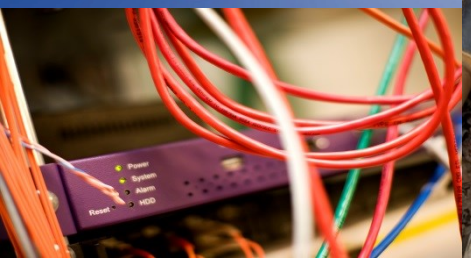
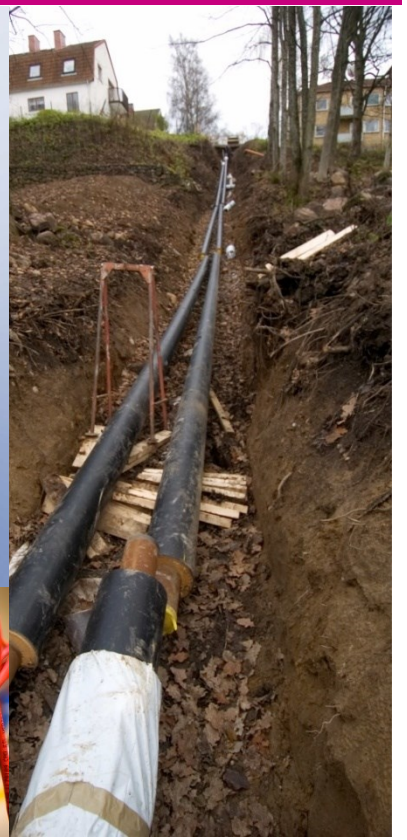




Informationssäkerhet och IT-säkerhet

Resultat från intervjustudie samt från workshops i fjärrvärmeföretag

Energimyndigheten

Hur ser det ut i fjärrvärmebranschen?

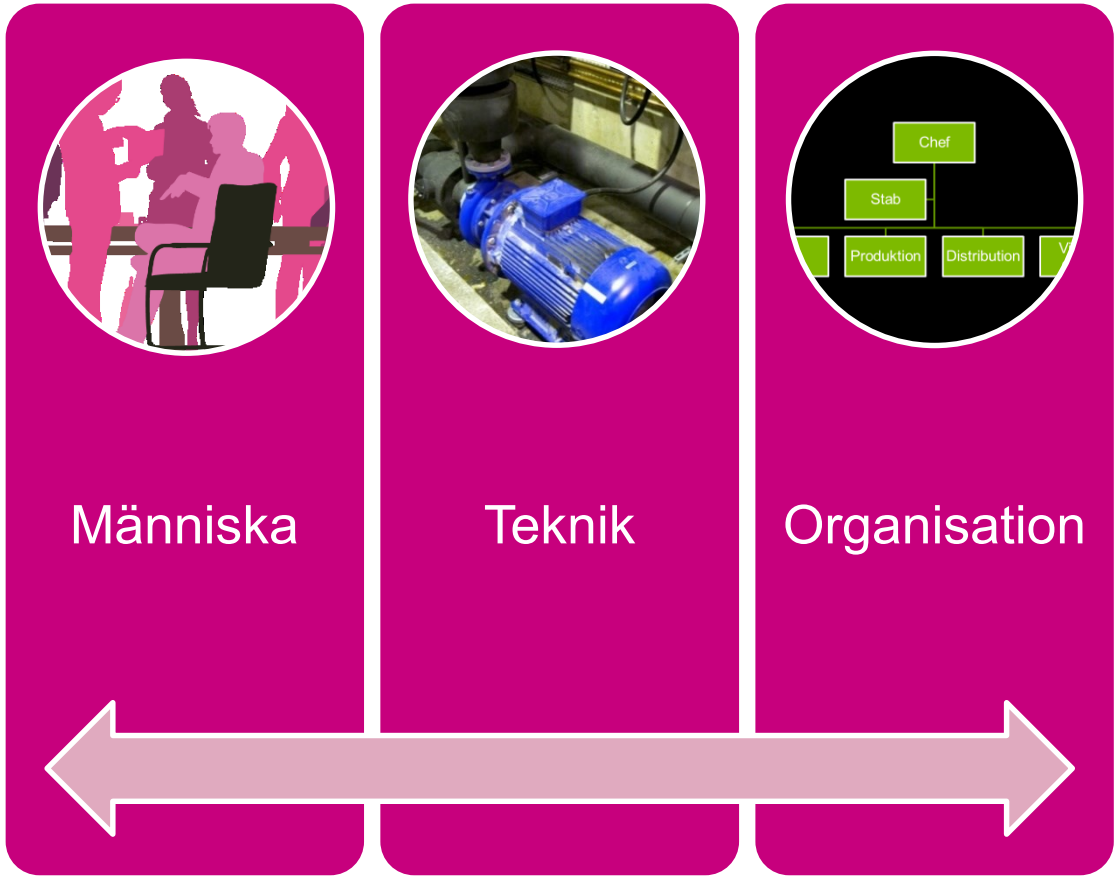
- Ökat medvetande om problematiken kring IT-säkerhet
- ”*Jo, fast det har ju fungerat bra hittills*..”
- Sårbarheter i hjärtat av verksamheterna

Om studierna

- Intervjustudie informationssäkerhet
  - 11 små och medelstora företag
  - Samma grundfrågor, men öppen fördjupning

