Stuxnet – eine Einführung

Thomas Reinhold

reit@hrz.tu-chemnitz.de

Gliederung des Vortrags

- Zum Begriff ”Cyberspace”
- Typen und Klassifikationen von Schadsoftware
- Das Konzept ”SCADA”
- Stuxnet
  - Die wichtigsten Ereignisse
  - Technische Details
  - Infektionen und Auswirkungen
  - Einschätzung

Zum Begriff ”Cyberspace”

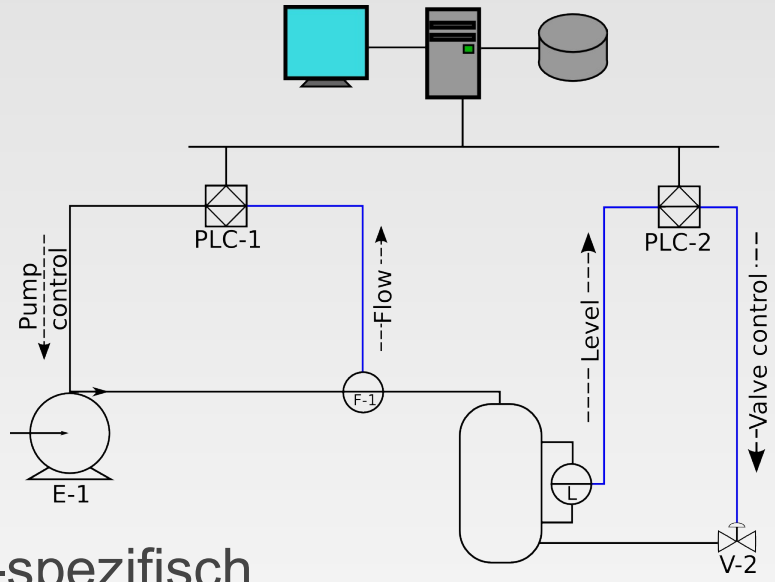
- EU Cybercrime Convention (2001)
  - *By connecting to communication and information services users create a kind of common space, called "cyber-space"*
- Aus Sicht der Hardware
  - Alle vernetzungsfähigen Computersysteme und deren Infrastrukturen
  - Alle Daten der Systeme und deren Austausch
  - Vom Smartphone über Server bis zum Industrierechner

Typen und Klassifikationen von Schadsoftware

- Software mit unerwünschter, ggf. schädlicher Funktion
- Klassifikation nach Verbreitungsart, Schaden, Absicht, Zielsystem, Kontrollmöglichkeiten …
  - Viren — Reproduktion durch Einschleusen in Software
  - Würmer — Aktive Selbstverbreitung über Netzwerkdienste
  - Trojaner — Schadcode verborgen in scheinbar nützlicher Software
  - Botnetze — Verborgene Software auf Rechnern, die über spezifische Kanäle ferngesteuert werden (Command-&-Control-Server)
- Stuxnet: Kombination dieser Technologien

Das Konzept ”SCADA”

- **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition
- Computer-gestützte automatisierte Steuerung komplexer technischer Prozesse
  - PLC – Programmable Logic Controller
  - Regelung technischer Aktoren
  - Auf Basis physischer Sensoren
  - Verwaltet durch einen zentralen Server
  - Aufbau und Konfiguration sehr Anlagen-spezifisch



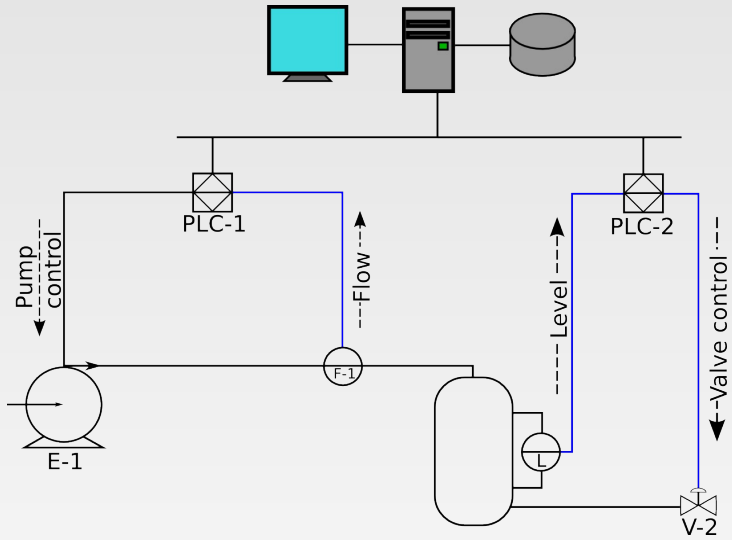
- Stuxnet: Siemens Simatic Step7 System / WinCC

Stuxnet – Die wichtigsten Ereignisse

- 22.6.2009 Älteste bekannte Stuxnet-Version
- 17.6.2010 Stuxnet auf iranischen Systemen entdeckt
- 19.7.2010 Siemens: SCADA-Anlagen betroffen
- 22.9.2010 Iran bestätigt Stuxnet-Infektionen
- 2.11.2010 Siemens: Stuxnet-Kontrollserver sind offline

