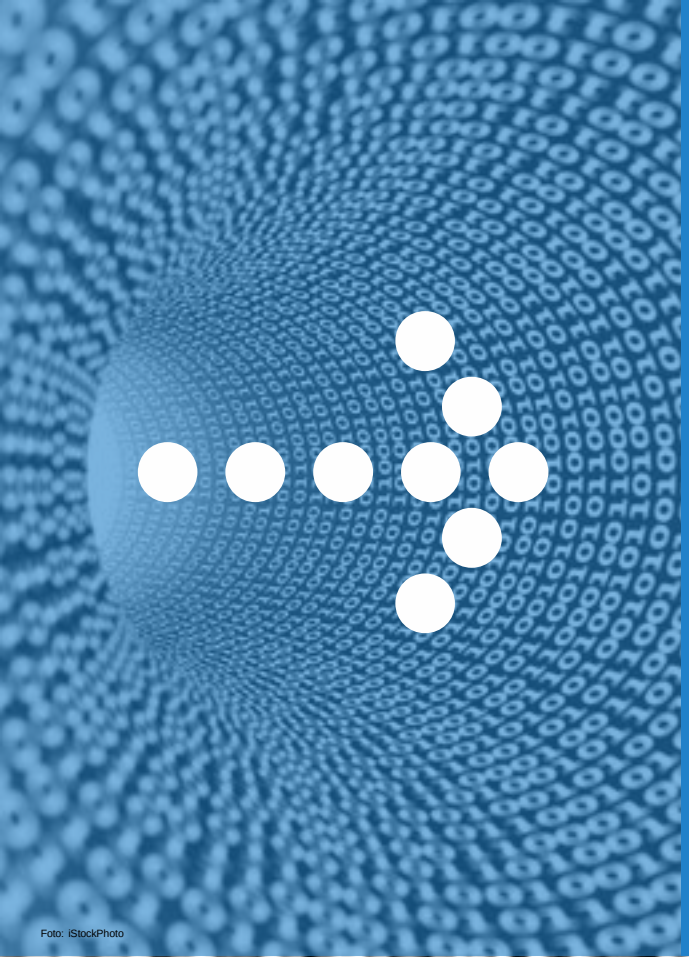


Foto: iStockPhoto

Pass 4 – Förebygg

Praktisk incidenthantering i industriella informations- och styrsystem

Myndigheten för samhällsskydd och beredskap

NCS3

FOI

Det generella informationssäkerhetsarbetet

Utgångsläge, ni har koll på:

- Vad är skyddsvärt?
- Vilka är hoten?
- Vilka skyddsåtgärder har vi?

- Och har ett kontinuerligt säkerhetsarbete!

Känn dig själv - verksamhet

- Vad är viktigt för verksamheten?
  - Vilken information behövs?
  - Vilka funktioner behövs?
  - Vilka system hanterar dessa?
  - Vilka stödsystem behövs?
- Vad kan ett avbrott för dessa leda till?
  - Vilka konsekvenser får det?
  - Hur kan man hantera dem?


Källa Pixabay.com

Känn dig själv - system

- Vilka system har vi (faktiskt!)?
  - Vilken funktion har de?
  - Vad vet vi om dem?
    - Onsite, Offsite, Moln
    - Systemberoenden
    - Resiliens
- Skyddsåtgärder, incidenthantering
  - Redundans
  - Säkerhetskopiering
  - Reservlösningar
  - Reservdelar
    - Hård- och mjukvara

Känn dig själv - processer

- Vem är ansvarig och har mandat?
  - Drift av system
  - Säkerhetsskydd
  - Informationssäkerhetsskydd
  - Verksamheten
  - Krishantering
  - Personal och ekonomi
- Vem har kompetensen
  - Internt, externt?
- Säkerhetsarbete
  - Kontinuitetsplanering

