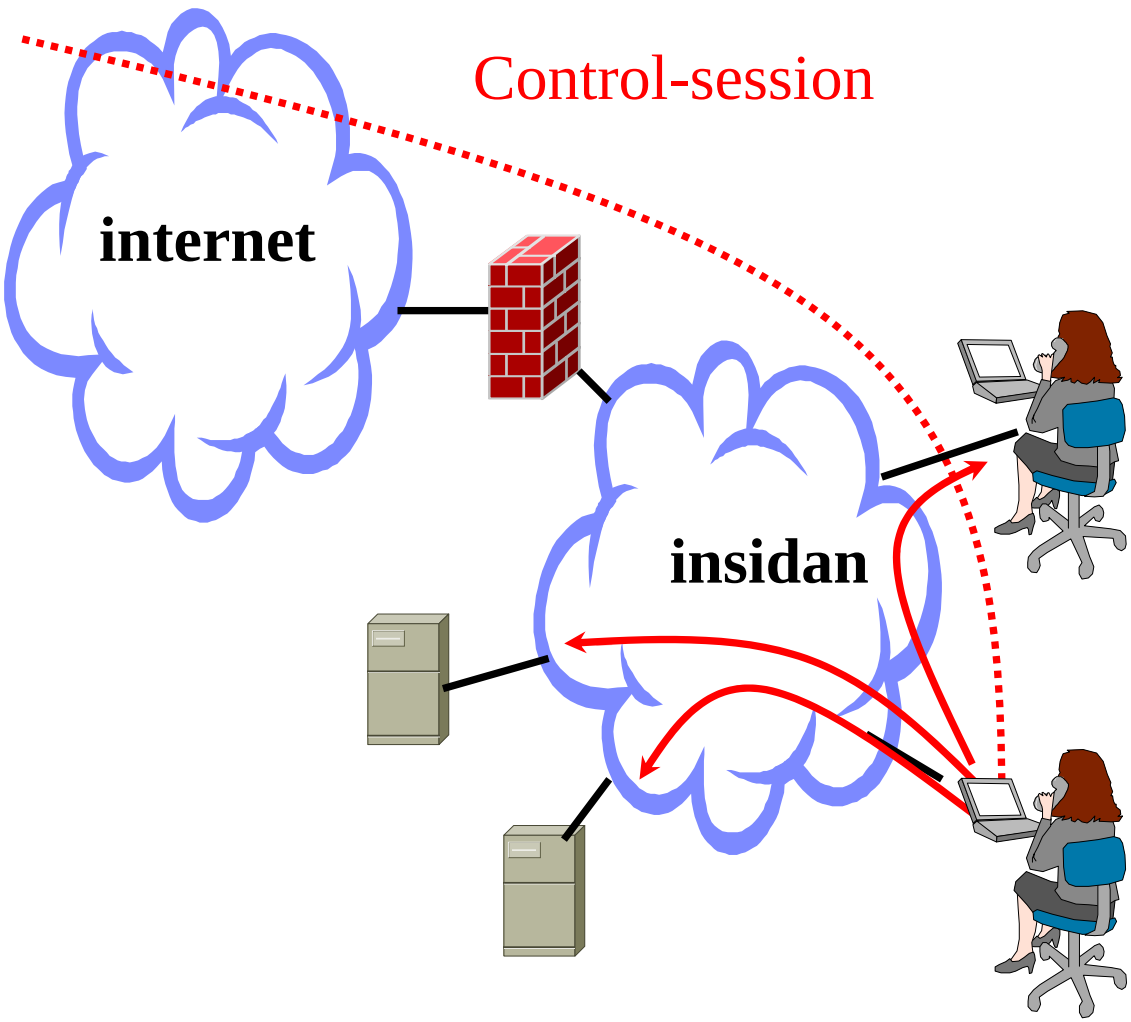
Kan man Surfa lugnt ?
Ciscos Lösning

Håkan Nohre, CISSP

hnohre@cisco.com

Hotbilden



Risk Management är .... ?

