ROMAB
ROBERT MALMGREN AB

Säkerhet vid konvergens av nät

Robert Malmgren
rom@romab.com

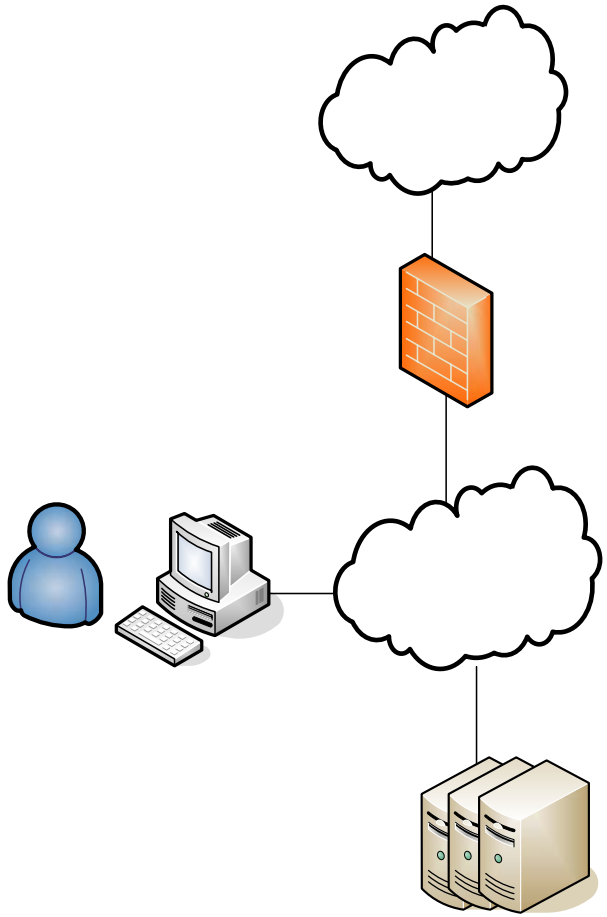
ROMAB
ROBERT MALMGREN AB

Några inledande ord

- *Gamla* sanningar
  - TV skickas via luften
  - Telefoni skickas via teleledningar
  - Datorer använder datornät och kablage
- *Nya* sanningar
  - TV skickas via kabel
  - Telefoni skickas via luften
  - *Allt* använder datorkommunikation – ibland via kablage, ibland via luften

