Molntjänster och utkontraktering av kritisk verksamhet – lagar och regler

Alireza Hafezi

Säkerhetsskydd?!

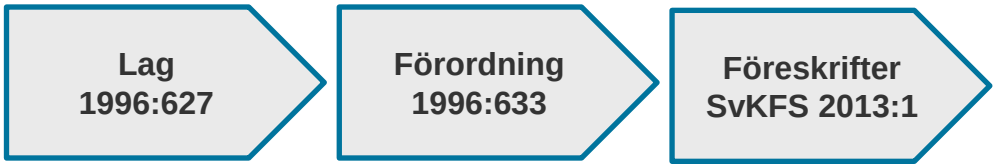
Säkerhetsskyddslagen, 6 §: Med säkerhetsskydd avses:

> skydd mot spionerи, sabotage och andra brott som kan hota rikets säkerhet,

> skydd av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet, och

> skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott (terrorism), ***även om brotten inte hotar rikets säkerhet***. Lag (2009:464) om ändring i säkerhetsskyddslagen.

Svenska Kraftnäts föreskrifter, SvKFS 2013:1



- Säkerhetsskyddsförordningen (1996:633)
- 45 § (1996:633): ”Myndigheterna skall meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) i fråga om säkerhetsskyddet inom sina verksamhetsområden.”
- Affärsverkets svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd (SvKFS 2013:1). Föreskrifterna gäller för enskilda och juridiska personer som bedriver elförsörjningsverksamhet.

Viktiga komponenter i SvKFS 2013:1

- Säkerhetsanalys
- Säkerhetsorganisation
- Informationssäkerhet
- Tillträdesbegränsning
- Säkerhetsprövning och registerkontroll
- Inplacering av befattningar i säkerhetsklasser
- Tillsyn

Säkerhetsanalys, 1 §

Inventering av skyddsvärda resurser kopplat till hot, risk och sårbarheter

En säkerhetsanalys innehåller:

- **Inventering av skyddsvärda resurser**.
- **Identifiering av hot mot de skyddsvärda resurserna**.
- **Analys av risker och sårbarheter**.
- **Upprättande av åtgärdsplan**

Hur påverkas risker och sårbarheter i samband med användning av molntjänst?

Säkerhetsorganisation, 2 §

Att säkerställa resurser för ett systematiskt säkerhetsarbete.

- **Säkerhetsskyddschef och ersättare**
- **Kontroll över säkerhetsskyddet**
- **Incidenter rapporteras till Svenska Kraftnät**

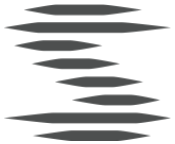
Hur hanteras krav på systematiskt säkerhetsarbete och säkerhetsorganisationen?

Informationssäkerhet

IT-system, §§ 13-21

- **Säkerhetsinstruktioner**
- **Analys av säkerhetsrisker vid anskaffning, utveckling, förändring, utkontraktering och avveckling**
- **Säkerhetsgranskning inför idrifttagning**
- **Tekniska funktioner för**
  - identifiering av användare
  - Styrning av åtkomst
  - Loggning
- **Hantering, rapportering och uppföljning av incidenter**

Har vi kontroll över förändringar som sker i IT-miljön och användning av systemet?



Säkerhetsprövning och registerkontroll, §§ 24-30

Klarlägga om personer som deltar i elverksamhet är lämpliga ur säkerhetssynpunkt

- **Inplacering i säkerhetsklasser, bilaga 1 och 2**
- **Säkerhetsprövning**
  - **Lämplighetsbedömning**
  - **Registerkontroll**

Har vi möjlighet att registerkontrollera personal hos leverantör av molntjänsten?

Tillsynsområden

Att kontrollera om företagets verksamhet uppfyller krav som följer av säkerhetsskyddslagen och andra bindande föreskrifter

> **Säkerhetsanalys**

> **Tillträdesbegränsning;** Fysiskt skydd (huvudkontor, datahall, arkivutrymme, anläggningar)

> **Informationssäkerhet;** Logiskt skydd (IT-säkerhetsarkitektur, kritiska IT-system)

> **Administrativa rutiner;** Inplacering i säkerhetsklasser, säkerhetsprövning, behörighetshantering, incidenthantering och -rapportering

Är detta reglerat i avtal med leverantör av molntjänsten?

