intäkter till följd av oplanerade produktionsbortfall.

Då det kan vara svårt att ha kännedom om exakta belopp är det viktigt att göra en initial uppskattning. Om en sådan uppskattning inte kan göras förrän efter incidenten har upphört, till följd av bristande resurser eller information, ska verksamhetsutövare rapportera incidenten i samband med att en sådan uppskattning har kunnat göras.

Om verksamhetsutövaren är en del av en koncern är det det drabbade bolaget inom koncernens årsomsättning som bör utgöra utgångspunkten för en sådan uppskattning. Om exempelvis en hel koncern påverkats av incidenten är det koncernens årsomsättning som avses, medan om det endast är ett bolag inom koncernen som påverkats så är det detta bolagets årsomsättning som avses.

Det finns inga föreskriftskrav om ekonomisk skada för nyetablerade bolag eller nya offentliga verksamheter som omfattas av CSL och som existerat under mindre än ett år. Detta mot bakgrund av att bestämmelsen tar fasta på andelen av årsomsättning, anslag eller totala intäkter under föregående räkenskapsår. Nyetablerade verksamhetsutövare kan dock välja att rapportera incidenter som resulterat i en större ekonomisk kostnad frivilligt.

3.1.3 Skada för andra fysiska eller juridiska personer

3 kap. 6 § CSL-föreskrifterna

Med betydande incident som har påverkat andra fysiska eller juridiska personer genom att vålla betydande skada avses en incident som

1. har inneburit att information i behov av utökat skydd som verksamhetsutövaren behandlar för annan juridisk person eller minst 500 fysiska personer har blivit tillgänglig för obehöriga, förvanskats eller förstörts,
2. har inneburit en föroreningsskada enligt 10 kap. 1 § miljöbalken, eller
3. verksamhetsutövaren har fått kännedom om att den inneburit
   a. att en juridisk person som tillhandahåller en viktig samhällsfunktion har gått in i stabsläge eller på annat sätt har eskalerat eller ändrat sin organisation på grund av incidenten
   b. allvarlig personskada eller sjukdom, eller
   c. dödsfall.

Not 13. Det inkluderar exempelvis sanktionsavgifter, viten och böter.

Enligt 3 kap. 6 § i CSL-föreskrifterna är en incident att betrakta som betydande om incidenten uppnår ett eller flera kriterier för betydande skada för andra fysiska eller juridiska personer. En incident anses ha orsakat betydande skada för andra om den har resulterat i att information i behov av utökat skydd tillhörande andra har påverkats, om den resulterat i en föroreningsskada eller om verksamhetsutövaren fått kännedom om att incidenten fått andra allvarliga konsekvenser för andra juridiska personer eller fysiska personer.

Enligt 3 kap. 6 § p. 1 CSL-föreskrifterna är incidenten att betrakta som betydande om den inneburit att information tillhörande andra juridiska eller fysiska personer har blivit tillgänglig för obehöriga, förvanskats eller förstörts. Informationen bör betraktas som förvanskad eller förstörd även i de fall den inte kan återställas inom en rimlig tid. Vad som är en rimlig tid ska verksamhetsutövaren bedöma då denne fastställer sina acceptabla tider för otillgänglighet och bristande funktionalitet i enlighet med 3 kap. 15 § Myndigheten för civilt försvars föreskrifter om säkerhetsåtgärder och ledningens utbildning för väsentliga och viktiga verksamhetsutövare (MCFFS 2026:11). Vilka de tiderna är för ett specifikt system bör enligt det allmänna rådet till 4 kap. 10 § samma författning framgå av systemets driftdokumentation. Till skillnad från 3 kap. 1 § p. 2 CSL-föreskrifterna så förutsätter inte detta kriterium att informationen har behandlats i ett sektorskritiskt system.

Vid bedömning av om incidenten är rapporteringspliktig enligt dessa kriterier måste verksamhetsutövaren utreda om:

- incidenten har påverkat information i behov av utökat skydd,
- informationen tillhör en juridisk person eller minst 500 fysiska personer, och
- informationen blivit tillgänglig för obehöriga, förvanskats eller förstörts.

Enligt 3 kap. 6 § p. 2 CSL-föreskrifterna ska incidenter även anses ha resulterat i betydande skada för andra om den inneburit en föroreningsskada enligt 10 kap. 1 § miljöbalken. En föroreningsskada är en miljöskada som genom förorening av ett mark- eller vattenområde, grundvatten, en byggnad eller en anläggning kan medföra skada eller olägenhet för människors hälsa eller miljön. Kriteriumet behöver endast tillämpas av de verksamhetsutövare som bedriver sådan typ av sektorsverksamhet inom vilken en incident kan resultera i föroreningsskada.

Enligt 3 kap. 6 § p. 3 CSL-föreskrifterna kan incidenter som verksamhetsutövaren ska ha fått kännedom om att de har inneburit andra allvarliga konsekvenser, såsom betydande påverkan på annan organisations förmåga att bedriva verksamhet eller allvarlig personskada, vara rapporteringspliktiga. Rapporteringsplikten gäller endast i de fall verksamhetsutövaren fått kännedom om att incidenten föranlett sådan typ av påverkan. Verksamhetsutövaren behöver således inte vidta särskilda åtgärder för att utreda om sådana konsekvenser har inträffat i syfte att följa bestämmelserna i föreskrifterna.

Det är endast i de fall en mottagare av verksamhetsutövarens tjänster utgör en juridisk person som tillhandahåller tjänster inom viktiga samhällsfunktioner påverkats som en incident kan uppfylla 3 kap. 6 § p. 3 a CSL-föreskrifterna.

Om verksamhetsutövaren får vetskap om att en sådan organisations förmåga att bedriva verksamhet allvarligt påverkats av incidenten, ska incidenten rapporteras. För att verksamhetsutövaren ska kunna avgöra om en incident omfattas av sådan rapporteringsplikt kan det vara bra att kartlägga vilka som är mottagare av verksamhetsutövarens tjänster samt om verksamhetsutövaren tillhandahåller tjänster som potentiellt kan äventyra mottagarens verksamhet på detta sätt.

EXEMPEL

Informationsförlust vållar skada för andra

Verksamhetsutövare D är en kommun. Kommunen innehar stora mängder personuppgifter om dess kommuninvånare, varav en del som berör orosanmälningar förvaras digitalt i en mapp. Det handlar om över 500 ärenden med personuppgifter. I samband med en migrering till ett nytt system flyttas mappen inte med på korrekt sätt till det nya systemet. När felet upptäcktes är den gamla ytan rensad. Då informationen inte kunde återställas inom den tidsram som verksamhetsutövaren fastställt som acceptabel är informationen att betrakta som förstörd. Information om mer än 500 personer har därmed förstörts, och incidenten blir rapporteringspliktig enligt 3 kap. 6 § CSL-föreskrifterna.

3.1.4 Incidenter som kan resultera i konsekvenser kan också vara betydande

Verksamhetsutövare har även en skyldighet att rapportera incidenter som **kan** resultera i allvarlig driftstörning, ekonomisk skada eller betydande skada för andra fysiska eller juridiska personer. Dessa bestämmelser är sammanslagna rutan nedan.

■ 3 kap. 2 § | ● 3 kap. 4 § | ▲ 3 kap. 7 § · CSL-föreskrifterna

Med betydande incident som kan orsaka allvarlig driftstörning | ekonomisk skada | påverka andra fysiska eller juridiska personer genom att vålla betydande skada för verksamhetsutövaren avses en incident där det inom verksamhetsutövarens system har uppstått

1. ett betydande cyberhot som sannolikt kan orsaka eller bidra till att orsaka konsekvenser enligt
   - ■ 1 § (allvarlig driftstörning)
   - ● 3 § (ekonomisk skada)
   - ▲ 6 § (påverka andra fysiska eller juridiska personer), eller
2. en betydande sårbarhet som möjliggör konsekvenser enligt
   - ■ 1 § (allvarlig driftstörning)
   - ● 3 § (ekonomisk skada)
   - ▲ 6 § (påverka andra fysiska eller juridiska personer).

Ett **cyberhot** är en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer enligt 1 kap 2 § p. 4 CSL. En **sårbarhet** är en avsaknad av något som förhindrar, eller bidrar till att förhindra, att en incident inträffar. Ett cyberhot eller en sårbarhet kan i nästa led betraktas som betydande om det riskerar att utlösa, respektive möjliggöra, allvarliga konsekvenser för verksamhetsutövarens system eller användarna av dessa system.