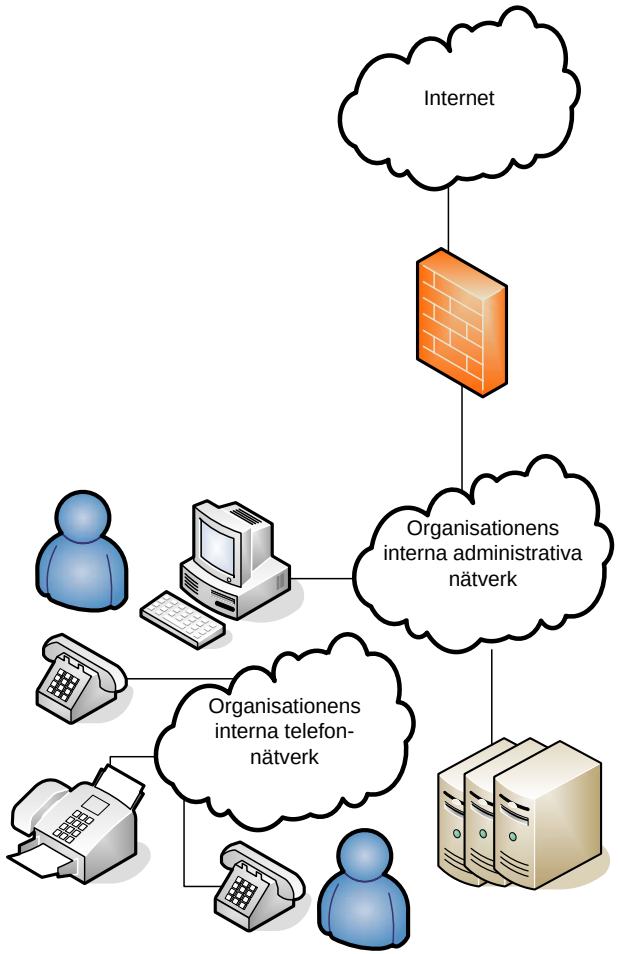
ROMAB
ROBERT MALMGREN AB

Den *enkla* nätskissen



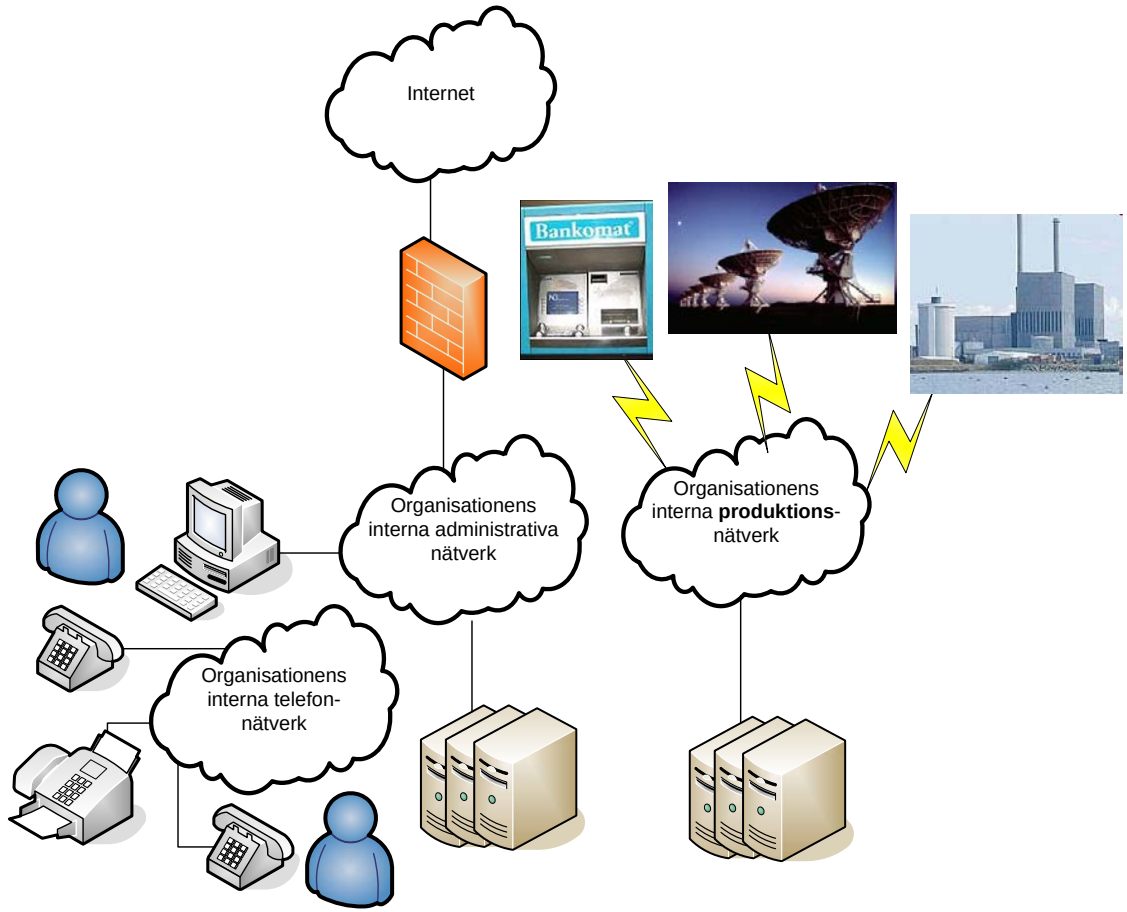
ROMAB
ROBERT MALMGREN AB

