

Konzept zur Sicherheitsüberprüfung von Industrial Control Systems

Denise Uerlings

Lehrgebiet Datennetze, IT-Sicherheit
und IT-Forensik

- Thema der Bachelorthesis
- Problemstellung
- Vorgehensweise
- Erste Ergebnisse

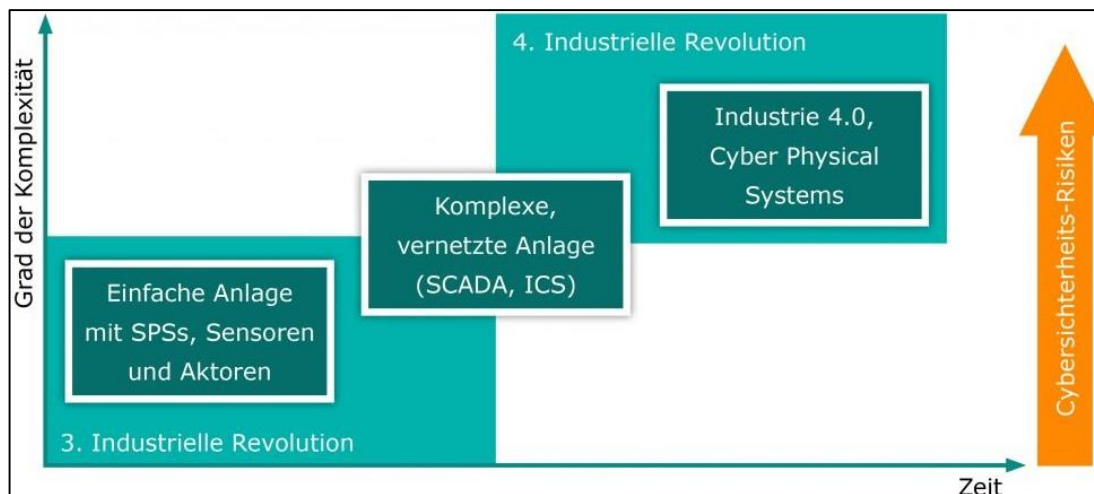
- Vergleich Office-IT und industriellen Penetrationstests
- Abweichende Ausgangslage in der Industrie
 - Dauerbetrieb der Systeme
 - Vermeidung von Ausfallzeiten
 - Sensible Systeme: empfindlich gegenüber Scans



- Unterschiede der Vorgehensweisen
- Konzeptentwicklung für Penetrationstests von industriellen Steuerungssystemen (ICS)



- Industrielle Steuerungssysteme:
 - messen, steuern und regeln Abläufe in produzierender Industrie
 - früher: von anderen IT-Systemen & Netzen entkoppelt
 - heute: fortschreitende Vernetzung von ICS-Systemen mit klassischer Office-IT (Industrie 4.0)
 - Mehr Gefährdungen für Systeme



- Angriffe auf kritische Infrastrukturen
 - Gefährdung der Grundversorgung der Bevölkerung

- Angriffe auf produzierende Industrie
 - wirtschaftliche Schäden, Imageschäden, Umweltschäden, Menschenleben

- Fazit:

Überprüfung und Sicherheit von industriellen Anlagen spielt eine große und wichtige Rolle!

- Begleitung und Durchführung von Office-IT Pentests
- Begleitung und Durchführung von Pentests im industriellen Umfeld
- Recherche/Austausch mit Unternehmen

- Ziel: maximale Pentest Ergebnisse bei minimalem Risiko für Anlagenverfügbarkeit
- Einige Tools von Office-IT Pentest auch bei OT* Pentests einsetzbar aber in Funktionen beschränken
- Grundsätzlich: keine Pentests im produktiven Betrieb außer explizit gewünscht
 - Gilt auch für Forensik
- Unterschiedliches Vorgehen im produktiven und nicht produktiven Betrieb

