

“The question is not if you are paranoid, it is if you are paranoid enough.”

Anonymous

ATT BYGGA SÄKRARE NÄT – VARFÖR DET INTE RÄCKER MED EN VALLGRAV LÄNGRE

Martin Englund

Senior Security Engineer

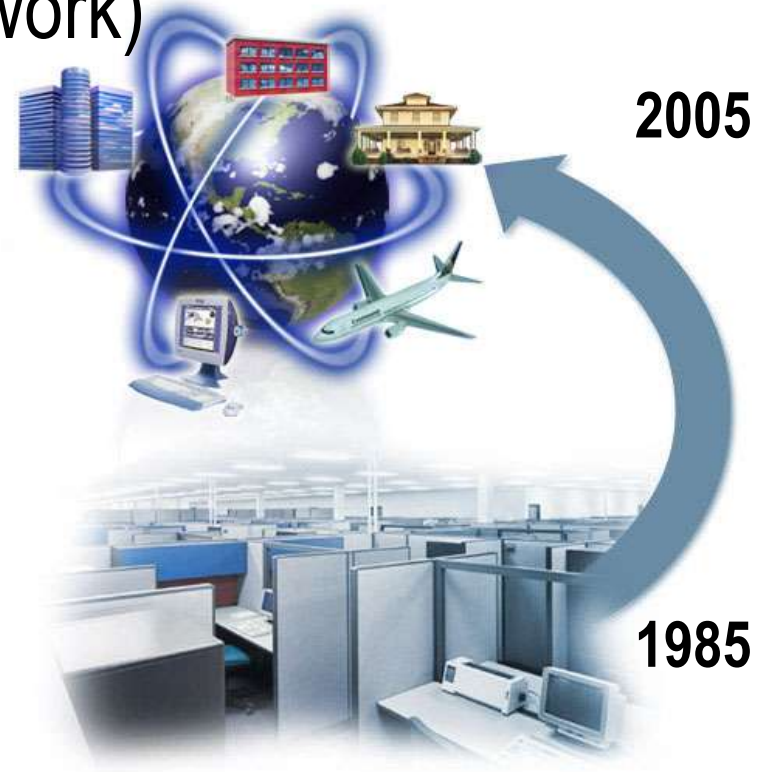
Sun IT Security Office

Agenda

- Introduktion & bakgrund
- Problemställning
- Lösningar
- Summering

Sun IT och SWAN

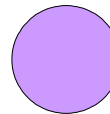
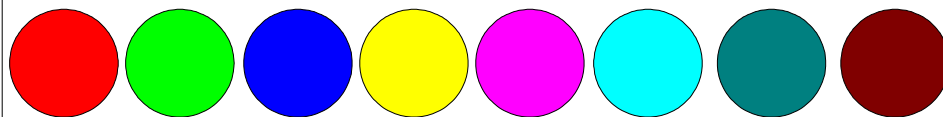
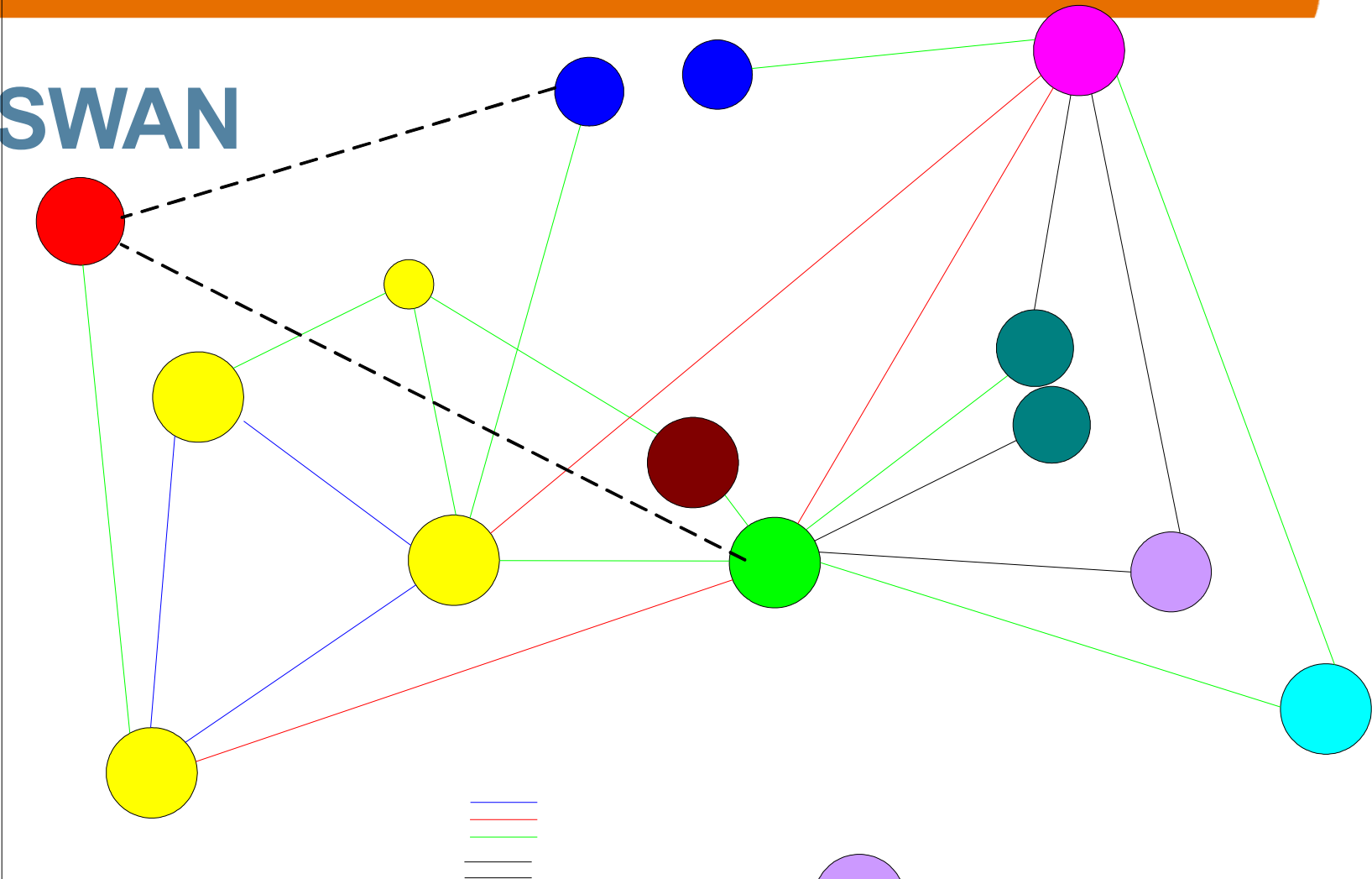
- Sun IT
 - > Sköter Suns IT-drift i över 170 länder
- SWAN (Sun Wide Area Network)
 - > Suns intranät
 - > Började som ett labnät för utvecklingen av TCP/IP till SunOS
 - > Användarvänlighet har fått gå före säkerhet
 - > Har växt mycket fort!



SWAN

- 1985: Pre-SWAN
 - > Bara lokala nätverk
- 1987: SWAN Phase I
 - > 14.4 kBps ring: Milpitas, Washington, Chelmsford, Dallas
- 1991: SWAN Phase I
 - > 20 fler städer och snabbare länkar
- 1993: SWAN Phase II
 - > T1 stamnät, två transatlantiska länkar till England
- 1995: SWAN Phase III
 - > Outsourcat till MCI, byte från Sun-utrustning till Cisco

SWAN



Agenda

- Introduktion & bakgrund
- **Problemställning**
- Lösningar
- Summering

Problemställning

- Vi har ett nästan platt nätverk utan segregation och med otillräcklig behörighetskontroll
- Hur får vi bättre kontroll på:
 - > Vem som har tillgång till nätverket?
 - > Vem som är vem?
 - > Vem som har tillgång till vad?
- Mitt jobb:
 - > Undersök hur vi förhindrar anonym åtkomst till nätverket

