Angriff auf die Leittechnik – Stuxnet und die Konsequenzen

ComConsult IT-Sicherheitsforum 2011
23.05.2011

Dr. Stephan Beirer
s.beirer@gai-netconsult.de

Am Borsigturm 58, 13507 Berlin

Tel / Fax: +49 30 417898-0/-300
E-Mail: info@gai-netconsult.de
Web: www.gai-netconsult.de

GAI NetConsult GmbH

- Gegründet 1994
- 30 Mitarbeiter (Stand 05/2011)
- Standort Berlin
- Bundesweiter Kundenstamm vom Mittelstand bis zu Großkonzernen
- Bereich „Informationssicherheit“ mit den Schwerpunkten Sicherheitsprüfung und Consulting / Konzeption
- Bereich „Entwicklung & Integration“ mit der Erstellung sicherer eBusiness-Anwendungen
- Wichtige Branchenschwerpunkte…
  - Energieversorger, Finanzdienstleister
  - Gesundheitswesen, Chemie, Pharma, …
- PR-Aktivitäten…
  - Kostenfreies Periodical: Security *Journal*

Dienstleistungen der GAI NetConsult im Leittechnik-Umfeld

- Sicherheitsorganisation
  - Aufbau von Sicherheits-Managementsystemen (ISMS)
  - Konzepte zur Betriebsorganisation
  - Erstellung von Sicherheitsrichtlinien und Standards
  - IT-Notfallplanung
- Sicherheitskonzeption
  - Beratung zu Sicherheitsfragen beim Systemdesign
  - Unterstützung bei Ausschreibungen und Lasten/Pflichtenhefterstellung
  - Technische Sicherheitsmaßnahmen auf Systemebene
  - Konzeption sicherer Netzwerke und Schnittstellen
  - Evaluierung, Auswahl und Einführung von Sicherheitsprodukten
- Audits und Sicherheits-Reviews
  - Technische Überprüfungen von Systemen und Komponenten, z.B. Abnahmeprüfungen
  - Organisatorische Audits auf Basis anerkannter Standards wie ISO 27001/27002

Angriff auf die Leittechnik – Stuxnet und die Konsequenzen

- **Rückblick:**
  - **Funktionsweise und Schadfunktion des Stuxnet-Wurms**
- Derzeitiger Stand
  - Systeme gepatcht - Lücken geschlossen?
  - Aktuelle Schwachstellen in der Prozessleittechnik
  - Gefährdung durch Nachahmungstäter
- Ausblick
  - Konsequenzen und Anforderungen an Leittechnik-Betreiber und Hersteller

Kurzer Rückblick – Sommer 2010

- 17.06.2010: Das russische Antivirus-Unternehmen VirusBlokAda entdeckt auf den Rechnern eines iranischen Kunden eine bisher unbekannte Schadsoftware, die sich über USB-Sticks verbreitet.

- 14./15.07.2010: Nähere Analysen des Virusspezialisten Frank Boldewin zeigen, dass die Schadsodsoftware offenbar gezielt Siemens WinCC/PCS7-Prozessleittechnik angreift.

- Es werden weiterführende Angriffe befürchtet. Betreiber kritischer Infrastrukturen werden umgehend durch die Behörden alarmiert.

- Inzwischen spricht sehr viel dafür, dass der Angriff gezielt auf die Zentrifugen-kaskaden der iranischen Urananreicherungsanlage Natanz ausgerichtet war.

Hintergrund – SIMATIC PCS7

- SIMATIC PCS7 ist eine Automatisierungs- und Prozessleittechnik von Siemens zur Steuerung und Überwachung von verfahrenstechnischen und Produktions-Prozessen.

- SIMATIC PCS7 wird weltweit in zahlreichen Branchen eingesetzt:
  - Gas- und Erdölindustrie
  - Chemie und Pharma
  - Nahrungs- und Genussmittel
  - Energieerzeugung, Kraftwerke

- Wie in allen modernen Prozessleitsystemen werden in PCS7 Standard-IT-Technologien eingesetzt.