- **Minimera risken på kostnadseffektivt sätt** ☒
- **Acceptera Risken** ☐
- **Överföra Risken (försäkring)** ☐
- **Låtsas som det regnar** ☐

Minimera Risken :

- **... att datorn tas över**
- **... att datorn fjärrkontrolleras**
- **....att datorn hackar andra datorer**
- **....att allt detta sker utan att vi märker det**

Cisco Network Admission Control (NAC)

Nätverket *kontrollerar* att alla datorer som ansluter sig till företagsnätet uppfyller policy, t.e.x

- **Körs ej som administratör**
- **Antivirus version**
- **Microsoft Service Pack/Hotfix**
- **Personlig brandvägg/ IPS**

oavsett hur den kopplar upp sig , trådlöst, trådat, IPSEC VPN, SSL VPN.....

Network Admission Control

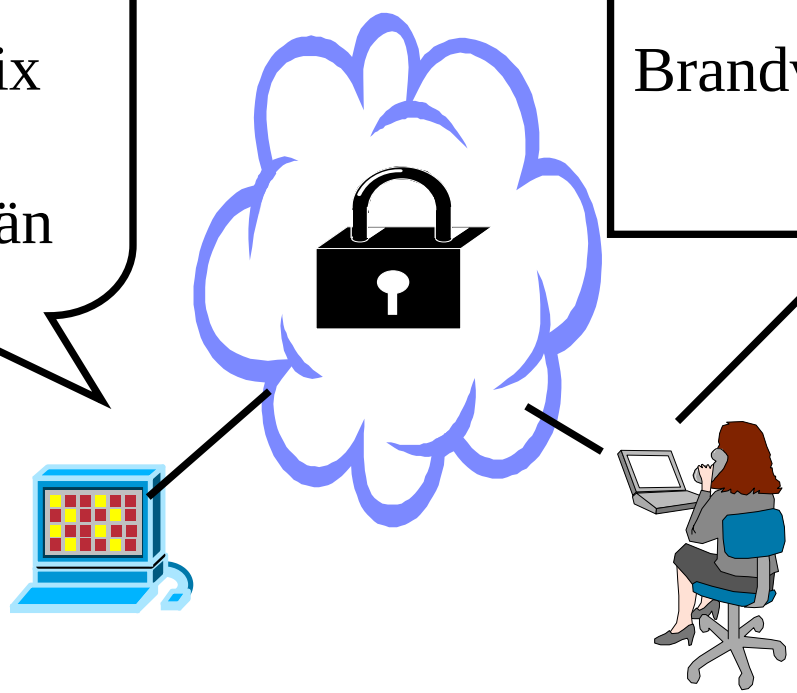
OS – XP, SP 2

Hotfix : KB834723....

