GAI NetConsult GmbH— Am Borsigturm 58 — 13507 Berlin — www.gai-netconsult.de — Tel: 030/417898-0

Tanzende Affen und andere Schwachstellen in SIMATIC S7-Steuerungen

Dr. Stephan Beirer (GAI NetConsult GmbH)

August 2011 Sonderdruck aus Security *Journal* #56

Im Sommer 2010 schreckte der Stuxnet-Angriff auf Siemens SIMATIC-Prozessleittechnik sowohl Leittechnik-Betreiber als auch Systemhersteller auf und löste eine intensive Diskussion über das Sicherheitsniveau im sog. SCADA-Umfeld aus [1]. Eine Vielzahl von kürzlich identifizierten weiteren Schwachstellen in Siemens S7 Steuerungskomponenten machen neuerlich klar, dass die Sicherheitsprobleme in der Prozessleittechnik keineswegs nur auf die dort eingesetzten PC-basierten Komponenten beschränkt sind, sondern dass es sich vielmehr um eine grundlegende Problematik handelt, die ein generelles Umdenken erfordern.

Anfang August fand in Las Vegas die Black Hat 2011 statt, eine der weltweit größten und bekanntesten Security Konferenzen, die jedes Jahr mehrere Tausend Sicherheitsexperten und Hacker anzieht. Traditionell wurde auch die diesjährige Konferenz wieder genutzt, um Schwachstellen in verschiedenen Produkten und Technologien aufzudecken und öffentlich vorzuführen. Mit besonderer Spannung wurde hierbei der Vortrag von Dillon Beresford erwartet, einem Sicherheitsexperten des US-amerikanischen Security-Dienstleisters NSS Lab. Beresford hatte den Stuxnet-Vorfall zum Anlass genommen, um sich bei eBay mehrere SIMATIC S7-Steuerungskomponeten des Herstellers Siemens zu beschaffen und sie einem umfassenden Sicherheitstest zu unterziehen. Dabei identifizierte er auf Anhieb eine ganze Reihe verschiedener Schwachstellen, die er auf der Black Hat zum ersten Mal der breiten Öffentlichkeit präsentierte.

SIMATIC S7 ist die Siemens-Produktfamilie sog. Speicherprogrammierbarer Steuerungen (SPSen). Diese Automatisierungskomponenten werden weltweit in zahlreichen Branchen zur Steuerung und Überwachung von verfahrenstechnischen und Produktions-Prozessen eingesetzt, beispielsweise in den Bereichen Gas- und Erdölindustrie, Chemie und Pharma, Nahrungs- und Genussmittel sowie in der Energieerzeugung, insbesondere im konventionellen Kraftwerksumfeld.

Abbildung-1: Easter-Egg: Bild tanzender Affen (Quelle: S7-300)

Schwachstellen-Zoo

Beresford identifizierte im Rahmen seiner Untersuchungen eine Vielzahl von verschiedenen Schwachstellen, die alle relevanten Modelle der S7-SPS-Familie betreffen, d.h. die S7-200, -300, -400 und S7-1200 Komponenten. Da die einzelnen Sicherheitslücken teilweise nur in bestimmten Modell- oder Firmware-Versionen nachgewiesen wurden und bisher noch keine hinreichenden offiziellen Informationen von Seiten des Systemherstellers Siemens zur Verfügung stehen, ist eine Bestimmung der genauen Anzahl der Lücken sowie eine Zuordnung zu den verschiedenen S7-Versionen derzeit nicht möglich. Im Folgenden werden die zurzeit bekannten Informationen zu den einzelnen Sicherheitslücken nach Schwachstellentypen zusammengefasst und klassifiziert:

- **Backdoor-Zugang**
  In verschiedenen Firmware-Versionen der S7-300 SPS existiert ein fest einprogrammierter, nicht deaktivierbarer und undokumentierter Standard-Nutzeraccount, dessen Passwort nicht geändert werden kann. Über diesen Nutzer lässt sich mittels Telnet- und HTTP-Zugang u.a. der Speicher der SPS auslesen und gegebenenfalls auch manipulieren. Desweiteren lässt sich mit diesem Account laut Angaben von Dillon Beresford eine Debugging-Shell aktivieren, über die weitreichende Manipulationen möglich sind.

Die Zugangsdaten für den Backdoor-Zugang finden sich bereits an diversen Stellen im Internet.

