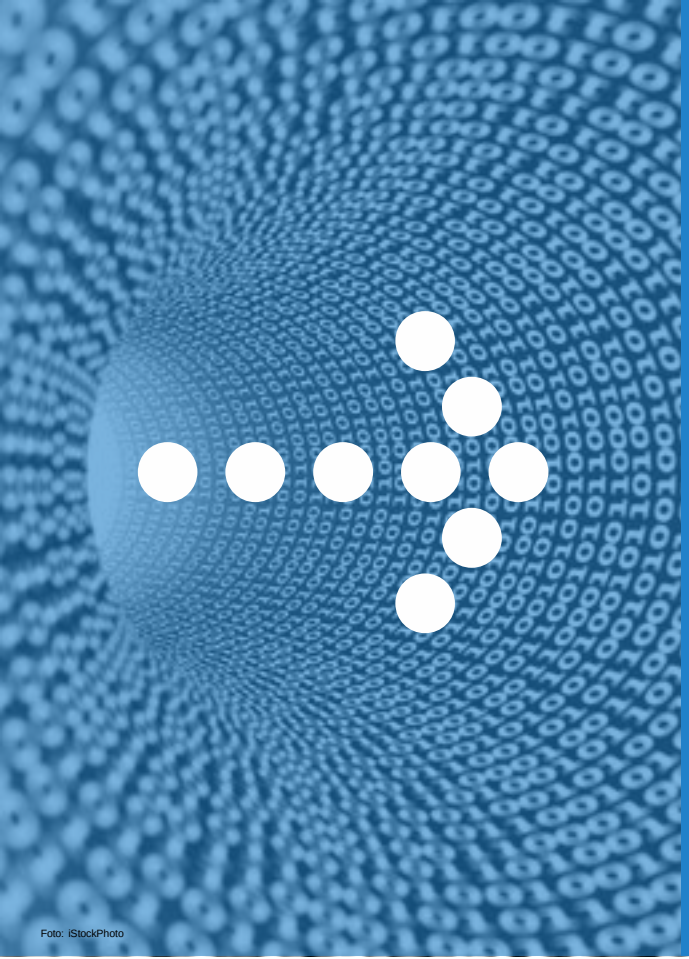


Foto: iStockPhoto

Pass 7
Hantera – Begränsa

Praktisk incidenthantering i industriella informations- och styrsystem

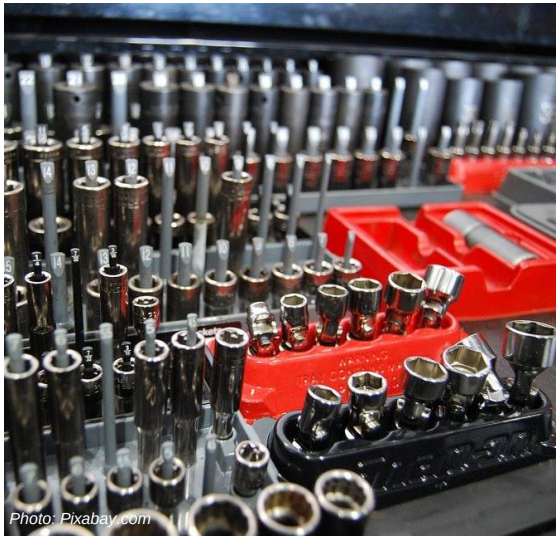
Myndigheten för samhällsskydd och beredskap

NCS3

FOI

Plan för hantering - Repetition

- Behövs mer information?
  - Även uppdaterad info under incidenten
- Akuta åtgärder
  - Begränsa spridning
  - Prioriterade åtgärder
- Åtgärder för att återställa



Fråga:

Ska man stänga av en infekterad klient?

Översikt – Begränsning

- Målsättning
  - Att begränsa påverkan från incidenten så mycket som möjligt
  - Att störa verksamheten så lite som möjligt med våra åtgärder
- Övergripande metoder
  - Stäng av vägar
  - Ta bort mål
  - Fortsatt spaning
- Dokumentera de åtgärder ni gör
  - Och skulle vilja ha gjort
  - Behov av bevis samt för efteranalys

Övergripande mål för hanteringen

- Polisanmäla?
- Avbryta angreppet?
- Återställa systemet?
- Kan systemet lämnas intakt om vi tar upp ett nytt system parallellt?
- Säkerställa långsiktig tillgänglighet genom att offra kortsiktig tillgänglighet?

Val av lösning för hantering

- Möts krav på tillgänglighet
  - Kritisk nivå för systemet
- Effektivitet för lösningen
- Omfattning (tid och resurser)
- Varaktighet
  - Möjlighet att återgå till normal drift
- Risker med lösningen

Metoder – Stäng av vägar

- Segmentering
  - Begränsa eller blockera
  - Dra ur nätverket
- Rättighetsbegränsning
  - Administrativ åtkomst
- Byt inloggningsuppgifter
- Stäng av icke viktiga system

Metoder – Ta bort mål

- Begränsa funktion
  - Slå av tjänster
  - Begränsa vem som har åtkomst
- Stäng av eller isolera
  - Autonom drift
  - Endast åtkomst från viss plats

Metoder – Fortsatt spaning

- Vilka system är påverkade
- Vilka system är INTE påverkade
- Hur påverkar våra åtgärder
- Förändringar i påverkan

- **Pågår incidenten fortfarande?**

Tips under hanteringen

- Ledaren måste leda
- Revidera analys baserad på ny info
- Omprioritering av resurser
- Dokumentera och kommunicera
  - Vad ni tror
  - Vad ni gör (förändringar)
  - Vad ni upptäcker

Återställning av system

- Görs när incidenten är över
  – Om det ej är kritiska system
- Säkerhetskopiering krävs
- Systemdokumentation krävs
- Prioritera viktiga system
  – Tyvärr ej självklart
- Återställ en ren kopia

Sammanfattning

- Målsättning
  - Att begränsa påverkan
  - Stör så lite som möjligt
- Övergripande metoder
  - Stäng av vägar
  - Ta bort mål
  - Fortsatt spaning
- Glöm inte att dokumentera vad ni gör!