Aufbau eines typischen PCS7-Leitsystems

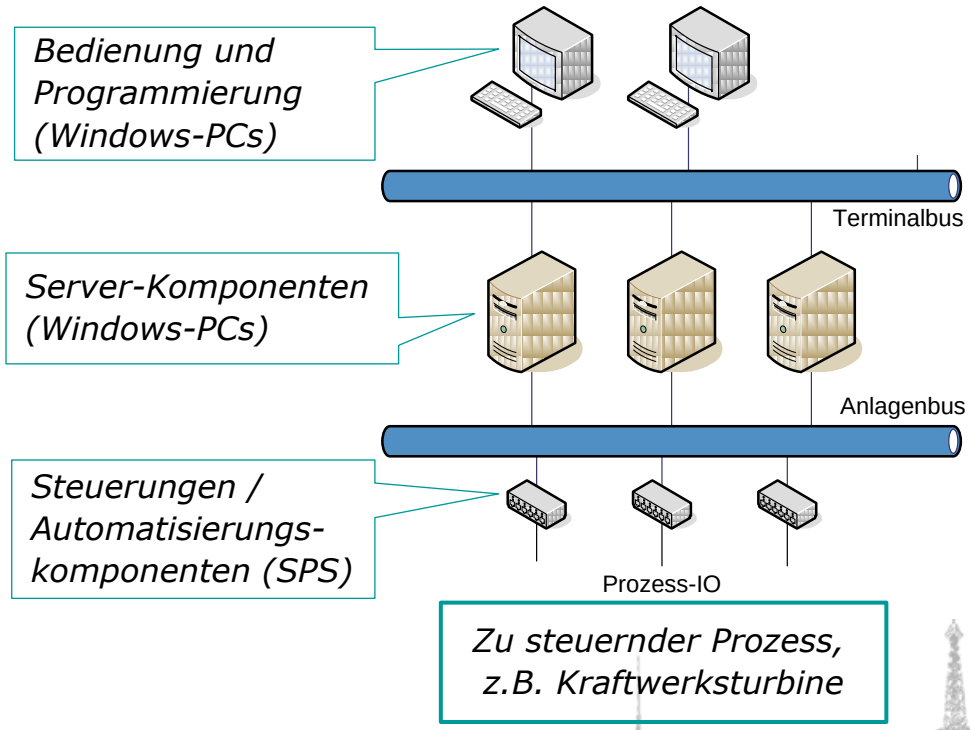
- Der physikalische Prozess wird durch eine S7-Automatisierungs-komponente bzw. SPS (Speicher-programmierbare Steuerung) überwacht (Eingänge - Sensoren) und geregelt (Ausgänge - Aktoren).

Quelle: Wikimedia, U. Ziegenfuss

- Das PCS7-Leitsystem dient zur übergeordneten Führung der gesamten Anlage.

- Das Leitsystem basiert auf Microsoft Windows-Komponenten; die SPSen auf einer proprietären Siemens-Firmware.

- Die Kommunikation erfolgt i.d.R. über IP- und Ethernet-basierte Protokolle.