- **Verschiedene DoS-Schwachstellen**
  Dillon Beresford präsentierte eine ganze Reihe von Sicherheitslücken, mit denen sich S7-SPSen über das Netzwerk zum Absturz bringen lassen (sog. DoS- oder Denial-of-Service-Schwachstellen). Dies ist für Automatisierungskomponenten eine besonders kritische Schwachstellekategorie, da hierdurch der durch die SPS gesteuerte physikalische Prozess unter Umständen in einen unkontrollierten Zustand geraten kann. Unter anderem lassen sich diese Schwachstellen durch wiederholtes Senden von Start/Stop-Kommandos und durch Netzwerk-Zugriffe auf ungültige Speicheradressen auslösen. Die SPS kann dann nur durch einen Reboot (Kaltstart) vor Ort wieder neu gestartet werden. Für die S7-1200 wurde eine weitere DoS-Schwachstelle im integrierten Webserver identifiziert, durch die die Steuerung durch häufige Netzwerkanfragen ebenfalls zum Absturz bzw. in den STOP-Zustand gebracht werden kann.

- **Nutzung unsicherer Netzwerkprotokolle**
  S7-SPSen nutzen zur Netzwerkkommunikation auf Layer 4 (Transport-Ebene) das standardisierte ISO-TSAP-Protokoll nach RFC 1006. Darauf aufbauend wird auf Applikationsebene (Layer 7) das sog. S7-Protokoll genutzt, ein proprietäres Industrieprotokoll, das ebenso wie das unterlagerte ISO-TSAP keine hinreichenden Sicherheitsmechanismen bietet. Über das S7-Protokoll ist es deshalb möglich den Speicher der SPS auszulesen und zu beschreiben, ebenso können beliebige Befehle an die SPS gesendet werden. Hierüber können bei einem Netzwerkzugriff auf die Automatisierungskomponenten unter anderem die SPS-Ausgänge und damit der gesteuerte Prozess beliebig manipuliert werden, ebenso kann die Programmierung der SPS unbefugt geändert werden.

- **Ineffektiver Authentisierungsmechanismus**
  Siemens hat bestimmte über das S7-ISO-TSAP-Protokoll realisierte Funktionsaufrufe und Netzwerkbefehle mit einem Passwort-Schutz versehen. Dieser Schutzmechanismus – der in der Regel in Produktivumgebungen nicht aktiviert ist - ist aus mehreren Gründen völlig ineffektiv realisiert. Zunächst lässt sich der Schutz durch eine sog. Replay-Attacke leicht aushebeln. Hierzu muss ein Angreifer nur einen per Passwort gesicherten, beliebigen Funktionsaufruf mitschneiden - anschließend kann der mitgelesene Passwort-Hash zur Ausführung beliebiger anderer Befehle „ wiederverwendet " werden. Desweiteren sind offenbar nicht alle über das Netzwerk ausführbare Befehle geschützt, insbesondere erfolgen die besonders kritischen Schreibzugriffe aus nicht nachvollziehbaren Gründen ungesichert – somit kann der Speicher der SPS – und damit auch der physikalische Prozess - auch ohne Passwortkenntnis nahezu beliebig manipuliert werden. Besonders pikant ist dabei, dass sich hierdurch auch der Passwortschutz selbst ohne Authentisierung deaktivieren lässt. Ebenso kann so ein neues Passwort gesetzt werden – anschließend ist der Zugriff auf die SPS nur noch eingeschränkt möglich. Dies könnte in vielen Umgebungen zu kritischen Betriebszuständen und schweren Störungen führen, wenn z.B. ein übergeordnetes Leitsystem keine Befehle mehr an eine SPS senden kann.

- **Easter-Egg**
  In verschiedenen S7-300 Firmware-Versionen wurde ein sog. Easter-Egg entdeckt: es handelt sich hierbei um ein Bild tanzender Affen, das offensichtlich einer der Entwickler als Scherz im Firmware-Code hinterlassen hatte (Abbildung-1). Während dieses Bild vermutlich keine direkte Sicherheitslücke darstellt, wird hierdurch die Effektivität der in der Entwicklung angewandten Qualitätsmanagement-Prozesse in Frage gestellt.

Grundlegende Problematik

Insbesondere zu den Schwachstellen, die auf der Nutzung des unsichereren S7-TSAP-Protokolls beruhen muss angemerkt werden, dass in Fachkreisen bereits seit längerem bekannt ist, dass sich die gängigen Automatisierungs- und Leittechnikkomponenten bei einem Netzwerkzugriff so wie oben geschildert nahezu beliebig manipulieren lassen. In der Regel werden im Umfeld der Leit- und Automatisierungstechnik generell Protokolle ohne sichere Authentisierungsverfahren eingesetzt. Diese grundsätzliche Problematik trifft dabei nicht nur für Siemens-Komponenten, sondern für die Mehrzahl der derzeit am Markt verfügbaren Systeme zu.

Bisher waren diese Designschwächen allerdings der breiten Öffentlichkeit nicht im Detail bekannt. Ebenso waren die für eine Ausnutzung der Sicherheitslücken notwendigen Tools nicht frei verfügbar. Dillon Beresford stellte während seines Black-Hat -Vortrags allerdings auch sogenannte Exploit-Module für das Angriffs- und Sicherheitstesttool Metasploit vor. Er wird diese nach eigenen Angaben derzeit noch nicht veröffentlichen, um

den Systemanwendern Gelegenheit zu geben, sich besser zu schützen. Allerdings sind die jetzt bekannten Informationen bereits ausreichend, um die Schwachstellen nachstellen zu können oder entsprechenden Angriffscode zu programmieren. Weitreichendes Fachwissen über Leit- und Automatisierungstechnik ist dafür nicht erforderlich.

