Peter Schwanke

Angriffe und IT-Forensik im industriellen Umfeld

Firmenportrait

- Juni 2002 gegründet
- Sitz: Leichlingen/Rheinland
- Beratungsschwerpunkte
  - IT-Risikomanagement
  - IT-Outsourcing/Cloud
  - Security Awareness
- Zielgruppe:
  - Mittelständische bis große Organisationen und Unternehmen

IT-RESULTING IM FOKUS

Industrial Security

Industrie 4.0 und IT- Sicherheit

- Ohne IT keine Produktion mehr möglich
- Vernetzung in der Produktion allgegenwärtig
- Vernetzung zwischen Produktions-IT und Office-IT nimmt rasant zu
- Öffnung der Produktions-IT zum Internet ist nicht mehr verhinderbar

Die Kernprobleme

Kernprobleme Produktion

- sehr lange Lebenszyklen der Anlagen
  - Vorhandensein „veralteter“ Technologien
    - und meist keine Chance des Austauschs
- Steuerungen sind leicht manipulierbar
- die Anzahl der manipulierbaren Komponenten ist extrem hoch
- die Komplexität ist enorm

Kernprobleme Produktion

- Steuerungen
  - jeder Hersteller hat eigene „Standards“
  - grundsätzlich sind alle leicht manipulierbar und angreifbar
- Sicherheit hat lange keine große Rolle gespielt
  - ein Grund: das lange „Inselleben“, daher:
    - kein spezifisches Sicherheitsmanagement
    - keine spezifischen Sicherheitskonzepte
      - spezifische Sicherheitspatches meist nicht vorhanden
  - Patches dürfen selber oft nicht eingespielt werden
    - es drohen Verlust von
      - Zulassung
      - Gewährleistung
      - Verfügbarkeit der Anlage etc.

Folgen

- die Bedrohungen der Office IT kommen der Fertigung sehr nahe
- Produktionsausfälle durch Sabotage oder „einfache“ Störungen nehmen zu
- Verlust von wertvollem Firmen Know-How
  - Produktionspläne und Prozesssteuerungen

Beispiele aus der Praxis

Ransomware - WannaCry

- Erpressungstrojaner für Windows Systeme
- Vermutlich über 200.000 Infektionen
- Bekannte Vorfälle aus der Office IT
- Schäden in Milliardenhöhe
  - mehr als 50 Bitcoin überwiesen
  - Hohe Dunkelziffer

Auch Infektionen auf industriellen Steuerungen!

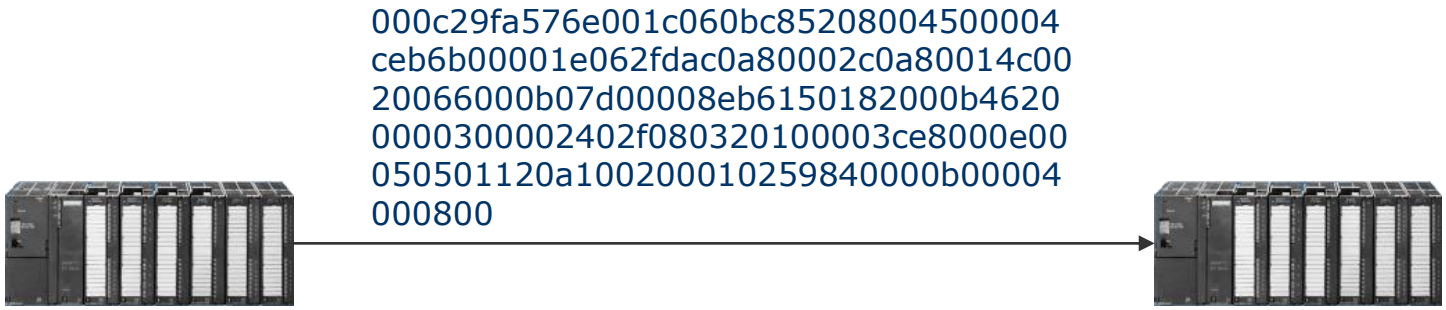
Angriffe bemerken

- Erkennung bei WannaCry einfach:
  - Funktion ist eingeschränkt (Denial of Service)
  - WannaCry will bemerkt werden

- Andere Angriffsformen
  - Möglicherweise kaum zu erkennen
  - Beispiel: Stuxnet – Jahrelang unentdeckt

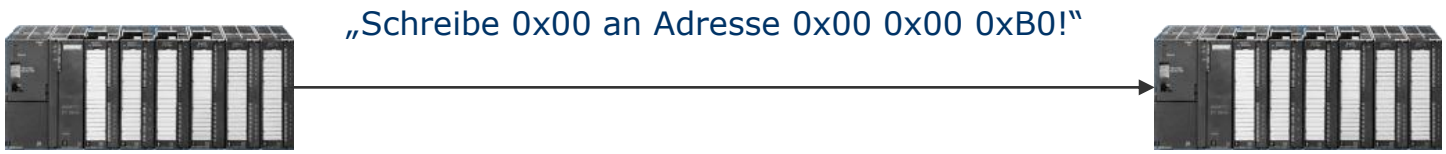
Beispiel: Siemens

- Einsatz von proprietären Protokollen
- S7 Communication
  - 1994 veröffentlicht
  - Heute noch sehr verbreitet