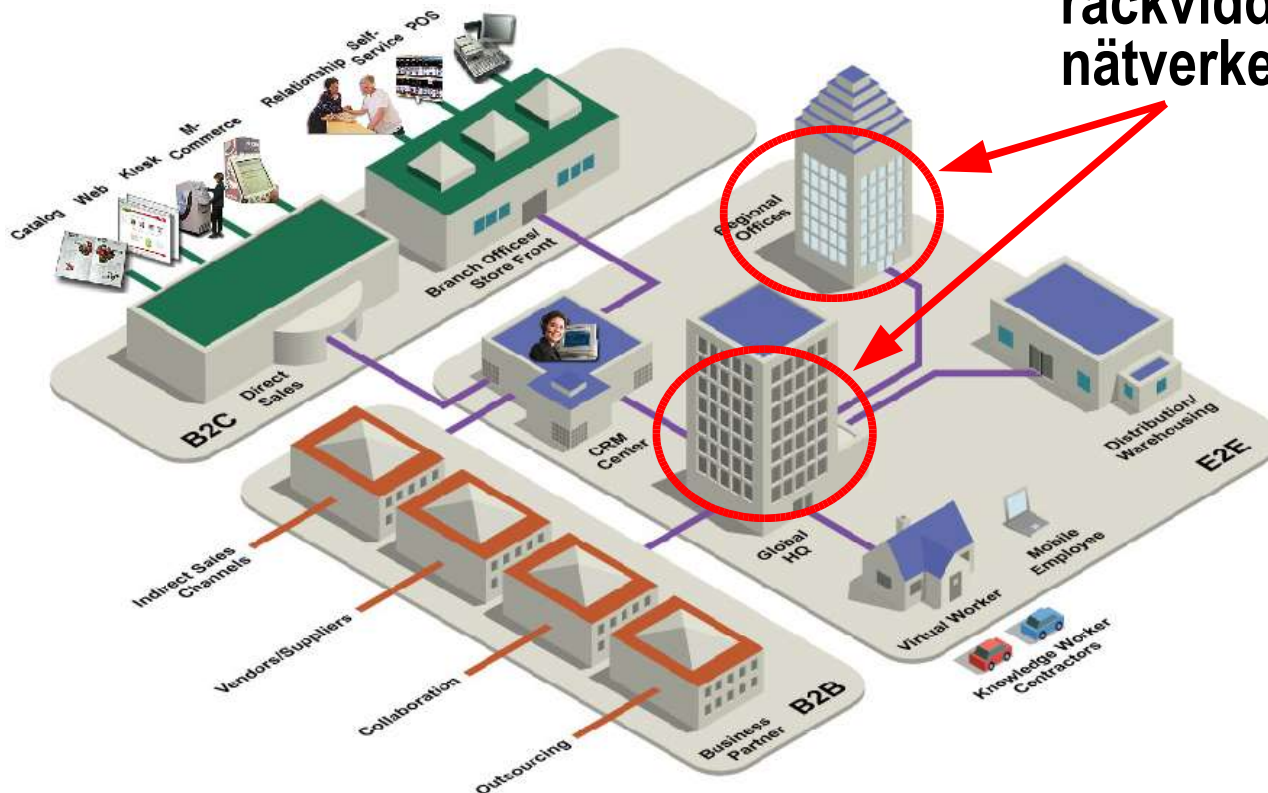


Hotbilder

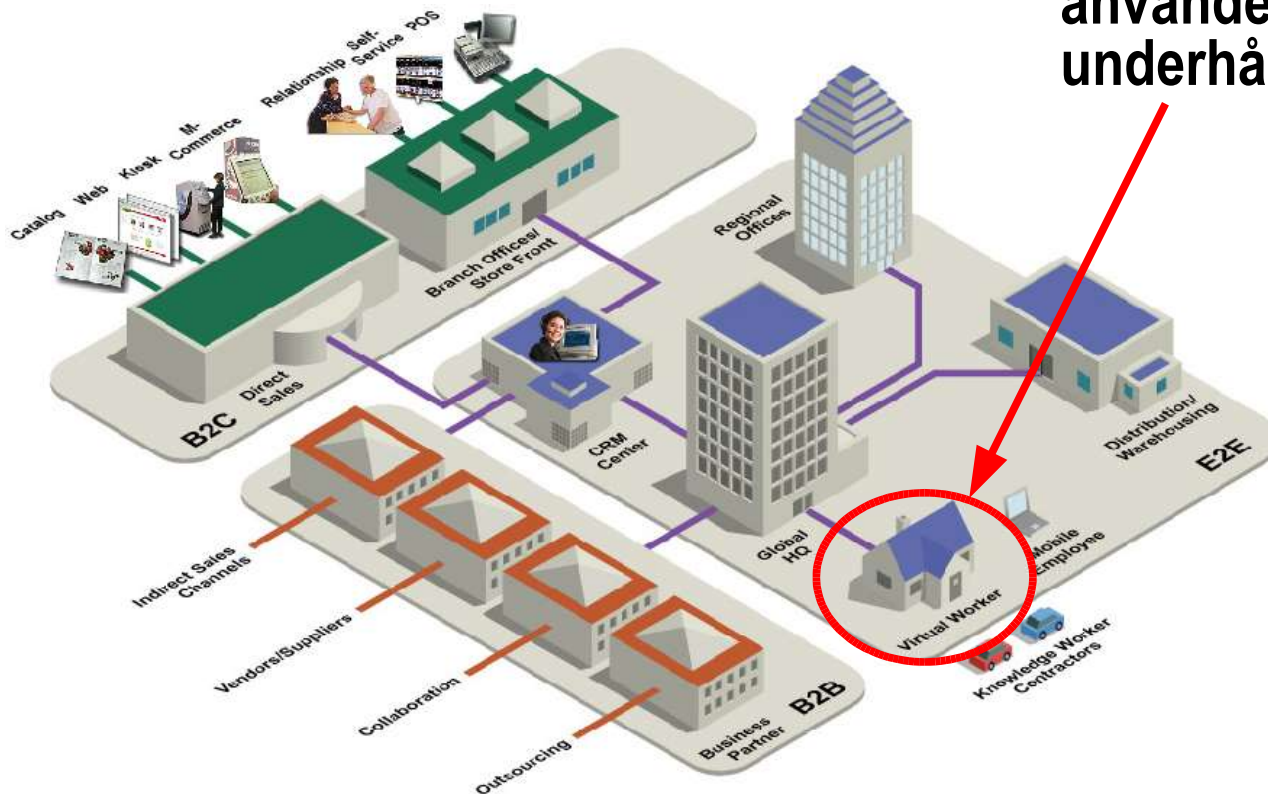
- Börja med att analysera hotbilderna
 - > Interna
 - > Externa
 - > Processer
 - > Personer
 - > Teknologier
 - > ...