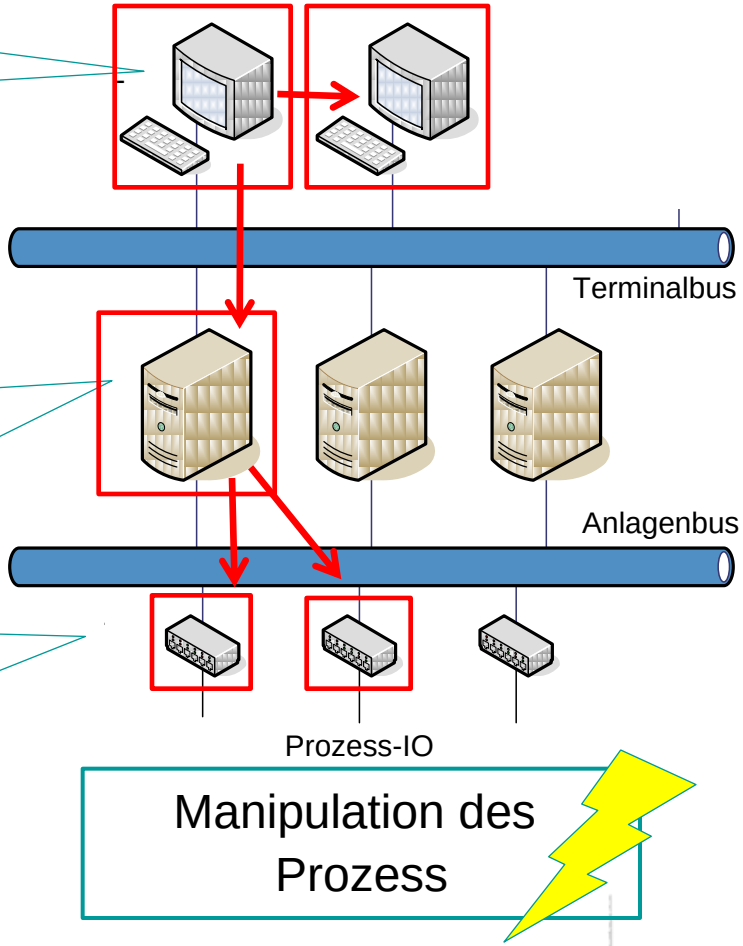


Ablauf einer typischen Infektion

Infektion, z.B. über USB-Stick
(Ausnutzung Windows-Lücken)

Automatische Verbreitung auf
weitere Leitsystem-Komponenten,
z.B. über das interne Netzwerk
(Ausnutzung PCS7-Lücken)

Umprogrammierung der
Steuerungen
(Ausnutzung SPS-Lücken)



Ausgenutzte Schwachstellen auf Windows-Ebene

- Stuxnet nutzt für die Verbreitung und Infektion sieben verschiedene Windows-Sicherheitslücken. Davon waren vier bis zur Entdeckung des Wurms nicht bekannt („Zero-Day Exploits").

- Als primäres Einfallstor nutzt er eine Schwachstelle in der automatischen Verarbeitung von LNK-Dateien, um sich über USB-Sticks und Netzwerk-Laufwerke zu verbreiten.
- Hierdurch kann er auch vom Netzwerk isolierte Leitsysteme befallen, sobald an eine PC-Komponente ein USB-Stick angeschlossen wird.
- Die gängige Schutzmaßnahme „Firewall" wird somit vollständig ausgehebelt.

- Durch verschiedene Privilegien-Eskalations-Schwachstellen verschafft er sich auf dem infizierten System Administrator bzw. Systemrechte.

Ausgenutzte Schwachstellen auf Windows-Ebene

- Zur Verbreitung im lokalen Netzwerk werden verschiedene Lücken in den Implementierungen von SMB und des Druckerspoolers ausgenutzt.

- Stuxnet installiert sich mit einem gültigen Hersteller-Zertifikat im System. Dem Betriebssystem wird so vorgegaukelt, der Wurm sei ein Kernel-Treiber.
- Hierdurch werden die Schutzmechanismen moderner Windowsbetriebssysteme effektiv ausgehebelt.
- Die hierfür nötigen Zertifikate wurden vermutlich gezielt gestohlen.

- Mittels „Rootkit"-Technologien wird das Betriebssystem manipuliert, so dass der Stuxnet-Wurm verborgen bleibt und eine Infektion auch durch einen Virenschutz nicht festzustellen war.
- Dies ist mit ein Grund, warum der Wurm ca. 1 Jahr unentdeckt blieb (Erstinfektion vmtl. im Juni 2009)!

Ausgenutzte Schwachstellen auf PCS7-Ebene

- Stuxnet sucht gezielt nach Siemens WinCC-/PCS7-Systemen, um diese zu kompromittieren.
- Hierzu nutzt er neben Windows-Lücken auch verschiedene Sicherheitslücken innerhalb des PCS7-Systems:
  - Fest einprogrammierte Standard-Passworte in der in PCS7 integrierten MSSQL-Datenbank
    - Das Passwort kann durch den Betreiber nicht geändert werden!
  - Unsichere MSSQL-Serverinstallation, u.a.
    - Betrieb der Datenbank mit hohen Rechten (Dienstaccount mit LocalSystem-Rechten)
    - Hoch-privilegierte Datenbanknutzer
    - Unsichere Stored Procedures wie xp_cmdshell
    - Erlaubt das Einfügen eigenen SQL-Codes
  - DLL-Preloading-Lücke in STEP7 Projektierungs-Archiven
    - Step7 = PCS7 Programmier-/Projektierungsumgebung
    - verschieden Lücken erlauben das Einschleusen und Ausführen von Programmcode
    - Hierdurch kann Stuxnet die häufig zwischen den Systemen ausgetauschten Projektdaten infizieren.