Om ett cyberhot eller en sårbarhet som anses vara betydande är så pass allvarlig att den bedöms kunna resultera i allvarlig driftstörning, ekonomisk skada eller betydande skada för andra, omfattas den av rapporteringsplikt. Notera att dessa bestämmelser inte bara gäller för de generella rapporteringskriterierna för allvarlig driftstörning, utan även för de sektorsspecifika rapporteringskriterierna.

Vid bedömning om incidenten är rapporteringspliktig enligt dessa kriterier måste verksamhetsutövaren utreda:

- om incidenten har resulterat i ett betydande cyberhot eller om en betydande sårbarhet har uppstått inom verksamhetsutövarens system, och om

    1. det betydande cyberhotet, på grund av dess karaktär eller andra omständigheter, kommer att leda till allvarlig driftstörning, ekonomisk skada eller betydande skada för andra, enligt CSL-föreskrifterna, om inget görs.
    2. eller den betydande sårbarheten, på grund av dess karaktär eller andra omständigheter, möjliggör att allvarlig driftstörning, ekonomisk skada eller betydande skada för andra uppstår, enligt CSL-föreskrifterna, uppstår.

För att ett **betydande cyberhot** eller att **en betydande sårbarhet** ska anses vara rapporteringspliktigt måste cyberhotet eller sårbarheten ha uppstått i verksamhetsutövarens system, inklusive system som tillhandahålls av leverantör. Det innebär att betydande cyberhot och betydande sårbarheter endast är att betrakta som betydande incidenter om de aktivt påverkar verksamhetsutövarens system.

Exempelvis betraktas betydande cyberhot som verksamhetsutövaren har upptäckt inom ramen för sin externa omvärldsbevakning men som inte utgör pågående incidenter inom verksamhetsutövarens system, inte som rapporteringspliktiga.[14]

Not 14. Enligt CSL kan verksamhetsutövare dock välja att rapportera både cyberhot och sårbarheter frivilligt.

TÄNK PÅ

Cyberhot uppstår inte enbart som en konsekvens av cyberangrepp

Det är viktigt att notera att cyberhot inte enbart utgör antagonistiska handlingar.

Ett rapporteringspliktigt cyberhot kan exempelvis utgöra skadlig kod som en angripare har introducerat i verksamhetsutövarens system, men det kan också handla om kod som introducerats av misstag och som interagerar med system på ett negativt sätt. Ett cyberhot kan också utgöras av en fysisk händelse, såsom ett elfel eller en fuktskada i ett system. Avgörande är att det är en omständighet, händelse eller handling som kan utlösa ett rapporteringspliktigt händelseförlopp.

Vid bedömningen om ett betydande cyberhot, eller en betydande sårbarhet, kan resultera i de ovan specificerade konsekvenserna bör verksamhetsutövaren beakta hur stor risken är att ett sådant utfall inträffar. Vid en sådan bedömning bör verksamhetsutövaren bland annat ta hänsyn till:

1. vad som sannolikt skulle kunna inträffa i system om cyberhotet eller sårbarheten realiseras,
2. vilket eller vilka system som påverkas av incidenten,
3. hur viktiga dessa system är för verksamhetsutövarens förmåga att bedriva sektorsverksamhet,
4. vilken typ av information de behandlar, samt
5. hur stor risken är att incidenten sprider sig till andra sektorskritiska system inom verksamhetsutövarens digitala miljö.

EXEMPEL

Betydande sårbarhet som kan leda till allvarlig driftstörning

Verksamhetsutövare E är ett flygbolag. Vid förvaltning av ett administrativt system upptäcker en tekniker att en bakdörr har installerats. Teknikern kan inte avgöra om angripare har utnyttjat bakdörren för att få vidare åtkomst till systemet.

Verksamhetsutövaren bedömer att angripare via sårbarheten skulle kunna få åtkomst till sektorskritiska system och klassificerar bakdörren som en betydande sårbarhet. Då incidenten sannolikt kan resultera i en allvarlig driftstörning, med påverkan på verksamhetsutövarens förmåga att bedriva sektorsverksamhet (4 kap. 5 §) eller information i behov av utökat skydd (3 kap. 2 §), betraktar verksamhetsutövaren även incidenten som betydande.

Incidenten är därmed rapporteringspliktig.

EXEMPEL

Information om cyberhot i omvärldsbevakningen

Verksamhetsutövare F är en svensk vindkraftspark. I deras omvärldsbevakning framgår det att en vindkraftspark i Danmark har utsatts för en skadlig kod som påverkat deras system för styrning och kontroll. Uppgifterna i media pekar på att det är skadlig kod från en antagonistisk aktör. Den svenska verksamhetsutövaren bedömer att händelsen utgör ett allvarligt cyberhot då en sådan incident skulle kunna resultera i en allvarlig driftstörning om cyberhotet drabbar dem. Dock är det inte rapporteringspliktig enligt 3 kap. 2 § p. 1 CSL-föreskrifterna eftersom att cyberhotet inte uppstått i den svenska verksamhetsutövarens system.

Notera att även om det inte är rapporteringspliktigt, så är det frivilligt att rapportera in cyberhot till Myndigheten för civilt försvar, eller efter den 1 juli 2026, NCSC.

3.1.5 Återkommande incidenter

3 kap. 8 § CSL-föreskrifterna

Incidenter som var för sig inte anses som en betydande incident ska anses vara en betydande incident om de

1. har inträffat minst två gånger inom sex månader
2. bedöms ha samma grundorsak, och
3. sammantaget medfört ekonomisk skada för verksamhetsutövaren enligt 3 §.

Enligt 3 kap. 8 § CSL-föreskrifterna ska även vissa typer av återkommande incidenter betraktas som betydande och därmed rapporteringspliktiga. Bestämmelsen om återkommande incidenter syftar till att fånga upp strukturella problem hos verksamhetsutövaren som resulterar i återkommande incidenter med höga kostnader. Det kan handla om brister i organisatoriska rutiner såväl som bristande tekniska säkerhetsåtgärder, exempelvis bristande rutiner för säkerhetsuppdateringar. Centralt för huruvida rapporteringsplikten blir gällande är om dessa incidenter leder till upprepade och kostsamma incidenter.

I den här bestämmelsen är grundorsaken central. Grundorsaken kan närmare härledas till en mer specifik utlösande faktor som bidragit till att en incident uppstått.

DEFINITION

Grundorsak

Med grundorsak avses vad som initierar händelseförloppet som gav upphov till incidenten.

Om en och samma grundorsak inträffar minst två gånger inom sex månader och sammantaget har medfört ekonomisk skada för verksamhetsutövaren enligt 3 kap. 3 § CSL-föreskrifterna är incidenterna sammantaget att betrakta som en betydande incident och därför rapporteringspliktig. Detta gäller oaktat vilka faktiska konsekvenser de har haft på verksamhetsutövaren i övrigt utöver de ekonomiska konsekvenserna.

För definitionen av den ekonomiska skadan som de återkommande incidenterna behöver ha medfört för att vara rapporteringspliktig, se avsnitt 3.1.2 i vägledningen. Nedan finns exempel på återkommande incidenter där en enskild incident inte blir rapporteringspliktig, men då typen av incident är återkommande och har samma grundorsak samt har medfört ekonomisk skada träffar den rekvisiten ovan och blir rapporteringspliktig.

EXEMPEL

Återkommande incidenter i journalsystem

Verksamhetsutövare G är en region. Regionen inför ett nytt journalsystem. Det visar sig att systemet innehåller buggar inom en och samma process vilket leder till upprepade mindre incidenter hos ett av regionens sjukhus under en sexmånadersperiod. Detta gör att personalen återkommande, men under kortare perioder, behöver använda alternativa arbetssätt. Sjukhusledningen bedömer att de enskilda incidenterna inte är betydande, men att de samlat utgör en betydande incident då incidenterna sammantaget inneburit en kostnad som överstiger 5 procent av sjukhusets totala intäkter i form av bland annat ökade personalkostnader till följd av övertid. Eftersom att det rör sig om flera återkommande incidenter som alla orsakats av det nya journalsystemet, och som därtill inneburit ekonomisk skada enligt 3 kap. 3 § CSL-föreskrifterna, blir incidenterna samlat rapporteringspliktiga enligt 3 kap 8 § CSL-föreskrifterna.

