Stöd för ifyllnad av formuläret för it-incidentrapportering

Syftet med detta dokument är att ge stöd till hur ”Formulär för it-incidentrapportering” ska fyllas i.

I det fall utrymmet i formulärets fritextfält inte räcker till för att ge efterfrågad information kan en bilaga bifogas.

Ytterligare stöd kan hittas på www.cert.se. Innehåll:

1. Grunduppgifter

Avsnittet innehåller ett antal grunduppgifter avseende organisationen som rapporterar it-incidenten.

1.1 Myndighetens namn

Ange namnet på den rapporterande myndigheten.

1.2 Organisationsnummer

Ange organisationsnumret för den rapporterande myndigheten.

1.3 Rapporterad av

Ange namnet på den person som rapporterat incidenten, vanligtvis den person som fyller i formuläret.

1.4 Myndighetens kontaktfunktion

Ange namnet på eller en kort beskrivning av myndighetens kontaktfunktion.

1.5 Kontaktfunktionens e-postadress

Ange e-postadressen till myndighetens kontaktfunktion.

1.6 Kontaktfunktionens telefonnummer

Ange telefonnummer till myndighetens kontaktfunktion.

1.7 Myndighetens ärendenummer

Ange den rapporterande myndighetens ärendenummer om ett sådant finns.

2. Berörda uppdragsgivare

Detta avsnitt behöver endast fyllas i av de myndigheter som tillhandahåller tjänster åt en eller flera andra organisationer (uppdragsgivare) och det är en sådan tjänst som har drabbats av it-incidenten.

Enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska en myndighet som tillhandahåller tjänster åt en annan organisation ska i samband med rapportering enligt första stycket informera och vid behov samråda med den eller de uppdragsgivare som berörs av incidenten.

2.1 Berörda uppdragsgivare, myndigheter

Ange de myndigheter som påverkats av it-incidenten – det vill säga myndigheter som använder tjänster från den rapporterande myndigheten och som har drabbats av it-incidenten.

2.2 Berörda uppdragsgivare, övriga organisationer

Ange de eventuella organisationer, utöver myndigheter, som påverkats av it-incidenten – det vill säga övriga organisationer som använder tjänster från den rapporterande myndigheten och som har drabbats av incidenten.

2.3 Information har lämnats till

Ange vilka berörda uppdragsgivare som har informerats i samband med rapporteringen (ange organisationens namn).

2.4 Samråd har skett med

Ange de berörda uppdragsgivare som samråd har skett med i samband med rapporteringen (ange organisationens namn).

3. Bedömd sekretess

3.1 Bedömd sekretess av rapporterad information

Ange vilken nivå av sekretess den rapporterade informationen har.

4. Polisanmälan

4.1 Är händelsen polisanmäld?

Ange Ja eller Nej.

4.2 Polisanmälan bifogad som bilaga

En kopia av polisanmälan ska bifogas som bilaga. Ange Ja om detta görs. Detta innebär att information i punkt 2 samt 5 – 9 inte behöver anges.

4.3 Polisanmälans diarienummer

Ange det diarienummer som polisanmälan tilldelats, i de fall myndigheten har kännedom om detta.

5. Beskrivning av it- incident

5.1 Typ av händelse

Ange om incidenten är konstaterad eller misstänkt.

5.2 Incidentstatus

Ange om incidenten är pågående, avbruten/hanterad eller avslutad.

5.3 Kort beskrivning av incidenten

Denna beskrivning bör innehålla information om vad som inträffat samt en övergripande redovisning av händelseförlopp och vidtagna åtgärder. Var gärna så specifik som möjligt.

6. Tidpunkt

I detta avsnitt anges när incidenten upptäckts och inträffat, samt om tiden för detta är uppskattad eller exakt.

6.1 När upptäcktes incidenten

Ange datum och klockslag för när incidenten upptäcktes samt om tiden är exakt eller uppskattad. Tidpunkt för upptäckt räknas från dess att information om it-incidenten hanteras i utpekad intern process för hantering av it-incidenter eller när säkerhetsansvarig eller motsvarande fått kännedom om incidenten.

6.2 När inträffade incidenten

Ange datum och klockslag för när incidenten inträffade samt om tiden är exakt eller uppskattad.

7. Kategori

I MSBs föreskrifter (MSBFS 2016:2) om statliga myndigheters rapportering av it-incidenter[1] anges ett antal kategorier av it- incidenter. I följande avsnitt förklaras dessa mer ingående.

7.1 Störning i mjukvara

Med detta avses fel i system eller programvara. Det kan vara att systemet är felaktigt implementerat, att oväntade funktioner uppkommer i system eller operativsystem. Även systemkrascher räknas hit, oavsett om systemkraschen gäller en applikation eller ett operativsystem.

---

[1] Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2).

7.2 Störning i hårdvara

Med detta avses fel i komponenter, oväntade funktioner i hårdvara eller hårdvarukomponenter.

7.3 Störning i driftmiljö

En störning kan exempelvis bestå i haveri i ett tekniskt system eller komponent i infrastrukturen. Det kan också vara en förlust av tillgänglighet i system. Hit räknas även störningar i system med säkerhetsfunktioner, exempelvis säkerhetskopiering, loggningssystem m.m. Det kan även vara att en molntjänst slutar fungera eller att servrar eller it-tjänster är otillgängliga.

