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

Stuxnet – Lessons learned?

Dr. Stephan Beirer (GAI NetConsult GmbH)

Februar 2011 Sonderdruck aus Security *Journal* #53

Stuxnet, eine Schadsoftware, die gezielt Siemens PCS7 Prozesssteuerungssysteme angreift, hat in den letzten Monaten viel Aufsehen erregt. Inzwischen ist klar, dass das Schadprogramm zum Angriff auf eine bestimmte, eng umrissene Zielumgebung programmiert wurde und dass für alle übrigen PCS7-Anwender keine akute Gefahr besteht. Es stellt sich allerdings die Frage, welche langfristigen Folgen der Stuxnet-Vorfall für die Informationssicherheit in modernen Leittechniksystemen haben wird und welche Schutzmaßnahmen die Betreiber solcher Systeme zukünftig ergreifen sollten. Der folgende Artikel ist die überarbeitete Fassung einer Veröffentlichung im „ew – das magazin für die energie wirtschaft" 1-2/2011.

Als im Juni 2010 bekannt wurde, dass wieder einmal eine neue Windows-Schadsoftware entdeckt worden war, schien diese Meldung zunächst keinen besonderen Nachrichtenwert aufzuweisen. Erst als die ersten Analysen zeigten, dass der Wurm – inzwischen „Stuxnet" getauft – offenbar gezielt bestimmte Prozesssteuerungssysteme des Herstellers Siemens angreift, wurden die wenigen Experten, die sich weltweit mit der IT-Sicherheitsproblematik im Leittechnik-Umfeld beschäftigen, schnell hellhörig [1]. Im Laufe der Wochen wurden durch die Untersuchungen von Sicherheitsbehörden und unabhängigen Experten mehr und mehr beängstigende Details des Schadsoftware-Angriffs aufgedeckt, über die inzwischen auch in den Massenmedien berichtet und in der Öffentlichkeit intensiv diskutiert wurde.

Gezielter Angriff auf die Leittechnik

Stuxnet muss als der erste öffentlich bekanntgewordene gezielt auf Prozesssteuerungsumgebungen ausgerichtete Schadsoftwareangriff angesehen werden. Ziel war es offenbar, ein ganz bestimmtes Siemens PCS7 Steuerungssystem so zu manipulieren, dass der von der Leittechnik gesteuerte physikalische Prozess im Sinne des Angreifers gestört wird. Die Siemens PCS7-Leittechnik ist generell weit verbreitet und wird zur Steuerung und Überwachung verfahrenstechnischer Prozesse in zahlreichen Branchen eingesetzt, beispielsweise in den Bereichen Gas - und Erdölindustrie, Chemie und Pharma, Nahrungs- und Genussmittel sowie in der Energieerzeugung, insbesondere im konventionellen Kraftwerksumfeld

Der Wurm nutzt für seinen Angriff eine Vielzahl von teilweise bis dahin unbekannten Sicherheitslücken aus. Ein Teil dieser Schwachstellen betrifft dabei die in Leittechniksystemen häufig für Engineering, Datenhaltung und Bedien- und Beobachtungsfunktionen eingesetzten Microsoft Windows Komponenten. Andere Schwachstellen sind PCS7-spezifisch und betreffen die Datenbank des Prozessleitsystems und die den physikalischen Prozess überwachenden und steuernden S7-Automatisierungskomponenten. Stuxnet nutzt die Windows-Schwachstellen vorrangig, um sich zwischen Rechnersystemen weiter zu verbreiten und das Zielsystem zu infizieren. Hervorzuheben ist hier insbesondere eine bis dahin unbekannte Lücke, mit deren Hilfe er sich bis zu seiner Entdeckung im Juni 2010 unbemerkt über Wechseldatenträger wie USB-Sticks oder mobile Festplatten verbreiten konnte. Dies ist insbesondere für Angriffe auf Prozesstechniksysteme relevant, da diese häufig weitgehend isoliert betrieben werden und deshalb Angriffe über öffentliche Netze, Web- oder Mailnutzung wenig erfolgversprechend sind. Dahingegen ist die Übertragung von Daten oder Programmcode per USB-Stick in Prozessumgebungen weitaus häufiger anzutreffen. Nach einer erfolgreichen Infektion prüft der Wurm die Programmierung der Automatisierungskomponenten auf ganz bestimmte Speicherinhalte und versucht so, sein Zielsystem zu identifizieren. Falls diese Prüfung erfolgreich ist – und nur dann – ändert Stuxnet die Programmierung der Steuerungen so, dass der überwachte Prozess manipuliert wird. Besonders perfide ist hierbei, dass der Wurm die veränderte Programmierung mit sog. Rootkit-Methoden verbirgt, so dass die Manipulationen auf infizierten Programmier- und Bediensystemen für den Nutzer gar nicht erkennbar sind.