Antivirus : Dat 4902

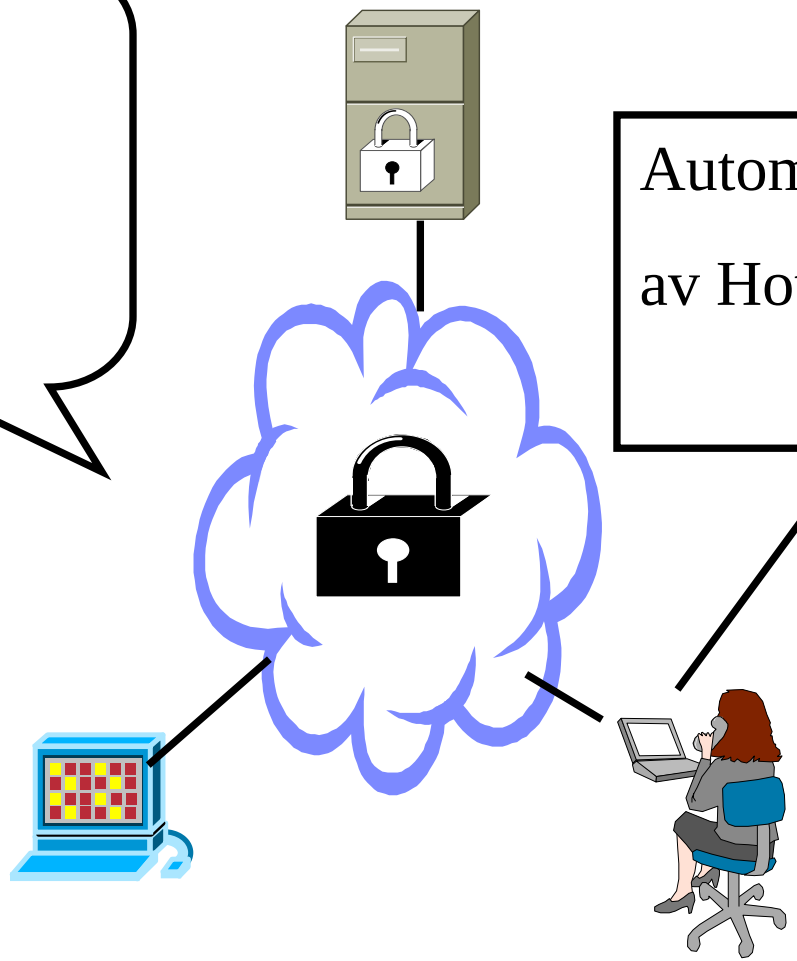
Brandvägg : På....

Hmmm....
Saknar hotfix
MS05-51
sätt i karantän



Network Admission Control

VLAN =
karantän



Automatisk Uppdatering

av Hotfix

Minimera Risken :

- **... att datorn tas över**
- **... att datorn fjärrkontrolleras**
- **....att datorn hackar andra datorer**
- **....att allt detta sker utan att vi märker det**

Intrusion Prevention System (IPS)