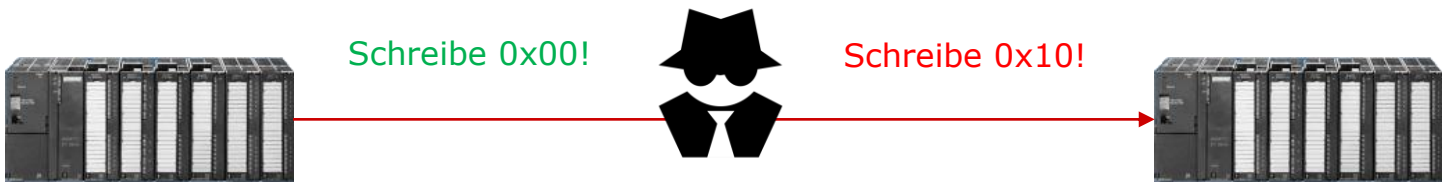
Beispiel: Siemens

- Einsatz von proprietären Protokollen
- S7 Communication
  - 1994 veröffentlicht
  - Heute noch sehr verbreitet
  - Protokollstruktur bekannt



Beispiel: Siemens

- Einsatz von proprietären Protokollen
- S7 Communication
  - 1994 veröffentlicht
  - Heute noch sehr verbreitet
  - Protokollstruktur bekannt
  - Angreifer kann Wissen nutzen

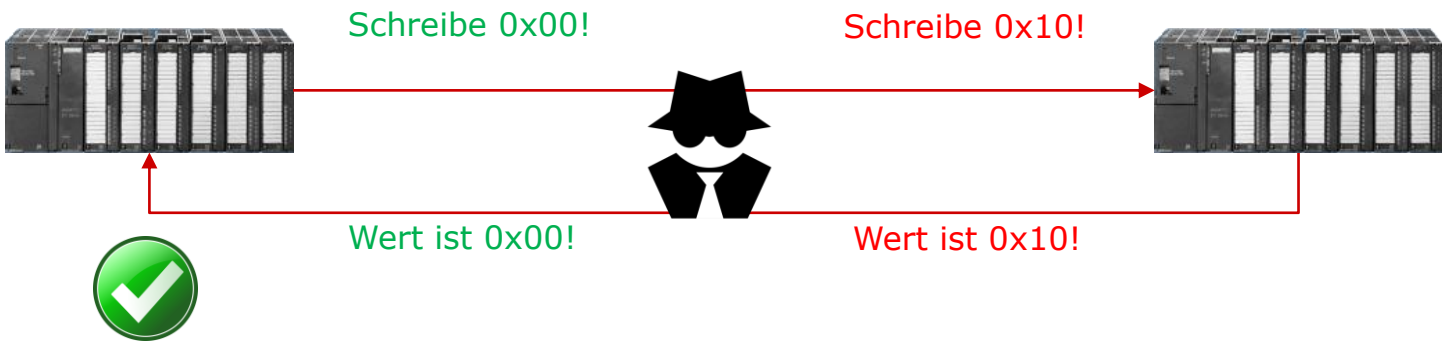


Beispiel: Siemens

- Einsatz von proprietären Protokollen
- S7 Communication
  - 1994 veröffentlicht
  - Heute noch sehr verbreitet
  - Protokollstruktur bekannt
  - Angreifer kann Wissen nutzen

Beispiel: Siemens

- Einsatz von proprietären Protokollen
- S7 Communication
  - 1994 veröffentlicht
  - Heute noch sehr verbreitet
  - Protokollstruktur bekannt
  - Angreifer kann Wissen nutzen



Forensische Untersuchung

- Forensische Methoden im industriellen Umfeld schwierig
- Geräte besitzen:
  - Spezielle Hardware
    - Ausbau einzelner Komponenten (Datenträger, Arbeitsspeicher, etc.) nicht vorgesehen
    - Daten können nicht extrahiert werden
  - Spezielle Software
    - Teilweise proprietäre Betriebssysteme
    - Write Filter (UWF, EWF, FBWF)
      - Daten werden nicht persistent geschrieben
      - Post-Mortem-Analyse somit evtl. überflüssig
      - Vorteil: System nach Neustart wieder Einsatzbereit

Forensic Readiness in der Fertigung

- Monitoring in Prozesse integrieren
  - Feingranular
  - Problem: riesige Datenmengen
- Intelligente Systeme nötig
  - Anomalie-Erkennung
- Intrusion Detection

Vielen Dank für Ihre Aufmerksamkeit!

Ihre Fragen bitte …

Peter Schwanke
peter.schwanke@add-yet.de