OT = Operational Technology

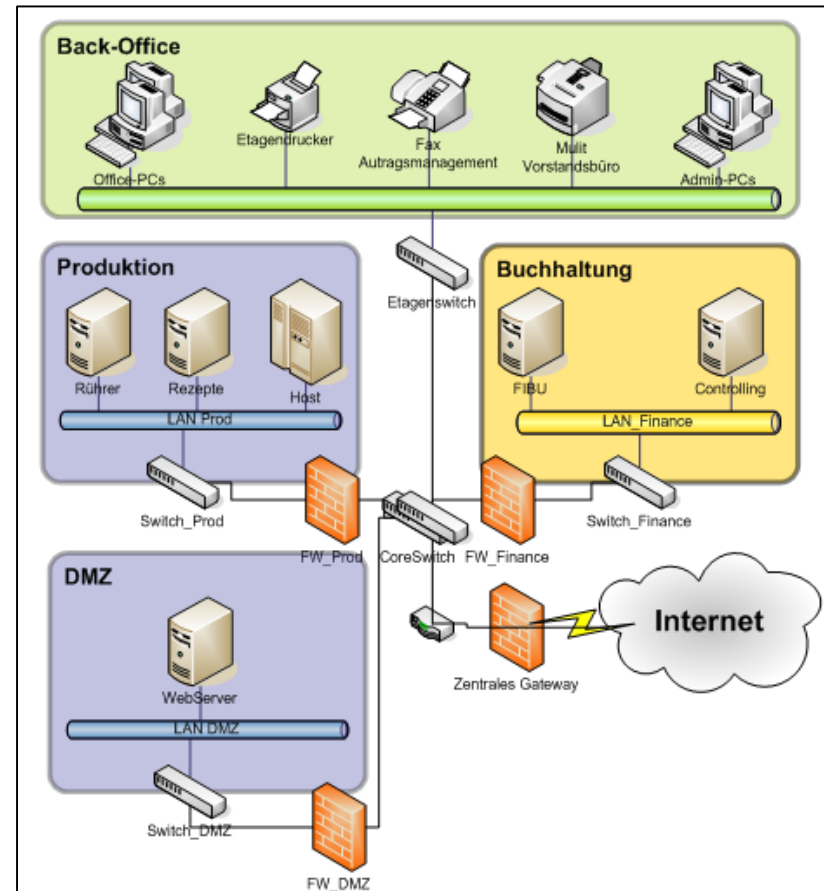
Hard- und Software, mit denen Leistungen physischer Geräte, Maschinen, Anlagen überwacht, kontrolliert und gesteuert werden

Pentests im nicht produktiven Betrieb:

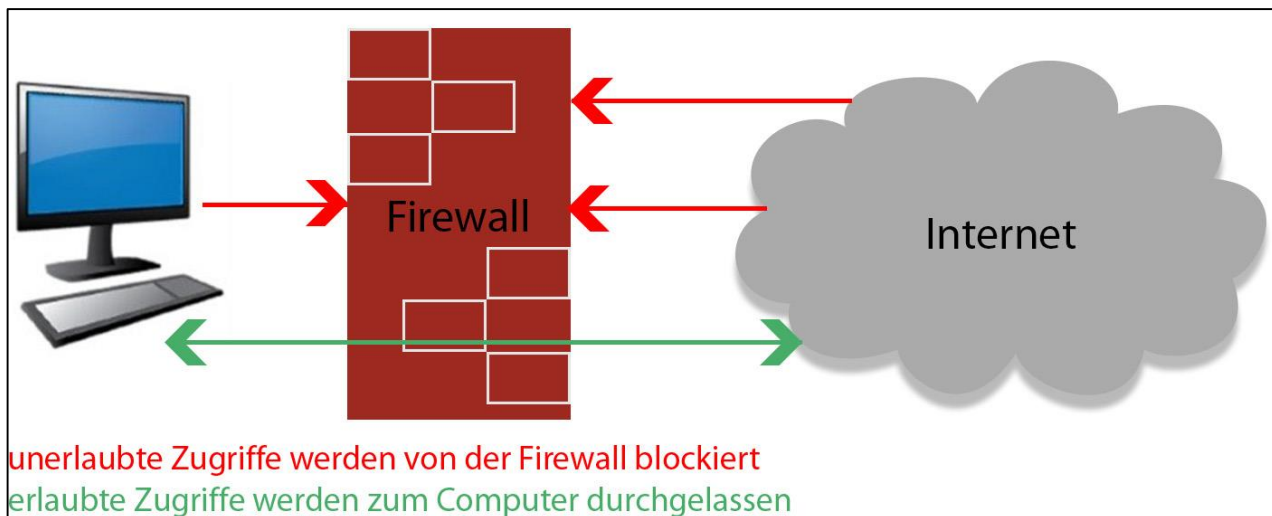
- Testen während Wartungsintervallen
- Pentests in Test- oder Standbyumgebung
- Clonen und Pentesten einzelner Systeme für Testzwecke z.B.
 - einzelne PCs
 - Steuerungskomponenten
 - Netzwerkkomponenten inkl. der realen Konfiguration



