



Säkerhet vid konvergens av nät

Robert Malmgren
rom@romab.com

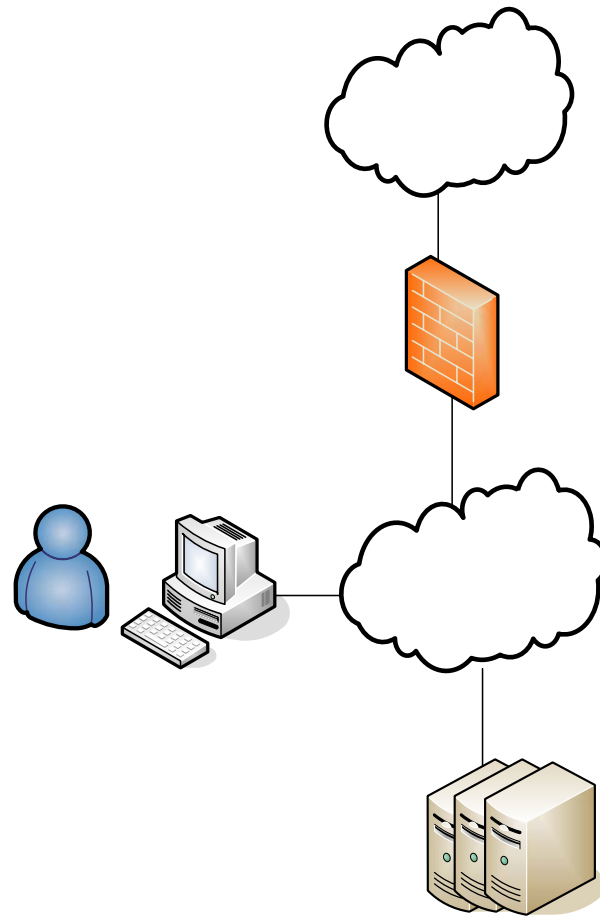


Några inledande ord

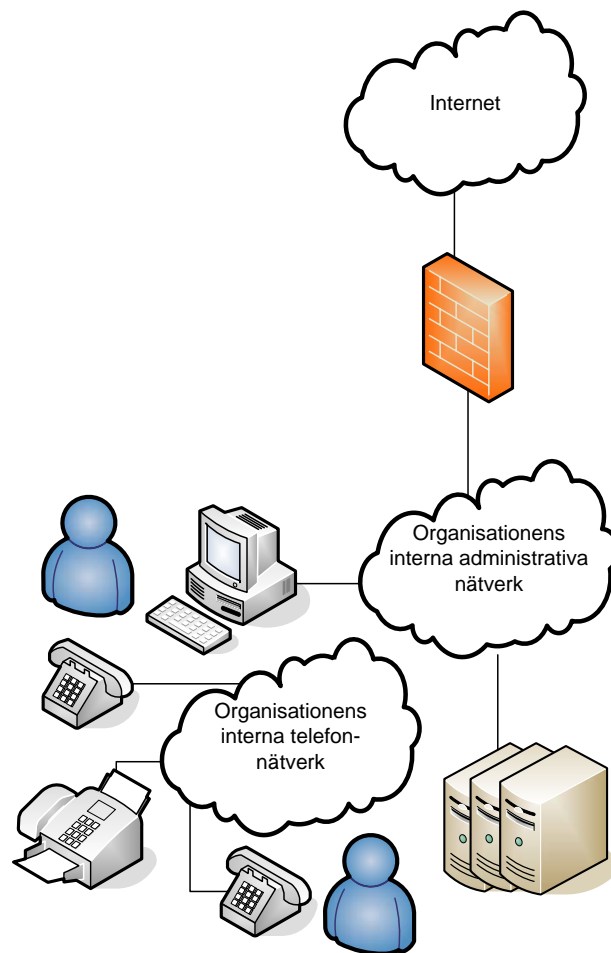
- *Gamla* sanningar
 - TV skickas via luften
 - Telefoni skickas via teleledningar
 - Datorer använder datornät och kablage
- *Nya* sanningar
 - TV skickas via kabel
 - Telefoni skickas via luften
 - *Allt* använder datorkommunikation – ibland via kablage, ibland via luften



