Stuxnet

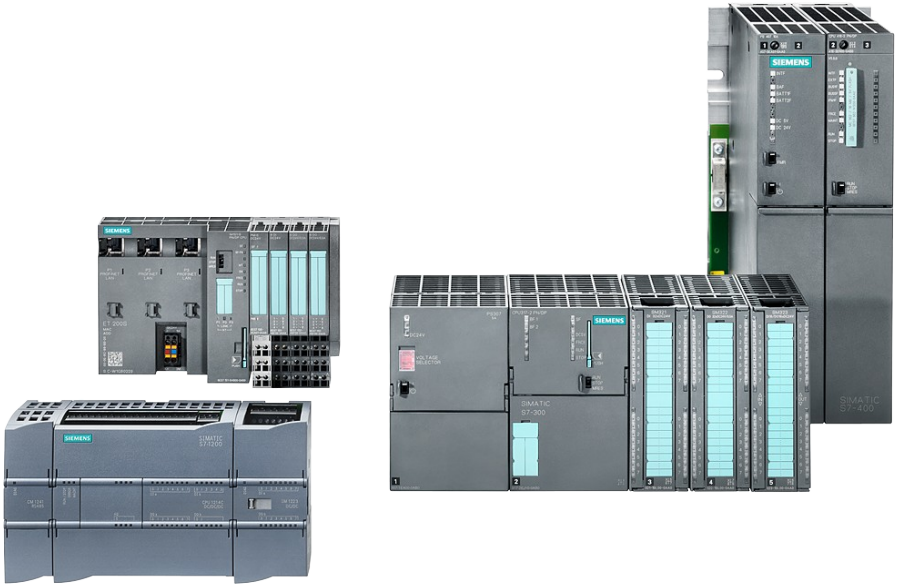
oder
Spy vs. Spy

Industriespionage und -sabotage

Stefan May <smay@4finger.net>

Industriekram

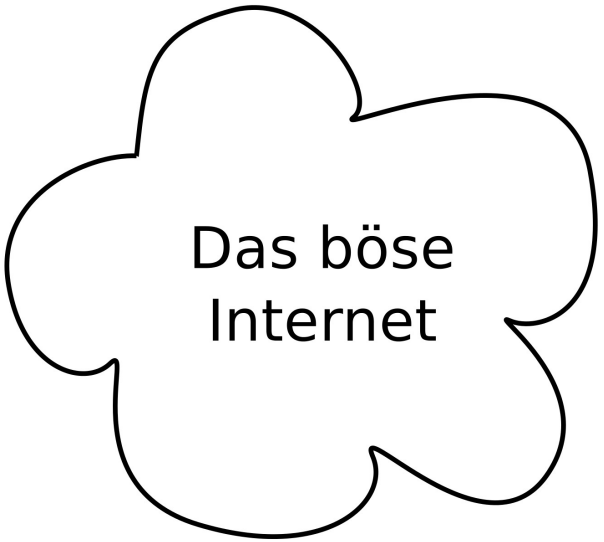
- SPS
  - **S**peicher **P**rogrammierbare **S**teuerung
  - **P**rogrammable **L**ogic **C**ontroller
- Feldbusse
- SCADA

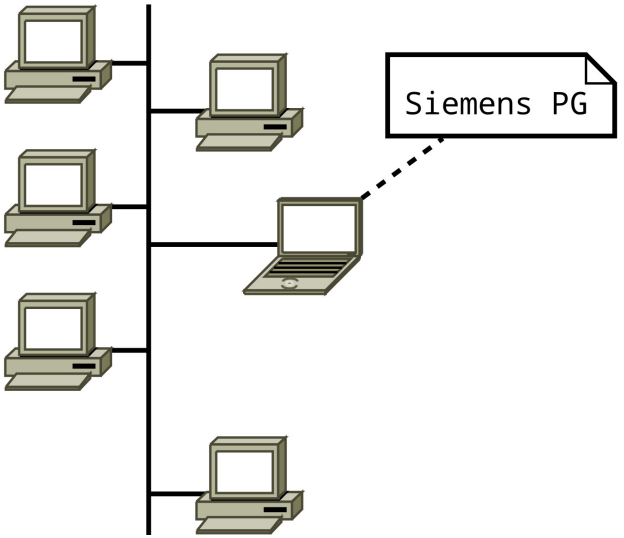


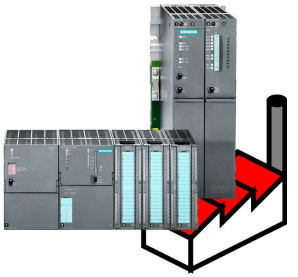
Stuxnet

- Malware mit industriellem Payload
- Entdeckt Mitte Juni 2010
- Dreistufige Infektion:
  - Windows
  - Siemens PCS 7, WinCC und Step7
  - Siemens S7-300 PLCs