- Theoretische Analyse der Architektur
→ Dokumentation
 - Welche Systeme haben welche Funktion
 - Konfiguration der Systeme
 - Was sind potentielle Angriffsvektoren
 - Wie kommt man weiter im System/Netz



- Dokumentation überprüfen
 - z.B. Anlagen ablaufen
 - stimmt Dokumentation mit Realität überein
- Netzwerksegmentierung/Firewall-Regeln
 - sind Firewall-Regelwerke von IT und OT aufeinander abgestimmt



Pentests im produktiven Betrieb:

- Testen mit **äußerster Vorsicht**
- Genaue Absprache mit Kunden
 - Miteinbeziehung der Kunden in Testvorgehen
 - z.B. Risikobetrachtung zusammen mit Kunden



- Überprüfung der Netzübergänge
 - Absicherung der Systeme nach außen
 - Fokus auf Systeme die Schnittstelle zum Office Netzwerk & dadurch Richtung Internet verfügbar sind (z.B. HMI – Windows Rechner mit WinCC)

- Passive Tools (Sniffen des Datenverkehrs)

No.	Time	Source	Destination	Protocol	Length	Info
12	2.578896	192.168.171.139	192.168.171.182	TCP	74	37993->502 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=30585128 TSecr=19061183
13	2.579125	192.168.171.182	192.168.171.139	TCP	74	502->37993 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=19061183 TSecr=30585128
14	2.579305	192.168.171.139	192.168.171.182	TCP	66	37993->502 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=30585126 TSecr=19061183
15	2.579500	192.168.171.182	192.168.171.139	Modbus/TCP	12	Transaction ID: 64795, Protocol ID: 0, Length: 6, Unit ID: 1
16	2.579680	192.168.171.182	192.168.171.139	TCP	66	502->37993 [ACK] Seq=1 Ack=13 Win=29056 Len=0 TSval=19061180 TSecr=30585128
17	2.587010	192.168.171.182	192.168.171.139	Modbus/TCP	78	Response: Trans: 64795; Unit: 1, Func: 6: Write Single Register
18	2.587334	192.168.171.139	192.168.171.182	TCP	66	37993->502 [ACK] Seq=13 Ack=13 Win=29312 Len=0 TSval=30585127 TSecr=19061183
19	2.587749	192.168.171.139	192.168.171.182	TCP	66	37993->502 [FIN, ACK] Seq=13 Ack=13 Win=29312 Len=0 TSval=30585128 TSecr=19061183
26	2.591935	192.168.171.182	192.168.171.139	TCP	66	502->37993 [FIN, ACK] Seq=13 Ack=14 Win=29056 Len=0 TSval=19061183 TSecr=30585129
27	2.592284	192.168.171.182	192.168.171.182	TCP	66	37993->502 [ACK] Seq=14 Ack=14 Win=29312 Len=0 TSval=30585129 TSecr=19061183

