Verksamheten för samhällets informations- och cybersäkerhet
cert@cert.se

Kurir för it-incident rapportering – Hanteringsregler

Innehåll

1. Förord

1.1. Inledning

Statliga myndigheter ska enligt förordning 2015:1052 från och med den 1 april 2016 till Myndigheten för samhällsskydd och beredskap (MSB) rapportera it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. MSB har med stöd av förordningens 21 § gett ut författningen MSBFS 2016:2 ”Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters rapportering av it-incidenter”.

För att underlätta rapporteringen av it-incidenter tillhandahåller MSB en kryptolösning som ett komplement för att ge skydd vid överföring av it-incidenter till MSB via e-post. Denna kryptolösning är tänkt som en tillfällig lösning tills ordinarie tekniska rapporteringsverktyg är driftsatt. Lösning kommer sedan att vara ett reservalternativ vid de tillfällen då det inte är möjligt att rapportera via ordinarie lösning. Varje myndighet ansvarar själva för att göra bedömning utifrån it-incidentrapportens innehåll om tillhandahållen lösning ger erforderligt skydd.

För vald lösning används filkrypto **Kurir 2.0**. Till kryptolösningen har det tagits fram Hanteringsregler (detta dokument), en snabbguide för installation samt en snabbguide för användning. Systemet kallas i fortsättningen **Kurir it-incident**.

OBS! Detta system är framtaget som ett stöd för rapportering av it-incidentincidenter. Regelverk, instruktioner och kryptonycklar m.m. har anpassats utifrån detta.

1.2. Dokumentets syfte

Detta dokument tar upp allmän information som alla berörda ska veta innan man på något sätt handhar någon del av systemet.

För detaljer kring t.ex. installation, användning, kryptonyckelhantering mm, se andra dokument t.ex. enl. referenser.

Detta dokument vänder sig till installatören (den som utför själva installationen av Kurir It-incident), utsedd kontaktpersonen/funktion mot MSB för it-incidentrapportering och alla användare av kryptolösningen för it-incidentrapportering vid myndigheten.

1.3. Kryptolösningens syfte

MSB tillhandahåller en kryptolösning som kan användas för att ge skydd vid överföring av it-incidentrapporter till MSB via e-post eller annan anvisad kontaktväg. Kryptolösningen baseras på programvaran ”KURIR”, version 2.0, med en av MSB framtagen hantering av kryptonycklar.

Kryptolösningen är tänkt som en övergångslösning tills ett tekniskt rapporterings-verktyg är driftsatt. Den kommer därefter att vara ett reservalternativ som kan användas vid de tillfällen då det inte är möjligt att rapportera ordinarie väg.

MSB bedömer att denna kryptolösning för inrapportering av it-incidenter får användas för att skydda information som omfattas av sekretess enligt 18 kap. 8§ och 18 kap. 13§ i offentlighets- och sekretesslagen, OSL (2009:400). Detta gäller dock inte sådan information som regleras i säkerhetsskyddslagen (1996:627).

Varje myndighet ansvarar själva för att bedöma utifrån it-incidentrapportens innehåll om tillhandahållen lösning ger erforderligt skydd. Om behov av att kunna rapportera in uppgifter som omfattas av sekretess och som rör rikets säkerhet föreligger (s.k. hemliga uppgifter), ska detta ske via lämpligt signalskyddssystem, personlig leverans eller REK/VÄRDE-post.

Programmet är lösenordskyddat och används för att kryptera/dekryptera filer, vilka sedan kan skickas på öppna nätverk t.ex. som bifogad fil med e-post. Programmet använder sig av elektroniska kryptonycklar, vilka distribueras på CD. Kryptonycklarna skyddas även av ett lösenord som distribueras med kryptonyckeln.

Kryptonycklar och tillhörande lösenord samt lösenord för inloggning till programmet ska i grunden hanteras på samma sätt som den information de skyddar eller kan komma att skydda.

1.4. Referenser

#	Ref	Rubrik	Ver	Datum
1	[Hant]	Kurir för it-incidentrapportering – Hanteringsregler	1.0	2016-03-21
2	[Install]	Kurir för it-incidentrapportering – snabbguide - installation	1.0	2016-03-21
3	[Anv]	Kurir för it-incidentrapportering – snabbguide – användare (Detta dokument)	1.0	2016-03-21
#	**Ref**	**Rubrik**	**Ver**	**Datum**
4	[Man]*	Kurir user manual (på CD) (Tutus)	1.0.0	141007

* = Leverantörens manual, innehåller flera hanteringsregler och funktioner, men dessa gäller inte för Kurir it-incident.

2. Systemet

2.1. Delar i systemet

Systemet består av följande delar:

1) Installations CD och licensnummer samt i samband med installation ett egen genererat lösenord.
2) Testnyckel (öppen) samt lösenord till testnyckeln.
3) Dator som programmet installeras på.
   (Myndigheten ansvara själv för anskaffandet av denna dator.
   se krav i guide för installation)
4) Kryptonycklar med lösenord (plomberade tillsammans).

2.2. Hantering

I grunden ska alla delar i systemet hanteras (förvaras, försändas, användas och förstöras) på samma sätt som gäller för den skyddsvärda informationen som hanteras i systemet och i enlighet med myndighetens interna hanteringsregler. Eftersom ingen radering kan anses ”säker” fullt ut, inte ens programmets egna fil-förstörare, ska alla delar i systemet även då den skyddsvärda informationen har raderats hanteras som om det fortfarande innehåller skyddsvärd information och ska hanteras i enlighet med myndighetens interna hanteringsregler.