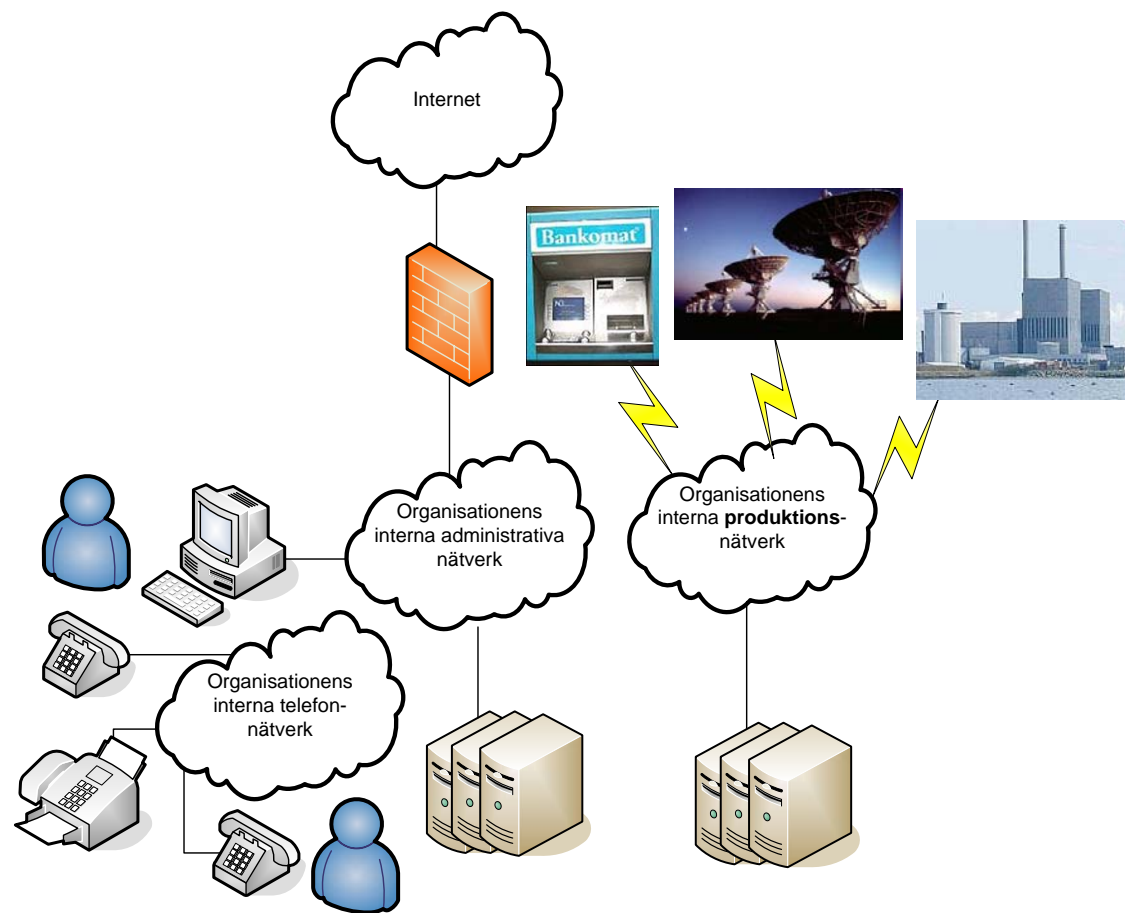
Den enkla nätsskissen



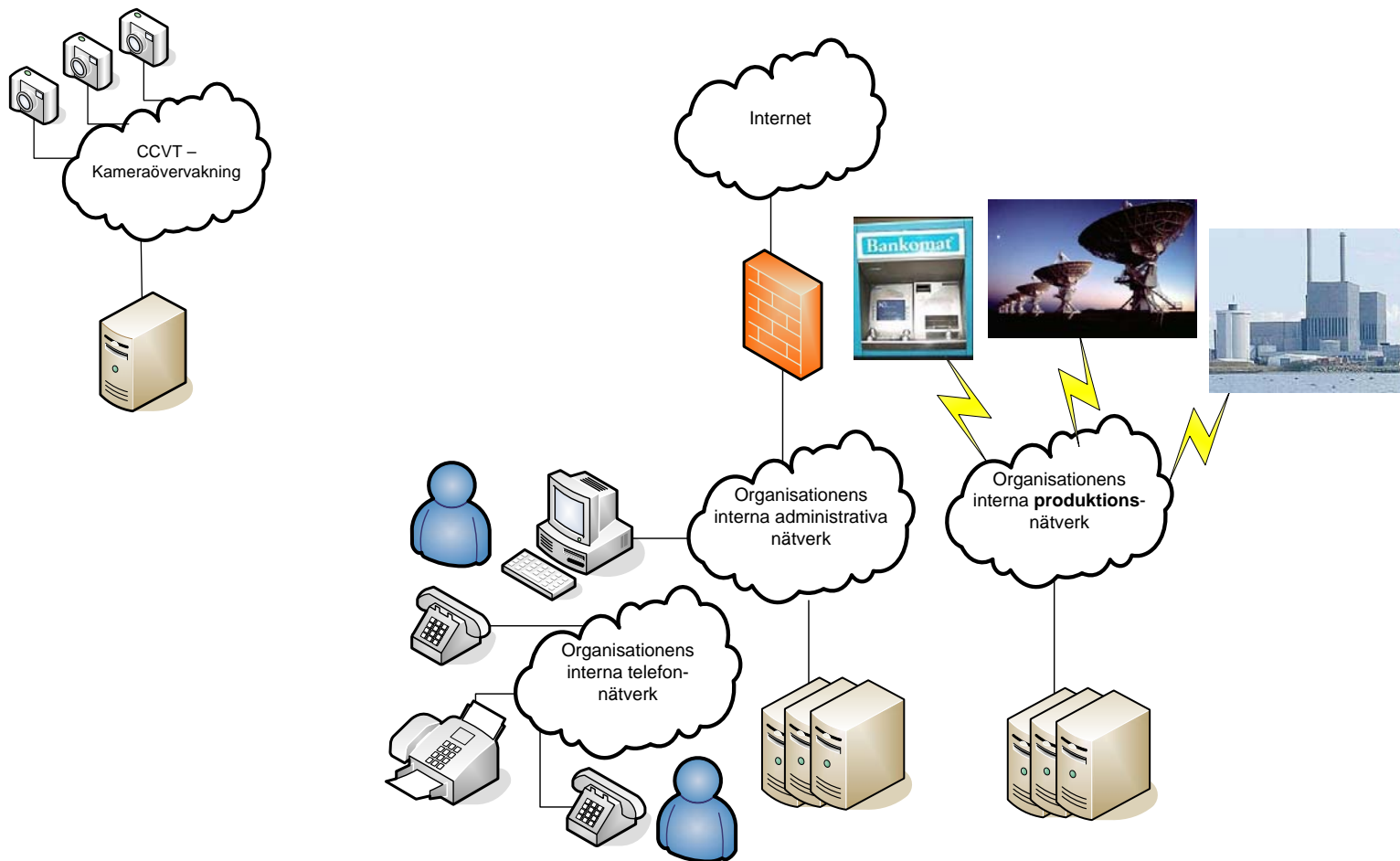