Hotbild #1

Anställda kopplar in otillåtna
(och felkonfigurerade)
WLAN som ger alla inom
räckvidd full tillgång till
nätverket



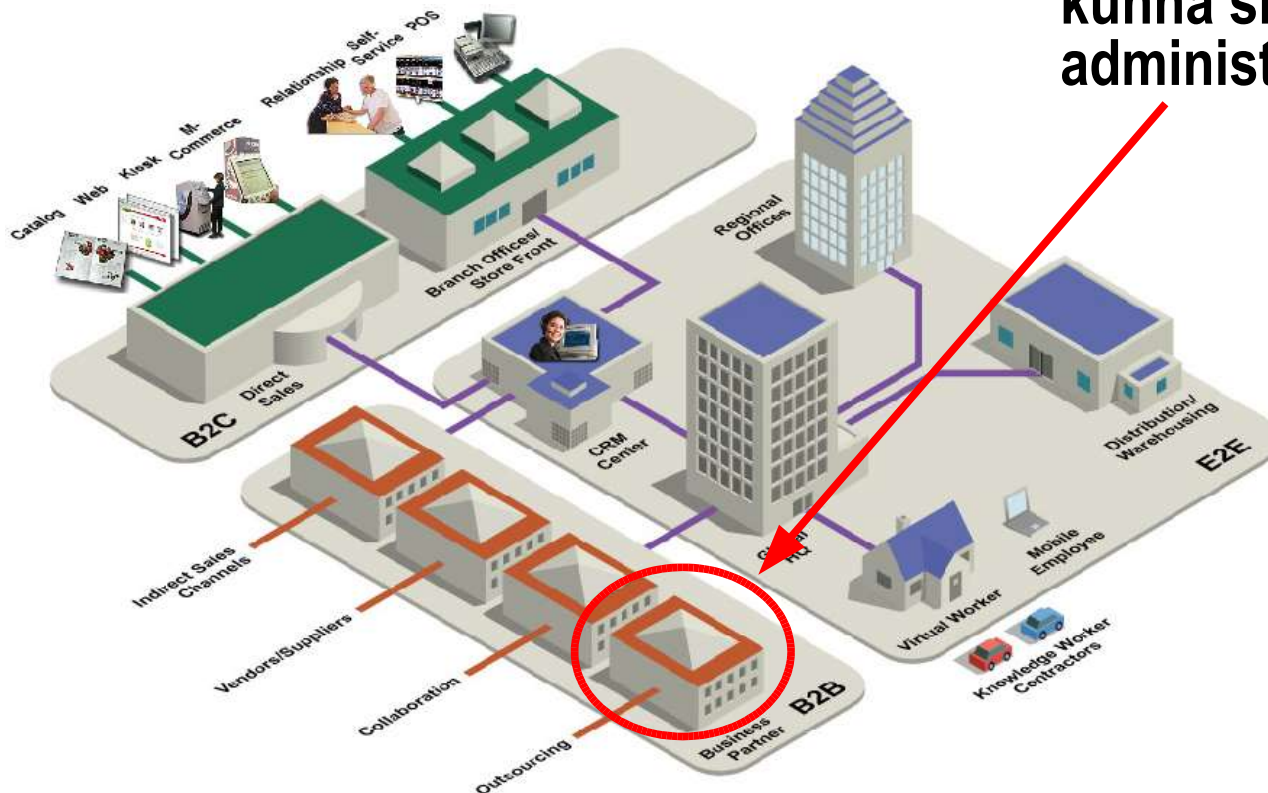
Hotbild #2