En fil som har krypterats med en av it-incidentrapporteringsnycklarna kan hanteras som öppen och skickas som bifogad fil över exempelvis internet. Den medföljande testnyckeln får inte hantera skyddsvärd information och ska hanteras på samma sätt som annan ”öppen” information.

Vilka regler som gäller för införsel/utförsel av skyddsvärd information till/från systemets dator definierar myndigheten själv. T.ex. om man använder USB-stickor.

Kopiering av kryptonycklar eller lösenord till kryptonyckel ska godkännas av CERT-SE, detta då CERT-SE är utfärdare av kryptonyckeln.

Lösenord för programmet och för inloggning på datorn, ska förvaras åtskilt från datorn och på ett sådant sätt, så att obehörig inte kan komma åt programmet Kurir It-incident 2.0. Detta reglerar myndigheten själv.

För hantering av kryptonycklar (och dess lösenord) se avsnitt Kryptonycklar.

2.3. Avinstallation/Avveckling/Förstöring

När programmet inte längre används, ska det avinstalleras och raderas från dator, se snabbguide installation.

Hårddisken ska även förstöras (destrueras) utifrån myndighetens interna hanteringsregler som gäller för den typ av information som har hanterats på hårddisken.

Vid avveckling av systemet ska installations CD samt licensnummer skickas tillbaka till MSB på enklaste sätt. Licensnummer skickas enklast till cert@cert.se och installations-CD skickas per brev till MSB, att: CERT-SE.

Myndighetens lösenord till programmet förstörs av myndigheten.

2.4. Funktionsprov/förbindelseprov

Vid installation av systemet Kurir 2.0 för it-incidentrapportering vid en myndighet tilldelas en testnyckel. Denna testnyckel ”Testnyckel_it-incidentrapport” används för att kunna genomföra funktionsprov/förbindelseprov med MSB/CERT-SE efter att programvaran har installerats. Funktionsprov/förbindelseprov bör göras efter genomförd installation för att säkerställa att installationen fungerar korrekt samt för att verifiera att myndighetens brandväggar tillåter krypterade filer med filändelsen ”.kke”. Testnyckeln får inte hantera sekretessbelagda eller andra skyddsvärda uppgifter. Funktionsprov/förbindelseprov görs till cert@cert.se.

3. Kryptonycklar (+Lösenord)

Det finns flera alternativ för kryptonycklar och giltighetstid för dessa. I den första försändelsen som distribuerats till alla myndigheter finns kryptonycklar som har som längst giltighetstid på 1 år per kryptonyckel. Gör myndigheten bedömningen att giltighetstid på 1 år är för lång tid utifrån den information som ska rapporteras eller om frekvensen av inrapportering medför att kortare giltighetstid bör användas så kan kvartalsnycklar användas. Behov av kvartalsnycklar anmäls till cert@cert.se.

3.1. Distribution

Kryptonycklarna kommer i en plomberad försändelse, tillsammans med aktuellt lösenord.

MSB meddelar när ny kryptonyckel ska tas i drift. I de fall myndighet använder kvartalsnycklar så sker detta enligt särskild process.

Vid behov kan nya nycklar beställas från MSB. Beställning görs via cert@cert.se.

3.2. Radering/Förstöring

Utgångna eller förbrukade kryptonycklar (och dess lösenord) eller kryptonycklar som inte behövs ska raderas så snart som möjligt.

På dator kan radering göras med överskrivningsverktyget som finns i programvaran Kurir, för att säkerställa en ordentlig radering.

CD med kryptonyckel (inkl. tillhörande lösenord) ska förstöras enligt myndighetens interna hanteringsregler.

4. Roller

I systemet för Kurir it-incident vid en myndighet finns följande roll:

Kontaktperson/funktion vid myndighet

- Ansvarar för att systemets hanteringsregler efterlevs, t.ex. att rätt lokaler, förvaringsutrymme används, men även att installation och användningen utförs på rätt sätt.
- Ansvarar för kontakten med MSB.
- Ansvarar speciellt för kryptonycklarna och lösenord för dessa (samt förstöring) och är denna kontaktperson som mottar kryptonycklar och lösenord från MSB.
- Inkluderar ansvaret för detta systems rapportering av installation/avinstallation och systemets incidentrapportering.
- Ansvarar för att myndigheten har tagit hand om systemets implementation i organisationen och att det finns interna hanteringsregler för hur själva it-incidentincidenten ska hanteras. Inkluderar även intern hantering inom själva organisationen, t.ex. på myndighetens olika orter.

5. Incidenthantering av kurir 2.0

5.1. Materielincident

Den som upptäcker förlust eller har misstanke om att manipulation av tilldelat system Kurir it-incident har skett, ska rapportera detta till myndighetens interna säkerhetsorganisation. MSB önskar bli informerade om en eventuell materielincident snarast möjligt till cert@cert.se.

5.2. Nyckelincident

Om kryptonyckeln till systemet inte har hanterats på ett korrekt sätt, kommit obehöriga till känna eller har förkommit, finns risk för att obehöriga kan komma åt den information som har krypterats med kryptonyckeln. En kryptonyckel som en obehörig kan ha fått tag i, ska inte användas utan ersättas av en ny kryptonyckel. I första hand tar man nästa nyckel, har man ingen nästa kryptonyckel så kontaktas cert@cert.se.

För rådgivning innan försändning av incidentrapport, kontakta MSB/CERT-SE 08-6785799.