Kapitel 4

Rapportering av incidenter

4. Rapportering av incidenter

4.1 Rapportering av betydande incidenter – steg för steg

Nedan följer en redogörelse över den process som påbörjas om en verksamhetsutövare som omfattas av CSL-föreskrifterna eller BF-föreskrifterna drabbas av en incident.

Figur 1. Från identifiering till rapportering

Rapporteringsplikten enligt såväl CSL som BF är indelad i flera steg i syfte att åstadkomma rätt balans mellan, å ena sidan, snabb rapportering som bidrar till att begränsa den potentiella spridningen av betydande incidenter och göra det möjligt för väsentliga och viktiga verksamhetsutövare att söka operativt stöd och, å andra sidan, ingående rapportering som ger värdefulla lärdomar av enskilda incidenter.

FAKTARUTA · Beredskapsförordningen

Annan definition av rapporteringspliktig incident enligt BF

Vissa statliga myndigheter omfattas av både beredskapsförordningens och cybersäkerhetslagens bestämmelser om rapporteringsplikt.

En incident blir rapporteringspliktig enligt CSL-föreskrifterna om den anses vara betydande (se 3–4 kap. CSL-föreskrifterna). För att en incident ska vara rapporteringspliktig enligt BF-föreskrifterna gäller istället att:

2 § Med it-incidenter som omfattas av rapporteringsskyldighet menas en incident som

a. negativt har påverkat säkerheten hos den information som har bedömts ha ett behov av utökat skydd
b. har inneburit att informationssystem som behandlar information som har bedömts ha behov av utökat skydd inte har kunnat upprätthålla avsedd funktionalitet
c. negativt har påverkat myndighetens förmåga att utföra sitt uppdrag, eller
d. i övrigt allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten tillhandahåller åt en annan organisation.

Med information som är i behov av ett utökat skydd avses information som på grund av externa krav kräver en viss nivå av skydd avseende konfidentialitet, riktighet inklusive autenticitet, eller tillgänglighet, alternativt information som myndigheten vid värdering bedömer ha behov av motsvarande nivå av skydd.

4.2 Hur rapportering ska ske

2 kap. 1 § CSL-föreskrifterna

När en incident har identifierats som betydande ska uppgifter anges på det sätt och lämnas via de kontaktvägar som har anvisats av Försvarets radioanstalt.

2 kap. 2 § CSL-föreskrifterna

Statliga myndigheter som för samma incident redan helt eller delvis uppfyllt rapporteringsplikt enligt förordningen (2022:524) om statliga myndigheters beredskap ska, inom de tidsfrister som anges i cybersäkerhetslagen, komplettera tidigare inlämnade rapporter för att även uppfylla rapporteringsplikten enligt cybersäkerhetslagen.

För mer information om hur du som verksamhetsutövare rapporterar in betydande incidenter, besök NCSC:s och Myndighetens för civilt försvars webbplatser. I de kommande avsnitten redogörs för de delar av rapporteringen där verksamhetsutövare kan behöva ytterligare stöd. För mer stöd om hur formuläret ska fyllas i, se bilaga 1.

4.2.1 Upplysning

TÄNK PÅ

Vänta inte med att rapportera

Upplysningen är en preliminär rapport och ska lämnas så snart som möjligt, dock senast inom 24 timmar, efter det att incidenten har bedömts vara betydande. När det gäller upplysningen är det viktigare att rapportera i tid och inkomma med preliminära uppgifter. Information kan revideras samt kompletteras i senare rapporteringsskeenden.

Vänta inte med att rapportera för att ni saknar all information. Det går att göra kompletteringar senare.

Det första steget i rapporteringen av betydande incidenter utgörs av en upplysning. Av 2 kap. 3 § i CSL-föreskrifterna framgår vilka uppgifter som ska rapporteras in. Vidare ska dessa uppgifter rapporteras in så snart det kan ske, dock enligt 3–4 kap. i CSL-föreskrifterna senast inom 24 timmar efter att incidenten har identifierats som betydande. Tidsangivelsen om 24 timmar är att betrakta som en bortre tidsgräns. Upplysningen syftar till att snabbt förse mottagande myndigheter med inledande uppgifter om den inträffade betydande incidenten och ge verksamhetsutövaren möjlighet att vid behov få hjälp. Uppgifterna som lämnas i upplysningen kan vara baserade på preliminära bedömningar.

Vilka uppgifter som ska lämnas i upplysningen regleras i 2 kap. 3 § CSL-föreskrifterna, och av rapporteringsformuläret (se bilaga 1 för mer vägledning).

2 kap. 3 § CSL-föreskrifterna

Upplysning ska lämnas så snart det kan ske, dock senast inom 24 timmar efter att incidenten identifierats som betydande enligt 3–4 kap.

Upplysning ska innehålla följande uppgifter:

1. verksamhetsutövarens namn, kontaktuppgifter och organisationsnummer
2. om incidenten är pågående
3. händelseförlopp samt när och hur incidenten upptäcktes
4. om incidenten har orsakats av misstänkt avsiktligt skadliga eller misstänkt olagliga handlingar
5. i det fall incidenten har sitt ursprung hos en leverantör; information om leverantören
6. påverkan på verksamhetsutövarens sektorsverksamhet
7. vilka konsekvenser incidenten medför eller riskerar att medföra, och
8. om incidenten har eller riskerar att få gränsöverskridande konsekvenser.

Uppgifterna som lämnas enligt p. 2–8 ska vara baserade på en preliminär bedömning av den betydande incidenten.

I upplysningen ska verksamhetsutövaren lämna sina kontaktuppgifter i syfte att berörda myndigheter kan kontakta verksamhetsutövaren vid behov, till exempel tillsynsmyndigheten i händelse av frågor om incidentrapporteringen eller NCSC/CERT-SE för frågor om operativt stöd.

Verksamhetsutövaren ska även lämna uppgift om den betydande incidenten misstänks ha orsakats av avsiktligt skadliga eller olagliga handlingar. En avsiktligt skadlig handling avser en handling med potentiellt skadliga konsekvenser för verksamhetsutövaren.

HÄNVISNING

Misstänker du brott?

Om ni misstänker att incidenten har orsakats av en olaglig handling, ska den också rapporteras in till Polismyndigheten.

För att anmäla dataintrång, utpressningsangrepp, överbelastningsangrepp eller nätfiske, kontakta Polismyndigheten: polisen.se/utsatt-for-brott/polisanmalan/bedrageri/dataintrang

Från och med den 1 oktober 2022 vidarebefordras inrapporterade incidenter som har sin grund i brottslig handling till Polismyndigheten, där en polisanmälan kan komma att upprättas.

Därtill ska verksamhetsutövaren beskriva påverkan på sektorsverksamhet. Detta avser påverkan på den egna sektorsverksamheten. Bedrivs verksamhet inom flera sektorer, är det den sektorsverksamhet eller de sektorsverksamheter som har påverkats av den betydande incidenten som ska uppges. Sektorsverksamhet utgörs av de typer av verksamhet som anges i kolumn 3 i bilaga 1 eller 2 till NIS2-direktivet.[15] Om incidenten är rapporteringspliktig enligt EU-kommissionens genomförandeförordning[16], ska erbjudna tjänster uppges istället för sektorsverksamhet. För mer vägledning om erbjudna tjänster, se PTS webbplats.

Slutligen ska verksamhetsutövaren uppge konsekvenser och gränsöverskridande konsekvenser. Vilka konsekvenser incidenten medför eller riskerar att medföra avser hur incidenten har påverkat den angivna sektorsverksamheten negativt. Det är viktigt att rapportera för att snabbt få en bild av incidentens initiala påverkan och omfattning.

Med gränsöverskridande konsekvenser avses konsekvenser utanför Sveriges gränser. Förmågan att upptäcka och effektivt hantera gränsöverskridande konsekvenser betonas särskilt i NIS2-direktivet, eftersom många medlemsstater inom EU använder sig av samma tjänster. Alla störningar, även sådana som inledningsvis är begränsade till en verksamhetsutövare eller en sektor, kan få

Not 15. För mer vägledning kring sektor och sektorsverksamhet, se Myndigheten för civilt försvar, Vägledning för anmälan och identifiering av verksamhetsutövare som omfattas av cybersäkerhetslagen, 2026.