Den *något mer kompletta* nätskissen



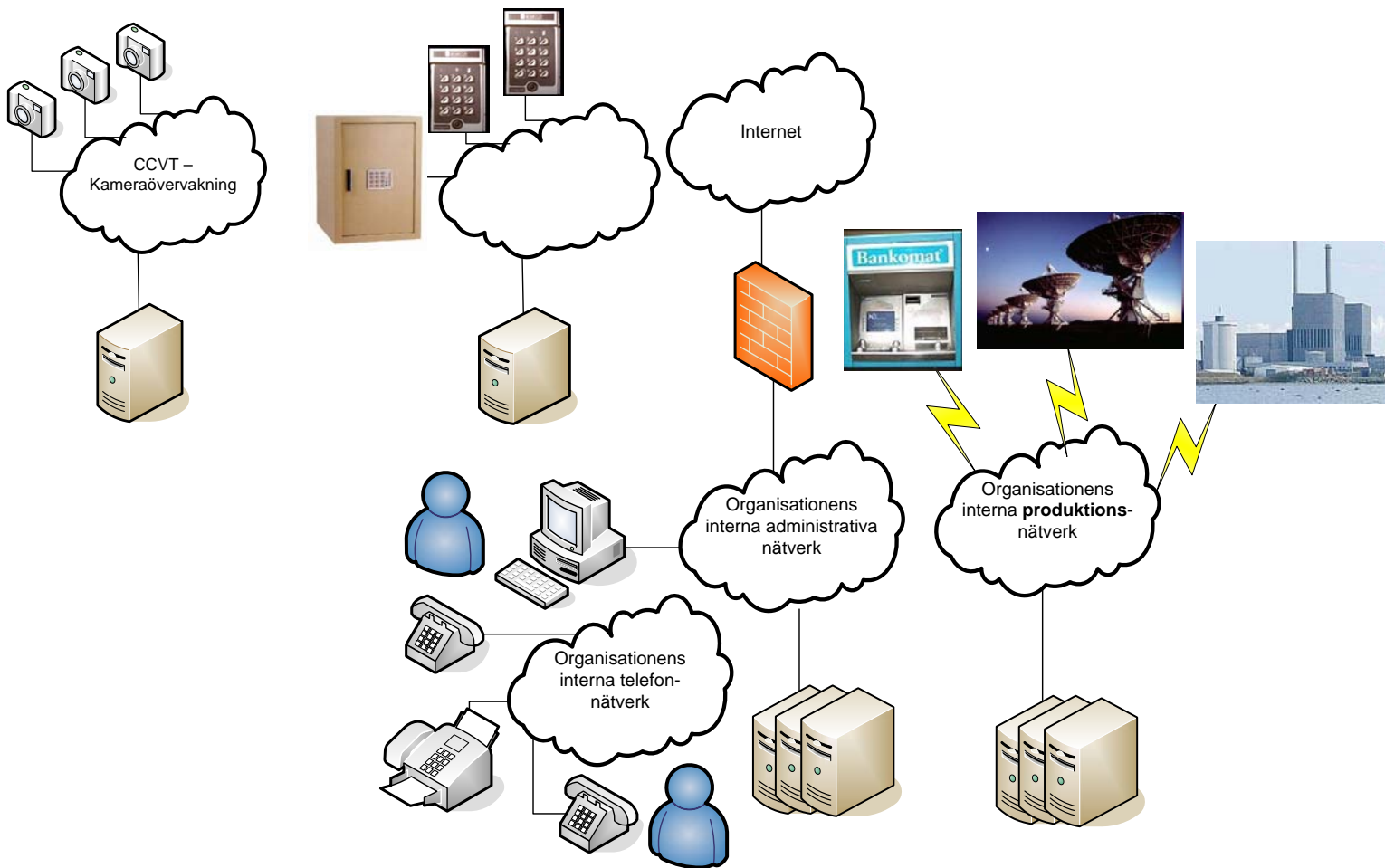
