Malin Ekblad
Säkerhetschef
malin.ekblad@trelleborg.se

Kommunstyrelsen

Bilaga 3 a - Rutin IT säkerhetincident-säkerhetsincidentrapportering

Enligt bestämmelser om rapportering av IT-incidenter enligt 20 § förordningen (2015:1052) är vi skyldiga att rapportera in IT-incidenter till MSB.

Det finns två förfarande att hantera säkerhetsincidentrapportering på; internt och externt, där allvarligheten på incidenten avgör tillvägagångsättet av rapporteringen. Vid extern rapportering finns beskrivning nedan, vid intern rapportering se separat formulär på Slettnet: ”Formulär för säkerhetsincident”.

IT-säkerhetsincidenter

De IT-säkerhetsincidenter som ska rapporteras in är sådana som;

- påverkat riktigheten, tillgängligheten eller konfidentialiteten hos den information som bedömts ha behov av utökat skydd, eller
- inneburit att informationssystem som behandlar information som bedömts ha behov av utökat skydd inte kunnat upprätthålla avsedd funktionalitet, eller
- påverkat myndighetens förmåga att utföra sitt uppdrag, eller i övrigt allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Varje myndighet behöver göra en självständig bedömning av vilka IT-incidenter som allvarligt kan påverka säkerheten i organisationens informationssystem.

Steg 1 (Inom 6 timmar)

- Notifiera närmaste chef om incidenten som tar ärendet vidare tills sin chef, som i sin tur sedan kontakta CERT-SE vid MSB via telefon 010-240 40 40. Detta händelseförlopp ska ske **inom 6h**.

- CERT-Se kommer ställa följande frågor:
    - Vad har hänt?

  - Hur och när upptäcktes problemet?
  - Vilka parter är inblandade i incidenthanteringen?
  - Finns det en brottsmisstanke och har en polisanmälan upprättats?
  - Behov av stöd från CERT-SE och kontaktvägar för detta?

- **Informera** IT avdelningen och informationssäkerhetssamordnaren om händelsen via formuläret: Formulär för säkerhetsincident som finns på Slettnet.

- Vidta nödvändiga åtgärder (vid osäkerhet kontakta IT)

Steg 2 (inom fyra veckor)

- Sammanställ en slutrapport enligt länken nedan, vilken ska **skickas inom fyra veckor** till e-postadress: rapport@it-incident.se.

Kräver skyddsvärdet extra säkerhet, tillhandahåller MSB en kryptolösning som avser att ge skydd vid överföring via e-post. Om uppgifter som omfattas av sekretess och som rör Sveriges säkerhet, så kallad säkerhetsskyddsklassificerad uppgift, tidigare så kallad ”hemliga uppgift”, säkerhetsskyddslagen 2018:585 ska överföras, så ska detta ske via lämpligt signalskyddssystem, personlig leverans eller eventuellt REK/VÄRDE-post.

Länk till MSB:s rapporteringsformulär för steg 2:

https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering/msbs-incidentrapporteringsformular-for-statliga-myndigheter.pdf