Die Ersteller von Stuxnet, die den Wurm vermutlich bereits im Juni 2009 entwickelten, verfügen offensichtlich über ein sehr tiefes und gleichzeitig breitgefächertes Know-how im Bereich aktueller Schadsoftware- und Angriffstechnologien, kennen sich aber auch mit modernen Prozessleitsystemen und deren Sicherheitslücken erstaunlich gut aus. Der Aufwand, der für diesen Angriff betrieben wurde, muss enorm gewesen sein – allein schon deshalb ist davon auszugehen, dass es sich hierbei um das Werk von Geheimdiensten oder ähnlichen Regierungsorganisationen handeln dürfte. Als potentielle Ziele von Stuxnet werden derzeit insbesondere zwei Anlagen im Iran gehandelt: die Urananreichungszentrifugen des iranischen Atomprogramms, sowie das Kernkraftwerk Bushehr.

© GAI NetConsult GmbH Nachdruck nur mit Genehmigung des Herausgebers

Bild 1: Die moderne Leittechnik rückt verstärkt in den Fokus von Hackern und Computerkriminellen

Gefahr gebannt?

Inzwischen sind verschiedene Sicherheitsupdates und Patches von Microsoft und Siemens verfügbar, die die von Stuxnet genutzten Sicherheitslücken schließen bzw. eine Infektion verhindern sollen. Ebenso wird der Wurm von allen relevanten Virenscannern erkannt und blockiert. Laut Angaben des PCS7-Herstellers Siemens ist es auf Grund der Selektivität des Wurms selbst bei einer akuten Infektion eines PCS7-Systems sehr unwahrscheinlich, dass der konkrete industrielle Prozess wirklich manipuliert wird. Ebenso scheint eine rückwirkungsfreie Entfernung der Schadsoftware möglich. Auch auf Grund der – im Vergleich zu anderen Computerwürmern – relativ geringen Anzahl von Infektionen scheint deshalb die Gefahr derzeit gebannt. Es stellt sich allerdings die Frage, welche längerfristigen Folgen der Vorfall für Betreiber von Prozesssteuerungs- und Leittechnik haben wird – insbesondere auch für solche, die sich nicht als mögliches Ziel eines gezielten, mit hohem Aufwand durchgeführten Angriffs sehen.

Dass auch in aktueller Leittechnik eine Vielzahl von Sicherheitslücken und Designschwachstellen vorhanden sind und dass das Sicherheitsniveau der hier eingesetzten Technik im Vergleich zur „klassischen" IT-Welt in Büro- und Rechenzentren um Jahre bis Jahrzehnte hinterherhinkt, ist eine kaum zu leugnende Tatsache. Auch wenn Sicherheitsvorfälle in diesen Bereichen in der Regel nicht öffentlich gemacht werden, sind Systemausfälle auf Grund von Schadsoftwarebefall, Netzwerkstörungen oder Fehlparametrierungen ein in Fachkreisen seit langem diskutiertes Thema. Durch Stuxnet wurde die Problematik jetzt auch einer breiten Öffentlichkeit bekannt, insbesondere rückt die Prozesstechnik damit als lohnendes Angriffsziel stärker in den Fokus der klassischen IT-Security-Szene aber auch von Computerkriminellen. Es ist bereits zu beobachten, dass seit dem Bekanntwerden von Stuxnet im Internet auf einschlägigen Webseiten, in Hacker-Foren und IT-Sicherheits-Blogs die Thematik der sog. SCADA Security intensiver diskutiert wird. Alleine im Oktober wurden im Internet durch Unbekannte zwei weitere Schwachstellen für in Leittechnikumgebungen eingesetzte Software samt der zugehörigen Angriffsprogramme publiziert. Kurz danach veröffent-

© GAI NetConsult GmbH Nachdruck nur mit Genehmigung des Herausgebers

lichte das auch für den Bereich der Kritischen Infrastrukturen zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI) eine offizielle Warnung zu einer in Hackerkreisen gerne genutzten Schwachstellensuchmaschine, über die sich auch im Internet zugängliche Leit- und Automatisierungskomponenten finden lassen.

