Die Waffen des Cyberwar

Thomas Reinhold

reit@hrz.tu-chemnitz.de

Gliederung des Vortrags

- Zum Begriff ”Cyberspace”
- Typen & Klassifikationen von Schadsoftware
- Exemplarisch: Stuxnet & Duqu
- Cybercrime & Cyberwar
- Das Attributionsproblem
- Der Aufwand eines Cyberkrieges

Zum Begriff ”Cyberspace”

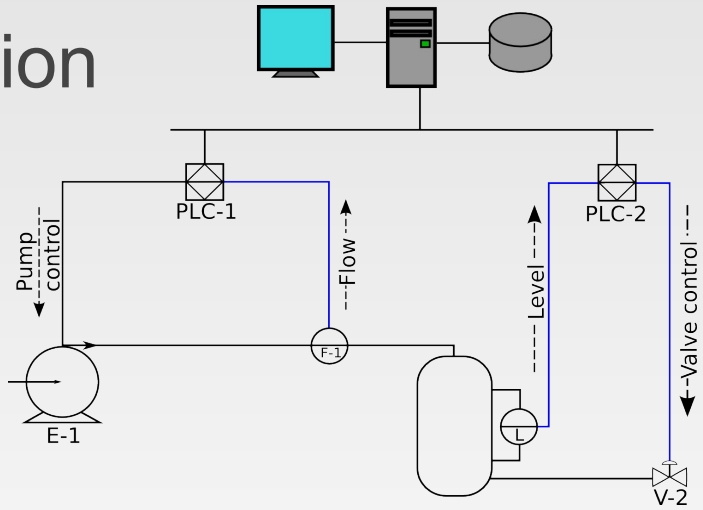
- EU Cybercrime Convention (2001)
  - *By connecting to communication and information services users create a kind of common space, called "cyber-space"*
- Aus Sicht der Hardware
  - Alle vernetzungsfähigen Computersysteme und deren Infrastrukturen
  - Alle Daten der Systeme und deren Austausch
  - Vom 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)
- => jeder Typ hat seine spezifischen Grenzen

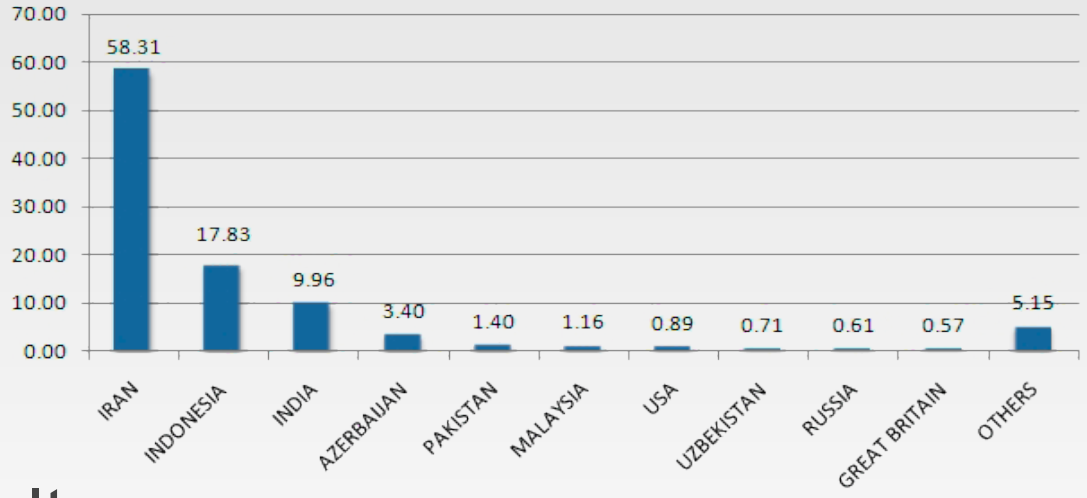
Stuxnet & Duqu

- Juni.09 – Nov.10 auf iranischen Siemens-Systemen
- SCADA = Supervisory Control and Data Acquisition
  Computer-gestützte automatisierte Steuerung komplexer Prozesse
- Targeted Attack: gezielte Manipulation einer konkreten Anlage
- Verbreitung und Infektion
  - Per USB Sticks und lokale Netzwerke
  - ab Windows95 aufwärts anfällig
  - Externer Informationsaustausch und Software-Updates



Stuxnet & Duqu (2)

- Stuxnet weltweit 3 Infektionswellen
- ca. 100,000 infizierte Systeme & 24 Siemens-Anlagen
- Schäden an iran. Uranzentrifugen (Natanz, Bushehr)
- Sept. 2011 ”Duqu”
- einfachere Version zur Vorfeldaufklärung
- vermutlich mit gleicher Software-Basis entwickelt



Cybercrime & Cyberwar

- Abgrenzung Krieg und Kriminalität/Spionage nötig
- Cyberspace neue Domäne des Krieges
- Typische Cyerattacken setzten Technologie außer Kraft, sind aber nicht auf deren Zerstörung ausgerichtet
- Probleme durch Verwendung des Kriegsbegriff
  - Selbstläuftertum von Angaben und Zahlen
  - Wahrgenommene Bedrohungspotentiale
  - Implikation bzgl. angemessener Reaktionen

Das Attributions-Problem

- ”Cyberattacken sind nicht ausreichend gezielt zuordbar und damit für Angreifer ohne negative Konsequenzen”
- Zuordnung wäre unmöglich wenn
  - verwendete Techniken einmalig und unbekannt
  - Angreifer komplett abgeschottet und anonym arbeiten
  - Motivation nicht durch politische Lage Rücksschlüsse zuläßt
  - Angreifer sehr zeitnah und schnell agiert

Das Attributions-Problem (2)

- Aber Angreifer hinterlassen Spuren:
  - Verwendung bekannter Technologien
  - Online-Identitäten/Login-Daten/Accounts/IP-Adressen
  - Command & Control-Server bleiben online
  - Verzögerte Reaktionszeiten
  - Politische Schlußfolgerungen
- Angemessene Reaktion auch ohne 100% Zuordbarkeit
- Definition des Angreifers eine politische Entscheidung

Der Aufwand eines Cyberkrieges

- Anforderungen für einen erfolgreichen Cyberkrieg
  - Sehr klares und genaues Missionsziel und entspr. Erlaubnisse
  - Spezifische Zielinformationen, i.a.R. Vorfeldaufklärung nötig
  - Unbekannte Sicherheitslücken (0day exploits)
  - Hochgradig professionelles Entwicklungs/Test/Angriffs-Team
  - Beständkeit des Angriffes in Qualität und Dauer
- Zeitpunkt des 1. Angriffs → Vorteil beim Verteidiger
- ~ Lebensspanne einer entdeckten Lücke: 500 Stunden
- Entwicklungsaufwand eines Angriffs ca. 2 bis 5 Jahre

Vielen Dank

für Ihre Aufmerksamkeit