Den *något mer kompletta* nätskissen



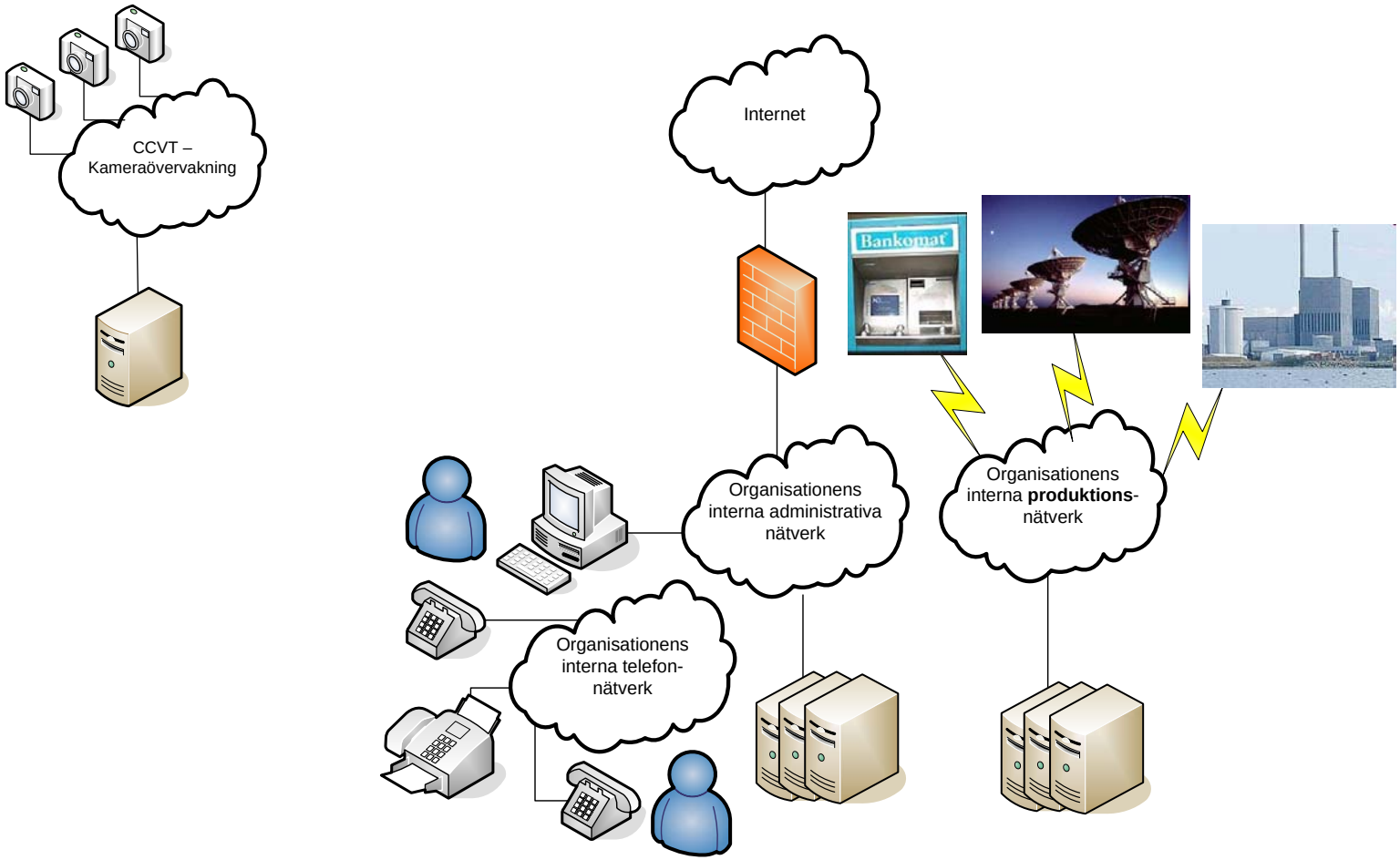
ROMAB
ROBERT MALMGREN AB

Den *än mer kompletta* nätskissen



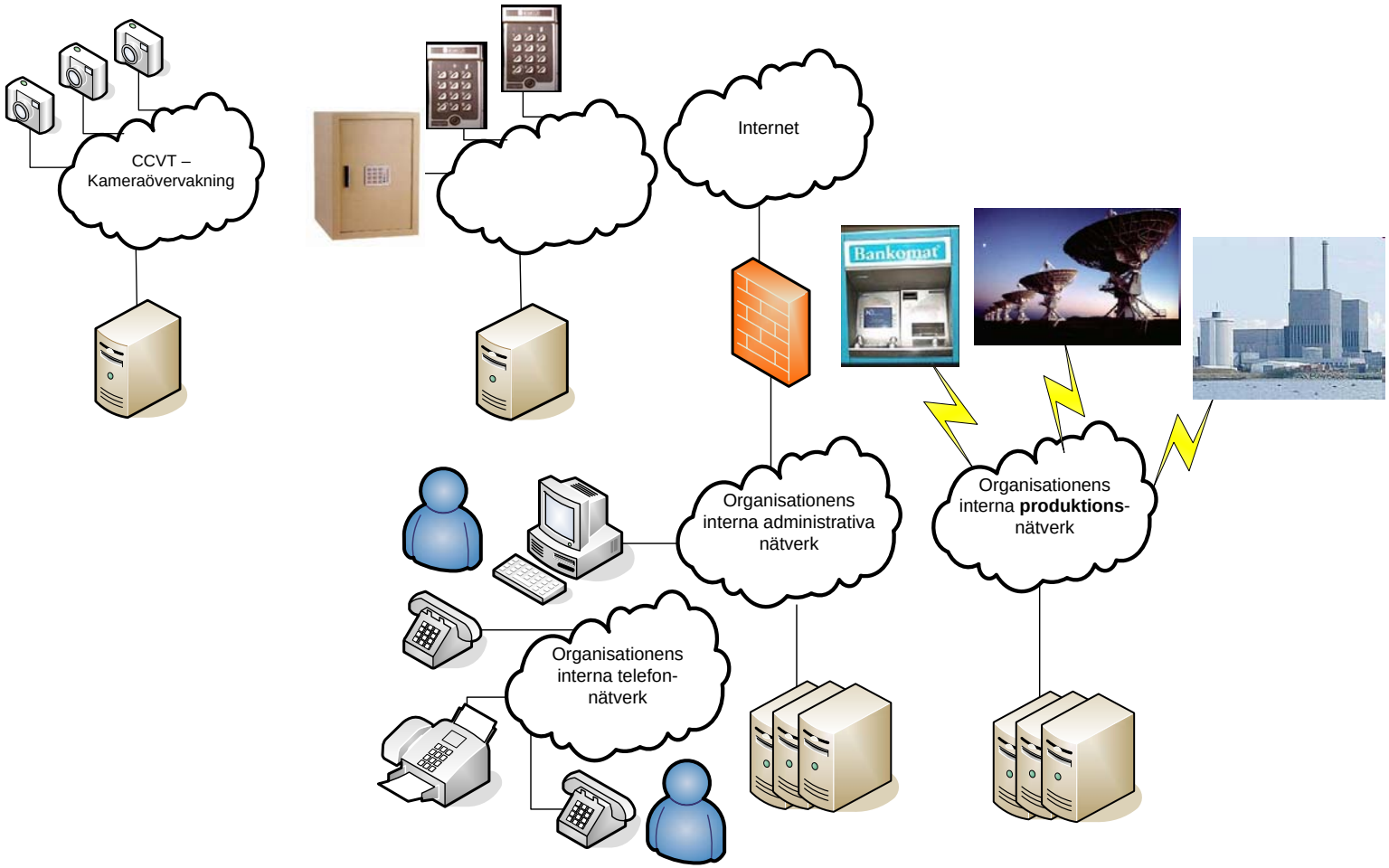