Den *än mer kompletta* nätskissen



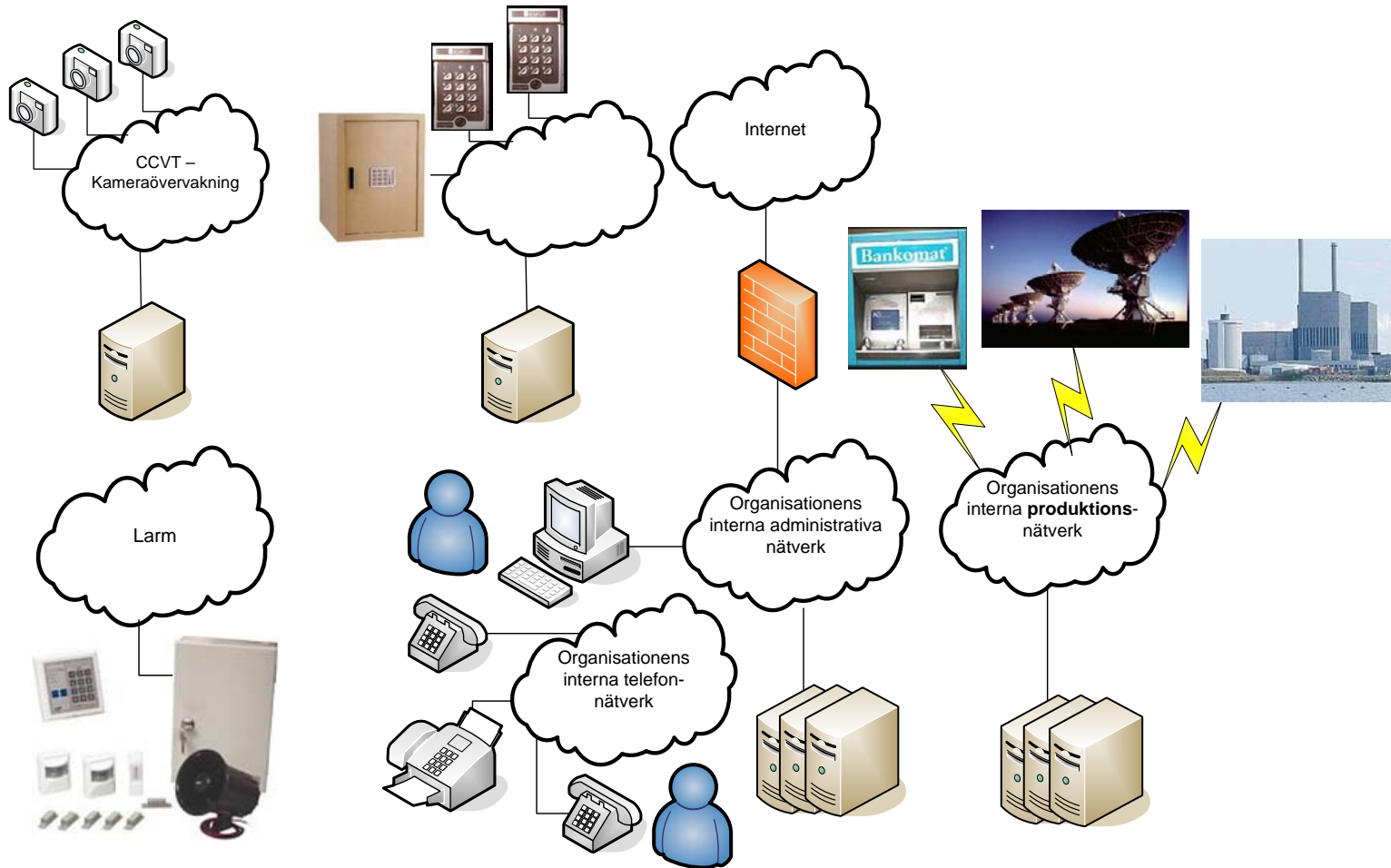
Den än mer kompletta nätskissen