Molntjänster och utkontraktering

Drivkraften:

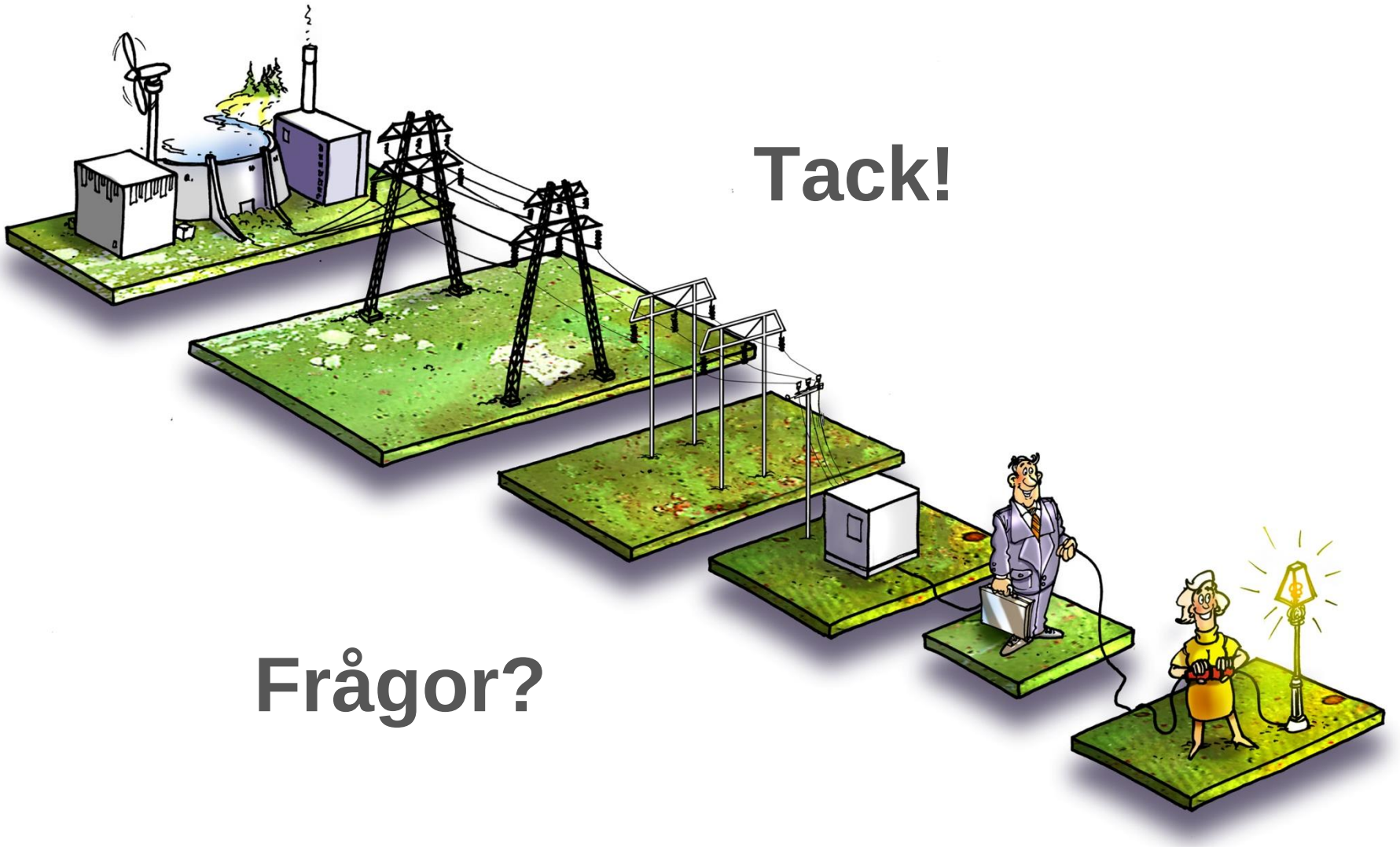
- **Mer fokus på kärnverksamheten och affärsnytta i företaget**
- **Minskade IT-kostnader**
- **Möjlighet till ökad mobilitet**
- **Ökad säkerhet**

Affärsrisker:

- **Operativ kontroll**
- **Otydligt ansvarsförhållande**
- **Immateriella rättigheter**
- **Inlåsningseffekter**

Att tänka på

- **Ta reda på om leverantören är mogen för din marknad.**
- **Tydlig kommunicera lag- och säkerhetskrav som gäller.**
- **Säkerställ vilka jurisdiktioner som gäller för tjänsten beroende på var data lagras och bearbetas.**
- **Säkerställa att det inte råder några oklarheter kring vem som äger de immateriella rättigheter till det som produceras inom ramen för tjänsten.**
- **Noggrant utvärdera potentiella molntjänsteleverantörer avseende riskhantering och säkerhetsmognad.**
- **Säkerställa att säkerhetsprocesser och rutiner hos leverantören är granskningsbara.**
- **Säkerställ att kontraktet visar tydligt vad leverantörens skyldighet är.**



Tack!

Frågor?