

# Ändringar som både hotar och skyddar

Rapport om säkrare ändringar i informationssystem

Satu Björn  
*Analytiker*

Avdelningen för cybersäkerhet och säkra kommunikationer  
Enheten för strategi och samordning



# Tematiska rapporter inom informations- och cybersäkerhet

- 2021: Hoten mot de digitala leveranskedjorna
- 2022: **Ändringar som både hotar och skyddar**
  - Utmaningar
  - Konsekvenser för samhällssäkerheten
  - Rekommendationer



# Återkommande orsak till incidenter



- Misstag (ofta i samband med ändringar)
- Systemfel (ofta efter att ändringar har uteblivit)



# Säkerhetsutmaningar

- Felkällor i komponenter och flöden
- Kunskap och kompetens
- Organisatoriska utmaningar
- Processuella utmaningar



**Säkerhetsutmaningar  
vid hantering av  
ändringar**

# Utmaningar

- Faktorer som avskräcker från att genomföra ändringar
- Utmaningar som växer när ändringar inte genomförs



Säkerhets-  
utmaningar vid  
uteblivna ändringar



# Konsekvenser

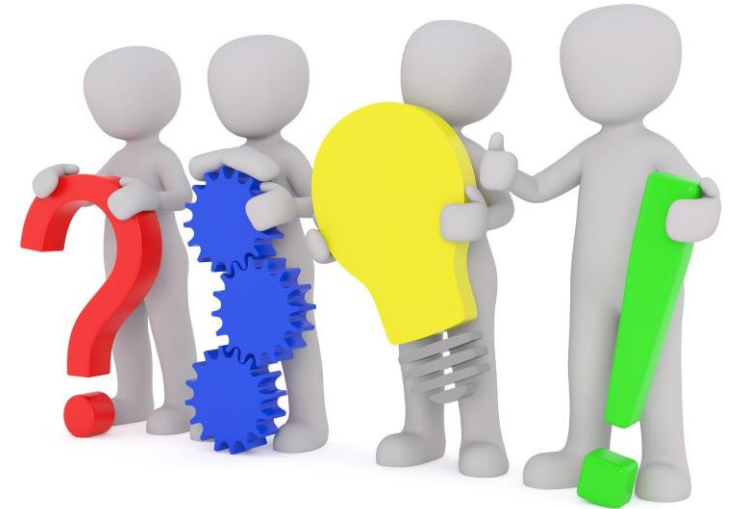
- När sådant som inte ska levereras ändå levereras
- När sådant som ska levereras inte levereras
- Sårbarhet av monoberoenden



**Konsekvenser  
för samhälls-  
säkerheten**

# Rekommendationer för säkrare ändringar

- Generella rekommendationer:
  - Följ "best practice"
  - Ta stöd av MSB:s vägledningar
    - Vägledning för säkerhetsåtgärder i informationssystem
    - Vägledning om grundläggande säkerhet i cyberfysiska system
    - Vägledning om fysisk informationssäkerhet i it-utrymmen



## fort. Rekommendationer för säkrare ändringar

- Ändringshantering är en del av organisationens systematiska säkerhetsarbete:
  - Dokumenterad
  - Tydliga roller
  - Instruktioner
  - Ändringskalender
  - Rätt kompetens och nödvändiga resurser
- Ha en kontinuitetsplan om något skulle gå fel
- Inför arbetssätt för ändringar under en pågående incident
- Säkerställ att arbetssättet efterföljs





# fort. Rekommendationer för säkrare ändringar

- Dokumentera
  - hur it-miljön är uppbyggd
  - hur dess respektive informationssystem hänger ihop
  - är beroende av varandra
  - skydda även utvecklings- och testmiljöer
- Inför och följ dokumenterade arbetssätt för att
  - Granska och testa nya komponenter
  - Granska och testa komponenter som ska tas bort
- Bedriv en aktiv omvärldsbevakning
- Skydda föråldrade system som organisationen är ovillig att byta ut





# Frågor eller funderingar

[strategiskanalys@msb.se](mailto:strategiskanalys@msb.se)

