



# Vad är nästa hot? KommitTs - Våren 2007

Thomas Nilsson

[thomas@certezza.net](mailto:thomas@certezza.net)

2007-05-09

# Om Certezza



*Ett oberoende informations- och IT-säkerhetsföretag som erbjuder lösningar för en säker IT-infrastruktur.*





# Ett historiskt perspektiv



# #1 - Mobil evolution?

1. Köpa enkäslig information till mobil enhet
  2. Skydda ägning känslig information
  3. Skydda ägning av känslig information
  4. Köpa enkäslig information till mobil enhet
- Eller, varför inte välja att köpa tjänsten som lär vara "*i princip*" säker?



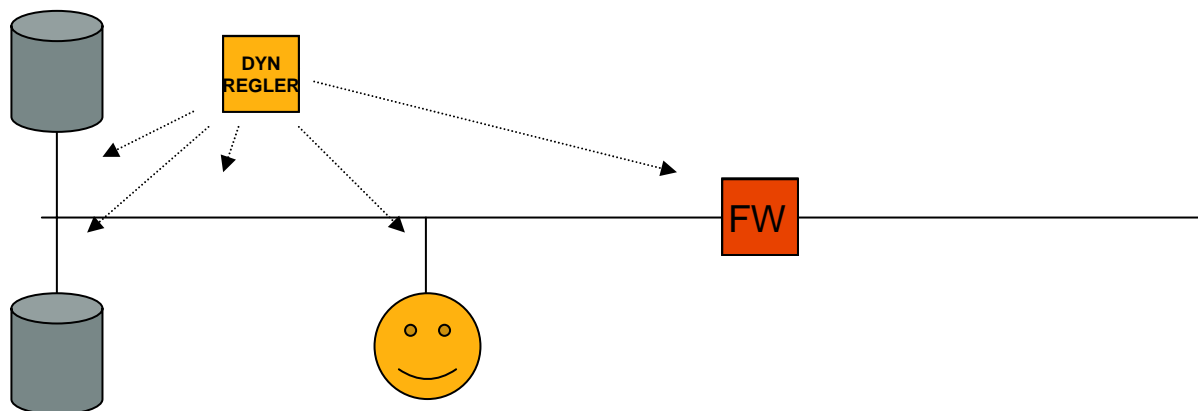
# #2 - Riskmedvetenhet

- Respekten för Internet avtar
  - Nya investeringar endast vid nya tillämpningar
  - Befintliga säkerhetslösningar förbättras sällan
- Nygamla risker
  - Ny teknik utsätts för gamla attacker
- Enkelspåriga riskanalyser
  - Viktig källa till informationssäkerhetspolicyn
  - Ålderdomliga hotbilder
  - Frånvaro av sakkunskap
  - En sökande & upptäckande process
    - Välj inte redan upptrampade stigar!



# #3 - Från nät- till informationsskydd

- IT-säkerhetsprodukterna förändras



- Vem du är bestämmer dina rättigheter
  - Regler komponeras dynamiskt
- Snyggt, eller? Vad är haken?

