FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Pentests für industrielle Steuerungen

Peter Schwanke

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Pentest - Überblick

- Penetrationstest: Sicherheitsüberprüfung
- Perspektive eines Angreifers
- Ziele:
  - Identifikation von Schwachstellen
  - Erhöhung der Sicherheit
  - Bestätigung der IT-Sicherheit
- Durchführung kann erfolgreichen Angriff nicht ausschließen
- reduziert Wahrscheinlichkeit für erfolgreichen Angriff

Pentesting

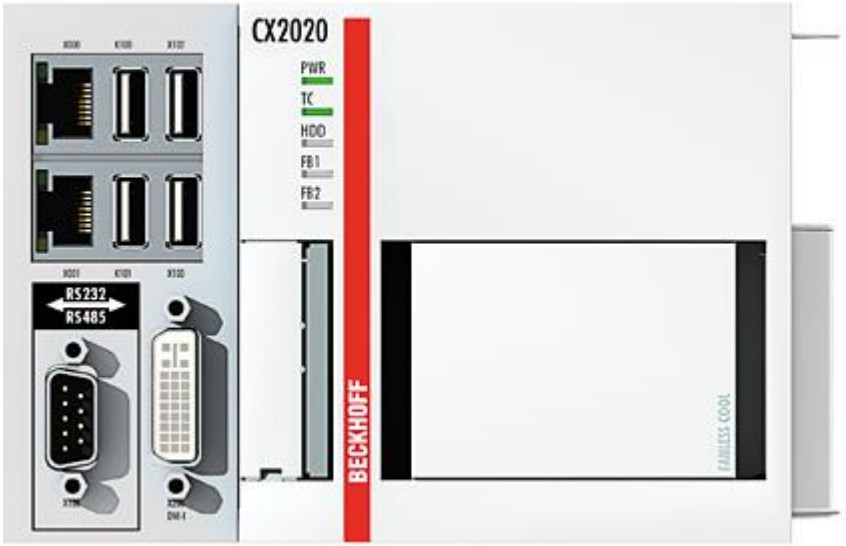
- Bekannte Vorgehensweise:
  - Pentesting unter realen Bedingungen:
    - praxisnah
    - Keine/wenig Manipulation an aktueller Konfiguration
- Probleme:
  - Zu testende Geräte evtl. „lebenswichtig“
  - Ausfall möglich, aber nicht tolerierbar
- Mögliche Alternativen:
  - Pentest an einem losgelösten Gerät
  - Pentest an einem virtualisierten Gerät

Motivation

- Industrie 4.0
- Angriffe auf kritische Infrastrukturen nehmen zu
- IT-Sicherheitsgesetz:
  - Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

Vorgehen

- Virtualisierung bestehender ICS
- Beispiel:
  - Virtualisierung einer Beckhoff CX2020
  - Sicherheitsüberprüfung an der virtuellen Maschine



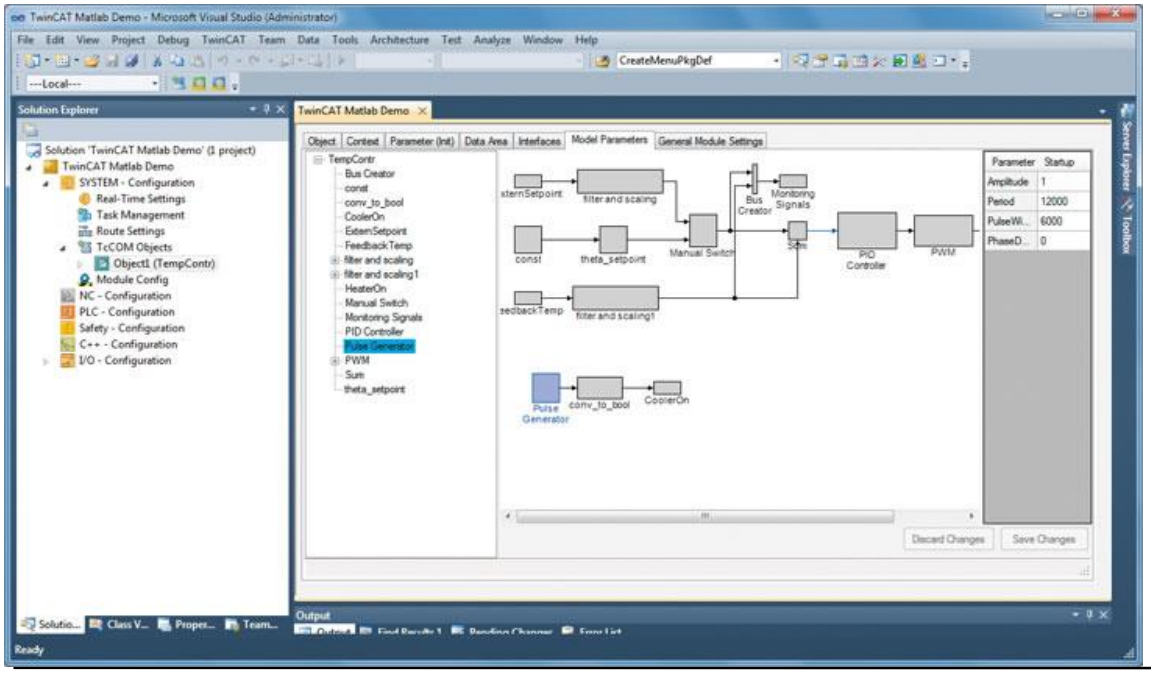
Bestandteile

- Windows Embedded Standard 7
- Webserver
- TwinCAT

TwinCAT

The Windows Control and Automation Technology

- Echtzeit-Steuerung
- Autorisierte Benutzer
- Verschlüsselter Login



Erste Ergebnisse

- Responsible disclosure

Schwachstellen

- Bruteforce:
  - Beliebig viele Login-Versuche möglich
- Replay:
- DoS:
  - Kommunikation mit Anlage kann gestört werden
  - Anlage kann zum Absturz gebracht werden
- Spoofing:
  - Angreifer kann sich als Beckhoff-Gerät ausgeben

Schwachstellen

- Verschlüsselung:
  - Angreifer kann Credentials entschlüsseln
- Authentisierung:
  - Kann umgangen werden

Ausblick

- Weitere Schwachstellen?
- IT-Forensik: Spuren?
- Bewertung (CVSS)

Fragen?