Och än mer kompletta nätskissen



...och än mer kompletta nätskissen

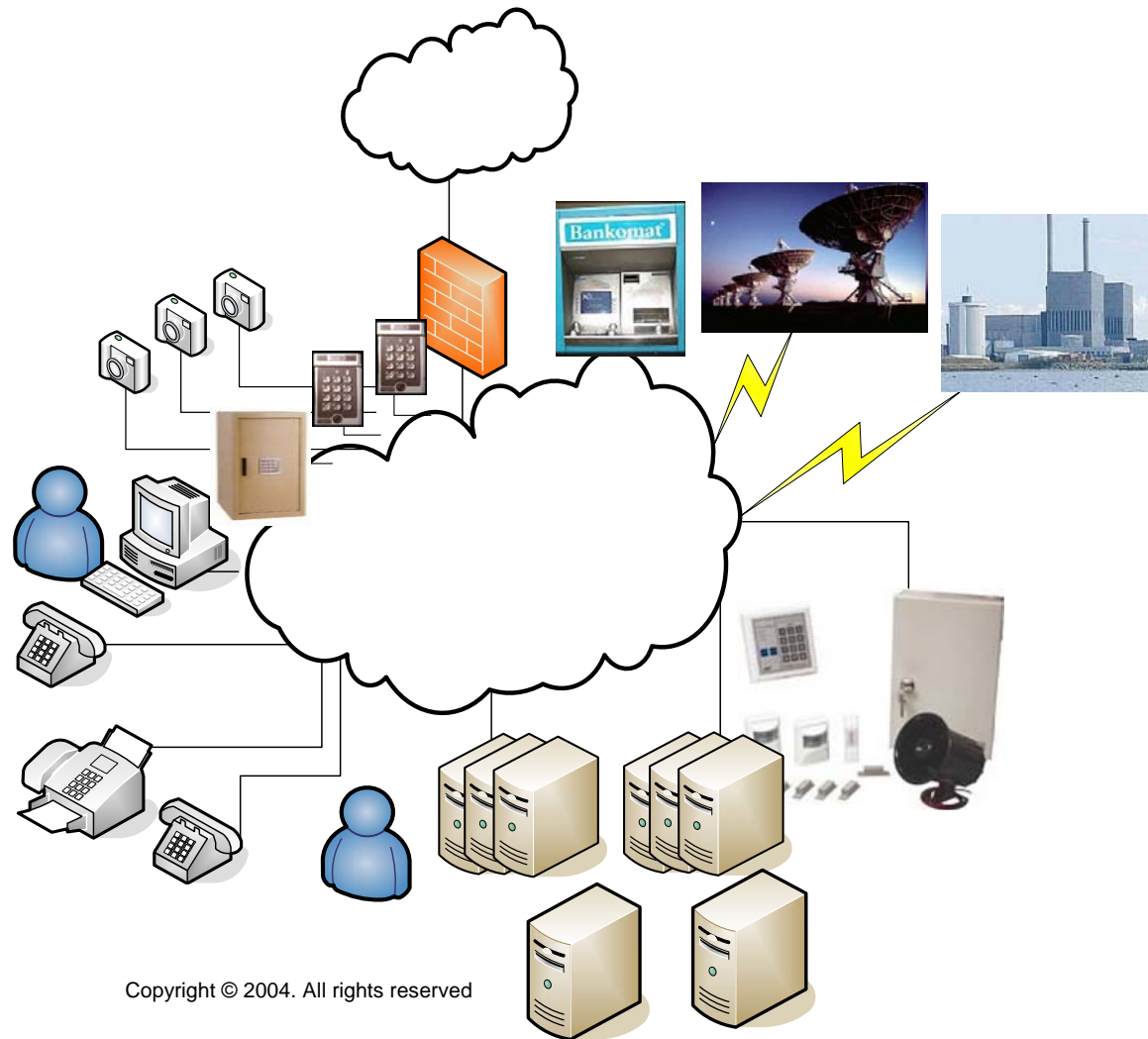