Anställda jobbar hemma och använder sig av dåligt underhållna datorer

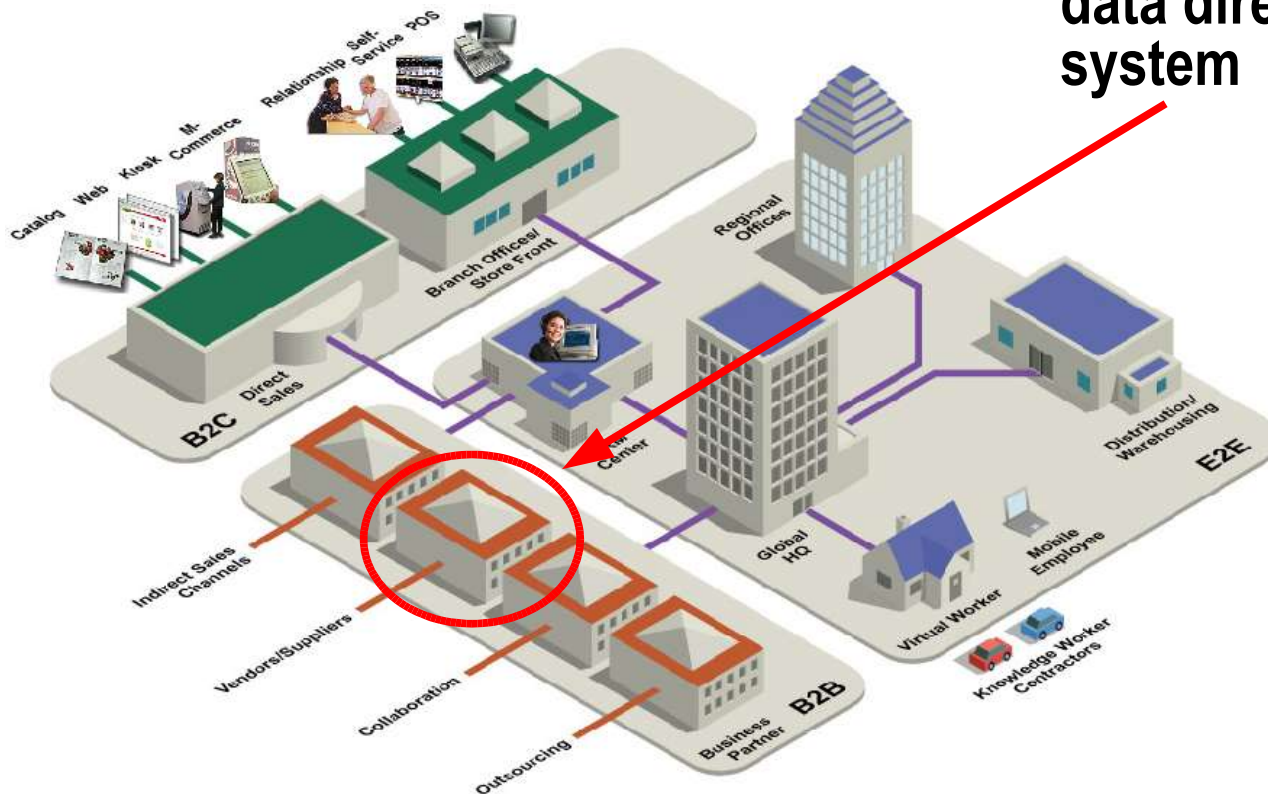
Hotbild #3

Outsourcing firmor ges (full) tillgång till nätverket för att kunna sköta drift och administration