Känn dig själv - externa beroenden

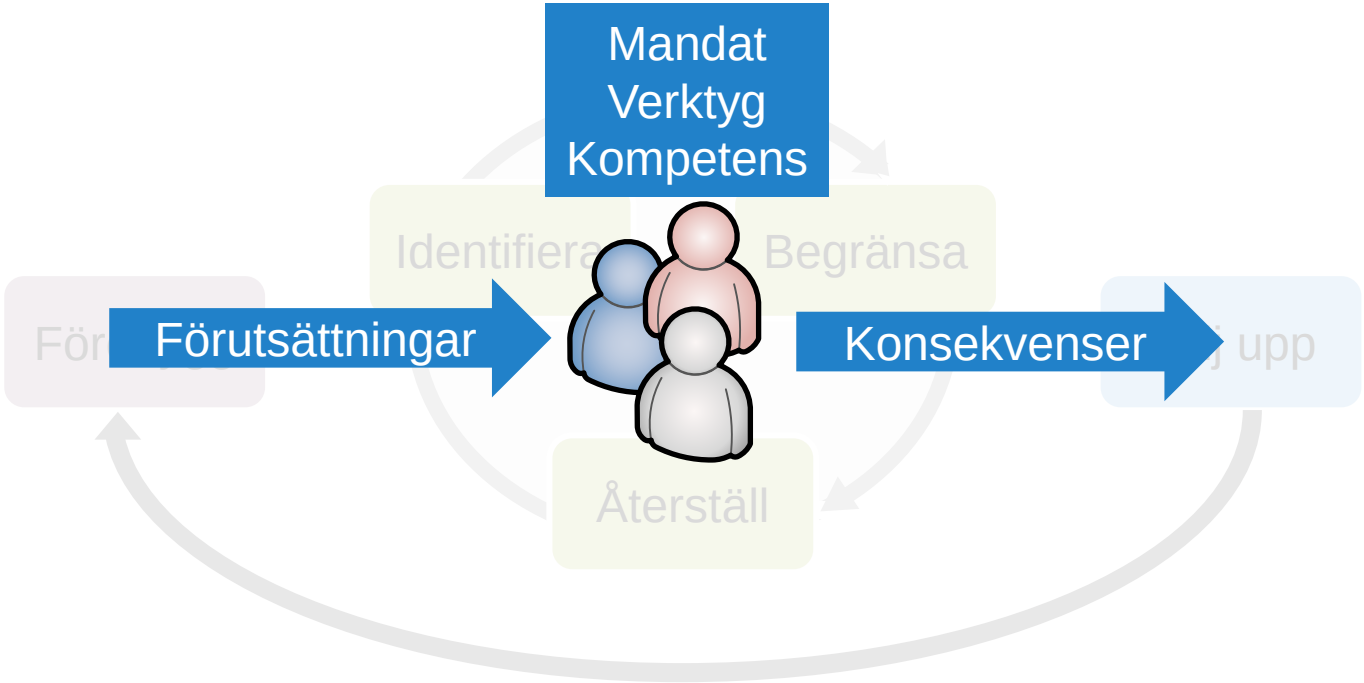
- Bastjänster
  - El
  - Fjärrkyla
  - Kommunikation
- Molntjänster
- Tjänsteleverans
- Konsulter

1-10-60-regeln för intrång

- 1 minut för att upptäcka
- 10 minuter för analys
- 60 minuter för åtgärd

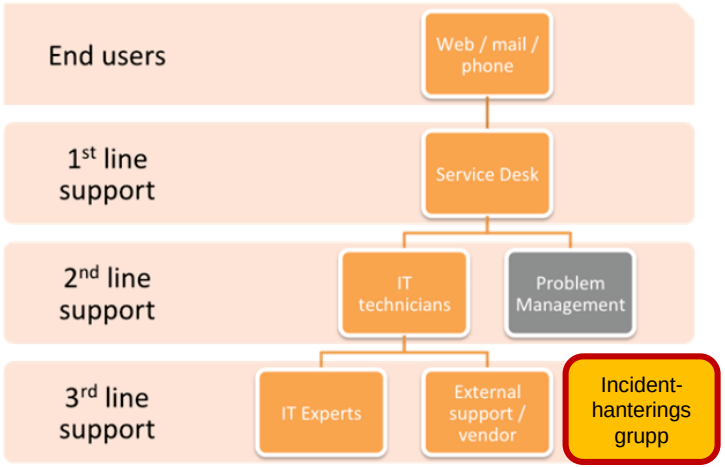
- För väldigt ambitiösa organisationer!