ROMAB
ROBERT MALMGREN AB

Den *<u>än</u> mer kompletta* nätskissen



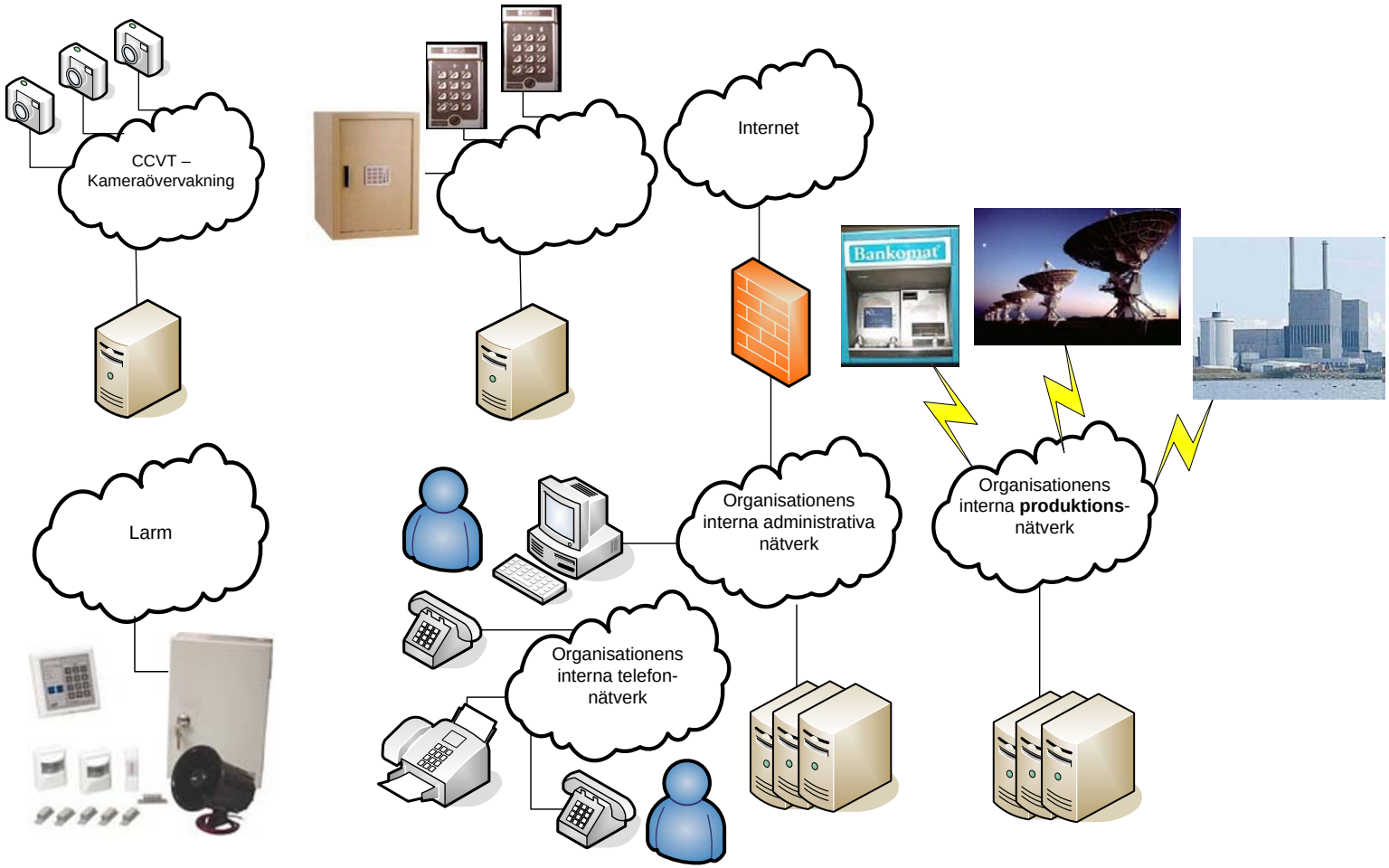
ROMAB
ROBERT MALMGREN AB

Och *<u>än</u> mer kompletta* nätskissen