Als generelle Maßnahmenempfehlung an Betreiber von SIMATIC-Komponenten gelten derzeit weiterhin die generell für alle Prozesskomponenten anzuwendenden üblichen Sicherheitsregeln, die strikt eingehalten werden sollten: die Komponenten dürfen nur in vertrauenswürdigen, strikt isolierten und gut geschützten Netzwerken betrieben werden, ebenso dürfen alle Wartungs- und Parametrierzugriffe vor Ort und aus der Ferne nur über vertrauenswürdige und nach Stand der Technik gesicherte Systeme erfolgen. Nach Erscheinen etwaiger Siemens-Sicherheitspatches sollte die Installation im Rahmen der Risikobewertungsprozesse individuell geprüft werden.

Verbesserungswürdige Informationspolitik

Besonders kritisiert wird derzeit die offizielle Informationspolitik von Siemens. Dazu muss zunächst angemerkt werden, dass Dillon Beresford verschiedene der jetzt gezeigten Schwachstellen ursprünglich bereits im Mai auf einer anderen Sicherheitskonferenz vorstellen wollte. Nach einer Intervention des amerikanischen Departments of Homeland Security und von Siemens sagte er diesen Vortrag ab. Nach eigenen Angaben stellte Beresford Siemens umfangreiche Informationen zu den einzelnen Schwachstellen sowie Exploit-Code zur Verfügung.

Anstatt die Problematik durch eine offensive Informationspolitik anzugehen, versuchen die zuständigen Siemensverantwortlichen offenbar seit Mai die Probleme totzuschweigen oder zumindest kleinzureden. So wurde zunächst die Existenz oder Ausnutzbarkeit verschiedener Schwachstellen verneint, bis Dillon Beresford durch entsprechende Veröffentlichungen das Gegenteil bewies. Alle bisher durch Siemens veröffentlichen Informationen und Stellungnahmen sind generell äußerst vage gehalten und gehen dabei überhaupt auch nur auf einige wenige der oben genannten Schwachstellen ein [2,3]. Auch mehr als zwei Wochen nach der Veröffentlichung der Sicherheitslücken auf der Black Hat gibt es zur Mehrzahl der Schwachstellen wie den DoS-Problemen oder den unsicheren Netzwerkprotokollen immer noch keine offiziellen Siemens-Aussagen, insbesondere in Bezug auf ihre Risikobewertung, die betroffenen Modelle oder Firmware-Versionen oder zu geplanten Patches.

Fazit

Nach dem Stuxnet-Vorfall wurde durch Dillon Beresfords Black-Hat-Präsentation erneut das derzeitige (Un-)Sicherheitsniveau in aktueller Leit- und Automatisierungstechnik vorgeführt. Im Gegensatz zum Stuxnet-Angriff, dessen Tiefe und Komplexität nahelegen, dass hier staatliche Organisationen mit einem entsprechend hohen Ressourceneinsatz involviert waren, wurde diesmal mehr als deutlich, dass weitreichende Angriffe gegen Prozesssteuerungstechnik auch mit einfachen Mitteln und mit klassischen „Hacker-Methoden" realisiert werden können [4].

Besonders kritisch ist hierbei, dass es sich bei mehreren der aufgezeigten kritischen Sicherheitslücken nicht um simple Programmier- oder Implementierungsfehler handelt, die sich durch ein einfaches Software- oder Firmwareupdate beheben lassen werden. Vielmehr sind die Grundursache Mängel im generellen Systemdesign der gesamten Leit- und Automatisierungstechnik, die sich nur durch eine umfassende Überarbeitung beseitigen lassen werden. Dies dürfte vermutlich erst in einer der kommenden System-Generationen realisierbar sein. Ebenso ist davon auszugehen, dass die Systeme anderer Hersteller von ähnlichen Schwachstellen betroffen sind. Die Hacker-Community und andere „Interessierte" sind durch Beresfords Analyse vermutlich hinreichend motiviert worden auch diese Komponenten einer umfassenden Überprüfung zu unterziehen, sobald sie ihrer habhaft werden können.

Referenzen

[1] S. Beirer, „Wurmangriffe und Hintertüren: Aktuelle Sicherheitsbedrohungen in der Prozessleittechnik", Security *Journal* #50, GAI NetConsult GmbH
[2] Siemens-1
[3] Siemens-2
[4] S. Beirer, „Stuxnet – Lessons learned? Angriff auf die Leittechnik", ew - das magazin für die energie wirtschaft 1-2/2011