7.4 Informationsförlust

Informationsförluster kan vara permanenta eller temporära. Exempelvis är en informationsförlust orsakad av brand i serverhall ofta permanent, medan systemfel eller en omfattande överbelastningsattack kan leda till temporär tillgänglighetsförlust. Kategorin förlust av tillgänglighet till information i myndighetens informationssystem kan exempelvis inkludera felaktig avyttring av teknisk utrustning som innehåller information som inte ska vara allmänt tillgänglig. Ange orsaken till varför informationsförlust uppstått, exempelvis om utrustningen stulits, tappats bort, att oavsiktlig radering skett eller eventuella andra orsaker.

7.5 Informationsläckage

Med informationsläckage avses otillåtet tillgängliggörande av information som inte ska vara allmänt tillgänglig. Informationsläckage innebär att myndighetens information inte gått förlorad men att någon på obehörigt sätt skaffat sig tillgång till den.

Läckage kan röra personuppgifter, eller annan information. Ange i så fall vilken typ av information det rör sig om. Var så specifik som möjligt.

Vid informationsläckage kan det vara svårt att bedöma hur stor spridning informationen fått eller om läckaget inneburit att aktören som skaffat sig tillgång till informationen behållit den för eget bruk. Osäkerhet kring hur stor spridning informationen fått bör därför beaktas vid bedömningen av hur allvarlig incidenten är.

7.6 Informationsförvanskning

Förvanskning av information kan leda till att informationen helt eller delvis har blivit korrumperad, manipulerad eller att det inte går att säkerställa dess riktighet.

7.7 Hindrad tillgång till information

Hindrad tillgång till information kan exempelvis innebära att informationen eller ett system där informationen finns inte kan användas på avsett sätt.

7.8 Säkerhetsbrist i produkt

Kategorin kan exempelvis innefatta it-incidenter orsakade av säkerhetsluckor eller annan sårbarhet i tekniskt hjälpmedel som används av myndigheten.

7.9 Angrepp

Det kan ofta vara svårt att i ett initialt skede avgöra varifrån ett angrepp kommer eller om det faktiskt rör sig om ett angrepp. Till angrepp räknas exempelvis överbelastningsattack (t.ex. DDoS), införande av skadlig kod,

intrång i informationssystem (s.k. hackning), olovligt nyttjande eller annat missbruk av lösenord, olovlig åtkomst till information genom skadliga program och obehörig användning av informationssystem.

Som angrepp räknas även angrepp som möjliggjorts eller genomförts av egen personal eller personer som på motsvarande sätt har en anknytning till den drabbade myndigheten, exempelvis inhyrd personal.

Huvudkategorin Angrepp är indelad i ett antal underkategorier i enlighet med den struktur och taxonomi som rekommenderas av Europeiska nät- och informationssäkerhetsbyrån, ENISA.[2] I denna kategori kan fler än ett svar väljas vid behov.

7.10 Handhavandefel

Med handhavandefel avses ett mänskligt handlande som innebär internt felaktigt bruk eller felaktig implementering av tekniskt system eller komponent. Det kan exempelvis vara misskonfigurationer eller att information distribueras på ett felaktigt sätt t.ex. pga. kompetens- eller kunskapsbrist eller stress.

7.11 Oönskad eller oplanerad störning i kritisk infrastruktur

Funktionen hos myndighetens informationssystem är ofta starkt beroende av tillgång till extern försörjning av el och kommunikationstjänster, men även interna system för att trygga funktionen i kritisk infrastruktur. Till kategorin bör därför räknas it-incidenter som orsakas av exempelvis elektriskt fel, vattenskada eller störning i funktioner för avbrottsfri kraftförsörjning, kylning eller ventilation.

7.12 Annan plötslig oförutsedd händelse som lett till skada

Detta kan vara it-incidenter som orsakats av en annan anledning än det som omfattas av kategorierna ovan och som därmed inte bedöms kunna sorteras in i någon av dessa kategorier. Detta skulle t.ex. kunna vara händelser orsakade av tredje part såsom leveransförseningar på nödvändiga reservdelar.

8. Omfattning och konsekvenser

8.1 Störning i verksamhetskritiska tjänster

Här avses den störning som har skett i verksamhetskritiska tjänster. Ange hur stor påverkan varit genom att välja ett av alternativen.

8.2 Återställning

Med återställning avses här arbetet med att återupprätta funktionaliteten hos drabbade system. Om återställning skett, ange tiden som har krävts för återställningsarbetet eller om återställningstiden är okänd.

8.3 Beskrivning av omfattning och konsekvenser

Beskriv myndighetens initiala bedömning av it- incidentens omfattning och konsekvenser, både faktiska och potentiella.

---

[2] ”Information sharing and common taxonomies between CSIRTs and Law Enforcement” (https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement/at_download/fullReport) December 2015

9. Övrigt

Här kan annan information om it-incidenten fyllas i som kan tänkas vara av intresse för MSB att känna till. Detta kan t.ex. vara kännedom om fel i programvara där rapporterande myndighet befarar att fler myndigheter är utsatta för samma problem. MSB kan då hjälpa till att sprida informationen.