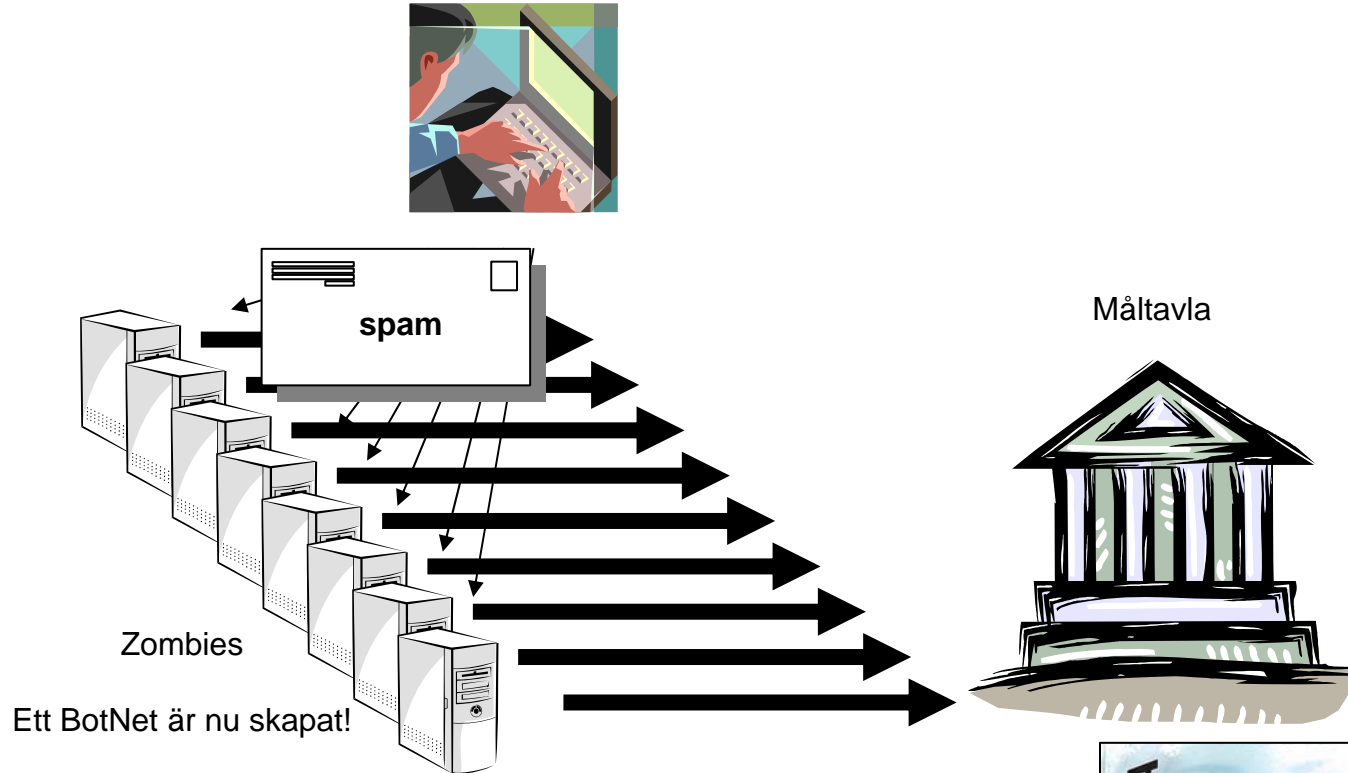


# #4 - Autentisering & kryptering

- Enskilt viktigaste byggstenarna!
- Nyckellängden var 90-talets fokusområde
- Design- och faktafel är nutidens realitet
  - Förstärkt 1-faktor, två olika 1-faktor osv
    - Du vet, Du har, Du är...
  - Nycklar förvaras och distribueras osäkert
    - Auguste Kerckhoff 1835-1903
  - Bankmissen
    - Krypterar utan att först autentisera
- Innehållskontroll?



# #5 - Attacker utan försvar



2005 ~5Gb/s, 2006 ~10Gb/s, i år?



# #6 - Dömd av 3:e part

- Er n  
berd
- Exe
- M
- Ö
- U
- Nivå
- B
- Omf
- Ti

To: removal@rt.njabl.org  
Subject: 82.99.51.0/24

Since two weeks ago we are the new "owner" of 82.99.51.0/24. It's not a dialup or dynamic environment. It's our external network and there is only static IP's, mostly firewalls, IDPs, spam-filters, DNS and other kind of computers that a security company needs for their business.

There are NO open relays, NO dial-up port IP, NO other dynamic address and we are NOT operating a system that directly sends out spam.

Attached are RIPE and IN-ADDR.ARPA info.

Please remove us!

Thanks /Thomas Nilsson, Certezza AB, Sweden

# #7 - Rättsproblematik

Saxat ur en faktapromemoria 2004/05:FPM23

- Network Address Translation (NAT)
  - Adresskonvertering mellan VoIP och vanlig telefoni
- Ex på IP-adress 123.456.789
- NTP = Network Transfer Protocols
- Voice over Internet Protocols (VoIP)
  - Använder Internet för överföring av telefonsamtal
- Voice over Broad Band
  - Använder en bredbandsuppkoppling för överföring av telefonsamtal



# Färskt i minnet

- Vad kommer vi att minnas från 2006?
  - Personligt, Nyheter, Sport, Väder

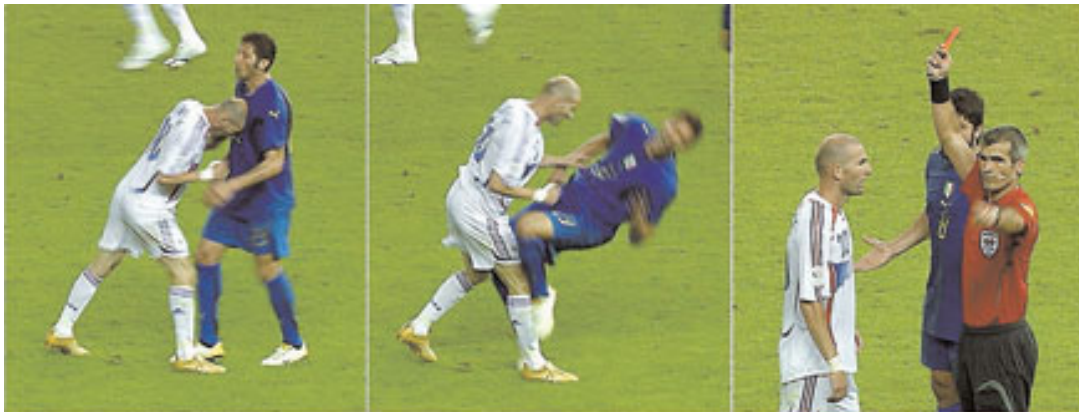


Foto: EPA, TV4

- Informations- och IT-säkerhetsrelaterat?