Stuxnet Verbreitungsweg







Stuxnet Windows

- Verbreitung durch mehrere 0-day Exploits
- Erstinfektion durch USB-Stick
- Verbreitung über LAN
- Suche nach Field-PGs
- Installation der **signierten** Treiber *mrxcls.sys* und *mrxnet.sys*

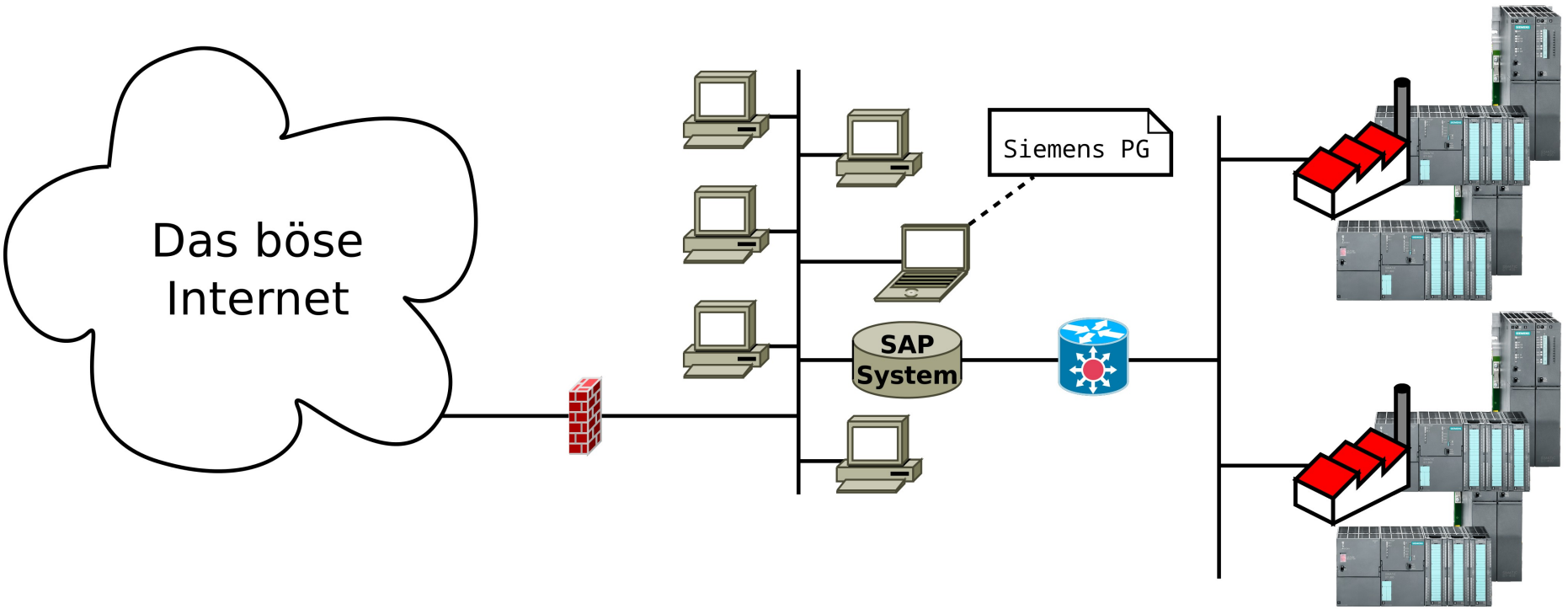
Stuxnet WinCC

- Infektion aller STEP7-Projektdateien:
  - die weniger als 3 Jahre als sind
  - die einen Odner *wincproj* mit gültiger MCP-Datei enthalten
  - außer im Ordner \Step7\Examples
- Ersetzt Datei *s7otbxdx.dll*
  - *Überwachung Schreib-/Lesezugriffe*
  - *Einfügen von SPS-Schadcode*
  - *Verstecken von SPS-Schadcode*

Stuxnet S7-300

- vor Infektion Prüfung verschiedener Eigenschaften
- Drei Varianten:
  - S7-300 mit CPU 315–2
    - Frequenzumrichter von Vacon
    - Frequenzumrichter von Fararo Paya
  - S7-400 mit CPU 417
- Im Abstand von 13 Tagen bis 3 Monaten Veränderung Frequenz (Motordrehzahl)

Aussichten



Quellen

-
- Vulnerability in Windows Shell Could Allow Remote Code Execution http://technet.microsoft.com/en-us/security/bulletin/MS10-046
- Vulnerability in Print Spooler Service Could Allow Remote Code Execution http://technet.microsoft.com/en-us/security/bulletin/MS10-061
- Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege http://technet.microsoft.com/en-us/security/bulletin/MS10-073
- Vulnerability in Task Scheduler Could Allow Elevation of Privilege http://technet.microsoft.com/en-us/security/bulletin/MS10-092
-