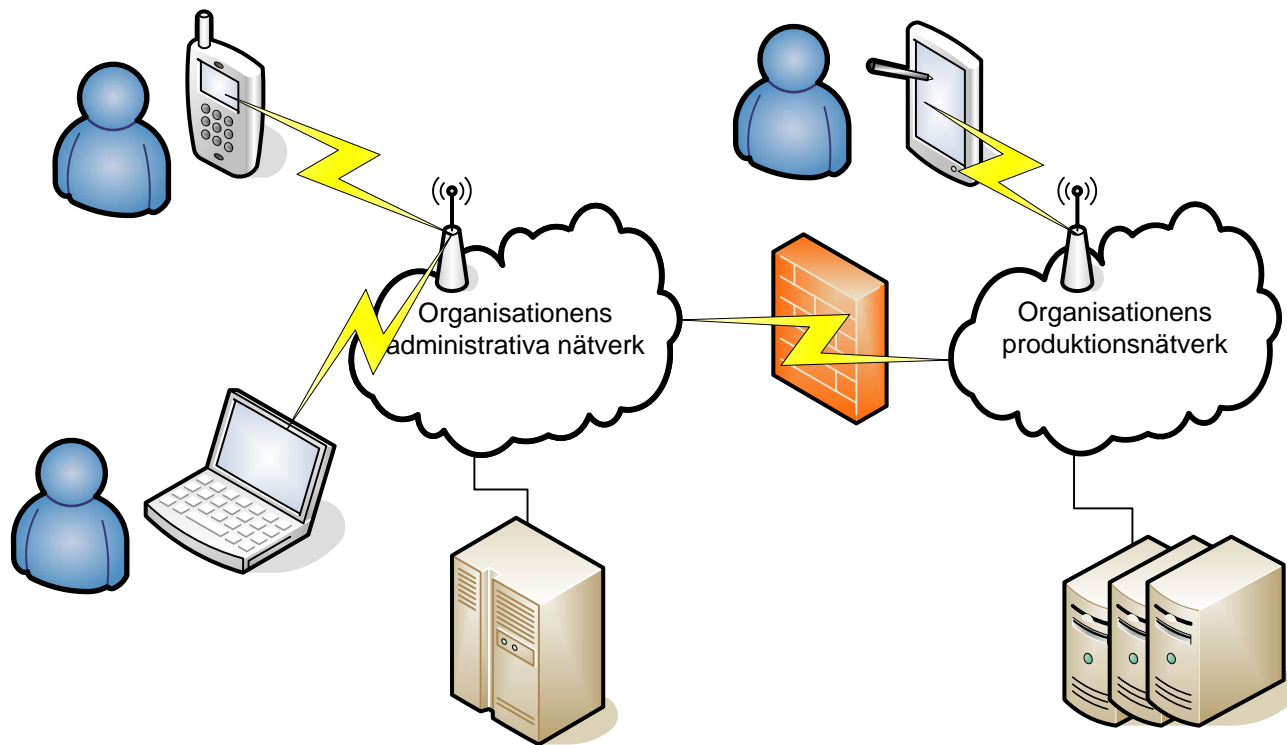
”IP over everything”

- 