ROMAB
ROBERT MALMGREN AB

…och *<u>än</u> mer kompletta* nätskissen



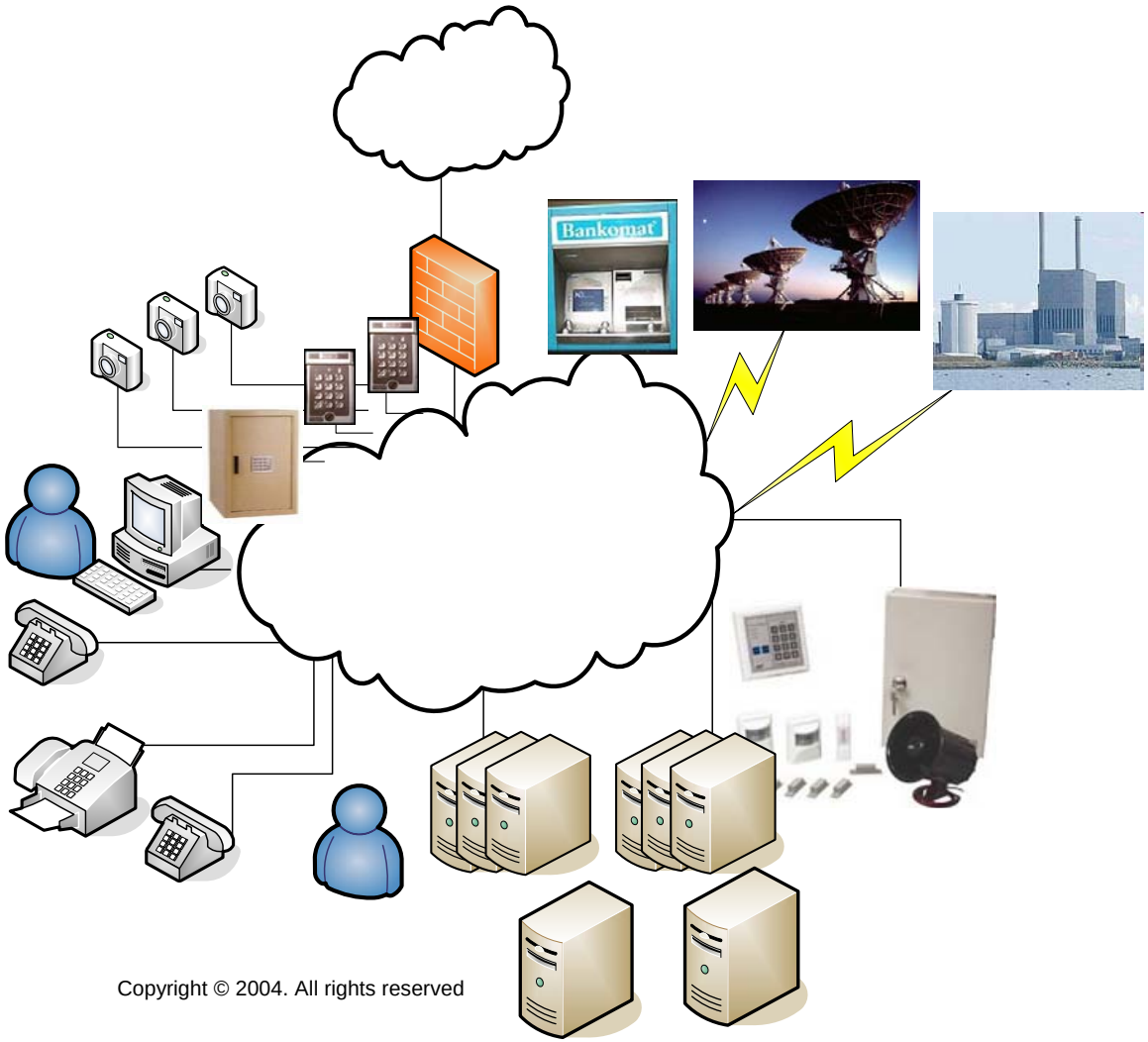
ROMAB
ROBERT MALMGREN AB

”IP over everything”