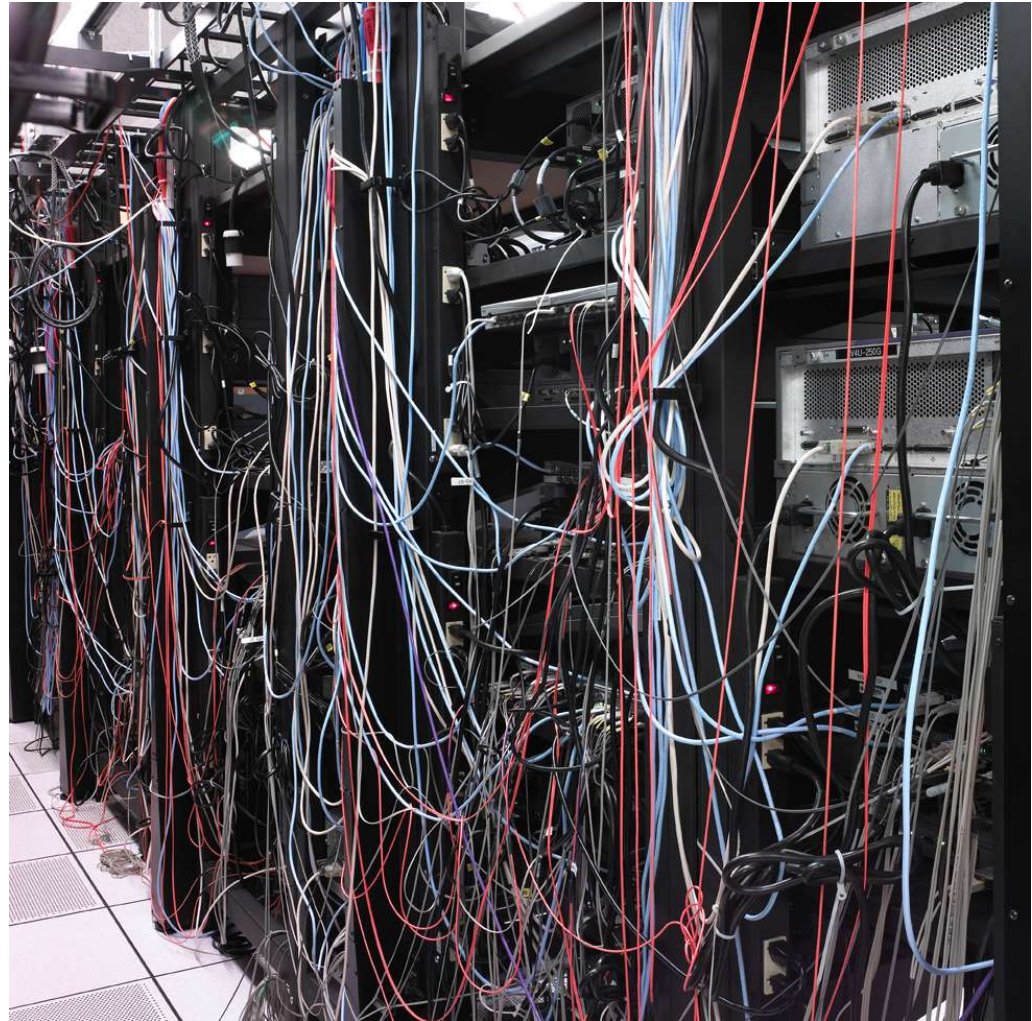
Hotbild #4

Partners tillåts att hämta data direkt ifrån interna system



Vad gör vi åt de nya hotbilderna?

- VPN
- WLAN
- Partners
- Outsourcing



Traditionell nätverksstruktur fungerar inte längre

- Borg och vallgrav (castle and moat)
 - > Fungerar bara om man har en tydligt definierad in- och utsida
- Vad gör man när man har för många på insidan som man inte litar på?
 - > NIDS? HIDS? WIDS? IPS?
 - > Åtgärdar bara symptomen inte problemet
- Vi har tagit bort portarna i ringmuren!



Agenda

- Introduktion & bakgrund
- Problemställning
- **Lösningar**
- Summering

Lösningar

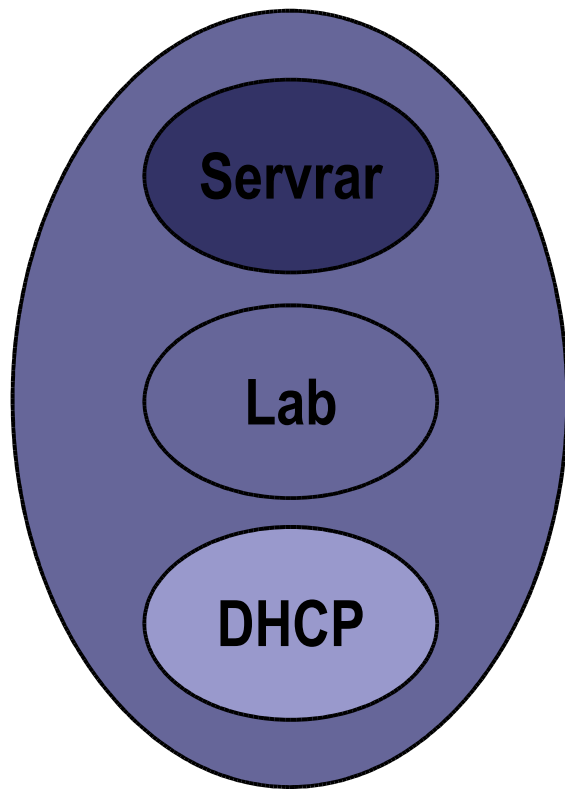
- Många sätt att lösa problemet
- Viktiga faktorer
 - > Kostnad
 - > Tid att implementera
 - > Platformsoberoende
 - > Skalbarhet