Not 16. EU-kommissionens genomförandeförordning 2024/2690 av den 17 oktober 2024 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster.

dominoeffekter i vidare bemärkelse, vilket kan leda till långtgående och långvariga effekter på tillhandahållandet av tjänster på hela den inre marknaden. Exempel på gränsöverskridande konsekvenser av en betydande incident kan vara att el som produceras i Sverige för konsumtion i Danmark kanske inte kommer att kunna levereras då produktionen ligger nere under en störning. För att hantera sådana gränsöverskridande konsekvenser och underlätta hantering och samarbete, ska det därför anges i upplysningen om incidenten har, eller riskerar att få, gränsöverskridande effekter.

FAKTARUTA · Beredskapsförordningen

Annan tidsfrist för statliga myndigheter som omfattas av BF-föreskrifterna

Det är viktigt att notera att en upplysning enligt BF ska lämnas redan efter 6 timmar medan en upplysning enligt CSL-föreskrifterna ska lämnas efter 24 timmar efter att incidenten har bedömts som rapporteringspliktig. I övrigt är tidsgränserna harmoniserade mellan regelverken. Det innebär att ett ytterligare rapporteringsskede tillkommer för den som rapporterar enligt BF i jämförelse med de tidigare gällande föreskrifterna om it-incidentrapportering för statliga myndigheter (MSBFS 2020:8), rapportering efter 72 timmar tillkommer alltså. Likaså tillkommer skyldigheten att inkomma med en lägesrapport.

Vilken information som ska lämnas regleras av CSL-föreskrifterna.

4.2.2 Incidentanmälan

Det andra steget i rapporteringen av en betydande incident utgörs av en incidentanmälan. Så snart det kan ske, men senast 72 timmar efter att verksamhetsutövaren har identifierat incidenten som betydande, ska verksamhetsutövaren lämna en uppdatering av uppgifterna som lämnats i upplysningen samt ytterligare uppgifter.

FAKTARUTA · CSL-föreskrifterna

· TILLHANDAHÅLLARE AV BETRODDA TJÄNSTER

Det råder andra tidsgränser för upplysning och incidentanmälan för tillhandahållare av betrodda tjänster. Tillhandahållare av betrodda tjänster har 24 timmar på sig att inkomma med upplysning och incidentanmälan. De kan lämnas in samtidigt eller vid ett par olika tillfällen, så länge det sker inom 24 timmar.

2 kap. 4 § CSL-föreskrifterna

Incidentanmälan ska lämnas så snart det kan ske, dock senast 72 timmar efter att verksamhetsutövaren har identifierat incidenten som betydande enligt 3–4 kap.

Incidentanmälan ska innehålla en uppdatering av uppgifter som har lämnats enligt 3 § samt följande uppgifter:

1. när incidenten inträffade
2. när incidenten upphörde eller en uppskattning av hur länge incidenten förväntas pågå
3. en bedömning om incidentens orsak
4. påverkan på system
5. i tillämpliga fall, information om angreppsindikatorer, och
6. i tillämpliga fall, påverkan på information i behov av utökat skydd.

Verksamhetsutövare som tillhandahåller betrodda tjänster ska komma in med information enligt första stycket inom 24 timmar.

I incidentanmälan ska verksamhetsutövaren uppge när incidenten inträffade, samt när den upphörde. Om tidpunkterna inte är kända vid rapporterings-tillfället kan man i formuläret uppge ungefärlig tidpunkt, eller okänd tidpunkt. Om incidenten inte har upphört, är den att betrakta som pågående tills dess verksamhetsutövaren kan återgå till normaldrift eller tills dess verksamhets-utövaren bedömer att hanteringen av incidenten är avslutad.

KATEGORIER

6 st orsakskategorier i formuläret

Incidenten har uppstått som en konsekvens av:

- **[Systemfel]:** ett fel i mjuk- eller hårdvara.
- **[Mänskligt misstag]:** en oavsiktlig handling, exempelvis till följd av oaktsamhet eller okunskap.
- **[Angrepp]:** en uppsåtlig handling, exempelvis cyberangrepp eller sabotage.
- **[Naturhändelse]:** ett naturfenomen, exempelvis oväder eller inverkan från skadedjur.
- **[Annan orsak]:** en typ av händelse som inte specificeras i ovan kategorier.
- **[Okänt]**: en okänd orsak.

I det fall incidenten bedöms vara orsakad av ett cyberangrepp ska även angreppsindikatorer uppges, om man har tillgång till sådan information. I detta skede ska verksamhetsutövaren lämna information om att man har, eller inte har, tillgång till sådan information. NCSC återkommer med anvisningar för hur information om angreppsindikatorer ska översändas. Angreppsindikatorer (Indicators of Compromise, IoC), är tekniska spår från ett cyberangrepp. Angreppsindikatorer kan exempelvis senare användas av andra organisationer för att upptäcka samma skadliga aktivitet i deras nätverks- eller informationssystem. Dessa kan även användas för att förstå hur ett angrepp har gått till.

Exempel på angreppsindikatorer är:

- IP-adresser som har försökt ansluta till organisationens nätverk
- länkar (url:er) till webbplatser som använts för nätfiske eller skadlig programvara
- uppgifter om skadlig kod (till exempel namn på skadlig kod eller filnamn)
- uppgifter om e-post (till exempel avsändarens e-postadress, mottagarens e-postadress, rubrik på e-post, information om header och innehåll, bifogade filer)
- uppgifter om nätverksaktivitet (portar, protokoll, adresser, headers, särskilda mönster i nätverkstrafiken, särskilda loggar)
- unika digitala fingeravtryck för skadliga filer (exempelvis virus eller trojaner)
- ovanliga eller misstänkta filer som inte borde finnas i organisationens system
- inloggningsförsök från avvikande platser eller tidpunkter eller
- användare som plötsligt får högre systembehörigheter

KATEGORIER

6 st systemskategorier i formuläret

System som…

- **[Administrativt system]:** används för administrativ databehandling, kontorsautomation eller affärssystem.
- **[System för processtyrning / operativ teknik (OT)]:** styr eller övervakar fysiska processer och utrustning, till exempel i industri, produktion, energi eller vattenförsörjning.
- **[System dedikerat till information eller kommunikation]:** lagrar, hanterar eller överför information, till exempel e-post, dokumenthantering, intranät eller kommunikationsplattformar.
- **[System för säkerhetslösningar]:** skyddar verksamheten, till exempel brandväggar, antivirus, inloggningslösningar eller övervakningssystem.
- **[Annat system]:** inte passar in i någon av kategorierna ovan.
- **[Okänt system]:** används när det inte går att avgöra vilka system som påverkats av incidenten.

Verksamhetsutövaren ska även uppge påverkan på system, där begreppet system hänvisar till nätverks- och informationssystem. Vidare ska det även uppges om information i behov av utökat skydd har påverkats. Information i behov av utökat skydd definieras närmare i tabell två i andra kapitlet i denna vägledning.

4.2.3 Slutrapport eller lägesrapport

KATEGORIER

6 st informationskategorier i formuläret

Kan exempelvis vara…

- **[Verksamhetskritisk information]:** vara driftdata, loggar eller systeminställningar.
- **[Konfidentiell information]:** driftdata, affärsavtal, interna styrrapporter.
- **[Information som är viktig för mottagare av era tjänster]:** bokningseller beställningsuppgifter.
- **[Känslig information]:** säkerhetsklassad information eller uppgifter om sårbarheter i system.
- **[Personuppgifter]:** namn, adress eller telefonnummer.
- **[Annan information i behov av utökat skydd]:** andra uppgifter som inte omfattas av kategorierna ovan.

2 kap. 5 § CSL-föreskrifterna

Slutrapport ska lämnas senast en månad efter incidentanmälan eller en månad efter att incidenten har hanterats. Den ska innehålla en uppdatering av uppgifter som har lämnats enligt 3–4 §§ samt följande uppgifter:

1. en slutlig bedömning av den betydande incidentens konsekvenser, där bedömningen i tillämpliga fall ska innehålla information om
   a. det uppskattade antalet mottagare av verksamhetsutövarens tjänster som drabbats av incidenten
   b. berört geografiskt område
   c. ekonomisk skada
   d. gränsöverskridande konsekvenser, och
   e. påverkan på viktiga samhällsfunktioner
2. så långt möjligt en detaljerad beskrivning av incidentens grundorsak,
3. en beskrivning av vilka tekniska och organisatoriska åtgärder som har vidtagits för att hantera incidenten, och, i tillämpliga fall, som har vidtagits eller kommer att vidtas för att
   a. hantera och minimera konsekvenserna av incidenten, och
   b. undvika att liknande incidenter inträffar.