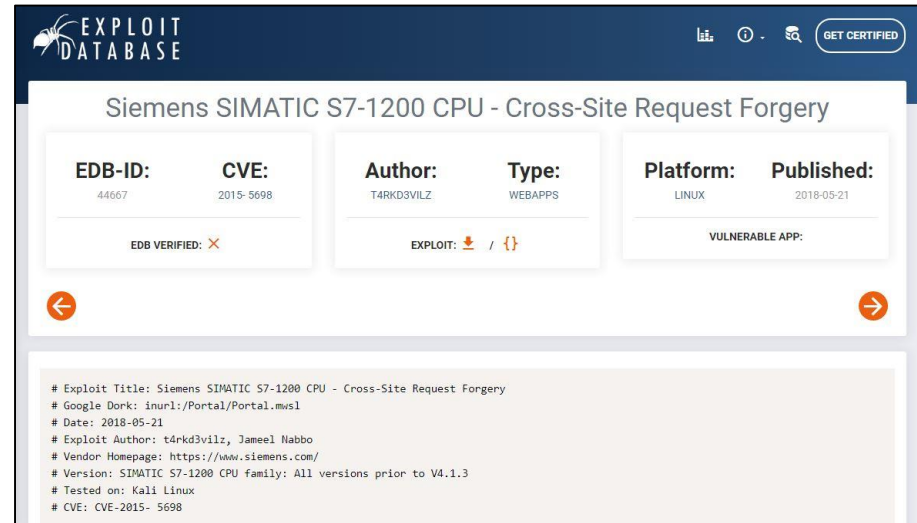

```

Frame 15: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0
Ethernet II, Src: Vmware_e1:12:81 (00:0c:29:e1:12:81), Dst: Vmware_c3:29:82 (00:0c:29:c3:29:82)
Internet Protocol Version 4, Src: 192.168.171.139 (192.168.171.139), Dst: 192.168.171.182 (192.168.171.182)
Transmission Control Protocol, Src Port: 37993 (37993), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 12
Modbus/TCP
  Transaction Identifier: 64795
  Protocol Identifier: 0
  Length: 6
  Unit Identifier: 1
Modbus
  Function Code: Write Single Register (6)
  Reference Number: 8
  Data: 014d
    
```

Beispiel eines Wireshark Mitschnitts

**HMI = Human
Machine Interface**

- Enumeration (z.B. nmap) mit angepasster Paketrate bzw. Geschwindigkeit verwenden
 - einzelne Systeme/Dienste priorisieren
 - Testen einzelner Dienste ohne Ausnutzung von Schwachstellen die Verfügbarkeit beeinflussen
 - keine automatisierten Schwachstellen Scans
 - vorsichtige Port Scans
 - Exploits im Netz frei verfügbar?
 - Logindaten von Diensten auf Standard-Anmeldeinformationen überprüfen



EXPLOIT DATABASE GET CERTIFIED

Siemens SIMATIC S7-1200 CPU - Cross-Site Request Forgery

EDB-ID:	CVE:	Author:	Type:	Platform:	Published:
44667	2015-5698	T4RKD3VILZ	WEBAPPS	LINUX	2018-05-21

EDB VERIFIED: ✗ EXPLOIT: 📄 / {} VULNERABLE APP:

```
# Exploit Title: Siemens SIMATIC S7-1200 CPU - Cross-Site Request Forgery
# Google Dork: inurl:/Portal/Portal.mvs1
# Date: 2018-05-21
# Exploit Author: t4rkd3vilz, Jameel Nabbo
# Vendor Homepage: https://www.siemens.com/
# Version: SIMATIC S7-1200 CPU family: All versions prior to V4.1.3
# Tested on: Kali Linux
# CVE: CVE-2015- 5698
```

Vielen Dank für Ihre
Aufmerksamkeit!