Gefahr von Nachahmungstätern

Besonders problematisch ist zunächst, dass die konkreten, von Stuxnet in der PCS7-Prozessleittechnik ausgenutzten Schwachstellen durch die Analysen verschiedener Experten jetzt in weitreichender Detailtiefe bekannt sind. Der Stuxnet-Programmcode kann zudem frei im Internet heruntergeladen werden. Ein mäßig begabter Schadsoftwareprogrammierer dürfte keine Schwierigkeiten haben, den Code durch sog. Reverse-Engineering zu analysieren und somit auch die ausgenutzten PCS7-Schwachstellen genau zu verstehen. Hierbei muss insbesondere betont werden, dass die von Siemens veröffentlichten Sicherheitspatches nur kleinere Änderungen am PCS7-System vornehmen, um eine Infektion mit dem Stuxnet-Wurm zu verhindern. Um die eigentlichen Schwachstellen – wie die Verwendung von fest programmierten Standardpasswörten oder die weitgehend ungehärtete Datenbankinstallation – zu beheben sind so weitreichende Änderungen notwendig, dass diese vermutlich frühestens im Zuge der Veröffentlichung einer neuen PCS7-Version vorgenommen werden können. Andere Schwachstellen, die der Wurm z.B. ausnutzt, um die Programmierung der Automatisierungskomponenten unbemerkt zu modifizieren oder das Prozessabbild in Steuerungskomponente zu manipulieren, sind nicht einmal klassische Programmierfehler, die mit einem Update behoben werden könnten – vielmehr handelt sich hier um grundlegende Designprinzipien, die nicht ohne Weiteres abgeändert werden können. Eine modifizierte Stuxnet-Variante könnte deshalb auch eine mit aktuellen Siemens-Patches versehene PCS7-Leittechnik erfolgreich angreifen.

Generell betrifft die Problematik keineswegs nur Betreiber von Siemens-basierter Leittechnik. Viele der von Stuxnet genutzten Schwachstellen wie ungesicherte Parametrier- bzw. Programmierschnittstellen sind prinzipiell auch in der Leit- und Automatisierungstechnik anderer Hersteller vorhanden und leicht ausnutzbar. Für einen Angriff müssten die Programmroutinen lediglich auf das jeweilige Ziel angepasst werden. Für eine Vielzahl von Angriffen, insbesondere wenn es allein um die Störung des Prozesses geht, ist nicht einmal spezifisches Fachwissen über die angegriffene Umgebung notwendig.

Es ist davon auszugehen, dass zukünftig auch gewöhnliche Kriminelle vermehrt versuchen werden, Sicherheitsschwachstellen im Leittechnikumfeld für Angriffe auszunutzen – sei es zur Wirtschaftsspionage, für Erpressungen oder zur Schädigung von Unternehmen. Solche Angriffe werden insbesondere auch dadurch erleichtert, dass die IT-Umgebungen im Prozesstechnikbereich nur schwer auf einem aktuellen Sicherheitsniveau gehalten werden können. So ist es in Produktivumgebungen beispielsweise kaum möglich Sicherheitsupdates für Betriebssysteme und Anwendungsprogramme zeitnah und im Monatszyklus einzuspielen. Ebenso können Schutzprogramme wie Virenscanner oft schon aus technischen Gründen nicht eingesetzt werden. Aufgrund der häufig fehlenden Unterstützung durch die Leittechniklieferanten sind die Anlagenbetreiber teilweise auch gezwungen, veraltete Betriebssysteme einzusetzen. Da diese von den Betriebssystemherstellern nicht mehr unterstützt und mit Sicherheitspatches versorgt werden, können aktuelle Sicherheitslücken hier dann gar nicht mehr behoben werden. Prinzipiell bietet Siemens hier in Bezug auf aktuelle PCS7-Umgebungen schon eine sehr gute Unterstützung: So werden Betriebssystemupdates zeitnah getestet und freigegeben sowie verschiedene Virenscanprodukte auf den Bedien- und Programmiersystemen unterstützt – allerdings müssen wir immer wieder feststellen, dass diese von Siemens empfohlenen Maßnahmen [2] von den Integratoren nicht umgesetzt werden. Auch die zunehmende, durchaus notwendige und sinnvolle Vernetzung mit den Büroumgebungen, die Nutzung von Fernwartungszugängen oder der Einsatz von Fremdhardware in Prozesstechnikumgebungen erhöht das Risiko für einen erfolgreichen Angriff signifikant.