Det tredje steget i rapporteringen av betydande incident utgörs av en slutrapport. Det finns två olika bortre tidsgränser för inlämnande av slutrapporten. Slutrapport ska lämnas senast en månad efter incidentanmälan, eller en månad efter att incidenten har hanterats. Med hanterats avses att incidenten slutligt är avhjälpt.

Slutrapporten ska innehålla en slutlig bedömning av incidentens konsekvenser. Detta inkluderar en uppskattning av antalet mottagare av tjänsten som drabbats av incidenten. På en övergripande nivå kan mottagare av tjänster ses som alla fysiska samt juridiska personer som använder de tjänster som verksamhetsutövaren tillhandahåller och som omfattas av CSL. Vem som är mottagare av tjänster kan vara olika beroende på vilken sektor som berörs. För att skapa jämförbarhet mellan sektorerna ska verksamhetsutövaren därför i formuläret uppge en uppskattning på antalet fysiska personer som påverkats av incidenten.

Därtill ska det berörda geografiska området som påverkats anges. Det geografiska området i denna kontext avser inom Sveriges gränser. Med ekonomisk skada menas det som framgår av 3 kap. 3 § i CSL-föreskrifterna (se avsnitt 3.1.2 i denna vägledning). Med gränsöverskridande konsekvenser avses konsekvenser utanför Sveriges gränser. Utöver detta ska verksamhetsutövaren uppge påverkan på viktiga samhällsfunktioner.[17]

Not 17. För mer vägledning kring viktiga samhällsfunktioner, se Myndigheten för civilt försvar Lista med de viktigaste samhällsfunktionerna, 2026.

Påverkan innebär att en viktig samhällsfunktion inte kan levereras till en del av befolkningen enligt normalfallet. Det handlar inte om att en enskild verksamhet inte kan leverera sina tjänster, utan att en hel samhällsfunktion blir påverkad till den grad att den får svårigheter att leverera till de som använder den. Verksamhetsutövaren ska basera bedömningen om påverkan på den samhällsviktiga funktionen utifrån tillgänglig information om påverkan.

Slutrapporten ska innehålla en detaljerad beskrivning av incidentens grundorsak. Med grundorsak avses vad som initierar, eller möjliggör, händelseförloppet som gav upphov till incidenten. Därtill ska vidtagna tekniska och/eller organisatoriska åtgärder, det vill säga de åtgärder som har vidtagits för att hantera incidenten, uppges. Det kan vara olika beroende på situation, exempelvis att informera anställda som kan påverkas av incidenten, eller att inleda en felsökning i interna system.

2 kap. 6 § CSL- föreskrifterna

Om incidenten fortfarande är pågående efter en månad ska verksamhetsutövaren istället för en slutrapport lämna en lägesrapport. Den ska innehålla följande uppgifter:

1. varför incidenten fortfarande är pågående
2. en uppskattning av hur länge incidenten förväntas pågå
3. om incidenten fortfarande påverkar eller riskerar att påverka verksamhetsutövarens sektorsverksamhet, och
4. i tillämpliga fall, information om angreppsindikatorer.

I det fall en incident fortfarande är pågående, det vill säga att verksamheten inte ännu har gått tillbaka till normaldrift, efter en månad så ska verksamhetsutövaren inkomma med en lägesrapport. En incident anses vara pågående tills dess verksamhetsutövaren kan återgå till normaldrift eller tills dess verksamhetsutövaren bedömer att hanteringen av incidenten är avslutad. Vilka uppgifter som ska rapporteras i lägesrapporten bedöms inte föranleda behov av närmare vägledning.

4.3 Rapportering av incidenter som träffar flera sektorer

Vissa verksamhetsutövare bedriver sektorsverksamhet inom flera sektorer som omfattas av CSL och behöver därför behöva ta hänsyn till olika kriterier för rapportering inom de olika sektorerna.

En incident som har haft konsekvenser inom flera sektorer ska inom ramen för rapporteringsplikten beaktas som en och samma incident och därför rapporteras som en incident. När rapporteringsplikt uppstår inom flera olika typer av sektorsverksamheter till följd av en och samma incident bör verksamhetsutövaren utgå från de tidsfrister som uppstår när incidenten först bedömdes vara rapporteringspliktig. Verksamhetsutövaren kan därefter komplettera med ytterligare information om påverkan på annan sektors-verksamhet vid ett senare tillfälle.

4.4 Skydd av information vid incidentrapportering

Information som lämnas till en myndighet är som utgångspunkt allmän handling. En myndighet får bara begränsa insynen om det finns en tillämplig sekretessbestämmelse i offentlighets- och sekretesslagen (2009:400) (OSL). Det är alltid enskilda uppgifter, inte hela handlingar eller ärenden, som kan omfattas av sekretess, och ett beslut att inte lämna ut en allmän handling i sin helhet eller att lämna ut sådan handling med förbehåll kan överklagas till kammarrätten. I händelse av en begäran om uppgifter i en incidentrapport genomför myndigheten en självständig bedömning av föreliggande sekretess.

Flera olika sekretessgrunder i OSL kan vara tillämpliga för att hantera sekretess av uppgifter i incidentrapporter. En av de mest centrala för verksamhetsutövare som rapporterar enligt CSL är 18 kap. 8 b § OSL som säger att:

”Sekretess gäller för uppgift i en incidentrapport enligt cybersäkerhetslagen (2025:1506) och för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas.” Denna bestämmelse ger ett starkare sekretesskydd och infördes i samband med att CSL trädde i kraft.

Notera att verksamhetsutövare är skyldiga att genomföra en bedömning om det finns säkerhetskyddsklassificerade uppgifter inom ramen för incident-rapporteringen. Om så är fallet gäller särskilda rutiner för att skicka in upp-lysning, incidentanmälan, samt slutrapport.

Kapitel 5

Informationsskyldighet vid betydande incidenter och betydande cyberhot

5. Informationsskyldighet vid betydande incidenter och betydande cyberhot

CSL-föreskrifterna innehåller, utöver bestämmelser om rapporteringen av betydande incidenter (3–4 kap. CSL-föreskrifterna), bestämmelser om informationsskyldighet till mottagare vid betydande incidenter och vid betydande cyberhot (5 kap. CSL-föreskrifterna).

Informationsskyldigheten är också en viktig del i att höja nivån på cybersäkerheten i hela samhället. Den syftar till att information till mottagare av tjänster ska lämnas för att begränsa och förhindra konsekvenser av incidenten. Vägledande för tillämpning av informationsskyldigheten är att bestämmelsen syftar till att minska negativa spridningseffekter av en betydande incident. Det är risken för spridningseffekter samt andra allvarliga konsekvenser som avgör vilka mottagare som bör informeras vid både betydande incidenter och betydande cyberhot.

Informationsskyldigheten till mottagare av verksamhetsutövares tjänster enligt CSL är fristående från incidentrapporteringsskyldigheten. Däremot är informationsskyldigheten vid betydande incidenter avhängig bestämmelserna om vad som utgör en betydande incident enligt CSL-föreskrifterna för de verksamheter som omfattas av 3–4 kap. i CSL-föreskrifterna.[18]

Not 18. PTS ansvarar för informationsskyldigheten för sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster (mellan företag), rymden och post- och budtjänster. För mer information om informationsskyldigheten för dessa sektorer, besök PTS webbplats.

5.1 Informationsskyldighet vid betydande incidenter

5 kap. 1 § CSL-föreskrifterna

Verksamhetsutövare ska, så snart det kan ske, informera mottagare om en betydande incident som har påverkat en eller flera externa tjänster som tillhandahålls till mottagare och ska då lämna följande uppgifter:

1. vad den betydande incidenten består i
2. i tillämpliga fall, vilka åtgärder som mottagarna av verksamhetsutövarens tjänster behöver vidta för att begränsa den betydande incidentens konsekvenser, och
3. i tillämpliga fall, vad konsekvenserna kan bli om mottagarna inte vidtar åtgärder enligt p. 2.

Information enligt första stycket ska inte lämnas om verksamhetsutövaren bedömer att sådan information kan försvåra hantering av den betydande incidenten eller förvärra dess konsekvenser.