Lösning #1: Ny nätverkslayout

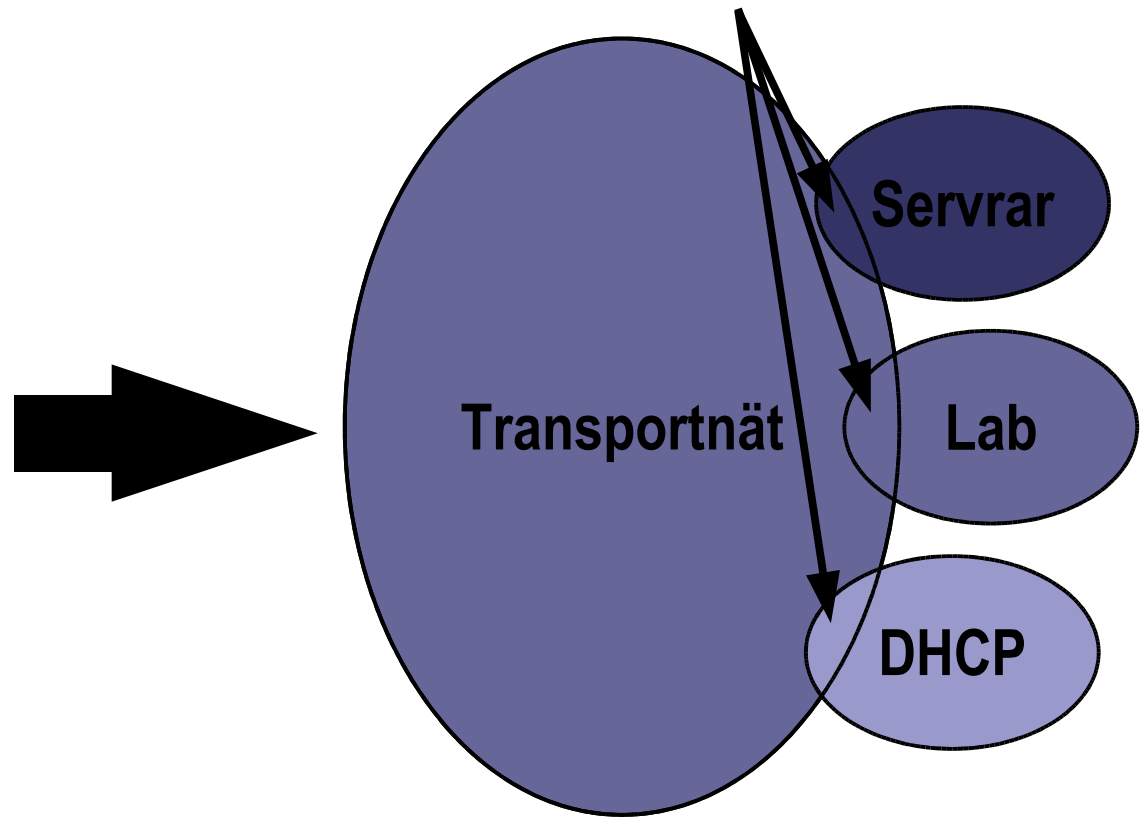
- Riktig segregering av nätverket
- Fördelar
 - > Elimineras grundproblemet
 - > Nätverket blir motståndskraftigare
 - > Lätt att lägga till filtrering
- Nackdelar
 - > Kräver mycket resurser att implementera
 - > Tar lång tid att implementera

Segregering av nätverket

Ingen gräns mellan nätverken



Tydligt definierade snittytor



Lösning #2: IPsec

- Kräv IPsec med ett CA-utfärdat certifikat för att komma åt datorerna på det interna nätverket
- Fördelar
 - > Reducerar behovet av perimeterskydd
 - > Ger en logisk segregation av nätverket
 - > IPsec finns till de flesta operativsystem
- Nackdelar
 - > Svårt att göra en gradvis driftsättning
 - > Komplicerad certifikathantering