Ausgenutzte Schwachstellen auf SPS-Ebene

- Das Ziel des Wurms ist eine Manipulation des physikalischen Prozess.
- Dazu muss er manipulierten Programmcode in die SPSen der Zielanlage laden.
- Auch hierbei werden verschiedene Sicherheitslücken und Designschwächen in den Steuerungseinheiten ausgenutzt:
  - S7 SPSen erlauben einen unauthentisierten Programmierzugriff
    - Bei Netzwerkzugriff ist somit eine Manipulation des Steuerungsprogramms möglich
  - Innerhalb der SPS sind sog. *Code Injection* und *Function Hooking* Angriffe möglich
    - Der Wurm kann hierdurch seinen eigenen Programmcode in die vorhandene Programmierung einschleusen, u.a. durch Manipulation von sog. Funktions- und Organisationsbausteine (FB/OB).
    - Hierdurch werden aus dem PC-Umfeld bekannte Rootkit-Technologien erstmals im SPS-Umfeld angewendet.
  - Das Speicher-Prozessabbild der SPS-Eingänge ist beschreibbar.
    - Der Steuerung wird hierdurch eine verfälschte physikalische Realität vorgegaukelt.
    - Diese Manipulationen sind im Leitsystem auch vom Bediener nicht erkennbar.
    - Die Problematik betrifft insbesondere auch Safety-Funktionen, die inzwischen häufig in die Leittechnik/SPSen integriert sind.

Angriff auf die Leittechnik – Stuxnet und die Konsequenzen

- Rückblick:
  - Funktionsweise und Schadfunktion des Stuxnet-Wurms
- **Derzeitiger Stand**
  - **Systeme gepatcht – Lücken geschlossen?**
  - **Aktuelle Schwachstellen in der Prozessleittechnik**
  - **Gefährdung durch Nachahmungstäter**
- Ausblick
  - Konsequenzen und Anforderungen an Leittechnik-Betreiber und Hersteller

Aktueller Stand 2011

- Der Stuxnet-Wurm wird zuverlässig von Virenschutzsoftware erkannt.
- Die von Stuxnet genutzten Windows-Lücken sind inzwischen alle durch Patches beseitigt.
- Siemens hat ein SIMATIC Security Update herausgegeben.
- Das SIMATIC Security Update verhindert eine Infektion des PCS7-System mit dem Stuxnet-Wurm.

- Aber: Die grundlegenden Sicherheitslücken in der PCS7-Applikation wurden bisher alle nicht behoben:
  - MSSQL Standard-Passworte, unsichere MSSQL-Serverinstallation, Code-Execution über STEP7 Projektdateien
  - Die notwendigen Änderungen sind vermutlich erst in einer umfassend überarbeiteten PCS7-Version realisierbar.
- Ebenso wenig gibt es eine Lösung für die grundlegenden Designschwächen auf Ebene der Steuerungskomponenten:
  - Hier wären fundamentale Änderungen am Systemdesign der Steuerungen notwendig.

Neue Qualität der Angriffsmethodik

- Stuxnet stellt eine völlig neue Qualität von Schadsoftware für den Bereich der Prozessteuerungs- und Leittechnik dar:
  - hochprofessionelle, aufwändig und gezielt erstellte Schadsoftware
  - z.T. erstmalige Anwendung modernster Hackingtechniken
  - erste bekannt gewordene Manipulation von Steuerungskomponenten durch Schadsoftware (und deren Tarnung auf allen Ebenen) mit direkten Auswirkungen auf den Prozess

- Die Stuxnet-Programmierung erforderte sehr detailliertes Insider-Wissen und verursachte einen Aufwand von vielen Mann-Monaten.

- Die Methodik der Angriffe und die – derzeit nicht behebbaren – Lücken im PCS7-System sind nun allerdings öffentlich bekannt!