Enligt 5 kap. 1 § CSL-föreskrifterna behöver verksamhetsutövare informera mottagare om betydande incidenter som har påverkat en eller flera externa tjänster som de tillhandahåller inom en sektorsverksamhet. Notera att verksamhetsutövaren endast behöver informera om den betydande incidenten, som har påverkat externa tjänster som tillhandahålls till mottagare. Om den betydande incidenten endast har påverkat den interna verksamheten, och inte fått följdeffekter på tillhandahållandet av externa tjänster, så behöver verksamhetsutövaren inte informera mottagare om den betydande incidenten.

Mottagare av tjänster kan ha olika innebörd beroende på vilken sektor som berörs. På en övergripande nivå kan mottagare av tjänster ses som alla fysiska samt juridiska personer som använder de tjänster som verksamhetsutövaren tillhandahåller och som utgör sektorsverksamhet enligt CSL. De mottagare som i sin tur ska informeras om en betydande incident inkluderar dem som kan eller kommer att påverkas av den specifika incidenten. Mottagare som använder vissa av verksamhetsutövarens externa tjänster, men som inte aktivt använder den påverkade tjänsten, behöver inte informeras om den betydande incidenten.

Tillvägagångssättet för informationsgivningen bör anpassas efter vilka som utgör mottagarna av den påverkade tjänsten. Mottagarna av tjänsten kan exempelvis informeras genom information på verksamhetsutövarens webbplats, via en direktkontakt med mottagaren, exempelvis via sms eller mejl, eller genom en kungörelse i en dagstidning. Det viktiga är att kommunikationssättet är ändamålsenligt för att minska eller motverka den betydande incidentens potentiellt negativa konsekvenser. Verksamhetsutövaren bör fördelaktigen använda sig av spårbara kanaler.

Noterbart är att verksamhetsutövaren inte alltid behöver dela information enligt punkt 2 och punkt 3 i 5 kap. 1 § CSL-föreskrifterna, utan den informationen ska endast delas i tillämpliga fall. Informationsskyldighetens punkt 2 och punkt 3 bör endast tillämpas i de fall verksamhetsutövaren vet att mottagare kan minska risken för följdverkningar om de vidtar vissa åtgärder, samt känner till vilka åtgärder som bör vidtas. Verksamhetsutövaren bör basera beslut om vilka åtgärder som mottagaren bör vidta på en bedömning på sådan information som den har tillgänglig eller med enkla medel kan komma över.

Verksamhetsutövaren ska informera mottagare av tjänster så snart det kan ske, men inte vid en tidpunkt där verksamhetsutövaren bedömer att det försvårar hanteringen av den betydande incidenten. Information till mottagare av tjänster ska inte lämnas i de fall verksamhetsutövaren bedömer att det kan försvåra hanteringen av den betydande incidenten.

EXEMPEL

Kommunalt vattenbolag informerar allmänheten om allvarlig driftstörning

Verksamhetsutövare H är ett kommunalt vattenreningsbolag. Vattenreningsbolaget har drabbats av en allvarlig driftstörning där ett system för styrning och kontroll av rening av dricksvatten har varit otillgängligt i mer än 4 timmar, vilket har påverkat dricksvattenförsörjningen i delar av kommunen. Eftersom att det är en betydande incident som riskerar att påverka delar av kommunens invånare, bedömer vattenreningsbolaget att de behöver informera invånarna om incidenten och att invånarna för en tid behöver vara sparsamma med sin vattenförbrukning. För att nå ut till så många mottagare som möjligt väljer bolaget att publicera information i enlighet med 5 kap. 1 § CSL-föreskrifterna på deras webbsida, samt att kontakta media för att nå ut med informationen.

5.2 Informationsskyldighet vid betydande cyberhot

5 kap. 2 § CSL-föreskrifterna

Verksamhetsutövare ska, så snart det kan ske, informera mottagare om ett betydande cyberhot som kan påverka system som tillhandahålls till mottagare och som inte utgör en betydande incident. Verksamhetsutövaren ska lämna följande uppgifter:

1. vad cyberhotet består i
2. i tillämpliga fall, vilka åtgärder mottagarna behöver vidta för att minimera risken för att cyberhotet resulterar i en incident, och
3. i tillämpliga fall, vad konsekvenserna kan bli om mottagarna inte vidtar dessa rekommenderade åtgärder.

Information enligt första stycket p. 1 ska inte lämnas om verksamhetsutövaren bedömer det som olämpligt med hänsyn till att det kan öka risken för att en incident uppstår.

Enligt 5 kap. 2 CSL-föreskrifterna ska verksamhetsutövare även informera mottagare av tjänster om betydande cyberhot. Noterbart behöver verksamhetsutövare endast informera mottagare av system. Det innebär att informationsskyldigheten om betydande cyberhot endast är tillämplig för de verksamhetsutövare som tillhandahåller system, alltså nätverks- och informationssystem, till mottagare.

I likhet med bestämmelserna om informationsskyldigheten vid betydande incidenter så bör informationsgivningen och valda kommunikationssätt vara ändamålsenliga med beaktande av vad bestämmelsen syftar till. Vilka mottagare som ska informeras om det betydande cyberhotet avgörs av vilka mottagare som kan drabbas av cyberhotet och därmed har nytta av informationen. Likaså bör verksamhetsutövare kommunicera med mottagarna på det sätt som är lämpligast för att motverka spridningseffekter och minska risken för allvarliga konsekvenser.

Verksamhetsutövaren behöver inte alltid dela information enligt punkt 2 och punkt 3. I likhet med bestämmelserna om informationsskyldighet vid betydande incidenter behöver informationen endast lämnas i tillämpliga fall. Verksamhetsutövaren bör basera beslut om vilka åtgärder som mottagaren bör vidta på en bedömning på sådan information som den har tillgänglig eller med enkla medel kan komma över.

Informationen bör delas med berörda verksamhetsutövare så snart det kan ske för att minska risken för att en eller flera incidenter uppstår. Om verksamhetsutövaren bedömer att informationsdelningen riskerar att öka risken för att en incident uppstår så behöver information enligt punkt 1 inte lämnas.

Bilagor

Bilaga 1 – Förklaring av formulärfält

Incidentrapportering enligt cybersäkerhetslagen och beredskapsförordningen

I denna bilaga beskrivs fälten i Myndigheten för civilt försvars rapporteringsverktyg för betydande incidenter. Bilagan är avsedd som stöd för verksamhetsutövare som omfattas av cybersäkerhetslagen (CSL) och statliga myndigheter som även omfattas av beredskapsförordningen (BF). Varje fält beskrivs kortfattat med en angivelse av om det är obligatoriskt och vilka rapportörer det berör.

Verksamhetsutövare inom sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster (mellan företag), post- och budtjänster samt rymden omfattas av CSL och rapporterar via samma formulär. Tröskelvärdena för vad som utgör en betydande incident regleras dock för dessa sektorer av kommissionens genomförandeförordning (EU) 2024/2690 och, från oktober 2026, av Post- och telestyrelsens föreskrifter. Se pts.se för närmare vägledning.

Färgen i högerkolumnen i tabellerna nedan visar för vem fältet är relevant:

Alla	Fältet besvaras av samtliga rapportörer.
CSL eller CSL+BF	Verksamhetsutövare som omfattas av CSL eller av båda regelverken.

Rapporteringsplikt

Rapportering inleds med att bedöma och uppge vilken eller vilka rättsliga grunder som ger upphov till rapporteringsplikt. Om verksamhetsutövaren omfattas av flera olika rapporteringspliktiga grunder, väljs dessa och formuläret fylls i en gång.

Typ av information	Information som ska lämnas	Gäller för
Rättslig grund för rapporteringsplikt	Ange den eller de rättsliga rapporteringsgrunder som har uppstått. Samma incident kan vara rapporteringspliktig enligt en eller flera av Cybersäkerhetslagen, Beredskaps-förordningen, Kommissionens genomförandeförordning samt PTS-föreskrifter enligt Cybersäkerhetslagen. Inom respektive rättslig grund finns det en följdfråga som ska besvaras kring incidentens omständighet. (**Obligatoriskt**)	Alla

Upplysning

Upplysning ska lämnas så snart det kan ske, dock senast 24 timmar efter att incidenten har identifierats som betydande. För statliga myndigheter enligt BF gäller en bortre tidsgräns om 6 timmar. För tillhandahållare av betrodda tjänster gäller senast 24 timmar för både upplysning och incidentanmälan. Upplysningen är en inledande rapport och preliminära uppgifter, såsom uppskattningar, räcker när faktiska uppgifter om den betydande incidenten inte finns att tillgå ännu.