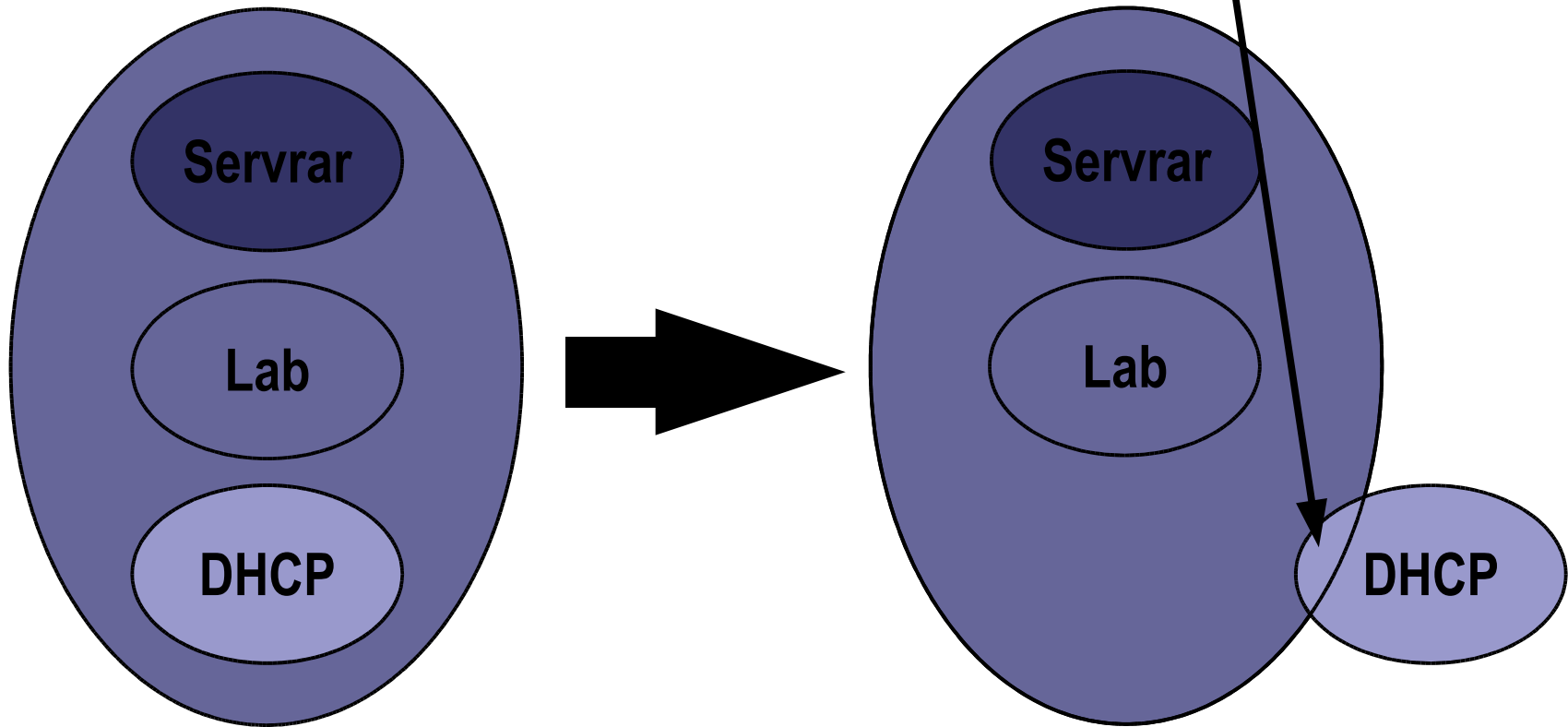
Lösning #3: 802.1x

- Kräver autentifiering av enheter som ansluts innan de ges full tillgång till nätverket
- Fördelar
 - > Delvis segregation av nätverket
- Nackdelar
 - > Saknar klientprogramvara för vissa plattformar
 - > Kräver stöd i switcharna (uppgradering/inköp)

Delvis segregation av nätverket m.h.a. 802.1x

Ingen gräns mellan nätverken

Tydligt definierad snittyta



Lösning #4: Blackbox (hotell-lösning)

- Installera en “blackbox” mellan varje nätverk och SWAN som kontrollerar åtkomsten
- Fördelar
 - > Enkel att driftsätta
 - > Delvis segregation av nätverket
- Nackdelar
 - > Dyr lösning när man har hundratals kontor
 - > Mest inriktad på web-traffik
 - > Leverantörsspecifik lösning

Agenda

- Introduktion & bakgrund
- Problemställning
- Lösningar
- **Summering**

Hur bygger man ett säkert nätverk?

- Segregera nätverket ordentligt från början
 - > Det är svårt och dyrt att göra i efterhand
- Var försiktig om ni outsourcar
 - > Se till att ha säkerhet med i kontraktet
- Filtrera i skärningspunkterna
 - > Använd t.ex. AppGate
- Lite inte på klienterna
 - > Anta att alla kommer från Internet



Frågor?

ATT BYGGA SÄKRARE NÄT – VARFÖR DET INTE RÄCKER MED EN VALLGRAV LÄNGRE

Martin Englund

martin.englund@sun.com

<http://blogs.sun.com/martin/>