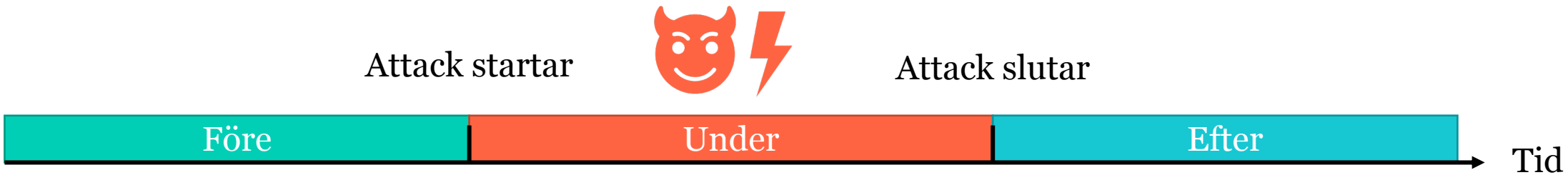
Skyddsåtgärder

Del av kursen ETE352 Cybersäkerhet – grunder och medvetenhet som ges vid Linköpings universitet

Mikael Asplund

LINKÖPINGS UNIVERSITET

Skyddsåtgärder



Förebygg (prevent)
Förbered återställning
Gör riskanalys
Kompetensutveckla
Förbered strategier

Undvik (avoid)
Tolerera
Upptäck (detect)
Svara (respond)
Dokumentera
Rapportera

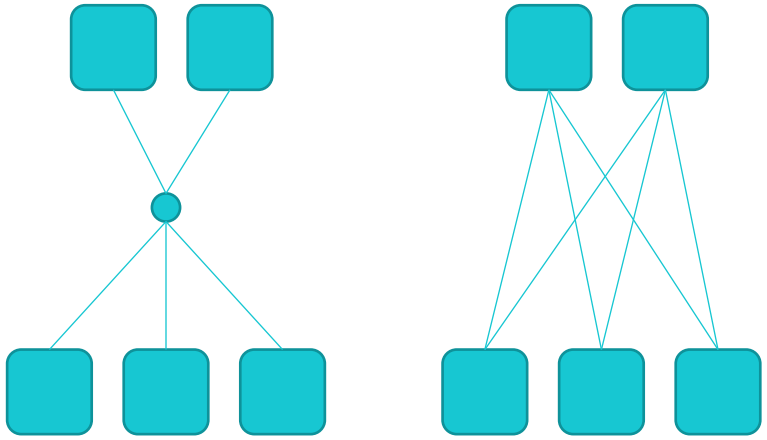
Återställ (recover)
Analysera
Rapportera/anmäl
Dra lärdom

Förebyggande designprinciper

- Försvar på djupet
- Principen om lägsta behörighet
- Undvik komplexitet
- Isolera och separera
- Designa för förändring

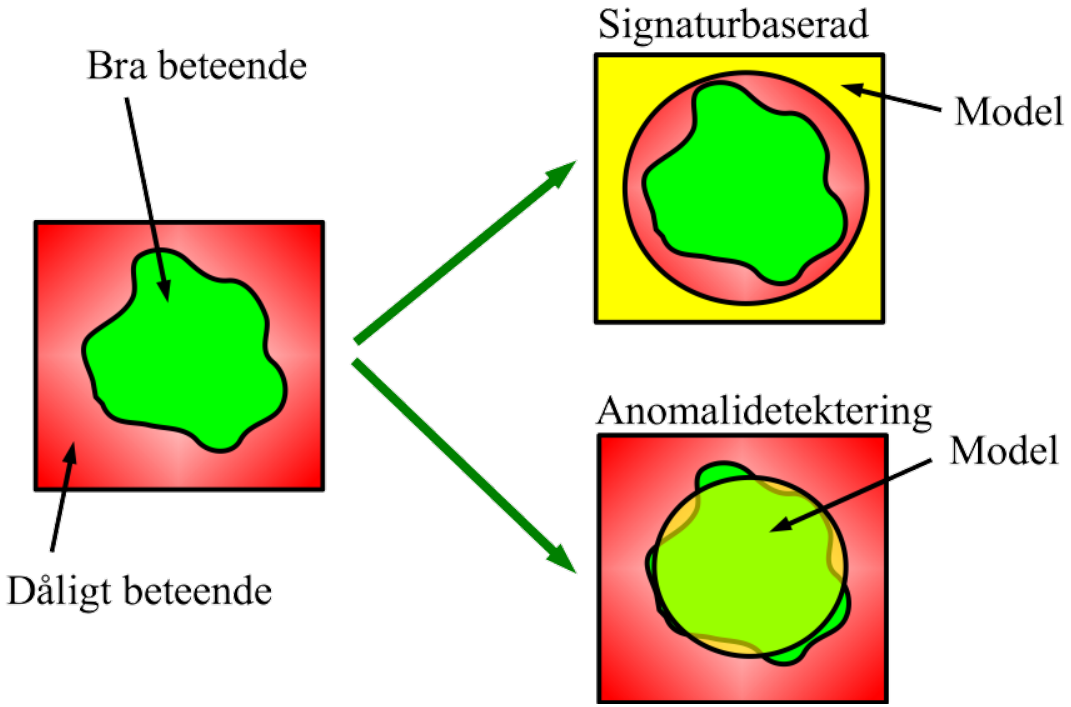
Feltolerans

- Fortsätta tillhandahålla tjänst trots fel/attacker
- Kräver redundans
  - Ingen single-point of failure
  - Alternativa sätt
  - Kan skapa ny komplexitet
- Begränsad tjänst bättre än ingen tjänst



Intrångsdetektering

- **Signaturbaserad**
  - Databas med kända attacker
  - Exempel: anti-virusprogram
  - Sällan falsklarm 👍
  - Missar nya hot 👎
- **Anomalidetektering**
  - Maskininlärning för säkerhet
  - Tränar in vad som är normalt – varnar för det som avviker
  - Fungerar för nya hot 👍
  - Resulterar oftare i falsklarm 👎



Begränsning av attacker

- Exempel på åtgärder
  - Blockera nätverkstrafik
  - Stäng av datorer
  - Byt lösenord
  - Inaktivera delsystem
- Kan försvåra forensisk analys
- Bör vara planerat i förväg

Återställning

- Plan för att bygga upp systemet från 0-läge
- Behöver testas regelbundet
  - Backup värdelöst utan fungerande återställning
- Risk för bakslag
  - Redundans även i backup/recovery

Incidentanalys och rapportering

- Brott ska polisanmälas
- I vissa fall ska incidenter rapporteras
  - Under attacken (notifiering)
  - Efter attacken
  - CERT-SE (www.cert.se)
- Oavsett – viktigt att lära sig varför det hände

https://cybersakerhet-grund.ida.liu.se

LINKÖPINGS UNIVERSITET