Typ av information	Information som ska lämnas	Gäller för
Information om verksamhets-utövaren	Verksamhetsutövarens organisationsnamn, organisations-nummer (eller motsvarande för utländsk organisation), samt namn, e-postadress och telefonnummer till kontakt-person nåbar under hanteringen samt för rapporteringen. (**Obligatoriskt**)	Alla
Information om leverantör vid leveranskedje-incident	Ange om incidenten hos den egna organisationen är ett resultat av en incident hos leverantör. Om incidenten uppstått hos en leverantör, ange då även leverantörens namn, organisationsnummer och beskriv tjänsten. (**Obligatoriskt**)	Alla
Incidentens händelseförlopp och upptäckt	Beskriv incidentens händelseförlopp och vad som gjorts för att hantera den. Ange även om incidenten fortfarande är pågående, när och hur den upptäcktes samt om det bedöms att den orsakats av en avsiktlig skadlig eller olaglig handling. Om incidenten bedöms ha orsakats av en avsiktlig skadlig eller olaglig handling, beskriv varför bedömningen gjorts. (**Obligatoriskt**)	Alla
Sektorsverksamhet hos organisationen som har påverkats av incidenten	Om incidenten är rapporteringspliktig enligt cybersäkerhets-lagen, uppge vilken eller vilka sektorsverksamheter som incidenten har påverkat och beskriv hur detta yttrat sig. (**Obligatoriskt**)	CSL eller CSL+BF
Incidentens gränsöverskridande konsekvenser	Ange om incidenten fått konsekvenser utanför Sverige och om så i vilka EU/EES-medlemstater eller andra länder utöver dessa. Beskriv även de gränsöverskridande konsekvenserna för länderna som har specificerats i den tidigare delfrågan. (**Obligatoriskt**)	Alla
Operativt stöd från CERT-SE vid pågående incident	Ange om ni vill få operativt stöd från CERT-SE. Det går alltid bra att kontakta CERT-SE på 010-240 40 40 för stöd, även efter upplysningen har skickats in. (**Obligatoriskt**)	Alla

Incidentanmälan

Incidentanmälan lämnas inom 72 timmar från det att incidenten identifierats som betydande. För tillhandahållare av betrodda tjänster gäller 24 timmar, vilket innebär att upplysning och incidentanmälan lämnas samtidigt. Uppgifterna från upplysningen uppdateras och kompletteras med fälten nedan. Sekretessbedömningen bör ses över på nytt eftersom incidentens karaktär kan ha förändrats.

Typ av information	Information som ska lämnas	Gäller för
Incidentens status	Om incidenten inte avslutats när upplysningen lämnats in, ska ni ange om incidenten fortfarande pågår vid tidpunkten då incidentanmälan görs. Om så, avgör hur länge den väntas pågå och beskriv det fortsatta händelseförloppet och vad som gjorts för att hantera den. Ni ska även avgöra när inträffade hos er organisation, när hantering inleddes och när incidenten upphörde (om incidenten är avslutad). (**Obligatoriskt**)	Alla
Incidentens orsak	Utifrån de givna alternativen, avgör vad som har orsakat incidenten och beskriv hur det valda alternativet gav upphov till incidenten. Om incidenten bedöms ha orsakats av ett angrepp, specificera om ni har tillgång till angreppsindikatorer eller inte. (**Obligatoriskt**)	Alla
Incidentens påverkan på system	Välj den eller de typer av system i er organisation som har påverkats av incidenten och specificiera hur konfidentialitet, riktighet, autenticitet och tillgänglighet hos systemen påverkats. Beskriv även i fritext hur systemet eller systemen fungerar i normalläge och hur de påverkats av incidenten. (**Obligatoriskt**)	Alla
Incidentens påverkan på information i system	Välj den eller de typer av information i behov av utökat skydd i er organisation som har påverkats av incidenten och specificiera hur konfidentialitet, riktighet, autencitet och tillgänglighet hos dessa påverkats. Beskriv även i fritext hur informationen har påverkats av incidenten. (**Obligatoriskt**)	Alla
Incidentens konsekvenser för mottagare av organisationens sektorsverksamhet	Ange inom vilka viktiga samhällsområden mottagare av era tjänster har påverkats och beskriv konsekvenserna som har uppstått och eller riskerar uppstå. (**Obligatoriskt**)	Alla

Lägesrapport

Om incidenten fortfarande pågår efter en månad lämnas en lägesrapport i stället för slutrapport. Slutrapport lämnas därefter inom en månad från att incidenten har hanterats.

Typ av information	Information som ska lämnas	Gäller för
Lägesrapport	Beskriv varför incidenten är fortsatt pågående inom en månad och vad som har gjorts för att hantera den sedan Incidentanmälan lämnats in. Ni ska även bedöma hur länge incidenten väntas pågå, huruvida er sektors-verksamhet fortsatt påverkas och om ni har tillgång till angreppsindikatorer. (**Obligatoriskt**)	Alla

Slutrapport

Slutrapport lämnas senast en månad efter incidentanmälan eller efter att incidenten har hanterats, beroende på vilket som inträffar senast. Pågår incidenten längre lämnas en lägesrapport (se avsnitt 4.2.3) och slutrapport därefter inom en månad från det att incidenten har hanterats.

Typ av information	Information som ska lämnas	Gäller för
Incidentens grundorsak	I incidentanmälan uppgavs tidigare orsaken till incidenten. I slutrapporten skall ni även uppge grundorsaken till incidenten, vilken kan vara samma om bedömningen kvarstår, eller nu inkomma med en annan bedömning. Ni ska även uppge i fritext hur grundorsaken gav upphov till incidenten. (**Obligatoriskt**)	Alla
Incidentens påverkan på viktiga samhällsfunktioner	Välj den eller de viktiga samhällsfunktioner som har påverkats av incidenten. Beskriv även i fritext hur denna påverkan har yttrat sig. (**Obligatoriskt**)	Alla
Incidentens påverkan på mottagare av organisationens tjänster	Ange antalet mottagare av era tjänster som har påverkats av incidenten i Sverige. Om ni har angett att incidenten fått gränsöverskridande konsekvenser, skall ni även ange hur många mottagare som påverkats utanför Sverige. Med mottagare i detta sammanhang avses antal fysiska personer som använder de tjänster verksamhetsutövaren tillhandahåller och som påverkas av incidenten. Ni ska även ange om er bedömning är fastställd eller en uppskattning. (**Obligatoriskt**)	Alla
Incidentens geografiska påverkan	Ange var i Sverige incidenten fått konsekvenser. Det är möjligt att ange hela landet, i specifika län eller en specifik plats (såsom en lokal, stad eller anläggning). (**Obligatoriskt**)	Alla
Incidentens gränsöverskridande konsekvenser	I slutrapporten ska ni bedöma om incidenten nu fått gränsöverskridande konsekvenser vid tillfället då rapporten lämnas. Om så, välj de EU/EES-medlemstater eller länder utanför och beskriv hur konsekvenserna yttrat sig. (**Obligatoriskt**)	CSL eller CSL+BF
Incidentens ekonomiska konsekvenser	Ange om det har uppkommit ekonomisk skada till följd av incidenten. Om så, välj vilken eller vilka typer av ekonomisk skada, hur stor andel av föregående års omsättning det motsvarar och uppskatta summan. Ni ska även gör en bedömning om summan är fastställd eller en uppskattning. (**Obligatoriskt**)	Alla
Organisationens åtgärder	Ange om er organisation haft kännedom om typen av incident sedan tidigare, om en kontinuitetsplan fanns och kunde användas, samt om det fanns mål för kontinuitetshantering. Ni ska även ange de åtgärder er organisation har vidtagit eller planerar att vidta genom att beskriva åtgärdens mål och syfte och status.	Alla
Stöd från Cybersäkerhets-rådgivningen	Ange om ni önskar få stöd från cybersäkerhetsrådgivningen med att förebygga liknande incidenter och om så vilken typ av stöd ni önskar få.	Alla

Bilaga 2 – Checklista för incidentrapportering

Checklistan kan ses som en summering av vad man som verksamhetsutövare ska tänka på vid incidentrapporteringen.