- Telefoni
  - VoIP, IP-kapabla PABX
- Larm
  - Sabotagelarm via IP istället för ”telia koppar”
- Passagesystem
  - IP-kapabla lås/kortläsare, undercentraler, servrar, etc
- Kameraövervakning
  - Digitala IP-kapabla kameror + hårddiskinspelning
- Produktionsnät
  - Styr och mät via regulatorer och sensorer
  - Fältbuss, proprietära protokoll, etc, inkapslade i IP

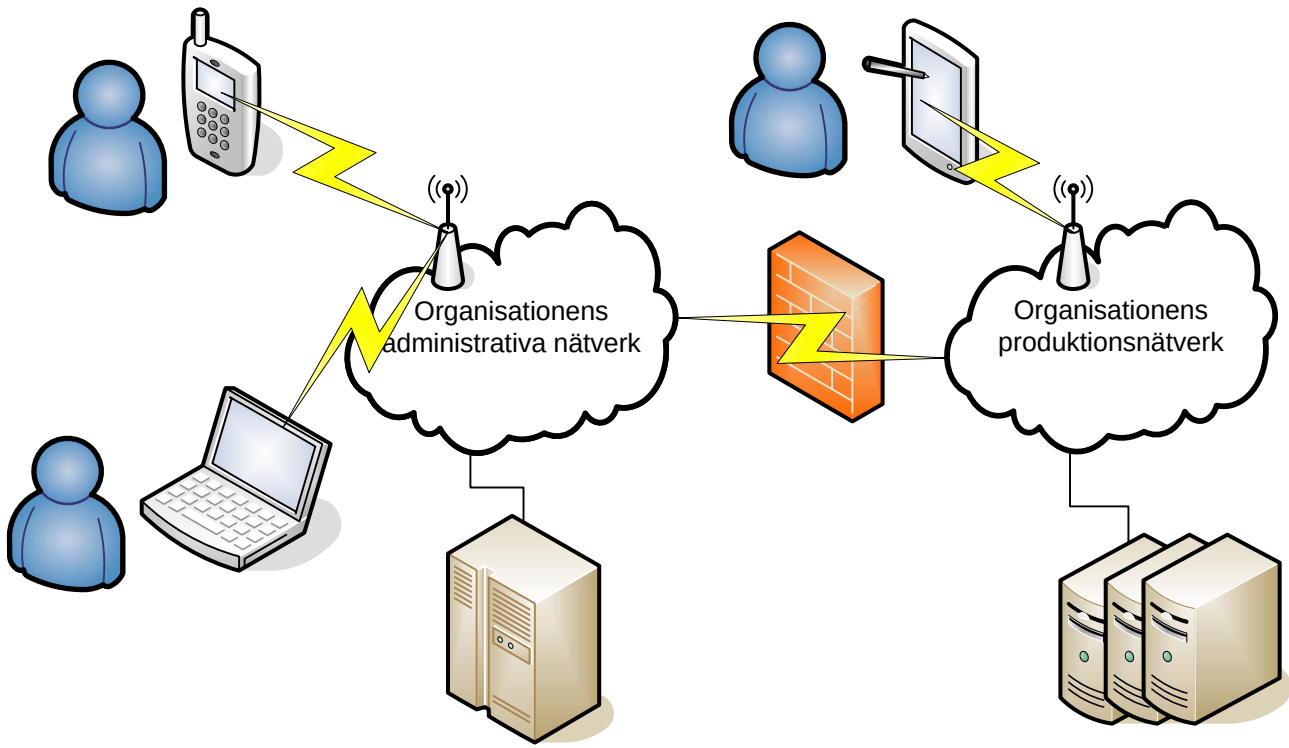
ROMAB
ROBERT MALMGREN AB

En möjlig framtid?



