Cybersäkerhetslagen och beredskapsförordningen • Incidentrapportering

Så rapporterar du – steg för steg

Handlingsguide: vad gör du när det väl händer?

SCENARIO

Klockan är 02:00. Du är it-tekniker på en mindre ort. Larmet går och något verkar fel.
Du upptäcker en pågående cyberattack mot er verksamhet. Vad gör du nu?

Steg för steg

☐ **1. Andas, du har tid att tänka**
Ett första skede (Upplysning) ska lämnas inom 24 timmar efter att incidenten bedömts vara rapporteringspliktig. För statliga myndigheter som omfattas av beredskapsförordningen gäller i stället 6 timmar. Det är okej att uppgifterna är preliminära, du kan komplettera/revidera i nästa skede.

☐ **2. Samla in basuppgifter**
Ha följande redo innan du loggar in på cyberportalen via **ncsc.se/csl**

- Organisationsnamn och organisationsnummer.
- Kontaktperson nåbar under incidenthanteringen (namn, e-post, telefon).
- Vilken sektorsverksamhet som er organisation bedriver och som incidenten påverkat.
- E-legitimation för inloggning (endast svensk eID accepteras).
- Saknar du svensk e-legitimation? Använd reservförfarandet, läs mer på **ncsc.se/csl**.

Överväg om ni vill ha operativt stöd från CERT-SE i hanteringen, kontaktuppgifter finns längst ned.

☐ **3. Sekretessbedöm innehållet**
Välj förfarande efter informationsklassning.

- **Inte säkerhetsskyddsklassificerade uppgifter:** rapportera i cyberportalen.
- **Säkerhetsskyddsklassificerade uppgifter:** det är frivilligt att lämna säkerhetsskyddsklassificerade uppgifter vid ifyllandet av formuläret. Läs mer på **ncsc.se/csl.**

Om cyberportalen är otillgänglig, använder du reservförfarandet. Läs mer på **ncsc.se/csl.**

☐ **4. Fyll i och skicka in första skedet (Upplysningen)**
Logga in på cyberportalen och lämna första skedet inom 24 timmar (Upplysningen). Vad som ska inkluderas framgår av tabellen på nästa sida, preliminära uppskattningar räcker.

☐ **5. Spara incident-ID**
Du får en kvittens med ett incident-ID. Spara det, du behöver det för att rapportera in det andra skedet inom 72 timmar (Incidentanmälan) och därefter det tredje skedet inom en månad (Slutrapport).

TÄNK PÅ

Vänta inte med att rapportera för att ni saknar information.
Upplysningen är preliminär, rapportera snabbt och revidera/komplettera i senare skeden.

NATIONELLT CYBERSÄKERHETSCENTER
En del av FRA

Medfinansieras av Europeiska unionen

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cybersäkerhetslagen och beredskapsförordningen • Incidentrapportering

Så rapporterar du – steg för steg

Från förberedelse till slutrapport: vad ska in, när och hur

Tidslinjen för incidentrapportering

Verksamhetsutövare

1 – 24 timmar
Upplysning
6 timmar för statliga myndigheter med beredskapsförordningen

2 – 72 timmar
Incidentanmälan
24 timmar för tillhandahållare av betrodda tjänster

3 – 1 månad
Slutrapport
Efter incidentanmälan eller efter att incidenten hanterats

NCSC
Via cyberportalen

Vad ingår i varje rapport?

Begrepp förklaras närmare i vägledningen om incidentrapportering och informationsskyldighet.

Upplysning
Inom 24 timmar

- Namn, kontaktuppgifter och organisationsnummer.
- Händelseförlopp: när och hur incidenten upptäcktes.
- Misstänkt avsiktligt skadlig eller olaglig handling.
- Ursprung hos leverantör, om tillämpligt.
- Påverkan på sektorsverksamheten och konsekvenser.
- Gränsöverskridande konsekvenser.

Incidentanmälan
Inom 72 timmar

- Uppdaterar uppgifterna från upplysningen.
- När incidenten inträffade och upphörde (eller hur länge den väntas pågå).
- Bedömning av incidentens orsak.
- Påverkan på nätverks- och informationssystem och samhällskonsekvenser.
- Om cyberangrepp, angreppsindikationer.
- Om tillämpligt, påverkan på information i behov av utökat skydd.

Slutrapport
Inom 1 månad

- Uppdaterar tidigare uppgifter.
- Slutlig bedömning av konsekvenser: antal drabbade, geografiskt område, ekonomisk skada.
- Gränsöverskridande konsekvenser och påverkan på viktiga samhällsfunktioner, om tillämpligt.
- Detaljerad beskrivning av grundorsaken.
- Vidtagna tekniska och organisatoriska åtgärder.
- Om incidenten fortfarande pågår, lämna lägesrapport i stället.

TÄNK PÅ

Incidenter som har sin grund i brottslig handling vidarebefordras till Polismyndigheten, där en polisanmälan kan komma att upprättas. Läs mer om hur rapportering ska ske i vägledningen om incidentrapportering och informationsskyldighet.

För stöd vid pågående incident, kontakta CERT-SE

Ring **010-382 80 00** eller mejla **cert@cert.se**. Telefonkontakt ersätter inte den skriftliga rapporteringen.

NATIONELLT CYBERSÄKERHETSCENTER
En del av FRA

Medfinansieras av Europeiska unionen

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE