KONFERENSEN

# INFORMATIONSSÄKERHET FÖR OFFENTLIG SEKTOR

4-5 SEPTEMBER 2018

#infosak18

Myndigheten för samhällsskydd och beredskap

# Avdelningen för cybersäkerhet och skydd av kritisk infrastruktur

Systematiskt Infosäkerhets-arbete

Skydd av kritisk infra

Samuel Taub, analytiker

Strategisk analys

Operativ cybersäkerhet

Peter Jonegård, bitr enhetschef

Vi har gemensamt att vi använder bland annat it-incidentrapporter som råvara.

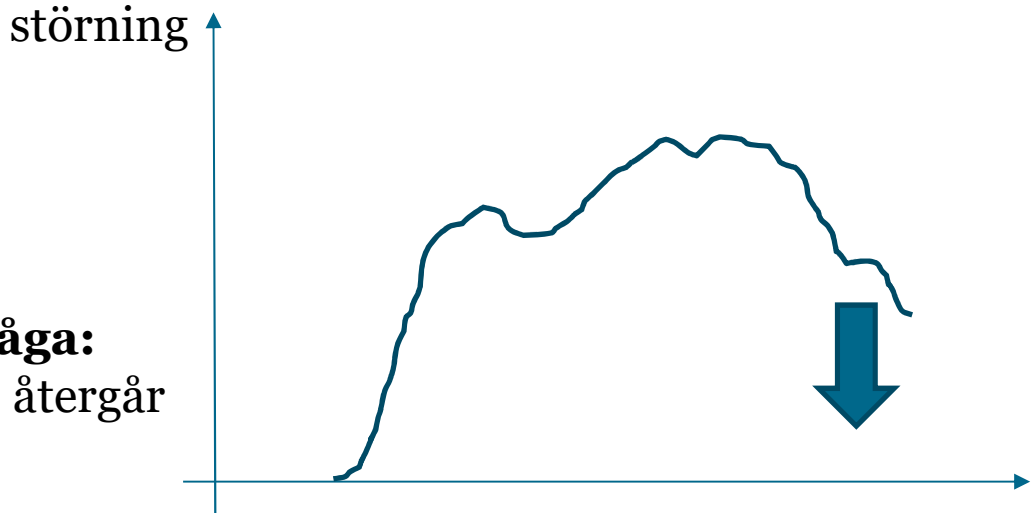
Myndigheten för samhällsskydd och beredskap

# CERT-SE

Enheten ITH utgör den nationella funktionen CERT-SE till vardags, beredskap 24/7
Totalt 24 personer vara många med tung kompetens inom it-säkerhet
Vi omvärldsbevakar och jobbar både förebyggande och med pågående incidenter

Vår övergripande**, förebyggande, fråga** på jobbet:
- Hur höjer vi it-säkerheten i Sverige med den information vi just fick in?
Informera om sårbarheter i produkter
Upplysa organisationer om sannolikt infekterade datorer
En incidentrapport kan innebära att vi ska varna andra i förebyggande syfte

Myndigheten för samhällsskydd och beredskap

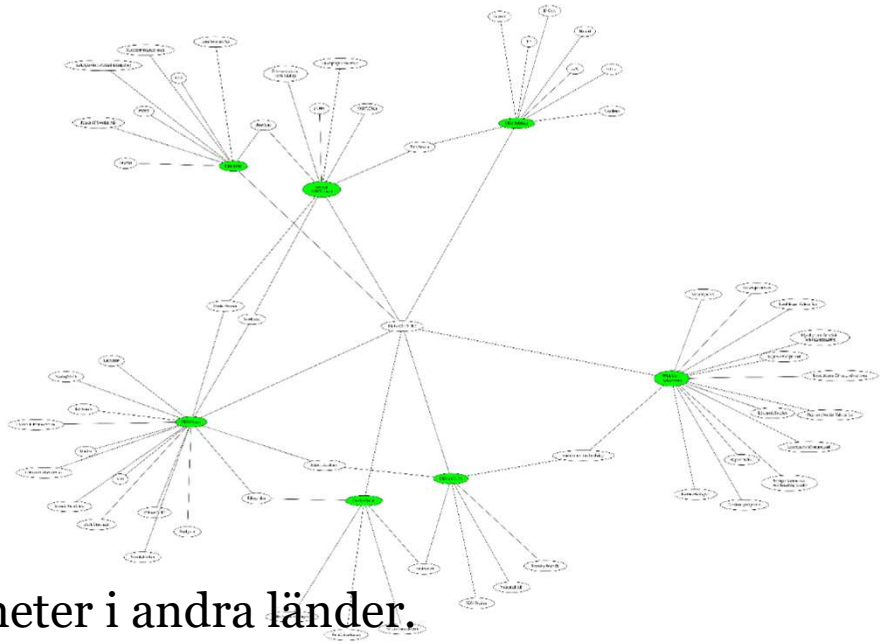



Vår övergripande, **avhjälpande fråga:**
- Hur bidrar vi till att verksamheten återgår till normal, säker nivå?

Vi kan fungera rådgivande eller som spindeln i nätet.
En initial incidentrapport när den drabbade organisationen fått koll på vad det handlar om är en bra start på det arbetet.
Alla rapporter vi får in idag tas upp på dagligt gruppmöte.
- Kan vi hjälpa till direkt?
- Hänger det inträffade ihop med andra saker vi känner till?

Myndigheten för samhällsskydd och beredskap

# CERT-SE med flera



Vi har etablerade nätverk med
it-säkgäng på svenska organisationer
i flera branscher och med våra motsvarigheter i andra länder.

När en incidentrapport kommer in jämför vi med vad vi redan hört från andra men kan också ställa frågor i våra nätverk.
Och kan förmedla erfarenheter och kontakter.
Ju fler som hör av sig, desto större underlag har vi för att förmedla info som kan vara avhjälpande vid incidenter.

Myndigheten för samhällsskydd och beredskap

# Kontakta CERT-SE när det händer

Häng inte upp er incidenthanteringsförmåga på oss, men vi ger alltid så mycket stöd vi har möjlighet till.

Vi hanterar information med respekt och stämmer av vad som redan är publikt.
OSL ger oss stöd att inte peka ut sårbarheter.

Myndigheten för samhällsskydd och beredskap

# Långsiktigt strategiskt arbete

- BÅT

Process för beredning av åtgärdsförslag (BÅT), en process i vilken vi analyserar inkomna incidentrapporter, tillsammans med andra källor, över tid, för att se trender, och bilda oss en uppfattning om vilka åtgärder som är rimliga och ger mest nytta att genomföra för att stärka samhällets informations- och cyberssäkerhet.

- Proaktiv nytta

Alla åtgärder och insatser ska grunda sig i att stärka samhällets informations- och cybersäkerhet, i det långsiktiga perspektivet eftersträvas att kunna göra proaktiv nytta.

- Stödjande/stöttande

MSB:s förmåga att agera stödjande/stöttande är beroende av de inflöden och den data vi har tillgängliga, i denna mängd är incidentrapporter, såväl det statliga obligatoriet (MSBFS2016:2), samt de incidentrapporter som kommer i och med NIS-direktivet väldigt viktiga.

- Inriktande

På lång sikt kan MSB, med rätt underlag agera inriktande, ge rekommendationer till regeringen, vad gäller samhällets informations- och cybersäkerhet, prioriteringar och strategiska beslut kan fattas på väl underbyggda analyser.

Myndigheten för samhällsskydd och beredskap

# Output

- Årsrapporter

MSB rapporterar årligen till regeringen baserat på de inkomna it-incidentrapporterna, rapporten finns på msb.se och sammanfattar det gångna årets incidenter, samt ger rekommendationer.

MSB rapporterar även till EU inom ramen för NIS direktivet, även det på årlig basis.

Samtliga rapporter är anonymiserade och inga incidenter beskrivs i sådan detalj att det går att härleda till någon specifik aktör.

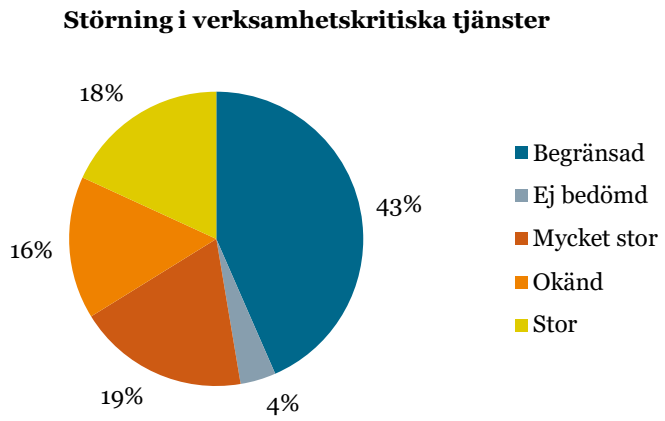
- Månadsrapporter

Cert SE producerar månadsrapporter, som, precis som årsrapporten beskriver månadens rapportering. Denna rapport distribueras idag till samtliga rapporteringspliktiga myndigheter.

Myndigheten för samhällsskydd och beredskap

# 2017 års rapportering

| Incidenttyp | Antal (stycken) |
|---|---|
| Angrepp | 78 |
| Störning i mjuk- eller hårdvara | 60 |
| Handhavandefel | 50 |
| Störning i driftmiljö | 45 |
| Oönskade eller oplanerade störningar i kritisk infrastruktur | 18 |
| Säkerhetsbrist i en produkt | 12 |
| Annan plötslig oförutsedd händelse som lett till skada | 9 |
| Informationsförvanskning | 4 |
| Informationsförlust eller informationsläckage | 3 |
| Hindrad tillgång till information | 2 |
| Totalt | 281 |




Dessa illustrationer kommer från årsrapporten 2017, i den utvecklas resonemang kring kategoriseringar och störningar.

Myndigheten för samhällsskydd och beredskap

# Låt din incidentrapport bli till nytta för dig, oss och alla

cert.se

informationssakerhet.se

fraga.nis@msb.se