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

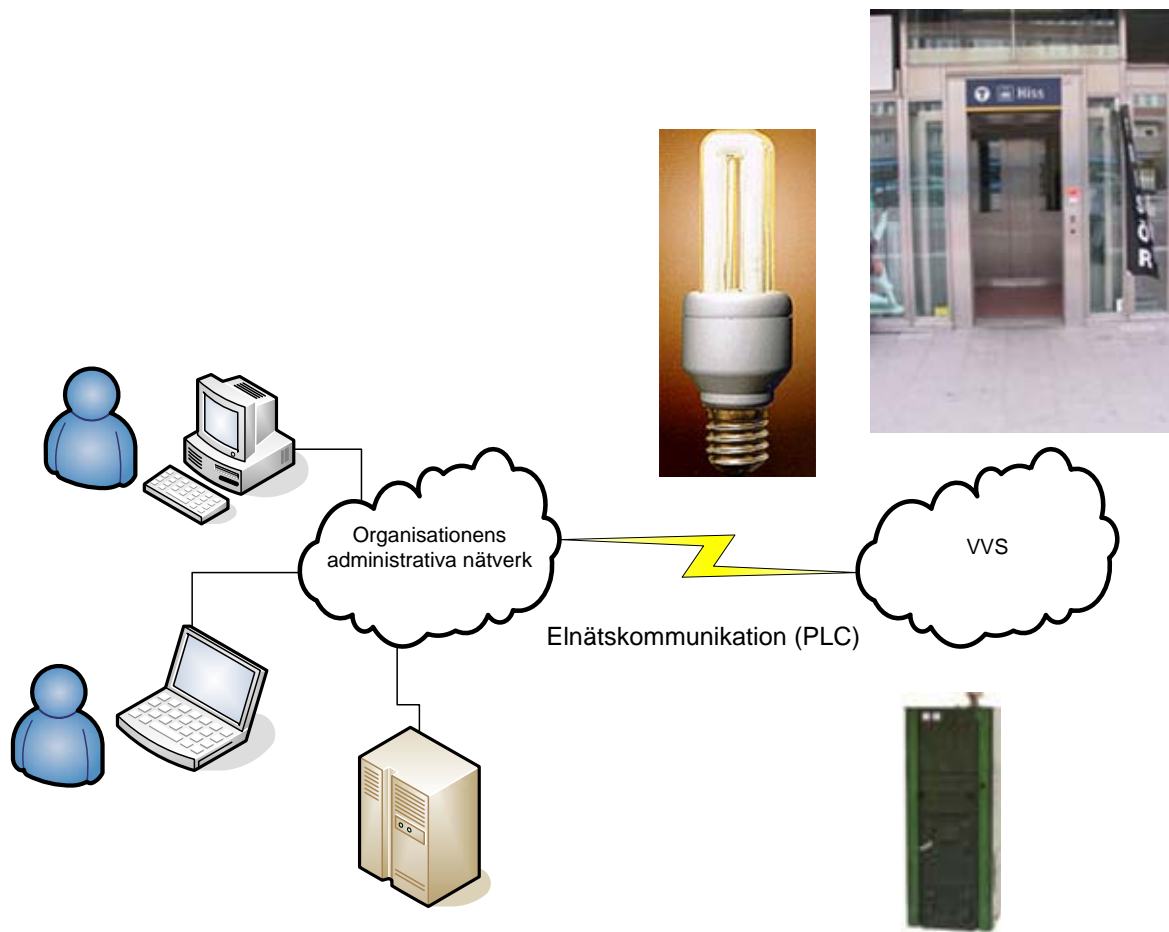
En möjlig framtid?