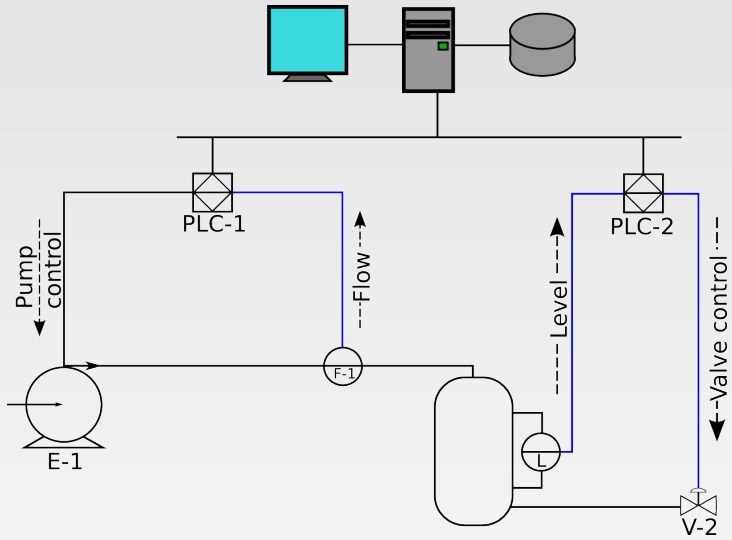
Stuxnet – Details

- Targeted Attack
  - Verbreitung in alle erreichbaren Step7-Systeme
  - Manipulation nur bei spezifischer Systemkonfiguration
  - Gezielte Infiltration einer konkreten Anlage
- Verbreitung und Infektion
  - Per USB Sticks und lokale Netzwerke
  - Fast alle Systeme ab Windows95 betroffen
  - Einsatz von vier Zero Day Exploits
  - Verwendung von zwei gestohlenen digitalen Zertifikaten
  - Externer Informationsaustausch und Software-Updates



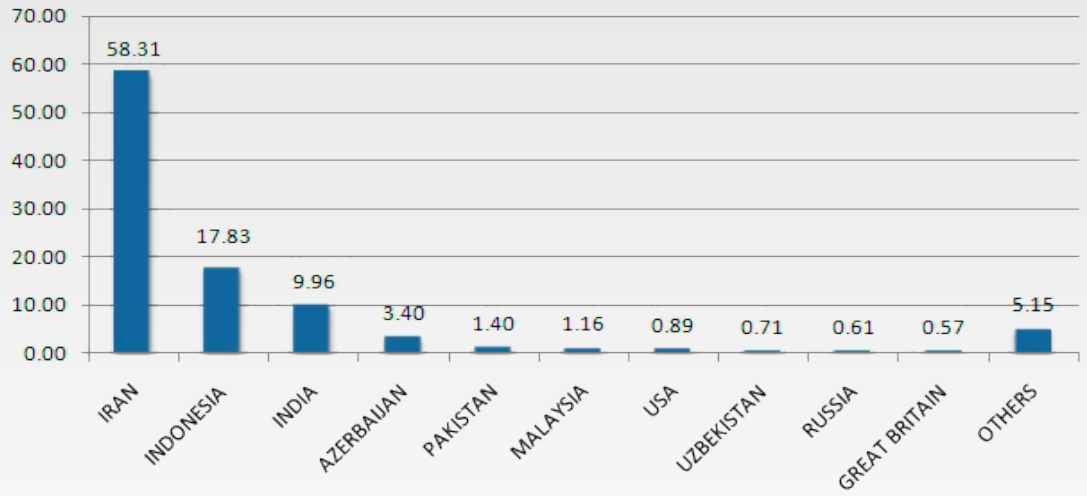
Stuxnet – Details (2)

- Software-Manipulation des spezifischen Systems
  - Step7-Kontrollsoftware (WinCC) als Hauptziel
  - Kommunikation und Steuerung der PLC infiltriert
  - Eigener PLC-Code eingeschleust
  - Manipulation der Sensorvisualisierung
- Hardware-Manipulation
  - Manipulation von Frequenz-Konvertern (für Motoren-Steuerung)
  - Synchronisierte zyklische Fehlsteuerung der Frequenzen



Stuxnet – Infektionen und Auswirkungen

- Infektionen weltweit
  - 3 Infektionswellen ausgehend von 5 iranischen Einrichtungen
  - Insgesamt 100,000 infizierte Systeme (Symantec Dossier)
  - 24 Siemensanlagen (Mitteilung Siemens 11.03.2011)
- Schäden
  - laut Siemens keine an ihren Anlagen
  - Iranische Uranzentrifugen (2009 Natanz, Bushehr)
  - Iranische Ölindustrie



Stuxnet – Einschätzung

- Technische Qualität
  - SCADA als Sicherheitsrisiko mit hohem Gefährdungspotential
  - Kompromitierung digitaler Zertifikate
  - Erfolgreiche Attacke auf abgeschottete Systeme
- Organisatorische Qualität
  - Exakte Kenntnisse über Ziel notwenig
  - Testgelände
  - SCADA Experten und hochklassige Software-Teams beteiligt
  - Millionen-Dollar-Projekt für Technologie und Entwicklung
  - Mehrjähriger Aufwand für eine ”*one shot weapon*” (R. Langner)

Vielen Dank

für Ihre Aufmerksamkeit