Incidenthanteringsgruppen



Sammansättning av gruppen

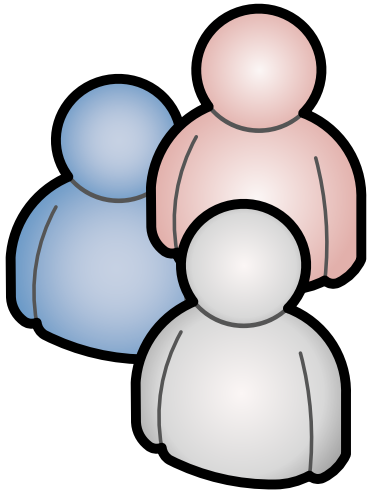
- Fast grupp eller kärngrupp?
- IT/OT-organisationen (Experterna)
  - Drift (ITIL)
- Koppling till verksamhet
  - Ledning (T.ex. CSO, CISO, CIO)
  - Säkerhetsorganisation
    - Krisgrupp
  - Verksamhetsrepresentanter
  - Kommunikation
  - HR
  - Jurister



Roller i ITIL:s Incident Management process

Roller i gruppen

- Insatsledare
  - Leder hanteringen
  - Bevakar och prioriterar
  - Kommunicerar
- Incidenthanterare (Tekniker)
  - Felsöker och avhjälper
  - Dokumenterar och återkopplar
- Springfolk



Förebygg – När och Vad

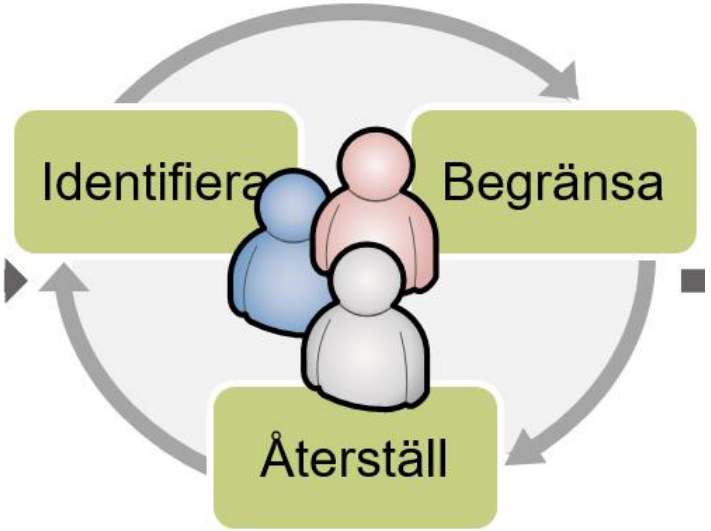
- **När** ska gruppen sammankallas?
  - Semi-incidentläge!
  - Beredskap att faktiskt agera!
  - Gäller det hela organisationen?
  - När ska normalläge återtas?
- **Mandat** att agera
  - Snabbare beslut behövs!
  - Till exempel att prioritera, stänga av system, extern kommunikation eller att ta in hjälp.

Mandat-matris

Mandat-matris			
Alla användare	- Omstart - 10 kkr	- Stäng av - 50 kkr	- Stäng av - 50 kkr
Grupp/kontor/enhet	- Normal drift	- Omstart - 10 kkr	- Stäng av - 50 kkr
Enskild användare	- Normal drift	- Normal drift	- Omstart - 10 kkr
	Låg Enskilt system	**Medel** Flera system	**Hög** Alla system

Förebygg - Incidenthanteringsplan

- Hur ska ni jobba under incidenten?
- Scenarier
  - Vad kan hända?
  - Hur kan ni hantera dem?
- Vilka resurser kan ni nyttja
  - Hur gör ni det?
- Kontinuitetsplaner
  - SLA?



Förebygg - Kommunikationsplan

- Internt
  - Beslutsfattare
  - Verksamhetsföreträdare
  - Experter
  - Personal
- Extern
  - Media
  - Kunder och leverantörer
  - Myndigheter

Förebygg – Verktyg för incidenthantering

- Verktyg och utrustning
  - Lokal
  - Whiteboards och infodelning
  - Datorer, USB-minnen
  - Plattform för samverkan
  - Oberoende!
- Dokumentation
  - Systemdokumentation
  - Av incidenten

Förebygg – Öva

- Pröva utformade planer, rutiner och teknik
  - Kontinuitetsplaner
  - Incidenthanteringsplan
  - Redundanta lösningar
- Öva in hanteringen
- Bidrar till kompetens i gruppen
- Höja beredskapen att nyttja gruppen
- Öka medvetenheten inom organisationen

Förebygg - Sammanfattning

- Skapa en incidenthanteringsgrupp
- Identifiera och upprätta planer
- Identifiera och skaffa verktyg
- Förbättra skyddsåtgärder
- Öva!