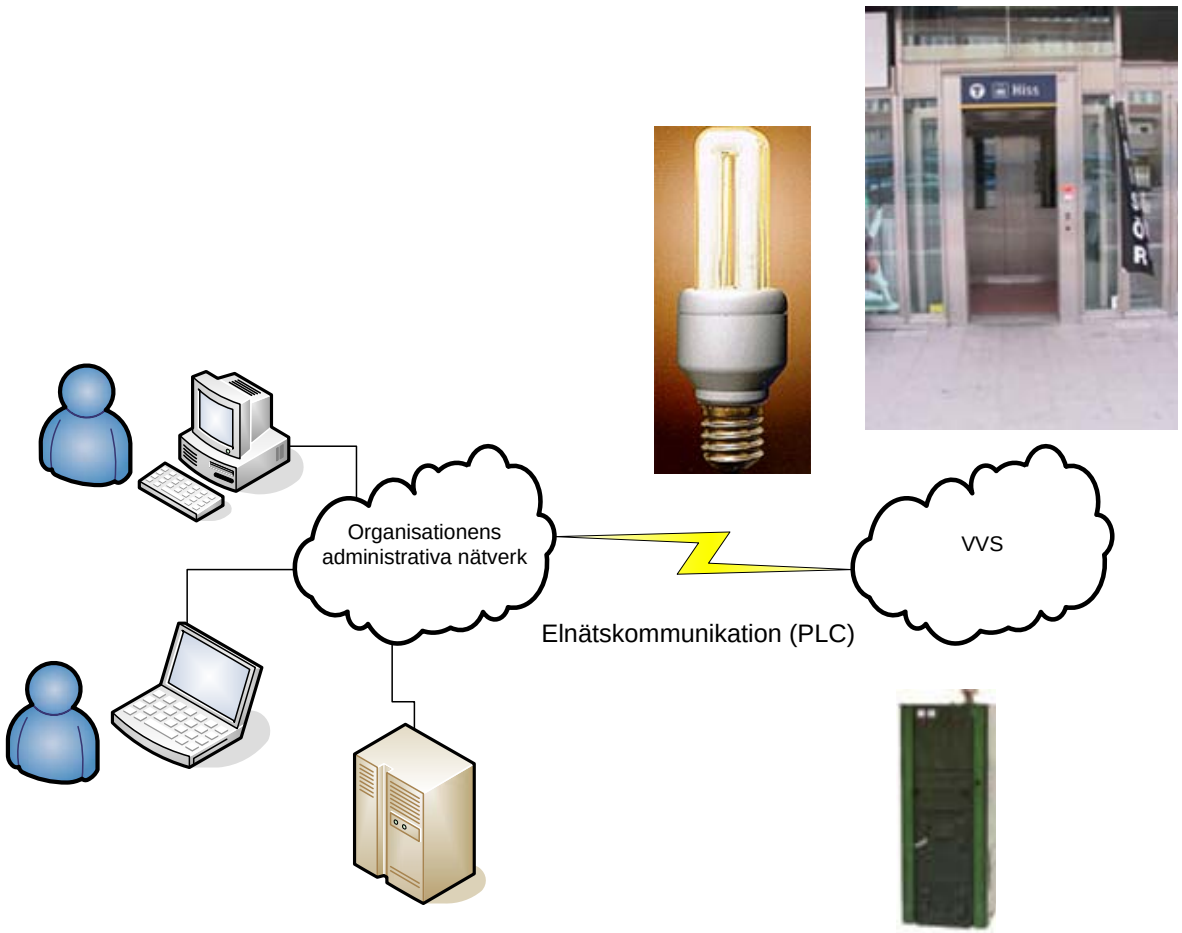
ROMAB
ROBERT MALMGREN AB

Andra framtida scenarios…



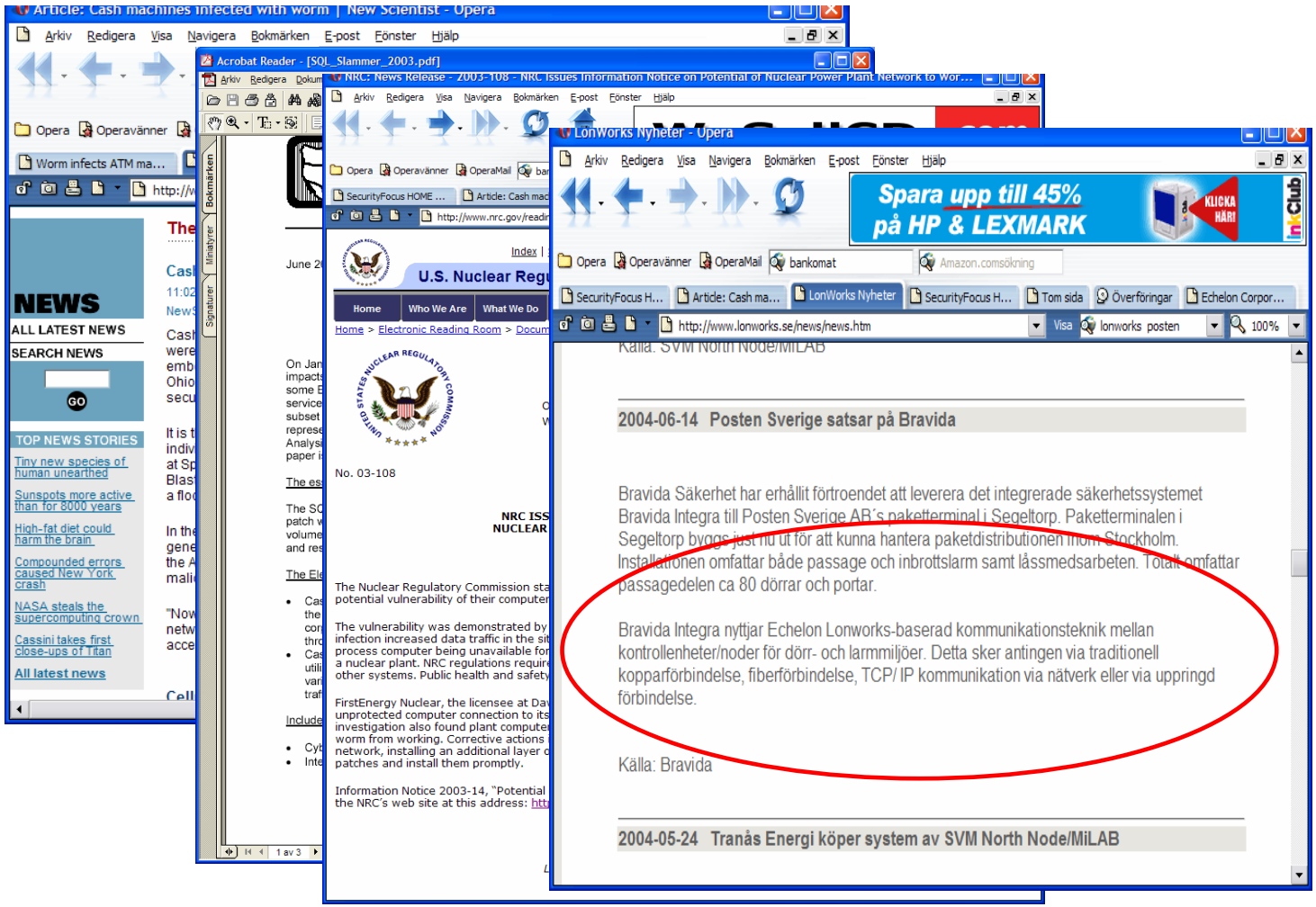
ROMAB
ROBERT MALMGREN AB

Andra framtida scenarios…



ROMAB
ROBERT MALMGREN AB

Verkliga händelser…



ROMAB
ROBERT MALMGREN AB

Viktiga observationer

- Stor chans för kulturkrock
  - Datakom och telekom är av tradition två skilda världar
  - Lås/larm/kameraövervakning/VVS utförs av icke IT- och IP-kunnig servicepersonal
  - **Stort** mått av ”security-by-obscurity” inom de (tidigare) avskärmade och stängda tjänsterna

ROMAB
ROBERT MALMGREN AB

Viktiga frågor vid konvergens

- TTR & MLE - Total time to recover & Maximum loss expectency
  - Hur lätt är det att räkna ut de värsta konsekvenserna och de sannolika scenarierna av att alla eller många kommunikationstjänster drabbas
- Vilken/vilka tjänst(er) styr kraven på tillgänglighet?
- Vet alla inblandade om vad nätet används till?
  - Förstår den lokale systemadministratören konsekvensen av lite ”allmänt nätpul”?
- Är en viss tjänst, tex larm eller passagesystem, designat för att existera i en blandad nätmiljö?
  - eller är den bara ”IP-fierad” och skall helst gå på isolerat nät?