Umdenken notwendig

Es ist offensichtlich, dass sich sowohl die System- und Komponentenhersteller als auch die Anlagenbetreiber in Zukunft bedeutend intensiver mit der Informationssicherheitsproblematik auseinandersetzen müssen. Hersteller, Lieferanten und Integratoren müssen zunächst ihre Systeme nach Stand der Technik und entsprechend ihrem hohen Schutzbedarf absichern. Das oft noch so praktizierte „Inselprinzip", nach dem die Prozessdatennetze als isolierte Welt betrachtet werden und ein Schutz nur am Netzübergang, z.B. durch Firewalls, stattfindet, ist heute so nicht mehr zeitgemäß. Allein schon durch die Vielzahl an Komponenten innerhalb der Prozessnetze und die vielfältigen Wechselwirkungen mit externen Systemen stellen diese mittlerweile keine abgeschlossene „Inselwelt" mehr dar. Auch lassen sich die zahlreichen und häufig komplexen externen Schnittstellen nicht allein durch einfache Firewalls sichern. Generell müssen Leittechniksysteme auch intern ein hohes Sicherheitsniveau aufweisen. Die leider immer noch viel zu häufig anzutreffenden „Altlasten" wie Standard-Passworte und unsichere Kommunikationsdienste müssen eliminiert und durch eine grundlegend sichere und robuste Systemarchitektur ersetzt werden. Insbesondere sind die Hersteller dazu aufgerufen, Lösungen für die zahlreichen Herausforderungen zu finden, die die Anlagenbe-

© GAI NetConsult GmbH Nachdruck nur mit Genehmigung des Herausgebers

treiber bei der Aufrechterhaltung eines dauerhaft sicheren Leittechnikbetriebs meistern müssen, beispielsweise im Bereich des Patchmanagements und bei der Nutzer- und Rechteverwaltung. Die derzeitige Technik bietet hierzu leider kaum praktikable Lösungen.

Auch auf Betreiber- und Anwenderseite besteht noch Handlungsbedarf, da die Sicherheitsproblematik nicht allein auf Herstellerseite gelöst werden kann. So müssen bei Neubeschaffungen konkrete Sicherheitsanforderungen explizit ausformuliert werden. Der einfache Hinweis, nach dem das System "sicher" sein muss, ist im Hinblick auf die komplexe Thematik in der Regel nicht ausreichend. Hilfreich kann dabei z.B. eine Ausarbeitung konkreter Anforderungen anhand des BDEW-Whitepapers „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme" [3] oder auf Basis des WIB-Dokuments „Process control Domain: security requirements for vendors V2.0" [4] sein. Ebenso muss die Prüfung auf Erfüllung von Sicherheitsanforderungen integraler Bestandteil von Abnahmetests werden. Auch in Bestandssystemen sollten in regelmäßigen Abständen Sicherheitsprüfungen durchgeführt werden, insbesondere nach relevanten Systemänderungen. Hierbei ist natürlich zu beachten, dass technische Tests niemals in Produktivumgebungen, sondern ausschließlich an vom physikalischen Prozess isolierten Testsystemen durchgeführt werden dürfen.

Durch individuell angepasste technische Maßnahmen müssen die Betreiber alle Schnittstellen zu externen Netzen und Systemen absichern, um eine bestmögliche Abschottung der sensiblen Prozesstechniksysteme sicherstellen zu können. Dies betrifft neben direkten Netzwerkanbindungen insbesondere mobile Programmier- und Parametriersysteme, die auch in externen Umgebungen wie dem Büronetz genutzt werden. Allerdings müssen neben rein technischen Maßnahmen in Zukunft auch verstärkt personelle und organisatorische Aspekte berücksichtigt werden. Da die IT-Sicherheitsproblematik nicht allein durch Technik gelöst werden kann, muss das Management der Informationssicherheit im Prozesstechnikumfeld in den betrieblichen Prozessen und in der Organisation integriert werden. Hierzu gehören beispielsweise auf Sicherheit ausgelegte Betriebs-, Service- und Wartungsprozesse, in denen die relevanten Managementaufgaben wie Änderungs- Release- und Störungsmanagement berücksichtigt sind. Ebenso müssen Verantwortlichkeiten und Rollen im Bezug auf die Informationssicherheit klar definiert sein. Hierfür ist der Aufbau eines Informationssicherheitsmanagementsystems (ISMS), beispielsweise nach der anerkannten Norm ISO 27001 auch im Prozesstechnikbereich hilfreich.

Die **GAI NetConsult GmbH** konzentriert sich als System- und Beratungshaus auf die Planung und Realisierung von sicheren eBusiness Lösungen. Dabei wird der gesamte Prozess von der Analyse über die Konzeption und Realisierung bis zur Überwachung angeboten.

WEITERE INFORMATIONEN

EIN SERVICE DER

GAI NetConsult

FÜR IHR ABONNEMENT BESUCHEN SIE BITTE UNSERE WEB-SEITE

www.gai-netconsult.de/

Referenzen /Links

[1] S. Beirer, „Aktuelle Sicherheitsbedrohungen in der Prozessleittechnik", Security *Journal* 50, 08/2010

[2] Siemens „Sicherheitskonzept PCS 7 Empfehlungen und Hinweise" **Mehr...**

[3] BDEW Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme" Mehr...

[4] WIB International Instrument Users' Association „Process control Domain: security requirements for vendors V2.0" http://www.wib.nl/download.html