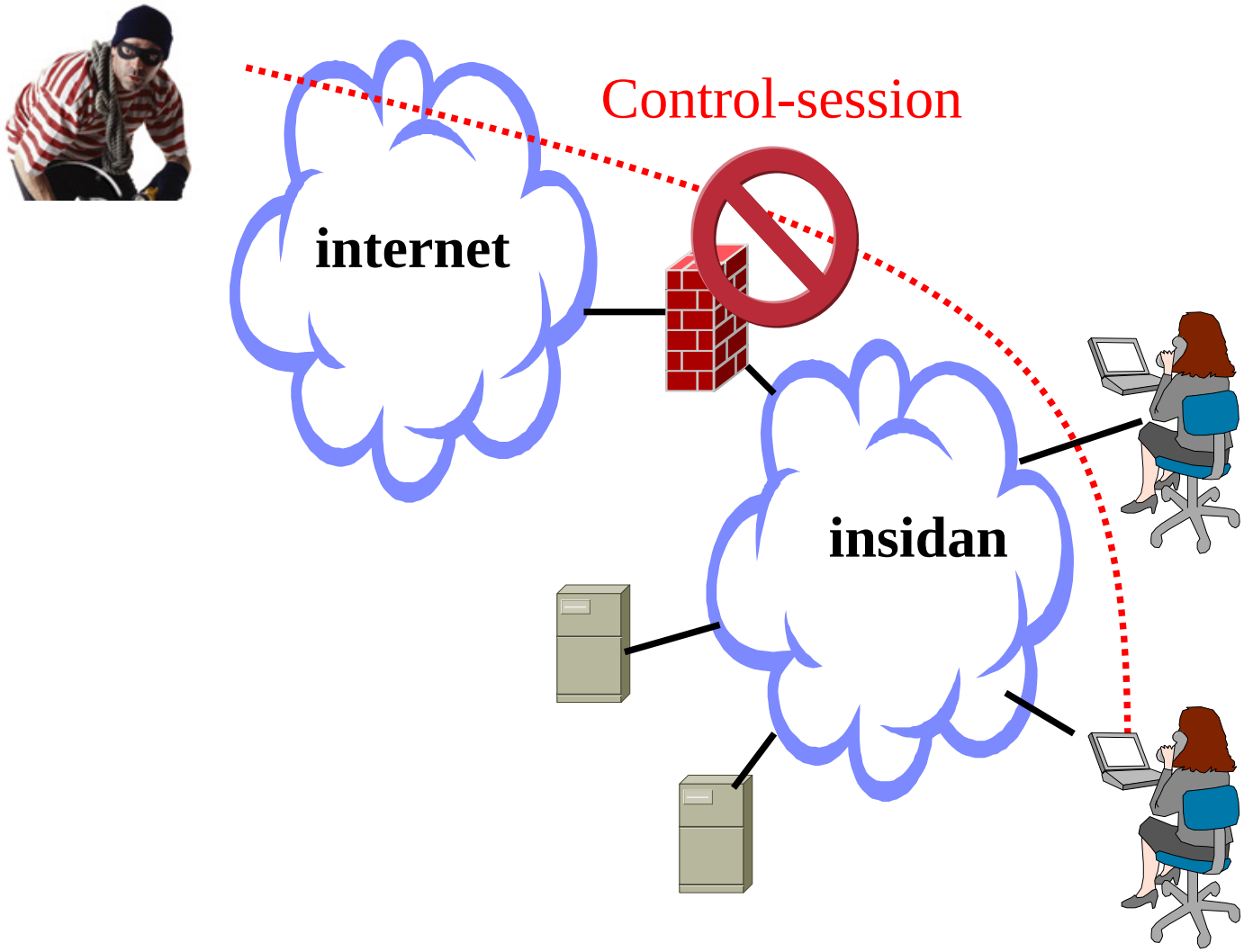
Brandvägg/IPS *kan* inspektera traffik på applikationsnivå för att upptäcka bakdörren (kontrollkanalen)

- **signaturbaserad**
- **anomalier (interaktiva mönster)**

Ej 100% skydd, en *perfekt* kontrollkanal är identisk med ”riktig” webtrafik och omöjlig att upptäcka