Checklista för incidentrapportering	
Steg 1 **Ha följande redo innan ni börjar rapportera**	☐ Organisationsnamn och organisationsnummer.
	☐ Namn, e-postadress och telefonnummer till kontaktperson för incidenten.
	☐ Vilken sektorsverksamhet hos er som incidenten har påverkat.
	☐ En preliminär bedömning av om incidenten kan ha gränsöverskridande konsekvenser.
	☐ e-legitimation för cyberportalen på www.cyberportal.ncsc.se.
Steg 2 **Identifiera incidenten**	☐ En händelse har inträffat som påverkar tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten i era system eller tjänster.
Steg 3 **Bedöm om incidenten är rapporteringspliktig**	☐ Incidenten har orsakat eller kan orsaka allvarlig driftstörning (se kapitel 3.1.1).
	☐ Incidenten har orsakat eller kan orsaka ekonomisk skada (se kapitel 3.1.2).
	☐ Incidenten har orsakat eller kan orsaka betydande skada för andra fysiska eller juridiska personer (se kapitel 3.1.3).
	☐ Har flera incidentert inträffat minst två gånger inom de senaste sex månaderna med samma grundorsak? Om ja, kan incidenterna sammantaget vara rapporteringspliktiga även om de var för sig inte uppfyller kriterierna, se avsnitt 3.1.5.

Checklistan fortsätter!

Checklista för incidentrapportering	
Steg 4 **Lämna upplysning inom 24 timmar**	☐ Upplysningen lämnas via cyberportalen på www.cyberportal.ncsc.se.
	☐ Upplysningen ska baseras på preliminära uppgifter. Ange vad ni vet och komplettera senare.
	☐ Statliga myndigheter som även omfattas av beredskapsförordningen: upplysning lämnas inom 6 timmar.
	☐ För tillhandahållare av betrodda tjänster gäller det att både upplysning och incidentanmälan ska lämnas inom 24 timmar, gå direkt till steg 5.
Steg 5 **Lämna incidentanmälan inom 72 timmar**	☐ Uppdatera informationen från upplysningen.
	☐ Ange när incidenten inträffade och när hanteringen inleddes.
	☐ Gör en bedömning av incidentens orsak.
	☐ Ange påverkan på system.
	☐ Inkludera angreppsindikatorer om sådana finns.
	☐ Ange påverkan på information i behov av utökat skydd om sådan påverkan funnits.
Steg 6 **Lämna slutrapport senast en månad efter incidentanmälan**	☐ Uppdatera informationen från upplysning och incidentanmälan.
	☐ Ange hur många externa användare som kan ha drabbats, vilket geografiskt område som berörs och uppskatta den ekonomiska skadan.
	☐ Ange gränsöverskridande konsekvenser och påverkan på viktiga samhällsfunktioner om det funnits.
	☐ Beskriv incidentens grundorsak så detaljerat som möjligt.
	☐ Beskriv vilka tekniska och organisatoriska åtgärder som ni har vidtagit för att begränsa skadan, samt åtgärder för att undvika liknande incidenter framöver.
	☐ Om incidenten fortfarande pågår ska ni istället lämna en lägesrapport (se nedan).

Checklistan fortsätter!

Checklista för incidentrapportering	
Lägesrapport **Om incidenten fortfarande pågår efter en månad**	☐ Förklara varför incidenten fortfarande är pågående.
	☐ Ange en uppskattning av hur länge incidenten förväntas pågå.
	☐ Ange om incidenten fortfarande påverkar sektorsverksamheten.
	☐ Inkludera angreppsindikatorer om tillämpligt.
	☐ Lämna slutrapport inom en månad efter att incidenten har hanterats.
Steg 7 **Informera mottagare av tjänster om den betydande incidenten**	☐ Om incidenten påverkar externa tjänster är det viktigt att informera mottagarna så fort som möjligt.
	☐ Beskriv vad incidenten består av.
	☐ Ange vilka åtgärder mottagarna behöver vidta för att begränsa konsekvenserna om tillämpligt.
	☐ Ange vad konsekvenserna kan bli om mottagarna inte vidtar åtgärder om tillämpligt.
	☐ Lämna inte information om det kan försvåra incidenthanteringen eller förvärra konsekvenserna.
Steg 8 **Kontrollera om incidenten även utgör en personuppgiftsincident**	☐ Har incidenten medfört att personuppgifter röjts, förlorats eller hanterats av någon obehörig?
	☐ Om ja, ska incidenten även rapporteras till Integritetsskyddsmyndigheten (IMY) inom 72 timmar. Det är en skyldighet enligt data-skyddsförordningen (GDPR).

Bilaga 3 – Ansvariga tillsynsmyndigheter

Det finns flera tillsynsmyndigheter för regleringen kopplad till CSL, vilka utövar tillsyn över olika sektorer. Tillsynsmyndigheterna genomför exempelvis tillsyn över att verksamhetsutövare anmäler sig, vidtar säkerhetsåtgärder, rapporterar betydande incidenter samt följer regleringen i övrigt.

Nedanstående myndigheter är tillsynsmyndigheter för respektive sektor:

- **Energimyndigheten:** Energi.
- **Finansinspektionen:** Bankverksamhet, Finansmarknadinfrastruktur.
- **Inspektionen för vård och omsorg:** Vårdgivare i hälso- och sjukvårdssektorn.
- **Livsmedelsverket:** Avloppsvatten, Dricksvatten, Produktion, bearbetning och distribution av livsmedel.
- **Läkemedelsverket:** Hälso- och sjukvårdssektorn, med undantag för vårdgivare, Tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik.
- **Länsstyrelserna:** Avfallshantering. Enskilda lärosäten med examenstillstånd. Forskning. Offentlig förvaltning med undantag för länsstyrelserna. Tillverkning av datorer, elektronikvaror och optik. Tillverkning av elapparatur. Tillverkning av övriga maskiner. Tillverkning, produktion och distribution av kemikalier.
- **Post- och telestyrelsen:** Digital infrastruktur, Digitala leverantörer, Förvaltning av IKT-tjänster, Post- och budtjänster, Rymden, Verksamhetsutövare som erbjuder domännamnsregistreringstjänster samt för länsstyrelserna.
- **Transportstyrelsen:** Transporter samt Tillverkning av motorfordon, släpfordon, påhängsvagnar och Tillverkning av andra transportmedel.

Med **Länsstyrelsen** avses Länsstyrelserna i Norrbottens, Skåne, Stockholms, Västra Götalands, Örebro respektive Östergötlands län. Verksamhetsutövarens säte avgör vilken av dessa länsstyrelser som utövar tillsyn.

- **Länsstyrelsen i Norrbottens län** är tillsynsmyndighet för kommuner och regioner som hör till Jämtlands, Norrbottens, Västerbottens eller Västernorrlands län och verksamhetsutövare som har sitt säte i något av dessa län.
- **Länsstyrelsen i Skåne län** är tillsynsmyndighet för kommuner och regioner som hör till Blekinge, Kronobergs eller Skåne län och verksamhetsutövare som har sitt säte i något av dessa län.
- **Länsstyrelsen i Stockholms län** är tillsynsmyndighet för kommuner och regioner som hör till Gotlands eller Stockholms län och verksamhetsutövare som har sitt säte i något av dessa län.

- **Länsstyrelsen i Västra Götalands län** är tillsynsmyndighet för kommuner och regioner som hör till Hallands eller Västra Götalands län och verksamhetsutövare som har sitt säte i något av dessa län.
- **Länsstyrelsen i Örebro län** är tillsynsmyndighet för kommuner och regioner som hör till Dalarnas, Gävleborgs, Södermanlands, Uppsala, Värmlands, Västmanlands eller Örebro län och verksamhetsutövare som har sitt säte i något av dessa län.
- **Länsstyrelsen i Östergötlands län** är tillsynsmyndighet för kommuner och regioner som hör till Jönköpings, Kalmar eller Östergötlands län och verksamhetsutövare som har sitt säte i något av dessa län.

Tillsynsmyndigheterna samverkar i ett gemensamt forum som leds av Myndigheten för civilt försvar. Syftet med forumet är att underlätta samordning och uppnå en effektiv och likvärdig tillsyn enligt CSL. Från och med den 1 juli 2026 kommer detta samarbetsforum att ledas av NCSC.

Incidentrapportering och informationsskyldighet

Myndigheten för civilt försvar

NATIONELLT CYBERSÄKERHETSCENTER
En del av FRA