- Vilken utrustning kan agera gateway mellan olika protokoll/nät/transportmekanismer?
  - Multifunktionsmaskiner: PSTN -> LAN?
  - Vad kan uppsåtligen missbrukas?

ROMAB
ROBERT MALMGREN AB

Säkerhetslösningar

- Hur strukturerar man upp det delade interna nätet för att minimera konsekvenser vid incidenter?
  - *Analyssteg* – Hot- och riskanalys. Tex måste samtliga tjänster mixas i ett nät? Vad kan vara IP-fierat men gå bredvid och vad bör man blanda?
  - Förändrat medvetande och attityd hos samtliga inblandade
  - *Design* - Isolerade IP-öar, enklaver eller säkerhetszoner med kontrollerad övergång (brandväggar) och layering (tex VLAN)
  - Bättre interna skydd och detektionsmöjligheter: IPS, IDS, nät- och tjänsteövervakning
- Måste ärvda protokoll ändras?
  - Autentisering, signering, kryptering, etc, adderas
  - Räcker tunnling i TLS/IPSec/SSH?

ROMAB
ROBERT MALMGREN AB

Sammanfattning

- Enligt lagen om att *allt skall rationaliseras* så kommer konvergens ske mellan tidigare disparata tjänster och nätverk
  - Viktigt att förstå behov, hotbild och konsekvenser innan konvergensen påbörjats.
- Hård integrering på applikationsnivå förvärrar det säkerhetsmässiga läget