IPS/Brandvägg kan upptäcka kontrollkanalen

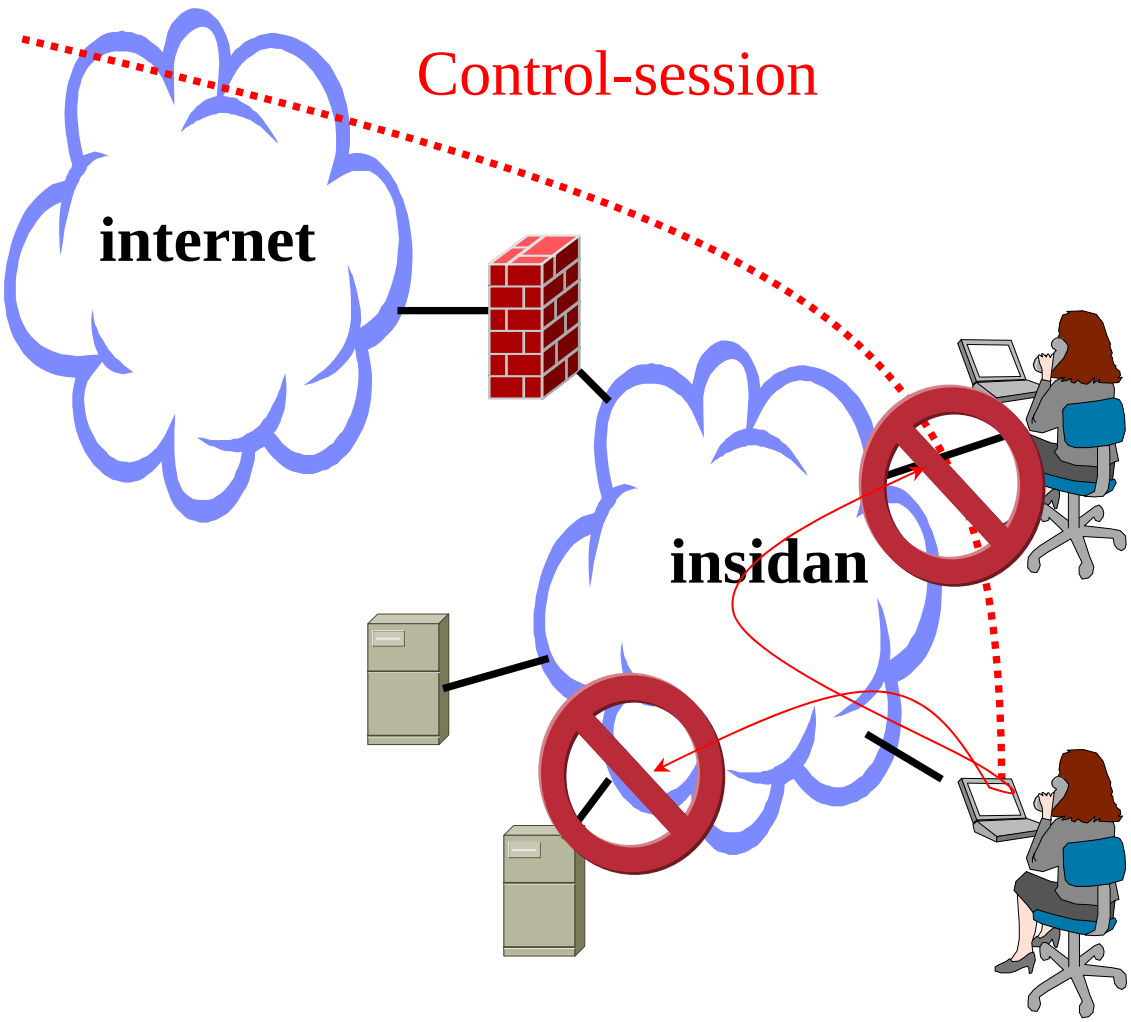
(om kontrollkanalen ej perfekt)



Minimera Risken :

- **... att datorn tas över**
- **... att datorn fjärrkontrolleras**
- **....att datorn hackar andra datorer**
- **....att allt detta sker utan att vi märker det**

Minimera Risken att dator attackerar andra datorer



Minimera Risken att datorn hackar andra datorer

- **Cisco NAC (de *andra datorerna uppfyller säkerhetspolicyn*)**
- **Låt switchen stoppa avlyssning (av lösenord) : ARP spoofing, DHCP spoofing, CAM overflow**
- **Begränsa trafikflöden (private VLAN edge)**
- **Intranet brandväggar/IPS**

Minimera Risken :