- RSA i workshopform
  - Fyra företag, varav ett stort
  - Genomfört på plats i företaget
  - 3-8 deltagare per företag
  - Konkret återkoppling endast direkt till respektive företag

Intervjustudien frågeområden



- Ledningssystem, policy, etc.
- Ansvar, kompetens
- Risk- och sårbarhetsanalys
- Informations-/systemklassning
- Incidenthantering, kontinuitet, planer, etc.
- IT-säkerhet och dokumentation

Ledningssystem och policy - systematik saknas

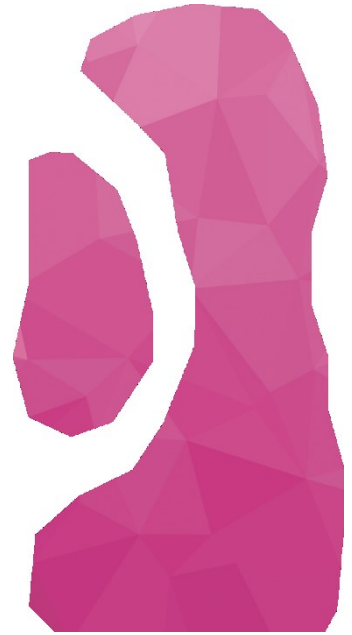
- 1/3 av företagen har policy för informationssäkerhet
- Förlitar sig på krav från administrativ IT
- Exempel på regler finns
- Policy viktig för kontinuitet i leverans, förtroende mm
- Kommunägda [redacted] Kommunens policy

Ansvar och kompetens

- Ibland utsedda ansvariga för informationssäkerhet
- Ofta otydliga ansvar
- Utbildning görs sällan
- Ofta saknas användarföreskrifter

Risk- och sårbarhetsanalys infosäk

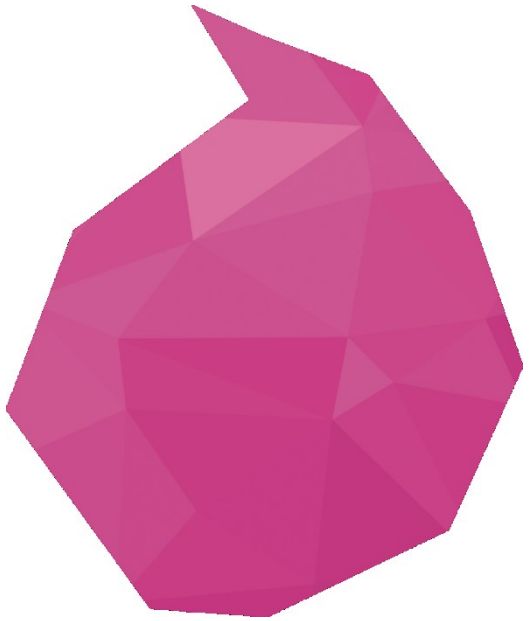
- Generellt noga med riskanalyser ur:
  - Säkerhetsperspektiv (arbetsmiljö, lagkrav)
  - Driftsäkerhet
  - Ledningen informeras om resultaten
- Ofta beroende av nyckelpersoner
- IT inkluderas inte alltid
- Styr- och kontrollsystemen inkluderas sällan



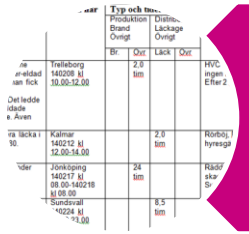
Informationsklassning

- Vilka system är mest skyddsvärda?
- Vilken information är mest skyddsvärd?
- Vilka behöver engageras för att klassificera dessa?

- Några gör systemklassning
- Ingen har genomfört informationsklassning



Viktigaste (kritiska) informationstillgångar



Mät- och styrvärden

Scada (info- och styrsystem)

Nyckelpersoner

Elektronisk kommunikation

Energimyndigheten

Incidenthantering, kontinuitet

- Incidenter händer, även i IT-system
- Dokumentation! Korrekt, uppdaterad och tillgänglig
- Organisation med utsedd grupp

- Engagerad och kunnig personal finns
- Men sambanden är komplexa, och förändras över tid
- Ev kontinuitetsplaner inkluderar inte IT-systemens beroenden

IT-säkerhet (särskilt för Scada)

- Skydd av värdefulla tillgångar
  - Information, hårdvara, mjukvara
- Skydd av Scada från kommunikation med Internet (direkt och indirekt)
  - ”Djupledsförsvar” av lökmodell
  - Åtkomstkontroll Internet – styrsystem
  - Dessutom vanlig IT-säk (password, antivirus, trafikövervakning etc.)

Djupledsförsvar
Säkerheten kan inte vara beroende av en enda funktion.

Mer IT-säkerhet

Djupledsförsvar
Säkerheten kan inte vara beroende av en enda funktion.

Bättre grundskydd
Gör systemen svårare att angripa.
IT-arkitektur,

Spårbarhet och övervakning

Logghantering och incidenthantering

Utbildning, övning
Grundförståelse på alla nivåer
Beredskap för process-IT

Energimyndigheten

Några utmaningar

- Antagonistiska angrepp
  - Få har drabbats nära styrsystemen
  - Relativt lätt att angripa och störa
- Nyckelpersoner *(”Den som tar över behöver följa mig 3-5 år”)*
- Dokumentation
- Ställ krav i avtal med underleverantörer IT
- Mer?