Gefahr von Nachahmungstätern

- Das Kopieren der Angriffsmethoden durch Nachahmungstäter ist mit erheblich weniger Aufwand und Expertenwissen möglich.

- Insbesondere sind Angriffe, die nur auf eine Störung des Prozesses (Sabotage) abzielen auch ohne Detailkenntnisse der angegriffenen Umgebung durchführbar:
  - Stoppen des SPS-Programms, zufälliges Setzen der Ausgänge
  - Angriffe durch sich selbst replizierende Schadsoftware (Stuxnet 2.0) oder bei direktem Zugriff

- Zukünftig ist eine Zunahme derartiger Vorfälle durch Trittbrettfahrer bzw. Kriminelle zu erwarten.

- Konsequenz: Die Risikoeinschätzung für derartige Bedrohungen für die Prozessleittechnik muss überprüft werden.

Generelle Problematik

- Die aufgezeigten Sicherheitsprobleme betreffen keineswegs nur die SIMATIC-Produkte sondern sind exemplarisch für die gesamte Branche.

- Die Leittechnik anderer Hersteller ist von ähnlichen Lücken betroffen:
  - Produktions- und Fertigungsleittechnik
  - Kraftwerksleittechnik
  - Gebäudeleittechnik
  - Verkehrsleittechnik

- Generell gilt: Das Sicherheitsniveau der in Leittechnik- und Automatisierungs-umgebungen eingesetzten Produkte entspricht häufig immer noch nicht den an diese Systeme gestellten Anforderungen.

Generelle Problemfelder und Ursachen

- Prozessnahe IT-Systeme sind Anlagenbestandteile
  - vom Anlagenhersteller geliefert
  - IT-Sicherheit häufig kein Design-Ziel, mangelndes Sicherheitsbewusstsein der Hersteller
  - beim Betreiber oft kein Detailwissen über genutzte IT-Technologien vorhanden
- Systeme haben andere Zeithorizonte
  - Nutzungszeiträume 10 - 25 Jahre
  - lange Entwicklungszyklen
- Ursprünglich vorhandene Isolation der Prozess- und Steuerungsnetze ist inzwischen de facto nicht mehr vorhanden
  - Vernetzung mit der Bürowelt („Datenintegration“)
  - Notwendiger Datenaustausch mit anderen Unternehmen oder Behörden
  - Fernwartung durch Hersteller, Dienstleister oder eigenes Personal
- Patch- und Updatemanagement
  - Aufgrund der Kritikalität der Systeme ist regelmäßiges Patchen meist nicht möglich.
  - Häufig keine Herstellerunterstützung für Patchprozess
  - Erheblicher Ressourcen- und Testaufwand auf Betreiberseite
  - Auch in Neu-Anlagen sind zeitnahe Updates nicht realistisch

Generelle Problemfelder und Ursachen

- Unsichere Netzwerkstruktur
  - Netzwerk-Design berücksichtigt häufig nur reine Verfügbarkeitsaspekte
  - Keine oder unzureichende Segmentierung: Störungen können sich ungehindert ausbreiten
- Unsichere Netzwerk-Protokolle
  - Heutige Industrieprotokolle übertragen das Konzept isolierter Feldbusse auf die vernetzte Ethernet-Welt → Deshalb sind meist keinerlei Sicherheitsmechanismen vorhanden.
  - Fehlende Authentisierung und Autorisierung: Schalten, Setzen von Sollwerten, Auslesen von Daten möglich...
  - Protokoll-Implementierung in Industrie-Komponenten fehlerhaft: 40% getesteter Geräte stürzen bei Standard-Protokoll-Tests ab
- Gängige Sicherungsmaßnahmen aus Office-IT im Prozess-Umfeld oft nicht anwendbar
  - Rahmenbedingungen stark unterschiedlich
  - Schwerpunkte wie Verfügbarkeit, Echtzeit-Anforderungen, Determinismus usw. nicht hinreichend berücksichtigt
  - Geregelte IT-Betriebsprozesse häufig nicht vorhanden

