Vad gör Sveriges nationella CERT?

Karl Selin

Incidenthanterare / IT-säkerhetsspecialist

Vad är en CERT?

Computer Emergency Response Team

- CSIRT
- CIRT
- CERT/CC

RFC 2350

- TI – Trusted Introducer
- EGC - European Government CERTs group
- FIRST

Vad är CERT-SE?

- Sveriges nationella CSIRT / CERT
- På uppdrag av regeringen
- Myndigheter och samhällskritisk verksamhet prioriteras
- Cirka 7 300 ärenden under 2019

CERT-SE:s uppdrag

Arbetar förebyggande med att öka it-säkerhetsmedvetandet genom att förmedla kunskap och fakta samt utfärda varningar och råd om sårbarheter i it-system.

Hanterar it-incidenter genom att skyndsamt sprida information samt arbeta med samordning av åtgärder för att avhjälpa eller lindra effekter av det inträffade.

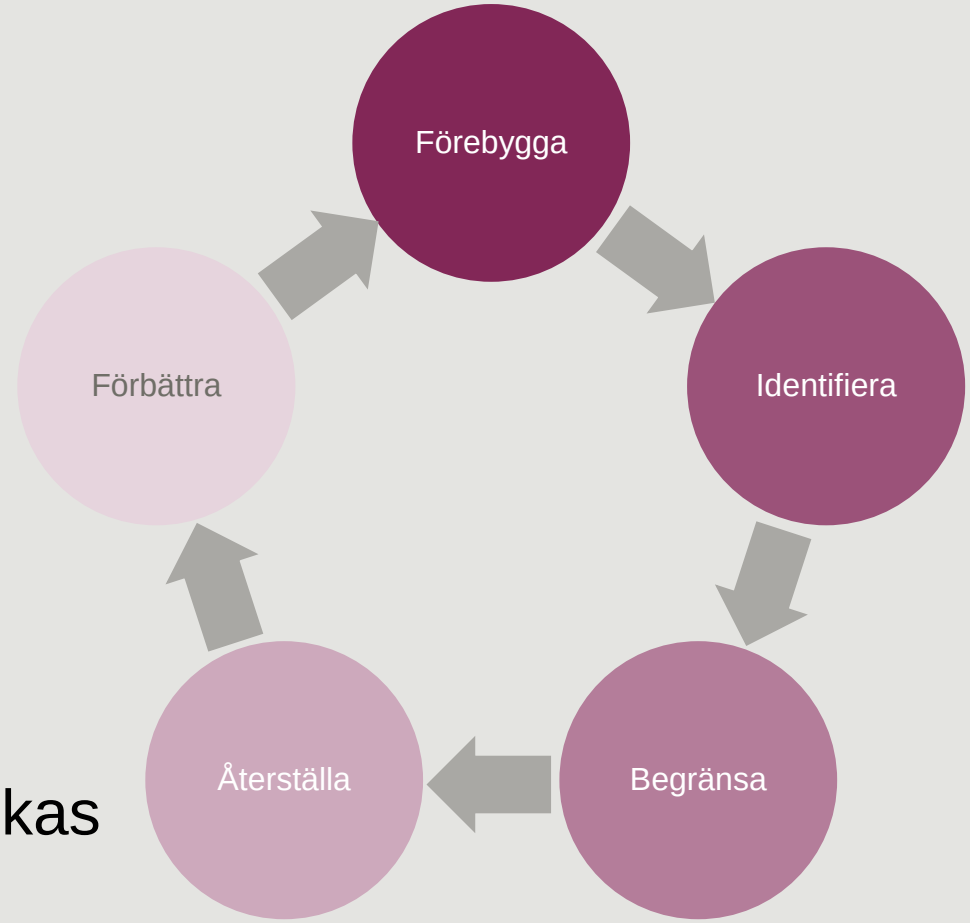
Är Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder.

Incidenthantering

- Vad har hänt?
- Hur och när upptäcktes incidenten?
- Vilka åtgärder har vidtagits?
- Är det en pågående incident?
- Hur kan vi hjälpa till?

Vi finns tillgängliga 24/7/365

Alltid med den grad av sekretess som önskas av de inblandade.



Vad gör CERT-SE?

- Medvetandehöjande aktiviteter
- Omvärldsbevakning av it- och informationssäkerhet
- Obligatorisk it-incidentrapportering / NIS-rapportering
- Forensisk analys
- Teknisk analys
- Abusehantering / Phishing
- Övningsverksamhet
- Capture the Flag / utmaningar

Medvetandehöjande

Vi producerar bland annat rapporter och tekniska rekommendationer.

- Månadsrapporter, blixtmeddelanden och veckobrev med senaste nytt
- Bloggartiklar
- Nyhetsbrevet Läget infosäk
- Skanningar och sårbarhetsanalys
- Föredrag och föreläsningar
- Mediekontakter
- Övningsrapporter

Myndighetssamarbeten

- Försvarsmakten / MUST / FMCERT
- Försvarets radioanstalt
- Polismyndigheten / NOA / UND / PMCERT
- Säkerhetspolisen
- Med flera…

- Svenskt cybersäkerhetscenter – NCSC-SE

Nationell samverkan

CERT-SE deltar i flera samverkansfora för informationsutbyte, omvärldsanalys och produktion av informationsmaterial inom informationssäkerhetsområdet.

- FIDI Drift
- FIDI Finans
- FIDI SCADA
- FIDI Telekom
- FIDI Hälso- och sjukvård
- Svenskt CERT-forum

Internationella samarbeten

Våra internationella samarbeten är betydelsefulla för utbyte av information och gemensam hantering av landsöverskridande incidenter.

Personlig kontakt och förtroende är avgörande. Konferenser, utbildningar och övningar är viktiga beståndsdelar.

- Norden – NCC
- Europa – ENISA, TF-CSIRT och EGC
- Globalt – IWWN, FIRST, NatCSIRT, DHS/CISA

En nationell CSIRT under en pandemi

- Uppdatering av kontaktlistor
- Utökad rapportering
- Informationsspridning
- Utökad övervakning av fokusområden
- Prioritering av ärenden
- Ökad mängd inkomna ärenden

- Business as usual…

Att ta med…

- CERT-SE
  - Sveriges nationella CERT/CSIRT
- Kontakta oss gärna
- Cyberhygien
  - Säkerhetskopior, säkerhetsuppdateringar, begränsade behörigheter
  - Multifaktorsautenticering
  - System- och nätverksdokumentation
  - Testa katastrofåterställningsrutiner

Utmaning! - Cybersäkerhetsmånaden 2020

- CERT-SE:s utmaning 2020 är nu tillgänglig på vår webb
  - Riktad till it-säkerhetsintresserade

Frågor?

Tack för oss!

www.cert.se
cert@cert.se