Andra framtida scenarios...



Andra framtida scenarios...



Verkliga händelser...



Article: Cash machines infected with worm | New Scientist - Opera

Acrobat Reader - [SQL_Slammer_2003.pdf]

NRC: News Release - 2003-108 - NRC Issues Information Notice on Potential of Nuclear Power Plant Network to Wor...

Worm infects ATM ma...

Opera

OperaMail

SecurityFocus HOME ...

Article: Cash mac

http://www.nrc.gov/read

U.S. Nuclear Reg

Home Who We Are What We Do

Home > Electronic Reading Room > Docum

On Jan impact some E service subset represe Analysis paper i

The es

No. 03-108

The SC patch v volume and res

The Ele

The Nuclear Regulatory Commission sta potential vulnerability of their computer

• Cas the cor thr

• Cas the util var traf

FirstEnergy Nuclear, the licensee at Da unprotected computer connection to its investigation also found plant computer worm from working. Corrective actions network, installing an additional layer o patches and install them promptly.

include

• Cyt

• Inte

Information Notice 2003-14, "Potential the NRC's web site at this address: htt

Lonworks Nyheter - Opera

Spara upp till 45% på HP & LEXMARK

Amazon.comsökning

SecurityFocus H... Article: Cash ma... Lonworks Nyheter SecurityFocus H... Tom sida Överföringar Echelon Corpor...

http://www.lonworks.se/news/news.htm

Källa: SVM NORTH NODE/MILAB

2004-06-14 Posten Sverige satsar på Bravida

Bravida Säkerhet har erhållit förtroendet att leverera det integrerade säkerhetssystemet Bravida Integra till Posten Sverige AB's paketterminal i Segeltorp. Paketterminalen i Segeltorp byggs just nu ut för att kunna hantera paketedistributionen inom Stockholm. Installationen omfattar både passage och inbrottslarm samt låssmedsarbeten. Totalt omfattar passagedelen ca 80 dörrar och portar.

Bravida Integra nyttjar Echelon Lonworks-baserad kommunikationsteknik mellan kontrollenheter/noder för dörr- och larmmiljöer. Detta sker antingen via traditionell kopparförbindelse, fiberförbindelse, TCP/IP kommunikation via nätverk eller via uppringd förbindelse.

Källa: Bravida

2004-05-24 Tranås Energi köper system av SVM North Node/MiLAB



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



Viktiga frågor vid konvergens

- TTR & MLE - Total time to recover & Maximum loss expectancy
 - 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?

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?



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