Angriff auf die Leittechnik – Stuxnet und die Konsequenzen

- Rückblick:
  - Funktionsweise und Schadfunktion des Stuxnet-Wurms
- Derzeitiger Stand
  - Systeme gepatcht - Lücken geschlossen?
  - Aktuelle Schwachstellen in der Prozessleittechnik
  - Gefährdung durch Nachahmungstäter
- **Ausblick**
  - **Konsequenzen und Anforderungen an Leittechnik-Betreiber und Hersteller**

Forderungen an Hersteller und Dienstleister

- Fundamentaler Paradigmenwechsel: Sichere Systemarchitektur und Umsetzung grundlegender Sicherheitsprinzipien
- Berücksichtigung von Sicherheitsanforderungen im gesamten Entwicklungsprozess
  - Integration von Sicherheitstests in Entwicklung und Freigabeprozesse
- Härtung von Applikationen und Basiskomponenten
  - Betriebssysteme, Datenbanken, Anwendungsserver, etc.
- Einsatz/Entwicklung gesicherter Netzwerkprotokolle
  - In Weiterverkehrsnetzen (z.B. Fernwirkprotokolle), aber auch in Anlagen-internen Netzen
  - Erweiterung der Standardprotokolle um Sicherheitsfunktionen wie Authentisierung und Verschlüsselung
- Umsetzung sicherer Wartungs- und Parametrier-/Programmierprozesse
  - Insbesondere für Fernwartung / Remote Access

Forderungen an Hersteller und Dienstleister

- Unterstützung eines angemessenen Schadsoftwareschutzes
  - Insbesondere müssen die Prozesse im Betrieb realistisch umsetzbar sein.
  - Bisherige Verfahren fordern häufig eine Validierung der einzelnen Pattern-Updates an einem dedizierten Testsystem.
  - Hierdurch sind zeitnahe Updates und ein aktueller Virenschutz nicht realistisch.
  - Ggf. können moderne Verfahren wie „Application Whitelisting" traditionelle Scan-Software auf kritischen Kernkomponenten eines Leitsystems ersetzen.

- Unterstützung eines hinreichenden Patchmanagements
  - Prüfung und Freigabe von Patches von Betriebssystem und Drittkomponenten (Datenbank, Hilfsapplikationen)
  - Ermöglichung von Patches mit minimierten Auswirkung auf die Betriebsprozesse, z.B. Parallelinstallation auf Redundanzkomponenten, automatisierte Backupprozesse, integrierte Unterstützung eines Rollbacks
  - Unterstützung von Testprozessen: Integration von Testprozeduren in Anwendungen

Grundlegende Maßnahmen auf Betreiberseite

- Formulierung konkreter Sicherheitsanforderungen bei Neubeschaffungen und in Ausschreibungen, z.B. anhand anerkannter Branchenrichtlinien
  - BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“
  - WIB-Richtlinie “Process control Domain: security requirements for vendors”
- Prüfung der Umsetzung im Rahmen des Abnahmetests

- Sicherung aller Schnittstellen zu externen Systemen
  - Büroumgebung, Partnerunternehmen, Standortvernetzung
  - Segmentierung von Prozessnetzen, z.B. nach Teilanlagen
  - Automatisierte Schadsoftwareprüfung in Schnittstellensystemen
  - Implementierung sicherer Fernwartungslösungen

- Absicherung mobiler Komponenten wie Programmiergeräte und Parametrier-Laptops
  - Härtung, Patchmanagement, Schadsoftwareschutz, ...

Grundlegende Maßnahmen auf Betreiberseite

- Umsetzung von geregelten und auf Sicherheit ausgerichteten IT-Betriebsprozessen für Leittechnik und unterstützende IT-Systeme
  - Service- und Wartungsprozesse
  - Change- und Releasemanagement
  - Definierte Test- und Freigabeverfahren
  - Monitoring, Logging, Überwachung
- Umsetzung einer Sicherheitsorganisation
  - Definition von Rollen und Verantwortlichkeiten für Sicherheitsprozesse
- Aufbau eines an die Prozesstechnik angepassten Informations-sicherheitsmanagementsystems (ISMS) nach anerkannten Normen
  - ISO/IEC 27001
  - ISA SP99 (derzeit noch im Entwurf)

Fragen & Antworten