# "Sämst" 2006

## FP's "intrång" i SAPnet

- Inloggning i publik web
  - Ej access till interna nätet
- <http://fc.sap.net>
  - Äldre version av FirstClass
  - Flera kända sårbarheter
- Login med känt konto
  - ~9mån innan upptäckt
  - Uppfångat i trådlöst nät?!?!
- Påverkade valresultatet!
  - Oklart i vilka riktningar
  - Analys pågår av Sören Holmberg



# ”Bäst” 2006

- Det som inte hände hos stora flertalet!
  - Inget intrång
  - Ingen informationsstöld
  - Inget avbrott
- Tråkigt utfall?
  - Är säkerhet tråkigt när det är som bäst?
- Sannolikt utfall?
  - Är vi säkra på att inget har hänt?

# Om sannolikhet

Minns Tages monolog från Dubbelgöken 1979

- Sannolikhet = Något som är likt sanningen
- Sannolikheten ändras före och efter en händelse
  - När det händer - Osannolikt att det kunde hända
- Än mindre sannolikt att det händer igen
  - Tur att det hände!
- ”... Vi måste lära våra barn, att alltid tala sannolikt, så att dom förstår, att det som hände i Harrisburg inte kan hända här. Eftersom det inte ens kunde hända där, vilket hade varit mycket mera sannolikt med tanke på att det var där det hände.”



# Nästa hot – Nio trender

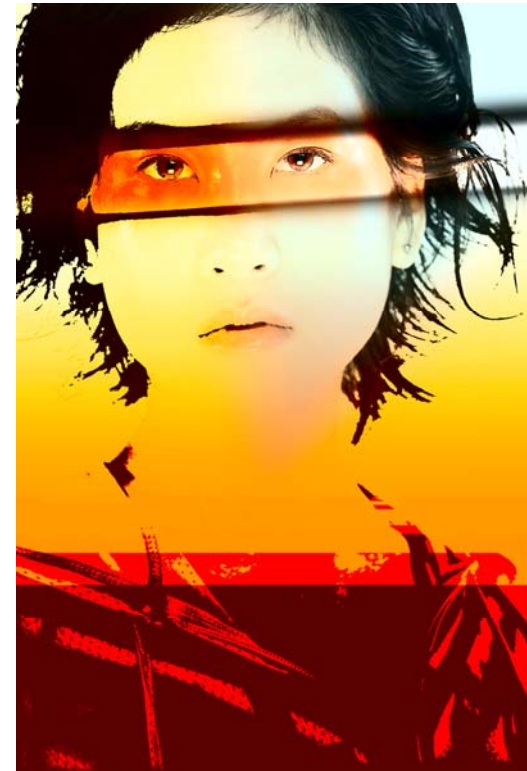
- Mjölkudden > Sverige > Världen
- Nördar > Extremister > Terrorister
- Virus > Maskar/Trojaner > Root kit
- SMTP > WWW > IM > VoIP
- Kassavalv > Datahall > "Internt" nät
- Ledning > IT-Chef > Tekniker
- Funktion > Benämning > 19 tum
- Plats > Autentisering > Hygienkontroll
- Nätsäk > IT-säk > Info-säk

# Fem fokusområden



- Elförsörjning
- Design
- Exponering
- Kontroll
- Mjukt

*Fem fokusområden  
med vardera fem tips...*



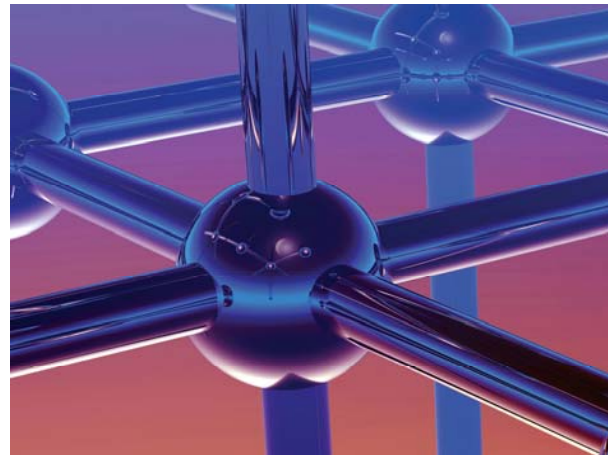
# Elförsörjning

- Så självklart, eller?



# Design

- Zonindelning
- Redundans
- Skydd
- Teknikval
- Dokumentation



# Exponering

- Internt via DMZ via Internet
- Port vs Protokoll vs Innehåll
- "Interna" nätet
- Mobilitet
- Tidsbegränsning



# Kontroll

- Normalt vs Onormalt
- Övervakning
- Autentisering
- Spårbarhet
- Tid



# Mjukt

- Skydda information
- Minskat teknikfokus
- Utbildning av användare
- Hot-, Risk- och Sårbarhetsanalys
- IT-säkerhet vs Administrativ-säkerhet vs Verksamheten



# Till sist – Incidentplanen!

- Hur agerar vi vid en incident?
  - Inte frågan om, utan när!
- Det mesta kan förbättras
  - Beslutsvägar, rutiner, stöd, mål etc
- Första steget är avgörande för utgången
  - Inget steg är också ett steg...
- Ett botemedel är att öva
  - Iscensätt skarpa incidenter
  - Bättre att öva en gång än ingen gång



[www.certezza.net](http://www.certezza.net)