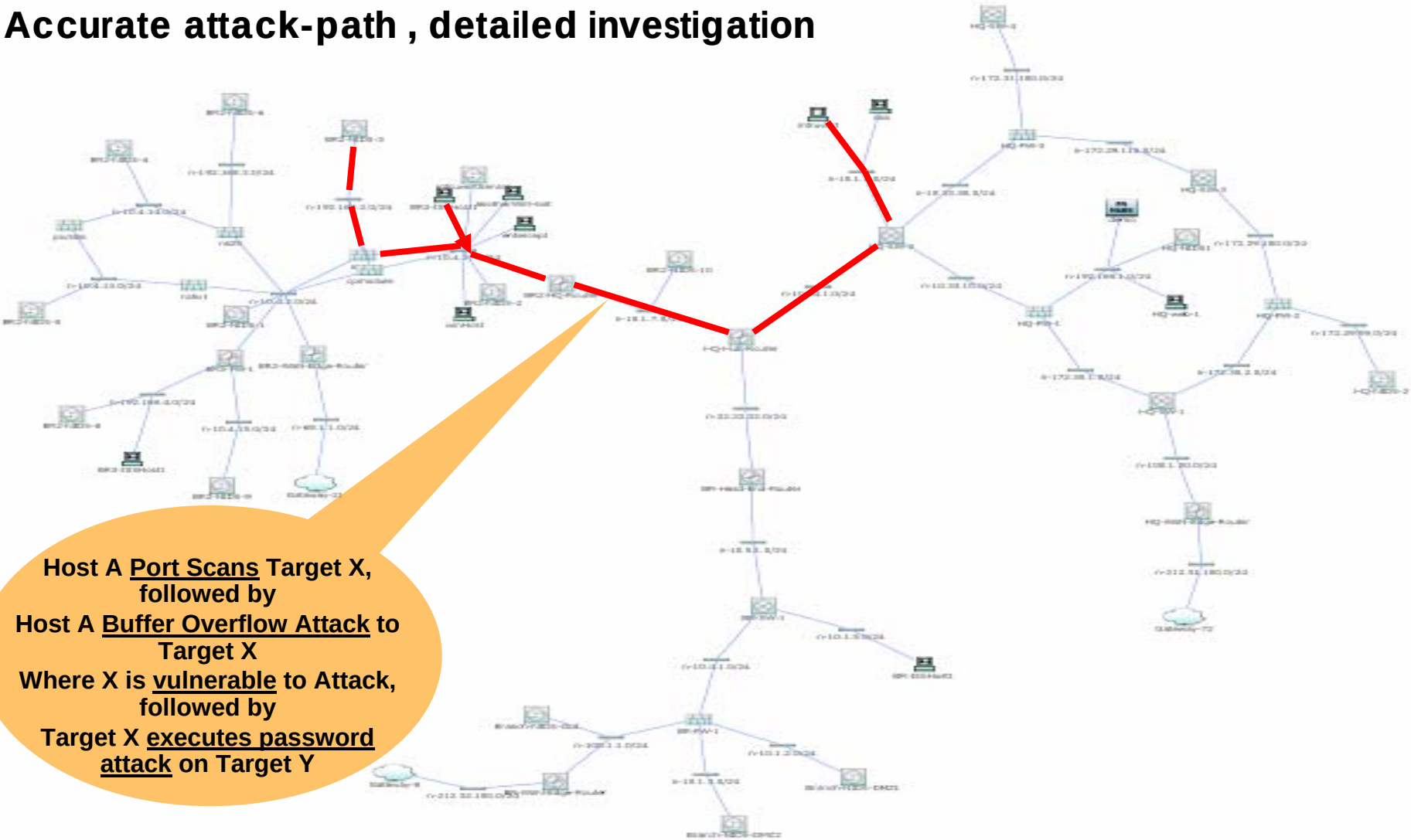
- **... att datorn tas över**
- **... att datorn fjärrkontrolleras**
- **... att datorn hackar andra datorer**
- **....att allt detta sker utan att vi märker det**

Logga. Korrelera. Åtgärda !

- **Brandväggsloggar**
- **IPS loggar**
- **Router loggar**
- **Switch loggar**
- **Operativsystems loggar**
- **Applikationsloggar**

Logga, Korrelera, Åtgärda

Accurate attack-path , detailed investigation



Sammanfattning

- **Minimera risken**
- **Kostnadseffektivt**
- **Ingen lösning är ”perfekt”**
- **Flera lager av försvar, proaktiva och reaktiva**

Läs mer

- **Self Defending Network**

  http://www.cisco.com/go/sdn
- **Cisco Network Admission Control**

  http://www.cisco.com/go/nac
- **Tekniska White Papers om nätverksäkerhet (inklusive säkerhet i switchar)**

  http://www.cisco.com/go/safe